М. П. Минеев, В. Н. Чубариков

ЛЕКЦИИ ПО АРИФМЕТИЧЕСКИМ ВОПРОСАМ КРИПТОГРАФИИ

Москва
2010

УДК 511

Минеев М. П., Чубариков В. Н.

Лекции по арифметическим вопросам криптографии. — М.: Изд-во «Попечительский совет Механико-математического факультета МГУ им. М. В. Ломоносова», 2010. — 186 с.

Книга является учебным пособием по арифметическим приложениям к криптографии. В её основу положены лекции по специальному курсу и занятия специального семинара, проводимые авторами на механико-математическом факультете МГУ имени М. В. Ломоносова.

В учебном пособии дан новый подход к изложению некоторых понятий и методов.

Для студентов университетов, педагогических вузов и вузов с углубленным изучением математики.

УДК 511

ПРЕДИСЛОВИЕ

Еще в начале 60-х годов XX столетия криптография использовалась исключительно для обеспечения безопасности военной и дипломатической связи, а также для целей разведывательной и контрразведывательной служб. Это требовало и требует высочайшего уровня развития криптографической науки и техники. Малейшее пренебрежение здесь может привести к тяжелейшим последствиям.

Так, гибель русских армий Самсонова и Ренненкампфа в 1914 году произошла во многом по причине, что действующие в то время шифры не смогли скрыть статистику открытого текста.

Во второй мировой войне "советская шифровальная служба в основном учла опыт своей российской предшественницы времен первой мировой войны". Известный специалист в области истории криптографии Д. Кан [19] писал: "Немецкая радиоразведка против Советского Союза была малоэффективной. В стратегическом отношении она вообще не имела ни одного сколько-нибудь заметного успеха. Немцы оказались не в состоянии вскрыть шифрсистемы, применявшиеся для засекречивания переписки высшего советского командования... Явная неспособность немецких криптографов вскрыть советские стратегические шифрсистемы, с помощью которых засекречивалась самая важная информация, вынудила одного немецкого криптографа признать, что, хотя Россия и проиграла первую мировую войну в эфире, во время второй мировой войны она сумела взять реванш за свое поражение...

Шифрпереписка советских разведчиков не поддавалась дешифрованию. Большинство из них использовало стандартную для советской агентуры того времени шифрсистему, которая была триумфом шифровальной техники. Она представляла собой доведенную до совершенства старую систему, применявшуюся русскими революционерами, и объединяла в себе шифр равнозначной замены с одноразовой гаммой...

В период "холодной войны" русские сумели вскрыть шифры американского посольства в Москве. Такие подвиги свидетельствуют об их осведомленности, базирующейся на глубоком понимании шифровального дела и криптоанализа".

Широкое распространение компьютеров, бурное развитие информационных технологий и внедрение автоматизированных методов и средств обработки информации практически во все сферы человече-

ской деятельности в 60-х годах привели к необходимости массового использования криптографических средств и постановке новых задач защиты информации в цифровой форме. В частности, А. Н. Колмогоров [23] ввел понятие "битовой" сложности для последовательностей, составленных из нулей и единиц, и понятие сложности выполнения арифметических операций над натуральными числами. До сих пор остается нерешенной проблема А. Н. Колмогорова о том, что операция умножения двух многозначных чисел сложнее операции сложения их. В 1961 г. А. А. Карацуба [20] доказал замечательную теорему о том, что два n-значных натуральных числа можно перемножить не за $O(n^2)$ битовых операций, как в "школьном" способе умножения чисел в столбик, а за число операций $O(n^\alpha)$, где $\alpha = \log_2 3 \approx 1,585\ldots$. Эта теорема положила начало совершенно новому направлению в вычислительной математике — теории быстрых вычислений.

Приведем основные вехи дальнейшего развития криптографии как науки, включающей в себя математические методы, относящиеся к аспектам защиты информации, как-то: сохранение информационных секретов от несанкционированных пользователей; обеспечение неизменности информации при несанкционированном воздействии различного рода неизвестных средств; идентификация пользователей, компьютерных терминалов, кредитных карт и др.; подтверждение источника информации или достоверности оригинала; обеспечение средствами, которые давали возможность связать полученную информацию с конкретным пользователем ("подпись"); ограничение доступа к ресурсам привилегированных пользователей; указание временных границ построения и существования той или иной информации; подтверждение получения информации; подтверждение легальности права на использование и преобразование информации пользователем; анонимность пользователя, включенного в некоторый процесс работы с информацией; предотвращение отрицания или отказа от предыдущих обязательств или действий пользователя; лишение пользователя санкции на использование информации.

В 1976 г. специалисты из Стэнфордского университета Диффи, Хэллман и Мёркль [14] сделали выдающееся открытие. Они ввели понятие открытого ключа и нашли новый изобретательный метод обмена ключами по открытому каналу связи, основанный на сложности нахождения значений функции "дискретный логарифм".

В 1978 г. Ривест, Шамир и Адлеман [39] дали первый практический способ шифрования с открытым ключом, получивший в дальнейшем название RSA-метода, а также новую схему построения циф-

ровой подписи. Их метод шифрования полагался на сложность разложения натуральных чисел на простые сомножители.

В 1985 г. Эль-Гамаль [16] получил новый класс систем шифрования с открытым ключом, основанный на сложности нахождения дискретного логарифма.

В 1991 г. был принят первый международный стандарт цифровой подписи (ISO/IEC 9796), в основе которого лежал метод RSA. В 1991 г. правительство США приняло стандарт цифровой подписи FIPS 186 на основе схемы Эль Гамаля, а в 1994 г. был принят российский государственный стандарт ГОСТ Р34.10-94, полагающийся также на вариацию схемы цифровой подписи Эль Гамаля.

Отметим, что к настоящему времени в криптографии сложились следующие основные математические средства работы: схемы шифрования, хэш-функции и схемы цифровой подписи.

Указанные цели, задачи и средства криптографии потребовали введения новых и развития старых теоретико-числовых методов.

Перейдем к описанию содержания настоящей книги.

Первая глава является введением в криптографию. Здесь дано понятие информации, ее кодирование и сформулированы основные задачи теории кодирования. Далее вводится понятие алфавитного кодирования. Рассматриваются коды Шеннона и Гилберта–Мура. Затем уточняются задачи о помехоустойчивости, об увеличении скорости передачи информации, о защите информации. Наконец, обсуждаются понятия симметричных и асимметричных шифров.

Во второй главе изучаются свойства префиксных кодов, доказывается неравенство Крафта – МакМиллана и выводится теорема о минимальной длине префиксного кода.

Третья глава посвящена конечным полям и циклическим кодам.

В четвертой главе исследуются рекуррентные соотношения и производящие функции. В частности, рассматриваются последовательность Фибоначчи, линейные рекуррентные уравнения второго и произвольного порядка. Особому изучению подвергнуты рекуррентные соотношения первого порядка в кольцах вычетов и рекуррентные соотношения произвольного порядка в конечных полях.

В пятой главе предлагается новый арифметический подход к искажению знаков в шифрах простой замены и Виженера. В частности, приведены методы искажения знаков в шифре простой замены с помощью извлечения корня квадратного и возведения в квадрат, а также комбинированный метод искажения частот появления знаков в шифре простой замены. Дан анализ методов искажения знаков в шифре простой замены. Найдено применение китайской теоремы

об остатках к шифру Виженера и получен арифметический вариант шифра Виженера.

В шестой главе изучаются асимметричные шифры. Вводится понятие однонаправленной функции. Решается задача “об укладке рюкзака” и дается ее применение к системе шифрования. Разбирается система RSA шифрования с открытым ключом. Рассмотрен интересный пример криптографической хэш-функции.

Наконец, седьмая глава называется “Задачи теории чисел”. Все задачи распределены по следующим разделам: квадратичные вычеты и невычеты по простому модулю, символ Лежандра; извлечение квадратного корня из числа по простому модулю; символ Якоби; извлечение квадратного корня из числа по составному модулю; целая часть квадратного корня из натурального числа; символ Кронекера; простейшие теоремы о распределении простых чисел; распознавание простых и составных чисел; непрерывные (цепные) дроби, критерий Лежандра для подходящих дробей; арифметика квадратичных полей, метод Лемера распознавания простых чисел; разложение вещественных квадратичных иррациональностей в непрерывную дробь, теорема Эйлера – Лагранжа; разложение квадратного корня из натурального числа в непрерывную дробь; вычисление основной единицы вещественного квадратичного поля; теорема П. Л. Чебышёва о попадании простых чисел в интервалы (постулат Бертрана); алгебраическое приложение: группы, коммутативные кольца, многочлены, поля, поля частных, конечные поля.

Настоящая книга является учебным пособием по некоторым приложениям теории чисел к криптографии. Она возникла из специального курса лекций и специального семинара, которые авторы вели в течение ряда лет для студентов-математиков механико-математического факультета Московского государственного университета имени М. В. Ломоносова. Это объясняет то, что книга состоит из двух частей: теоретической и задачника по теории чисел. Все задачи в ней даются с полными решениями.

Мы не пытались описать арифметические приложения криптографии во всей их полноте и общности, а ставили перед собой задачу “научить учиться” на некоторых конкретных проблемах криптографии.

Благодарим наших коллег, аспирантов и студентов за поддержку, критические замечания и требовательность к нашей работе.

М. П. Минеев, В. Н. Чубариков

Глава I

ВВЕДЕНИЕ

§ 1. Понятие информации и ее кодирование

Важнейшей причиной возрастания интереса к теории чисел в последнее время явилось мощное развитие вычислительной техники и методов хранения, обработки, передачи, извлечения, классификации и оценки качества информации.

Будем предполагать, что всякая информация находится на некотором носителе и представляет собой некоторое сообщение. Преобразование этого сообщения для получения (выделения) тех или иных свойств информации называется *кодированием.* Например, носителем информации является сообщение с помощью букв некоторого алфавита, азбуки, цифр и других символов.

Существо методов кодирования можно пояснить на примере азбуки Морзе. В ней буквы латинского и кириллического алфавитов заменяются наборами из "точек" и "тире", которые можно передавать с помощью телеграфного аппарата. Приведем таблицу соответствия букв этих алфавитов символам в азбуке Морзе.

А	A	·–	K	K	– · –	Ф	F	· · –·
Б	B	– · ··	Л	L	· – ··	Х	H	· · ··
В	W	· – –	М	M	––	Ц	C	– · –·
Г	G	– – ·	Н	N	–·	Ч		– – –·
Д	D	– · ·	О	O	– – –	Ш		– – ––
Е	E	·	П	P	· – –·	Щ	Q	– – ·–
Ж	V	· · ·–	Р	R	· – ·	Ъ,Ь	X	– · ·–
З	Z	– – ··	С	C	· · ·	Ы	Y	– · ––
И	I	··	Т	T	–	Ю		· · ––
Й	J	· – ––	У	U	· · –	Я		· – ·–

Кстати отметим, что азбука Морзе при передаче сообщения предполагает использование знака пробела между буквами, словами и предложениями, который обычно достаточно часто встречается в нем. С другой стороны, с помощью двух знаков 0 и 1 можно представить алфавит из 32 букв, не требующий обозначения пробела между буквами при передаче сообщения. Для этого достаточно рассмотреть 32

двоичных слова длины 5:

$$(00000),\ (00001),\ (00010),\ \ldots\ ,(11111).$$

Далее все сообщения будут представлены в дискретном виде, т.е. в виде последовательности букв конечного алфавита. Запись информации с помощью букв (символов) этого алфавита задает кодирование информации. Другие примеры кодирования доставляют, например, запись натурального числа в некоторой позиционной системе счисления, изображение точки в многомерном пространстве декартовыми координатами и т.д.

Необходимость передачи информации и ее преобразования повлекла за собой разработку современной теории кодирования (обеспечение помехоустойчивости при передаче сообщений по каналам связи, увеличение скорости передачи информации) и теории защиты информации (криптография). Можно предположить, что на передачу каждого символа алфавита требуется одинаковое время. Тогда увеличение скорости передачи сообщения может произойти за счет уменьшения длины закодированного сообщения, что приводит к понятию оптимального кодирования. В 1948 г. К. Шеннон [48] дал полное решение задачи о возможности передачи информации при заданном качестве с использованием оптимальных методов кодирования и декодирования.

Эти лекции, в основном, посвящены методам кодирования и декодирования информации. В частности, будем рассматривать один из видов кодирования — шифрование сообщения, обеспечивающее практическую невозможность его восстановления (дешифрования) незаконными пользователями в течение некоторого данного временного промежутка.

К настоящему моменту известны два вида шифрования — симметричное и открытое (асимметричное). При симметричном шифровании законные пользователи снабжаются секретными ключами, с помощью которых они осуществляют зашифрование и расшифрование сообщения. Незаконному пользователю эти ключи неизвестны, что является препятствием для него дешифровать шифртекст. В 70-е годы прошлого века в работе Диффи и Хеллмана [14] появился второй вид шифрования, называемый открытым шифрованием, которое не требует секретного распределения ключей. Новым элементом открытого шифрования является использование односторонней функции, вычисление значений которой достаточно просто, но вычисление значений обратной функции без знания некоторого “секрета” представляет собой весьма трудную задачу. Во введении

мы описываем одну из систем открытого шифрования — систему Ривеста–Шамира–Адлемана (систему RSA) [39].

Еще одной разновидностью открытого шифрования являются методы выработки общего открытого ключа законными пользователями для большого их числа с помощью обмена сообщениями по открытому каналу связи. В частности, с этой целью в [46] построена группа, образованная рациональными точками эллиптической кривой, определенной над некоторым подполем конечного поля. Открытое шифрование создало возможности для использования его для построения цифровой подписи, систем идентификации, систем распределения ключей, методов разделения секретов, технологии хэш-функций, криптографических протоколов (см., например, [1], [46]).

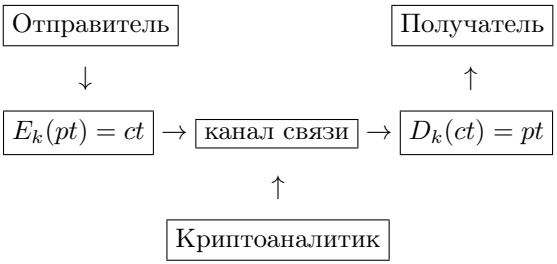
§ 2. Основные задачи теории кодирования

Простейшая схема передачи сообщения (исходного текста, информации) имеет вид

В частности, отметим,что под помехами понимают и несанкционированный доступ к информации.

Отправитель может как-то изменить *исходный текст* или зашифровать его, т.е. получить *криптотекст* или *криптограмму.* Часто криптотекст имеет возможность противостоять помехам, хотя он может посылаться и по ненадежному или по *открытому каналу связи.* Получатель расшифровывает криптотекст и получает исходное сообщение. Процесс шифрования исходного текста иногда называется *кодированием,* а процесс расшифрования криптотекста *декодированием.* Заметим, что стойкость методов кодирования при современном массовом их использовании, т.е. степень невозможности прочтения исходного текста, полученного из канала связи в виде криптотекста, зависит, как правило, от некоторой небольшой информации, имеющейся у отправителя и получателя ее (быть может, различной) и называющейся *ключами* рассматриваемой криптосистемы.

Пусть pt обозначает открытый текст, $ct = E_k(pt)$ — кодированный текст, $D_k(ct) = pt$ — декодированный текст, и элемент k принадлежит $\mathcal{K}$ — некоторому *"пространству ключей".* Тогда процесс передачи информации можно представить более подробной схемой



Среди основных задач теории кодирования находятся следующие.

1) Обеспечение *помехоустойчивости* при передаче информации по каналам связи. Отметим, что информация при прохождении по каналу связи может искажаться, поэтому ставится задача после приема ее абонентом восстановление истинной информации.

2) Увеличение *скорости передачи сообщений* по каналам связи, в частности, передача сообщений с помощью возможно меньшего количества символов.

3) *Защита информации* от несанкционированного доступа при хранении и передаче ее по каналам связи, нахождение критериев надежности криптографических систем.

§ 3. Алфавитное кодирование

Алфавит A представляет собой конечный набор символов (букв, знаков) $(a_1, a_2, \ldots, a_r)$, $r \geqslant 1$. Конечный набор букв (возможно с повторением) из A называется *словом в алфавите* A. Множество всех слов в алфавите A обозначим символом $S(A)$. Пусть задан другой алфавит $B = \{b_1, b_2, \ldots, b_s\}, s \geqslant 1$ и $S(B)$ — множество его слов. Рассмотрим непустые подмножества M в $S(A)$ и C в $S(B)$. Отображение $\mathcal{F}\colon M \to C$ называется *кодированием,* при этом слова из множества M называются *сообщениями,* а их образы в C — *кодами сообщений* из M, кроме того, A называется *алфавитом сообщений,* а B — *кодирующим алфавитом.* Кодирование $\mathcal{F}$ (или код C) называется *взаимно однозначным* или *однозначно декодируемым,* если каждое кодовое сообщение из C имеет ровно одно сообщение из M в качестве прообраза отображения $\mathcal{F}$.

Пусть задано отображение Σ букв алфавита A в множество $S(B)$, т.е. $\Sigma\colon a_k \to B_k$, $k = 1, \ldots, r$. Определим кодирование $\mathcal{F}_\Sigma\colon S(A) \to S(B)$, удовлетворяющее следующим условиям

1) $\mathcal{F}_\Sigma(a_k) = B_k$, $k = 1, \ldots, r$;

2) $\mathcal{F}_\Sigma(a_{k_1} a_{k_2} \ldots a_{k_s}) = B_{k_1} B_{k_2} \ldots B_{k_s}$, $1 \leqslant k_1, k_2, \ldots, k_s \leqslant r$, $s \geqslant 1$;

где под произведением слов B_kB_l понимается приписывание слова B_l справа к слову B_k. Отображение $\mathcal{F}_\Sigma$ называется *алфавитным кодированием, задаваемым схемой* Σ. Множество кодовых слов $\{B_1, B_2, \ldots, B_r\}$ обозначается символом $C(\Sigma)$ и называется *кодом алфавита* A *в схеме* Σ.

Вопрос об однозначном декодировании кодового сообщения является принципиально важным. Суть его поясним на примерах.

Пример 1. Пусть $A = \{a_1, a_2, a_3\}$ и $B = \{b_1, b_2\}$. Пусть, также, задана схема Σ алфавитного кодирования вида:

$$\Sigma : a_1 \to b_1, a_2 \to b_2, a_3 \to b_2b_2.$$

Тогда слово $a_1a_2a_3$ кодируется словом $b_1b_2b_2b_2$, которое нельзя однозначно декодировать. Если в кодовом слове расставить скобки следующим образом $(b_1)(b_2)(b_2)(b_2), (b_1)(b_2)(b_2b_2), (b_1)(b_2b_2)(b_2)$, то соответствующее сообщение будет иметь вид $a_1a_2a_2a_2, a_1a_2a_3$ или $a_1a_3a_2$.

Пример 2. Пусть $A = \{a_1, a_2\}, B = \{b_1, b_2\}$ и

$$\Sigma : a_1 \to b_1, a_2 \to b_1b_2.$$

Эта схема кодирования задает однозначное декодирование кодового сообщения (слова) C. Действительно, перед каждой буквой b_2 в сообщении C находится буква b_1. Это позволяет выделить всевозможные пары b_1b_2 в сообщении C. Оставшаяся часть сообщения C будет состоять из букв b_1. Далее заменим каждую из выделенных пар b_1b_2 на букву a_2 алфавита A, а каждую из оставшихся букв b_1 на букву a_1. Получим открытое сообщение, являющееся прообразом сообщения C.

Например, пусть задано кодовое сообщение C вида $b_1b_1b_2b_1b_2b_1b_1b_1b_2$. Выделим в нем все пары b_1b_2. Найдем $b_1(b_1b_2)(b_1b_2)b_1b_1(b_1b_2)$. Следовательно, открытое сообщение имеет вид $a_1a_2a_2a_1a_1a_2$.

Докажем теперь достаточный признак однозначного декодирования кодового сообщения.

Пусть сообщение C имеет вид $C'C''$. Тогда C' называется префиксом или началом сообщения C, а C'' — суффиксом или концом сообщения C. Пустое (не содержащее букв алфавита B) сообщение и само сообщение C будем считать началом и концом сообщения C. Начала и концы сообщения C, отличные от пустого и самого сообщения C, называются собственными префиксами и соответственно собственными суффиксами сообщения C.

Пусть, как и раньше, для любой буквы a_k, $k = 1, \ldots, r$ из алфавита A задано отображение $\mathcal{F}_\Sigma(a_k) = B_k$ и $C(\Sigma) = \{B_1, \ldots, B_r\}$.

Говорят, что схема Σ обладает свойством префикса, если ни одно слово из $C(\Sigma)$ не является префиксом никакого другого слова из $C(\Sigma)$. Например, пусть заданы алфавиты $A = \{a_1, a_2, a_3, a_4\}$ и $B = \{0, 1\}$. Определим схему Σ, как отображение $\mathcal{F}_\Sigma(a_k) = B_k$, $k = 1, \ldots, 4$, где $B_1 = 0$, $B_2 = 10$, $B_3 = 110$, $B_4 = 111$. Тогда эта схема Σ обладает свойством префикса.

Утверждение. *Пусть схема Σ обладает свойством префикса. Тогда алфавитное кодирование по этой схеме обладает однозначным декодированием.*

▷ Будем рассуждать от противного. Пусть при кодировании $\mathcal{F}_\Sigma\colon S(A) \to S(B)$ слово C не имеет однозначного декодирования, т.е.

$$C = \mathcal{F}_\Sigma(a_{k_1} a_{k_2} \ldots a_{k_s}) = B_{k_1} B_{k_2} \ldots B_{k_s},\ 1 \leqslant k_1, k_2, \ldots, k_s \leqslant r,\ s \geqslant 1;$$

$$C = \mathcal{F}_\Sigma(a_{l_1} a_{l_2} \ldots a_{l_t}) = B_{l_1} B_{l_2} \ldots B_{l_t},\ 1 \leqslant l_1, l_2, \ldots, l_t \leqslant r,\ t \geqslant 1.$$

Так как слова $a_{k_1} a_{k_2} \ldots a_{k_s}$ и $a_{l_1} a_{l_2} \ldots a_{l_t}$ различны, то при некотором $n, 1 \leqslant n \leqslant r$, имеем $a_{k_1} = a_{l_1}, \ldots, a_{k_{n-1}} = a_{l_{n-1}}, a_{k_n} \neq a_{l_n}$. Следовательно, $B_{k_1} = B_{l_1}, \ldots, B_{k_{n-1}} = B_{l_{n-1}}, B_{k_n} \neq B_{l_n}$. Поскольку последние слова представляют одно и то же слово C, одно из слов B_{k_n} или B_{l_n} является префиксом другого, что противоречит свойству префикса для схемы Σ. ◁

Пример 2 показывает, что свойство префикса для схемы Σ не является необходимым для однозначного декодирования сообщения.

Пример 3. Важной задачей алфавитного кодирования является построение кода с минимальной средней длиной. Пусть задан алфавит $A = (a_1, \ldots, a_m)$ и известны соответствующие вероятности $p_1, \ldots, p_m$ появления букв из алфавита A в открытом тексте. Пусть буквы алфавита A занумерованы по убыванию вероятностей, т.е. $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_m$. Далее вводятся величины Q_s, называемые кумулятивными вероятностями, следующим образом

$$Q_1 = 0, \ldots, Q_s = \sum_{k=1}^{s-1} p_k, \quad s = 2, \ldots, m.$$

Построим код Шеннона. Кодовым словом b_s в нем, отвечающим букве $a_s, s = 1, \ldots, m$, является двоичная последовательность, представляющая собой первые $l_s = [-\log_2 p_s] + 1$ знаков после запятой в двоичной записи числа Q_s.

Покажем, что код Шеннона является префиксным. При $r > s$

имеем

$$Q_r - Q_s = \sum_{k=s}^{r-1} p_k \geqslant p_s.$$

По построению кода Шеннона длина l_s кодового слова b_s удовлетворяет неравенству

$$l_s = [-\log_2 p_s] + 1 > -\log_2 p_s.$$

Следовательно, $p_s > 2^{-l_s}$. Отсюда получим

$$Q_r - Q_s = \sum_{k=s}^{r-1} p_k \geqslant p_s > 2^{-l_s}.$$

Это означает, что кодовое слово b_s не является префиксом слова b_r. Тем самым, код Шеннона будет префиксным. Оценим среднюю длину кодовых слов. Получим

$$\bar{l} = \sum_{s=1}^{m} p_s l_s = \sum_{s=1}^{m} p_s([-\log_2 p_s] + 1) \leqslant H(p) + 1,\ \bar{l} > H(p).$$

где $H(p) = -\sum\limits_{s=1}^{m} p_s \log_2 p_s$.

Пример 4. Код Шеннона требует упорядочения букв алфавита по частоте их появления в тексте. Построим префиксный код Гилберта – Мура, в котором это требование отсутствует.

Пусть, как и раньше, величины Q_s являются кумулятивными вероятностями и определяются следующим образом

$$Q_1 = 0, \ldots, Q_s = \sum_{k=1}^{s-1} p_k, \quad s = 2, \ldots, m.$$

Вычислим величины $\sigma_s = Q_s + p_s/2$, $s = 1, 2, 3, \ldots, m$. Кодовым словом b_s в коде Гилберта – Мура, отвечающим букве a_s, $s = 1, \ldots, m$, является двоичная последовательность, представляющая собой первые $l_s = [-\log_2 (p_s/2)] + 1$ знаков после запятой в двоичной записи числа σ_s.

Покажем, что код Гилберта – Мура является префиксным. При $r > s$ имеем

$$\sigma_r - \sigma_s = \sum_{k=s}^{r-1} p_k + \frac{p_r - p_s}{2} \geqslant p_s + \frac{p_r - p_s}{2} = \frac{p_r + p_s}{2} \geqslant \frac{\max\{p_r, p_s\}}{2}.$$

По построению кода Гилберта – Мура длина l_s кодового слова b_s, отвечающего букве a_s, удовлетворяет неравенству

$$l_s = [-\log_2 (p_s/2)] + 1 > -\log_2 (p_s/2).$$

Следовательно, $p_s/2 > 2^{-l_s}$. Отсюда получим

$$\sigma_r - \sigma_s = \sum_{k=s}^{r-1} p_k \geqslant \frac{\max\{p_r, p_s\}}{2} \geqslant 2^{-\min\{l_r, l_s\}}.$$

Это означает, что кодовое слово b_s не является префиксом слова b_r, и наоборот. Тем самым, код Гилберта – Мура будет префиксным. Оценим теперь среднюю длину кодовых слов. Получим

$$\bar{l} = \sum_{s=1}^{m} p_s l_s = \sum_{s=1}^{m} p_s([-\log_2(p_s/2)] + 1) \leqslant H(p) + 2,\ \bar{l} > H(p) + 1.$$

где $H(p) = -\sum\limits_{s=1}^{m} p_s \log_2 p_s$.

§ 4. О помехоустойчивости

Поясним задачу обеспечения помехоустойчивости при передаче сообщения по каналу связи на конкретном примере.

Пусть задан алфавит сообщений $A = \{a_1, a_2, \ldots, a_{32}\}$ и кодирующий алфавит $B = \{0, 1\}$. Определим кодирование следующей схемой Σ вида

$$\Sigma : a_k \to \bar{\varepsilon}^{(k)} = (\varepsilon_1^{(k)}, \varepsilon_2^{(k)}, \varepsilon_3^{(k)}, \varepsilon_4^{(k)} \varepsilon_5^{(k)}), \quad \varepsilon_j^{(k)} = 0; 1,$$

причем $k = 1, 2, \ldots, 32; j = 1, \ldots, 5$.

Таким образом код алфавита A в схеме Σ состоит из 32 векторов в пространстве размерности 5, координатами которых являются числа 0 и 1.

Расстояние между двумя кодовыми словами определяется как число несовпадающих соответствующих их координат (*расстояние Хэмминга*). Пусть $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)})$ обозначает указанное выше число несовпадающих координат векторов $\bar{\varepsilon}^{(k)}$ и $\bar{\varepsilon}^{(m)}$. Тогда находим $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)}) = \sum\limits_{i=1}^{5} |\varepsilon_i^{(k)} - \varepsilon_i^{(m)}|$. Отсюда имеем, что выполняются следующие три свойства расстояния:

а) для любых $1 \leqslant k, m \leqslant 32$ имеем $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)}) \geqslant 0$, кроме того, $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)}) = 0$ тогда и только тогда, когда $\bar{\varepsilon}^{(k)} = \bar{\varepsilon}^{(m)}$ (неотрицательность);

б) для любых $1 \leqslant k, m \leqslant 32$ имеем $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)}) = \rho(\bar{\varepsilon}^{(m)}, \bar{\varepsilon}^{(k)})$ (симметричность);

в) для любых $1 \leqslant k, l, m \leqslant 32$ имеем $\rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(m)}) \leqslant \rho(\bar{\varepsilon}^{(k)}, \bar{\varepsilon}^{(l)}) + \rho(\bar{\varepsilon}^{(l)}, \bar{\varepsilon}^{(m)})$ (неравенство треугольника).

Свойства а) и б) очевидны. Свойство в) следует из цепочки соот-

ношений

$$\rho(\bar{\varepsilon}^{(k)},\bar{\varepsilon}^{(m)})=\sum_{i=1}^{5}|\varepsilon_i^{(k)}-\varepsilon_i^{(m)}|=\sum_{i=1}^{5}|\varepsilon_i^{(k)}-\varepsilon_i^{(l)}+\varepsilon_i^{(l)}-\varepsilon_i^{(m)}|\leqslant$$

$$\leqslant\sum_{i=1}^{5}|\varepsilon_i^{(k)}-\varepsilon_i^{(l)}|+\sum_{i=1}^{5}|\varepsilon_i^{(l)}-\varepsilon_i^{(m)}|=\rho(\bar{\varepsilon}^{(k)},\bar{\varepsilon}^{(l)})+\rho(\bar{\varepsilon}^{(l)},\bar{\varepsilon}^{(m)}).$$

Рассмотрим следующий пример.

Пусть отправителю и получателю сообщений известно, что послана информация длины $5n$, в которую могут входить общим числом $n\geqslant 1$ только четыре следующих сообщения

$$\bar{a}=(1,1,0,0,0),\ \bar{b}=(0,0,1,1,0),\ \bar{c}=(1,0,0,1,1),\ \bar{d}=(0,1,1,0,1).$$

Пусть также получателю известно, что во время передачи сообщения могла произойти ошибка не более, чем одной координаты в каждом из n векторов.

Покажем, что указанного рода ошибки можно исправить.

Действительно, расстояние Хэмминга между любыми двумя из векторов $\bar{a},\bar{b},\bar{c}$ и $\bar{d}$ не меньше, чем 3. Рассмотрим шары $B_{\bar{a}},B_{\bar{b}},B_{\bar{c}},B_{\bar{d}}$ радиуса 1 с центрами соответственно в точках $\bar{a},\bar{b},\bar{c}$ и $\bar{d}$. Эти шары состоят только из точек

$$\begin{aligned}
B_{\bar{a}}=\ &\{11000,\ 11001,\ 11010,\ 11100,\ 10000,\ 01000\},\\
B_{\bar{b}}=\ &\{00110,\ 00111,\ 00100,\ 00010,\ 01110,\ 10110\},\\
B_{\bar{c}}=\ &\{10011,\ 10010,\ 10001,\ 10111,\ 11011,\ 00011\},\\
B_{\bar{d}}=\ &\{01101,\ 01100,\ 01111,\ 01001,\ 00101,\ 11101\}.
\end{aligned}$$

Построенные шары не пересекаются. Предположим противное. Пусть точка $\bar{\varepsilon}=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4,\varepsilon_5)$ принадлежит указанным выше шарам $B_{\bar{x}}$ и $B_{\bar{y}}$. Тогда по неравенству треугольника имеем

$$3\leqslant\rho(\bar{x},\bar{y})\leqslant\rho(\bar{x},\bar{\varepsilon})+\rho(\bar{\varepsilon},\bar{y})\leqslant 1+1=2.$$

Это неравенство противоречиво. Следовательно, шары $B_{\bar{a}},B_{\bar{b}},B_{\bar{c}},B_{\bar{d}}$ не пересекаются.

Таким образом, если получен вектор $\bar{\delta}$, то его принадлежность одному из указанных четырех шаров определяет искомое кодовое слово как центр этого шара.

Возникает вопрос: как избежать перебора всех векторов размерности 5, координатами которых являются либо 0, либо 1, при построении четырех векторов $\bar{\varepsilon}^{(s)}=(\varepsilon_1^{(s)},\varepsilon_2^{(s)},\varepsilon_3^{(s)},\varepsilon_4^{(s)},\varepsilon_5^{(s)})$, $s=1,2,3,4$, таких, чтобы для них выполнялось условие $\rho(\bar{\varepsilon}^{(s)},\bar{\varepsilon}^{(t)})\geqslant 3$ при $s\neq t$. Пусть ε_k, $r=1,2$, принимает одно из значений 0 или 1. Тогда опре-

делим функцию $\chi(\varepsilon_1, \varepsilon_2)$ следующим образом

$$\chi(0,0) = \chi(1,1) = 0,\ \chi(0,1) = \chi(1,0) = 1.$$

Рассмотрим векторы X вида $X = (\varepsilon_1, \varepsilon_2, \varepsilon_1, \varepsilon_2, \chi(\varepsilon_1, \varepsilon_2))$, где $\varepsilon_k,\ k = 1, 2$, принимает одно из значений 0 или 1. Векторов X будет ровно 4. Покажем, что расстояние между двумя различными векторами из них не меньше, чем 3. Рассмотрим два различных вектора $X = X(\varepsilon_1, \varepsilon_2) = (\varepsilon_1, \varepsilon_2, \varepsilon_1, \varepsilon_2, \chi(\varepsilon_1, \varepsilon_2))$ и $X' = X'(\varepsilon_1', \varepsilon_2') = (\varepsilon_1', \varepsilon_2', \varepsilon_1', \varepsilon_2', \chi(\varepsilon_1', \varepsilon_2'))$. Покажем, что $\rho(X, X') \geqslant 3$. Очевидно, что $(\varepsilon_1, \varepsilon_2) \neq (\varepsilon_1', \varepsilon_2')$. Возможны только три следующих случая. Имеем а) $\varepsilon_1 \neq \varepsilon_1',\ \varepsilon_2 \neq \varepsilon_2'$, тогда из определения расстояния находим $\rho(X, X') = 4$; б) $\varepsilon_1 = \varepsilon_1',\ \varepsilon_2 \neq \varepsilon_2'$, тогда из определения расстояния получим $\rho(X, X') = 3$; в) $\varepsilon_1 \neq \varepsilon_1',\ \varepsilon_2 = \varepsilon_2'$, тогда $\rho(X, X') = 3$.

Следовательно, имеем $\rho(X, X') \geqslant 3$.

В заключение параграфа приведем другое доказательство неравенства треугольника. Рассмотрим множество M векторов $\bar{x} = (x_1, x_2, \ldots, x_n)$ с целочисленными координатами, принимающими значения от 0 до $l - 1$. Неотрицательное целое число $\rho(\bar{x}, \bar{y})$, указывающее число мест, на которых находятся различные компоненты векторов $\bar{x}$ и $\bar{y}$, удовлетворяет всем свойствам расстояния. Свойства неотрицательности и симметричности функции ρ очевидны. Докажем неравенство треугольника для функции ρ. Рассмотрим любые три вектора $\bar{x}, \bar{y}$ и $\bar{z}$. Разместим их друг под другом так, чтобы координаты с одинаковыми номерами находились в одном столбце. Перемена мест столбцов не меняет значение функции ρ. Если у двух векторов координаты с одинаковыми номерами i не совпадают, то будем обозначать их так: $\omega_i, \bar{\omega}_i$. Пусть $\rho(\bar{x}, \bar{y}) = k$. Поменяем координатные столбцы для векторов $\bar{x}, \bar{y}, \bar{z}$ так, что получилась следующая таблица

$$\bar{x} = (x_1, x_2, \ldots, x_{m_1}, x_{m_1+1}, \ldots, x_k, x_{k+1}, \ldots, x_{k+m_2}, x_{k+m_2+1}, \ldots, x_n),$$

$$\bar{y} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{m_1}, \bar{x}_{m_1+1}, \ldots, \bar{x}_k, x_{k+1}, \ldots, x_{k+m_2}, x_{k+m_2+1}, \ldots, x_n),$$

$$\bar{z} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{m_1}, x_{m_1+1}, \ldots, x_k, \bar{x}_{k+1}, \ldots, \bar{x}_{k+m_2}, x_{k+m_2+1}, \ldots, x_n).$$

Имеем $\rho(\bar{x}, \bar{z}) = m_1 + m_2,\ \rho(\bar{z}, \bar{y}) = k - m_1 + m_2$, причем $m_1 \leqslant k,\ m_2 \leqslant n - k$. Таким образом находим

$$\rho(\bar{x}, \bar{z}) + \rho(\bar{z}, \bar{y}) = m_1 + m_2 + k - m_1 + m_2 = k + 2m_2 \geqslant k = \rho(\bar{x}, \bar{y}).$$

Тем самым установлено неравенство треугольника для функции ρ.

§ 5. Об увеличении скорости передачи информации

Пример сжатия информации и увеличения скорости передачи сообщений доставляет азбука Морзе. Кодирующий алфавит этой азбуки состоит из двух букв: точки и тире. Алфавит открытого сообщения состоит из 30 букв кириллицы. Для построения схемы алфавитного кодирования можно было обойтись тридцатью пятиразрядными двоичными словами. Однако для кодирования каждой буквы кириллической азбуки используются кодовые слова различной длины, не превосходящей 4.

Поясним суть данного эффекта на известном простом примере. Суть его такова [3, с. 18–22]. Пусть задана информация, составленная из четырех сообщений A_1, A_2, A_3, A_4, некоторой длины и вероятности их появления в тексте равны $P(A_1) = 1/2$, $P(A_2) = 1/4$, $P(A_3) = P(A_4) = 1/8$.

Указанные сообщения можно закодировать двоичными словами длины 2 следующим образом:

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ 00 & 01 & 10 & 11 \end{pmatrix}.$$

Данное кодирование не учитывает вероятностей появления сообщений. Расположим указанные сообщения в порядке убывания их вероятностей. Разобьем заданную информацию сообщений на две приблизительно равновероятные группы. Первой группе сопоставим символ 0, второй группе — символ 1. Указанный процесс продолжим аналогичным образом. Результаты сведем в таблицу

$$\begin{array}{llllll} A_1 & 1/2 & 0 & & & \\ A_2 & 1/4 & 1 & 0 & & \\ A_3 & 1/8 & 1 & 1 & 0 & \\ A_4 & 1/8 & 1 & 1 & 1 & \end{array}$$

Таким образом получено следующее кодирование сообщений:

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ 0 & 10 & 110 & 111 \end{pmatrix}.$$

Пусть требуется передать текст из 1000 сообщений A_k, $k = 1, 2, 3, 4$. Тогда согласно распределению вероятностей в данном тексте будет примерно ≈ 500 сообщений A_1 запись их потребует $\approx 500 \times 1$ символов, ≈ 250 сообщений A_2 и $\approx 250 \times 2$ символов, ≈ 125 сообщений A_3

и $\approx 125 \times 3$ символов и, наконец, ≈ 125 сообщений A_4 и $\approx 125 \times 3$ символов. Таким образом указанный способ кодирования потребует $\approx 500 \times 1 + 250 \times 2 + 125 \times 3 + 125 \times 3 = 1750$ символов и средняя длина кодового слова $\approx 1{,}75$ символа.

С другой стороны, способ кодирования, не учитывающий вероятности сообщений, более точно, рассматривающий равномерное распределение сообщений A_1, A_2, A_3, A_4 в тексте из 1000 слов, требует для кодирования информации $1000 \times 2 = 2000$ символов и средняя длина кодового слова равна 2.

Следовательно, учет вероятностей появления тех или иных символов при кодировании приводит к более экономному и эффективному коду Фано. Отметим также, что код Фано обладает свойством префикса.

Приведем еще один пример кода Фано. Пусть алфавит сообщения состоит из восьми букв. Каждая буква сообщения встречается со следующими вероятностями:

$$P(a_1) = 0{,}3, \quad P(a_2) = P(a_3) = P(a_4) = 0{,}15,$$
$$P(a_5) = P(a_6) = P(a_7) = 0{,}07, \quad P(a_8) = 0{,}04.$$

Кодирующий алфавит состоит из трех символов $\{0, 1, 2\}$. Расположим буквы в порядке убывания вероятностей в сообщении. Затем все буквы алфавита разбиваем на три группы с приблизительно одинаковой вероятностью их появления в сообщении. Кодирование производим следующим образом. В первую группу попала одна буква a_1. Ее кодируем символом 0. Каждую букву второй группы — a_2, a_3 — кодируем символом 1. Буквы a_4, a_5, a_6, a_7, a_8, попавшие в третью группу, кодируем символом 2. Далее с получившимися группами поступаем аналогичным образом. Первая группа, состоящая из одной буквы, из дальнейшего кодирования исключается. Во второй группе букве a_2 присваиваем следующий кодовый символ 0, а букве a_3 — символ 1, и прекращаем кодирование букв второй группы. Третью группу букв разбиваем на три подгруппы $\{a_4\}, \{a_5, a_6\}$ и $\{a_7, a_8\}$ с приблизительно равными вероятностями. Буквам первой подгруппы присваиваем кодовый символ 0, буквам второй — символ 1, наконец, буквам третьей подгруппы — символ 2. Дальнейшее кодирование букв первой подгруппы не производим. Во второй подгруппе букве a_5 присваиваем кодовый символ 0, а букве a_6 — символ 1. Наконец, в третьей подгруппе букве a_7 присваиваем кодовый символ 0, а букве a_8 — символ 1. Имеем таблицу

алфавит	вероятность	кодов. символ			кодов. слово
a_1	0,3	0			0
a_2	0,15	1	0		10
a_3	0,15	1	1		11
a_4	0,15	2	0		20
a_5	0,07	2	1	0	210
a_6	0,07	2	1	1	211
a_7	0,07	2	2	0	220
a_8	0,04	2	2	1	221

Из построения этого кода Фано видно, что он обладает свойством префикса.

§ 6. О защите информации

Сначала определим основные понятия криптографии: открытого текста, шифра. Нам понадобится математическая модель алгебраической системы шифра (шифросистемы), предложенная в основных чертах К. Шенноном.

Информация защищается с помощью процедуры *шифрования,* использующей обратимое преобразование. Выбор этого преобразования для зашифровки данных сообщения осуществляется из некоторого множества обратимых преобразований с помощью *ключа.*

Требования однозначности дешифрования определяет обратную функцию, отображающую множество возможных (при выбранном ключе) шифрованных текстов в множество возможных открытых текстов. Ключ, определяющий выбор правила дешифрования, называется *ключом дешифрования.*

Формализуем сказанное. Обозначим через X конечное множество возможных открытых текстов, через $\mathcal{K}$ — конечное множество ключей и через Y — конечное множество шифрованных текстов. Правило шифрования на некотором ключе $k \in \mathcal{K}$ обозначим символом E_k. Оно определяется отображением $E_k : X \to Y$. Множество всех правил шифрования обозначается буквой E, т.е. $E = \{E_k \mid k \in \mathcal{K}\}$. Шифрованный текст $E_k(X)$ с помощью ключа k открытого текста X имеет вид $E_k(X) = \{E_k(x) \mid x \in X\}$.

Пусть D_k обозначает правило дешифрования текста $E_k(X)$ на ключе $k \in \mathcal{K}$, т.е. $D_k\colon E_k(X) \to X$. Множество шифров по всем ключам обозначим буквой D, т.е. $D = \{D_k \mid k \in \mathcal{K}\}$. Предполагается, если $k \in \mathcal{K}$ представляется в виде (k_s, k_d), где k_s — ключ шифрования, k_d — ключ дешифрования, то E_k понимается как E_{k_s}, а D_k — как

D_{k_d}.

Суммируя все сказанное, дадим следующее определение.

Шифром (шифросистемой) называют совокупность Σ вида $\Sigma = (X, \mathcal{K}, Y, E, D)$, для которой выполняются свойства

1) для любого сообщения $x \in X$ и для любого ключа $k \in \mathcal{K}$ имеем $D_k(E_k(x)) = x$;

2) $Y = \bigcup\limits_{k \in \mathcal{K}} E_k(X)$.

Как правило, множества X и Y представляют собой объединения декартовых степеней некоторых конечных множеств A и B,

$$A^l = \underbrace{A \times \cdots \times A}_{l}.$$

Тогда для любых натуральных чисел L и L_1 множества X и Y представляются в виде

$$X = \bigcup_{l=1}^{L} A^l,\ Y = \bigcup_{l=1}^{L_1} B^l.$$

§ 7. О симметричных шифрах

Определим *шифр простой замены.* Пусть $X = Y = \bigcup\limits_{l=1}^{L} A^l$, $\mathcal{K} \subset S(A)$, где $S(A)$ — симметрическая группа подстановок множества A. Для любого ключа $k \in \mathcal{K}$, открытого текста $x = (x_1, \ldots, x_l)$ и шифрованного текста $y = (y_1, \ldots, y_l)$ правила шифрования и дешифрования шифра простой замены определяются формулами

$$E_k(x) = (k(x_1), \ldots, k(x_l)), \quad D_k(x) = (k^{-1}(y_1), \ldots, k^{-1}(y_l)),$$

где k^{-1} — подстановка, обратная к подстановке k.

В более общей ситуации шифр простой замены определяется для

$$X = \bigcup_{l=1}^{L} A^l,\ Y = \bigcup_{l=1}^{L_1} B^l,$$

причем количества элементов в множествах A и B равны и множество ключей $\mathcal{K}$ совпадает с множеством биекций A на B.

Приведем пример шифра простой замены в русском алфавите из 33 букв. Возьмем известную фразу из букваря

мама мыла рамы.

В качестве ключа будем заменять каждую букву на соседнюю справа в алфавите. Получим

нбнб нъмб сбнъ.

Конечно, такой шифр не является стойким. Применение этого шифра можно усложнить. Например, можно взять несколько подстановок, и на каждом шаге шифрования пользоваться очередной

подстановкой.

Определим еще один шифр, называемый *шифром перестановки.*

Пусть $X = Y = A^L$, и пусть $\mathcal{K} \subset S_L$, где S_L — симметрическая группа подстановок множества $\{1, 2, \dots L\}$. Для любого ключа k, открытого текста $x = (x_1, \dots, x_L)$ и шифрованного текста $y = (y_1, \dots, y_L)$ правила шифрования и дешифрования шифра перестановки определяются формулами

$$E_k(x) = (x_{k(1)}, \dots, x_{k(L)}), \quad D_k(y) = (y_{k^{-1}(1)}, \dots, y_{k^{-1}(L)}),$$

где k^{-1} — подстановка, обратная к подстановке k.

Приведем пример шифра перестановки. Зашифруем выражение **этобылоуморя.**

В качестве ключа рассмотрим подстановку

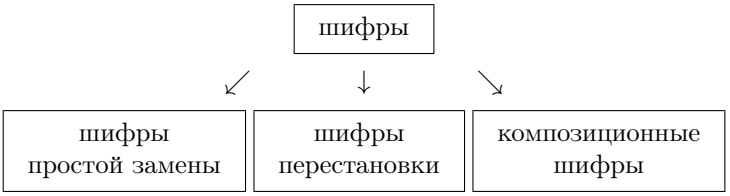
$$\begin{pmatrix} 123456789101112 \\ 312654978121011 \end{pmatrix}.$$

Получим шифр

тоэылбуморяо.

Введенные шифры являются представителями двух наиболее важных классов симметричных шифров. Еще один класс шифров можно получить композицией (или последовательным применением) некоторых шифров простой замены и шифров перестановки.

Итак, получена следующая классификация симметричных шифров



§ 8. О шифровании с открытым ключом

Поясним на примере основные моменты шифрования с открытым ключом. Пусть абонент B передает сообщение абоненту A.

1) Абонент A выбирает два различных простых числа p, q и полагает $n = pq$.

2) Абонент A находит значение функции Эйлера $\varphi(n) = (p-1)(q-1)$, выбирает число $e, 0 < e < \varphi(n)$, такое, что $(e, \varphi(n)) = 1$, и пару чисел (n, e) объявляет *открытым ключом,* а число d такое, что $de \equiv 1 \pmod{\varphi(n)}$ — *секретным ключом.*

3) Абонент B задает сообщение m, $0 \leqslant m \leqslant n-1$, создает *шифрованное сообщение* $E(m) \equiv m^e \pmod{n}$ и посылает его по открытому

каналу связи абоненту A.

4) Абонент A с помощью секретного ключа d дешифрует его следующим образом

$$D(E(m)) \equiv (m^e)^d \equiv m^{de} \equiv m \pmod{n}.$$

Таким образом абонент A получил сообщение абонента B.

5) Докажем, что $D(E(m)) = m$. Достаточно установить, что $m^{de} \equiv m \pmod{n}$.

Если числа m и n взаимно просты, то по теореме Эйлера имеем $m^{\varphi(n)} \equiv m \pmod{n}$. Тогда из условия $de \equiv 1 \pmod{\varphi(n)}$, имеем искомое утверждение $m^{de} \equiv m \pmod{n}$.

Пусть теперь $(m, n) > 1$. Тогда достаточно доказать, что справедливы сравнения

$$m^{de} \equiv m \pmod{p},\ m^{de} \equiv m \pmod{q},$$

поскольку из условия $(p, q) = 1$, $pq = n$, следует, что $m^{de} \equiv m \pmod{n}$.

Представим число de в виде $de = 1 + k\varphi(n)$. Тогда при $p \nmid m$ по малой теореме Ферма имеем

$$m^{p-1} \equiv 1 \pmod{p},\ m^{de} \equiv m(m^{p-1})^{k(q-1)} \equiv m \pmod{p}.$$

Пусть теперь $p \mid m$. Тогда $m \equiv 0 \pmod{p}$ и $m^{de} \equiv m \pmod{p}$.

Аналогично доказывается утверждение, что $m^{de} \equiv m \pmod{n}$.

Заметим, что секретным ключом в данной системе шифрования является набор чисел $(p, q, \varphi(n), d)$, а открытый ключ составляет пара чисел (n, e).

В дальнейшем будет построено несколько способов шифрования с открытым ключом, в частности, шифрование методом рюкзака.

Глава II
ПРЕФИКСНЫЕ КОДЫ. КОДЫ ШЕННОНА И ГИЛБЕРТА–МУРА

§ 1. Префиксные коды. Неравенство Крафта – МакМиллана

Пусть задан алфавит сообщений A, состоящий из r букв $a_1, \ldots, a_r$, и кодирующий алфавит B, состоящий из q букв $b_1, \ldots, b_q$.

Зададим отображение Σ букв алфавита A в множество $S(B)$ слов алфавита B, т.е. взаимно однозначное отображение $\Sigma\colon a_k \to B_k$, $k = 1, \ldots, r$. Определим кодирование $\mathcal{F}_\Sigma\colon S(A) \to S(B)$, удовлетворяющее следующим условиям

1) $\mathcal{F}_\Sigma(a_k) = B_k$, $k = 1, \ldots, r$;

2) $\mathcal{F}_\Sigma(a_{k_1} a_{k_2} \ldots a_{k_s}) = B_{k_1} B_{k_2} \ldots B_{k_s}$, $1 \leqslant k_1, k_2, \ldots, k_s \leqslant r$, $s \geqslant 1$;

где под произведением слов $B_k B_l$ понимается приписывание слова B_l справа к слову B_k. Множество кодовых слов $\{B_1, B_2, \ldots, B_r\}$ обозначают символом $C(\Sigma)$ и называют *кодом алфавита A в схеме Σ*.

Выделим некоторые классы алфавитных кодов. Код алфавита A в схеме Σ называют однозначно декодируемым, если любое конечное слово из букв алфавита B имеет не более одного прообраза. Частным случаем однозначно декодируемых кодов являются префиксные коды. Код назовем префиксным, если для любых слов B_k, B_l, являющихся образами букв a_k, a_l соответственно, каждое из них не является префиксом (началом) другого.

Пусть l_k длина слова $B_k, k = 1, \ldots, r$. Средней длиной кода в схеме Σ называется величина $L(\Sigma) = \sum\limits_{k=1}^{r} p_k l_k$, где p_k — частота появления буквы a_k в открытом тексте.

Теорема (Неравенство Крафта – МакМиллана)**.** *Для того, чтобы существовал префиксный код с длинами $l_1, \ldots l_r$, необходимо и достаточно, чтобы выполнялось неравенство*

$$\sum_{k=1}^{r} r^{-l_k} \leqslant 1.$$

▷ *Необходимость.* Пусть существует префиксный код с длинами $l_1, \ldots, l_r$ и $l = \max\{l_1, \ldots, l_r\}$. Символом n_m обозначим количество

кодовых слов длины m, где $m = 1, \ldots, r$. Тогда имеем

$$K = \sum_{k=1}^{r} r^{-l_k} = \sum_{m=1}^{l} \frac{n_m}{r^m}.$$

Из определения находим $n_m \leqslant r^m$. Следовательно, $K \leqslant l$. Покажем как с помощью одного приема Э. Ландау [34], [ч.II, отдел IV, гл.3, §2, с.41], можно уточнить это неравенство. Возьмем произвольное натуральное число s. Возведем величину K в степень s. Получим

$$K^s = \left(\sum_{m=1}^{l} \frac{n_m}{r^m} \right)^s = \sum_{m=1}^{ls} \frac{b_m}{r^m},$$

где

$$b_m = \sum_{m_1 + \cdots + m_s = m} n_{m_1} \ldots n_{m_s},$$

причем величина b_m представляет собой количество способов из s кодовых слов из набора $B_1, \ldots, B_r$ составить кодовое слово длины m. Так как из свойства префиксности кода следует его однозначная декодируемость, то для величины b_m имеем неравенство $b_m \leqslant r^m$. Отсюда находим $K^s \leqslant ls$. Следовательно, $K \leqslant (ls)^{1/s}$. Устремим s к бесконечности. Получим, что $K \leqslant 1$.

Достаточность. Построим префиксный код с заданным набором длин $l_1, \ldots, l_r$ кодовых слов. Определим величину $l = \max\{l_1, \ldots, l_r\}$. Количество однобуквенных слов обозначим через n_1, двухбуквенных — через n_2 и т.д.

Проведем индукцию по числу букв в кодовых словах. Так как алфавит A состоит из r букв, то можно произвольным образом выбрать $n_1 \leqslant r$ однобуквенных кодовых слов. Двухбуквенных слов имеется в точности r^2. Так как код является префиксным, то нельзя использовать слова, начинающиеся с n_1 выбранных букв. Тогда количество n_2 двухбуквенных обязано удовлетворять неравенству $n_2 \leqslant r^2 - n_1 r$. Предположим, что при $1 \leqslant k \leqslant l$ построены кодовые слова с длинами, не превосходящими k. Их количество n_k будет не превосходить $n_k \leqslant r^k - n_{k-1} r - \cdots - n_1 r^{k-1}$. Докажем утверждение для $k+1$-буквенных слов при условии, что $k + 1 \leqslant l$. Префиксный код, содержащий n_{k+1} кодовых слов длины $k + 1$, должен удовлетворять соотношению $n_{k+1} \leqslant r^{k+1} - n_k r - \cdots - n_1 r^k$, поскольку следует исключить слова, которые являются префиксами. Таким образом, на l-м шаге получим

$$0 \leqslant n_l \leqslant r^l - n_1 r^{l-1} - \cdots - n_{l-1} r.$$

Отсюда после простых преобразований найдем

$$1 \geqslant \frac{n_1}{r} + \frac{n_2}{r^2} + \cdots + \frac{n_l}{r^l} = \sum_{k=1}^{r} \frac{1}{r^{l_k}} = K. \qquad \triangleleft$$

§ 2. Теорема о минимальной длине префиксного кода

Пусть задано распределение вероятностей $p = \{p_1, \ldots, p_r\}$, $p_1, \ldots, p_r \geqslant 0$, $p_1 + \cdots + p_r = 1$. В частности, обозначим через $1/r$ распределение вероятностей $1/r, \ldots, 1/r$. Определим величину

$$H(p) = -\sum_{k=1}^{r} p_k \ln p_k,$$

причем будем считать, что $0 \ln 0 = 0$. Величина $H(p)$ называется *энтропией,* отвечающей распределению вероятностей p.

Лемма 1. *Пусть r — любое фиксированное натуральное число и $p = \{p_1, \ldots, p_r\}$, $p_1, \ldots, p_r \geqslant 0$, $p_1 + \cdots + p_r = 1$ — произвольное распределение вероятностей. Тогда $H(p) \leqslant H(1/r) = \ln r$, причем при распределении вероятностей $\{1/r, \ldots, 1/r\}$ достигается строгий максимум энтропии $H(p)$.*

$\triangleright$ Соединим точку с координатами $(p_1, \ldots, p_r)$ и точку $(1/r, \ldots, 1/r)$ отрезком. Тогда любую точку на этом отрезке можно задать при $0 \leqslant t \leqslant 1$ в следующем виде (барицентрические координаты)

$$p(t) = \left(tp_1 + \frac{1-t}{r}, \ldots, tp_r + \frac{1-t}{r} \right),$$

$$p(0) = (1/r, \ldots, 1/r), \quad p(1) = p = (p_1, \ldots, p_r).$$

Покажем, что функция $H(p(t)) = -\sum\limits_{k=1}^{r} p_k(t) \ln p_k(t)$ принимает максимальное значение при $t = 0$. При $0 \leqslant t \leqslant 1$ имеем

$$H'_t(p(t)) = -\sum_{k=1}^{r} p'_k(t) \ln p_k(t) - \sum_{k=1}^{r} p'_k(t),$$

$$H''_{tt}(p(t)) = -\sum_{k=1}^{r} \frac{(p'_k)^2(t)}{p_k(t)} < 0, \quad H'_t(p(t))|_{t=0} = 0. \qquad \triangleleft$$

Далее нам понадобится понятие выпуклости функции одной переменной (см., например, [2], [гл. V, §14]). Функция $f(x)$ называется выпуклой вверх на интервале (a, b), если для любых неотрицательных чисел $\lambda_1, \ldots, \lambda_r$ с условием $\lambda_1 + \cdots + \lambda_r = 1$ и для любых

$x_1, \ldots, x_r$ из (a, b) выполняется неравенство

$$\lambda_1 f(x_1) + \cdots + \lambda_r f(x_r) \leqslant f(\lambda_1 x_1 + \cdots + \lambda_r x_r).$$

Другими словами, график функции $y = f(x)$ на плоскости xOy лежит "над" любой секущей, проходящей через точки $(x_1, f(x_1))$ и $(x_2, f(x_2))$, где x_1, x_2 из (a, b). Например, функция $\ln x$ является выпуклой вверх на бесконечном промежутке $(0, +\infty)$.

Лемма 2. *Пусть заданы два распределения вероятностей* $p = \{p_1, \ldots, p_r\}$ *и* $q = \{q_1, \ldots, q_r\}$. *Тогда справедливо неравенство*

$$-\sum_{k=1}^{r} p_k \ln p_k \leqslant -\sum_{k=1}^{r} p_k \ln q_k,$$

причем равенство достигается при совпадении распределений вероятностей p *и* q.

▷ Доказываемое неравенство эквивалентно следующему

$$\sum_{k=1}^{r} p_k \ln \frac{q_k}{p_k} \leqslant 0.$$

Используя свойство выпуклости функции логарифм, при $p_1 \geqslant 0, \ldots,$ $p_r \geqslant 0$, $p_1 + \cdots + p_r = 1$ имеем

$$\sum_{k=1}^{r} p_k \ln \frac{q_k}{p_k} \leqslant \ln \left(\sum_{k=1}^{r} p_k \frac{q_k}{p_k} \right) = \ln 1 = 0. \qquad \triangleleft$$

Теорема (О минимальной длине кода)**.** *1) Пусть задано распределение вероятностей* $p = (p_1, \ldots, p_r)$ *появления букв* $a_1, \ldots, a_r$ *алфавита* A *некоторого открытого сообщения, и пусть задан префиксный код схемой* Σ *и кодовыми словами* $B_1, \ldots, B_r$ *из кодирующего алфавита* B *с длинами* $l_1, \ldots, l_r$ *соответственно. Пусть, также, энтропия* $H(p)$ *распределения вероятностей* p *равна* $H(p) = -\sum\limits_{k=1}^{r} p_k \ln p_k$ *и длина кода равна* $L(\Sigma) = \sum\limits_{k=1}^{r} p_k l_k$. *Тогда справедливо неравенство* $L(\Sigma) \geqslant H / \ln r$.

2) Пусть задано распределение вероятностей $p = (p_1, \ldots, p_r)$ *появления букв* $a_1, \ldots, a_r$ *алфавита* A *некоторого открытого сообщения. Тогда существует префиксный код длины* $L(\Sigma)$, *удовлетворяющей неравенству* $L(\Sigma) \leqslant 1 + H / \ln r$.

▷ 1) Из неравенства Крафта – МакМиллана имеем $K = \sum\limits_{k=1}^{r} r^{-l_k} \leqslant$ $\leqslant 1$. Положим $q_k = 1/(r^{l_k} K)$. Воспользуемся леммой 2 и неравен-

ством Крафта – МакМиллана. Получим

$$H = H(p) = -\sum_{k=1}^{r} p_k \ln p_k \leqslant -\sum_{k=1}^{r} p_k \ln q_k = \sum_{k=1}^{r} p_k (l_k \ln r + \ln K) =$$
$$= L(\Sigma) \ln r + \ln K \leqslant L(\Sigma) \ln r.$$

2) Определим натуральные числа $l_k, k = 1, \ldots, r$, из неравенств

$$r^{-l_k} \leqslant p_k < r^{-l_k+1}.$$

Если $p_k = 0$, то полагаем $l_k = 0$ вместо приведенных выше неравенств.

По выбору чисел $l_1, \ldots, l_r$ имеем

$$\sum_{k=1}^{r} r^{-l_k} \leqslant \sum_{k=1}^{r} p_k = 1.$$

Следовательно, по утверждению 2) теоремы о неравенстве Крафта – МакМиллана существует префиксный код с некоторой схемой Σ и с выбранными ранее длинами $l_1, \ldots, l_r$ кодовых слов.

Оценим сверху длину $L(\Sigma)$ этого кода. Из неравенства $p_k < r^{-l_k+1}$ находим $l_k < 1 - \frac{\ln p_k}{\ln r}$. Отсюда получим

$$L(\Sigma) = \sum_{k=1}^{r} p_k l_k < \sum_{k=1}^{r} p_k \left(1 - \frac{\ln p_k}{\ln r}\right) = 1 + \frac{H}{\ln r}. \qquad \triangleleft$$

Глава III
КОНЕЧНЫЕ ПОЛЯ. ЦИКЛИЧЕСКИЕ КОДЫ

§ 1. Конечные поля. Неприводимые многочлены над конечным полем

Сначала в качестве примера рассмотрим конечное поле, состоящее из четырех элементов: $0, 1, a, b$. Аддитивную и мультипликативную группы этого поля опишем таблицами Кэли. В первой таблице на пересечении строки, номер которой указан в левом столбце, и столбца, номер которого указан в верхней строке таблицы, находится результат сложения соответствующих элементов поля. Имеем

	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Аналогичным образом строится вторая таблица для операции умножения

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Для завершения построения поля из четырех элементов необходимо проверить выполнение дистрибутивного закона, т.е.выполнение следующих равенств

$$a(1+a) = a + a^2, \quad a(1+b) = a + ab, \quad a(a+b) = a^2 + ab,$$
$$b(1+a) = b + ba, \quad b(1+b) = b + b^2, \quad b(a+b) = ba + b^2.$$

Эта проверка осуществляется непосредственно по приведенным выше таблицам Кэли.

Опишем теперь все конечные поля, т.е. поля состоящие из конечного числа элементов. Они называются полями Галуа. Пусть p — лю-

бое простое число. Множество классов вычетов по модулю p в кольце целых чисел образует поле $\mathbf{Z}_p$ из p элементов.

Для построения конечных полей нам понадобится кольцо многочленов $\mathbf{Z}_p[x]$ от неизвестного x с коэффициентами из $\mathbf{Z}_p$. Каждый многочлен $f(x)$ из $\mathbf{Z}_p[x]$ можно записать в виде $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, где n — степень многочлена, $a_n, a_{n-1}, \ldots, a_1, a_0$ — коэффициенты многочлена, a_0 — свободный член, $a_n \neq 0$ — коэффициент при старшей степени многочлена. Если $a_n = 1$, то многочлен $f(x)$ называется нормированным многочленом. Многочлен $f(x)$ из $\mathbf{Z}_p[x]$ называется неприводимым, если он не может быть представлен в виде произведения двух многочленов положительной степени.

Пример. Выпишем все неприводимые многочлены первой, второй, третьей и четвертой степеней из кольца многочленов $\mathbf{Z}_2[x]$. Имеем

$$x, \quad x+1, \quad x^2+x+1, \quad x^3+x^2+1,$$

$$x^4+x^3+x^2+x+1, \quad x^4+x^3+1, \quad x^4+x+1.$$

Проверка неприводимости многочленов осуществляется делением с остатком многочленов на все неприводимые многочлены меньшей степени.

Далее будем пользоваться тем, что кольцо многочленов над любым полем является кольцом с однозначным разложением на неприводимые многочлены, т.е. каждый нормированный многочлен единственным образом с точностью до порядка сомножителей представляется в виде произведения нормированных неприводимых многочленов.

Заметим, что количество нормированных многочленов степени n равно p^n. Символом $((n))$ обозначим количество нормированных неприводимых многочленов степени n.

Рассмотрим функцию комплексного переменного

$$\zeta_p(z) = \frac{1}{1-pz}.$$

Докажем следующее вспомогательное утверждение.

Лемма 1. *При $|z| < 1/p$ справедливо равенство*

$$\zeta_p(z) = \prod_{m=1}^{\infty} \left(\frac{1}{1-z^m}\right)^{((m))}.$$

▷ Преобразуем правую часть равенства. Имеем

$$\prod_{m=1}^{\infty}\left(\frac{1}{1-z^m}\right)^{((m))}=\prod_{m=1}^{\infty}\prod_{Q}\frac{1}{1-z^m}=\prod_{m=1}^{\infty}\prod_{Q}(1+z^m+z^{2m}+\dots),$$

где $Q=Q(x)$ пробегает все нормированные неприводимые многочлены степени m. Внутреннее произведение по Q содержит конечное число членов, не превосходящее количества всех нормированных многочленов степени m, т.е. величины p^m. Для изучения вопроса об абсолютной сходимости бесконечного произведения достаточно рассмотреть при $|z|<1/p$ ряд

$$\sum_{m=1}^{\infty}\sum_{Q}(|z|^m+|z|^{2m}+\dots)\leqslant\sum_{m=1}^{\infty}p^m(|z|^m+|z|^{2m}+\dots)\leqslant$$

$$\leqslant\sum_{m=1}^{\infty}\frac{p^m|z|^m}{1-|z|^m}\leqslant\sum_{m=1}^{\infty}p^m|z|^m.$$

Последний ряд сходится при $|z|<1/p$. Следовательно, и рассматриваемое бесконечное произведение сходится при тех же z.

Используя однозначность разложения нормированного многочлена в произведение неприводимых многочленов, приходим к равенству

$$\prod_{m=1}^{\infty}\prod_{Q}\frac{1}{1-z^m}=\sum_{m=1}^{\infty}\sum F_mz^m,$$

где слагаемые в сумме $\sum\limits_{F_m}$ пробегают все нормированные многочлены степени m.

Таким образом, при $|z|<1/p$ находим

$$\prod_{m=1}^{\infty}\prod_{Q}\frac{1}{1-z^m}=\sum_{m=1}^{\infty}p^mz^m=\frac{1}{1-pz}.$$ ◁

Теорема 1. *При $n\geqslant 1$ справедливо равенство*

$$((n))=\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}.$$

▷ Из утверждения леммы имеем

$$-\sum_{m=1}^{\infty}((m))\ln(1-z^m)=\ln(1-pz).$$

Отсюда, используя разложение в степенной ряд, находим

$$\sum_{m=1}^{\infty}((m))\sum_{s=1}^{\infty}\frac{z^{ms}}{s}=\sum_{k=1}^{\infty}\frac{p^k z^k}{k}.$$

Приравнивая коэффициенты двух степенных, получим

$$\frac{p^k}{k}=\sum_{ms=k}\frac{((m))}{s},\quad \text{т.е.}\quad \frac{p^k}{k}=\frac{1}{k}\sum_{d|k}((d))d.$$

Следовательно, $p^k=\sum\limits_{d|k}((d))d$. Далее, используя формулу Чебышёва – Мёбиуса обращения суммы по делителям, приходим к следующему равенству

$$((n))=\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}. \qquad \triangleleft$$

Как следствие утверждения теоремы находим.

Следствие. *Пусть n — любое натуральное число и p — любое простое число. Тогда найдется неприводимый многочлен степени n с коэффициентами из поля $\mathbf{Z}_p$. Более того, справедливо неравенство $((n))\geqslant p^n/(2n)$.*

$\triangleright$ При $n=1$ следствие, очевидно, верно, т.к. $((1))=p$. При $n\geqslant 2$ из утверждения теоремы имеем

$$((n))=\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}\geqslant\frac{1}{n}(p^n-p^{[n/2]}-\cdots-1)=$$

$$=\frac{1}{n}\left(p^n-\frac{p^{[n/2]+1}-1}{p-1}\right)\geqslant\frac{p^n}{2n}. \qquad \triangleleft$$

Пример. Для неприводимого многочлена x^4+x+1 в кольце многочленов $\mathbf{Z}_2[x]$ факторкольцо, полученное как множество всех классов вычетов по модулю многочлена x^4+x+1, образует поле Галуа $GF(2^4)$ из шестнадцати элементов. В каждом классе вычетов по модулю многочлена x^4+x+1 имеется единственный многочлен степени, не превосходящей трех. Всего таких многочленов в $\mathbf{Z}_2[x]$ ровно $2^4=16$.

Теорема 2. *Пусть n — любое натуральное число и p — любое простое число. Тогда существует поле из p^n элементов.*

$\triangleright$ Пусть $f(x)$ — неприводимый многочлен степени n с коэффициентами из поля $\mathbf{Z}_p$. Определим классы вычетов по модулю $f(x)$. Два многочлена $A(x)$ и $B(x)$ принадлежат одному классу вычетов, если

$f(x)$ делит $A(x) - B(x)$. Для этого вводят следующее обозначение:

$$A(x) \equiv B(x) \pmod{f(x)}.$$

Над классами вычетов по модулю $f(x)$ стандартным образом можно определить операции сложения, вычитания и умножения. Далее, для неприводимого многочлена $f(x)$ и любого многочлена $A(x)$ можно найти многочлен $X(x)$ такой, что

$$A(x)X(x) \equiv 1 \pmod{f(x)}.$$

Последнее утверждение следует из того, что с помощью алгоритма Евклида находятся многочлены $X(x)$ и $Y(x)$ с коэффициентами из $\mathbf{Z}_p$ такие, что выполняется равенство

$$A(x)X(x) + f(x)Y(x) = 1.$$

Таким образом определяется деление в кольце классов вычетов по модулю неприводимого многочлена $f(x)$. Тем самым, классы вычетов по модулю неприводимого многочлена образуют поле. Эти классы вычетов можно отождествить с многочленами степени, меньшей n. Их количество в $\mathbf{Z}_p[x]$ будет равно p^n. $\triangleleft$

Лемма 2. *Любая конечная подгруппа мультипликативной группы поля является циклической подгруппой.*

$\triangleright$ Пусть элементы a и b имеют порядки m и n соответственно, и пусть $l = [m, n]$ — наименьшее общее кратное этих чисел. Из канонического разложения чисел m и n на простые сомножители находим $l = m_0 n_0, (m_0, n_0) = 1$ и $m = m_0 m_1, n = n_0 n_1$. Тогда элемент $c = a^{m_1} b^{n_1}$ имеет порядок l. Действительно, пусть натуральное число s — порядок элемента c. Тогда число s — наименьшее натуральное число с условием $c^s = 1$. Имеем, также, $c^l = (a^{m_1} b^{m_1})^l = a^{mn_0} b^{nm_0} = 1$. Разделим число l с остатком на s. Получим $l = sl_1 + r, 0 \leqslant r < s$. Отсюда находим $c^r = c^{l - sl_1} = 1$. Следовательно, $r = 0$. В противном случае $0 < r < s, c^r = 1$, что противоречит минимальности выбора натурального числа s с условием $c^s = 1$. Таким образом, $s \mid l$.

Далее, имеем $1 = c^{sm_0} = a^{ms} b^{n_1 m_0 s} = b^{n_1 m_0 s}$. Порядок элемента b равен n. Отсюда следует, что $n_1 m_0 s$ делится на n, т.е. $n_0 \mid s$. Аналогично находим $1 = c^{sn_0} = a^{n_0 m_1 s}$. Следовательно, $m_0 \mid s$. Так как m_0 и n_0 взаимно просты, то $l \mid s$, где $l = m_0 n_0$.

Из доказанного следует, что $l = s$, т.е. элемент c имеет порядок l.

Пусть конечная подгруппа G мультипликативной группы поля имеет порядок τ. Тогда максимальный из порядков m элементов этой подгруппы не превосходит τ. Аналогично предыдущему можно показать, порядок каждого элемента подгруппы является делителем числа m, т.е. все элементы из G удовлетворяют уравнению $x^m - 1 = 0$.

Так как количество корней алгебраического уравнения в любом поле не превосходит степени многочлена, то $\tau \leqslant m$. Следовательно, $\tau = m$. Это означает, что в группе G имеется элемент порядка τ, т.е. группа G является циклической. ◁

Лемма 3. *Мультипликативная группа конечного поля из p^n элементов является циклической группой.*

▷ Поскольку мультипликативная группа конечного поля имеет конечный порядок, по предыдущей лемме она является циклической группой. ◁

Из теоремы 2 вытекает, что все элементы конечного поля K, состоящего из p^n элементов, удовлетворяют уравнению $x^{p^n} - x = 0$, т.е. имеет место разложение на линейные множители следующего вида

$$x^{p^n} - x = \prod_{a \in K} (x - a),$$

где символ a пробегает все элементы поля K.

Пример. Пусть $GF(2^4)$ — поле Галуа из 16 элементов, представляющее собой все классы вычетов в кольце многочленов $\mathbf{Z}_2[x]$ по модулю неприводимого многочлена $x^4 + x + 1$ в $\mathbf{Z}_2[x]$. Пусть, также a — образующая мультипликативной группы поля. Тогда имеем $a^4 + a + 1 = 0$. Следовательно, все ненулевые элементы поля можно представить в виде

$$a^0 = 1,\ \ a^1 = a,\ \ a^2 = a^2,\ \ a^3 = a^3,\ \ a^4 = a + 1,\ \ a^5 = a^2 + a,$$
$$a^6 = a^3 + a^2,\ \ a^7 = a^3 + a + 1,\ \ a^8 = a^2 + 1,\ \ a^9 = a^3 + a,$$
$$a^{10} = a^2 + a + 1,\ \ a^{11} = a^3 + a^2 + a,\ \ a^{12} = a^3 + a^2 + a + 1,$$
$$a^{13} = a^3 + a^2 + 1,\ \ a^{14} = a^3 + 1,\ \ a^{15} = 1.$$

Заметим, что количество образующих мультипликативной группы поля $GF(p^n)$ равно $\varphi(p^n - 1)$.

Теорема 3. *Пусть n — любое натуральное число и p — любое простое число. Тогда для двух неприводимых многочленов $f(x)$ и $g(x)$ поля их классов вычетов по модулям этих многочленов изоморфны.*

▷ При доказательстве теоремы 2 установлено, что конечное поле классов вычетов по модулю неприводимого многочлена $f(x)$ степени n из кольца $\mathbf{Z}_p[x]$, изоморфно полю корней многочлена $x^{p^n} - x$. Это и доказывает искомый изоморфизм. ◁

Теорема 4. *Пусть n — любое натуральное число и p — любое простое число. Тогда с точностью до изоморфизма существует единственное поле из p^n элементов.*

▷ Поскольку мультипликативная группа конечного поля из p^n является циклической группой, каждый элемент a этой группы удовлетворяет уравнению $x^{p^n-1}-1=0$, причем найдется элемент, порядок которого равен p^n-1. Таким образом установлен изоморфизм мультипликативных групп конечных полей из p^n элементов. ◁

§ 2. Циклические коды

Пусть V — линейное k-мерное подпространство арифметического n-мерного пространства $L=L_{\mathbf{F}}, k\leqslant n$, наборов $\mathbf{v}=(v_{n-1},\ldots,v_1,v_0)$ с координатами из любого поля $\mathbf{F}$, например, $\mathbf{Z}_2$. Тогда подпространство V называется *циклическим кодом,* если для любого набора $\mathbf{a}=(a_{n-1},\ldots,a_1,a_0)$ из V набор $\mathbf{a}'=(a_{n-2},\ldots,a_1,a_0,a_{n-1})$ принадлежит V. Другими словами, набор $\mathbf{a}'$ получен из набора $\mathbf{a}$ циклическим сдвигом всех координат на одну координату вправо.

Для описания циклических кодов воспользуемся кольцом многочленов $\mathbf{F}[x]$. Набору $(a_{n-1},\ldots,a_1,a_0)$ поставим в соответствие многочлен $f(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ степени, не превосходящей $n-1$. Тогда циклическому сдвигу отвечает умножение многочлена $f(x)$ на переменную x и рассмотрение класса вычетов по модулю x^n-1. Действительно, имеем

$$xf(x)=x(a_{n-1}x^{n-1}+\cdots+a_1x+a_0)=a_{n-1}(x^n-1)+$$
$$+a_{n-2}x^{n-1}+a_{n-3}x^{n-2}+\cdots+a_0x+a_{n-1}=a_{n-1}(x^n-1)+g(x).$$

Следовательно, получим сравнение

$$g(x)\equiv xf(x)\pmod{(x^n-1)},$$

где многочлен $g(x)$ из кольца $\mathbf{F}[x]$ отвечает циклическому сдвигу всех координат вектора $\mathbf{a}$ на одну координату вправо.

В любом классе вычетов в кольце многочленов $\mathbf{F}[x]$ по модулю x^n-1 содержится в точности один многочлен степени, меньшей n. Совокупность всех этих классов образует кольцо $\mathbf{F}_n$.

Теорема. *Пусть $\mathbf{F}_n$ — кольцо классов вычетов по модулю x^n-1 в кольце $\mathbf{F}[x]$, где $\mathbf{F}$ — некоторое поле. Для того чтобы линейное подпространство V из $\mathbf{F}^n$ было циклическим кодом необходимо и достаточно, чтобы оно было идеалом в кольце $\mathbf{F}_n$.*

▷ *Необходимость.* Дано, что код V — циклический. Далее, для любого набора $\mathbf{v}=(a_{n-1},\ldots,a_1,a_0)$ из V умножение многочлена $f(x)=a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ из $\mathbf{F}_n$ на переменную x дает многочлен $g(x)=a_{n-2}x^{n-1}+a_{n-3}x^{n-2}+\cdots+a_0x+a_{n-1}\in\mathbf{F}_n$, который отвечает циклическому сдвигу $\mathbf{v}'=(a_{n-2},\ldots,a_1,a_0,a_{n-1})$ из V. Отсюда следует, что многочленам $f(x)$, $xf(x)$, $x^2f(x)$, $\ldots$, $x^{n-1}f(x)$ из $\mathbf{F}_n$

также отвечают кодовые слова $\mathbf{v}$, $\mathbf{v}'$, $\mathbf{v}''$, …, $\mathbf{v}^{(n-1)}$ из V. Поскольку $\mathbf{V}$ является подпространством, любая линейная комбинация наборов $\mathbf{v}$, $\mathbf{v}'$, $\mathbf{v}''$, …, $\mathbf{v}^{(n-1)}$ принадлежит $\mathbf{V}$, т.е. для любых постоянных c_0, c_1, …, c_{n-1} из $\mathbf{F}$ имеем

$$c_0\mathbf{v} + c_1\mathbf{v}' + c_2\mathbf{v}'' + \ldots + c_{n-1}\mathbf{v}^{(n-1)} \in \mathbf{V}.$$

Другими словами, многочлен

$$c_0 f(x) + c_1 x f(x) + c_2 x^2 f(x) + \ldots + c_{n-1} x^{n-1} f(x) = c(x) f(x)$$

принадлежит $\mathbf{F}_n$. Это обстоятельство позволяет сказать, что множество всех многочленов, отвечающих наборам из подпространства $\mathbf{V}$, образует идеал в кольце многочленов $\mathbf{F}_n$. Необходимость утверждения теоремы доказана.

Достаточность. Пусть J — любой идеал в кольце многочленов $\mathbf{F}_n$. Возьмем любой многочлен $f(x) = a_{n-1}x^{n-1} + \cdots + a_0$ из J. Ему отвечает кодовое слово $\mathbf{v} = (a_{n-1}, \ldots, a_1, a_0)$. Рассмотрим многочлен $xf(x) \in J$. Ему отвечает кодовое слово $\mathbf{v}' = (a_{n-2}, \ldots, a_0, a_{n-1})$, которое является циклическим сдвигом на одну координату вправо кодового слова $\mathbf{v}$, тем самым идеалу J кольца $\mathbf{F}_n$ отвечает циклический код. ◁

Теорема. *Пусть $\mathbf{F}_n$ — кольцо классов вычетов по модулю $x^n - 1$ в кольце многочленов $\mathbf{F}[x]$, где $\mathbf{F}$ — некоторое поле. Тогда кольцо $\mathbf{F}_n$ является кольцом главных идеалов, т.е. найдется фиксированный многочлен из $\mathbf{F}_n$ такой, что все элементы идеала кратны этому многочлену.*

▷ Пусть $f(x)$ — нормированный многочлен наименьшей степени, принадлежащий рассматриваемому идеалу J. Возьмем любой многочлен $g(x) \in J$ и разделим его с остатком на $f(x)$. Получим

$$g(x) = f(x)q(x) + r(x),$$

где многочлен $r(x)$ либо имеет степень меньшую, чем степень многочлена $f(x)$, либо равен $r(x) \equiv 0$ в $\mathbf{F}_n$. Поскольку $r(x)$ также принадлежит идеалу J, первая возможность не имеет места ($f(x)$ — многочлен наименьшей степени из J). Следовательно, $r(x) \equiv 0$. ◁

Многочлен $f(x)$ наименьшей степени, принадлежащий идеалу J, называется *многочленом, порождающим идеал J* из кольца $\mathbf{F}_n$.

Теорема. *Пусть многочлен $f(x)$ порождает идеал J из $\mathbf{F}_n$. Тогда $f(x)$ является делителем $x^n - 1$.*

▷ Разделим многочлен $x^n - 1$ с остатком на $f(x)$ в кольце многочленов $\mathbf{F}[x]$. Получим

$$g(x) = f(x)q(x) + r(x),$$

где многочлен $r(x)$ либо имеет степень меньшую, чем степень многочлена $f(x)$, либо равен $r(x) \equiv 0$ в $\mathbf{F}[x]$. Поскольку $r(x)$ также принадлежит идеалу J, первая возможность не имеет места. Следовательно, $r(x) \equiv 0$. $\triangleleft$

Таким образом, имеем $x^n - 1 = f(x)h(x)$. Многочлен $h(x)$ называется *проверочным многочленом* для кода V, порожденного многочленом $f(x)$.

Пример. Разложим многочлен $x^7 - 1$ на неприводимые множители над полем $\mathbf{F} = \mathbf{Z}_2$. Имеем

$$x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

Рассмотрим циклический код Хемминга, порожденный многочленом $x^3 + x^2 + 1$ в кольце $\mathbf{F}_7$ классов вычетов многочленов из $\mathbf{F}[x]$ по модулю $x^7 - 1$. Приведем таблицу базисных векторов (кодовых слов), отвечающих многочленам $x^3 f(x)$, $x^2 f(x)$, $xf(x)$, $f(x)$. Находим

$x^3 f(x)$	1	1	0	1	0	0	0
$x^2 f(x)$	0	1	1	0	1	0	0
$xf(x)$	0	0	1	1	0	1	0
$f(x)$	0	0	0	1	1	0	1

Код будет состоять из 16 кодовых слов. Все они получаются умножением слева двоичных векторов $\mathbf{c} = (c_1, c_2, c_3, c_4)$ с координатами, принимающими значения либо 0, либо 1, на порождающую матрицу F вида

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Таким образом, получим выражение для кодового слова

$$K = K(\mathbf{c}) = \mathbf{c}F = (c_1, c_1 + c_2, c_2 + c_3, c_1 + c_3 + c_4, c_2 + c_4, c_3, c_4).$$

Рассмотрим теперь идеал, порожденный проверочным многочленом

$$h(x) = (x-1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1 \in \mathbf{Z}_2[x].$$

Строим таблицу базисных векторов, отвечающих многочленам $x^2 h(x)$, $xh(x)$, $h(x)$. Находим

$x^2 h(x)$	1	1	1	0	1	0	0
$xh(x)$	0	1	1	1	0	1	0
$h(x)$	0	0	1	1	1	0	1

Матрица H, образованная векторами, отвечающими многочленам $x^2h(x)$, $xh(x)$, $h(x)$, координаты которых записаны в обратном порядке, имеет вид

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Пусть H^T — транспонированная к H матрица. Тогда получим $GH^T = 0$.

Любой вектор из ортогонального дополнения $V^\perp$ к кодовому пространству V в пространстве L называется проверочным вектором.

Пусть, как и раньше, порождающий многочлен $f(x)$ для кода V записан в форме $f(x) = a_{k-1}x^{k-1} + \ldots + a_0$. Тогда в качестве порождающей матрицы F можно выбрать матрицу размером $(n-k)\times n$, строками которой будут коэффициенты многочленов $x^{n-k-1}f(x)$, $\ldots$, $xf(x)$, $f(x)$, т.е. матрица F имеет вид

$$F = \begin{pmatrix} a_{k-1} & a_{k-2} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_{k-1} & a_{k-2} & \ldots & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_{k-1} & a_{k-2} & \ldots & a_0 \end{pmatrix}.$$

Рассмотрим $h(x)$ — проверочный многочлен, т.е. многочлен из кольца $\mathbf{F}_n$ классов вычетов по модулю $x^n - 1$ в кольце многочленов $\mathbf{F}[x]$. Он удовлетворяет сравнению $f(x)h(x) \equiv 0 \pmod{(x^n - 1)}$ и в качестве представителя класса вычетов можно взять многочлен $h(x)$ степени, не превосходящей $n-k-1$, т.е. $h(x) = h_{n-k-1}x^{n-k-1} + \ldots + h_0$.

Составим матрицу H порядка $k \times n$, имеющую следующий вид

$$H = \begin{pmatrix} 0 & \ldots & 0 & h_0 & h_1 & \ldots & h_{n-k-1} \\ 0 & \ldots & h_0 & \ldots & h_{n-k-2} & h_{n-k-1} & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ h_0 & \ldots & h_{n-k-2} & h_{n-k-1} & 0 & \ldots & 0 \end{pmatrix}.$$

Здесь в первой строке первые k координат равны 0, а оставшиеся координаты являются коэффициентами многочлена $h(x)$, во второй строке первые $k-1$ координата равны 0, а оставшиеся — коэффициенты многочлена $xh(x)$, и т.д., наконец, k-я строка состоит из коэффициентов многочлена $x^{k-1}h(x)$.

Будем называть матрицу проверочной для кода V, если каждая строка ее ортогональна любому кодовому слову. Покажем, что матрица H является проверочной матрицей для кода V.

Возьмем любой кодовый вектор $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ из кода V. Ему отвечает многочлен $a(x) = \sum\limits_{k=0}^{n-1} a_k x^k$. Поскольку множество всех многочленов, отвечающих кодовым словам из V, образуют главный идеал, порожденный многочленом $f(x)$, получим равенство $a(x) = f(x)b(x)$, где $b(x)$ — многочлен. Аналогично, подпространству $V^{\perp}$ отвечает главный идеал, порожденный многочленом $h(x)$, и потому любой многочлен $d(x) = \sum\limits_{k=0}^{n-1} d_k x^k$ представляется в виде $d(x) = h(x)e(x)$, где $e(x)$ — многочлен.

Тогда находим

$$a(x)d(x) = b(x)f(x)h(x)e(x) \equiv 0 \pmod{(x^n - 1)},$$

поскольку $f(x)h(x) \equiv 0 \pmod{(x^n - 1)}$.

Следовательно, все коэффициенты многочлена $a(x)d(x)$ равны 0 в поле $\mathbf{F}$. Таким образом, свободный член этого многочлена равен 0 в $\mathbf{F}$, т.е.

$$\sum_{k=1}^{n-1} a_k d_{n-1-k} = 0.$$

Глава IV
РЕКУРРЕНТНЫЕ СООТНОШЕНИЯ. ПРОИЗВОДЯЩИЕ ФУНКЦИИ

§ 1. Рекуррентные соотношения

Часто при организации вычислительного процесса приходят к рекуррентным соотношениям вида

$$x_{n+1} = f(x_n), \quad n = 0, 1, \ldots.$$

Пример 1. Рассмотрим задачу приближенного вычисления значения функции $1/x$ при $1/2 \leqslant x < 1$. Предположим известно приближение s_n этой функции с точностью до n знаков после запятой в двоичной системе счисления, т.е.

$$\left| s_n - \frac{1}{x} \right| < 2^{-n}.$$

После возведения этого неравенства в квадрат и домножения на x получим

$$0 \leqslant s_n^2 x - 2s_n + \frac{1}{x} < x2^{-2n} < 2^{-2n}.$$

Следовательно, положив $s_{n+1} = f(s_n) = 2s_n - xs_n^2$, находим

$$-2^{-2n} < s_{n+1} - \frac{1}{x} \leqslant 0,$$

т.е. величина s_{n+1} приближает значение функции $1/x$ с точностью до $2n$ двоичных знаков.

В качестве s_1 можно взять значение $s_1 = 3/2$, если $1/2 < x < 1$, и $s_1 = 7/4$, если $x = 1/2$. Тогда $|s_1 - 1/x| < 1/2$. Тогда получим

$$\left| s_n - \frac{1}{x} \right| < 2^{-2^{n-1}}.$$

Таким образом, последовательность $\{s_n\}$ сходится к величине $1/x$ и ошибка при замене $1/x$ на s_n не превосходит $2^{-2^{n-1}}$.

Пример 2. Пусть теперь при $1/4 \leqslant a < 1$ требуется приближенно вычислить $\sqrt{a}$, и пусть s_1 удовлетворяет условию $|s_1 - \sqrt{a}| < 2^{-1}$. В частности, при $1/4 < a < 1$ можно положить $s_1 = 3/4$, а при $a = 1/4$ — положить $s_1 = 5/8$.

Предположим, что s_n приближает $\sqrt{a}$ с точностью до k знаков после запятой в двоичной записи чисел, т.е. $|s_n - \sqrt{a}| < 2^{-k}$. Возведем последнее неравенство в квадрат. Получим

$$0 \leqslant s_n^2 - 2s_n\sqrt{a} + a < 2^{-2k}.$$

Отсюда, положив $s_{n+1} = \frac{1}{2}\left(s_n + \frac{a}{s_n}\right)$, имеем

$$|s_{n+1} - \sqrt{a}| < \frac{1}{2^{2k+1}s_n}.$$

Покажем, что при любом натуральном n справедливо неравенство $s_n \geqslant 1/2$. Индукция по параметру n. При $n = 1$ утверждение верно. Пусть оно верно при $n = m$. Докажем его при $n = m + 1$. Имеем

$$s_{m+1} = \frac{1}{2}\left(s_m + \frac{a}{s_n}\right) \geqslant \sqrt{a} \geqslant \frac{1}{2}.$$

Тем самым, при указанном выборе s_1 находим

$$\left|s_n - \sqrt{a}\right| < 2^{-2^{n-1}}.$$

Пример 3. Пусть $s_{n+1} = f(s_n)$ и функция $f(t)$ имеет вторую непрерывную производную, причем $|f''(t)| \leqslant M$. Предположим далее, что $\lim\limits_{n\to\infty} s_n = s$, $s = f(s)$, $f'(s) = 0$. Тогда имеем

$$f(s_n) = f(s + (s_n - s)) = f(s) + f'(s)(s_n - s) + \frac{1}{2}f''(\xi)(s_n - s)^2.$$

Таким образом находим

$$|s_{n+1} - s| \leqslant \frac{M}{2}(s_n - s)^2.$$

Пример 4. Пусть требуется при $1/8 \leqslant a < 1$ вычислить приближенно значение $\sqrt[3]{a}$. Воспользуемся для построения функции $f(s)$ предыдущим примером. Пусть $s_{n+1} = f(s_n)$ и $s = \lim\limits_{n\to\infty} s_n$, и пусть выполняются соотношения $s = f(s) = \sqrt[3]{a}$, $f'(s) = 0$. Пусть α, β и γ, δ — неизвестные коэффициенты и формулы имеют вид

$$f_1(s) = \alpha s + \beta\frac{a}{s^2}, \quad f_2 = \gamma s + \delta\frac{s^4}{a}.$$

Тогда из соотношений $s = f_k(s), f_k'(s) = 0, r = 1, 2$, находим

$$1 = \alpha + \beta, \quad \alpha - 2\beta = 0,$$

$$1 = \gamma + \delta, \quad \gamma + 4\delta = 0.$$

Отсюда получаем вид формул

$$f_1(s) = \frac{2}{3}s + \frac{a}{3s^2}, \quad f_2(s) = \frac{4}{3}s - \frac{s^4}{3a}.$$

Рассмотрим первую формулу $s_{n+1} = \frac{2}{3}s + \frac{a}{3s^2}$. Положим $s_1 = 3/4$ при $1/8 \leqslant a < 1$. Имеем $|s_1 - \sqrt[3]{a}| < 1/2$. Далее, для любого $n \geqslant 1$ из неравенства между средним арифметическим и средним геометрическим следует

$$s_{n+1} = f_1(s_n) = \frac{s_n}{3} + \frac{s_n}{3} + \frac{a}{3s_n^2} \geqslant \sqrt[3]{a} \geqslant \frac{1}{2}.$$

Оценим сверху разность $s_{n+1} - \sqrt[3]{a}$. Имеем

$$0 \leqslant s_{n+1} - \sqrt[3]{a} = \frac{1}{3}\left(2s_n + \frac{a}{s_n^2} - 3\sqrt[3]{a}\right) =$$

$$= \frac{1}{3s_n^2}(s_n - \sqrt[3]{a})^2(2s_n + \sqrt[3]{a}) \leqslant \frac{8}{3}(s_n - \sqrt[3]{a})^2.$$

Таким образом, получим

$$|s_n - \sqrt[3]{a}| \leqslant (8/3)^{n-1}2^{-2^{n-1}}.$$

Рассмотрим теперь вторую формулу $f_2(s) = \frac{4}{3}s - \frac{s^4}{3a}$. Положим $t_1 = 3/4$ при $1/8 \leqslant a < 1$. Имеем $|t_1 - \sqrt[3]{a}| < 1/2$. Далее находим

$$t_{n+1} = f_2(t_n),$$

$$t_{n+1} - \sqrt[3]{a} = -\frac{1}{3a}(t_n^4 - 4t_n\sqrt[3]{a} + 3a\sqrt[3]{a}) = -\frac{1}{3a}(t_n - \sqrt[3]{a})^3(t_n + 3\sqrt[3]{a}).$$

Кроме того, $t_1 = 3/4$, $t_2 > 0$ и $\max f(t) = \sqrt[3]{a}$, поэтому для всех $n \geqslant 2$ имеем $0 \leqslant t_n \leqslant \sqrt[3]{a}$ и $t_{n+1} \geqslant t_n$. Это доказывает сходимость последовательности $\{t_n\}$ к $\sqrt[3]{a}$ и скорость сходимости удовлетворяет неравенству

$$|t_{n+1} - \sqrt[3]{a}| \leqslant \frac{4}{3\sqrt[3]{a^2}}|t_n - \sqrt[3]{a}|^3 \leqslant \frac{16}{3}|t_n - \sqrt[3]{a}|^3.$$

§ 2. Последовательность Фибоначчи

Начнем рассмотрение со следующего примера. Пусть задано множество всех двоичных слов длины n, $n \geqslant 1$. Обозначим через f_n количество всех слов длины n, не содержащих двух нулей подряд. Отметим, что эта задача не имеет смысла при $n = 1$ и $n = 2$, но значения $f_0 = 1$ и $f_1 = 2$ согласуются с соотношениями, полученными далее. Перечислим все слова длины 2, не содержащие двух нулей подряд: $01, 10, 11$. Таким образом, имеем $f_2 = 3$. Выведем формулу $f_n = f_{n-1} + f_{n-2}$ по индукции. Предположим, что эта формула верна для f_k при $k < n$. Все слова длины n разобьем на два класса. К первому классу отнесем слова, имеющие 1 последним символом. Остальные слова отнесем ко второму классу. Рассмотрим любое слово из первого класса, не содержащее двух нулей подряд. Для него

все остальные $n-1$ символ можно выбрать произвольно с условием, что подряд не находятся два нуля. Это означает, что в первый класс входят f_{n-1} слов. Пусть теперь слово находится во втором классе. Тогда 0 является его последним символом, а предпоследним символом может быть только 1. Оставшаяся часть слова из $n-2$ символов строится произвольно, только, чтобы в нем не было двух подряд идущих нулей. Значит, во втором классе будет f_{n-2} слов. Тем самым в формуле каждый последующий член равен сумме двух предыдущих. Этот ряд чисел называется последовательностью Фибоначчи.

Выведем далее формулу для f_n как функцию от n, т.е. найдем $F(n) = f_n$. С последовательностью $f_0, f_1, f_2, \ldots, f_n, \ldots$ свяжем производящий ряд

$$\Phi(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n + \ldots.$$

Поскольку $0 < f_n < 2^n$, радиус круга сходимости данного ряда будет положителен. Домножим этот ряд на x и получившийся ряд сложим с первоначальным. Находим

$$(1+x)\Phi(x) = f_0 + (f_1 + f_0)x + (f_2 + f_1)x^2 + \ldots + (f_n + f_{n-1})x^n + \ldots =$$
$$= 1 + \sum_{k=1}^{\infty} f_{k+1} x^k = 1 + \left(\sum_{k=2}^{\infty} f_k x^k \right) / x = 1 + \left(\Phi(x) - 1 - 2x\right) / x.$$

Отсюда получим

$$\Phi(x)(1 - x - x^2) = 1 + x.$$

Следовательно, имеем

$$\Phi(x) = \frac{1+x}{1-x-x^2} = \frac{A}{x-\alpha_1} + \frac{B}{x-\alpha_2},$$

где

$$\alpha_1 = -\frac{1+\sqrt{5}}{2}, \quad \alpha_2 = \frac{\sqrt{5}-1}{2}$$

корни квадратного уравнения $x^2 + x - 1 = 0$, кроме того,

$$A = \frac{1}{2}\left(\frac{1}{\sqrt{5}} - 1\right), \quad B = -\frac{1}{2}\left(\frac{1}{\sqrt{5}} + 1\right).$$

Разлагая простейшие дроби в степенной ряд, найдем

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right).$$

Пусть, теперь, задана некоторая последовательность чисел u_0, u_1, …, u_n, … или запишем коротко $\{u_n\}$, $n \geqslant 0$. *Производящей функцией* или производящим рядом этой последовательности называется

степенной ряд вида

$$G(x) = u_0 + u_1 z + \ldots + u_n z^n + \ldots \quad \text{или коротко} \quad G(x) = \sum_{n=0}^{\infty} u_n z^n.$$

Будем предполагать, что степенной ряд $G(z)$ имеет положительный радиус круга сходимости, т.е. представляет собой аналитическую функцию в точке $z = 0$. Заметим, что если последовательность $\{u_n\}$ ограничена, то производящий ряд $G(z)$ сходится внутри единичного круга $|z| < 1$.

Над производящими рядами можно определить арифметические операции: сложение двух рядов, умножение ряда на скаляр, перемножение двух рядов. Непосредственно можно проверить, что справедливо тождество

$$(1 - z)(1 + z + z^2 + \ldots + z^n + \ldots) = 1,$$

т.е. ряд $1 - z$ обратим в кольце степенных рядов. Более того, для того чтобы ряд $G(z) = \sum\limits_{n=0}^{\infty} u_n z^n$ имел обратный элемент относительно умножения в кольце степенных рядов, необходимо и достаточно, чтобы $u_0 \neq 0$, т.е. $G(0) \neq 0$.

Действительно, необходимость следует из равенства $G(z)H(z) = 1$, $H(z) = \sum\limits_{n=0}^{\infty} v_n z^n$. Отсюда имеем $u_0 v_0 = 1$, т.е. $u_0 \neq 0$. Докажем достаточность. По условию имеем, что $u_0 \neq 0$. Рассмотрим ряд $G_1(z) = G(z)/u_0 = 1 - F(z)$, причем $F(0) = 0$. Далее найдем

$$\big(1 - F(z)\big)\big(1 + F(z) + (F(z))^2 + \ldots + (F(z))^n + \ldots\big) = 1.$$

Коэффициенты ряда $H_1(z) = \sum\limits_{n=0}^{\infty} (F(z))^n$ могут рекуррентным образом выражены через u_0, u_1, …, u_n, … и $G_1(z)H_1(z) = 1$, т.е. $H(z) = u_0 H_1(z)$ является обратным к ряду $G(z)$.

Приведем таблицу наиболее известных производящих рядов, отвечающих им последовательностей и радиусов их кругов сходимости.

$G(z)$	u_k	r
$(1+z)^n$	$\binom{n}{k}$	$\mathbf{C}$
$(1-az)^{-1}$	a^k	$\lvert z\rvert < 1$
$(1+z)^\alpha$	$\alpha(\alpha-1)\ldots(\alpha-k+1)/k!$	$\lvert z\rvert < 1$
e^z	$1/k!$	$\mathbf{C}$
$\ln(1+z)$	$(-1)^{k-1}/k$	$\lvert z\rvert < 1$

§ 3. Линейные рекуррентные уравнения второго порядка

Сначала рассмотрим линейное рекуррентное уравнение второго порядка, поскольку можно явно выписать решение этого уравнения. Уравнение имеет следующий вид

$$u_{n+2} = au_{n+1} + bu_n, \quad n \geqslant 0.$$

Здесь a и b — абсолютные постоянные. Пусть также заданы начальные условия $u_0 = a_0$, $u_1 = a_1$.

Решить линейное рекуррентное уравнение означает, что надо u_n как функцию от n, т.е. представить u_n в виде $u_n = U(n)$.

Пусть, теперь, $G(z)$ — производящая функция последовательности $\{u_n\}$, $n \geqslant 0$. Тогда, сложив два равенства

$$\begin{aligned} azG(z) &= au_0z + au_1z^2 + \ldots + au_{n-1}z^n + \ldots, \\ bz^2G(z) &= \qquad bu_0z^2 + \ldots + bu_{n-2}z^n + \ldots, \end{aligned}$$

получим

$$(az + bz^2)G(z) = G(z) - a_0 - (a_1 - aa_0)z.$$

Отсюда находим

$$G(z) = \frac{a_0 + (a_1 - aa_0)z}{1 - az - bz^2}.$$

Пусть имеет место разложение

$$1 - az - bz^2 = (1 - \alpha z)(1 - \beta z), \alpha \neq \beta.$$

Тогда справедливо следующее разложение на простейшие дроби

$$G(z) = \frac{1}{\alpha - \beta}\left(\frac{a_1 - aa_0 + \alpha a_0}{1 - \alpha z} - \frac{a_1 - aa_0 + \beta a_0}{1 - \beta z}\right).$$

Отсюда получим u_n как функцию от n, рассматривая коэффициент при z^n. Имеем

$$u_n = (a_1 - aa_0)\frac{\alpha^n - \beta^n}{\alpha - \beta} + a_0\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}.$$

§ 4. Линейные рекуррентные уравнения произвольного порядка

Пусть последовательность $\{u_n\}, n \geqslant 0$, удовлетворяет линейному с постоянными коэффициентами рекуррентному уравнению порядка r следующего вида

$$u_{n+r} = a_1u_{n+r-1} + a_2u_{n+r-2} + \ldots + a_ru_n, \quad n \geqslant 0,$$

причем заданы первые r членов последовательности $u_s = c_s$, $0 \leqslant s \leqslant r - 1$, числа c_s — абсолютные постоянные и они задают начальные условия для данного рекуррентного уравнения. Будем счи-

тать также, что $a_r \neq 0$. Тогда производящая функция последовательности $\{u_n\}$, $n \geqslant 0$ представляет собой следующее выражение $G(z) = \sum\limits_{n=0}^{\infty} u_n z^n$.

Определим многочлен

$$K(z) = 1 - a_1 z - a_2 z^2 - \ldots - a_r z^r.$$

Используя рекуррентное уравнение, имеем

$$G(z)K(z) = c_0 + c_1 z + \ldots + c_{r-1} z^{r-1} = C(z).$$

Следовательно, $G(z) = C(z)/K(z)$. Далее, над полем комплексных чисел имеем разложение

$$K(z) = (1 - \alpha_1 z)^{e_1}(1 - \alpha_2 z)^{e_2} \ldots (1 - \alpha_k z)^{e_r},$$

$$e_1 + e_2 + \ldots + e_k = r, \quad e_1, e_2, \ldots, e_k \geqslant 1,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_k$ — корни характеристического многочлена

$$H(z) = z^r - a_1 z^{r-1} - \ldots - a_r = (z - \alpha_1)^{e_1}(z - \alpha_2)^{e_2} \ldots (z - \alpha_k)^{e_k},$$

$e_1 + e_2 + \ldots + e_k = r$, причем $K(z) = z^r H(1/z)$.

Разложим теперь производящую функцию $G(z)$ на простейшие дроби. При некоторых постоянных β_{ks} получим

$$G(z) = \frac{C(z)}{K(z)} = \sum_{m=1}^{k} \sum_{s=1}^{e_k} \frac{\beta_{ks}}{(1 - \alpha_m z)^s}.$$

Таким образом достаточно разложить в степенной ряд бином $B = \beta(1 - \alpha z)^{-s}$. Находим

$$B = \beta\Bigg(1 + (-s)(-\alpha z) + \ldots + \frac{(-s)(-s-1)\ldots(-s-n+1)}{n!}(-\alpha z)^n + \ldots\Bigg) = \beta \sum_{n=0}^{\infty} \binom{n+s-1}{n} (\alpha z)^n.$$

Следовательно, внутренняя сумма в разложении $G(z)$ на простейшие дроби имеет вид

$$\sum_{s=1}^{e_k} \frac{\beta_{ks}}{(1 - \alpha_m z)^s} = \sum_{s=1}^{e_k} \beta_{ks} \sum_{n=0}^{\infty} \binom{n+s-1}{n} (\alpha_m z)^n =$$

$$= \sum_{n=0}^{\infty} \sum_{s=1}^{e_k} \beta_{ks} \binom{n+s-1}{n} (\alpha_m z)^n = \sum_{n=0}^{\infty} P_m(n) \alpha_m^n z^n,$$

где $P_m(n)$ — многочлен, степень которого не превосходит $e_m - 1$.

Отсюда находим

$$u_n = \sum_{m=1}^{k} P_m(n)\alpha_m^n.$$

§ 5. Рекуррентные соотношения первого порядка в кольцах вычетов

Пусть, теперь, для любого натурального n задано рекуррентное соотношение $x_{n+1} = f(x_n)$ и множество значений x_n конечно и не превосходит N. Тогда в последовательности $x_1, x_2, \ldots, x_k$ при $k > N$ найдутся одинаковые значения x_s. Значит, последовательность $\{x_n\}$ имеет период, не превосходящий N. Периодом последовательности $\{x_n\}$ называется минимальное натуральное число T такое, что $x_{n+T} = x_n$ при всех n, превосходящих некоторое число n_0.

Рассмотрим последовательность $\{x_n\}$, заданную рекуррентным соотношением $x_{n+1} \equiv ax_n \pmod N$ по некоторому натуральному модулю $N \geqslant 2$ и $(a, N) = 1$. Из определения имеем $x_n \equiv a^{n-1}x_1 \pmod N$. Пусть T — наименьшее натуральное число с условием $a^T \equiv 1 \pmod N$. Тогда T является периодом последовательности $\{x_n\}$.

Наконец, пусть задана последовательность вида $x_{n+1} \equiv ax_n + c \pmod m$. Вновь обратимся к задаче о нахождении периода этой последовательности. Справедлива следующая теорема.

Теорема. *Для того чтобы последовательность* $x_{n+1} \equiv ax_n + c \pmod m$ *имела период* m *необходимо и достаточно, чтобы выполнялись следующие условия*

а) *числа* c *и* m *взаимно просты,*

б) *число* $a - 1$ *делится на любой простой делитель числа* m,

в) *число* $a - 1$ *делится на* 4, *если* $4 \mid m$.

▷ Пусть $m = m_1m_2$ и $(m_1, m_2) = 1$. Представим x_n, a, c в виде $x_n \equiv m_2y_n + mm_1 \pmod m, a \equiv m_2a_1 + m_1a_2 \pmod m, c \equiv m_2c_1 + m_1c_2 \pmod m$, где y_n, a_1, c_1 могут принимать значения из полной системы вычетов по модулю m_1, а вычеты z_n, a_2, c_2 — из полной системы вычетов по модулю m_2. Тогда по решению x_n сравнения $x_{n+1} \equiv ax_n + c \pmod m$ однозначно находятся решения y_n, z_n системы сравнений

$$y_{n+1} \equiv a_1y_n + c_1 \pmod{m_1}, z_{n+1} \equiv a_2z_n + c_2 \pmod{m_2},$$

и наоборот.

Пусть T_1 — период последовательности $\{y_n\}$ и T_2 — период последовательности $\{z_n\}$. Тогда период T последовательности $\{x_n\}$ равен наименьшему общему кратному чисел T_1 и T_2.

Необходимость. Дано, что последовательность $x_{n+1} \equiv ax_n + c \pmod m$ имеет период m, т.е. число m является минимальным натуральным числом таким, что для любого n справедливо сравнение $x_{n+m} \equiv x_n \pmod m$.

Докажем сначала, что числа c и m взаимно просты. Рассуждаем от противного. Пусть существует простое число p с условием $p \mid (c, m)$. Тогда $x_{n+1} \equiv ax_n \pmod p$ и последовательность $\{x_n\}$ по модулю p должна иметь период p. Если $p \mid a$, то этот период равен 1, а если $(a, p) = 1$, то максимальное значение периода будет равно $p-1$ при условии, что a является первообразным корнем по модулю p. Итак, при любом значении величины a период по модулю p последовательности $\{x_n\}$ меньше p. Это противоречит условию теоремы. Следовательно, $(c, m) = 1$.

Пусть $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение на простые сомножители числа m. Поскольку период по модулю m последовательности $\{x_n\}$ равен m, в силу предыдущего рассмотрения достаточно положить $m = p^\alpha$, где p — простое число и α — любое натуральное число.

Докажем, что $p \mid (a-1)$. Предположим, что $a \not\equiv 1 \pmod p$. Далее, из определения последовательности $\{x_n\}$ при $a \not\equiv 1 \pmod p$ находим

$$x_{n+m} \equiv ax_{n+m-1} + c \equiv a^2 x_{n+m-2} + ac + c \equiv \dots \equiv$$
$$\equiv a^m x_n + c\frac{a^m - 1}{a - 1} \pmod m.$$

Отсюда получим

$$(a^m - 1)x_n + c\frac{a^m - 1}{a - 1} \equiv 0 \pmod m.$$

Следовательно, из справедливости этого сравнения при любом x_n из полной системы вычетов по модулю m имеем

$$\frac{a^m - 1}{a - 1} \equiv 0 \pmod m.$$

Из этого сравнения находим $a^m \equiv 1 \pmod m$. Откуда следует, что $a^{p^\alpha} \equiv 1 \pmod p$, но это сравнение противоречит теореме Эйлера $a^{p^\alpha} \equiv a^p \equiv a \pmod p$. Необходимость условия $p \mid (a-1)$ доказана.

Пусть теперь $4 \mid m$ и $m = 2^\alpha m_1, (m_1, 2) = 1$ и $\alpha \geqslant 2$. Тогда достаточно рассмотреть случай $m = 2^\alpha, \alpha \geqslant 2$. Покажем, что $4 \mid (a-1)$. Предположим противное, т.е. $a \equiv 3 \pmod 4$. Из условия, что период по модулю 2^α последовательности $\{x_n\}$ равен 2^α, по аналогии с предыдущим находим

$$\frac{a^{2^\alpha} - 1}{a - 1} \equiv 0 \pmod{2^\alpha}.$$

Индукцией по параметру $\alpha \geqslant 2$ при $a \equiv 3 \pmod 4$ докажем, что

$$\frac{a^{2^{\alpha-1}}-1}{a-1} \equiv 0 \pmod{2^\alpha}.$$

Это утверждение противоречит предыдущему.

При $\alpha = 2$ получим

$$\frac{a^2-1}{a-1} \equiv a+1 \equiv 0 \pmod 4.$$

Предположим, что утверждение имеет место при $\alpha = n$, т.е.

$$\frac{a^{2^{n-1}}-1}{a-1} \equiv 0 \pmod{2^n}.$$

Докажем утверждение при $\alpha = k+1$. Имеем

$$\frac{a^{2^k}-1}{a-1} \equiv \frac{(a^{2^{k-1}}-1)(a^{2^{k-1}}-1)}{a-1} \equiv 0 \pmod{2^{k+1}}.$$

Таким образом необходимость полностью доказана.

Достаточность. Пусть p — простое число и α — натуральное число. Достаточно доказать, что период последовательности $\{u_n\}$, заданной сравнением $u_{n+1} \equiv Au_n + C \pmod{p^\alpha}$, при условиях $(C,p) = 1, p \mid (A-1)$ (p — нечетное простое число) или $4 \mid (A-1)$, если $4 \mid 2^\alpha$, равен p^α. Имеем

$$u_{n+p^\alpha} \equiv A^{p^\alpha}u_n + C(A^{p^\alpha-1} + \ldots 1) \pmod{p^\alpha}, u_{n+p^\alpha} \equiv u_n \pmod{p^\alpha}.$$

Следовательно, при $A \not\equiv 1 \pmod p$ для любого номера n получим

$$u_n(A^{p^\alpha}-1) + C\frac{A^{p^\alpha}-1}{A-1} \equiv 0 \pmod{p^\alpha}.$$

Таким образом для того, чтобы последовательность $\{u_n\}$ по модулю p^α имела период p^α при $A \equiv 1 \pmod p$ достаточно установить соотношения

$$A^{p^\alpha} \equiv 1 \pmod{p^\alpha}, \quad A^{p^{\alpha-1}} \not\equiv 1 \pmod{p^\alpha}.$$

Но при $A \not\equiv 1 \pmod p, (A,p) = 1$ имеем

$$A^{p^\alpha} \equiv A \pmod p,$$

что противоречит предыдущим соотношениям. Итак, следующие условия $(A,C) = 1$ и $A \equiv 1 \pmod 4$ обеспечивают период p^α последовательности $\{u_n\}$ по модулю p^α.

Аналогично, по модулю 2^α, $\alpha \geqslant 2$ условия $(A,C) = 1$ и $A \equiv 1 \pmod 4$ обеспечивают период 2^α последовательности $\{u_n\}$. Достаточность доказана. ◁

§ 6. Рекуррентные соотношения произвольного порядка в конечных полях

Пусть задано конечное поле $\mathbf{F}_q$ из $q = p^m$ элементов, где p — любое простое число и m — любое натуральное число. Пусть элементы $a_1, a_2, \ldots, a_r$ принадлежат полю $\mathbf{F}_q$, $r \geqslant 1$ — натуральное число. В поле $\mathbf{F}_q$ определим рекуррентную последовательность $\{u_n\}, n \geqslant 0$, удовлетворяющую линейному с постоянными коэффициентами $a_1, a_2, \ldots, a_r$ рекуррентному уравнению порядка r следующего вида

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \ldots + a_r u_n, \quad n \geqslant 0, \tag{1}$$

причем заданы первые r членов последовательности $u_s = c_s, 0 \leqslant s \leqslant r-1$, числа c_s — абсолютные постоянные из $\mathbf{F}_q$. Они задают начальные условия для данного рекуррентного уравнения. Будем считать, что $a_r \neq 0$ в $\mathbf{F}_q$.

Положим $a_0 = -1$. Тогда (1) примет вид

$$\sum_{s=0}^{r} a_s u_{n+r-s} = 0. \tag{2}$$

Последнее соотношение (2) дает возможность доопределить последовательность u_n для всех целых номеров n. При всех положительных n последовательность u_n совпадает с ранее определенной последовательностью.

Из (2) следует, что для любого целого числа n член последовательности u_{n+r} зависит только от r предыдущих членов последовательности $u_{n+r-1}, u_{n+r-2}, \ldots, u_n$. Далее, только нулевой r-набор $(u_{r-1}, u_{r-2}, \ldots, u_0)$, $u_s = c_s = 0$, $0 \leqslant s \leqslant r-1$, даст нулевую последовательность $u_n = 0$ для любого $n \geqslant 0$. Всего различных ненулевых r-наборов с элементами из поля $\mathbf{F}_q$ будет $q^r - 1$. Стало быть, при различных m и n встретятся одинаковые r-наборы $(u_{m+r-1}, u_{m+r-2}, \ldots, u_m)$ и $(u_{n+r-1}, u_{+r-2}, \ldots, u_n)$. Это означает, что $u_{m+r} = u_{n+r}$, т.е. для любого целого k справедливо равенство $u_k = u_{n-m+k}$ в $\mathbf{F}_q$. Следовательно, последовательность u_n имеет ненулевой период $T \leqslant |n-m| \leqslant q^r - 1$, более того, она является чисто периодической.

Дадим другое представление последовательности (1). Для этого определим рекуррентные последовательности $\psi_1(x), \ldots, \psi_r(x)$, удовлетворяющие при $1 \leqslant s \leqslant r$ уравнению (1) с начальными условиями вида

$$\psi_s(x) = \begin{cases} 1, & \text{если} \quad x = s, \\ 0, & \text{если} \quad x \neq s, \end{cases}$$

где $1 \leqslant x \leqslant r$.

Лемма 1. *Справедливо следующее равенство*

$$u_{n+m} = u_{n+1}\psi_1(m) + \ldots + u_{n+r}\psi_r(m). \tag{3}$$

▷ По условию леммы имеем, что при $m = 1, 2, \ldots, r$ равенство (3) имеет место. Далее, каждая из последовательностей $\{u_{n+1}\}$, …, $\{u_{n+r}\}$ является решением (1) со своими начальными условиями. Из линейности уравнения (1) находим, что любая линейная комбинация этих решений также будет решением (1). Следовательно, равенство (3) справедливо при любых n и m. ◁

Последовательности (1) поставим в соответствие *характеристический многочлен*

$$f(x) = 1 - a_1 x - a_2 x^2 - \ldots - a_r x^r = -\sum_{s=0}^{r} a_s x^s.$$

Пусть $T \geqslant 1$ — период последовательности u_n. Определим многочлен $g(x) = \sum\limits_{t=0}^{T-1} u_t x^t$. Тогда справедливо следующее утверждение.

Лемма 2. *Имеет место равенство*

$$f(x)g(x) = (1 - x^T)h(x),$$

где

$$h(x) = \sum_{m=0}^{r-1} h_m x^m, \; h_m = \sum_{s=0}^{m} a_s u_{m-s}.$$

▷ Используя периодичность последовательности u_n с периодом T, при $|x| < 1$ находим

$$U(x) = \sum_{t=0}^{\infty} u_t x^t = \left(\sum_{t=0}^{T-1} u_t x^t\right)(1 + x^T + x^{2T} + \ldots) = \frac{g(x)}{1 - x^T}.$$

Далее, имеем

$$U(x)f(x) = \left(\sum_{t=0}^{\infty} u_t x^t\right)\left(\sum_{s=0}^{r} a_s x^s\right) = \sum_{m=0}^{\infty} x^m \sum_{\substack{s=0 \\ s+t=m}}^{r} a_s u_t.$$

При $m \geqslant r$ из (1) получим

$$\sum_{\substack{s=0 \\ s+t=m}}^{r} a_s u_t = \sum_{s=0}^{r} a_s u_{m-s} = 0.$$

Следовательно, $U(x)f(x) = h(x)$, где

$$h(x) = \sum_{m=0}^{r-1} h_m x^m,\ h_m = \sum_{\substack{s=0 \\ s+t=m}}^{r} a_s u_t = \sum_{s=0}^{m} a_s u_{m-s} \quad \text{при} \quad m \leqslant r-1.$$

Отсюда находим

$$\frac{f(x)g(x)}{1-x^T} = h(x). \qquad \triangleleft$$

Для многочленов с коэффициентами из конечного поля имеет место следующее утверждение.

Лемма 3. *Пусть многочлен $f(x) \in \mathbf{F}_q[x]$ и $f(0) \neq 0$. Тогда найдется натуральное число C такое, что $f(x)$ является делителем многочлена $x^C - 1$. Более того, для характеристического многочлена $f(x)$ последовательности (1) с начальными условиями $u_0 = \ldots = u_{r-2} = 0$, $u_{r-1} = 1$, и для многочлена $g(x) = \sum\limits_{t=0}^{T} u_t x^t$ справедливо равенство $f(x)g(x) = x^{r-1}(x^T - 1)$.*

$\triangleright$ Без ограничения общности можно считать, что $f(0) = 1$ и многочлен $f(x)$ имеет вид

$$f(x) = 1 - a_1 x - a_2 x^2 - \ldots - a_r x^r = -\sum_{s=0}^{r} a_s x^s,\ a_0 = -1.$$

Зададим специальные начальные условия для рекуррентного уравнения (1): $u_0 = \ldots = u_{r-2} = 0$, $u_{r-1} = 1$. Получим периодическую последовательность u_n с периодом $T \geqslant 1$. Положим $g(x) = \sum\limits_{t=0}^{T-1} u_t x^t$. Далее применяем лемму 2. Имеем

$$f(x)g(x) = (1 - x^T)h(x),$$

где

$$h(x) = \sum_{m=0}^{r-1} h_m x^m, \quad h_m = \sum_{s=0}^{m} a_s u_{m-s}.$$

Для коэффициентов многочлена $h(x)$ находим цепочку равенств

$$\begin{gathered} c_0 = a_0 u_0 = 0, \\ c_1 = a_0 u_1 + a_1 u_0 = 0, \\ \ldots \qquad \ldots \qquad \ldots \\ c_{r-1} = a_0 u_{r-1} + a_1 u_{r-2} + \ldots + a_{r-1} u_0 = -1. \end{gathered}$$

Следовательно, $f(x)g(x) = x^{r-1}(x^T - 1)$. Поскольку $f(0) = 1$, многочлен x^{r-1} будет взаимно прост с $f(x)$. Отсюда получим, что многочлен $f(x)$ является делителем $x^T - 1$ в кольце многочленов $\mathbf{F}_q[x]$. $\triangleleft$

Утверждение леммы 3 позволяет дать следующее определение. Назовем *порядком многочлена* $f(x)$ из $\mathbf{F}_q[x]$ минимальное натуральное число C такое, что $f(x)$ является делителем $x^C - 1$ в кольце многочленов $\mathbf{F}_q[x]$.

Отсюда находим, что порядок $\operatorname{ord} f$ многочлена $f(x)$ не меньше его степени $r = \deg f$.

Из леммы 3 следует, что $C \leqslant T$, где T — период последовательности (1) с начальными условиями $u_0 = \ldots = u_{r-2} = 0$, $u_{r-1} = 1$.

Лемма 4. *Пусть задан многочлен $f(x) \in \mathbf{F}_q[x]$ $f(0) \neq 0$, и пусть при некотором натуральном числе T многочлен $f(x)$ является делителем многочлена $x^T - 1$ в $\mathbf{F}_q[x]$. Пусть, также, $C = \operatorname{ord} f$. Тогда имеем, что $T \equiv 0 \pmod{C}$, т.е. число T делится на C.*

$\triangleright$ Разделим натуральное число T с остатком на C. Получим $T = uC + v$, $0 \leqslant v < C$. Поскольку $T \geqslant C$, находим, что $u \geqslant 1$. По условию леммы имеем, что найдутся многочлены $g_C(x)$ и $g_T(x)$, удовлетворяющие соотношениям

$$f(x)g_C(x) = x^C - 1,\ f(x)g_T(x) = x^T - 1.$$

Отсюда находим

$$f(x)(g_T(x) - g_C(x)) = x^C(x^{T-C} - 1).$$

Так как $(f(x), x^C) = 1$, то $f(x) \mid (x^{T-C} - 1)$. Следовательно, найдется многочлен $G_1(x)$ такой, что $f(x)G_1(x) = x^{T-C} - 1$. Далее, имеем

$$f(x)(G_1(x) - g_C(x)) = x^C(x^{T-2C} - 1).$$

Продолжая этот процесс u раз, найдем $f(x)G_u(x) = x^v - 1$. Неравенство $v > 0$ противоречит условию минимальности выбора натурального числа C с условием $f(x)g_C(x) = x^C - 1$. Следовательно, $v = 0$ и число T делится на C. $\triangleleft$

Лемма 5. *Пусть порядок характеристического многочлена $f(x) \in \mathbf{F}_q[x]$, $f(0) \neq 0$, последовательности (1) равен C, и пусть натуральное число T является периодом этой последовательности в $\mathbf{F}_q$ с начальными условиями $u_0 = \ldots = u_{r-2} = 0$, $u_{r-1} = 1$. Тогда имеем, что $T = C$.*

$\triangleright$ По лемме 4 имеем, что $T = uC$, $u \geqslant 1$. Далее воспользуемся леммой 2. Получим $f(x)g(x) = x^{r-1}(x^{uC} - 1)$. Из определения мно-

гочлена $g(x)$ и условия $T \geqslant r$ находим

$$g(x) = \sum_{t=0}^{T-1} u_t x^t = \sum_{t=r-1}^{T-1} u_t x^t = x^{r-1} \sum_{t=0}^{T-r} u_{t+r-1} x^t = x^{r-1} G(x).$$

Следовательно,

$$G(x) = (1 + x^C + \ldots + x^{(u-1)C}) g_0(x), \tag{4}$$

где $f(x)g_0(x) = x^C - 1$, причем степень многочлена $g_0(x)$ равна $C - r$ и свободный член $g_0(x)$ равен 1.

Из (4) имеем, что $u_C = \ldots = u_{C+r-2} = 0$ и $u_{C+r-1} = 1$. Таким образом, период последовательности (1) с начальными условиями $u_0 = \ldots = u_{r-2} = 0$ и $u_{r-1} = 1$ не превосходит C. С другой стороны, число C делитель периода этой последовательности, т.е. не меньше C. Значит, период этой последовательности равен C. ◁

Далее, понадобится определение неприводимого многочлена над полем $\mathbf{F}_q$. Говорят, что многочлен $f(x)$ из $\mathbf{F}_q[x]$ неприводим над полем $\mathbf{F}_q$, если не существует многочленов $g(x),\ h(x) \in \mathbf{F}_q[x]$, таких, что $f(x) = g(x)h(x)$.

Лемма 6. *Пусть порядок характеристического многочлена $f(x) \in \mathbf{F}_q[x],\ f(0) \neq 0$, последовательности (1) равен C, и пусть натуральное число T является периодом этой последовательности в $\mathbf{F}_q$ с начальными условиями $u_0 = \ldots = u_{s-1} = 0,\ u_s = 1,\ u_{s+1} = u_{r-1} = 0$, где s — любое целое число из промежутка от 0 до $r-1$, т.е. последовательность u_n совпадает с последовательностью $\psi_s(n)$, введенной выше. Тогда имеем, что $T = C$.*

▷ Предыдущая лемма была доказана для последовательности $\psi_{r-1}(n)$ и в этом случае по формулировке она совпадает с леммой 6. Для последовательностей $\psi_s(n),\ s = 0, \ldots, r-2$ ход доказательства леммы 6 ничем не отличается доказательства леммы 5. ◁

Лемма 7. *Пусть характеристический многочлен $f(x) \in \mathbf{F}_q[x]$ последовательности (1) неприводим над $\mathbf{F}_q$ и пусть начальные условия таковы: $u_0 = c_0,\ \ldots,\ u_{r-2} = c_{r-2},\ u_{r-1} = c_{r-1}$, где $c_0 \ldots c_{r-2}c_{r-1} \neq 0$. Тогда последовательность (1) является чисто периодической с периодом, равным порядку многочлена $f(x)$.*

▷ По лемме 1 для любых m и n имеем

$$u_{n+m} = u_{m-1}\psi_1(n) + \ldots + u_{m-r+1}\psi_{r-1}(n).$$

В частности, пусть C — период каждой из последовательностей $\psi_1(n), \ldots, \psi_r(n)$. По лемме 6 он совпадает с порядком характеристического многочлена $f(x)$ этой последовательности. Отсюда находим

$$u_{n+m+C} = u_{m-1}\psi_1(n+C) + \ldots + u_{m-r+1}\psi_r(n+C) =$$

$$u_{m-1}\psi_1(n) + \ldots + u_{m-r+1}\psi_{r-1}(n) = u_{n+m},$$

т.е. период T последовательности u_n не превосходит C.

С другой стороны, по лемме 4 справедливо неравенство $T \geqslant C$. Следовательно, $T = C$, и последовательность u_n будет чисто периодической. ◁

Лемма 8. *Пусть многочлен $f(x) \in \mathbf{F}_q[x]$ неприводим над $\mathbf{F}_q$ и пусть его степень равна r. Тогда порядок многочлена $f(x)$ является делителем числа $q^r - 1$.*

▷ По лемме 7 любая последовательность (1) с ненулевыми начальными условиями имеет период, равный C — порядку характеристического многочлена $f(x)$. Из неприводимости многочлена $f(x)$ следует, что $f(0) \neq 0$. Число всех различных последовательностей (1) с ненулевыми начальными условиями в количестве r будет равно $q^r - 1$. Как и ранее, будем считать, что последовательность (1) определена для всех целых n. Тогда последовательности, полученные сдвигом номера n на любое целое число, будут совпадать с первоначальной последовательностью, но они отвечают различным начальным условиям $(u_0, u_1, \ldots, u_{r-1})$. Так как значения последовательности определяются ее значениями на периоде, то все начальные условия разбиваются на непересекающиеся подмножества по $C = \operatorname{ord} f$ элементов в каждом. Таким образом доказано, что C делит $q^r - 1$. ◁

Лемма 9. *Пусть многочлен $f(x) \in \mathbf{F}_2[x]$ неприводим над $\mathbf{F}_2$ и его степень равна r. Пусть, также, число $2^r - 1$ — простое. Тогда период ненулевой последовательности u_n с характеристическим многочленом $f(x)$ равен числа $2^r - 1$.*

▷ По предыдущей лемме длина C периода последовательности (1) является делителем простого числа $2^r - 1$. Следовательно, $C = 2^r - 1$.◁

Заметим, что простые числа вида $2^r - 1$ называются *простыми числами Мерсенна,* причем r также является простым числом. Имеется гипотеза, что простых чисел Мерсенна бесконечно много. Не доказано также, что простые числа Мерсенна имеют нулевую плотность во множестве всех чисел Мерсенна. Другими словами, обозначим через $\pi_M(x)$ количество простых $p_1 = 2^p - 1$, где p пробегает все простые числа, не превосходящие x. Тогда предполагают, что $\lim\limits_{x\to\infty} \pi_M(x)/\pi(x) = 0$, где $\pi(x)$ — количество всех простых чисел, не превосходящих x.

Глава V

АРИФМЕТИЧЕСКИЙ ПОДХОД К ИСКАЖЕНИЮ ЗНАКОВ В ШИФРАХ ПРОСТОЙ ЗАМЕНЫ И ВИЖЕНЕРА

§ 1. Введение

Наиболее простой тип преобразования исходного текста состоит в том, что происходит замена каждой буквы алфавита некоторой буквой с помощью подстановки этого алфавита. Такой шифр называется шифром простой однобуквенной замены.

Метод вскрытия шифра простой замены при достаточно большой длине текста использует частотные характеристики появления фиксированной буквы или сочетания букв первоначального открытого текста, которые совпадают с частотными характеристиками зашифрованного текста. Подтверждением устойчивости этой характеристики служит закон больших чисел, согласно которому частота появления любой фиксированной буквы в достаточно длинном тексте при дополнительной гипотезе о независимости появления каждой буквы практически одна и та же на протяжении всего текста. Опыт показывает, что с определенной точностью этот закон справедлив для реальных открытых текстов (например, текстов литературных произведений прозы). Имеются таблицы частот появления букв в разнообразных текстах различных языков мира.

Первое, дошедшее до нас, описание подобного частотного метода криптоанализа относится к IX веку [43], с.30–32. Оно принадлежит известному "философу арабского мира" Абу Юсуф Якуб ибн Исхак ибн ас-Сабах ибн Умран ибн Исмаил аль-Кинди. Его знаменитый трактат "Рукопись по дешифрованию криптографических сообщений" был открыт в 1987 г. в Стамбуле в оттоманском архиве Сулаймания. Как указывает С. Сингх [43], в этом трактате дан подробный анализ статистики, фонетики и синтаксиса арабского языка и приведена "революционная система криптоанализа аль-Кинди, которая умещается в следующие два коротких абзаца.

Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, это взять другой незашиф-

рованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву “первой”, букву, которая по частоте появления стоит на втором месте, назовем “вторая”, букву, которая по частоте появления стоит на третьем месте, назовем “третья” и т.д., пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его “первой” буквой незашифрованного текста, второй по частоте появления символ заменим “второй” буквой, третий по частоте появления символ заменим “третьей” буквой и т.д., пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать.”

Следует отметить, что и сам криптоанализ аль-Кинди мог появиться в то время только при достижении достаточно высокого уровня развития как светского образования в таких науках, как математика, статистика и лингвистика, так и религиозного образования.

Для того, чтобы значительно усложнить задачу вскрытия шифра простой замены применяют методы “рандомизации” и “сжатия” открытых текстов [1], с.106. Они используются в компьютерных архиваторах.

Другой пример “сжатия” алфавита приводится в книге С. Сингха [43] в приложении F (с. 416-417): “Шифр ADFGVX”.

Зашифровывание здесь состоит в том, матрица размером 6×6 заполняется 26 буквами и 10 цифрами в произвольном порядке. Каждая строка и каждый столбец задаются одной из шести букв: A, D, F, G, V и X. Расположение элементов в матрице служит ключом. Например, матрица имеет вид

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Каждый символ в матрице зашифровывается буквами, которые обозначают строку и столбец, в котором находится этот символ. Напри-

мер, **8** заменяется на **AA**, символ **p** — на **AD**.

Таким образом алфавит шифртекста будет использовать только 6 букв: A, D, F, G, V, X. Тем самым, произведено "сжатие" алфавита, но тем не менее для взлома шифрсообщения здесь достаточно воспользоваться частотным анализом для биграмм. Как указано в [43], применение дополнительно перестановки символов с использованием еще одного ключа приводит к более сложному криптоанализу. Буквы A, D, F, G, V, X выбраны с той целью, чтобы они существенно отличались в представлении в виде точек и тире азбуки Морзе.

Отметим также, что указанные выше виды шифрования основаны на комбинаторных соображениях.

Далее предлагается другой подход прямого искажения частот появления знаков в шифрованном тексте, основанный на арифметических функциях извлечения корня квадратного и возведения в квадрат чисел по некоторому модулю.

§ 2. Метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного

Изложим метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного по некоторому модулю. Пусть алфавит открытого текста состоит из n букв. Шифрование исходного текста способом простой однобуквенной замены (см. [27] — [24]) основано на некоторой подстановке множества букв алфавита. Следовательно, эта подстановка является ключом такой криптосистемы, и, значит, количество возможных ключей будет равно $n!$. Отметим, что различным символам шифрованного текста соответствуют различные буквы исходного текста. Далее, в исходном тексте различные буквы, как правило, встречаются с разной частотой при достаточно большой его длине.

В качестве модельной ситуации рассмотрим русский алфавит, состоящий из 31 буквы (отождествляются буквы е,ё и ь,ъ). Известна таблица относительных частот встречаемости букв этого алфавита, упорядоченная в порядке убывания частот, в тексте на русском языке (см., например, [31]). Расположим буквы в порядке убывания частот:

1) о — 0,090, **2)** е, ё — 0,072, **3)** а — 0,062, **4)** и — 0,062,
5) н — 0,053, **6)** т — 0,053 **7)** с — 0,045, ..., **31)** ф — 0,002.

Поскольку число 31 — простое, все вычеты по модулю 31 можно разбить на три класса: квадратичные вычеты, квадратичные невычеты и вычет, отвечающий нулю. Как известно, количество квадратичных невычетов и количество квадратичных вычетов в полной

системе вычетов по простому модулю одинаково и в данном случае оно равно 15. Все квадратичные вычеты по модулю 31 исчерпываются следующими классами вычетов по модулю 31: $1, 2^2, 3^2, \ldots, 15^2$. Занумеруем сначала все наименьшие положительные квадратичные вычеты по модулю 31 по убыванию их величины, а затем также занумеруем квадратичные невычеты в порядке убывания.

Если a — квадратичный вычет по модулю 31, то решения сравнения $x^2 \equiv a \pmod{31}$ представляют собой два различных вычета по модулю 31: $a_1 = b$ и $a_2 = 31 - b$.

Рассмотрим теперь некоторый открытый текст и зашифруем его с помощью метода простой замены. Расположим буквы шифрованного текста в порядке убывания частот, нумеруя их от 1 до 31.

Каждой из первых пятнадцати занумерованных букв взаимно однозначно сопоставим квадратичные вычеты по модулю 31 в соответствии с их порядком нумерации, затем следующие пятнадцать букв взаимно однозначно отобразим в квадратичные невычеты по модулю 31 также в соответствии с их порядком нумерации и, наконец, оставшейся букве сопоставим нулевой вычет по модулю 31.

Далее продолжим шифрование следующим образом. Пусть буква α зашифрована числом a и a — квадратичный вычет по модулю 31, и пусть вычеты a_1, a_2 решения сравнения $x^2 \equiv a \pmod{31}$. Тогда последовательности указанного числа a в криптограмме шифра простой замены ставим в соответствие последовательность чисел $a_1, a_2, a_1, a_2, \ldots$. Например, если в криптограмме имеется 5 мест, на которых стоит число a, то заменяем в этих местах число a на следующую последовательность чисел a_1, a_2, a_1, a_2, a_1. Пусть, теперь, буква α закодирована числом a и a — квадратичный невычет по модулю 31 или 0. Тогда в криптограмме это число a оставляем без изменения.

Для восстановления первоначальной криптограммы надо все числа, отвечающие квадратичным вычетам по модулю 31 возвести в квадрат по модулю 31.

Остается передать получателю текста номера тех мест, на которых стоят квадратичные невычеты по модулю 31. Осуществим это следующим образом.

Последовательно обозначим места, на которых стоят квадратичные вычеты по модулю 31, — единицами, а места, на которых стоят квадратичные невычеты, — нулями. Полученную последовательность чисел $\varepsilon_1, \ldots, \varepsilon_n$, составленную из нулей и единиц, можно рассматривать как запись некоторого числа m в двоичной системе счисления. Таким образом отправителю достаточно передать построенное число m.

Итак, абонент $\mathcal{A}$ должен послать "секретное" число m абоненту $\mathcal{B}$ по каналу связи.

Для этого можно воспользоваться, например, известным алгоритмом А. Шамира для передачи секретной информации по каналу связи (см., например, [31, 47]). Приведем здесь этот алгоритм.

Абоненты $\mathcal{A}$ и $\mathcal{B}$ выбирают достаточно большое простое число $p > m$. Затем абонент $\mathcal{A}$ выбирает секретный ключ a, $1 < a < p-1$, $(a, p-1) = 1$, а абонент $\mathcal{B}$ — секретный ключ b, $1 < b < p-1$, $(b, p-1) = 1$. Для проверки условия взаимной простоты a и $p-1$ абонент $\mathcal{A}$ может использовать алгоритм Евклида. В случае, если числа a и $p-1$ не взаимно просты, то следует проверить на взаимную простоту числа $a+1$ и $p-1$ и т.д. Указанный процесс выбора ключа a оборвется через конечное число шагов, так как, например, $(p-2, p-1) = 1$. Аналогичным образом может поступить и абонент $\mathcal{B}$. Далее абонент $\mathcal{A}$ находит натуральное число α такое, что

$$a\alpha \equiv 1 \pmod{p-1}, \quad 1 < \alpha < p-1.$$

Аналогично поступает абонент $\mathcal{B}$. Он находит число β с условиями

$$b\beta \equiv 1 \pmod{p-1}, \quad 1 < \beta < p-1.$$

Итак, абонент $\mathcal{A}$ имеет секретный ключ (a, α), а абонент $\mathcal{B}$ — секретный ключ (b, β).

Теперь абонент $\mathcal{A}$ пересылает число m абоненту $\mathcal{B}$ по открытому каналу за следующие четыре шага.

1-й шаг. Абонент $\mathcal{A}$ посылает абоненту $\mathcal{B}$ число

$$m_1 \equiv m^a \pmod{p}, \quad 0 < m_1 < p-1.$$

2-й шаг. Абонент $\mathcal{B}$ посылает абоненту $\mathcal{A}$ число

$$m_2 \equiv m_1^b \pmod{p}, \quad 0 < m_2 < p-1.$$

3-й шаг. Абонент $\mathcal{A}$ посылает абоненту $\mathcal{B}$ число

$$m_3 \equiv m_2^\alpha \pmod{p}, \quad 0 < m_3 < p-1.$$

4-й шаг. Абонент $\mathcal{B}$ находит число m с помощью секретного ключа β следующим образом:

$$m = m_4 \equiv m_3^\beta \pmod{p}, \quad 0 < m_4 < p-1.$$

Действительно, имеем

$$m_4 \equiv m^{ab\alpha\beta} = m^{a\alpha \cdot b\beta} \equiv m \pmod{p},$$

т.е. получаем $m_4 \equiv m \pmod{p}$, $\quad 0 < m, m_4 < p-1$.

Следовательно, $m = m_4$.

Далее можно рекуррентным образом продолжить процедуру "сжатия алфавита".

Пусть l — натуральное число и q — простое число вида $q = 2^l + 1$. Тогда простое число q обязано быть простым числом Ферма $q = F_m = 2^{2^m} + 1$, $m \geqslant 0$. На сегодняшний день известно только пять простых чисел Ферма $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 2^8 + 1 = 257$ и $F_4 = 2^{16} + 1 = 65537$. Мультипликативная группа поля F_q является циклической и состоит из $q-1 = 2^l$ элементов. Каждый из них имеет порядок $2^k, 0 \leqslant k \leqslant 2^l$.

Пусть теперь алфавит A состоит из $q = 2^l + 1$, $l = 2^m$, $0 \leqslant m \leqslant 4$, символов. Тогда, используя процедуру, описанную выше, в точности l раз, приходим к шифрованному тексту, алфавит которого отвечает только квадратичным невычетам и нулевому вычету по модулю q. Таким образом алфавит шифрованного текста будет состоять из $(q+1)/2$ символа.

§ 3. Метод искажения знаков в шифре простой замены с помощью возведения в квадрат

Дадим способ искажения частот встречаемости букв в шифртексте, полученного простой заменой и основанного на арифметической функции возведения в квадрат по некоторому модулю.

Опишем процедуру шифрования.

Пусть, как и раньше, алфавит сообщения состоит из 31 буквы (например, русский алфавит, в котором отождествляются буквы е,ё и ь,ъ).

Разобьем все вычеты по модулю 31 на два класса: первый класс состоит из 15 квадратичных невычетов, второй — из 15 квадратичных вычетов и нуля.

1) Зашифруем открытый текст методом простой замены с помощью некоторой подстановки.

2) Расположим буквы шифрованного текста в порядке убывания частот. После этого каждой из первых пятнадцати букв присвоим последовательные значения квадратичных невычетов по модулю 31 в соответствии с их порядком нумерации, затем остальным буквам присваиваются последовательные значения квадратичных вычетов и 0.

3) Далее, тем буквам зашифрованного текста в соответствии с пунктом 2), которым соответствуют квадратичные невычеты поставим в соответствие квадраты этих чисел по модулю 31 из отрезка $[0, 30]$, а для букв, отвечающих квадратичным вычетам и нулю, сохраним те же значения квадратичных вычетов и нуля.

4) Подведем итог процедуры шифрования. Итак, получен зашифрованный текст S, алфавит которого состоит только из квадратичных вычетов и нуля по модулю 31, т.е. содержит только 16 знаков.

5) Чтобы провести расшифрование, надо знать те места, на которых стоят квадраты квадратичных невычетов. Для этого составим двоичное число m, отвечающее шифртексту, следующим образом: те места, на которых стояли квадратичные невычеты, обозначим 1; а остальные — 0.

Тем самым, процедура шифрования завершена.

Процедура расшифрования происходит следующим образом.

а) Абоненту передается зашифрованный текст S и число m. Число m передается с помощью известного алгоритма А. Шамира (см., например, [31, 27, 47]).

б) Для восстановления первоначальной криптограммы, полученной в 1), необходимо на местах, отвечающих 1 в двоичной записи числа m (т.е. на местах, где стоят квадраты квадратичных невычетов), поставить первоначальные квадратичные невычеты, решая сравнение $x^2 \equiv t \pmod{31}$ относительно x, причем надо выбрать именно то решение данного сравнения, которое возводилось в квадрат.

в) При простом числе $p = 31$ имеем $p \equiv 3 \pmod 4$. Тогда вычет числа -1 является квадратичным невычетом по модулю 31. Пусть a — квадратичный невычет по модулю 31. Тогда сравнению $x^2 \equiv a^2 \pmod{31}$ отвечают два решения a и $-a \pmod{31}$, из которых a — квадратичный невычет (по выбору), и $-a = (-1)a$ является квадратичным вычетом, как произведение двух квадратичных невычетов.

г) Простой способ извлечения корня квадратного из числа b простому модулю $p \equiv 3 \pmod 4$ (см., например, [10]) т.е. способ нахождения решения сравнения $x^2 \equiv b \pmod p$, таков $x \equiv \pm b^{\frac{p+1}{2}} \pmod p$. Проверка числа на принадлежность к квадратичным вычетам или невычетам по модулю p осуществляется с помощью критерия Л. Эйлера: $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

Пусть, теперь, количество букв алфавита будет простым числом p, сравнимым с 1 по модулю 4. Разобьем все вычеты по модулю p на два класса: в первый класс войдут все квадратичные невычеты по модулю p, не превосходящие $(p-1)/2$ (их количество равно $(p-1)/4$); во второй класс — оставшиеся квадратичные невычеты, все квадратичные вычеты и 0.

Процедура шифрования по сравнению с предыдущей несколько изменяется.

1) Как и раньше, текст шифруется способом простой замены.

2) Затем буквы шифрованного текста располагаем в порядке убывания частот их появления. Первым $(p-1)/4$ буквам присваиваем значения последовательных квадратичных невычетов из первого класса, остальным буквам присваиваем значения из второго класса.

3) Буквам, которые соответствуют числа из первого класса, поставим в соответствие квадраты этих чисел по модулю p из отрезка $[0, p-1]$.

4) Составим двоичное число m, отвечающее шифртексту, следующим образом: места, на которых находятся числа из первого класса, обозначим 1, а остальные — 0.

Далее поступаем, как в предыдущем случае. Отметим, что извлечение квадратного корня по модулю p в данном случае будет несколько сложнее (см. [10]).

§ 4. Комбинированный метод искажения частот появления знаков в шифре простой замены

Опишем комбинированный метод искажения частот появления знаков в шифре простой замены, основанный на предыдущих методах возведения в квадрат и извлечения корня квадратного по некоторому модулю. Пусть, как и прежде, алфавит состоит из 31 знака.

1) Возьмем любую подстановку из 31 знака и зашифруем текст методом простой замены с помощью этой подстановки.

2) Расположим буквы шифрованного текста в порядке убывания частот. После этого каждой из первых пятнадцати букв присвоим последовательные значения квадратичных невычетов по модулю 31 в соответствии с их порядком нумерации, затем остальным буквам присваиваются последовательные значения квадратичных вычетов и 0.

3) Далее, тем буквам зашифрованного текста в соответствии с пунктом 2), которым соответствуют квадратичные невычеты поставим в соответствие квадраты этих чисел по модулю 31 из отрезка $[0, 30]$, а для букв, отвечающих квадратичным вычетам и нулю, поставим в соответствие значения квадратных корней из этих вычетов по модулю 31 и нуля, причем для квадратичного вычета a по модулю 31 решения $a_1, a_2, (a_1 < a_2)$ сравнения $x^2 \equiv a \pmod{31}$ заменяют последовательность чисел a в криптограмме на последовательность чисел $a_1, a_2, a_1, a_2, \ldots$.

4) Наконец, составим двоичное число m, отвечающее шифртексту, следующим образом: те места, на которых стояли квадратичные невычеты, обозначим 1; а остальные — 0.

Процедура шифрования завершена.

Опишем процедуру расшифрования.

а) Абоненту передается зашифрованный текст S и число m. Число m передается с помощью известного алгоритма А. Шамира.

б) Для восстановления первоначальной криптограммы, полученной в 1), необходимо на местах, отвечающих 1 в двоичной записи числа m (т.е. на местах, где стоят квадраты квадратичных невычетов), поставить первоначальные квадратичные невычеты, решая сравнение $x^2 \equiv t \pmod{31}$ относительно x, причем надо выбрать именно то значение x, которое возводилось в квадрат.

При простом числе $p = 31$ имеем $p \equiv 3 \pmod 4$. Тогда вычет числа -1 является квадратичным невычетом по модулю 31. Пусть a — квадратичный невычет по модулю 31. Тогда сравнению $x^2 \equiv a^2 \pmod{31}$ отвечают два решения a и $-a \pmod{31}$, из которых a — квадратичный невычет (по выбору), и $-a = (-1)a$ является квадратичным вычетом, как произведение двух квадратичных невычетов.

Способ извлечения корня квадратного из числа b по простому модулю $p \equiv 3 \pmod 4$ (см., например, [10]) т.е. способ нахождения решения сравнения $x^2 \equiv b \pmod p$, таков: $x \equiv \pm b^{\frac{p+1}{2}} \pmod p$. Проверка числа на принадлежность к квадратичным вычетам или невычетам по модулю p осуществляется с помощью критерия Л.Эйлера: $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

в) Продолжим восстановление первоначальной криптограммы. На местах, отвечающих 0 в двоичной записи числа m, поставим первоначальные значения квадратичных вычетов по модулю 31, возводя в квадрат вычеты, стоящие на этих местах.

Процедура расшифрования завершена.

§ 5. Анализ методов искажения знаков в шифре простой замены

Возможности, связанные с использованием шифра простой замены с дальнейшим сглаживанием частот появления знаков в зашифрованном тексте, требуют установления степени сглаживания. Здесь можно пойти по следующему пути.

В шифре простой замены соответствующие частоты появления знаков в зашифрованном тексте и в первоначальном открытом тексте совпадают. Поэтому возникает задача о “сглаживании” и “искажении” этих частот, в частности, о приближении ее к равномерному распределению частот появления знаков в шифрованном тексте или о замене априорной функции распределения появления частот алфавитных символов открытого текста другой функцией распределения их частот в зашифрованном тексте.

При анализе зашифрованного текста можно выделить характерные черты последовательности действий.

1. Установление количества различных алфавитных символов в зашифрованном тексте.

2. Подсчет частот появления алфавитных символов и определенных сочетаний этих символов в зашифрованном тексте.

3. Нахождение особенностей зашифрованного текста: распознавание алфавитных символов, отвечающих гласным и согласным буквам в открытом тексте; выявление наиболее распространенных сочетаний символов и т.п.

Пусть количество различных алфавитных символов $a_1, \ldots, a_n$ зашифрованного текста равно n, а сам зашифрованный текст состоит из N алфавитных символов. Символами $N_k, N_{l,m}$ обозначим количество появлений в зашифрованном тексте символа $a_k, k = 1, \ldots, n$ и соответственно наборов символов (a_l, a_m), $l, m = 1, \ldots, n$. Количество всех возможных различных наборов (a_l, a_m) обозначим через b. Тогда имеем $b \leqslant n^2$. Пусть $d_k = \frac{N_k}{N}$ — частота появления символа a_k, а величина $b_{l,m} = \frac{N_{l,m}}{N}$ — частота появления набора (a_k, a_l).

Как известно, в шифре простой замены ключ шифрования определяется подстановкой σ символов алфавита открытого текста.

Определим характеристики приближения к равномерному распределению при всех возможных шифрах простой замены данного открытого текста следующим образом

$$M = \min_{\sigma} \sum_{k=1}^{n} \left| d_k - \frac{1}{n} \right|, \quad B = \min_{\sigma} \sum_{l,m=1}^{n} \left| b_{l,m} - \frac{1}{b} \right|.$$

Равномерность распределения алфавитных символов зашифрованного сообщения можно охарактеризовать также в духе критерия Г. Вейля равномерного распределения последовательности по модулю единица. Пусть $1 \leqslant s_{k,1} < s_{k,2} < \ldots \leqslant N$ и $1 \leqslant t_{l,m,1} < t_{l,m,2} < \ldots$ — номера, которые занимает буква $a_k, k = 1, \ldots, n$, и соответственно набор (a_l, a_m) в зашифрованном тексте с помощью шифра простой замены, отвечающего подстановке σ. Рассмотрим при любом фиксированном целом $h \neq 0$ суммы

$$S_k(\sigma) = \frac{1}{N_k} \sum_{s_{k,l} \leqslant N} e^{2\pi i h \frac{s_{k,l}}{n}}, \quad T_{l,m}(\sigma) = \frac{1}{N_{l,m}} \sum_{\substack{r \\ t_{l,m,r} \leqslant N}} e^{2\pi i \frac{t_{l,m,r}}{n}}.$$

Тогда величина W, определяемая соотношением

$$W = \min_{\sigma} \sum_{k=1}^{n} |S_k(\sigma)|, \quad D = \min_{\sigma} \sum_{l,m=1}^{n} |T_{l,m}|.$$

будет характеризовать открытый текст и равномерность появления знаков в шифре простой замены.

§ 6. Применение китайской теоремы об остатках к шифру Виженера

Продолжим построение шифров на основе теоретико-числовых алгоритмов [27]–[29].

Рассмотрим известный многоалфавитный шифр Виженера. Он является обобщением одноалфавитного шифра простой замены и шифром гаммирования с периодической гаммой (см., например, [4], с. 151–152; [5], с.11).

Пусть количество символов алфавита равно составному числу n. Каждому символу $\alpha_r, r = 1, \ldots, n$, алфавита присваивается некоторый вычет a_r по модулю n, причем различным символам отвечают различные вычеты. Пусть, также, число n представимо в виде $n = dq$, $(d, q) = 1$, $d > 1$, $q > 1$. Например, $n = 35 = dq = 5 \cdot 7$ или $n = 36 = 4 \cdot 9$.

Тогда можно предложить следующий способ шифрования.

1. *Предварительные преобразования.* Представим каждое число $1 \leqslant a \leqslant n$ в виде

$$a \equiv qb + dc \pmod{n}, \tag{1}$$

где $1 \leqslant b \leqslant d, 1 \leqslant c \leqslant q$. Тогда по китайской теореме об остатках вычет a по модулю n однозначно определяет вычеты b по модулю d и c по модулю q и наоборот.

Составим две таблицы Виженера, отвечающие вычетам b и c. Пусть $b_1, \ldots, b_d$ — полная система вычетов по модулю d, например, $1, 2, \ldots, d$, и $c_1, \ldots, c_q$ — полная система вычетов по модулю q. Тогда таблицы Виженера будут иметь вид

$$\begin{array}{ll} \underline{b_1, b_2, \ldots, b_{d-1}, b_d,} & \underline{c_1, c_2, \ldots, c_{q-1}, c_q,} \\ b_2, b_3, \ldots, b_d, \quad b_1, & c_2, c_3, \ldots, c_q, \quad c_1, \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\ b_d, b_1, \ldots, b_{d-2}, b_{d-1}, & c_q, c_1, \ldots, c_{q-2}, c_{q-1}. \end{array}$$

Для каждой из приведенных выше таблиц Виженера при некоторых натуральных числах s, t с условиями $1 \leqslant s \leqslant d$, $1 \leqslant t \leqslant q$, возьмем свой ключ $k = (b_{k_1}, b_{k_2}, \ldots, b_{k_s})$ для первой таблицы и соответственно $p = (c_{p_1}, c_{p_2}, \ldots, c_{p_t})$ для второй таблицы. Над каждым вычетом первой строки первой таблицы выписываем в строку символы ключа k следующим образом

$$b_{k_1}, b_{k_2}, \ldots b_{k_s}, b_{k_1}, b_{k_2}, \ldots.$$

Аналогично выписываем ключ p над второй таблицей.

2. *Процедура шифрования открытого текста.*

Пусть задан открытый текст $a_{h_1}a_{h_2}\dots a_{h_u}$. По формуле (1) преобразуем его в два текста. Имеем

$$b_{h_1}b_{h_2}\dots b_{h_u};\quad c_{h_1}c_{h_2}\dots c_{h_u}.$$

На пересечении h_1-го столбца и k_1-й строки в первой таблице находим символ x_1, а на пересечении h_1-го столбца и p_1-й строки второй таблицы находим символ y_1. Повторим эту процедуру для следующего символа a_{h_2} и т.д. Получим шифрованный текст

$$x_1y_1x_2y_2\dots x_uy_u$$

или два шифрованных текста $x_1x_2\dots x_u$ и $y_1y_2\dots y_u$, или $z_1z_2\dots z_u$, где $z_t = qx_t + dy_t, 1 \leqslant t \leqslant u$.

3. *Процедура расшифрования.*

По ключам k и p в первой и второй таблицах Вижинера находим строки с номерами k_1 и p_1 соответственно. На этих строках находим элементы x_1 в первой таблице и y_1 во второй таблице, а затем по этим элементам находим, отвечающие им столбцы, и получаем элементы b_{h_1} и c_{h_1}. По тому же правилу восстанавливаются элементы b_{h_2} и c_{h_2} и т.д.

Далее, используя формулу (1), по паре символов (b_{q_t}, c_{q_t}) находим символ a_{q_t}, $t = 1,\dots,u$. Процедура расшифрования завершена.

Наконец, дадим обобщение предыдущей процедуры шифрования. Пусть алфавит состоит из m символов, причем имеет место представление $m = m_1\dots m_r$ с попарно простыми множителями $m_1, m_2, \dots, m_r$, превосходящими единицу. Определим числа M_s и M'_s следующими условиями

$$m_1m_2\dots m_r = M_sm_s,\quad M_sM'_s \equiv 1 \pmod{m_s}, s = 1,2,\dots,r.$$

Положим

$$a = M_1M'_1b_1 + M_2M'_2b_2 + \dots + M_rM'_rb_r. \tag{2}$$

И пусть $b_1, b_2, \dots, b_r$ независимо друг от друга пробегают полные системы по модулям $m_1, m_2, \dots, m_r$ соответственно. Тогда a пробегает полную систему вычетов по модулю $m_1m_2\dots m_r$ (см., например, [10], гл. IV,§3).

Пусть, например, $m = 30$, $m = m_1m_2m_3 = 2\cdot3\cdot5 = 2\cdot15 = 3\cdot10 = 5\cdot6$. Тогда $M_1M'_1 \equiv 15\cdot1 \equiv 1 \pmod 2$, $M_2M'_2 \equiv 10\cdot1 \equiv 1 \pmod 3$, $M_3M'_3 \equiv 6\cdot1 \equiv 1 \pmod 5$.

Поэтому имеем $a \equiv 15b_1 + 10b_2 + 6b_3 \pmod{30}$.

Пусть, теперь, $b_{1,s}, b_{2,s}, \ldots, b_{m_s,s}$ — полная система вычетов по модулю m_s, например, $1, 2, \ldots, m_s, 1 \leqslant s \leqslant r$. Составим r таблиц Виженера для каждого из алфавитов $b_{1,s}, b_{2,s}, \ldots, b_{m_s,s}$, $1 \leqslant s \leqslant r$.

Для каждой из приведенных выше таблиц Виженера при некотором натуральном числе t_s с условиями $1 \leqslant t_s \leqslant m_s$, задаем ключ $k_s = (b_{k_1,s}, b_{k_2,s}, \ldots, b_{k_{t_s},s})$, $1 \leqslant s \leqslant r$.

Пусть, далее, задан открытый текст $a_{h_1} a_{h_2} \ldots a_{h_u}$. По формуле (2) преобразуем его в r текстов. Имеем

$$b_{h_1,s} b_{h_2,s} \ldots b_{h_u,s}, \quad s = 1, 2, \ldots, r.$$

Аналогично вышеприведенному с помощью таблицы Виженера с номером s и ключа k_s шифруем текст $b_{h_1,s} b_{h_2,s} \ldots b_{h_u,s}$, $s = 1, 2, \ldots, r$. Расшифрование проводится также аналогично вышеизложенному.

§ 7. Арифметический вариант шифра Виженера

Рассмотрим один из возможных путей обобщения шифра Виженера (см. [31, 4]), использующий возможность аддитивного представления целых чисел. Пусть m — количество всех символов алфавита и для натуральных чисел m, m_1, m_2 справедливы равенства $m = m_1 m_2$, $(m_1, m_2) = 1$, $m_1 > 1$, $m_2 > 1$. Например, $m = 30$, $m_1 = 5$, $m_2 = 6$.

Далее, пусть α_1 пробегает полную систему вычетов по модулю m_2, а α_2 — полную систему вычетов по модулю m_1. Тогда сумма $m_1\alpha_1 + m_2\alpha_2$ пробегает полную систему вычетов по модулю m (см. [10]). Другими словами, любое целое число a с условием $1 \leqslant a \leqslant m$ при некоторых фиксированных b_1 по модулю m_2 и b_2 по модулю m_1 единственным образом представляется в виде

$$a \equiv b_1 m_1 a_1 + b_2 m_2 a_2 \pmod{m}, \tag{1}$$

где $1 \leqslant a_1 \leqslant m_2$, $1 \leqslant a_2 \leqslant m_1$, находятся из сравнений $b_1 m_1 a_1 \equiv a \pmod{m_2}$ и $b_2 m_2 a_2 \equiv a \pmod{m_1}$.

Таким образом, каждому целому числу a, $1 \leqslant a \leqslant m$, отвечает единственная пара целых чисел (a_1, a_2), удовлетворяющая сравнению (1). Расположение пар (a_1, a_2) в указанном выше соответствии может служить частью секретного ключа. По формуле (1) этот ключ однозначно задается парой (b_1, b_2), где $1 \leqslant b_1 \leqslant m_2$, $1 \leqslant b_2 \leqslant m_1$. Следовательно, число возможных ключей равно $m = m_1 m_2$.

Более того, каждому символу a алфавита можно поставить некоторым образом в соответствие любую пару $(\beta_1, \beta_2$ с условием $1 \leqslant \beta_1 \leqslant m_2$, $1 \leqslant \beta_2 \leqslant m_1$. Тогда число всевозможных ключей будет равно $m_1! m_2!$.

Далее, составим таблицу Виженера по следующему правилу: в строку с номером k поместим элементы $((\beta_1+ck) \pmod{m_2}, (\beta_2+ck) \pmod{m_1})$, где различные пары $(\beta_1 \pmod{m_2}, \beta_2 \pmod{m_1})$ образуют первую строку, величина k изменяется от 0 до $m-1$ и c — любое целое число, взаимно простое с m. Для того, чтобы полученная таблица была таблицей Виженера необходимо и достаточно, чтобы строки с разными номерами были различными. Предположим, что в построенной таблице строки с номерами k и k' совпадают. Тогда, очевидно, имеем $c(k-k') \equiv 0 \pmod{m_2}$, $c(k-k') \equiv 0 \pmod{m_1}$. Отсюда получим, что $m \mid (k-k')$. Это означает, что $k = k'$. Тем самым доказано, что построенная таблица является таблицей Виженера. Отметим, что число c также может служить частью секретного ключа.

Шифрование и дешифрование по построенной таблице осуществляется стандартным образом.

Обратим внимание еще на один момент составления таблицы Виженера. Пусть количество символов алфавита равно m, число m представляется в виде $m = m_1 \dots m_r$, $r \geqslant 2$, и m_k, m_l попарно взаимно просты при $k, l = 1, \dots, r$. Далее, каждому символу a, являющемуся вычетом по модулю m, взаимно однозначным образом поставим в соответствие набор $(a_1, \dots, a_r)$, где a_k, $k = 1, \dots, r$, принимает значения из полной системы вычетов по модулю m_k. Например, это соответствие можно установить следующим образом. Положим $M_k = mm_k^{-1}$. Тогда любой вычет a по модулю m однозначным образом представляется в виде $a \equiv M_1a_1 + \dots + M_ra_r \pmod{m}$, где a_k, $k = 1, \dots, r$, принимает значения из полной системы вычетов по модулю m_k. Различным наборам $(a_1, \dots, a_r)$, где $0 \leqslant a_k < m_k$, $k = 1, \dots, r$, отвечают различные вычеты a по модулю m. Таким образом, при указанных соответствиях существует $m_1! \dots m_r!$ секретных ключей.

По аналогии с предыдущим, составим таблицу Виженера по следующему правилу: в строку с номером k поместим элементы $((a_1 + ck) \pmod{m_1}, \dots, (a_r + ck) \pmod{m_r})$, где различные пары $(a_1 \pmod{m_1}, \dots, a_r \pmod{m_r})$ образуют первую строку, величина k изменяется от 0 до $m-1$ и c — любое целое число, взаимно простое с m. Строки с разными номерами в этой таблице будут различными, так что получена таблица Виженера.

Глава VI

АСИММЕТРИЧНЫЕ ШИФРЫ

§ 1. Введение

При симметричном шифровании каждый из абонентов должен иметь копию общего секретного ключа. При открытом шифровании используются два ключа, один из которых открытый, а второй — секретный. Открытый ключ каждого абонента может быть опубликован и по этому ключу любой желающий может послать данному абоненту секретное сообщение, но прочитать его может только тот абонент, которому оно адресовано по секретному ключу, известному только ему.

Идея шифрования с открытым ключом тесно связана с понятием однонаправленной (односторонней) функцией. На качественном уровне оно определяется так. *Взаимно однозначное отображение $f : X \to Y$ двух текстов X и Y называется* **строго однонаправленной,** *если выполняется следующее условие: существует "эффективный" метод вычисления $f(x)$ для всех $x \in X$, но не существует "эффективного" метода для вычисления x из соотношения $y = f(x)$ для всех $y \in f(X)$, где $f(X)$ — образ множества X при отображении f.*

В качестве начальной иллюстрации приведем замечательный пример из книги Саломаа [40] однонаправленной функции. Построение ее основано на телефонном справочнике. Шифрование происходит побуквенно. Возьмем, например, "Большую телефонную книгу Юго-западного административного округа города Москвы за 2008–2009 гг." Для необходимой буквы $x \in X$ в справочнике ищем слово, начинающееся на x, и шифруем соответствующим телефонным номером. Например, зашифруем слово "мехмат". Находим

м →	майский →	1349396
е →	евросеть, торговый дом →	9353857
х →	химической физики институт →	9397249
м →	московский университет →	1340483
а →	алтайский →	4204600
т →	тамань →	4258233

Таким образом, слово "мехмат" шифруется следующей последова-

тельностью кодовых обозначений: “1349396 9353857 9397249 1340433 4204600 4258233”. Однонаправленная функция, использованная для шифрования, ставит для законного расшифровальщика непреодолимые трудности. Он и наблюдатель испытывают одинаковые трудности. Если же легальный абонент имеет обратный телефонный справочник, то процедура расшифрования упрощается.

Уточним понятие односторонней функции. *Взаимно однозначное соответствие* $f\colon X \to Y$ *называется* **однонаправленной функцией с секретом** *(с лазейкой), если*

а) существует “эффективный” метод вычисления $f(x)$ *для всех* $x \in X$;

б) существует “эффективный” метод вычисления $f^{-1}(y)$ *для всех* $y \in f(X)$, *но он не может быть получен “эффективно” из соотношения* $y = f(x)$ *для всех* $y \in f(X)$*: необходима дополнительная секретная информация “секрет” (“лазейка”).*

В качестве одного из первых примеров применения односторонних функций рассмотрим задачу о сохранении паролей.

Пусть доступ к компьютеру при его включении контролируется паролями. Как организовать доступ к нему только законных пользователей? Например, при включении компьютера можно воспользоваться списком законных пользователей, но опасность заключается в том, что трудно сохранить его в секрете. Для этой цели была предложена следующая процедура, которая явилась одним из первых примеров применения односторонних функций в криптографии.

Пусть $f(x)$ — односторонняя функция, определенная на множестве X возможных паролей. Для каждого пароля π законного пользователя компьютера сохраним в памяти компьютера допустимое значение $f(\pi)$. Пользователь компьютера, имеющий доступ к нему, вводит в него слово x. Компьютер проверяет законность доступа, вычисляя $f(x)$ и сверяя полученный результат со списком допустимых значений $f(\pi)$, имеющийся в его памяти. Совпадение значения $f(x)$ с одним из значений $f(\pi)$ открывает возможность доступа.

Таким образом, чтобы обеспечить доступ к компьютеру надо найти такое x, что значение $f(x)$ будет совпадать хотя бы с одним значением $f(\pi)$ из списка допустимых значений $f(\pi)$. Заметим, что при ограниченной мощности вычислительных средств эта задача не выполнима в реальное время, даже если известны все допустимые значения $f(\pi)$ и сама функция f.

В 1981 г. Лампорт (см., например, [18]) предложил усилить защиту доступа к компьютеру. Пусть некоторый пароль каким-то образом стал известен незаконному пользователю. Для усиления гаран-

тии законного доступа к компьютеру можно выполнить следующую процедуру.

1. Каждому законному пользователю дается свой начальный пароль π_0.

2. Затем для некоторого натурального числа m вычисляются m последовательных итераций функции f: $\pi_1 = f(\pi_0)$, $\pi_2 = f(\pi_1)$, …, $\pi_m = f(\pi_{m-1})$, и пользователь сохраняет значения π_0, π_1, …, π_{m-1}.

3. Наконец, в память компьютера вводится $\pi_m = f(\pi_{m-1})$.

Проверка законности доступа к компьютеру производится всегда по одному и тому же алгоритму: по представленному паролю вычисляются его m итераций функции f и сравниваются со списком, имеющимся в памяти компьютера.

4. Для получения доступа к компьютеру пользователь вводит в него π_{m-1} и вычисляет значение $\pi_m = f(\pi_{m-1})$.

5. Проведя проверку значения $f(\pi_{m-1}) = \pi_m$, пользователь стирает из памяти компьютера π_m и заменяет его на π_{m-1}.

6. В следующем сеансе связи роль π_{m-1} будет выполнять π_{m-2} и т.д.

Рассмотренная процедура позволяет провести m сеансов связи. Проведение одной процедуры несколько раз в криптографии представляет некоторое несовершенство. Тем не менее, приведенный алгоритм дает первое представление о криптографических возможностях однонаправленных функций.

Обратимся теперь к построению некоторых односторонних функций.

Сначала рассмотрим функцию, построенную с помощью возведения в степень по модулю простого числа. Ее часто называют дискретным возведением в степень или возведением в степень по модулю. Строится она следующим образом.

Задают большое простое число p и первообразный корень g по модулю p. Далее, в приведенной системе вычетов по модулю p определяют взаимно однозначное отображение $x \to f(x) \equiv g^x \pmod{p}$.

Заметим, что возведение в степень числа g выполняется достаточно просто. Оно сводится, в частности, к последовательным возведениям числа g в квадрат. Например, вычислим g^{11}. Имеем $11 = 2^3 + 2^1 + 2^0$. Отсюда находим

$$g^{11} = \left((g^2)^2\right)^2 \cdot g^2 \cdot g.$$

С другой стороны, все известные алгоритмы вычисления обратной функции f^{-1}, т.е. вычисления дискретного логарифма или индекса вычета по модулю p, требуют для вычисления ее значения времени,

которое растет относительно $\log_2 p$ не полиномиальным образом (величина $[\log_2 p]$ равна количеству цифр в записи натурального числа p в двоичной системе счисления). Отметим,что, если число p содержит несколько сотен цифр, то в современных ЭВМ использование этих алгоритмов не является целесообразным.

Рассмотрим, теперь, пример криптосистемы с открытым ключом, основанной на вычислении дискретного логарифма в конечном поле. Задача будет состоять в том, чтобы согласовать секретные ключи классической криптосистемы.

Пусть, например, абонент $\mathcal{A}$ желает передать абоненту $\mathcal{B}$ сообщение $a_1, \ldots, a_n$ на языке конечного поля $\mathbf{Z}_p$. С этой целью они вырабатывают секретный ключ Δ: $\delta_1, \ldots, \delta_n$. Далее, абонент $\mathcal{A}$ передает по открытому каналу связи абоненту $\mathcal{B}$ шифртекст $a_1 + \delta_1, \ldots, a_n + \delta_n$. Зная ключ Δ, абонент $\mathcal{B}$ прочитывает текст сообщения. Недостатком этого метода шифрования является необходимость передачи ключа Δ абонентом $\mathcal{A}$ абоненту $\mathcal{B}$, поскольку "длина ключа" совпадает с длиной передаваемого текста. Возникает задача уменьшения длины ключа, передаваемого по каналу связи.

На практике, как правило, последовательность Δ вырабатывается детерминированным образом, но так, чтобы на конечном участке она "выглядела" бы как случайная. В первую очередь стремятся к тому, чтобы последовательность Δ по модулю p имела максимальный период. В частности, ее можно задать рекуррентным образом: $\delta_{m+1} \equiv a\delta_m + c \pmod p$, $m \geqslant 0$. Тогда для того, чтобы согласовать ключ Δ, достаточно произвести согласование только первого члена последовательности δ_0. Один из методов такого согласования предложен Диффи и Хеллманом. Он основан на использовании дискретного логарифма.

§ 2. Задача об укладке рюкзака

Сначала сформулируем задачу о рюкзаке или задачу об укладке ранца.

Пусть каждый из имеющихся n предметов обладает массой m_i, объемом v_i, ценой c_i и численной оценкой полезности p_i, где $i = 1, 2, \ldots, n$. Требуется составить набор предметов с номерами $i_1, i_2, \ldots, i_k$ (число k не фиксировано) так, чтобы их суммарная масса не превосходила M, т.е. $m_{i_1} + m_{i_2} + \ldots m_{i_k} \leqslant M$, суммарный объем не превосходил величины v, т.е. $v_{i_1} + v_{i_2} + \ldots + v_{i_k} \leqslant v$, при этом суммарная цена $c_{i_1} + c_{i_2} + \ldots + c_{i_k}$ была бы наименьшей и суммарная полезность $p_{i_1} + p_{i_2} + \ldots + p_{i_k}$ была бы наибольшей.

В 1978 г. Р. Меркль предложил для построения криптосистем с

открытым ключом использовать следующую частную аддитивную задачу об укладке рюкзака.

Пусть задано множество натуральных чисел $a_1, a_2, \ldots, a_n$ и натуральное число S. Требуется найти набор $x = (x_1, x_2, \ldots, x_n)$, элементами x_s, $1 \leqslant s \leqslant n$, которого являются числа 0 и 1, такой, что

$$x_1 a_1 + x_2 a_2 + \ldots + x_k a_k = S.$$

При этом интересной будет как задача нахождения решения, так и задача его существования.

Имеется также мультипликативный аналог задачи об укладке рюкзака. Пусть, как и прежде, задано множество натуральных чисел $a_1, a_2, \ldots, a_n$ и натуральное число P Требуется найти набор $x = (x_1, x_2, \ldots, x_n)$, элементами x_s, $1 \leqslant s \leqslant n$, которого являются числа 0 и 1, такой, что

$$a_1^{x_1} \cdot a_2^{x_2} \cdot \ldots \cdot a_k^{x_k} = P.$$

Для некоторых наборов $a_1, a_2, \ldots, a_n$ нетрудно найти решение частной аддитивной задачи об укладке рюкзака. Пусть, например, задана последовательность $a_1 = 1$, $a_2 = 2$, …, $a_s = 2^{s-1}$, …, $a_n = 2^{n-1}$. При $1 \leqslant S \leqslant 2^n - 1$ найдется единственное решение уравнения

$$x_1 \cdot 2^0 + x_2 \cdot 2^1 + \ldots + x_n \cdot 2^{n-1} = S.$$

Решение $(x_1, \ldots, x_n)$ строим следующим образом. Сначала находим натуральное число k_1 из условия $2^{k_1-1} \leqslant S < 2^{k_1}$. Полагаем $x_{k_1} = 1$, $x_{k_1+1} = \ldots x_n = 0$, и $S_1 = S - 2^{k_1-1}$. Если $2^{k_1-1} = S$, то решение найдено и оно имеет вид $(x_1, \ldots, x_{k_1}, \ldots, x_n) = (0, \ldots, 1, \ldots, 0)$.

Пусть, теперь, $2^{k_1-1} < S$. Тогда находим натуральное число k_2 из условия $2^{k_2-1} \leqslant S < 2^{k_2}$. Полагаем $x_{k_2} = 1$, $x_{k_2+1} = \ldots x_{k_1-1} = 0$, и $S_2 = S_1 - 2^{k_2-1}$. Если $2^{k_2-1} = S_1$, то решение найдено и оно имеет вид $(x_1, \ldots, x_{k_2}, x_{k_2+1}, \ldots, x_{k_1-1}, x_{k_1}, \ldots, x_n) = (0, \ldots, 1, 0 \ldots, 0, 1, \ldots, 0)$ и т.д.

Таким образом найдено решение частного случая аддитивной задачи об укладке рюкзака.

Рассмотрим теперь более общие наборы чисел $a_1, a_2, \ldots, a_n$. Назовем набор натуральных чисел $a_1, a_2, \ldots, a_n$ сверх растущим, если для любого k, $1 < k \leqslant n$, справедливо неравенство $\sum\limits_{s=1}^{k-1} a_s < a_k$.

Например, сверх растущим является набор $(2, 3, 7, 15, 31)$, так как имеют место неравенства

$$2 < 3,\ 2 + 3 < 7,\ 2 + 3 + 7 < 15,\ 2 + 3 + 7 + 15 < 31.$$

Далее решим аддитивную задачу об укладке рюкзака для сверх растущего набора чисел.

Сначала находим натуральное число k_1 из условия $a_{k_1-1} \leqslant S < a_{k_1}$. Полагаем $x_{k_1} = 1$, $x_{k_1+1} = \ldots x_n = 0$, и $S_1 = S - a_{k_1-1}$. Если $a_{k_1-1} = S$, то решение найдено и оно имеет вид $(x_1, \ldots, x_{k_1}, \ldots, x_n) = (0, \ldots, 1, \ldots, 0)$.

Пусть, теперь, $a_{k_1-1} < S$. Тогда находим натуральное число k_2 из условия $a_{k_2-1} \leqslant S < a_{k_2}$. Полагаем $x_{k_2} = 1$, $x_{k_2+1} = \ldots x_{k_1-1} = 0$, и $S_2 = S_1 - a_{k_2-1}$. Если $a_{k_2-1} = S_1$, то решение найдено и оно имеет вид $(x_1, \ldots, x_{k_2}, x_{k_2+1}, \ldots, x_{k_1-1}, x_{k_1}, \ldots, x_n) = (0, \ldots, 1, 0 \ldots, 0, 1, \ldots, 0)$ и т.д.

Таким образом решение найдено.

В качестве примера решим аддитивную задачу об укладке рюкзака для сверх растущего набора $(2, 3, 7, 15, 31)$ и $S = 24$. Поскольку $a_4 = 15 \leqslant 24 < 31 = a_5$, положим $x_5 = 0$, $x_4 = 1$. Далее находим $S_1 = S - a_4 = 25 - 15 = 9$. Отсюда получим $x_3 = 1$, $S_2 = S_1 - a_3 = 9 - 7 = 2 = a_1$. Следовательно, $x_2 = 0, x_1 = 1$. Таким образом, имеем решение $(x_1, \ldots, x_5) = (1, 0, 1, 1, 0)$, т.е. $S = 24 = 2 + 7 + 15$.

§ 3. Система шифрования, основанная на задаче о рюкзаке

Предположим, что элементы открытого текста обозначаются k-разрядными двоичными числами, где k — некоторое натуральное число. Например, для русского алфавита, состоящего из 31 буквы, каждую из них можно обозначить пятиразрядным двоичным числом от $0 = (00000)_2$ до $30 = (11110)_2$, т.е. а = 00000, б = 00001, …, е = 00101, …, н = 01101, …, т = 10010, ….

Далее, каждый пользователь выбирает следующие параметры:

1) сверх растущий набор $a = (a_1, \ldots, a_k)$,

2) натуральное число m такое, что $m > a_1 + a_2 + \ldots + a_k$,

3) натуральное число α такое, что $1 \leqslant \alpha < m$ и $(\alpha, m) = 1$.

По выбранным параметрам вычисляются:

1) натуральное число β такое, что $\alpha\beta \equiv 1 \pmod m$, где $1 \leqslant \beta < m$,

2) k-элементный набор $w = (w_1, w_2, \ldots, w_k)$, где $w_s = \alpha a_s$, $s = 1, \ldots, k$.

Заметим, что набор w не обязан быть сверх растущим.

Например, если возьмем сверхрастущий набор $a = (a_1, \ldots, a_5) = (2, 3, 7, 15, 31), m = 61 > 2 + 3 + 7 + 15 + 31 = 58, \alpha = 17$, $(17, 61) = 1$, то получим $\beta = 18$ и $w = (w_1, \ldots, w_5) \equiv \alpha a = (34, 51, 58, 11, 39) \pmod{61}$.

Пусть, теперь, требуется передать по открытому каналу связи сообщение $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$, где ε_s принимают значения либо 0,

либо 1. Набор чисел w является открытым ключом шифрования K_E. Секретным ключом (ключом дешифрования) будет пара чисел $K_D = (m, \beta)$. Затем вычисляется число $C \equiv \varepsilon_1 w_1 + \varepsilon_2 w_2 + \ldots + \varepsilon_k w_k \pmod m$ и число C передается по каналу связи. Абонент, получив число C, приступает к дешифровке. Он находит наименьший положительный вычет v числа βC по модулю m, т.е. $v \equiv \beta C \pmod m$.

Отсюда имеем

$$v \equiv \beta C \equiv \sum_{s=1}^{k} \varepsilon_s \beta w_s \equiv \sum_{s=1}^{k} \varepsilon_s \beta \alpha a_s \equiv \sum_{s=1}^{k} \varepsilon_s a_s \pmod m.$$

Поскольку

$$\sum_{s=1}^{k} \varepsilon_s a_s \leqslant \sum_{s=1}^{k} a_s < m,$$

предыдущее сравнение превращается в равенство. Следовательно, $v = \sum\limits_{s=1}^{k} \varepsilon_s a_s$.

Далее пользуемся решением аддитивной задачи об укладке рюкзака и находим единственное решение $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$.

Рассмотрим пример. Пусть требуется передать слово “НЕТ”. В открытом тексте каждая буква русского алфавита записывается пятизначным двоичным числом. Имеем, что “Н” есть $\varepsilon^{(1)} = (\varepsilon_5^{(1)}, \varepsilon_4^{(1)}, \ldots, \varepsilon_1^{(1)}) = (01101)$, “Е” — $\varepsilon^{(2)} = (\varepsilon_5^{(2)}, \varepsilon_4^{(2)}, \ldots, \varepsilon_1^{(2)}) = (00101)$, “Т” — $\varepsilon^{(3)} = (\varepsilon_5^{(3)}, \varepsilon_4^{(3)}, \ldots, \varepsilon_1^{(3)}) = (10010)$.

Как и в предыдущем примере, возьмем сверх растущий набор $a = (a_1, a_2 \ldots, a_5) = (2, 3, 7, 15, 31), m = 61, \alpha = 17$. Получим открытый ключ K_E шифрования $w = (w_1, w_2, \ldots, w_5) = (34, 51, 58, 11, 39)$ и секретный ключ $K_D = (m, \beta) = (61, 18)$ дешифрования.

С помощью открытого ключа K_E шифруем каждую букву. Находим

$$E_K(\text{Н}) = \varepsilon_5^{(1)} w_1 + \varepsilon_4^{(1)} w_2 + \ldots + \varepsilon_1^{(1)} w_5 = 1{\cdot}34 + 0{\cdot}51 + 1{\cdot}58 + 1{\cdot}11 + 0{\cdot}39 = 103,$$

$$E_K(\text{Е}) = \varepsilon_5^{(2)} w_1 + \varepsilon_4^{(2)} w_2 + \ldots + \varepsilon_1^{(2)} w_5 = 1{\cdot}34 + 0{\cdot}51 + 1{\cdot}58 + 0{\cdot}11 + 0{\cdot}39 = 92,$$

$$E_K(\text{Т}) = \varepsilon_5^{(3)} w_1 + \varepsilon_4^{(3)} w_2 + \ldots + \varepsilon_1^{(3)} w_5 = 0{\cdot}34 + 1{\cdot}51 + 0{\cdot}58 + 0{\cdot}11 + 1{\cdot}39 = 90.$$

Далее по открытому каналу связи абоненту передается набор из трех чисел $103, 92, 90$. Для того, чтобы расшифровать сообщение, он умножает эти числа на $\beta = 18$ и приводит результат к наименьшим невычетам по модулю 61. Получает набор из трех чисел $24, 9, 34$. Для этих трех чисел, наконец, решается аддитивная задача об укладке

рюкзака. Имеем единственное решение

$$S = 24 = 2 + 7 + 15,\ \varepsilon^{(1)} = (0,1,1,0,1),\ 9 = 2 + 7,\ \varepsilon^{(2)} = (0,0,1,0,1),$$
$$34 = 31 + 3,\ \varepsilon^{(3)} = (1,0,0,1,0).$$

Тем самым, прочитано слово "НЕТ".

Заметим, что при увеличении длины сверх растущего набора a можно шифровать уже не отдельные буквы алфавита на основе аддитивной задачи об укладке рюкзака, а k-граммы.

Рассмотрим на примере способ шифрования биграмм. Пусть задан сверх растущий набор из десяти чисел

$$a = (a_1, a_2, \ldots, a_{10}) = (2, 3, 7, 31, 60, 119, 239, 477, 954),$$

причем $\sum\limits_{s=1}^{10} a_s = 1907$.

В качестве модуля m возьмем число 1909. Положим $\alpha = 3$. Отсюда получим $\beta = 1273$, поскольку $\alpha\beta \equiv 1 \pmod m$ и $3 \cdot 1273 \equiv 1 \pmod{1909}$.

Находим открытый ключ K_E шифрования

$$w = \alpha a = (w_1, w_2, \ldots, w_{10}) = (6, 9, 21, 45, 93, 180, 357, 717, 1431, 953).$$

Секретный ключ K_D дешифрования имеет вид $K_D = (m, \beta) = (1909, 1273)$.

Пусть, как и раньше, по открытому каналу связи требуется передать слово "НЕТ". Разобьем слово НЕТ на биграммы (в качестве пустышки возьмем букву а). Получим НЕ-ТА. В открытом тексте буквы обозначаются пятизначными двоичными числами. Имеем Н есть 01101, Е — 00101, Т — 10010, А — 00000. Отсюда находим НЕ — 0110100101, ТА — 1001000000.

Далее шифруем биграммы НЕ и ТА. Соответственно имеем

$$1 \cdot 6 + 0 \cdot 9 + 1 \cdot 21 + 0 \cdot 45 + 0 \cdot 93 + 1 \cdot 180 +$$
$$+0 \cdot 357 + 1 \cdot 717 + 1 \cdot 1431 + 0 \cdot 953 \equiv 446 \pmod{1909},$$
$$0 \cdot 6 + 0 \cdot 9 + 0 \cdot 21 + 0 \cdot 45 + 0 \cdot 93 + 1 \cdot 180 +$$
$$+0 \cdot 357 + 0 \cdot 717 + 0 \cdot 1431 + 1 \cdot 953 \equiv 1310 \pmod{1909}.$$

Абоненту передается два числа: 446, 1310. Он начинает дешифровку домножением этих чисел на $\beta = 1273$ и нахождением наименьших положительных вычетов по модулю 1909. Получает набор двух чисел: 785, 1073. Наконец, решая аддитивную задачу об укладке рюкзака, находит ответ.

§ 4. Система Ривеста – Шамира – Адельмана шифрования с открытым ключом

Перейдем к построению системы RSA шифрования с открытым ключом. Отметим основные элементы, необходимые для этой системы.

1) Надо уметь находить большие простые числа, по крайней мере, два простых числа p и q.

2) Кодирование сообщений в системе RSA основывается на числе $n = pq$.

3) В основе декодирования системы RSA лежит знание чисел p и q.

4) Безопасность системы RSA обеспечивается алгоритмической сложностью разложения на простые сомножители числа n.

Сначала опишем схему процесса шифрования и дешифрования. Пусть требуется передать по открытому каналу связи сообщение “МУДРОМУ ДОСТАТОЧНО”. Подготовим его к передаче с помощью системы RSA. Сначала возьмем $p = 73,\ q = 97, n = pq = 7081$. Представим текст сообщения в виде последовательности классов вычетов по модулю $n = 7081$. Каждую букву русского алфавита и пробел заменим двузначным числом. Имеем следующую таблицу.

А	10	К	20	Ф	30
Б	11	Л	21	Х	31
В	12	М	22	Ц	32
Г	13	Н	23	Ч	33
Д	14	О	24	Ш	34
Е	15	П	25	Щ	35
Ж	16	Р	26	Ъ,Ь	36
З	17	С	27	Ы	37
И	18	Т	28	Э	38
Й	19	У	29	Ю	39
		пробел	55	Я	40

Тогда открытый текст запишется в виде

$$22291426242229551424272810282433 2324.$$

Последнее числовое сообщение разобьем на блоки чисел, каждое из которых не превосходит $n = 7081$. Находим

$$2229 - 1426 - 2422 - 2955 - 1424 - 2728 - 1028 - 2433 - 2324.$$

Каждый блок шифруется отдельно по системе RSA. Разумеется, разбиение сообщения на блоки не однозначно, и количество цифр в каж-

дом блоке может быть различным. Но имеется запрет, состоящий в том, что блок не может начинаться с нуля в связи с требованием однозначной расшифровки текста.

При расшифровке шифртекста находится система блоков чисел. Эти блоки соединяют вместе и получают числовое сообщение. Наконец, заменяют последовательные пары чисел буквами.

Шифрование сообщения. Сначала выберем различные простые числа p и q. Найдем число $n = pq$ и значение функции Эйлера $\varphi(n) = (p-1)(q-1)$. Далее, выбираем число e такое, что $(e, \varphi(n)) = 1,\ 1 \leqslant e < \varphi(n)$. Пару чисел (n, e) называют шифрующим ключом и она объявляется открытым ключом. Пусть a обозначает любой блок сообщения, причем $1 \leqslant a < n$. Тогда зашифрование происходит по следующему правилу: $E(a) \equiv a^e \pmod{n}$, т.е. блок b зашифрованного сообщения имеет вид $b = E(a) \equiv a^e \pmod{n}$.

Дешифрование сообщения. Найдем элемент d, обратный к e по модулю $\varphi(n)$, т.е. $de \equiv 1 \pmod{\varphi(n)}$. Пара чисел $(\varphi(n), d)$ называется секретным ключом или дешифрующим ключом системы шифрования RSA. Пусть b — блок зашифрованного сообщения. Тогда дешифрование $D(b)$ получается из соотношения $D(b) \equiv b^d \pmod{n}$.

Докажем, теперь, что $D(E(a)) = a$. Рассмотрим сначала случай $(a, n) = 1$. Используя теорему Эйлера, т.е. утверждение $a^{\varphi(n)} \equiv 1 \pmod{n}$, найдем

$$D(E(a)) \equiv (a^e)^d = a^{ed} \equiv a \pmod{n}.$$

Пусть, теперь $(a, n) > 1$. Так как $n = pq$, то либо $p \mid a$, либо $q \mid a$. Без ограничения общности будем считать, что $p \mid a$. Тогда $a \equiv 0 \pmod{p}$. Следовательно, $a^{ed} \equiv 0 \equiv a \pmod{p}$. Аналогично, доказывается, что $a^{ed} \equiv a \pmod{q}$. Отсюда получим, что

$$p \mid (a^{ed} - a),\ q \mid (a^{ed} - a),\ n = pq \mid (a^{ed} - a),\ a^{ed} \equiv a \pmod{n},$$

т.е. при любом целом числе a имеем $D(E(a)) = a$.

Пример 1. Этот замечательный пример взят из [1]. Зашифруем аббревиатуру RSA с помощью системы шифрования RSA. Возьмем простые числа $p = 17$ и $q = 31$. Имеем $n = pq = 17 \cdot 31 = 527$ и $\varphi(n) = (p-1)(q-1) = 16 \cdot 30 = 480$. Возьмем $e = 7$. Получим $(e, \varphi(n)) = (7, 480) = 1,\ 1 < 7 < 480$. Найдем элемент d, обратный к $e = 7$ по модулю $\varphi(n) = 480$. Для этого с помощью алгоритма Евклида находим целые числа α и β такие, что $e \cdot \alpha + \varphi(n) \cdot \beta = 1$. Имеем

$$480 = 7 \cdot 68 + 4,\ 7 = 4 \cdot 1 + 3,\ 4 = 3 \cdot 1 + 1.$$

Отсюда получим

$$1 = 4 - 3 \cdot 1 = 4 - (7 - 4 \cdot 1) \cdot 1 = 4 \cdot 2 - 7 \cdot 1 = (480 - 7 \cdot 68) \cdot 2 - 7 \cdot 1 =$$
$$= 480 \cdot 2 - 7 \cdot 137 = e \cdot (-137) + \varphi(n) \cdot 2.$$

Поскольку $-137 \equiv 343 \pmod{480}$, имеем $d = 343$.

Теперь подготовим открытый текст сообщения к шифрованию. Представим его в виде последовательности чисел, находящихся на интервале от 0 до 526. Используя двоичную запись порядковых номеров букв R, S, A, находим

$$R \to 18 = (10010)_2,\ S \to 19 = (10011)_2,\ A \to 1 = (00001)_2.$$

Следовательно, сообщение "RSA" будет представлено числом $(100101001100001)_2$. Разобьем это число на блоки чисел. Получим два числа M_1 и M_2 :

$$RSA \to (100101001)_2 - -(100001)_2 = (297)_{10} - -(33)_{10} = M_1 - -M_2.$$

Далее переходим к шифрованию чисел M_1 и M_2. Имеем

$$C_1 = E(M_1) \equiv M_1^e \equiv 297^7 \pmod{527}.$$

Проведем вычисления. Находим

$$C_1 \equiv \left((297)^2\right)^3 \cdot 297 \equiv 200^3 \cdot (-230) \equiv -1840000000 \equiv 474 \pmod{527}.$$

Наконец, шифруем M_2. Получим

$$C_2 = E(M_2) \equiv M_2^e \equiv 33^7 \equiv 407 \pmod{527}.$$

Итак, шифртекст состоит из двух чисел: $(474) - -(407)$.

При расшифровании выполняем следующую последовательность действий. Находим

$$D(C_1) \equiv C_1^{343} \pmod{527},\ D(C_2) \equiv C_2^{343} \pmod{527}.$$

При возведении в степень удобно воспользоваться записью числа 343 в двоичной системе счисления. Имеем

$$343 = 256 + 64 + 4 + 2 + 1 = 2^8 + 2^6 + 2^4 + 2^2 + 2 + 1,$$
$$474^2 \equiv 174 \pmod{527},\ 474^4 \equiv 174^2 \equiv 237 \pmod{527},$$
$$474^8 \equiv 307 \pmod{527},\ 474^{16} \equiv 443 \pmod{527},$$
$$474^{32} \equiv 205 \pmod{527},\ 474^{64} \equiv 392 \pmod{527},$$
$$474^{128} \equiv 307 \pmod{527},\ 474^{256} \equiv 443 \pmod{527}.$$

Следовательно, окончательно получим

$$474^{343} \equiv 443 \cdot 392 \cdot 443 \cdot 237 \cdot 174 \cdot 474 \equiv 297 \pmod{527},$$

$$407^{343} \equiv 33 \pmod{527}.$$

Переходя отсюда к буквенной записи, имеем аббревиатуру RSA.

Приведем несколько простейших случаев, когда шифрование методом RSA будет нестойким.

Разложение на множители числа n, вычисление $\varphi(n)$ и дешифрование сообщения. Пусть при данном натуральном числе n значение функции Эйлера $\varphi(n)$ известно. Тогда легко находится секретный ключ $(\varphi(n), d)$. В частности, если известно разложение числа n на простые сомножители $n = pq$, где p и q — простые числа, то $\varphi(n) = (p-1)(q-1)$.

Пусть, теперь, известны числа n и $\varphi(n)$ и известно, что число n является произведением двух простых сомножителей, причем сами сомножители неизвестны. Тогда можно найти простые числа p и q такие, что $n = pq$, т.е. найти разложение на простые сомножители числа n. Имеем

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1,$$

т.е. находим $p + q = n - \varphi(n) + 1$.

Зная произведение pq и сумму $p+q$, по теореме Виета заключаем, что числа p и q являются корнями квадратного уравнения

$$x^2 - (n - \varphi(n) + 1)x + n = 0.$$

С другой стороны, используя соотношение $(p+q)^2 - (p-q)^2 = 4pq = 4n$, числа p и q можно найти из системы линейных уравнений

$$\begin{cases} p + q = n - \varphi(n) + 1, \\ p - q = \sqrt{(n - \varphi(n) + 1)^2 - 4n}. \end{cases}$$

Разложение на множители числа n, малые делители и о близости простых сомножителей друг к другу. Пусть n — нечетное натуральное число и в своем разложении на простые сомножители оно имеет в точности два простых сомножителя p и q. Далее, для числа n имеет место равенство

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Другими словами, для числа n справедливо соотношение $n = x^2 - y^2 = (x-y)(x+y)$ с неизвестными натуральными числами x и y. Очевидно, что $0 < x - y \leqslant \sqrt{n}$. Перебором натуральных чисел, не превосходящих $\sqrt{n}$, найдем наименьший простой делитель числа n.

Пусть, теперь, $0 < \frac{p-q}{2} \leqslant \alpha$ — мало. Тогда справедливы соотношения

$$n \leqslant n + \left(\frac{p-q}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 \leqslant n + \alpha^2.$$

Следовательно,

$$\sqrt{n} \leqslant \frac{p+q}{2} \leqslant \sqrt{n+\alpha^2}.$$

Отсюда получим, что перебор чисел $0 < x \leqslant \alpha$, для которых $n + x^2$ дает полный квадрат y^2 натурального числа y, обеспечивает разложение числа n на простые сомножители.

Дешифрование сообщения и малый показатель степени e открытого ключа. Пусть несколько абонентов в открытом ключе криптосистемы RSA имеют одну и ту же степень e. Например, три абонента имеют открытые ключи (n_1, e), (n_2, e) и (n_3, e) с взаимно простыми модулями n_1, n_2, n_3. Пусть один из абонентов посылает циркулярное числовое сообщение M. По условию шифрования выполняются неравенства $0 < M < \min\{n_1, n_2, n_3\}$. Наблюдатель может получить три шифрованных текста y_1, y_2, y_3 вида

$$y_1 \equiv M^3 \pmod{n_1},\ y_2 \equiv M^3 \pmod{n_2},\ y_3 \equiv M^3 \pmod{n_3},$$

причем $0 < y_1 < n_1$, $0 < y_2 < n_2$ и $0 < y_3 < n_3$.

Далее, по китайской теореме об остатках существует единственный вычет y по модулю $n_1 n_2 n_3$ с условием $0 < y < n_1 n_2 n_3$, удовлетворяющий системе сравнений

$$\begin{cases} y \equiv y_1 \pmod{n_1}, \\ y \equiv y_2 \pmod{n_2}, \\ y \equiv y_3 \pmod{n_3}. \end{cases}$$

Поскольку $0 < M < \min\{n_1, n_2, n_3\}$, имеем $0 < M^3 < n_1 n_2 n_3$. Следовательно, из условия шифрования получим

$$\begin{cases} M^3 \equiv y_1 \pmod{n_1}, \\ M^3 \equiv y_2 \pmod{n_2}, \\ M^3 \equiv y_3 \pmod{n_3}. \end{cases}$$

Отсюда и из неравенств $0 < y$, $M^3 < n_1 n_2 n_3$ находим, что $y = M^3$, т.е. $0 < y < \sqrt[3]{n_1 n_2 n_3}$, и корень y системы сравнений можно найти перебором.

§ 5. Криптографические хэш-функции

Пусть задано некоторое входное сообщение m. Хэш-функцией (или функцией сгущения, или контрольной функцией) назовем легко вычислимое числовое отображение $h(m)$, ставящее в соответствие сообщению m некоторое "короткое" сообщение $h(m)$.

Другими словами, хэш-функцией называется любая функция $y = h(x_1x_2\dots x_n)$ сообщения $x = x_1x_2\dots x_n$ произвольной длины n ставит в соответствие целое число y фиксированной длины.

Примером хэш-функции может служить контрольная сумма для сообщения $x_1x_2\dots x_n$, т.е. функция $h(x_1x_2\dots x_n) \equiv x_1 + x_2 + \dots + x_n \pmod{2^\omega}$, где ω является максимальным размером машинного слова.

Контрольные суммы часто используются для обнаружения непреднамеренных ошибок при передаче сообщения. Однако, легко внести преднамеренную ошибку, сохранив при этом значение контрольной суммы. Поэтому рассмотренная функция не годится для криптографических применений.

Основными требованиями, предъявляемыми к криптографической хэш-функции, будут следующие.

1) Для любого заданного x из $\mathbf{Z}_2^{(n)}$ значение функции $y = h(x)$ должно вычисляться достаточно "легко" и "быстро".

2) Для любого y практически невозможно найти x такое, что $y = h(x)$.

3) Для любого сообщения x практически невозможно найти $x' \neq x$ такое, что $h(x') = h(x)$.

4) Практически невозможно найти пару различных сообщений x и x' таких, что $h(x') = h(x)$.

Как показывает опыт, разработка хэш-функций, удовлетворяющих приведенным выше требованиям, является сложной, громоздкой в деталях, задачей.

Следующий пример хэш-функции предложил Дамгард (см., например, [18], с.112–113). Пусть задано множество $\mathcal{E}$ наборов длины n, составленных из 0 и 1. На этом множестве определим две односторонние функции f_0 и f_1 со следующими свойствами:
1) отображения f_0 и f_1 являются взаимно однозначными из $\mathcal{E}$ на $\mathcal{E}$, т.е. эти функции задают перестановки элементов множества $\mathcal{E}$;
2) пару (a, b) из декартова произведения множеств $\mathcal{E} \times \mathcal{E}$ называют встречей функций f_0 и f_1, если $f_0(a) = f_1(b.)$ Будем говорить, что пара функций f_0 и f_1 не встречаются с друг другом, если алгоритмически сложно найти их встречу. Будем считать, что f_0 и f_1 не встречаются с друг другом.

Пусть $\{0,1\}^*$ обозначает множество всех конечных последова-

тельностей, составленных из 0 и 1. Итак, пусть заданы две односторонние функции f_0 и f_1 со свойствами 1) и 2), и некоторый элемент $e \in \mathcal{E}$. Определим сжимающую функцию $\mathcal{F}$, заданную на множестве $\{0,1\}^*$, следующим образом $\mathcal{F}\colon \{0,1\}^* \to \mathcal{E}$, причем для любого $x = x_1 x_2 \dots x_k$ из $\{0,1\}^*$ имеем

$$\mathcal{F}(x) = f_{x_1}\left(f_{x_2}\left(\dots f_{x_k}(e)\dots\right)\right).$$

Утверждение 1. *Пусть функции f_0 и f_1 являются односторонними и не встречаются друг с другом. Тогда функция $\mathcal{F}$ не имеет совпадений.*

▷ Предположим, что $\mathcal{F}$ имеет по крайней мере одно совпадение. Выберем среди слов, для которых есть совпадение, слово с минимальной длиной. Если их несколько, то возьмем любое из них с минимальной длиной. Таким образом, найдутся различные $x = x_1 x_2 \dots x_k$ и $x' = x'_1 x'_2 \dots x'_{k'}$ такие, что $\mathcal{F}(x) = \mathcal{F}(x')$. Без ограничения общности можно считать, что $k < k'$. Пусть сначала $x \neq x'$. Тогда точки $a = f_{x_1}^{-1}(\mathcal{F}(x))$ и $b = f_{x'_1}^{-1}(\mathcal{F}(x'))$ дают встречу функций f_{x_1} и $f_{x'_1}$, одна из которых есть f_0, а другая — f_1. Это противоречит условию утверждения. Пусть, теперь, $x_1 = x'_1$. Тогда пара точек $x_2 \dots x_k$ и $x'_2 \dots x'_{k'}$ образует еще одно совпадение для функции $\mathcal{F}$, но с меньшей длиной слова, что противоречит выбору слов x и x'. Это и доказывает, что функция $\mathcal{F}$ не имеет совпадений. ◁

Отсюда имеем, что $\mathcal{F}$ представляет собой хэш-функцию.

Пример 1. Пусть g — первообразный корень по простому модулю p, $p \nmid c$ и $|c| \not\equiv 1 \pmod p$. Определим функции $f_0(x) \equiv g^x \pmod p$ и $f_1(x) = cf_0(x)$. Покажем, что эти функции не встречаются друг с другом. Предположим противное, т.е. найдется пара чисел a и b такая, что $f_0(a) = f_1(b)$. Это означает, что $g^a \equiv cg^b \pmod p$. Последнее эквивалентно тому, что $g^{a-b} \equiv c \pmod p$, т.е. $f_0(a-b) = c$. Следовательно, число c находится как прообраз при отображении обратном f_0, но это противоречит тому, что функция f_0 — односторонняя.

Пример 2. Пусть $n = pq$, где p и q — простые числа, сравнимые с 1 по модулю 4, и — нечетное натуральное число, не превосходящее $\varphi(n)$. Определим функции $f_0(x) \equiv x^e \pmod n$ на вычетах по модулю n, которые не являются квадратами по модулю n и $f_1(x) \equiv x^2 \pmod n$. Покажем, что эти функции не встречаются друг с другом. Предположим противное, т.е. найдется пара чисел a и b такая, что $f_0(a) = f_1(b)$. Это означает, что $a^e \equiv b^2 \pmod n$. Последнее эквивалентно тому, что $a^{e(p-1)/2} \equiv 1 \pmod p$ и $a^{e(q-1)/2} \equiv 1 \pmod q$. Так как вычет a по модулю n не является квадратом, то a не является квадратичным вычетом по крайней мере по одному из чисел p и q.

Это означает, что хотя одно из последних сравнений противоречиво, поскольку оно превращается либо в сравнение $-1 \equiv 1 \pmod{p}$, либо в сравнение $-1 \equiv 1 \pmod{q}$. Таким образом, f_0 и f_1 являются парой функций, которые не встречаются друг с другом.

Покажем теперь, как построить хэш-функцию для сообщения M произвольной длины. Разобьем данное сообщение M на блоки сообщений $M_1, M_2, \ldots, M_n$ одинаковой длины m. Если длина исходного сообщения M не кратна m, то оно дополняется до длины, кратной m, по некоторому заранее оговоренному правилу, задающему однозначность дополнения текста сообщения.

Далее, на основе стойкой шифрующей или односторонней функции с m-битовым входом используется некоторое итерационное соотношение вида

$$H_s = E(H_{s-1}, M_s), \quad 1 \leqslant s \leqslant n,$$

причем число H_0 выбирается специальным способом.

Наконец, число $H = H_n$ принимают за значение хэш-функции. Отметим также, что опыт использования многих криптографических схем показывает, что сам по себе стойкий шифр не всегда приводит к стойкой хэш-функции, но при ее построении существенной является также конкретная схема построения шифра.

Глава VII

ЗАДАЧИ ПО ТЕОРИИ ЧИСЕЛ

§ 1. Квадратичные вычеты и невычеты по простому модулю. Символ Лежандра

1. Пусть a, m — натуральные числа, $(2a, m) = 1$. Тогда сравнение $ax^2 + bx + c \equiv 0 \pmod m$ эквивалентно сравнению $z^2 \equiv b^2 - 4ac \pmod m$.

▷ Имеем цепочку равносильных сравнений

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod m, (2ax + b)^2 \equiv b^2 - 4ac \pmod m.$$

Полагая $z = 2ax + b$, получим сравнение $z^2 \equiv b^2 - 4ac \pmod m$. ◁

Обозначим буквой p нечетное простое число. Далее при $(a, p) = 1$ рассмотрим следующее сравнение

$$x^2 \equiv a \pmod p \qquad (1).$$

Число a называется квадратичным вычетом по модулю p, если сравнение (1) разрешимо и квадратичным невычетом по модулю p, если оно не имеет решений.

2. Пусть сравнение (1) разрешимо. Тогда оно имеет два решения.

▷ Пусть $x_0 \pmod p$ — решение сравнения (1). Тогда вычет $(-x_0) \pmod p$ также является решением (1) и $x_0 \not\equiv -x_0 \pmod p$. ◁

3. Приведенная система вычетов по модулю p состоит из $\frac{p-1}{2}$ квадратичных вычетов, сравнимых по модулю p с числами $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, и $\frac{p-1}{2}$ квадратичных невычетов по модулю p.

▷ Пусть a — квадратичный вычет по модулю p. Тогда существует вычет x_0 из приведенной системы вычетов такой, что $x_0^2 \equiv a \pmod p$. Все вычеты из приведенной системы вычетов исчерпываются следующими:

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}.$$

Их квадраты $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, являются несравнимыми по модулю p. Следовательно, они представляют собой все $\frac{p-1}{2}$ квадратичных вычетов по модулю p. Остальные $\frac{p-1}{2}$ вычетов из приведенной системы вычетов являются квадратичными невычетами по модулю p.◁

4. Пусть все числа $1, 2, \ldots, p-1$ разбиты на две совокупности, причем вторая из них содержит не менее одного числа. Кроме того, имеем:

1) произведение чисел одной совокупности сравнимо по модулю p с числом первой совокупности,

2) произведение двух чисел различных совокупностей сравнимо по модулю p с числом второй совокупности.

Эти условия являются необходимыми и достаточными для того, чтобы первая совокупность состояла из всех квадратичных вычетов по модулю p, а вторая — из всех квадратичных невычетов по модулю p.

▷ Согласно условию 1) среди чисел первой совокупности окажутся все квадратичные вычеты по модулю p :

$$1^2 = 1 \cdot 1,\ 2^2 = 2 \cdot 2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 = \frac{p-1}{2} \cdot \frac{p-1}{2}.$$

Поскольку вторая совокупность содержит по крайней мере одно число, это число будет квадратичным невычетом по модулю p. Следовательно, по условию 2) второй совокупности принадлежат все квадратичные невычеты по модулю p. ◁

5. Для любого простого числа p сравнение

$$(x^2-2)(x^2-3)(x^2-6) \equiv 0 \pmod{p}$$

имеет решение.

▷ Это сравнение имеет решение, поскольку хотя бы одно из чисел $2, 3, 6$ является квадратичным вычетом по модулю p. ◁

6. Пусть $c_1, \ldots, c_m$ — различные корни сравнения

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \quad (a_n, p) = 1,$$

где коэффициенты многочлена $f(x)$ — целые числа. Тогда многочлен $f(x)$ можно представить в виде

$$f(x) = (x - c_1) \ldots (x - c_m) g(x) + ph(x),$$

причем степень многочлена $g(x)$ равна $n - m$ и степень многочлена $h(x)$ не превосходит $m - 1$. Кроме того, m — количество корней сравнения $f(x) \equiv 0 \pmod{p}$ не превосходит его степени n.

▷ Применим метод математической индукции по m. При $m = 1$ запишем многочлен $f(x)$ по формуле Тейлора в точке $x = c_1$. Получим

$$f(x) = a_n (x - c_1)^n + b_{n-1}(x - c_1)^{n-1} + \cdots + b_1 (x - c_1) + b_0,$$

причем коэффициенты $b_{n-1}, \ldots, b_1, b_0$ однозначно определяются по коэффициентам $a_n, a_{n-1}, \ldots, a_1, a_0$. Поскольку $f(c_1) \equiv 0 \pmod{p}$,

коэффициент b_0 делится на p, т.е. $b_0 = pb'_0$. Тем самым, многочлен $f(x)$ представлен в виде $f(x) = (x - c_1)g_1(x) + ph_1(x), h_1(x) = b'_0$. Кроме того, имеем $m = 1 \leqslant n$.

Предположим утверждение верно для $m - 1$ корня $c_1, \ldots, c_{m-1}$ сравнения $f(x) \equiv 0 \pmod p$. Тогда многочлен $f(x)$ представляется в виде $f(x) = (x - c_1) \ldots (x - c_{m-1})g_{m-1}(x) + ph_{m-1}(x)$ и $m - 1 \leqslant n$. Подставим $x = c_m$ в многочлен $f(x)$. Получим

$$f(c_m) \equiv (c_m - c_1) \ldots (c_m - c_1)g_{m-1}(c_m) \pmod p.$$

Поскольку корни $c_1, \ldots, c_{m-1}, c_m$ различны по модулю p, то $g_{m-1}(c_m) \equiv 0 \pmod p$. Следовательно, по доказанному при некотором целом числе d_0 имеем $g_{m-1}(x) = (x - c_m)g_m(x) + pd_0$. Подставляя это равенство в выражение для $f(x)$, найдем

$$f(x) = (x - c_1) \ldots (x - c_m)g_m(x) + ph_m(x),$$

$$h_m(x) = (x - c_1) \ldots (x - c_{m-1})d_0 + h_{m-1}(x).$$

Кроме того, из сравнения степеней имеем $m \leqslant n$. ◁

Символ Лежандра $\left(\frac{a}{p}\right)$ определяется следующим образом. Он равен 1, если сравнение (1) разрешимо и равен -1, если сравнение (1) не имеет решений.

7. (*Критерий Эйлера*). Справедливо сравнение

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Другими словами, для того чтобы вычет a по модулю p являлся квадратичным вычетом по модулю p, необходимо и достаточно, чтобы выполнялось сравнение

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

▷ По малой теореме Ферма имеем сравнение

$$a^{p-1} \equiv 1 \pmod p.$$

Оно эквивалентно следующему

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Оба сомножителя в последнем сравнении не могут одновременно делиться на p, поскольку их разность 2 не делится на p. Сравнению

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

удовлетворяют все $\frac{p-1}{2}$ квадратичных вычетов по модулю p. Так как сравнение не может иметь решений больше его степени, то квадратичными вычетами по модулю исчерпываются все его решения. Следовательно, сравнению

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

удовлетворяют только квадратичные невычеты по модулю p. ◁

8. Имеют место следующие равенства

$$\alpha)\ \left(\frac{1}{p}\right) = 1, \quad \beta)\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \gamma)\ \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

$$\delta)\ \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \text{ для } (b,p) = 1.$$

▷ По критерию Эйлера (задача 6), подставляя значения a, равные 1, -1, ab, получим утверждения $\alpha)$, $\beta)$, $\gamma)$. Так как для $(b,p) = 1$ имеем $\left(\frac{b^2}{p}\right) = 1$, то из $\gamma)$ следует $\delta)$. ◁

9. Имеем $\sum\limits_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0$. Кроме того, если $(a,p) = 1$ и b — произвольное число, то $\sum\limits_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0$.

▷ Поскольку количество квадратичных вычетов и невычетов по модулю p одинаково, то сумма $\sum\limits_{x=1}^{p-1} \left(\frac{x}{p}\right)$ равна нулю. При $(a,p) = 1$ и произвольном b, если x пробегает полную систему вычетов по модулю p, то $ax + b$ будет пробегать полную систему вычетов по модулю p. Следовательно,

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0.$$ ◁

10. Пусть n является квадратичным невычетом по модулю p. Тогда имеем

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv 0 \pmod{p}.$$

▷ По критерию Эйлера имеем

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv \sum_{d|n} \left(\frac{d}{p}\right) \pmod{p}.$$

Пусть $n = \prod\limits_{q|n} q^{a_q}$ — каноническое разложение числа n на простые сомножители. Тогда свойству мультипликативности символа Лежанд-

ра имеем

$$\sum_{d|n}\left(\frac{d}{p}\right)=\prod_{q|n}\left(1+\left(\frac{q}{p}\right)+\cdots+\left(\frac{q^{a_q}}{p}\right)\right).$$

Так как $\left(\frac{n}{p}\right)=-1$, то при некотором $q\mid n$ имеем $\left(\frac{q^{a_q}}{p}\right)=-1$. Следовательно, одна из скобок последнего произведения обращается в нуль. ◁

11. Пусть n_p — наименьший положительный квадратичный невычет по модулю p. Тогда имеем $n_p<\frac{1}{2}+\sqrt{\frac{1}{4}+p}$.

▷ Так как n_p — наименьший положительный квадратичный невычет по модулю p, то вычеты $n_p,\ldots,(n_p-1)n_p$ будут являться квадратичными невычетами по модулю p. Далее имеем $n_p(n_p-1)<p$. В противном случае нашлось бы число k такое, что $(k-1)n_p<p<kn_p$. Следовательно, вычет kn_p был бы наименьшим положительным квадратичным невычетом по модулю p, что противоречит выбору n_p. Неравенство $n_p^2-n_p-p<0$ справедливо при $n_p<\frac{1}{2}+\sqrt{\frac{1}{4}+p}$.◁

12. Пусть $(a,p)=1, p_1=\frac{p-1}{2}$, и имеет место сравнение

$$ax\equiv\varepsilon_x r_x\pmod p,\quad 1\leqslant x,r_x\leqslant p_1,\tag{2}$$

где ε_x равно либо 1, либо -1. Тогда имеем

$$\varepsilon_x=(-1)^{[2ax/p]}.$$

▷ Преобразуем $[2ax/p]$. Имеем

$$\left[\frac{2ax}{p}\right]=\left[2\left[\frac{ax}{p}\right]+2\left\{\frac{ax}{p}\right\}\right]=2\left[\frac{ax}{p}\right]+\left[2\left\{\frac{ax}{p}\right\}\right].$$

Таким образом, число $[2ax/p]$ будет четным, если наименьший неотрицательный вычет числа ax по модулю p не превосходит p_1, т.е. $\varepsilon_x=1$; число $[2ax/p]$ будет нечетным, если наименьший неотрицательный вычет числа ax по модулю p превосходит p_1, т.е. $\varepsilon_x=-1$. Следовательно, $\varepsilon_x=(-1)^{[2ax/p]}$. ◁

13. (*Гаусс*). Пусть $(a,p)=1, p_1=\frac{p-1}{2}$. Тогда имеем

$$\left(\frac{a}{p}\right)=(-1)^{\alpha_{a,p}},\ \alpha_{a,p}=\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right].$$

▷ Перемножая сравнения (2) предыдущей задачи, получим

$$a^{\frac{p-1}{2}}p_1!\equiv\varepsilon_1\ldots\varepsilon_{p_1}r_1\ldots r_{p_1}\pmod p.$$

Поскольку $p_1!=r_1\ldots r_{p_1}$, отсюда имеем

$$a^{\frac{p-1}{2}}\equiv\varepsilon_1\ldots\varepsilon_{p_1}\pmod p.$$

Далее, используя критерий Эйлера и утверждение предыдущей задачи, найдем

$$\left(\frac{a}{p}\right) = (-1)^{\alpha_{a,p}},\ \alpha_{a,p} = \sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]. \qquad \triangleleft$$

14. Пусть $(a,p)=1, (a,2)=1, p_1 = \frac{p-1}{2}$. Тогда имеем

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\beta_{a,p}},\ \beta_{a,p} = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}.$$

$\triangleright$ Поскольку a — нечетное, число $a+p$ будет четным. Используя свойство мультипликативности символа Лежандра и утверждение предыдущей задачи, получим цепочку равенств

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\alpha((a+p)/2,p)}.$$

Следовательно,

$$\alpha((a+p)/2,p) = \sum_{x=1}^{p_1} \left[\frac{(a+p)x}{p}\right] = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x = \beta(a,p). \qquad \triangleleft$$

15. (*Второе дополнительное соотношение квадратичного закона взаимности*). Справедливо равенство

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{если } p \equiv \pm 1 \pmod 8, \\ -1, & \text{если } p \equiv \pm 3 \pmod 8. \end{cases}$$

$\triangleright$ В утверждении предыдущей задачи подставим $a=1$, получим искомую формулу. $\triangleleft$

16. Пусть $p \equiv 3 \pmod 4$ и $q = 2p+1$ — простые числа. Тогда число Мерсенна $M_p = 2^p - 1$ является составным и число q будет его делителем.

$\triangleright$ По малой теореме Ферма имеем

$$2^{2p} - 1 \equiv 0 \pmod q, \quad (2^p-1)(2^p+1) \equiv 0 \pmod q.$$

Поскольку числа 2^p-1 и 2^p+1 взаимно просты, то число q может делить только одно из них. По утверждению предыдущей задачи число 2 является квадратичным вычетом по модулю q. Действительно,

$$\left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}((2p+1)^2-1)} = (-1)^{\frac{p(p+1)}{2}} = 1.$$

По критерию Эйлера это утверждение эквивалентно тому, что $2^p \equiv 1 \pmod q$. $\triangleleft$

17. Пусть $(a,p)=1, (a,2)=1, p_1=\frac{p-1}{2}$. Тогда имеем

$$\left(\frac{a}{p}\right)=(-1)^{\alpha_{a,p}},\ \alpha_{a,p}=\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right].$$

▷ Утверждение этой задачи следует из утверждений задач 14 и 15. ◁

18. (*Квадратичный закон взаимности*). Пусть p,q — различные нечетные простые числа. Тогда имеем

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

▷ Из утверждения задачи 15 имеем

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\alpha(q,p)+\alpha(p,q)}.$$

Величина $\alpha(q,p)+\alpha(p,q)$ равна

$$\sum_{x=1}^{p_1}\left[\frac{qx}{p}\right]+\sum_{y=1}^{q_1}\left[\frac{py}{q}\right].$$

Но последняя сумма равна количеству целых точек внутри прямоугольника со сторонами $0<x<p/2$ и $0<y<q/2$, т.е. равна $\frac{p-1}{2}\frac{q-1}{2}$. Диагональ $y=\frac{qx}{p}$ этого прямоугольника делит его на два треугольника. Количество целых точек треугольника, лежащего под этой диагональю равно $\alpha(q,p)$, а количество целых точек треугольника, лежащего над этой диагональю равно $\alpha(p,q)$. Это и доказывает искомое утверждение. ◁

19. Справедливы соотношения:

$$1)\ \left(\frac{3}{p}\right)=\begin{cases}1, & \text{если } p\equiv\pm1 \pmod{12}\\ -1, & \text{если } p\equiv\pm5 \pmod{12},\end{cases}$$

$$2)\ \text{при } p>3 \text{ имеем } \left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right).$$

▷ 1) По квадратичному закону взаимности имеем

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Далее, по свойству символа Лежандра при $p\geqslant 3$ получим

$$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{если } p\equiv1 \pmod{3},\\ \left(\frac{-1}{3}\right)=-1, & \text{если } p\equiv2 \pmod{3}.\end{cases}$$

Наконец, имеем

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 4, \\ -1, & \text{если } p \equiv -1 \pmod 4 \end{cases}$$

Отсюда следует искомая формула.

2) Используя предыдущее утверждение, имеем

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right). \qquad \triangleleft$$

20. а) Сравнение $x^2 + 1 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 4$.

б) Сравнение $x^2 + 3 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 6$.

в) Простых чисел вида $p \equiv 1 \pmod 4$ бесконечно много.

г) Простых чисел вида $p \equiv 1 \pmod 6$ бесконечно много.

д) Сравнение $x^2 + 2 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 8$ или $p \equiv 3 \pmod 8$.

$\triangleright$ а) Условие разрешимости сравнения $x^2 + 1 \equiv 0 \pmod p$ эквивалентно тому, что символ Лежандра $\left(\frac{-1}{p}\right)$ равен 1. По первому дополнительному соотношению квадратичного закона взаимности имеем

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 4, \\ -1, & \text{если } p \equiv -1 \pmod 4. \end{cases}$$

б) Имеем

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 6, \\ -1, & \text{если } p \equiv -1 \pmod 6. \end{cases}$$

в) Предположим, что простых чисел вида $p \equiv 1 \pmod 4$ конечное число: $p_1, \ldots, p_n$. Число $(2p_1 \ldots p_n)^2 + 1$ в качестве своих простых делителей будет иметь только простые числа вида $4k + 1$ и они все будут отличны от чисел $p_1, \ldots, p_n$. Наименьший, отличный от единицы, среди делителей числа $(2p_1 \ldots p_n)^2 + 1$ будет простым. Это противоречит предположению об исчерпании всех простых вида $4k + 1$ числами $p_1, \ldots, p_n$. Следовательно, простых чисел вида $p \equiv 1 \pmod 4$ бесконечно много.

г) Пусть простые числа вида $6k + 1$ исчерпываются числами $p_1, \ldots, p_n$. Число $(2p_1 \ldots p_n)^2 + 3$ имеет простые делители только вида $6k+1$, наименьший из которых, отличный от единицы, будет простым и отличным от $p_1, \ldots, p_n$. Следовательно, предположение о том, что простых чисел вида $6k + 1$ конечно, не имеет места.

д) Разрешимость сравнения $x^2 + 2 \equiv 0 \pmod{p}$ эквивалентна условию $\left(\frac{-2}{p}\right) = 1$. По дополнительным соотношениям квадратичного закона взаимности имеем

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}}.$$

Следовательно,

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 8,\ p \equiv 3 \pmod 8, \\ -1, & \text{если } p \equiv -1 \pmod 8,\ p \equiv -3 \pmod 8. \end{cases}$$ ◁

21. При нечетном простом числе p число -4 будет биквадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv 1 \pmod 4$.

▷ Из тождества

$$x^4 + 4 = ((x+1)^2 + 1)((x-1)^2 + 1)$$

следует, что число -4 будет биквадратичным вычетом по модулю p тогда и только тогда, когда число -1 будет квадратичным вычетом по модулю p. По утверждению предыдущей задачи последнее эквивалентно тому, что $p \equiv 1 \pmod 4$. ◁

22. Пусть $p \equiv 5 \pmod 8$. Тогда сравнение $x^4 + 1 \equiv 0 \pmod p$ не имеет решений.

▷ Предположим противное. Пусть существует решение x_0 сравнения $x_0^4 + 1 \equiv 0 \pmod p$. Справедливо равенство $p - 1 = 4u$, где u — нечетное число. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 \equiv x_0^4 \pmod p, -1 = (-1)^u \equiv x_0^{4u} \equiv x_0^{p-1} \equiv 1 \pmod p.$$

Следовательно, предположение о разрешимости сравнения $x^4 + 1 \pmod p$ неверно. ◁

23. а) При нечетном простом числе p число -1 будет биквадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv 1 \pmod 8$.

б) Существует бесконечно много простых чисел вида $8k + 1$.

▷ а) Пусть $p \equiv 1 \pmod 8$. Тогда $(p-1)/2$ квадратичный вычет по модулю p удовлетворяет сравнению $x^{(p-1)/2} \equiv 1 \pmod p$. Предположим, теперь, что сравнение $x^4 \equiv -1 \pmod p$ не имеет решений. Тогда сравнению $x^{(p-1)/4} \equiv 1 \pmod p$ не удовлетворяет ни один квадратичный вычет по модулю p. Поскольку они удовлетворяют либо сравнению $x^{(p-1)/4} \equiv 1 \pmod p$, либо сравнению $x^{(p-1)/4} \equiv -1 \pmod p$, все $(p-1)/2$ квадратичных вычета по модулю p удовлетворяют второму сравнению. Но это невозможно, поскольку количество

несравнимых вычетов по модулю p не превосходит степени сравнения $(p-1)/4$. Следовательно, сравнение $x^4+1 \equiv 0 \pmod p$ имеет по крайней мере одно решение.

По предыдущей задаче для $p \equiv 5 \pmod 8$ сравнение $x^4+1 \equiv 0 \pmod p$ не имеет решений.

Пусть $p \equiv 3$ или $7 \pmod 8$, т.е. $p \equiv 3 \pmod 4$. Но тогда даже сравнение $x^2+1 \equiv 0 \pmod p$ не имеет решений.

б) Пусть существует только конечное число простых чисел вида $8k+1$. Буквой P обозначим их произведение. Тогда по утверждению предыдущей задачи число $(2P)^4+1$ будет иметь простые делители вида $8k+1$ и они будут взаимно просты с P. Таким образом, предположение о существовании только конечного числа простых чисел вида $8k+1$ неверно. ◁

24. Пусть k — натуральное число, p — простое число и $p \equiv 2^k+1 \pmod{2^{k+1}}$. Тогда сравнение $x^{2^k}+1 \equiv 0 \pmod p$ не имеет решений.

▷ Предположим противное. Пусть существует решение x_0 сравнения $x_0^{2^k}+1 \equiv 0 \pmod p$. Справедливо равенство $p-1=2^k u$, где u — нечетное число. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 \equiv x_0^{2^k} \pmod p, -1 = (-1)^u \equiv x_0^{2^k u} \equiv x_0^{p-1} \equiv 1 \pmod p.$$

Следовательно, предположение о разрешимости сравнения $x^{2^k}+1 \pmod p$ неверно. ◁

25. Пусть k — натуральное число и сравнение $x^{2^k}+1 \equiv 0 \pmod p$ разрешимо. Тогда $p \equiv 1 \pmod{2^{k+1}}$.

▷ Представим число $p-1$ в виде $p-1=2^r u$, где u — нечетное число. Предположим, что $r \leqslant k$. По условию задачи существует решение x_0 сравнения $x_0^{2^k} \equiv -1 \pmod p$. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 = (-1)^u \equiv x_0^{2^k u} \equiv x_0^{2^{k-r} 2^r u} \equiv x_0^{2^{k-r}(p-1)} \equiv 1 \pmod p.$$

Следовательно, предположение, что $r \leqslant k$ неверно, и $p \equiv 1 \pmod{2^{k+1}}$.◁

26. Пусть a — одно из чисел 2 или 3, число p — нечетное простое, и сравнение $z^2+a \equiv 0 \pmod p$ разрешимо. Тогда существует единственное представление числа p в виде $p=x^2+ay^2$, где x, y — натуральные числа, $x \equiv zy \pmod p$.

▷ Пусть $|z_0| \leqslant \frac{p-1}{2}$ решение сравнения $z_0^2+a \equiv 0 \pmod p$. Тогда получим $mp = z_0^2+a$. Оценим величину m. Имеем

$$1 \leqslant m = \frac{1}{p}(z_0^2+a) \leqslant \frac{1}{p}\left(\frac{(p-1)^2}{4}+a\right) \leqslant \frac{p^2-2p+13}{4p} < p.$$

Пусть m_0 — наименьшее натуральное число в представлении вида $m_0 p = x^2 + ay^2$. Тогда из доказанного выше находим $1 \leqslant m_0 < p$. Предположим, что $m_0 > 1$. Возьмем числа u, v из условий

$$u \equiv x \pmod{m_0}, v \equiv y \pmod{m_0}, 1 \leqslant |u| \leqslant m_0/2, 1 \leqslant |v| \leqslant m_0/2.$$

Тогда получим

$$u^2 + av^2 \equiv x^2 + ay^2 \equiv 0 \pmod{m_0}$$

Следовательно, при некотором r имеем $m_0 r = u^2 + av^2$, где либо $r \leqslant \frac{(1+a)m_0}{4} < m_0$, либо $r = m_0, u = m_0/2, v = m_0/2, a = 3$. Последний случай невозможен, поскольку

$$x = y = m_0/2 = u = v, m_0 p = x^2 + 3y^2 = u^2 + 3v^2 = m_0^2,\ 1 < m_0 < p.$$

Таким образом

$$m_0^2 rp = (x^2 + ay^2)(u^2 + av^2) = x^2u^2 + a^2y^2v^2 + a(x^2v^2 + y^2u^2) = \\ = (xu + ayv)^2 + a(xv - yu)^2.$$

Кроме того, справедливы сравнения

$$xv - yu \equiv xy - yx \equiv 0 \pmod{m_0},\ xu + ayv \equiv x^2 + ay^2 \equiv 0 \pmod{m_0}.$$

Из последних соотношений получим

$$rp = X^2 + aY^2, \quad 1 \leqslant r < m_0.$$

Это противоречит тому, что $m_0 > 1$ — минимальное число в указанном представлении. Следовательно, $m_0 = 1$.

Докажем, что представление вида $p = x^2 + ay^2, x \equiv zy \pmod{p}$ — единственно. Пусть $p = x_1^2 + ay_1^2, x_1 \equiv zy_1 \pmod{p}$ — другое представление простого числа p. Тогда

$$p^2 = (x^2 + ay^2)(x_1^2 + ay_1^2) = (xx_1 + ayy_1)^2 + a(xy_1 - yx_1)^2$$

Поскольку $xy_1 - yx_1 \equiv 0 \pmod{p}$, имеем $xy_1 - yx_1 = 0$. Следовательно, $xx_1 + ayy_1 = p$. Отсюда получим

$$xp = x(xx_1 + ayy_1) - ay(xy_1 - yx_1) = x^2x_1 + ay^2x_1 = x_1(x^2 + ay^2) = x_1 p,$$

т.е. $x = x_1, y = y_1$. ◁

27. Пусть $p \equiv 1 \pmod 4$, $(k, p) = 1$,

$$S(k) = \sum_{x=0}^{p-1} \left(\frac{x(x^2 + k)}{p} \right).$$

Тогда: 1) $S(k)$ — четное число,

2) $S(kt^2) = \left(\frac{t}{p}\right) S(k)$,

3) при $\left(\frac{r}{p}\right) = 1$ и $\left(\frac{n}{p}\right) = -1$ имеем

$$p = \left(\frac{S(r)}{2}\right)^2 + \left(\frac{S(n)}{2}\right)^2,$$

4) справедливо неравенство $|S(k)| \leqslant 2\sqrt{p}$.

▷ 1) Поскольку $\left(\frac{-1}{p}\right) = 1$, слагаемые, отвечающие $x = x_1$ и $x = -x_1$, равны между собой, а слагаемое, отвечающее $x = 0$, равно 0. Следовательно, $S(k)$ — четное число.

2) Имеем

$$S(kt^2) = \sum_{x=0}^{p-1} \left(\frac{xt(x^2t^2 + kt^2)}{p}\right) = \left(\frac{t}{p}\right) S(k).$$

3) Положим $p_1 = (p-1)/2$. Поскольку для любого числа t от 1 до p_1 справедливы равенства

$$S^2(rt^2) = S^2(r), \quad S^2(nt^2) = S^2(n), \quad S(0) = 0,$$

где r — некоторый квадратичный вычет и n — некоторый квадратичный невычет по модулю p.

Заметим, что, если t пробегает все числа от 1 до p_1, то rt^2 пробегает все квадратичные вычеты, а nt^2 — все квадратичные невычеты по модулю p. Следовательно,

$$p_1(S^2(r) + S^2(n)) = \sum_{t=1}^{p_1} S^2(rt^2) + \sum_{t=1}^{p_1} S^2(nt^2) + S^2(0) =$$

$$= \sum_{k=0}^{p-1} S^2(k) = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1} \left(\frac{xy}{p}\right) \sum_{k=0}^{p-1} \left(\frac{(x^2+k)(y^2+k)}{p}\right).$$

Далее имеем

$$T(x,y) = \sum_{k=0}^{p-1} \left(\frac{(x^2+k)(y^2+k)}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{k(y^2-x^2+k)}{p}\right).$$

Следовательно, при $kk_1 \equiv 1 \pmod p$ имеем

$$T(x,y) = \sum_{k=1}^{p-1} \left(\frac{kk_1((y^2-x^2)k_1 + kk_1)}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{(y^2-x^2)k+1)}{p}\right).$$

Таким образом

$$T(xy) = \begin{cases} p-1, & \text{если } x \equiv \pm y \pmod p, \\ -1, & \text{если } x \not\equiv \pm y \pmod p. \end{cases}$$

Наконец, получаем

$$p_1\left(S^2(r)+S^2(n)\right)=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)T(x,y)=\sum_{x=1}^{p-1}(T(x,x)+T(x,-x))+$$

$$+\sum_{x=1}^{p-1}\sum_{\substack{y=1\\ x\not\equiv\pm y \pmod p}}^{p-1}\left(\frac{xy}{p}\right)T(x,y)=2(p-1)^2-2(p-1)(-1)=2(p-1)p.$$

Отсюда имеем искомую формулу

$$p=\left(\frac{S(r)}{2}\right)^2+\left(\frac{S(n)}{2}\right)^2.$$

4) Из утверждения 3) следует, что $|S(k)|\leqslant 2\sqrt{p}$. ◁

28. Число 2 является квадратичным невычетом по модулю нечетного простого числа p тогда и только тогда, когда имеет вид $4k+3$, где k — любое натуральное число.

▷ По второму дополнительному соотношению квадратичного закона взаимности имеем

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Отсюда получаем

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{если } p\equiv 1 \pmod 4,\\ -1, & \text{если } p\equiv 1 \pmod 4.\end{cases}$$ ◁

29. Число 3 является наименьшим положительным квадратичным невычетом по модулю нечетного простого числа p тогда и только тогда, когда $p\equiv 5 \pmod{12}$.

▷ Имеем

$$\left(\frac{2}{p}\right)=1,\quad \left(\frac{3}{p}\right)=-1.$$

Следовательно, $p\equiv 1 \pmod 4$, и по квадратичному закону взаимности получаем

$$-1=\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right).$$

Отсюда находим, что число p принадлежит прогрессиям $p\equiv 1 \pmod 4$ и $p\equiv 2 \pmod 3$. Из этого однозначно определяется прогрессия с разностью 12 и начальным членом 5 такая, что $p\equiv 5 \pmod{12}$. ◁

30. Пусть q_k — k-е простое число, которое является наименьшим положительным квадратичным невычетом по модулю p. Тогда чис-

ло p принадлежит одной из $\varphi(4q_2\dots q_k)/2^k$ с разностью $4q_2\dots q_k$ и некоторыми начальными членами a, взаимно простыми с $4q_2\dots q_k$.

▷ Используя квадратичный закон взаимности, найдем, что число p удовлетворяет условиям

$$p\equiv 1 \pmod 4, \quad p\equiv 1 \pmod 3,$$

$$\left(\frac{p}{q_s}\right)=1,\ s=2,\dots,k-1; \quad \left(\frac{p}{q_k}\right)=-1.$$

Отсюда и следует искомое утверждение. ◁

31. Имеем $\sum\limits_{x=1}^{p-2}\left(\frac{x(x+1)}{p}\right)=-1$.

▷ Определим вычет x_1 по модулю p из сравнения $xx_1\equiv 1 \pmod p$. Далее преобразуем сумму

$$\sum_{x=1}^{p-2}\left(\frac{x(x+1)}{p}\right)=\sum_{x=1}^{p-2}\left(\frac{x_1^2}{p}\right)\left(\frac{x(x+1)}{p}\right)=$$

$$=\sum_{x=1}^{p-2}\left(\frac{xx_1(xx_1+x_1)}{p}\right)=\sum_{x=1}^{p-2}\left(\frac{1+x_1}{p}\right).$$

Поскольку при $1\leqslant x\leqslant p-2$ последовательность $1+x_1$ пробегает все вычеты приведенной системы вычетов по модулю p, кроме 1, искомая сумма будет равна -1. ◁

32. Пусть $p>2$ — простое число и N — количество натуральных чисел n с условием $1\leqslant n\leqslant p-2$ таких, что n и $n+1$ одновременно являются квадратичными вычетами по модулю p. Тогда имеем $N=\frac{1}{4}\left(p-4-\left(\frac{-1}{p}\right)\right)$.

▷ Имеем

$$N=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)+\left(\frac{n+1}{p}\right)+\left(\frac{n(n+1)}{p}\right)\right).$$

Отсюда следует искомая формула для N. ◁

33. Пусть $p>2$ — простое число и $f(x)=ax^2+bx+c$ — многочлен

с целыми коэффициентами, $(a,p)=1$ и $\Delta=b^2-4ac$. Тогда имеем

$$S=\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & \text{если } p\nmid\Delta,\ \left(\frac{\Delta}{p}\right)=1,\\ \left(\frac{a}{p}\right), & \text{если } p\nmid\Delta,\ \left(\frac{\Delta}{p}\right)=-1,\\ (p-1)\left(\frac{a}{p}\right), & \text{если } p\mid\Delta.\end{cases}$$

▷ Имеем цепочку равенств

$$S=\sum_{x=0}^{p-1}\left(\frac{4a^2}{p}\right)\left(\frac{ax^2+bx+c}{p}\right)=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{4a^2x^2+4abx+4ac}{p}\right)=$$

$$=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{(2ax+b)^2-\Delta}{p}\right)=\left(\frac{a}{p}\right)V,$$

где $V=V(\Delta)=\sum\limits_{x=0}^{p-1}\left(\frac{x^2-\Delta}{p}\right)$.

Рассмотрим случай $\left(\frac{\Delta}{p}\right)=1$, т.е. при некотором d, взаимно простом с p, имеем $\Delta\equiv d^2 \pmod p$. Делая замену переменной x на dx, получим

$$V=\sum_{x=0}^{p-1}\left(\frac{x^2-1}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x(x+2)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{1+2x'}{p}\right),$$

где $xx'\equiv 1 \pmod p$.

Следовательно,

$$V=\sum_{x=0}^{p-1}\left(\frac{1+2x}{p}\right)-1=-1.$$

Пусть, теперь, $\left(\frac{\Delta}{p}\right)=-1$ и число n обозначает наименьший невычет по модулю p. Тогда имеем

$$\sum_{\Delta=1}^{p-1}V(\Delta)=\frac{p-1}{2}(V(1)+V(n))=0.$$

Отсюда получаем искомую формулу для суммы S. ◁

34. Пусть $p>2$ — простое число $(a,p)=1$ и τ_a — сумма Гаусса вида

$$\tau_a=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{ax}{p}},\quad \tau=\tau_1.$$

Тогда имеем

$$\tau_a = \left(\frac{a}{p}\right)\tau, \quad |\tau| = \sqrt{p}.$$

▷ Имеем

$$\tau_a = \sum_{x=1}^{p-1}\left(\frac{a^2}{p}\right)\left(\frac{x}{p}\right)e^{2\pi i\frac{ax}{p}} = \left(\frac{a}{p}\right)\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)e^{2\pi i\frac{ax}{p}} = \left(\frac{a}{p}\right)\tau.$$

Преобразуем квадрат модуля суммы Гаусса, делая замену переменной суммирования $y = tx$. Получим

$$|\tau|^2 = \tau\bar{\tau} = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x}{p}}\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)e^{-2\pi i\frac{y}{p}} =$$

$$= \sum_{x=1}^{p-1}\sum_{t=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x(1-t)}{p}} = \sum_{t=1}^{p-1}\left(\frac{x}{p}\right)\sum_{x=1}^{p-1}e^{2\pi i\frac{x(1-t)}{p}}.$$

При $t = 1$ сумма по x равна $p-1$, а при $t \neq 1$ она равна $-\left(\frac{t}{p}\right)$. Следовательно, имеем

$$|\tau|^2 = p - 1 - \sum_{t=2}^{p-1}\left(\frac{t}{p}\right) = p, |\tau| = \sqrt{p}. \quad \triangleleft$$

35. Пусть $m > 2, (a, m) = 1$,

$$S_{a,m} = \sum_{x=0}^{m-1} e^{2\pi i\frac{ax^2}{m}}.$$

Тогда

a) при любом простом числе p имеем

$$S_{a,p} = \tau_a, |S_{a,p}| = \sqrt{p};$$

b) справедливы следующие соотношения

$$|S_{a,m}| = \begin{cases} \sqrt{m}, & \text{если} \quad m \equiv 1 \pmod 2, \\ 0, & \text{если} \quad m \equiv 2 \pmod 4, \\ \sqrt{2m}, & \text{если} \quad m \equiv 0 \pmod 4, \end{cases}$$

c) имеем равенство

$$S_{1,m} = \frac{1 + i^{-m}}{1 + i^{-1}}\sqrt{m};$$

d) при $m > 1, (2A, m) = 1$ и любом целом числе a имеем

$$\left|\sum_{x=0}^{m-1} e^{2\pi i\frac{Ax^2+ax}{m}}\right| = \sqrt{m}.$$

▷ a) Имеем

$$S_{a,p}=\sum_{x=0}^{p-1}e^{2\pi i\frac{ax^2}{p}}=1+\sum_{y=1}^{p-1}\left(1+\left(\frac{y}{p}\right)\right)e^{2\pi i\frac{ay}{p}},$$

так как

$$1+\left(\frac{y}{p}\right)=\begin{cases}2, & \text{если} \quad y\equiv x^2 \pmod p,\\ 0, & \text{если} \quad y\not\equiv x^2 \pmod p.\end{cases}$$

Таким образом, получим

$$S_{a,p}=1+\sum_{x=1}^{p-1}e^{2\pi i\frac{ax}{p}}+\tau_a=\tau_a.$$

Следовательно, по утверждению предыдущей задачи имеем

$$|S_{a,p}|=|\tau_a|=|\tau|=\sqrt{p}.$$

b) Преобразуем модуль суммы $S_{a,m}$, делая замену переменной $y=x+t$. Получим

$$|S_{a,m}|^2=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}e^{2\pi i\frac{x^2-y^2}{m}}=\sum_{t=0}^{m-1}e^{-2\pi i\frac{at^2}{m}}\sum_{x=0}^{m-1}e^{-2\pi i\frac{2atx}{m}}.$$

Далее, имеем

$$\sum_{x=0}^{m-1}e^{-2\pi i\frac{2atx}{m}}=\begin{cases}m, & \text{если} \quad m\mid 2t,\\ 0, & \text{если} \quad m\not\mid 2t.\end{cases}$$

Следовательно, при $m\equiv 1 \pmod 2$ имеем

$$|S_{a,m}|^2=me^{-2\pi i\frac{a\cdot 0^2}{m}}=m, \quad |S_{a,m}|=\sqrt{m}.$$

Пусть, теперь, $m=2m_1$ — четное число. Тогда имеем

$$|S_{a,m}|^2=m\left(e^{-2\pi i\frac{a\cdot 0^2}{m}}+e^{-2\pi i\frac{a\cdot m_1^2}{m}}\right)=m\left(1+e^{-2\pi i\frac{am_1}{2}}\right).$$

Отсюда получим

$$|S_{a,m}|^2=\begin{cases}0, & \text{если} \quad m_1\equiv 1 \pmod 2,\\ 2m, & \text{если} \quad m_1\equiv 0 \pmod 2.\end{cases}$$

Последние соотношения влекут искомые равенства.

c) Воспользуемся формулой Пуассона суммирования значений функции в целых точках в следующем виде. Пусть a и b — полуцелые числа, $f(x)$ имеет непрерывную первую производную на отрезке $[a,b]$ и $M=\max\limits_{x\in[a,b]}|f'(x)|$. Тогда при любом $K\geqslant 1$ справедливо

соотношение

$$\sum_{a<n\leqslant b} f(n) = \sum_{k=-K}^{K} \int_a^b f(x)e^{2\pi ikx}\,dx + R, \quad |R| \leqslant \frac{8M(b-a)\ln K}{K}.$$

При $K \geqslant 1$ получим

$$S_{1,m} = \sum_{n=1}^{m} e^{2\pi i\frac{n^2}{m}} = \sum_{k=-2K}^{2K} I_k + R,$$

где

$$I_k = \int_{0,5}^{N+0,5} e^{2\pi i\left(\frac{x^2}{m}+kx\right)}, |R| \ll \frac{m\ln K}{K}.$$

Преобразуем интеграл I_k. Имеем

$$I_k = e^{-\frac{\pi i}{2}k^2 m} \int_{0,5}^{m+0,5} e^{\frac{2\pi i}{m}(x+0,5km)^2}\,dx = e^{-\frac{\pi i}{2}k^2 m} \int_{0,5+0,5km}^{0,5+(1+0,5k)m} e^{\frac{2\pi i}{m}x^2}\,dx.$$

Суммируя интегралы I_k отдельно по четным $k = 2l$ и по нечетным $k = 2l-1$, находим

$$S_{1,m} = \sum_{l=-K}^{K} \int_{0,5+lm}^{0,5+(1+l)m} e^{2\pi ix^2/m}\,dx + i^{-m} \int_{0,5+(l-0,5)m}^{0,5+(l+0,5)m} e^{2\pi ix^2/m}\,dx + R =$$

$$\sqrt{m}(1+i^{-m}) \int_{-\infty}^{\infty} e^{2\pi iz^2}\,dz + O\left(m^{1/4}K^{-1/2}\right) + R.$$

Переходя к пределу при $K \to \infty$, получим

$$S_{1,m} = \sqrt{m}(1+i^{-m}) \int_{-\infty}^{\infty} e^{2\pi iz^2}\,dz.$$

При $m = 1$ имеем $S_{1,1} = 1$. Следовательно,

$$1 = S_{1,1} = (1+i^{-1}) \int_{-\infty}^{\infty} e^{2\pi iz^2}\,dz.$$

Таким образом имеем

$$S_{1,m} = \frac{1+i^{-m}}{1+i^{-1}}\sqrt{m}.$$

d) Определим число b из сравнения $a \equiv 2Ab \pmod m$. Тогда имеем

$$|T_{A,m}| = \left| \sum_{x=0}^{m-1} e^{2\pi i \frac{A(x+b)^2}{m}} \right|$$

Так как m — нечетное число, то по утверждению предыдущей задачи имеем $|T_{A,m}| = |S_{A,m}| = \sqrt{m}$. ◁

36. Пусть p — нечетное простое число, M, Q — целые числа, $1 \leqslant M < M + Q \leqslant p$. Тогда

a) имеем неравенство

$$\left| \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) \right| \leqslant \sqrt{p} \ln p;$$

b) справедливы соотношения

$$|R - Q/2| < (\sqrt{p} \ln p)/2, \quad |N - Q/2| < (\sqrt{p} \ln p)/2,$$

где R — количество квадратичных вычетов и N — количество квадратичных невычетов по модулю p на отрезке от M до $M + Q - 1$.

▷ a) Имеем равенство

$$S = \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \sum_{y=M}^{M+Q-1} \left(\frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(x-y)}{p}} \right) =$$

$$= \frac{1}{p} \sum_{a=0}^{p-1} \left(\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}} \right) \left(\sum_{y=M}^{M+Q-1} e^{-2\pi i \frac{ay}{p}} \right) = \frac{1}{p} \sum_{a=1}^{p-1} \tau_a L_{a,p}.$$

Следовательно

$$|S| \leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} |L_{a,p}| = \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \left| \frac{e^{-2\pi i \frac{aM}{p}} - e^{-2\pi i \frac{a(M+Q)}{p}}}{1 - e^{-2\pi i \frac{a}{p}}} \right| \leqslant$$

$$\leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \frac{1}{|\sin(\frac{\pi a}{p})|} = \frac{2}{\sqrt{p}} \sum_{a=1}^{(p-1)/2} \frac{1}{\sin(\frac{\pi a}{p})}.$$

Поскольку при $0 \leqslant y \leqslant 1/2$ справедливо неравенство $\sin \pi y \geqslant 2y$, имеем оценку

$$|S| \leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{(p-1)/2} \frac{p}{a} \leqslant \sqrt{p} \left(\int_1^{\frac{p-1}{2}} \frac{dt}{t} + \left(\frac{1}{2} + \int_1^{\infty} \frac{\rho(t)}{t^2}\, dt \right) + \frac{1}{p-1} - \right.$$

$$-\int\limits_{\frac{p-1}{2}}^{\infty}\frac{\rho(t)}{t^2}\,dt\Bigg) < \sqrt{p}\left(\ln\left((p-1)/2\right)+\gamma+\frac{1}{p-1}\right) < \sqrt{p}\ln p.$$

b) По утверждению предыдущей задачи имеем $|R-N| < \sqrt{p}\ln p$. Кроме того, $R+N=Q$. Отсюда следует искомое утверждение. ◁

37. Пусть p — нечетное простое число, $N \geqslant 1$, и

$$S = \max_N |T(N)|, \quad T(N) = \sum_{n=1}^{N}\left(\frac{n}{p}\right).$$

Тогда при $p\to\infty$ справедливо неравенство $S \leqslant (c+o(1))\sqrt{p}\ln p$, где

$$c = \begin{cases} 1/\pi^2, & \text{если} \quad \left(\frac{-1}{p}\right)=1,\\ 1/(2\pi), & \text{если} \quad \left(\frac{-1}{p}\right)=-1.\end{cases}$$

▷ Пользуясь приемом И. М. Виноградова, получим

$$T(N) = \sum_{n=1}^{N}\left(\frac{n}{p}\right) = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\sum_{m=1}^{N}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(n-m)}{p}} =$$

$$\frac{1}{p}\sum_{a=1}^{p-1}\left(\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e^{2\pi i\frac{an}{p}}\right)\left(\sum_{m=1}^{N}e^{-2\pi i\frac{am}{p}}\right).$$

Пользуясь периодичностью с периодом p всех функций в сумме $T(N)$, находим

$$T(N) = \frac{\tau}{p}\sum_{0<|a|\leqslant(p-1)/2}\left(\frac{a}{p}\right)\sum_{m=1}^{N}e^{-2\pi i\frac{am}{p}}.$$

Просуммируем геометрическую прогрессию. Имеем

$$\sum_{m=1}^{N}e^{-2\pi i\frac{am}{p}} = \frac{e^{-2\pi i\frac{a}{p}}-e^{-2\pi i\frac{a(N+1)}{p}}}{1-e^{-2\pi i\frac{a}{p}}}.$$

Таким образом

$$T(N) = \frac{\tau}{p}\sum_{0<|a|\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{e^{2\pi i\frac{aN}{p}}-1}{1-e^{2\pi i\frac{a}{p}}}.$$

Воспользуемся при $0<|a|\leqslant(p-1)/2$ и $p\to\infty$ следующим асимптотическим соотношением

$$\frac{1}{1-e^{2\pi i\frac{a}{p}}} = -\frac{1}{2\pi i\frac{a}{p}}\left(1+O\left(\frac{a}{p}\right)\right) = -\frac{p}{2\pi i a}+O(1).$$

Рассмотрим сначала случай $\left(\frac{-1}{p}\right)=1$. Получим

$$|T(N)|=\frac{\sqrt{p}}{2\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{e^{-2\pi i\frac{aN}{p}}-e^{2\pi i\frac{aN}{p}}}{a}\right|+O(\sqrt{p})=$$

$$=\frac{\sqrt{p}}{\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{\sin 2\pi\frac{aN}{p}}{a}\right|+O(\sqrt{p}).$$

Так как для любого вещественного числа α справедливо неравенство

$$\sum_{n\leqslant x}\frac{|\sin(\alpha n)|}{n}\leqslant\frac{2}{\pi}\ln x+O(1),\qquad(*)$$

то имеем

$$|T(N)|\leqslant\frac{\sqrt{p}}{\pi}\sum_{0<a\leqslant(p-1)/2}\frac{\left|\sin 2\pi\frac{aN}{p}\right|}{a}+O(\sqrt{p})\leqslant$$

$$\leqslant\frac{2\sqrt{p}}{\pi^2}\ln\frac{p-1}{2}(1+o(1)).$$

Следовательно,

$$S=\max_{N\geqslant 1}|T(N)|\leqslant\left(\frac{2}{\pi^2}+o(1)\right)\sqrt{p}\ln p.$$

Рассмотрим случай $\left(\frac{-1}{p}\right)=-1$. Объединяя в сумме $T(N)$ слагаемые, отвечающие значениям a и $-a$, получим

$$|T(N)|=\frac{\sqrt{p}}{2\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{e^{-2\pi i\frac{aN}{p}}+e^{2\pi i\frac{aN}{p}}-2}{a}\right|+O(\sqrt{p})=$$

$$=\frac{\sqrt{p}}{\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{1-\cos 2\pi\frac{aN}{p}}{a}\right|+O(\sqrt{p}).$$

Далее, так как для любого вещественного α и $x\to\infty$ справедливо неравенство

$$\sum_{n\leqslant x}\frac{1-\cos(\alpha n)}{n}\leqslant\ln x+O(1),\qquad(**)$$

то

$$|T(N)|\leqslant\frac{\sqrt{p}}{\pi}\sum_{0<a\leqslant(p-1)/2}\frac{1-\cos 2\pi\frac{aN}{p}}{a}+O(\sqrt{p})\leqslant$$

$$\leqslant \frac{\sqrt{p}}{\pi} \ln p(1 + o(1)).$$

Таким образом,

$$S = \max_{N \geqslant 1} \leqslant \left(\frac{1}{\pi} + o(1) \right) \sqrt{p} \ln p.$$

Э. Ландау улучшил эти оценки в два раза. Приведем их вывод. Положим $p_1 = \sqrt{p} \ln p$. Разобьем промежуток суммирования на два: $0 < |a| \leqslant p_1$ и $p_1 < |a| \leqslant (p-1)/2$.

Представим модуль суммы $T(N)$ в следующем виде

$$|T(N)| = \frac{\sqrt{p}}{2\pi} |T_1(N) + T_2(N)| + O(\sqrt{p}),$$

где

$$T_1(N) = \sum_{0 < |a| \leqslant p_1} \left(\frac{a}{p} \right) \frac{e^{2\pi i \frac{aN}{p}} - 1}{a},$$

$$T_2(N) = \sum_{p_1 < |a| \leqslant (p-1)/2} \left(\frac{a}{p} \right) \frac{e^{2\pi i \frac{aN}{p}} - 1}{a}.$$

Рассуждения, аналогичные приведенным выше, дают для суммы $T_1(N)$ следующие выражения

$$T_1(N) = 2i \sum_{0 < |a| \leqslant p_1} \left(\frac{a}{p} \right) \frac{\sin 2\pi \frac{aN}{p}}{a},$$

если $\left(\frac{-1}{p} \right) = 1$;

$$T_1(N) = -2 \sum_{0 < |a| \leqslant p_1} \left(\frac{a}{p} \right) \frac{1 - \cos 2\pi \frac{aN}{p}}{a},$$

если $\left(\frac{-1}{p} \right) = -1$.

Пользуясь неравенствами $(*)$, $(**)$, получим

$$|T_1(N)| \leqslant \begin{cases} \frac{4}{\pi} \ln p_1 + O(1) = \frac{2}{\pi} \ln p(1 + o(1)), & \text{если} \quad \left(\frac{-1}{p} \right) = 1, \\ 2 \ln p_1 + O(1) = \ln p(1 + o(1)), & \text{если} \quad \left(\frac{-1}{p} \right) = -1, \end{cases}$$

Теперь оценим модуль суммы $T_2(N)$. Заметим, что при $1 \leqslant x \leqslant p$ и любом целом a неполная сумма Гаусса имеет оценку

$$\left| \sum_{n \leqslant x} \left(\frac{n}{p} \right) e^{2\pi i \frac{an}{p}} \right| \ll \sqrt{p} \ln p.$$

Используя формулу Абеля суммирования по целым числам промежутка, положив $f(x) = 1/x$, $C(x) = \sum_{n \leqslant x} c_n$, $c_n = \left(\frac{a}{p}\right)(e^{2\pi i \frac{aN}{p}} - 1)$, преобразуем сумму

$$T_2(N) = \sum_{p_1 < |a| \leqslant (p-1)/2} \left(\frac{a}{p}\right) \frac{e^{2\pi i \frac{aN}{p}} - 1}{a} =$$

$$= f\left(\frac{p-1}{2}\right) C\left(\frac{p-1}{2}\right) - \int\limits_{p_1}^{\frac{p-1}{2}} C(x) f'(x)\, dx.$$

Получим $T_2(N) \ll 1$. Таким образом, $|T(N)| \leqslant (c + o(1))\sqrt{p} \ln p$, где

$$c = \begin{cases} 1/\pi^2, & \text{если } \left(\frac{-1}{p}\right) = 1 \\ 1/(2\pi), & \text{если } \left(\frac{-1}{p}\right) = -1. \end{cases}$$

Тем самым, искомое неравенство доказано. ◁

38. Пусть $k \geqslant 1$ — натуральное число, $p_1, \ldots, p_k$ — различные простые числа, $Q = p_1 \ldots p_k$, $a_1, \ldots, a_k$ — целые числа, $Q \geqslant x \geqslant 1$ — вещественное число и

$$S(x) = \sum_{m \leqslant x} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right).$$

Тогда при $Q \to \infty$ имеем неравенство

$$|S(x)| \leqslant 2\pi^2 \sqrt{Q} \ln Q (1 + o(1)).$$

▷ Имеем

$$S(x) = \sum_{m \leqslant Q} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right) \sum_{n \leqslant x} \frac{1}{Q} \sum_{a=0}^{Q-1} e^{2\pi i a \frac{m-n}{Q}} =$$

$$= \frac{1}{Q} \sum_{a=0}^{Q-1} A(a) B(a),$$

где

$$A(a) = \sum_{m=1}^{Q} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right) e^{2\pi i a \frac{m}{Q}}, \quad B(a) = \sum_{n \leqslant x} e^{-2\pi i a \frac{n}{Q}}.$$

Преобразуем сумму $A(a)$. Для каждого $s = 1, \ldots, k$, положим $Q = p_s Q_s$. Тогда по китайской теореме об остатках для любого вычета m по модулю Q найдется единственный набор вычетов $(m_1, \ldots, m_k)$, $0 \leqslant m_1 < p_1, \ldots, 0 \leqslant m_k < p_k$, такой, что

$$m \equiv m_1 Q_1 + \cdots + m_k Q_k \pmod{Q}.$$

Отсюда имеем

$$A(a)=\prod_{s=1}^{k}A_s,\quad A_s=\sum_{m_s=0}^{p_s-1}\left(\frac{m_sQ_s+a_s}{p_s}\right)e^{-2\pi ia\frac{m_s}{p_s}}.$$

Определим Q'_s из сравнения $Q_sQ'_s\equiv 1\pmod{p_s}$ и обозначим символом $\tau(p)$ сумму Гаусса

$$\tau(p)=\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)e^{2\pi i\frac{m}{p}}.$$

Тогда сумму A_s можно представить в виде

$$A_s=e^{2\pi ia\frac{a_sQ'_s}{p_s}}\left(\frac{-aQ'_s}{p_s}\right)\tau_{p_s}.$$

Следовательно,

$$A(a)=\chi(a)\tau,\ \chi(a)=\prod_{s=1}^{k}e^{2\pi ia\frac{a_sQ'_s}{p_s}}\left(\frac{-aQ'_s}{p_s}\right),\ \tau=\prod_{s=1}^{k}\tau_{p_s},\ |\tau|=\sqrt{Q}.$$

Таким образом, сумма $S(x)$ примет вид

$$S(x)=\frac{\tau}{Q}\sum_{0<|a|<Q/2}\chi(a)B(a)=\frac{\tau}{Q}\sum_{0<|a|<Q/2}\chi(a)\frac{e^{2\pi ia\frac{x}{Q}}-1}{1-e^{2\pi i\frac{a}{Q}}}.$$

Пользуясь асимптотическим разложением при $0<|a|<Q/2$ и $Q\to\infty$ для дроби вида

$$\frac{1}{1-e^{2\pi i\frac{a}{Q}}}=-\frac{Q}{2\pi ia}+O(1),$$

получим

$$|S(x)|\leqslant\frac{\sqrt{Q}}{2\pi}\left|\sum_{0<|a|<Q/2}\chi(a)\frac{e^{-2\pi ia\frac{x}{Q}}-1}{a}\right|+O(\sqrt{Q}).$$

Отсюда имеем

$$|S(x)|\leqslant\frac{\sqrt{Q}}{\pi}\sum_{0<a<Q/2}\frac{|\sin\pi a\frac{x}{Q}|}{a}+O(\sqrt{Q}).$$

Воспользовавшись неравенством $(*)$ из предыдущей задачи, находим

$$|S(x)|\leqslant\frac{2}{\pi^2}\sqrt{Q}\ln Q(1+o(1)).$$

Таким образом искомая оценка доказана. ◁

§ 2. Извлечение квадратного корня из числа по простому модулю

1. Пусть $p \equiv 3 \pmod 4$. Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(p+1)/4} \pmod p.$$

▷ По критерию Эйлера разрешимость сравнения $x^2 \equiv a \pmod p$, $(a, p) = 1$, эквивалентна выполнению сравнения $a^{(p-1)/2} \equiv 1 \pmod p$. Отсюда получим

$$a^{2(p+1)/4} \equiv a^{(p+1)/2} \equiv a \pmod p.$$

Следовательно, искомое решение сравнения имеет вид $x \equiv \pm a^{(p+1)/4} \pmod p$. ◁

2. Пусть $p \equiv 5 \pmod 8$. Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(p+3)/8} 2^{(p-1)s/4} \pmod p,$$

где

$$s = \begin{cases} 0, & \text{при } a^{(p-1)/4} \equiv 1 \pmod p, \\ 1, & \text{при } a^{(p-1)/4} \equiv -1 \pmod p. \end{cases}$$

▷ По критерию Эйлера имеем $a^{(p-1)/2} \equiv 1 \pmod p$. Отсюда получим $a^{(p-1)/4} \equiv \pm 1 \pmod p$. Если $a^{(p-1)/4} \equiv 1 \pmod p$, то

$$a^{2(p+3)/8} \equiv a^{(p+3)/4} \equiv a \pmod p.$$

Тогда в этом случае искомое решение имеет вид $x \equiv \pm a^{(p+3)/8} \pmod p$.

Пусть теперь $a^{(p-1)/4} \equiv -1 \pmod p$. Поскольку 2 — квадратичный невычет по модулю p, по критерию Эйлера имеем $2^{(p-1)/2} \equiv -1 \pmod p$. Следовательно,

$$\left(2^{(p-1)/4} a^{(p+3)/8}\right)^2 \equiv 2^{(p-1)/2} a^{(p+3)/4} \equiv a \pmod p.$$

Таким образом, в этом случае искомое решение представляется в виде

$$x \equiv \pm 2^{(p-1)/4} a^{(p+3)/8} \pmod p.$$ ◁

3. Пусть $p \equiv 1 \pmod 8$, N — квадратичный невычет по модулю p и $p = 2^k h + 1$, $k \geqslant 3$, $(h, 2) = 1$. Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(h+1)/2} N^{(hu_{k-1})/2} \pmod p,$$

где $u_0 = 0$; $u_r = 2^{k-1}s_r + \frac{u_{r-1}}{2}$, $1 \leqslant r \leqslant k-1$;

$$s_r = \begin{cases} 0, & \text{при } a^{2^{k-r-1}h} N^{(hu_{r-1})/2} \equiv 1 \pmod p, \\ 1, & \text{при } a^{2^{k-r-1}h} N^{(hu_{r-1})/2} \equiv -1 \pmod p. \end{cases}$$

▷ По критерию Эйлера имеем

$$a^{(p-1)/2} \equiv 1 \pmod p, N^{(p-1)/2} \equiv 1 \pmod p.$$

Таким образом $a^{2^{k-1}h} \equiv 1 \pmod p$. Извлекаем из $a^{2^{k-1}h}$ квадратные корни до тех пор, пока не получим сравнение $a^{2^{k_1}h} \equiv -1 \pmod p$, $0 \leqslant k_1 < k$ или сравнение $a^h \equiv 1 \pmod p$. В первом случае перейдем к сравнению $N^{2^{k_0}h} a^{2^{k_1}h} \equiv 1 \pmod p$, $k_0 = k-1$ и повторим процедуру извлечения квадратных корней из выражения $N^{2^{k_0}h} a^{2^{k_1}h}$ до тех пор, пока не приходим либо к сравнению $N^{2^{k_0-k_1+k_2}h} a^{2^{k_2}h} \equiv -1 \pmod p$, либо к сравнению $N^{2^{k_0-k_1}h} a^h \equiv 1 \pmod p$ и т.д. Наконец, при некотором s имеем либо

$$N^{2^{sk_0-k_s}h} a^h \equiv 1 \pmod p,$$

либо

$$N^{2^{(s+1)k_0-k_s}h} a^h \equiv 1 \pmod p,$$

Таким образом, при некотором $m > 0$ получим

$$\left(N^{2^{m-1}h} a^{(h+1)/2}\right)^2 \equiv N^{2^m h} a^{h+1} \equiv a \pmod p.$$

Отсюда находим искомое решение сравнения $x^2 \equiv a \pmod p$. Имеем

$$x \equiv \pm N^{2^{m-1}h} a^{(h+1)/2} \pmod p. \qquad \triangleleft$$

§ 3. Символ Якоби

Пусть P — нечетное число, $P > 1$, и $P = p_1 p_2 \dots p_r$ — разложение его на простые сомножители (среди них могут быть и равные). Пусть, далее, $(a, P) = 1$. Тогда *символ Якоби* $\left(\frac{a}{P}\right)$ определяется следующим равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right).$$

1. Пусть P — нечетное число, $P > 1, (a, P) = 1$ и $a \equiv a_1 \pmod P$. Тогда имеем

$$\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right).$$

▷ Поскольку для символа Лежандра для нечетного простого числа p и при $(a,p)=1$, $a \equiv a_1 \pmod p$ справедливо справедливо равенство

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right),$$

по определению символа Якоби имеет место искомое равенство. ◁

2. Пусть P_1, P_2 — нечетные числа. Тогда имеем

$$P_1P_2 - 1 \equiv (P_1-1) + (P_2-1) \pmod 4,$$
$$P_1^2P_2^2 - 1 \equiv (P_1^2-1) + (P_2^2-1) \pmod{64}.$$

▷ Поскольку

$$P_1P_2 - P_1 - P_2 + 1 \equiv (P_1-1)(P_2-1) \equiv 0 \pmod 4,$$
$$P_1^2P_2^2 - P_1^2 - P_2^2 + 1 \equiv (P_1^2-1)(P_2^2-1) \equiv 0 \pmod{64},$$

искомые сравнения имеют место. ◁

3. При нечетном $P > 1$ справедливы следующие соотношения:

1) $\left(\frac{1}{P}\right) = 1$;

2) при $(a,P) = (b,P) = 1$ имеем $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$,

3) $\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)$;

4) при $(a,P) = (a,Q) = 1$, $(P,2) = (Q,2) = 1$ имеем

$$\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right);$$

5) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$;

6) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$;

7) при $(P,2) = (Q,2) = 1$, $(P,Q) = 1$ имеем

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

▷ Равенства 1) – 4) прямо следуют из определения символа Якоби.

Равенства 5) и 6) докажем методом математической индукции по параметру P. При $P = 3$ они имеют место. Предположим они справедливы при $P < Q$, где Q — нечетное число. Докажем, что они верны при $P = Q$. Если Q — простое число, то искомые равенства следуют из квадратичного закона взаимности для символа Лежандра. Если же Q — составное число, то его можно представить в виде $Q = Q_1Q_2, 1 < Q_1, Q_2 < Q$. Далее, имеем цепочку равенств

$$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{Q_1}\right)\left(\frac{-1}{Q_2}\right) = (-1)^{\frac{Q_1-1}{2}+\frac{Q_2-1}{2}} = (-1)^{\frac{Q_1Q_2-1}{2}} = (-1)^{\frac{Q-1}{2}}.$$

Утверждение 7) докажем по индукции по двум параметрам P и Q. Оно верно при $P = 3$ и любом нечетном $Q > 3$, а также при $Q = 3$ и любом нечетном $P > 3$. Докажем утверждение при $P = 3$. Если Q — простое число, то оно справедливо по квадратичному закону взаимности для символа Лежандра. Пусть Q — составное число. Тогда его можно представить в виде $Q = Q_1Q_2$, $1 < Q_1, Q_2 < Q$. По предположению индукции и утверждениям 2), 4) имеем

$$\left(\frac{Q}{3}\right) = \left(\frac{Q_1}{3}\right)\left(\frac{Q_2}{3}\right) = (-1)^{\frac{Q_1-1}{2}}\left(\frac{3}{Q_1}\right)(-1)^{\frac{Q_2-1}{2}}\left(\frac{3}{Q_2}\right) = \\ = (-1)^{\frac{Q-1}{2}}\left(\frac{3}{Q}\right).$$

Предположим, что при всех неравных между собой нечетных P, Q, с условиями либо $P < P_0, Q \leqslant Q_0$, либо $P \leqslant P_0, Q < Q_0$, где P_0, Q_0 — нечетные числа, справедливо равенство

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Докажем это утверждение при $P = P_0$ и $Q = Q_0$. Если P_0, Q_0 — простые числа, то утверждение следует из квадратичного закона взаимности для символа Лежандра. Пусть, теперь, хотя бы одно из чисел P_0, Q_0 является составным. Для определенности, пусть P_0 — составное число. Тогда $P_0 = P_1P_2, 1 < P_1, P_2 < P_0$. По свойству 4) мультипликативности символа Якоби и по предположению индукции имеем

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{P_1}\right)\left(\frac{Q}{P_2}\right) = (-1)^{\frac{P_1-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P_1}{Q}\right)(-1)^{\frac{P_2-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P_2}{Q}\right) = \\ = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

◁

4. Пусть P и Q — нечетные взаимно простые числа. Тогда имеем

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \begin{cases} -(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}, & \text{если } P < 0,\ Q < 0; \\ (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}, & \text{в противном случае.} \end{cases}$$

▷ При $P > 0$, $Q > 0$ искомая формула получена в предыдущей задаче.

Пусть $P < 0$, $Q < 0$. Тогда имеем

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \left(\frac{-|P|}{|Q|}\right)\left(\frac{-|Q|}{|P|}\right) = \left(\frac{|P|}{|Q|}\right)\left(\frac{|Q|}{|P|}\right)\left(\frac{-1}{|Q|}\right)\left(\frac{-1}{|P|}\right) = \\ = (-1)^{\frac{|P|-1}{2}\frac{|Q|-1}{2}+\frac{|P|-1}{2}+\frac{|Q|-1}{2}} = -(-1)^{\left(\frac{|P|-1}{2}+1\right)\left(\frac{|Q|-1}{2}+1\right)} =$$

$$= -(-1)^{\frac{|P|+1}{2}\frac{|Q|+1}{2}} = -(-1)^{\frac{-P+1}{2}\frac{-Q+1}{2}} = -(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Пусть, теперь, числа P и Q имеют разные знаки. Для определенности положим $P > 0$, $Q < 0$. Тогда, используя предыдущую задачу, находим

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \left(\frac{P}{|Q|}\right)\left(\frac{-|Q|}{P}\right) = \left(\frac{P}{|Q|}\right)\left(\frac{|Q|}{P}\right)\left(\frac{-1}{P}\right) =$$

$$= (-1)^{\frac{P-1}{2}\frac{|Q|-1}{2}+\frac{P-1}{2}} = (-1)^{\frac{P-1}{2}\frac{|Q|+1}{2}} = (-1)^{\frac{P-1}{2}\frac{-Q+1}{2}} = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.\triangleleft$$

5. При $n > 1$ имеем $\left(\frac{n}{4n-1}\right) = 1, \left(\frac{-n}{4n-1}\right) = -1$.

▷ Имеем

$$\left(\frac{n}{4n-1}\right) = \left(\frac{4n}{4n-1}\right) = \left(\frac{1}{4n-1}\right) = 1,$$

$$\left(\frac{-n}{4n-1}\right) = \left(\frac{-4n}{4n-1}\right) = \left(\frac{-1}{4n-1}\right)\left(\frac{4n}{4n-1}\right) = -1. \qquad \triangleleft$$

§ 4. Извлечение квадратного корня из числа по составному модулю

1. Пусть $\alpha > 0$ — натуральное число, $(a, p) = 1$. Тогда $T = T(p^\alpha)$ — число решений сравнения

$$x^2 \equiv a \pmod{p^\alpha} \tag{2}$$

равно следующему значению

$$T(2^\alpha) = \begin{cases} 1, & \text{если } \alpha = 1, \\ 0, & \text{если } \alpha = 2,\ a \equiv 3 \pmod 4, \\ 2, & \text{если } \alpha = 2,\ a \equiv 1 \pmod 4, \\ 0, & \text{если } \alpha > 2,\ a \not\equiv 1 \pmod 8, \\ 4, & \text{если } \alpha > 2,\ a \equiv 1 \pmod 8; \end{cases}$$

$$T(p^\alpha) = 1 + \left(\frac{a}{p}\right), \text{ если } p > 2.$$

▷ Пусть $p = 2$. Тогда при $\alpha = 1$ сравнение (2) принимает вид $x^2 \equiv 1 \pmod 2$ и $T(2) = 1$. Если $\alpha = 2$, $a \equiv 3 \pmod 4$, то сравнение (2) имеет вид $x^2 \equiv 3 \pmod 4$ и оно не имеет решений. Если же $\alpha = 2$, $a \equiv 1 \pmod 4$, то (2) имеет 2 решения $x \equiv \pm 1 \pmod 4$. Если нечетное a не сравнимо с единицей по модулю 8, то сравнение (2) по модулю 8 не имеет решений, следовательно и по модулю 2^α, $\alpha \geqslant 3$, оно не имеет решений.

Пусть, теперь, $\alpha > 2$, $a \equiv 1 \pmod 8$. Для каждого нечетного числа x, $0 < x < 2^\alpha$, найдется число b, $0 < b < 2^\alpha$, $b \equiv 1 \pmod 8$, такое, что

$$x^2 \equiv b \pmod{2^\alpha}.$$

Пусть нечетное x_0 решение предыдущего сравнения. Найдем количество всех его решений. Для любого другого решения x имеем

$$x^2 \equiv x_0^2 \pmod 2^\alpha,$$

т.е. $2^\alpha \mid (x - x_0)(x + x_0)$. Отсюда получим

$$2^{\alpha-2} \mid \frac{x - x_0}{2} \cdot \frac{x + x_0}{2},$$

поскольку числа x и x_0 — нечетные. Число не может одновременно делить числа $\frac{x-x_0}{2}$ и $\frac{x+x_0}{2}$. Следовательно, выполняется сравнение

$$x \equiv \pm x_0 \pmod{2^{\alpha-1}}.$$

Среди чисел $0 < x < 2^\alpha$ этому сравнению удовлетворяют точно четыре различных числа, т.е. если $T(b) \neq 0$, то $T(b) = 4$.

Таким образом, имеем

$$\sum_{\substack{b=1 \\ b \equiv 1 (\mathrm{mod}\ 8)}}^{2^\alpha} T(b) = 2^{\alpha-1}.$$

Значит, количество различных чисел b, для которых $T(b) \neq 0$, равно $2^{\alpha-3}$. Это в точности те числа, которые удовлетворяют условиям $b, 0 < b < 2^\alpha, b \equiv 1 \pmod 8$. Последнее и доказывает, что $T(2^\alpha) = 4$ при $\alpha > 2, a \equiv 1 \pmod 8$.

Пусть $p \geqslant 3$. Возможны две ситуации:

$$\text{a)}\ \left(\frac{a}{p}\right) = -1 \text{ и b)}\ \left(\frac{a}{p}\right) = 1.$$

В случае a) сравнение $x^2 \equiv a \pmod p$ не имеет решений. Следовательно

$$T(p^\alpha) = 0 = 1 + \left(\frac{a}{p}\right).$$

Рассмотрим случай b). Сравнение $x^2 \equiv a \pmod p$ имеет два решения $x \equiv \pm x_0 \pmod p$. Предположим, что x_α решение сравнения $x_\alpha^2 \equiv a \pmod{p^\alpha}$. Найдем $x_{\alpha+1} \equiv x_\alpha \pmod{p^\alpha}$ и $x_{\alpha+1}^2 \equiv a \pmod{p^{\alpha+1}}$. Положим $x_{\alpha+1} = x_\alpha + p^\alpha y, 0 \leqslant y < p$. Имеем

$$(x_\alpha + p^\alpha y)^2 \equiv a \pmod{p^{\alpha+1}}.$$

Следовательно, при $\alpha > 0$ получим

$$2x_\alpha y \equiv a_1 \pmod{p}, a_1 = p^{-\alpha}(a - x_\alpha^2).$$

Поскольку $(2x_\alpha, p) = 1$, последнее сравнение имеет единственное решение.

Таким образом, сравнение $x^2 \equiv a \pmod{p^\alpha}$ имеет два решения, и поэтому всегда справедливо равенство

$$T(p^\alpha) = 1 + \left(\frac{a}{p}\right). \qquad \triangleleft$$

2. Пусть a, m — натуральное число, $(a, m) = 1$. Тогда $T = T(m)$ — число решений сравнения

$$x^2 \equiv a \pmod{m} \tag{3}$$

равно

$$T(m) = \begin{cases} 0, & \text{если } 4 \parallel m,\ a \not\equiv 1 \pmod 4, \\ 0, & \text{если } 8 \mid m,\ a \not\equiv 1 \pmod 8, \\ 0, & \text{если } \exists p \mid m,\ p > 2,\ \left(\frac{a}{p}\right) = -1. \end{cases}$$

Пусть, далее, каноническое разложение на простые сомножители числа m имеет вид $m = 2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k}, (a, m) = 1$ и k обозначает количество нечетных простых делителей числа m. Пусть, наконец, выполнены следующие необходимые условия разрешимости сравнения $x^2 \equiv a \pmod{m}$:

$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2,\ a \equiv 1 \pmod 8 \text{ при } \alpha \geqslant 3,$$

$$\left(\frac{a}{p_1}\right) = 1, \quad \left(\frac{a}{p_2}\right) = 1, \quad \dots, \quad \left(\frac{a}{p_k}\right) = 1.$$

Тогда количество решений $T(m)$ этого сравнения равно

$$T(m) = \begin{cases} 2^k, & \text{если } 4 \not\mid m, \\ 2^{k+1}, & \text{если } 4 \parallel m, \\ 2^{k+2}, & \text{если } 8 \mid m. \end{cases}$$

▷ Функция $T(m)$ — мультипликативная, т.е.

$$T(m) = T(2^\alpha) T(p_1^{\alpha_1}) \dots T(p_k^{\alpha_k}).$$

Отсюда, используя утверждение предыдущей задачи, получим искомое утверждение. $\triangleleft$

3. Пусть $V(n)$ — число решений сравнения $\omega^2 \equiv -1 \pmod n$ и каноническое разложение на простые сомножители числа n имеет

вид $n = 2^{\alpha} p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Тогда $V(n)$ равно

$$V(n) = \begin{cases} 0, & \text{если либо } 4 \mid n, \text{ либо } \exists p \mid n,\ p \equiv 3 \pmod 4, \\ 2^k, & \text{если } 4 \nmid n,\ \forall p \mid n,\ p \equiv 1 \pmod 4. \end{cases}$$

▷ Поскольку

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 4, \\ -1, & \text{если } p \equiv -1 \pmod 4, \end{cases}$$

искомое утверждение следует из утверждения предыдущей задачи.◁

4. Пусть n — натуральное число, $n > 1$, и пусть ω — решение сравнения $\omega^2 \equiv -1 \pmod n$. Тогда существует единственное представление числа n в виде $n = x^2 + y^2$, где x, y — взаимно простые числа и $y \equiv \omega x \pmod n$.

▷ Дробь $\frac{\omega}{n}$ — несократимая, так как вычет ω является решением сравнения $\omega^2 \equiv -1 \pmod n$. По лемме Дирихле при $\tau = \sqrt{n}$ и $\alpha = \frac{\omega}{n}$ существует несократимая дробь a/b со знаменателем b, не превосходящем $\sqrt{n}$, такая, что

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}.$$

Положим $\omega b - na = c$. Имеем $\omega b \equiv c \pmod n$. Из леммы Дирихле получим $0 < |c| < \sqrt{n}, 0 < b \leqslant \sqrt{n}$. Следовательно,

$$0 < b^2 + c^2 < 2n.$$

Кроме того, справедливы сравнения

$$b^2 + c^2 \equiv b^2 + \omega^2 b^2 \equiv (1 + \omega^2) b^2 \equiv 0 \pmod n.$$

Таким образом имеем равенство $b^2 + c^2 = n$.

Докажем, что числа b и c взаимно просты. Имеем цепочку равенств

$$n = b^2 + (\omega b - na)^2 = (1 + \omega^2) b^2 - 2\omega n b a + n^2 a^2,$$

$$1 = \frac{1 + \omega^2}{n} b^2 - \omega b a - \omega b a + n a^2 = db - ac.$$

Равенство $db - ac = 1$ и доказывает, что $(b, c) = 1$. Если $c > 0$, то искомое решение имеет вид $x = b, y = c$. Если же $c < 0$, то следует положить $x = -c, y = b$. Действительно,

$$n = (-c)^2 + b^2, \quad -c > 0, \quad b > 0, \quad (-c, b) = 1,$$

$$b \equiv -\omega^2 b \equiv -\omega c \equiv \omega(-c) \pmod n.$$

Докажем единственность решения (x, y). Предположим, что (x_1, y_1) — другое решение, удовлетворяющее условию задачи. Имеем

цепочку соотношений

$$n^2 = (x^2+y^2)(x_1^2+y_1^2) = (xx_1+yy_1)^2 + (xy_1-yx_1)^2,$$
$$xx_1+yy_1 \equiv xx_1+\omega x\omega x_1 \equiv (1+\omega^2)xx_1 \equiv 0 \pmod{n},$$
$$xx_1+yy_1 > 0, xx_1+yy_1 = n, xy_1-yx_1 = 0,$$
$$xn = x(xx_1+yy_1) - y(xy_1-yx_1) = x_1(x^2+y^2) = x_1 n.$$

Следовательно, $x = x_1$, $y = y_1$. ◁

5. Пусть $m > 1$. Тогда число представлений числа m в виде

$$m = x^2+y^2, \quad (x,y) = 1,$$

где x, y — целые числа, равно учетверенному числу решений сравнения

$$z^2+1 \equiv 0 \pmod{m}.$$

▷ Так как $(x,y) = 1$, то $x \neq 0$, $y \neq 0$, $x \neq y$. Далее, вместе с решением (x,y) уравнения $x^2+y^2 = m$ решениями его являются $\pm x$, $\pm y$. Следовательно, решению (x,y), $x > 0$, $y > 0$, отвечают четыре решения.

По предыдущей задаче для каждого ω, удовлетворяющего сравнению $\omega^2 \equiv -1 \pmod{m}$, существует единственное решение уравнения $x^2+y^2 = m$, для которого $(x,y) = 1$, $x > 0$, $y > 0$, $y \equiv \omega x \pmod{m}$.

Пусть, теперь, (x,y) решение уравнения $x^2+y^2 = m$, $(x,y) = 1$, $x > 0$, $y > 0$. Тогда имеем $(x,m) = 1$ и существует единственное ω, удовлетворяющее сравнению $y \equiv \omega x \pmod{m}$. Кроме того, имеет место цепочка сравнений

$$0 \equiv m \equiv x^2+y^2 \equiv x^2+\omega^2x^2 \equiv (1+\omega^2)x^2 \pmod{m},$$
$$1+\omega^2 \equiv 0 \pmod{m}.$$

Таким образом, каждому решению уравнения поставлено во взаимно однозначное соответствие решение сравнения $1+\omega^2 \equiv 0 \pmod{m}$. ◁

6. Пусть $m \geqslant 1$ и $U(m)$ — число представлений числа m в виде

$$m = x^2+y^2,$$

где x, y — целые числа. Тогда $U(n)$ равно

$$U(m) = 4\sum_{d^2|m} V(m/d^2),$$

где $V(n)$ — число решений сравнения

$$z^2+1 \equiv 0 \pmod{n}.$$

▷ Все решения уравнения $x^2 + y^2 = m$, имеющие d наибольшим общим делителем чисел x и y соберем вместе. Получим

$$m/d^2 = x_1^2 + y_1^2, x_1 = x/d^2, y_1 = y/d^2, (x_1, y_1) = 1.$$

Следовательно, используя утверждение предыдущей задачи, получим искомую формулу. ◁

7. Функции $V(n)$, $U(n)/4$, $W(n) = \sum\limits_{d|n} \chi_4(d)$, где $\chi_4(m)$ — неглавный характер Дирихле по модулю 4,

$$\chi_4(m) = \begin{cases} 0, & \text{если } m \equiv 0 \pmod 4, \\ 1, & \text{если } m \equiv 1 \pmod 4, \\ -1, & \text{если } m \equiv 3 \pmod 4, \end{cases}$$

являются мультипликативными.

▷ Мультипликативность функции $V(m)$ следует из китайской теоремы об остатках. Далее, пусть $m = m_1 m_2, (m_1, m_2) = 1$. Тогда

$$U(m_1 m_2)/4 = \sum_{d^2 | m_1 m_2} V(m_1 m_2/d^2) =$$

$$= \sum_{d_1^2 | m_1} V(m_1/d^2) \sum_{d_2^2 | m_2} V(m_2/d^2) = U(m_1)/4 \cdot U(m_2)/4,$$

где $d_1 \mid m_1$, $d_2 \mid m_2$, $d = d_1 d_2$. Таким образом, функция $U(m)/4$ является мультипликативной.

Наконец, при $(m_1, m_2) = 1$ имеем

$$W(m_1 m_2) = \sum_{d | m_1 m_2} \chi_4(d) = \sum_{d_1 | m_1} \chi_4(d_1) \sum_{d_2 | m_2} \chi_4(d_2) = W(m_1) W(m_2).$$

◁

8. Справедливо равенство

$$U(m) = 4 \sum_{d|m} \chi_4(d).$$

▷ В силу мультипликативности функций в правой и левой частях равенств достаточно проверить равенство при $m = p^\alpha$. Имеем

$$W(p^\alpha) = \sum_{0 \leqslant \beta \leqslant \alpha} \chi_4(p^\beta) = \begin{cases} 1, & \text{если } p = 2, \\ \alpha + 1, & \text{если } p \equiv 1 \pmod 4, \\ 1, & \text{если } p \equiv 3 \pmod 4,\ 2 \mid \alpha, \\ 0, & \text{если } p \equiv 3 \pmod 4,\ 2 \nmid \alpha. \end{cases}$$

Далее, справедливы соотношения

$$V(p^m)=\begin{cases}1, & \text{если} \quad p=2, m=1,\\ 0, & \text{если} \quad p=2, m>1,\\ 0, & \text{если} \quad p\equiv 3 \pmod 4,\ m\geqslant 1,\\ 2, & \text{если} \quad p\equiv 1 \pmod 4,\ m\geqslant 1.\end{cases}$$

Следовательно, при четном α получим

$$U(p^\alpha)/4=V(p^\alpha)+V(p^{\alpha-2})+\cdots+V(p^2)+V(1)=$$

$$=\begin{cases}1, & \text{если} \quad p=2,\\ 2\cdot\alpha/2+1=\alpha+1, & \text{если} \quad p\equiv 1 \pmod 4,\\ 1, & \text{если} \quad p\equiv 3 \pmod 4,\end{cases}$$

и при нечетном α имеем

$$U(p^\alpha)/4=V(p^\alpha)+V(p^{\alpha-2})+\cdots+V(p)=$$

$$=\begin{cases}1, & \text{если} \quad p=2,\\ 2\cdot(\alpha+1)/2=\alpha+1, & \text{если} \quad p\equiv 1 \pmod 4,\\ 0, & \text{если} \quad p\equiv 3 \pmod 4.\end{cases}$$

Отсюда следует искомое равенство. ◁

§ 5. Целая часть квадратного корня из натурального числа

1. Пусть a — фиксированное положительное число, x_1 — любое положительное число и последовательность $\{x_n\}$ при $n\geqslant 1$ задана следующей итерационной формулой Герона

$$x_{n+1}=\frac{1}{2}\left(x_n+\frac{a}{x_n}\right).$$

Тогда имеем:

1) при $n\geqslant 2$ последовательность x_n ограничена снизу числом $\sqrt{a}$;

2) последовательность x_n — невозрастающая;

3) $\lim\limits_{n\to\infty} x_n=\sqrt{a}$;

4) $\frac{x_{n+1}-\sqrt{a}}{x_{n+1}+\sqrt{a}}=\left(\frac{x_n-\sqrt{a}}{x_n+\sqrt{a}}\right)^2$;

5) $\Delta_n:=x_n-\sqrt{a}=\frac{2q^{2^{n-1}}}{1-q^{2^{n-1}}}\sqrt{a}\to 0$ при $n\to\infty$, где $q=\frac{x_1-\sqrt{a}}{x_1+\sqrt{a}}$.

▷ 1) При $n\geqslant 2$ имеем

$$x_n-\sqrt{a}=\frac{1}{2}\left(x_{n-1}+\frac{a}{x_{n-1}}\right)-\sqrt{a}=\frac{(x_{n-1}-\sqrt{a})^2}{2x_{n-1}}\geqslant 0.$$

2) Используя утверждение 1), при $n \geqslant 1$ находим

$$x_n - x_{n+1} = x_n - \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) = \frac{x_n^2 - a}{2x_n} \geqslant 0.$$

3) Из утверждений 1) и 2) имеем, что последовательность x_n, $n \geqslant 2$, ограничена снизу числом $\sqrt{a}$ и является невозрастающей. По теореме Вейерштраса она имеет предел, равный $x \geqslant \sqrt{a} > 0$. Следовательно, справедливо равенство

$$\lim_{n\to\infty} x_{n+1} = \frac{1}{2}\left(\lim_{n\to\infty} x_n + \frac{a}{\lim\limits_{n\to\infty} x_n}\right),$$

т.е. $x = (x + a/x)/2$, $x = \sqrt{a}$.

4) Справедливо равенство

$$x_{n+1} \pm \sqrt{a} = \frac{(x_n \pm \sqrt{a})^2}{2x_n}.$$

Следовательно,

$$\frac{x_{n+1} - \sqrt{a}}{x_{n+1} + \sqrt{a}} = \left(\frac{x_n - \sqrt{a}}{x_n + \sqrt{a}}\right)^2.$$

5) Полагая $\frac{x_1 - \sqrt{a}}{x_1 + \sqrt{a}} = q$, из предыдущего утверждения находим цепочку соотношений

$$\frac{x_n - \sqrt{a}}{x_n + \sqrt{a}} = q^{2^{n-1}}, \quad x_n = \frac{1 + q^{2^{n-1}}}{1 - q^{2^{n-1}}}.$$

Таким образом, поскольку $|q| < 1$, имеем

$$\Delta_n := x_n - \sqrt{a} = \frac{2q^{2^{n-1}}}{1 - q^{2^{n-1}}}\sqrt{a} \to 0$$

при $n \to \infty$. ◁

2. Пусть n — натуральное число, $s_1 = \left[\frac{n+1}{2}\right]$ и последовательность $\{s_k\}$ при $k \geqslant 1$ задана следующей итерационной формулой

$$s_{k+1} = \left[\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right].$$

Тогда имеем:

1) если $y \geqslant x$, то $[y] \geqslant [x]$;

2) $[(n+1)/2] \geqslant [\sqrt{n}]$;

3) при $k \geqslant 2$ справедливо неравенство $s_k \geqslant [\sqrt{n}]$;

4) если справедливо неравенство $s_k > [\sqrt{n}]$, то $s_k > s_{k+1}$;

5) найдется натуральное m такое, что $s_m = [\sqrt{n}]$.

▷ 1) От противного. Предположим, что $[y] < [x]$. Тогда имеем цепочку неравенств

$$[y] + 1 \leqslant [x], y < [y] + 1 \leqslant [x] \leqslant x, y < x.$$

Последнее противоречит неравенству $y \geqslant x$, имеющему место по условию.

2) Справедливо неравенство $\frac{n+1}{2} \geqslant \sqrt{n}$. Следовательно, по утверждению 1) имеем $\left[\frac{n+1}{2}\right] \geqslant [\sqrt{n}]$.

3) Имеем неравенство $\frac{1}{2}\left(s_{k-1} + \frac{n}{s_{k-1}}\right) \geqslant \sqrt{n}$. Следовательно, по утверждению 1) находим

$$s_k = \left[\frac{1}{2}\left(s_{k-1} + \frac{n}{s_{k-1}}\right)\right] \geqslant [\sqrt{n}].$$

4) От противного. Предположим, что $s_k \leqslant s_{k+1}$. Тогда имеем цепочку равносильных неравенств

$$\left[\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right] \geqslant s_k, \quad \frac{1}{2}\left(s_k + \frac{n}{s_k}\right) - \left\{\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right\} \geqslant s_k.$$

Следовательно,

$$\frac{1}{2}\left(\frac{n}{s_{k-1}} - s_k\right) \geqslant \left\{\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right\} \geqslant 0.$$

С другой стороны, по условию задачи имеет место следующая цепочка неравенств

$$s_k > [\sqrt{n}],\ s_k \geqslant [\sqrt{n}] + 1 > \sqrt{n},\ s_k > \sqrt{n},\ s_k^2 > n,\ \frac{1}{2}\left(\frac{n}{s_k} - s_k\right) < 0.$$

Последнее неравенство противоречит полученному выше. Следовательно, сделанное выше предположение неверно.

5) По утверждениям 2) и 3) для любого натурального числа k выполняется неравенство $s_k \geqslant \sqrt{n}$. Далее, по утверждению 4), если бы всегда выполнялось строгое неравенство $s_k > \sqrt{n}$, то бесконечная последовательность натуральных чисел $\{s_k\}$ была бы монотонно убывающей. Следовательно, существует натуральное m такое, что $s_m = \sqrt{n}$. ◁

§ 6. Символ Кронекера

Пусть $d \equiv 0$ или $1 \pmod 4$, и пусть d отлично от точного квадрата, т.е. $d = 5, 8, 13, 17, 20, 21, \ldots$ или $-3, -4, -7, -8, \ldots$.

При $p \mid d$ положим $\left(\frac{d}{p}\right) = 0$.

При $p \nmid d$ положим

$$\left(\frac{d}{p}\right) = \begin{cases} \left(\frac{2}{|d|}\right) \text{ символ Якоби}, & \text{если } p = 2, \\ \left(\frac{d}{p}\right) \text{ символ Лежандра}, & \text{если } p > 2. \end{cases}$$

Пусть, также, m — натуральное число, $m = p_1 p_2 \dots p_r$ — его разложение на простые сомножители. Тогда *символ Кронекера* $\left(\frac{d}{m}\right)$ определяется следующим равенством

$$\left(\frac{d}{m}\right) = \left(\frac{d}{p_1}\right)\left(\frac{d}{p_2}\right)\dots\left(\frac{d}{p_r}\right).$$

Положим также $\left(\frac{d}{1}\right) = 1$.

1. Пусть $d \equiv 0$ или $1 \pmod 4$, и пусть d отлично от точного квадрата. Пусть, также, m — нечетное положительное число. Тогда значения символов Якоби и Кронекера $\left(\frac{d}{m}\right)$ совпадают.

▷ Утверждение задачи прямо следует из определений символов Якоби и Кронекера. ◁

2. Пусть $m_1 > 0$ и $m_2 > 0$. Тогда имеем $\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$.

▷ Утверждение прямое следствие определения символа Кронекера. ◁

3. Пусть m — натуральное число, $(d, m) = 1$. Тогда $R = R(4m)$ — число решений сравнения $x^2 \equiv d \pmod{4m}$ равно

$$R(4m) = 2 \sum_{r|d}{}' \left(\frac{d}{r}\right),$$

где штрих в знаке суммирования означает, что r пробегает бесквадратные значения.

▷ Рассмотрим сначала случай нечетного числа d, т.е. $d \equiv 1 \pmod 4$. Имеем $(d, 4m) = 1$. Пусть $4m = \prod\limits_{p|4m} p^{l_p}$ — каноническое разложение числа $4m$ на простые сомножители. Тогда число $R(4m)$ решений сравнения $x^2 \equiv d \pmod{4m}$ равно

$$R(4m) = \prod_{p|4m} R(p^{l_p}).$$

По утверждению 1 § 4 имеем

$$R(2^l) = \begin{cases} 2, & \text{если} \quad l = 2, \\ 2\left(1 + \left(\frac{d}{2}\right)\right), & \text{если} \quad l \geqslant 3. \end{cases}$$

Кроме того, при $p \geqslant 3$ по тому же утверждению получим $R(p^l) = 1 + \left(\frac{d}{p}\right)$.

Таким образом, находим

$$R(4m) = 2\prod_{p|m}\left(1+\left(\frac{d}{p}\right)\right) = 2\sum_{r|d}{}'\left(\frac{d}{r}\right).$$

Это и есть искомая формула.

Пусть, теперь, d будет четным числом. Тогда $d \equiv 0 \pmod 4$. Поскольку $(d,m)=1$, число m будет нечетным. Сравнение $x^2 \equiv d \equiv 0 \pmod 4$ имеет два решения.

Далее, находим

$$R(4m) = 2\prod_{p|m} R(p^{l_p})$$

и по утверждению 1 § 4 справедливо равенство $R(p^l) = 1 + \left(\frac{d}{p}\right)$. Отсюда следует искомое равенство. ◁

4. Пусть m — натуральное число, $(d,m)=1$. Тогда

1) для нечетного числа d имеем $\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right)$ (символ Якоби);

2) для четного числа $d = 2^b u$, $(u,2)=1$, имеем $\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{\frac{u-1}{2}\frac{m-1}{2}} \left(\frac{m}{|u|}\right)$ (оба символа в правой части равенства — символы Якоби).

▷ 1) Поскольку d — нечетное число, $d \equiv 1 \pmod 4$ и d не является квадратом. Представим число m в виде $m = 2^a u$, где u — нечетное число. По утверждению задачи 2 и по определению символа Кронекера имеем

$$\left(\frac{d}{m}\right) = \left(\frac{d}{2^a u}\right) = \left(\frac{d}{2}\right)^a \left(\frac{d}{u}\right) = \left(\frac{2}{|d|}\right)^a \left(\frac{d}{u}\right).$$

Из утверждения 4 § 3 имеем

$$\left(\frac{d}{m}\right) = \left(\frac{2}{|d|}\right)^a \left(\frac{u}{|d|}\right) = \left(\frac{2^a u}{|d|}\right) = \left(\frac{m}{|d|}\right).$$

2) Пусть, теперь, d четное число. Тогда $d = 2^b u$, где u — нечетное число. По определению символа Кронекера имеем

$$\left(\frac{d}{m}\right) = \left(\frac{2^b u}{m}\right) = \left(\frac{2}{m}\right)^b \left(\frac{u}{m}\right).$$

Далее, из утверждения III.4 получим

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|u|}\right). \qquad ◁$$

Теперь покажем, что символ Кронекера как функция от m при фиксированном d является групповым характером $\chi_d(m) = \left(\frac{d}{m}\right)$.

5. Символ Кронекера $\left(\frac{d}{m}\right)$ как функция от m обладает следующими свойствами:

1) $\left(\frac{d}{m}\right) = 0$ при $(d, m) > 1$,

2) $\left(\frac{d}{1}\right) = 1$,

3) $\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$,

4) $\left(\frac{d}{m}\right) = \left(\frac{d}{m}\right)$ при $m_1 \equiv m_2 \pmod{|d|}$,

5) найдется m такое, что $\left(\frac{d}{m}\right) = -1$.

▷ Утверждения 1) и 2) следуют прямо из определения символа Кронекера. Утверждение 3) совпадает с утверждением задачи 2.

4) Пусть $(|d|, m_1) > 1$. Тогда из условия $m_1 \equiv m_2 \pmod{|d|}$ следует, что $(|d|, m_2) > 1$. Поэтому имеем

$$\left(\frac{d}{m_1}\right) = 0 = \left(\frac{d}{m_2}\right).$$

Пусть $(|d|, m_1) = 1$. Тогда имеем $(|d|, m_2) = 1$. Рассмотрим сначала случай нечетного d. Используя утверждение предыдущей задачи и свойство символа Якоби, получим

$$\left(\frac{d}{m_1}\right) = \left(\frac{m_1}{|d|}\right) = \left(\frac{m_2}{|d|}\right) = \left(\frac{d}{m_2}\right).$$

Пусть, теперь, d — четное число, $d = 2^b u$. Из утверждения предыдущей задачи имеем

$$\left(\frac{d}{m_1}\right) = \left(\frac{2}{m_1}\right)^b (-1)^{(u-1)(m_1-1)/4} \left(\frac{m_1}{|u|}\right),$$

$$\left(\frac{d}{m_2}\right) = \left(\frac{2}{m_2}\right)^b (-1)^{(u-1)(m_2-1)/4} \left(\frac{m_2}{|u|}\right).$$

Поскольку $|u|$ делит $|d|$, имеем $m_1 \equiv m_2 \pmod{|u|}$. Следовательно, по свойству символа Якоби получим

$$\left(\frac{m_1}{|u|}\right) = \left(\frac{m_2}{|u|}\right).$$

Далее, так как 4 делит $|d|$, то $m_1 \equiv m_2 \pmod 4$. Отсюда имеем

$$(-1)^{(u-1)(m_1-1)/4} = (-1)^{(u-1)(m_2-1)/4}.$$

Наконец, по закону взаимности для символа Якоби получим

$$\left(\frac{2}{m_1}\right) = (-1)^{\frac{m_1^2-1}{8}}, \quad \left(\frac{2}{m_2}\right) = (-1)^{\frac{m_2^2-1}{8}},$$

и при $b > 2$ из условия 8 делит $|d|$ следует, что $m_1 \equiv m_2 \pmod 8$. Отсюда при $b > 2$ находим

$$\left(\frac{2}{m_1}\right)^b = \left(\frac{2}{m_2}\right)^b.$$

При $b = 2$ это утверждение очевидно.

5) Рассмотрим сначала случай нечетного числа d, взаимно простого с числом m. В этом случае $d \equiv 1 \pmod 4$ и d не является квадратом. При $d < 0$ имеем $|d| \equiv 3 \pmod 4$. Следовательно, найдется простое число p такое, что $|d| = p^l u$, $(p, u) = 1$, u, l — нечетные числа. Возьмем число s квадратичным невычетом по модулю p. По китайской теореме об остатках найдется вычет m по модулю $|d|$, удовлетворяющий условиям

$$m \equiv s \pmod p, \quad m \equiv 1 \pmod u.$$

По утверждению предыдущей задачи имеем

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right) = \left(\frac{m}{p}\right)^l \left(\frac{m}{u}\right) = \left(\frac{s}{p}\right)^l \left(\frac{1}{u}\right) = (-1)^l = -1.$$

Пусть, теперь, d — четное число. Тогда $d = 2^b u, b \leqslant 2, u$ — нечетное число.

Пусть, сначала, b будет нечетным числом. Тогда выберем число $m > 0$ из условий

$$m \equiv 5 \pmod 8, \quad m \equiv 1 \pmod{|u|},$$

что возможно, поскольку $(8, |u|) = 1$. Далее, имеем $(|d|, m) = 1$ и по утверждению предыдущей задачи получим

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|u|}\right) = \left(\frac{2}{m}\right) \cdot 1 \cdot \left(\frac{1}{|u|}\right) = -1.$$

Рассмотрим оставшийся случай: $d = 2^b u$ и b — четные числа, u — нечетное число и не является точным квадратом. При $m > 0$ и $(|d|, m) = 1$ по утверждению предыдущей задачи получим

$$\left(\frac{d}{m}\right) = (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|d|}\right).$$

Пусть, сначала, будет $u \equiv 3 \pmod 4$. Выберем $m > 0$, удовлетворяющее условиям

$$m \equiv -1 \pmod 4, \quad m \equiv 1 \pmod{|u|}.$$

Тогда числа m и $|d|$ — взаимно просты. Следовательно, имеем

$$\left(\frac{d}{m}\right) = (-1)^{\frac{u-1}{2}} \left(\frac{1}{|d|}\right) = -1.$$

Пусть, теперь, $u \equiv 1 \pmod 4$. Тогда при $m > 0$ и $(|d|, m) = 1$ находим

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|u|}\right).$$

Число $|u|$ не является точным квадратом (при положительном d это очевидно; если же $d < 0$, то $|u| = -u \equiv -1 \pmod 4$). Следовательно, найдется нечетное простое число p такое, что $|u| = p^l v, (p, v) = 1$, и числа v, l — нечетные. Выберем квадратичный невычет s по модулю p. Так как числа 2, p, v взаимно просты, то по китайской теореме об остатках существует $m > 0$ такое, что

$$m \equiv s \pmod p, \quad m \equiv 1 \pmod v, \quad m \equiv 1 \pmod 2.$$

Числа m и $|d|$ взаимно просты. Имеем

$$\left(\frac{d}{m}\right) = \left(\frac{d}{p^l v}\right) = \left(\frac{d}{p}\right)^l \left(\frac{m}{v}\right) = \left(\frac{s}{p}\right)\left(\frac{1}{v}\right) = -1. \triangleleft$$

6. $\left(\frac{d}{|d|-1}\right) = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$

$\triangleright$ Пусть d — нечетное число. Тогда по утверждению задачи 4 имеем

$$\left(\frac{d}{|d|-1}\right) = \left(\frac{|d|-1}{|d|}\right) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$$

Пусть, теперь, d будет четным числом. Представим его в виде $d = 2^b u$, $b \geqslant 2$, u — нечетное число. По утверждению задачи 4 находим

$$\left(\frac{d}{|d|-1}\right) = \left(\frac{2}{|d|-1}\right)^b (-1)^{\frac{u-1}{2}} \left(\frac{|d|-1}{|u|}\right).$$

При $b = 2$, очевидно, $\left(\frac{2}{|d|-1}\right)^b = 1$. При $b \geqslant 3$ имеем

$$\left(\frac{2}{|d|-1}\right) = (-1)^{\frac{(|d|-1)^2-1}{8}} = 1.$$

Далее, поскольку $|u|$ делит $|d|$, получим

$$(-1)^{\frac{u-1}{2}} \left(\frac{|d|-1}{|u|}\right) = (-1)^{\frac{u-1}{2}} \left(\frac{-1}{|u|}\right) =$$

$$= (-1)^{\frac{u-1}{2}+\frac{|u|-1}{2}} = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$$

Тем самым, искомая формула доказана. $\triangleleft$

7. Пусть n, m — натуральные числа, $n \equiv -m \pmod{|d|}$. Тогда имеем

$$\left(\frac{d}{n}\right) = \begin{cases} \left(\frac{d}{m}\right), & \text{если } d > 0, \\ -\left(\frac{d}{m}\right), & \text{если } d < 0. \end{cases}$$

▷ Имеем

$$\left(\frac{d}{n}\right) = \left(\frac{d}{|d|m - m}\right) = \left(\frac{d}{m(|d| - 1)}\right) = \left(\frac{d}{m}\right)\left(\frac{d}{|d| - 1}\right).$$

Отсюда искомая формула следует из утверждения предыдущей задачи. ◁

8. Пусть $m \geqslant 1$ — нечетное число, $(n, m) = 1$. Тогда символ Якоби $\left(\frac{n}{m}\right)$ можно представить через символ Кронекера следующими способами:

$$\left(\frac{n}{m}\right) = \begin{cases} 1, & \text{если } m = k^2, \\ \left(\frac{m}{n}\right), & \text{если } m \equiv 1 \pmod 4, m \neq k^2, \\ \left(\frac{-m}{n}\right), & \text{если } m \equiv 3 \pmod 4. \end{cases}$$

▷ Если m — полный квадрат, то определению символа Якоби имеем $\left(\frac{n}{m}\right) = 1$.

Пусть, теперь, $m \equiv 1 \pmod 4$, m — не квадрат и $n = 2^b u$, u — нечетное число. Тогда по квадратичному закону взаимности для символа Якоби и по утверждению последней задачи получим

$$\left(\frac{n}{m}\right) = \left(\frac{2^d}{m}\right)\left(\frac{|u|}{m}\right) = \left(\frac{m}{2^d}\right)\left(\frac{m}{|u|}\right) = \left(\frac{m}{2^d|u|}\right) = \left(\frac{m}{|n|}\right) = \left(\frac{m}{n}\right).$$

Пусть, далее, $m \equiv 3 \pmod 4$, $u > 0$. Используя предыдущие аргументы, найдем

$$\left(\frac{n}{m}\right) = \left(\frac{2^d}{m}\right)\left(\frac{u}{m}\right) = \left(\frac{m}{2^d}\right)(-1)^{\frac{u-1}{2}}\left(\frac{m}{u}\right) =$$

$$= (-1)^{\frac{u-1}{2}}\left(\frac{m}{2^d u}\right) = (-1)^{\frac{u-1}{2}}\left(\frac{m}{n}\right) = \left(\frac{-m}{n}\right).$$

Пусть, наконец, $m \equiv 3 \pmod 4$, $u < 0$. Повторяя с очевидными изменениями предыдущие рассуждения, получим

$$\left(\frac{n}{m}\right) = \left(\frac{2^d}{m}\right)\left(\frac{-1}{m}\right)\left(\frac{|u|}{m}\right) = -\left(\frac{m}{2^d}\right)(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{|u|}\right) =$$

$$= -(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{2^d|u|}\right) = -(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{|n|}\right) = \left(\frac{-m}{n}\right). \qquad \triangleleft$$

9. Пусть $d \equiv 0$ или $1 \pmod 4$ и не является полным квадратом, m — натуральное число. Тогда символ Кронекера $\left(\frac{d}{m}\right)$ можно представить через символ Якоби следующим способом:

$$\left(\frac{d}{m}\right) = \begin{cases} 1, & \text{если } (m,d) > 1, \\ \left(\frac{m}{|d|}\right), & \text{если } (m,d) = 1,\ d \equiv 1 \pmod 4, \\ \left(\frac{d/4}{m}\right), & \text{если } (m,d) = 1,\ d \equiv 0 \pmod 4. \end{cases}$$

▷ Из определения символа Кронекера следует, что при $(m,d) > 1$ имеем $\left(\frac{d}{m}\right) = 0$. Далее, из утверждения задачи 4 при $(m,d) = 1$, $d \equiv 1 \pmod 4$, получим $\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right)$. Наконец, при $(m,d) = 1, d \equiv 0 \pmod 4$, $d = 2^b u$, $(u,2) = 1$, из утверждения задачи 4 находим

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|u|}\right) =$$

$$= \left(\frac{2}{m}\right)^{b-2} (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|u|}\right) = \left(\frac{d/4}{m}\right).$$

Таким образом, искомая формула доказана. ◁

10. 1) Существует нечетное простое число p такое, что символ Кронекера $\left(\frac{d}{p}\right)$ равен -1.

2) Пусть n не является точным квадратом. Тогда существует бесконечно много нечетных простых чисел p таких, что $\left(\frac{n}{p}\right) = -1$.

3) Пусть сравнение $x^2 \equiv n \pmod p$ разрешимо для всех достаточно больших простых чисел p. Тогда n — полный квадрат.

▷ 1) Из утверждения предыдущей задачи достаточно рассмотреть случай $d \equiv 1 \pmod 4$. Имеем

$$\left(\frac{d}{p}\right) = \left(\frac{p}{|d|}\right).$$

Поскольку $|d|$ не является полным квадратом, в каноническом разложении его степень некоторого простого числа q входит в нечетной степени. Найдем число p из условий

$$\left(\frac{p}{q}\right) = -1, \quad \left(\frac{p}{r}\right) = 1$$

для любого простого делителя $r \neq q$ числа $|d|$. Это число p должно принадлежать некоторой арифметической прогрессии с разностью $|d|$.

2) Так как n не является полным квадратом, то в каноническом разложении n на простые сомножители найдется простое число q,

которое входит в это каноническое разложение в нечетной степени. Простые числа p будем искать из следующих условий

$$\left(\frac{q}{p}\right) = -1, \quad \left(\frac{r}{p}\right) = 1$$

для любого простого делителя $r \neq q$ числа n.

3) По условию задачи существует p_0 такое, что для всех $p \geqslant p_0$ разрешимо сравнение $x^2 \equiv n \pmod{p}$, т.е. $\left(\frac{n}{p}\right) = 1$. В силу утверждения 2), если n — не квадрат, то существует бесконечно много простых чисел p, для которых $\left(\frac{n}{p}\right) = -1$. Это противоречит условию, что $\left(\frac{n}{p}\right) = 1$ для всех достаточно больших p. ◁

§ 7. Простейшие теоремы о распределении простых чисел

1. Пусть $n \geqslant 2$ — натуральное число. Тогда справедливо следующее неравенство $\prod\limits_{p \leqslant n} p < 4^n$, где p пробегает все простые числа, не превосходящие n.

▷ Проведем индукцию по n. При $n = 2$ утверждение задачи верно. Предположим, что утверждение задачи имеет место при $n = m$. Докажем его при $n = m + 1$. Если $m + 1$ — четное число, то

$$\prod_{p \leqslant m+1} p = \prod_{p \leqslant m} p < 4^m < 4^{m+1}.$$

Пусть, теперь, $m + 1 = 2k + 1$, $k \geqslant 1$. Тогда каждое простое число p из отрезка от $k + 2$ до $2k + 1$ является делителем биномиального коэффициента $\binom{2k+1}{k}$, т.е.

$$\prod_{k+2 \leqslant p \leqslant 2k+1} p \mid \binom{2k+1}{k}.$$

Кроме того, при $k \geqslant 1$ справедливо неравенство

$$\binom{2k+1}{k} < 4^k.$$

Оно также доказывается индукцией по k. При $k = 1$ неравенство верно. Предположим, что оно верно при $k = r$. Докажем его при $k = r + 1$. Имеем

$$\binom{2r+3}{r+1} = \binom{2r+1}{r} \frac{(2r+3)(2r+2)}{(r+2)(r+1)} < 2\frac{2r+3}{r+2} 4^r < 4^{r+1}.$$

Отсюда находим

$$\prod_{p\leqslant 2k+1} p \leqslant \binom{2k+1}{k} \prod_{p\leqslant k+1} p < 4^{2k+1}. \qquad \triangleleft$$

Пусть $x > 1$ и p — простое число. Определим функцию Мангольдта $\Lambda(n)$ натурального аргумента n следующим соотношением

$$\Lambda(n) = \begin{cases} \ln p, & \text{если} \quad n = p^\alpha, \\ 0, & \text{в противном случае.} \end{cases}$$

Далее, определим функцию Чебышёва $\psi(x)$ вещественного аргумента x равенством

$$\psi(x) = \sum_{n\leqslant x} \Lambda(n) = \sum_{\substack{p,\alpha \\ p^\alpha \leqslant x}} \ln p.$$

Пусть символ $[a, b, \ldots, c]$ обозначает наименьшее общее кратное чисел $a, b, \ldots, c$.

2. При $n \geqslant 2$ справедливо равенство

$$[2, 3, \ldots, n] = e^{\psi(n)}.$$

▷ Имеем $[2, 3, \ldots, n] = \prod\limits_{p\leqslant n} p^{e_p}$, где показатели e_p определяются из неравенств $p^{e_p} \leqslant n \leqslant p^{e_p+1}$. Следовательно,

$$e_p = \left[\frac{\ln n}{\ln p}\right] = \sum_{\substack{\alpha \\ p^\alpha \leqslant n}} 1.$$

С другой стороны, находим

$$\psi(n) = \sum_{m\leqslant n} \Lambda(m) = \sum_{p\leqslant n} \ln p \sum_{\substack{\alpha \\ p^\alpha \leqslant n}} 1 = \sum_{p\leqslant n} e_p \ln p.$$

Отсюда получим

$$e^{\psi(n)} = \prod_{p\leqslant n} p^{e_p}. \qquad \triangleleft$$

3. При $n \geqslant 1$ имеем неравенство $\psi(2n + 1) \geqslant 2n \ln 2$.

▷ Из цепочки равенств

$$I = \int_0^1 x^n (1-x)^n \, dx = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \int_0^1 x^{n+k+1} \, dx = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{n+k+1}$$

следует, что $[n+1, n+2, \ldots, 2n+1]I$ является натуральным числом. Следовательно, $[2, 3, \ldots, 2n + 1]I \geqslant 1$. Отсюда, используя утверждение предыдущей задачи, находим $e^{\psi(2n+1)} I \geqslant 1$.

Далее, для любого x из отрезка $[0,1]$ имеем неравенство $x(1-x) \leqslant 1/4$. Стало быть, $I \leqslant 2^{-2n}$. Подставим эту оценку величины I в предыдущее неравенство, получим $e^{\psi(2n+1)} \geqslant 2^{2n}$, т.е. $\psi(2n+1) \geqslant 2n \ln 2$. ◁

Обозначим символом $\pi(x)$ количество всех простых чисел, не превосходящих x. Пусть, далее, $\theta(x)$ обозначает сумму $\theta(x) = \sum\limits_{p \leqslant x} \ln p$. Из утверждения задачи 1 при $n = [x]$ имеем

$$\theta(x) = \theta(n) \leqslant 2n \ln 2 \leqslant 2x \ln 2.$$

4. Для любого $x \geqslant 4$ справедливы неравенства

$$\frac{Ax}{\ln x} \leqslant \pi(x) \leqslant \frac{Bx}{\ln x},$$

где A и B — некоторые положительные постоянные, удовлетворяющие условиям $A \leqslant 1 \leqslant B$.

▷ Имеем

$$\ln \sqrt{x}(\pi(x) - \pi(\sqrt{x})) \leqslant \theta(x) \leqslant 2x \ln 2.$$

Следовательно,

$$\pi(x) \leqslant 2 \ln 2 \frac{x}{\ln \sqrt{x}} + \pi(\sqrt{x}) \leqslant 4 \ln 2 \frac{x}{\ln x} \left(1 + \frac{1}{4 \ln 2 \sqrt{x} \ln x}\right) \leqslant$$
$$\leqslant 6 \ln 2 \frac{x}{\ln x}, \quad B = 6 \ln 2.$$

Оценим функцию $\pi(x)$ снизу. Очевидно, имеем $\pi(x) \geqslant \frac{\theta(x)}{\ln x}$. Далее, находим

$$\theta(x) = \psi(x) - \sum_{\substack{p^\alpha \leqslant x \\ \alpha \geqslant 2}} \ln p \geqslant \psi(x) - \sqrt{x} \ln x \log_2 x.$$

Отсюда и из утверждения предыдущей задачи получим

$$\theta(x) \geqslant (x-2) \ln 2 - \sqrt{x} \ln x \log_2 x \geqslant \frac{\ln 2}{3} x.$$

Таким образом, находим $\pi(x) \geqslant \frac{\ln 2}{3} \cdot \frac{x}{\ln x}$, $A = \frac{\ln 2}{3}$. ◁

§ 8. Распознавание простых и составных чисел

1. Для того чтобы натуральное число $n \geqslant 2$ было простым необходимо и достаточно, чтобы выполнялось сравнение

$$(n-1)! \equiv -1 \pmod{n}.$$

▷ *Необходимость.* Пусть n — простое число. Тогда для любого вычета a по модулю n, отличного от 1 и -1, найдется вычет b по модулю n такой, что $ab \equiv 1 \pmod{n}$ и $a \not\equiv b \pmod{n}$. В произведении $(n-1)!$ сгруппируем попарно такие вычеты a и b. Без пары останутся только 1 и -1. Следовательно, $(n-1)! \equiv -1 \pmod{n}$.

Достаточность. Предположим противное, т.е. n — составное число, $a \mid n$, $1 < a < n$. Из условия $n \mid (n-1)! + 1$ следует, что $a \mid (n-1)! + 1$. Отсюда имеем противоречивую цепочку сравнений

$$-1 \equiv (n-1)! \equiv 0 \pmod{a}.$$

Таким образом, предположение о том, что число n — составное является неверным. Следовательно, n — простое число. ◁

2. Пусть a, n — натуральные числа, $(a, n) = 1$ и $a^{n-1} \not\equiv 1 \pmod{n}$. Тогда n — составное число.

▷ Это утверждение есть логическое обращение малой теоремы Ферма: пусть p — простое число, $(a, p) = 1$; тогда $a^{p-1} \equiv 1 \pmod{p}$.◁

Составное число n, для которого $a^{n-1} \equiv 1 \pmod{n}$, называется псевдопростым числом Ферма (по основанию a). Составное число n, удовлетворяющие для всякого a, взаимно простого с n, условию $a^{n-1} \equiv 1 \pmod{n}$, называется числом Кармайкла. Наименьшим таким числом является $561 = 3 \cdot 11 \cdot 17$.

3. Пусть n — нечетное число, a — натуральное число, $(a, n) = 1$ и

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Тогда n — составное число.

▷ Это утверждение есть логическое обращение критерия Эйлера для квадратичного вычета по простому модулю n: пусть n — нечетное простое число, a — натуральное число, $(a, n) = 1$, $\left(\frac{a}{n}\right)$ — символ Якоби. Тогда

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \quad ◁$$

Нечетное составное число n, для которого при a, взаимно простом с n, выполняется сравнение

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n},$$

называется псевдопростым числом Эйлера (по базе a).

Известно, что число 561 является числом Кармайкла, но по утверждению задачи 1 нельзя установить, что оно составное. Так как $5^{280} \equiv 67 \pmod{561}$, то по утверждению задачи 2 число 561 является составным.

4. Пусть p — простое число, k — натуральное число, $k < p$, $n = kp^2 + 1$ и

$$2^k \not\equiv 1 \pmod{n}, \quad 2^{n-1} \equiv 1 \pmod{n}.$$

Тогда число n — простое.

▷ Покажем сначала, что $p \mid \varphi(n)$. Пусть $d > 1$ обозначает минимальное натуральное число такое, что $2^d \equiv 1 \pmod{n}$. Разделим числа $n-1$, $\varphi(n)$ с остатком на d. Получим

$$n - 1 = dq_1 + r_1, \quad \varphi(n) = dq_2 + r_2, \quad 0 \leqslant r_1, r_2 \leqslant d - 1.$$

Отсюда имеем

$$2^{r_1} - 1 \equiv 2^{(n-1)-dq_1} - 1 \equiv 0 \pmod{n},$$

$$2^{r_2} - 1 \equiv 2^{\varphi(n)-dq_2} - 1 \equiv 0 \pmod{n}.$$

Следовательно, в силу выбора числа d минимальным с условием $2^d - 1 \equiv 0 \pmod{n}$ имеем, что $r_1 = 0, r_2 = 0$.

Далее, d не делит k, так как $2^k \not\equiv 1 \pmod{n}$.

Таким образом, находим $kp^2 = n - 1 = dm$, $d \not| k$. Отсюда имеем $p \mid d$. Значит, $p \mid d \mid \varphi(n)$.

Предположим, что n составное число. Тогда покажем, что существует простой делитель q числа n такой, что $q \equiv 1 \pmod{p}$. Число n взаимно просто с p, поскольку $n = kp^2 + 1$. Пусть $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$. Тогда имеем $\varphi(n) = (q_1^{\alpha_1} - q_1^{\alpha_1 - 1}) \dots (q_1^{\alpha_r} - q_1^{\alpha_r - 1})$. Поскольку $p \mid \varphi(n)$, найдется простой делитель q числа n такой, что $p \mid (q^\alpha - q^{\alpha-1})$. Далее, $(p, q) = 1$, поэтому $p \mid q - 1$.

Положим $q = up + 1$. Имеем $n = kp^2 + 1 = (up + 1)(vp + 1)$. Следовательно, $uvp + u + v = kp$. Отсюда при некотором натуральном s находим, что $u + v = ps$. Далее получим противоречивое неравенство

$$p \leqslant uv < k < p.$$

Таким образом предположение о том, что число n составное, неверно. ◁

В 1951 г. Миллер и Вилер [26], используя компьютер и утверждение предыдущей задачи, доказали, что $180(2^{127} - 1)^2 + 1$ — простое число.

5. Пусть p — нечетное простое число, k — натуральное число, $k \leqslant 2p + 1, n = 2kp + 1$, и пусть существует натуральное число a такое, что

$$a^{n-1} \equiv 1 \pmod{n}, \quad a^{2k} \not\equiv 1 \pmod{n}.$$

Тогда n — простое число.

▷ Покажем, как и предыдущей задаче, что $p \mid \varphi(n)$. Пусть d обозначает порядок элемента a по модулю n. Тогда, проводя те же рассуждения, что и в предыдущей задаче, находим $d \mid n-1$, $d \mid \varphi(n)$. Поскольку $a^{2k} \not\equiv 1 \pmod n$, число d не является делителем числа $2k$. Следовательно, из равенства $n-1 = 2kp = dm$ имеем $p \mid d$. Но $d \mid \varphi(n)$, поэтому $p \mid \varphi(n)$.

Пусть число n — составное и $n = \prod\limits_{q \mid n} q^{\alpha_q}$ — каноническое разложение его на простые сомножители. Имеем $\varphi(n) = \prod\limits_{q \mid n}(q^{\alpha_q} - q^{\alpha_q - 1})$. Так как $p \mid \varphi(n)$, то найдется $q \mid n$ такое, что $p \mid q^{\alpha_q} - q^{\alpha_q - 1}$. Следовательно, $p \mid q-1$, т.е. $q \equiv 1 \pmod p$. Поскольку q нечетное число, имеем $q \equiv 1 \pmod{2p}$, т.е. при некотором натуральном u справедливо равенство $q = 1 + 2pu$. Далее, $n = 1 + 2kp$, поэтому $n = (1+2pu)(1+2pv)$. Отсюда находим $n \geqslant (1+2p)^2$. С другой стороны, $n = 1 + 2kp \leqslant 1 + 2(2p+1)p < (1+2p)^2$. Последние два неравенства противоречивы. Следовательно, предположение о том, что n — составное число, неверно. ◁

Наименьшее натуральное число l с условием $a^l \equiv 1 \pmod m$, $(a, m) = 1$, называется порядком натурального числа a по модулю m или число a по модулю m принадлежит показателю l.

Заметим, что для простого числа p и $d \mid p-1$ количество $I = I(d)$ решений сравнения $x^d \equiv 1 \pmod p$ равно d. Действительно, по утверждению задачи I.6 величина $I(d) \leqslant d$. Далее, по малой теореме Ферма сравнение $x^{p-1} \equiv 1 \pmod p$ имеет $p-1$ решений, — все вычеты из приведенной системы вычетов по модулю p. Рассмотрим сравнение

$$\frac{x^{p-1}-1}{x^d-1} = (x^d)^{\frac{p-1}{d}-1} + \cdots + x^d + 1 \equiv 0 \pmod p.$$

По теореме 6 § 1 количество его решений $p-1-I(d)$ не превосходит степени многочлена $p-1-d$. Следовательно, $I(d) \geqslant d$. Таким образом, $I(d) = d$.

6. Пусть p — простое число и l делит $p-1$. Тогда количество чисел порядка l из приведенной системы вычетов по модулю p равно $\varphi(l)$.

▷ Обозначим символом $\psi(l)$ количество чисел порядка l из приведенной системы вычетов по модулю p. Сначала докажем, что $\psi(l)$ обладает свойством мультипликативности, т.е. для любых $(l_1, l_2) = 1$, $l_1 \mid p-1$, $l_2 \mid p-1$ имеем $\psi(l_1 l_2) = \psi(l_1)\psi(l_2)$.

Пусть число h_1 имеет порядок l_1, число h_2 — порядок l_2 и число $h_1 h_2$ — порядок l. Докажем, что $l = l_1 l_2$. Действительно, находим

$(h_1h_2)^{l_1l_2} \equiv 1 \pmod p$, т.е. $l \leqslant l_1l_2$. С другой стороны, имеем $1 \equiv (h_1h_2)^{ll_2} \equiv h_1^{ll_2} \pmod p$. Следовательно, $l_1 \mid ll_2$. Но так как $(l_1, l_2) = 1$, то $l_1 \mid l$. Аналогично доказывается, что $l_2 \mid l$. Отсюда $l_1l_2 \mid l$. Значит, $l_1l_2 \leqslant l$. Таким образом, получаем $l = l_1l_2$.

Итак, установлено соответствие: паре чисел (h_1, h_2) с указанными выше свойствами ставится в соответствие их произведение h_1h_2 по модулю p. Покажем, что оно взаимно-однозначное. Пусть (h_1', h_2') — другая пара с тем же произведением $h_1'h_2' \equiv h_1h_2 \pmod p$. Тогда $h_1'h_1^{-1} \equiv h_2'h_2^{-1} \pmod p$. Таким образом, числа $h_1'h_1^{-1}$ и $h_2'h_2^{-1}$ имеют один и тот же порядок δ, причем $\delta \mid l_1$, $\delta \mid l_2$. Следовательно, $\delta = 0$ и $h_1'h_1^{-1} \equiv h_2'h_2^{-1} \equiv 1 \pmod p$. Это означает, что пары (h_1, h_2) и (h_1', h_2') по модулю p совпадают.

Заметим, что обратное отображение можно задать так: $h_1 = h^{l_2}$, $h_2 = h^{l_1}$.

Таким образом установлено, что $\psi(l_1)\psi(l_2) = \psi(l_1l_2)$.

Пусть, далее, $q^t \mid p-1$, q — простое число. Тогда для того, чтобы число h имело порядок q^t по модулю p, необходимо и достаточно, чтобы выполнялись условия

$$h^{q^t} \equiv 1 \pmod p, \quad h^{q^{t-1}} \not\equiv 1 \pmod p.$$

Поскольку сравнение $x^{q^t} \equiv 1 \pmod p$ имеет q^t не сравнимых по модулю p решений, находим

$$\psi(q^t) = q^t - q^{t-1} = \varphi(q^t).$$

По свойству мультипликативности функций $\psi(l)$ и $\varphi(l)$ отсюда следует, что $\psi(l) = \varphi(l)$. ▷

Число a называется первообразным корнем по модулю m, если порядок его равен $\varphi(m)$. Из утверждения предыдущей задачи следует, что количество первообразных корней по нечетному простому модулю p равно $\varphi(p-1)$. Тем не менее, докажем теорему о существовании первообразного корня по простому модулю, дающую способ построения его.

7. Для нечетного простого числа существует первообразный корень.

▷ Пусть p и q — простые числа, l — натуральное число и $p \equiv 1 \pmod{q^l}$. Докажем, что найдется число a, принадлежащее показателю q^l по модулю p. Так как по утверждению задачи I.6 количество не сравнимых корней полиномиального сравнения не превосходит его степени, то при $p \geqslant 3$ количество решений сравнения $x^{(p-1)/q} \equiv 1 \pmod p$ не превосходит $\frac{p-1}{q} \leqslant \frac{p-1}{2} \leqslant p-2$. Следовательно, найдется такой вычет $b, (b, p) = 1$, что $b^{(p-1)/q} \not\equiv 1 \pmod p$. Положим

$a = b^{(p-1)/q^l}$. Тогда имеем

$$a^{q^l} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Пусть a принадлежит по модулю p показателю δ. Из предыдущего сравнения имеем, что δ делит q^l. Возможны два случая $\delta = q^l$ и $\delta \mid q^{l-1}$. Рассмотрим второй случай. Из определения порядка по модулю p числа a имеем

$$b^{(p-1)/q} = a^{q^{l-1}} \equiv 1 \pmod{p}.$$

Это противоречит выбору числа b. Следовательно, число a по модулю p принадлежит показателю q^l.

Докажем теперь, что существует число g, принадлежащее показателю $p-1$ по модулю p, т.е. число g будет первообразным корнем по модулю p.

При $p = 2$ число 1 удовлетворяет условию задачи. Пусть p будет нечетным простым числом и каноническое разложение на простые сомножители числа $p-1$ имеет вид $p-1 = \prod\limits_{q|p-1} q^{\alpha_q}$. Ранее доказано, что существует число a_q, принадлежащее показателю q^{α_q} по модулю p. Положим $g = \prod\limits_{q|p-1} a_q$ и буквой Δ обозначим показатель, которому число g принадлежит по модулю p. Из теоремы Эйлера имеем $\Delta \mid p-1$. Возможны два случая: либо $\Delta = p-1$, либо при некотором простом q и натуральном u имеем $p-1 = qu\Delta$.

Рассмотрим второй случай. Имеем

$$1 \equiv g^{\Delta u} \equiv g^{(p-1)/q} \equiv a_q^{(p-1)/q} \prod_{\substack{r|p-1 \\ r \neq q}} a_r^{(p-1)/q} \equiv a_q^{(p-1)/q} \not\equiv 1 \pmod{p}.$$

Это соотношение противоречиво. Следовательно, второй случай не возможен. Таким образом, $\Delta = p-1$. ▷

Пусть $m > 1$ — натуральное число и пусть существует натуральное число g такое, что числа g^0, g^1, g^2, …, $g^{\varphi(m)-1}$ образуют приведенную систему вычетов по модулю m. Тогда число g называется первообразным корнем по модулю m.

8. Для того чтобы по модулю $m > 1$ существовал первообразный корень необходимо и достаточно, чтобы число m имело вид 2, 4, p^α, $2p^\alpha$, где p — нечетное простое и l — натуральное.

▷ Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ — каноническое разложение числа m на простые сомножители. По теореме Эйлера для каждого числа a, взаимно простого с p, и любого натурального α, справедливо сравнение $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$.

Пусть буква q обозначает наименьшее общее кратное чисел $\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r})$. Тогда имеем $a^q \equiv 1 \pmod m$. Следовательно, если $q < \varphi(m)$, то первообразных корней по модулю m не существует.

Если p — нечетное простое и α — натуральное число, то $\varphi(p^\alpha)$ — четное число. Отсюда получим, что если по модулю m существует первообразный корень, то m не может иметь двух различных нечетных простых делителей.

Таким образом, первообразный корень может существовать по модулям m вида 2^α, p^α, $2^\beta p^\alpha$. Пусть $\beta \geqslant 2$. Тогда $\varphi(2^\beta) = 2^{\beta-1}$ — четное число и по модулю $m = 2^\beta p^\alpha$ не существует первообразных корней. Следовательно, первообразные корни могут существовать по модулям 2^α, p^α, $2p^\alpha$.

Рассмотрим случай $m = 2^\alpha$. При $\alpha = 1$ число 1 — первообразный корень по модулю 2, при $\alpha = 2$ число 3 — первообразный корень по модулю 4.

Индукцией по α докажем, что при $\alpha \geqslant 3$ по модулю 2^α нет первообразных корней. При $\alpha = 3$ для любого нечетного $a = 2b + 1$ имеем $a^2 = 4b(b+1) + 1 \equiv 1 \pmod 8$. Следовательно, по модулю 8 первообразных корней нет.

Предположим, что утверждение справедливо при $\alpha = l$, т.е. для любого нечетного числа порядок его меньше $\varphi(2^l) = 2^{l-1}$. Это означает, что

$$a^{2^{l-2}} \equiv 1 \pmod{2^l} \quad \text{или} \quad a^{2^{l-2}} = 1 + 2^l d$$

при некотором целом числе $d = d(a)$.

Докажем утверждение при $\alpha = l + 1$. Имеем

$$a^{2^{l-1}} - 1 = (1 + 2^l d)^2 - 1 = 2^{l+1} d(1 + 2^{l-1} d) \equiv 0 \pmod{2^{l+1}}.$$

Таким образом, порядок любого нечетного числа по модулю 2^l при $l \geqslant 3$ не превосходит $2^{l-2} = \varphi(2^l)/2$, т.е. по модулю 2^l, $l \geqslant 3$ нет первообразных корней.

Рассмотрим теперь случай $m = p^\alpha$, где p — нечетное простое число.

Индукцией по α докажем, что при $\alpha \geqslant 1$ по модулю p^α существует первообразный корень. При $\alpha = 1$ это утверждение совпадает с утверждением предыдущей задачи.

Пусть g — первообразный корень по модулю p. Положим

$$h = \begin{cases} g, & \text{если} \quad g^{p-1} \not\equiv 1 \pmod{p^2}, \\ g + p, & \text{если} \quad g^{p-1} \equiv 1 \pmod{p^2}. \end{cases}$$

Тогда имеем $h^{p-1} \not\equiv 1 \pmod{p^2}$. Достаточно проверить, что в случае

$g^{p-1} \equiv 1 \pmod{p^2}$, выполняется следующее соотношение

$$h^{p-1} - 1 \equiv (g+p)^{p-1} - 1 \equiv -pg^{p-2} \not\equiv 0 \pmod{p^2}.$$

Покажем сначала, что h является первообразным корнем по модулю p^2. Пусть h по модулю p^2 принадлежит показателю δ. Тогда имеем $h^\delta \equiv 1 \pmod{p^2}$. Следовательно, $h^\delta \equiv g^\delta \equiv 1 \pmod{p}$. Так как g — первообразный корень по модулю p, то δ кратно $p-1$. С другой стороны, по теореме Эйлера δ делит $\varphi(p^2) = p(p-1)$. Таким образом, показатель δ может быть равен либо $p-1$, либо $p(p-1)$. По выбору числа h имеем

$$h^{p-1} = 1 + kp, \quad k \not\equiv 0 \pmod{p}; \quad h^{p-1} \not\equiv 1 \pmod{p^2}.$$

Это означает, что h не принадлежит по модулю p^2 показателю $p-1$. Остается только возможность $\delta = p(p-1)$, т.е. h является первообразным корнем по модулю p^2.

Предположим, что число h является первообразным корнем по модулю p^l, т.е. h по модулю p^l принадлежит показателю $\varphi(p^l)$.

Докажем, что утверждение верно при $\alpha = l+1$, т.е. h — первообразный корень по модулю p^{l+1}. Пусть h по модулю p^{l+1} принадлежит показателю Δ. Поскольку выполняется сравнение $h^\Delta \equiv 1 \pmod{p^{l+1}}$, получим $h^\Delta \equiv 1 \pmod{p^l}$. Но число h — первообразный корень по модулю p^l. Следовательно, Δ кратно $\varphi(p^l) = p^{l-1}(p-1)$. По теореме Эйлера имеем $h^{p^l(p-1)} \equiv 1 \pmod{p^{l+1}}$. Следовательно, Δ является делителем числа $\varphi(p^{l+1}) = p^l(p-1)$. Отсюда находим, что Δ равно либо $\varphi(p^l) = p^{l-1}(p-1)$, либо $\varphi(p^{l+1})$. Далее, по биному Ньютона имеем

$$h^{p^{l-1}(p-1)} = (1+kp)^{p^{l-1}} \equiv 1 + kp^l \not\equiv 1 \pmod{p^{l+1}},$$

т.е. h по модулю p^{l+1} не принадлежит показателю $\varphi(p^l)$ и $\Delta \neq \varphi(p^l)$. Следовательно, $\Delta = \varphi(p^{l+1})$ и число h — первообразный корень по модулю p^{l+1}.

Рассмотрим случай $m = 2p^\alpha, p$ — нечетное простое число. Пусть g — первообразный корень по модулю p^α. Тогда

$$h = \begin{cases} g, & \text{если } g \equiv 1 \pmod{2}, \\ g + p^\alpha, & \text{если } g \equiv 0 \pmod{2} \end{cases}$$

является первообразным корнем по модулю $2p^\alpha$. ◁

Утверждение следующей задачи дает способ разыскания первообразных корней по некоторому модулю m. Из утверждения предыдущей задачи имеем, что m равно одному из значений 2, 4, p^α, $2p^\alpha$, где p — нечетное простое число и α — натуральное число.

9. Для того чтобы число g, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы для любого простого делителя q числа $\varphi(m)$ выполнялось условие

$$g^{\varphi(m)/q} \not\equiv 1 \pmod{m}.$$

▷ *Необходимость.* Поскольку g — первообразный корень по модулю m, число g по модулю m принадлежит показателю $\varphi(m)$ и, следовательно, для любого простого делителя q выполняются условия

$$g^{\varphi(m)/q} \not\equiv 1 \pmod{m}.$$

Достаточность. Пусть δ — показатель, которому принадлежит g по модулю m. По теореме Эйлера число g является делителем $\varphi(m)$. Предположим, что $\delta < \varphi(m)$. Тогда имеем $\varphi(m) = \delta q u$, где q — некоторое простое число. Следовательно,

$$g^{\varphi(m)/q} = g^{\delta u} \equiv 1 \pmod{m},$$

что противоречит условию задачи. ◁

Следующий признак распознавания простоты числа принадлежит Е. Люка и Д. Х. Лемеру [13].

10. Пусть $N \geqslant 2$ — натуральное число, $N - 1 = \prod\limits_{q \mid N-1} q^{\alpha_q}$ — каноническое разложение числа $N - 1$ на простые сомножители, и пусть найдется натуральное число a такое, что

$$a^{N-1} \equiv 1 \pmod{N},$$

и для любого $q \mid N - 1$ выполняется условие

$$a^{(N-1)/q} \not\equiv 1 \pmod{N}.$$

Тогда число N является простым.

▷ Пусть число a по модулю N принадлежит показателю δ. Тогда из условия $a^{N-1} \equiv 1 \pmod{N}$ следует, что $\delta \mid N - 1$. Предположим, что $\delta < N - 1$. Тогда найдется простое число q, делящее $N - 1$, такое, что $N - 1 = qu\delta$. Далее, имеем

$$1 \equiv a^{\delta u} \equiv a^{(N-1)/q} \not\equiv 1 \pmod{N}.$$

Противоречие. Следовательно, $\delta = N - 1$, и число a по модулю N принадлежит показателю $N - 1$.

Далее, по теореме Эйлера находим $a^{\varphi(N)} \equiv 1 \pmod{N}$. Отсюда имеем, что $N - 1 \mid \varphi(N)$. Следовательно, $N - 1 \leqslant \varphi(N)$.

Пусть N — составное число. Тогда найдется число p такое, что $p \mid N, 1 < p < N$. Стало быть, справедливы неравенства

$$\varphi(N) < N\left(1 - \frac{1}{p}\right) < N\left(1 - \frac{1}{N}\right) = N - 1.$$

Это противоречит предыдущему неравенству для $N-1$. Таким образом, доказано, что N — простое число. $\triangleleft$

11. Пусть $N \geqslant 2$ — натуральное число, $N-1 = \prod\limits_{q|N-1} q^{\alpha_q}$ — каноническое разложение числа $N-1$ на простые сомножители, и пусть для каждого простого числа $q \mid N-1$ найдется натуральное число a_q такое, что

$$a_q^{N-1} \equiv 1 \pmod N,$$

и для любого $q \mid N-1$ выполняется условие

$$a_q^{(N-1)/q} \not\equiv 1 \pmod N.$$

Тогда число N является простым.

$\triangleright$ Пусть q — простое число, являющееся делителем $N-1$ и число a_q по модулю N принадлежит показателю δ_q. Тогда из условия $a_q^{N-1} \equiv 1 \pmod N$ следует, что $\delta_q \mid N-1$, т.е. при некотором натуральном числе u_q имеем $N-1 = \delta_q u_q$.

Докажем, что $(q, u_q) = 1$. Предположим противное, т.е. $q \mid u_q$. Тогда при некотором натуральном v_q получим $N-1 = \delta_q q v_q$. Отсюда, используя условие задачи, получим противоречивое соотношение

$$1 \equiv a_q^{\delta_q v_q} = a_q^{(N-1)/q} \not\equiv 1 \pmod N.$$

Следовательно, $(q, u_q) = 1$. Значит, $\delta_q = q^{\alpha_q} w_q$, $(q, w_q) = 1$.

Рассмотрим число $b = \prod\limits_{q|N-1} a_q^{w_q}$. Докажем, что число b по модулю N принадлежит показателю $N-1$ и удовлетворяет условию предыдущей задачи.

Для любого простого $q \mid N-1$ число $a_q^{w_q}$ по модулю N принадлежит показателю q^{α_q}. Следовательно, число b по модулю N принадлежит показателю $\prod\limits_{q|N-1} q^{\alpha_q} = N-1$.

Далее, имеем

$$b^{N-1} = \prod_{q|N-1} a_q^{\delta_q w_q \frac{N-1}{\delta_q}} \equiv 1 \pmod N.$$

Рассмотрим любой простой делитель r числа $N-1$. Находим

$$b^{\frac{N-1}{r}} = a_r^{\frac{(N-1)w_r}{r}} \prod_{\substack{q|N-1 \\ q \neq r}} a_q^{\frac{(N-1)w_q}{r}} \not\equiv 1 \pmod N,$$

поскольку при простом $q \mid N-1, q \neq r$, имеем

$$a_q^{\frac{(N-1)w_r}{r}} = a_q^{\delta_q \frac{(N-1)w_q}{r\delta_q}} \equiv 1 \pmod N,$$

и поскольку показатель $\frac{(N-1)w_r}{r}$ не делится на δ_r, получим

$$a_r^{\frac{(N-1)w_r}{r}} \not\equiv 1 \pmod{N}.$$

Таким образом для числа N выполнены условия предыдущей задачи. Следовательно, N — простое число. ◁

12. Пусть $N \geqslant 2$ — натуральное число, $N-1 = FR$, $(F,R)=1$, $R<F$, $F = \prod\limits_{q|F} q^{\alpha_q}$ — каноническое разложение числа F на простые сомножители, и пусть найдется натуральное число a такое, что

$$a^{N-1} \equiv 1 \pmod{N},$$

и для любого $q \mid F$ выполняется условие

$$(a^{(N-1)/q} - 1, N) = 1.$$

Тогда число N является простым.

▷ Предположим, что N — составное число. Пусть $p \geqslant 2$ — наименьший простой делитель числа N. Тогда $p \leqslant \sqrt{N}$. По условию задачи имеем $a^{N-1} \equiv 1 \pmod{p}$, и для любого простого $q \mid F$ справедливо соотношение $a^{(N-1)/q} \not\equiv 1 \pmod{p}$. Буквой δ обозначим показатель, которому принадлежит число a по модулю p. Тогда $\delta \mid N-1$ и $N-1 = \delta u$. Возьмем любой простой делитель q числа F. Покажем, что $(q,u)=1$. Предположим противное, т.е. $q \mid u$. Тогда при некотором натуральном v имеем $N-1 = \delta q v$. Из определения δ и условия задачи находим противоречивое соотношение

$$1 \equiv a^{\delta v} = a^{(N-1)/q} \not\equiv 1 \pmod{p}.$$

Следовательно, для любого $q \mid F$ имеем $(q,u)=1$ и $q^{\alpha_q} \mid \delta$. Отсюда получим, что $F \mid \delta$. Из малой теоремы Ферма находим $\delta \mid p-1$. Таким образом, $F \mid p-1$. Стало быть, $p \geqslant F+1 > \sqrt{N}$. Это противоречит тому, что наименьший простой делитель составного числа N не превосходит $\sqrt{N}$. Значит, число N — простое. ◁

§ 9. Непрерывные (цепные) дроби. Критерий Лежандра для подходящих дробей

Рассмотрим любое вещественное число α. Пусть $a_0 = [\alpha]$ — наибольшее целое число, не превосходящее α, и $\{\alpha\} = \alpha - a_0$ — дробная часть числа α. Положим $\alpha = \alpha_0$

$$\alpha_1 = \begin{cases} 0, & \text{если} \quad \{\alpha\} = 0, \\ 1/\{\alpha\} & \text{в противном случае.} \end{cases}$$

Для нецелого α имеем

$$\alpha = a_0 + \frac{1}{\alpha_1}, \alpha_1 > 1.$$

Подобным образом при $s \geqslant 1$ для нецелого α_s имеем

$$\alpha_s = a_s + \frac{1}{\alpha_{s+1}}, \alpha_{s+1} > 1.$$

Таким образом число α разлагается в следующую простую непрерывную дробь

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_s + \cfrac{1}{\alpha_{s+1}}}}}.$$

Для удобства будем обозначать непрерывную дробь числа α в виде

$$\alpha = [a_0, a_1, a_2, \ldots, a_s, \alpha_{s+1}].$$

1. Для того чтобы вещественное число α разлагалось в конечную непрерывную дробь необходимо и достаточно, чтобы оно было рациональным числом.

▷ *Необходимость.* Процесс разложения числа α оборвется, скажем, на s-м шаге, если α_{s+1} равно целому числу a_{s+1}. Отсюда следует, что α — рациональное число.

Достаточность. Пусть $\alpha = p/q, (p, q) = 1$, — рациональное число. Тогда при нецелом α имеем $a_0 = [p/q]$ и

$$\frac{1}{\alpha_1} = \frac{p}{q} - \left[\frac{p}{q}\right], \alpha_1 > 1, \alpha_1 = [\alpha_1] + \frac{1}{\alpha_2}, a_1 = [\alpha_1],$$

т.е. для целого числа r_1 находим

$$p - q\left[\frac{p}{q}\right] = \frac{q}{\alpha_1} = r_1, 0 < r_1 < q.$$

Подобно этому получим

$$q - r_1\left[\frac{q}{r_1}\right] = \frac{r_1}{\alpha_2} = r_2, 0 < r_2 < r_1, \alpha_2 = [\alpha_2] + \frac{1}{\alpha_3}, a_2 = [\alpha_2].$$

Наконец, имеем

$$r_{s-1} - r_s\left[\frac{r_{s-1}}{r_s}\right] = \frac{r_s}{\alpha_{s+1}} = r_{s+1}, 0 < r_{s+1} < r_s,$$

и отношение r_s/r_{s+1} — натуральное число.

Таким образом, если α — рациональное число, то вычисление непрерывной дроби подобно алгоритму Евклида для нахождения наибольшего общего делителя чисел p и q, причем находим

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_s + \cfrac{1}{a_{s+1}}}}}.$$

Тем самым получено искомое разложение рационального числа α в конечную непрерывную дробь. ◁

Числа $a_0, a_1, a_2, \ldots$ называются неполными частными числа α, а дробь

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

называется n-й подходящей дробью.

2. Подходящие дроби p_n/q_n при $n \geqslant 2$ удовлетворяют следующим соотношениям

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2}, \\ q_n = a_n q_{n-1} + q_{n-2}, \end{cases}$$

кроме того, имеем

$$p_0 = a_0, \quad q_0 = 1; \quad p_1 = a_0 a_1 + 1, \quad q_1 = a_1.$$

▷ По определению имеем

$$\frac{p_0}{q_0} = [a_0] = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = [a_0, a_1] = \frac{a_0 + \frac{1}{a_1}}{1} = \frac{a_1 a_0 + 1}{a_1}.$$

Проведем индукцию по параметру $n \geqslant 2$. При $n = 2$ находим

$$\frac{p_2}{q_2} = [a_0, a_1, a_2] = \frac{\left(a_1 + \frac{1}{a_2}\right) a_0 + 1}{a_1 + \frac{1}{a_2}} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0},$$

т.е. справедливы равенства

$$\begin{cases} p_2 = a_2 p_1 + p_0, \\ q_2 = a_2 q_1 + q_0. \end{cases}$$

Предположим, что утверждение имеет место при $n = m$, т.е.

$$\begin{cases} p_m = a_m p_{m-1} + p_{m-2}, \\ q_m = a_m q_{m-1} + q_{m-2}. \end{cases}$$

Докажем его при $n = m + 1$. Используя замену a_m на $a_m + \frac{1}{a_{m+1}}$ и предположение индукции, находим

$$\frac{p_{m+1}}{q_{m+1}} = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} =$$

$$= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} = \frac{a_{m+1}p_m + p_{m-1}}{a_{m+1}q_m + q_{m-1}}.$$

Отсюда следуют искомые равенства для числителей и знаменателей подходящих дробей

$$\begin{cases} p_{m+1} = a_{m+1}p_m + p_{m-1}, \\ q_{m+1} = a_{m+1}q_m + q_{m-1}. \end{cases}$$ ◁

3. При $n \geqslant 1$ справедливы следующие равенства

$$p_n q_{n-1} - p_{n-1}q_n = (-1)^{n-1}$$

или

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}},$$

а при $n \geqslant 2$ имеем

$$p_n q_{n-2} - p_{n-2}q_n = (-1)^n a_n.$$

При $n \geqslant 0$ подходящие дроби p_n/q_n несократимы.

▷ Проведем индукцию по параметру n. Базовые утверждения индукции справедливы. Действительно,

$$p_1 q_0 - p_0 q_1 = (a_1 a_0 + 1) \cdot 1 - a_0 \cdot a_1 = 1,$$

$$p_2 q_0 - p_0 q_2 = (a_2 p_1 + p_0) q_0 - p_0(a_2 q_1 + q_0) = a_2(p_1 q_0 - p_0 q_1) = a_2.$$

Предположим, что утверждения имеют место при $n = m$, т.е.

$$p_m q_{m-1} - p_{m-1}q_m = (-1)^{m-1}$$

$$p_m q_{m-2} - p_{m-2}q_m = (-1)^m a_m.$$

Докажем его при $n = m + 1$. По предположению индукции находим

$$p_{m+1}q_m - p_m q_{m+1} = (a_m p_m + p_{m-1})q_m - p_m(a_m q_m + q_{m-1}) =$$

$$= p_{m-1}q_m - p_m q_{m-1} = -(-1)^{m-1} = (-1)^m,$$

$$p_{m+1}q_{m-1} - p_{m-1}q_{m+1} = (a_m p_m + p_{m-1})q_{m-1} - p_{m-1}(a_m q_m + q_{m-1}) =$$

$$= a_m(p_m q_{m-1} - p_{m-1}q_m) = (-1)^{m-1}a_m = (-1)^{m+1}a_m.$$

Искомые равенства доказаны. При $n \geqslant 1$ из равенства $p_n q_{n-1} - p_{n-1}q_n = (-1)^{n-1}$ следует, что числа p_n и q_n взаимно просты. ◁

4. 1) Пусть $n \geqslant 2$. Тогда для знаменателей подходящих дробей справедливо неравенство $q_n \geqslant q_{n-1} + 1$, так что $q_n \geqslant n$.

2) При $n \geqslant 1$ имеем

$$\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}, \quad \frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}.$$

▷ 1) По утверждению задачи 2 при $n \geqslant 2$ имеем

$$q_n = a_n q_{n-1} + q_{n-2} \geqslant q_{n-1} + 1.$$

Далее $q_2 = a_2 a_1 + 1 \geqslant 2$. Следовательно, используя предыдущее неравенство, получим

$$q_n \geqslant q_{n-1} + 1 \geqslant q_{n-2} + 2 \geqslant \ldots \geqslant q_2 + n - 2 \geqslant n.$$

2) По утверждению предыдущей задачи при $n \geqslant 2$ имеем

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}.$$

Отсюда при $n = 2m$ получим

$$\frac{p_{2m}}{q_{2m}} - \frac{p_{2m-2}}{q_{2m-2}} > 0,$$

а при $n = 2m + 1$

$$\frac{p_{2m+1}}{q_{2m+1}} - \frac{p_{2m-1}}{q_{2m-1}} < 0. \qquad \triangleleft$$

5. Пусть $A_n = [a_0, a_1, a_2, \ldots, a_n]$ является n-й подходящей дробью числа α. Тогда при $n \to \infty$ существует предел последовательности A_n.

▷ По утверждению 2) предыдущей задачи и первому тождеству задачи 3 имеем $A_1 \geqslant A_{2n+1} \geqslant A_{2n} \geqslant A_2$. Отсюда следует существование пределов при $n \to \infty$ последовательностей $\{A_{2n}\}$ и $\{A_{2n+1}\}$.

Далее по первому тождеству задачи 2 и утверждению 1) задачи 3 получим

$$|A_{2n} - A_{2n-1}| = \frac{1}{q_{2n} q_{2n-1}} \leqslant \frac{1}{2n(2n-1)}.$$

Следовательно, $\lim\limits_{n\to\infty} A_{2n} = \lim\limits_{n\to\infty} A_{2n+1}$, а это означает, что существует предел последовательности $\{A_n\}$. $\triangleleft$

Число $\alpha_n = [a_n, a_{n+1}, a_{n+2}, \ldots]$ называется n-м остатком разложения числа α в непрерывную дробь.

6. Справедливы следующие соотношения

$$\alpha = \alpha_0, \quad \alpha = \frac{\alpha_1 a_0 + 1}{\alpha_1}, \quad \alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}},\ n \geqslant 2.$$

Для рационального числа $\alpha = [a_0, a_1, \ldots, a_N]$ эти равенства справедливы от $n = 0$ до N.

▷ Проведем индукцию по параметру n. При $n = 1$ по определению имеем

$$\alpha = a_0 + \frac{1}{\alpha_1} = \frac{\alpha_1 a_0 + 1}{\alpha_1}.$$

Пусть утверждение верно при $n = m$, т.е.

$$\alpha = \frac{\alpha_m p_{m-1} + p_{m-2}}{\alpha_m q_{m-1} + q_{m-2}}.$$

Докажем его при $n = m + 1$. Для этого воспользуемся равенством $\alpha_m = a_m + \frac{1}{\alpha_{m+1}}$, предположением индукции и утверждением задачи 2. Получим

$$\alpha = \frac{\left(a_m + \frac{1}{\alpha_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{\alpha_{m+1}}\right) q_{m-1} + q_{m-2}} = \frac{\alpha_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{\alpha_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} =$$

$$= \frac{\alpha_{m+1} p_m + p_{m-1}}{\alpha_{m+1} q_m + q_{m-1}}. \triangleleft$$

7. Любое иррациональное число однозначным образом разлагается в непрерывную дробь.

▷ Предположим, что имеется два различных разложения числа α в непрерывную дробь $\alpha = [a_0, a_1, a_2, \ldots] = [b_0, b_1, b_2, \ldots]$. Очевидно, что $a_0 = [\alpha] = b_0$. Далее, найдется такой номер n, что при $0 \leqslant k < n$ справедливы равенства $a_k = b_k$ и $a_n \neq b_n$. Из разложений $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = [a_0, a_1, \ldots, a_{n-1}, \beta_n]$ по утверждению предыдущей задачи получим

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} = \frac{\beta_n p_{n-1} + p_{n-2}}{\beta_n q_{n-1} + q_{n-2}}.$$

Отсюда следует, что

$$(\alpha_n - \beta_n)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = 0.$$

Из утверждения задачи 3 выводим, что $\alpha_n = \beta_n$. Следовательно, $a_n = [\alpha_n] = [\beta_n] = b_n$, что противоречит сделанному выше предположению. $\triangleleft$

Заметим, что для рационального числа $\alpha = [a_0, a_1, \ldots, a_N]$ при $a_N > 1$ имеется еще одно разложение в непрерывную дробь $\alpha = [a_0, a_1, \ldots, a_{N-1}, a_N - 1, 1]$. Если же $a_N = 1$, то $[a_0, \ldots, a_{N-1}, a_N] = [a_0, \ldots, a_{N-1} + 1]$. Следовательно, для рационального числа существуют два разложения в непрерывную дробь: длина дроби N в одном случае четное число, а в другом — нечетное. В случае же иррационального числа α при любом $n \geqslant 1$ имеем $\alpha_n > 1, a_n = [\alpha_n]$.

8. Для любого иррационального числа α при $n \geqslant 1$ справедливо равенство

$$q_n\alpha - p_n = \frac{(-1)^n\delta_n}{q_{n+1}}, \quad 0 < \delta_n < 1,$$

причем последовательность δ_n/q_{n+1} — убывающая.

Если же α — рациональное число, то при $1 \leqslant n \leqslant N-2$, где N — длина непрерывной дроби, имеет место то же утверждение, и $\delta_{N-1} = 1$.

▷ Используя утверждение задачи 6, имеем цепочку равенств

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = -\frac{p_nq_{n-1} - p_{n-1}q_n}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \\ = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}.$$

Следовательно,

$$\delta_n = \frac{q_{n+1}}{\alpha_{n+1}q_n + q_{n-1}} = \frac{a_{n+1}q_n + q_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}.$$

Поскольку $a_n < \alpha_n < a_n + 1$ при иррациональном α и при $1 \leqslant n \leqslant N-2$ при рациональном α, получим неравенство $0 < \delta_n < 1$. Далее докажем, что последовательность δ_n/q_{n+1} убывает. Имеем цепочку соотношений

$$\frac{\delta_n}{q_{n+1}} = \frac{1}{\alpha_{n+1}q_n + q_{n-1}} \geqslant \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} = \\ = \frac{1}{q_{n+1} + q_n} \geqslant \frac{1}{a_{n+2}q_{n+1} + q_n} = \frac{1}{q_{n+2}} > \frac{\delta_{n+1}}{q_{n+2}}. \quad \triangleleft$$

9. Пусть α — иррациональное число. Тогда предел при $n \to \infty$ подходящих дробей p_n/q_n равен α.

▷ Настоящее утверждение прямо следует из утверждения предыдущей задачи. ◁

10. Пусть α — вещественное число. Тогда для подходящих дробей p_n/q_n справедливо неравенство

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_nq_{n+1}}.$$

Если $\alpha = p_{n+1}/q_{n+1}$, то неравенство обращается в равенство.

▷ Утверждение непосредственно следует из утверждений задач 9 и 3. ◁

11. Известно следующее разложение числа π в непрерывную дробь

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 21, 31, 14, 2, 1, 2, 2, 2, 2, 84, 2, 1, 1, 15, 3, 13, \dots].$$

Тогда имеем следующую таблицу:

n		0	1	2	3	4	5	6	7	8
a_n		3	7	15	1	292	1	1	1	21
p_n	1	3	22	333	355	103993	104348	208341	312689	6774810
q_n	0	1	7	106	113	33102	33215	66317	99532	2156489

Кроме того, справедливо неравенство

$$\left|\pi - \frac{312689}{99532}\right| < \frac{1}{99532 \cdot 2156489} < \frac{1}{2 \cdot 10^{11}}.$$

▷ Таблица составлена применением формулы задачи 2. Неравенство следует из утверждения задачи 10. ◁

Рациональное число a/b, $(a,b) = 1$, $b \geqslant 1$ называется наилучшим приближением к числу α, если для любой дроби c/d, $(c,d) = 1$ с условиями $\frac{c}{d} \neq \frac{a}{b}$, $1 \leqslant d \leqslant b$ выполняется неравенство

$$|d\alpha - c| > |b\alpha - a|.$$

12. Всякое наилучшее рациональное приближение к вещественному числу есть его подходящая дробь.

▷ Пусть дробь a/b — будет наилучшее рациональное приближение к числу $\alpha = [a_0, a_1, a_2, \dots]$, и пусть a/b не совпадает ни с одной подходящей дробью p_n/q_n, $n \geqslant 0$, числа α.

Возможны следующие случаи расположения числа a/b:

$$1)\ \frac{a}{b} < \frac{p_0}{q_0} = a_0, \quad 2)\ \frac{p_0}{q_0} \leqslant \frac{a}{b} \leqslant \frac{p_1}{q_1}, \quad 3)\ \frac{a}{b} > \frac{p_1}{q_1}.$$

В случае 1) имеем $a/b < a_0 = [\alpha] \leqslant \alpha$. Следовательно, поскольку $b \geqslant 1$, справедливы неравенства

$$0 \leqslant \alpha - a_0 < \alpha - \frac{a}{b} \leqslant b\alpha - a.$$

Таким образом число a/b не является наилучшим приближением к числу α, что противоречит предположению и поэтому случай 1) невозможен.

Рассмотрим случай 2). Имеем, что дробь a/b не совпадает ни с одной из подходящих дробей и заключена между подходящими дробями p_{k-1}/q_{k-1} и p_{k+1}/q_{k+1} с номерами одинаковой четности.

При $p_{k-1}/q_{k-1} < p_{k+1}/q_{k+1}$ справедливы неравенства

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{|aq_{k-1} - bp_{k-1}|}{bq_{k-1}} \geqslant \frac{1}{bq_{k-1}},$$

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}.$$

Отсюда следует, что $b > q_k$.

Далее, имеем

$$\left|\alpha - \frac{a}{b}\right| \geqslant \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geqslant \frac{1}{bq_{k+1}},$$

т.е. $|b\alpha - a| \geqslant 1/q_{k+1}$.

С другой стороны, по утверждению задачи 8 находим $|q_k\alpha - p_k| < 1/q_{k+1}$.

Следовательно, получим $|q_k\alpha - p_k| < |b\alpha - a|$. Это противоречит тому, что дробь a/b является наилучшим приближением числа α.

Если же $p_{k-1}/q_{k-1} > p_{k+1}/q_{k+1}$, то вместо дроби p_{k-1}/q_{k-1} следует взять дробь p_{k+1}/q_{k+1} и провести те же рассуждения. Получим, что $b > q_k$, и рассуждения, подобные предыдущим, приводят к противоречию. Тем самым случай 2) невозможен.

Рассмотрим, теперь, случай 3). Имеем $\frac{a}{b} > \frac{p_1}{q_1} \geqslant \alpha$. Следовательно, получим

$$\left|\alpha - \frac{p_1}{q_1}\right| > \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geqslant \frac{1}{bq_1},$$

т.е. $|b\alpha - a| > 1/q_1 = 1/a_1$.

Из определения непрерывной дроби находим $|\alpha - a_0| \leqslant 1/a_1$. Следовательно, $|b\alpha - a| > |\alpha - a_0|$. Это вновь противоречит тому, что дробь a/b является наилучшим приближением числа α.

Таким образом, ни один из рассматриваемых случаев невозможен, что и доказывает утверждение задачи. ◁

13. Всякая подходящая дробь с номером $n \geqslant 1$ вещественного числа является его наилучшим приближением, за исключением числа $\alpha = a + \frac{1}{2}$, где a — любое целое число.

▷ Проведем индукцию по номеру подходящей дроби. При $\alpha = a + \frac{1}{2}$ и целом a имеем $\frac{p_0}{q_0} = a$, $\frac{p_1}{q_1} = a + \frac{1}{2} = \alpha$. Следовательно,

$$\left|\alpha - \frac{p_0}{q_0}\right| = |\alpha - (a+1)|,$$

т.е. число $a+1$, не являющееся подходящей дробью, будет также наилучшим приближением α. Тем не менее, подходящая дробь $p_1/q_1 = \alpha$ будет наилучшим рациональным приближением числа α при $n = 1$.

При $\alpha < [\alpha] + \frac{1}{2}$ любое целое число, отличное от $p_0/q_0 = [\alpha]$, отстоит от него на расстояние, большее, чем $1/2$, т.е. не будет наилучшим приближением. Следовательно, дробь p_0/q_0 будет наилучшим приближением при $n = 0$.

При $\alpha > [\alpha] + \frac{1}{2}$ имеем $\frac{p_1}{q_1} = [\alpha] + 1, q_1 = 1$, и подходящая дробь с номером $n = 1$ числа α является наилучшим рациональным приближением.

Предположим, что утверждение верно при $n = m-1$, где $m \geqslant 1$ при $\alpha < [\alpha] + \frac{1}{2}$ и $m \geqslant 2$ при $\alpha \geqslant [\alpha] + \frac{1}{2}$. Докажем утверждение при $n = m$. Для любого $q \leqslant q_{m-1}$ и любого целого числа pпо предположению индукции имеем $|q_{m-1}\alpha - p_{m-1}| < |q\alpha - p|$. Далее покажем, что $|q_m\alpha - p_m| < |q_{m-1}\alpha - p_{m-1}|$, поэтому достаточно рассмотреть случай, когда $q_{m-1} < q \leqslant q_m$.

Пусть сначала $q = q_m$. Рассмотрим случай $q_{m+1} = 2$. Тогда по утверждению задачи 3 имеем $m = 1$ и $q_2 = a_1a_2+1 = 2$. Следовательно, $a_1 = a_2 = 1$, $\frac{p_1}{q_1} = a_0+1$, $\frac{p_2}{q_2} = a_0+\frac{1}{2}$, и для величины α справедливо неравенство $a_0+\frac{1}{2} < \alpha < a_0+1$. Таким образом, при $1 \leqslant q \leqslant q_1 = 1$ получим при любом целом числе z $\left|\alpha - \frac{p_1}{q_1}\right| < \frac{1}{2} < |\alpha - z|$, т.е. подходящая дробь p_1/q_1 является наилучшим приближением к числу α.

Пусть, теперь, $q_{m+1} > 2$. Тогда для любого $p \neq p_m$ и $q = q_m$ имеем неравенство $\left|\frac{p_m}{q_m} - \frac{p}{q}\right| \geqslant \frac{1}{q_m}$. Кроме того, из утверждения задачи 10 получим

$$\left|\alpha - \frac{p_m}{q_m}\right| \leqslant \frac{1}{q_m q_{m+1}} < \frac{1}{2q_m}.$$

Следовательно,

$$\left|\alpha - \frac{p}{q}\right| \geqslant \left|\frac{p}{q} - \frac{p_m}{q_m}\right| - \left|\frac{p_m}{q_m} - \alpha\right| \geqslant \frac{1}{q_m} - \left|\alpha - \frac{p_m}{q_m}\right| > \left|\alpha - \frac{p_m}{q_m}\right|,$$

т.е. дробь p_m/q_m может являться наилучшим приближением числа α.

Рассмотрим оставшийся случай $q_{m-1} < q < q_m$. Представим p и q в виде следующей линейной комбинации векторов (p_{m-1}, q_{m-1}) и (p_m, q_m) с неизвестными коэффициентами u и v. Имеем

$$\begin{cases} up_m + vp_{m-1} = p, \\ uq_m + vq_{m-1} = q. \end{cases}$$

Решая эту систему уравнений и используя утверждение задачи 3, находим $u = (-1)^{m-1}(pq_{m-1} - qp_{m-1}) \neq 0$, $v = (-1)^{m-1}(pq_m - qp_m) \neq 0$. Поскольку $q_m > q = uq_m + vq_{m-1}$, целые числа u и v имеют противоположные знаки. Далее по утверждению задачи 8 выражения $q_m\alpha - p_m$ и $q_{m-1}\alpha - p_{m-1}$ имеют разные знаки, следовательно, выражения $u(q_m\alpha - p_m)$ и $v(q_{m-1}\alpha - p_{m-1})$ имеют одинаковый знак. Таким образом, находим

$$q\alpha - p = u(q_m\alpha - p_m) + v(q_{m-1}\alpha - p_{m-1}).$$

Отсюда и из утверждения задачи 8 получим

$$|q\alpha - p| > |q_{m-1}\alpha - p_{m-1}| > |q_m\alpha - p_m|.\triangleleft$$

Пусть заданы вещественное число α и рациональное число p/q, $(p,q) = 1$, $q \geqslant 1$ с условием $0 < \alpha - \frac{p}{q} = \frac{\theta}{q^2}$. Разложим число p/q в непрерывную дробь при $\theta > 0$ с нечетным числом неполных частных и при $\theta < 0$ с четным числом неполных частных. Пусть p'/q' обозначает предпоследнюю подходящую дробь в этой непрерывной дроби.

14. (Лежандр). Для того чтобы число p/q было подходящей дробью числа α, необходимо и достаточно, чтобы выполнялось неравенство $|\theta| \leqslant \frac{q}{q+q'}$.

$\triangleright$ *Необходимость.* Пусть $\alpha = [a_0, a_1, a_2, \dots]$ — разложение числа α в непрерывную дробь и $\frac{p}{q} = \frac{p_k}{q_k}$ есть k-я подходящая дробь этого числа. Тогда имеем $\frac{p'}{q'} = \frac{p_{k-1}}{q_{k-1}}$. Следовательно, из утверждения задачи 6 получим

$$\alpha - \frac{p}{q} = \frac{p\alpha_k + p'}{q\alpha_k + q'} - \frac{p}{q} = \frac{p'q - pq'}{q(q\alpha_k + q')} = \frac{(-1)^k}{q(q\alpha_k + q')} = \frac{\theta}{q^2}.$$

Поскольку $\alpha_k \geqslant 1$, отсюда находим неравенство

$$|\theta| = \frac{q}{q\alpha_k + q'} \leqslant \frac{q}{q + q'}.$$

Достаточность. По условию имеем $|\theta| \leqslant qq + q'$. Рассмотрим указанное выше разложение числа $\frac{p}{q} = [a_0, a_1, \dots, a_k]$ в непрерывную дробь, $\frac{p'}{q'} = [a_0, a_1, \dots, a_{k-1}]$ — предпоследняя дробь в этом разложении. Тогда получим $pq' - p'q = (-1)^{k-1}$.

Пусть число α_k определяется из уравнения $\alpha = \frac{p\alpha_k + p'}{q\alpha_k + q'}$. Тогда находим

$$\alpha - \frac{p}{q} = \frac{p\alpha_k + p'}{q\alpha_k + q'} - \frac{p}{q} = \frac{p'q - pq'}{q(q\alpha_k + q')} = \frac{(-1)^k}{q(q\alpha_k + q')} = \frac{\theta}{q^2}.$$

Отсюда и из условия задачи имеем

$$|\theta| = \frac{q}{q\alpha_k + q'} \leqslant \frac{q}{q + q'}.$$

Следовательно, $\alpha_k \geqslant 1$. Поскольку имеем равенство $\alpha = [a_0, a_1, \dots, a_k, \alpha_k]$, где $\alpha_k \geqslant 1$, находим, что α_k — полное частное числа α, а p/q — подходящая дробь в разложении числа α в непрерывную дробь. $\triangleleft$

15. Пусть справедливы неравенства $0 < \left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{2q^2}$. Тогда рациональное число p/q является подходящей дробью числа α.

▷ Неравенство $|\theta| \leqslant \frac{q}{q+q'}$ предыдущей задачи будет выполнено, если $|\theta| \leqslant \frac{1}{2}$, поскольку $q' \leqslant q$. Это означает, что выполнено неравенство $\alpha - \frac{p}{q} \leqslant \frac{1}{2q^2}$. Итак, по утверждению предыдущей задачи число p/q будет подходящей дробью числа α. ◁

16. При $k \geqslant 1$ по крайней мере для одной из двух последовательных подходящих дробей $\frac{p}{q} = \frac{p_k}{q_k}$ и $\frac{p_{k+1}}{q_{k+1}}$ числа α выполняется следующее неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$.

▷ Предположим противное, т.е. выполняются неравенства

$$\left|\alpha - \frac{p_k}{q_k}\right| \geqslant \frac{1}{2q_k^2}, \quad \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| \geqslant \frac{1}{2q_{k+1}^2}.$$

Подходящие дроби p_k/q_k и p_{k+1}/q_{k+1} числа α на числовой оси лежат по разные стороны от этого числа α. Имеем цепочку соотношений

$$\frac{1}{q_k q_{k+1}} = \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \left|\frac{p_{k+1}}{q_{k+1}} - \alpha\right| + \left|\alpha - \frac{p_k}{q_k}\right| \geqslant \frac{1}{2q_k^2} + \frac{1}{2q_{k+1}^2}.$$

Отсюда следует, что $(q_{k+1} - q_k)^2 \leqslant 0$, т.е. $q_{k+1} = q_k$. Это равенство невозможно при $k \geqslant 1$. ◁

17. При $k \geqslant 1$ по крайней мере для одной из трех последовательных подходящих дробей $\frac{p}{q} = \frac{p_k}{q_k}$, $\frac{p_{k+1}}{q_{k+1}}$ и $\frac{p_{k+2}}{q_{k+2}}$ числа α выполняется следующее неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$.

▷ Предположим противное, т.е. при $n = k, k{+}1, k{+}2$ выполняются неравенства

$$\left|\alpha - \frac{p_n}{q_n}\right| \geqslant \frac{1}{\sqrt{5}q_n^2}.$$

Используя утверждение задачи 6, при $n = k, k{+}1, k{+}2$ имеем цепочку равенств

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right| =$$

$$= \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})},$$

где $\beta_{n+1} = q_{n-1}/q_n$.

Отсюда при $m = k-1, k, k+1$ находим $\alpha_m + \beta_m \leqslant \sqrt{5}$. Далее воспользуемся равенствами

$$\alpha_m = a_m + \frac{1}{\alpha_{m+1}}, \quad \frac{1}{\beta_m} = \frac{q_{m-1}}{q_{m-2}} = \frac{a_{m-1}q_{m-2} + q_{m-3}}{q_{m-2}} = a_{m-1} + \beta_{m-1}.$$

При $m = k, k+1$ получим

$$\frac{1}{\alpha_m} + \frac{1}{\beta_m} = \alpha_{m-1} + \beta_{m-1} \leqslant \sqrt{5}.$$

Следовательно,

$$1 = \frac{1}{\alpha_m}\alpha_m \leqslant \left(\sqrt{5} - \frac{1}{\beta_m}\right)(\sqrt{5} - \beta_m),$$

т.е. $\beta_m + 1/\beta_m \leqslant \sqrt{5}$. Так как β_m рациональное число, то в предыдущем неравенстве выполняется строгое неравенство. Воспользовавшись также тем, что $\beta_m < 1$, имеем $\beta_m > \frac{1}{2}(\sqrt{5} - 1)$.

Далее имеем

$$a_k = \frac{1}{\beta_{k+1}} - \beta_k < \sqrt{5} - \beta_{k+1} - \beta_k < \sqrt{5} - 2\frac{\sqrt{5}-1}{2} = 1.$$

Это противоречит тому, что $a_k \geqslant 1$. ◁

18. Для любого иррационального числа α существует бесконечная последовательность p/q подходящих дробей числа α, удовлетворяющих неравенству

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

▷ Это утверждение прямое следствие предыдущей задачи. ◁

19. Для числа $\alpha = \frac{\sqrt{5}+1}{2}$ при $A > \sqrt{5}$ неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$$

имеет только конечное число решений.

Другими словами, константа $A = \sqrt{5}$ в предыдущей задаче является наилучшей возможной.

▷ Пусть справедливы соотношения

$$\alpha = \frac{p}{q} + \frac{\delta}{q^2}, \quad |\delta| < \frac{1}{A} < \frac{1}{\sqrt{5}}.$$

Тогда имеем

$$\frac{\delta}{q} - \frac{q}{2}\sqrt{5} = \frac{q}{2} - p.$$

Возводим это равенство в квадрат. Находим

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = \left(\frac{q}{2} - p\right)^2 - \frac{5q^2}{4} = p^2 - pq - q^2.$$

При достаточно большом q получим

$$\left|\frac{\delta^2}{q^2} - \delta\sqrt{5}\right| < 1.$$

Следовательно, $p^2 - pq - q^2 = 0$, т.е. $(2p-q)^2 = 5q^2$, что невозможно. ◁

Имеется гипотеза о том, что для всякого алгебраического числа его неполные частные ограничены. В силу периодичности непрерывной дроби для квадратичной иррациональности эта гипотеза справедлива для таких чисел. С другой стороны, Г. Давенпорт [14] доказал, что для любого сколь угодно большого числа M найдется иррациональное алгебраическое число, отличное от квадратичной иррациональности, такое, что бесконечная последовательность его неполных частных превосходит M. Более точно его результат формулируется следующим образом.

20. Пусть θ — любое иррациональное число, $P > 2$ — любое большое простое число. Тогда, по крайней мере, одно из чисел

$$P^2\theta,\ \theta,\ \theta + \frac{1}{P},\ \ldots,\ \theta + \frac{P-1}{P}$$

имеет для бесконечного множества номеров n неполные частные a_n, превосходящие $P - 2$.

▷ По утверждению задачи 8 для иррационального числа $P\theta$ имеем

$$P\theta - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n((P\theta)_{n+1}q_n + q_{n-1})},$$

где символ $(P\theta)_{n+1}$ обозначает $(n+1)$-й остаток (полное частное) при разложении числа $P\theta$ в непрерывную дробь.

Следовательно,

$$\left|P\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Если q_n делится на P для бесконечного множества номеров n, то $q_n = Pq'_n$. Тогда для бесконечного множества рациональных приближений $\frac{p_n}{q'_n}$ к числу $P^2\theta$ справедливо неравенство

$$\left|P^2\theta - \frac{p_n}{q'_n}\right| < \frac{1}{P(q'_n)^2}.$$

Поскольку $P > 2$, по утверждению задачи 15 имеем, что p_n/q'_n является подходящей дробью иррационального числа $P^2\theta$. Далее, из утверждения задачи 8 для иррационального числа $P^2\theta$ находим

$$P^2\theta - \frac{p_n}{q'_n} = \frac{(-1)^n}{q'_n(\alpha_{n+1}q'_n + q'_{n-1})},$$

где символ α_{n+1} обозначает остаток (полное частное) при разложении числа $P^2\theta$ в непрерывную дробь, отвечающий подходящей дроби p_n/q'_n.

Таким образом получим неравенство

$$\frac{1}{q'_n(\alpha_{n+1}q'_n + q'_{n-1})} < \frac{1}{P(q'_n)^2}.$$

Воспользуемся тем, что $1 \leqslant a_{n+1} \leqslant \alpha_{n+1} < a_{n+1} + 1$. Тогда из предыдущего неравенства имеем

$$Pq'_n < \alpha_{n+1}q'_n + q'_{n-1} < (a_{n+1} + 2)q'_n.$$

Следовательно, $(n+1)$-е неполное частное a_{n+1} числа $P^2\theta$ превосходит $P - 2$.

Пусть, теперь, для всех достаточно больших номеров n знаменатели q_n подходящих дробей p_n/q_n числа $P\theta$ взаимно просты с P. Определим целые числа A_n из сравнения $p_n \equiv A_n q_n \pmod P$, $0 \leqslant A_n < P$. По крайней мере одно из чисел $0, 1, \ldots, P - 1$ бесконечно часто встречается как A_n. Обозначим это число буквой A. Тогда для указанных номеров n при некотором целом числе r_n имеем $p_n = Aq_n + Pr_n$.

Таким образом получим

$$\left|\theta - \frac{A}{P} - \frac{r_n}{q_n}\right| < \frac{1}{Pq_n^2}.$$

Отсюда имеем, что r_n/q_n является подходящей дробью числа $\theta - \frac{A}{P}$, и бесконечное множество неполных частных этого числа превосходит $P - 2$. ◁

§ 10. Арифметика квадратичных полей. Метод Лемера распознавания простых чисел

Целые числа из кольца $\mathbf{Z}$ будем называть целыми рациональными числами. Пусть $\mathbf{Q}$ — поле рациональных чисел. Рассмотрим D — бесквадратное целое рациональное число. Множество всех чисел α вида $\alpha = r + s\sqrt{D}$ с рациональными числами r и s образует поле $\mathbf{Q}(\sqrt{D})$ — квадратичное расширение поля рациональных чисел.

Числа α из $\mathbf{Q}(\sqrt{D})$, удовлетворяющие уравнению

$$z^2 + pz + q = 0$$

с целыми рациональными коэффициентами p и q, называются целыми в поле $\mathbf{Q}(\sqrt{D})$. Положим

$$\rho = \begin{cases} \sqrt{D}, & \text{если} \quad D \equiv 2 \quad \text{или} \equiv 3 \pmod 4, \\ (1 + \sqrt{D})/2, & \text{если} \quad D \equiv 1 \pmod 4. \end{cases}$$

1. Любое целое число α из $\mathbf{Q}(\sqrt{D})$ имеет вид $\alpha = r + s\rho$, где r и s — целые рациональные числа.

▷ По теореме Виета число $\alpha = r + s\sqrt{D}$ будет целым числом из $\mathbf{Q}(\sqrt{D})$, тогда и только тогда, когда $\alpha + \bar{\alpha} = 2r = m$ и $\alpha\bar{\alpha} = r^2 - Ds^2$ являются целыми рациональными числами. Поскольку $\frac{m^2}{4} - Ds^2$ — целое рациональное число и число D свободно от квадратов, рациональное число s в представлении в виде несократимой дроби в знаменателе может иметь только 2, т.е. $s = n/2$, $n \in \mathbf{Z}$ и число $(m^2 - Dn^2)/4$ является целым рациональным.

Так как число D свободно от квадратов, то $D \not\equiv 0 \pmod 4$. Возможны два случая: 1) $D \equiv 1 \pmod 4$ и 2) $D \equiv 2$ или $\equiv 3 \pmod 4$.

Сначала рассмотрим случай 1) $D \equiv 1 \pmod 4$. Имеем $m^2 \equiv n^2 \pmod 4$. Это эквивалентно $m \equiv n \pmod 2$. Следовательно, $m = n + 2k$. Отсюда при целых рациональных k и n получим

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{D} = k + n\frac{1+\sqrt{D}}{2} = k + n\rho.$$

Это означает, что в случае $D \equiv 1 \pmod 4$ в качестве базиса в кольце целых поля $\mathbf{Q}(\sqrt{D})$ можно взять числа 1 и $\rho = \frac{1+\sqrt{D}}{2}$.

Рассмотрим случай 2) $D \equiv 2$ или $\equiv 3 \pmod 4$. Поскольку выполняется сравнение $m^2 - Dn^2 \equiv 0 \pmod 4$, число n не может быть нечетным. Действительно, тогда имели бы $D \equiv m^2 \pmod 4$, т.е. либо $D \equiv 0 \pmod 4$ при четном m, либо $D \equiv 1 \pmod 4$ при нечетном m, что не так. Пусть теперь n — четное число. Тогда $m^2 \equiv 0 \pmod 4$. Следовательно, m — четное число. Таким образом, в случае 2) $D \equiv 2$ или $\equiv 3 \pmod 4$ в качестве базиса кольца целых поля $\mathbf{Q}(\sqrt{D})$ можно взять числа 1 и $\rho = \sqrt{D}$. ◁

Число $\alpha + \bar{\alpha} = \mathrm{Sp}(\alpha)$ называется следом числа α, а число $\alpha\bar{\alpha} = N(\alpha)$ — нормой этого числа.

Пусть $\alpha = r + s\rho \in \mathbf{Q}(\sqrt{D})$. Тогда

$$N(\alpha) = \begin{cases} r^2 - Ds^2, & \text{если} \quad D \equiv 2 \quad \text{или} \quad \equiv 3 \pmod 4, \\ r^2 + rs + \frac{1-D}{4}s^2, & \text{если} \quad D \equiv 1 \pmod 4. \end{cases}$$

Как функция от α след $\mathrm{Sp}(\alpha)$ является линейной функцией, т.е.

1) для любых $\alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D})$ имеем $\mathrm{Sp}(\alpha_1 + \alpha_2) = \mathrm{Sp}(\alpha_1) + \mathrm{Sp}(\alpha_2)$,

2) для любого $c \in \mathbf{Q}$ имеем $\mathrm{Sp}(c\alpha) = c\,\mathrm{Sp}(\alpha)$,

а функция норма $N(\alpha)$ числа α является мультипликативной:

1) для любых $\alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D})$ имеем $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$,

2) $N(\alpha) = 0$ тогда и только тогда, когда $\alpha = 0$.

Целое число ε поля $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ называется единицей, если ε делит число 1.

2. Целое число ε из $\mathbf{F}$ будет единицей тогда и только тогда, когда $N(\varepsilon) = \pm 1$.

▷ *Необходимость.* Пусть $\varepsilon \in \mathbf{F}$ — целое число и $\varepsilon \mid 1$. Тогда найдется целое число η такое, что $\varepsilon\eta = 1$. Следовательно, $N(\varepsilon\eta) = N(\varepsilon)N(\eta) = 1$. Отсюда находим, что $N(\varepsilon) = \pm 1$.

Достаточность. Так как ε — целое число поля $\mathbf{F}$, то число ε удовлетворяет уравнению с целыми рациональными коэффициентами

$$\varepsilon^2 - \mathrm{Sp}(\varepsilon)\varepsilon + N(\varepsilon) = 0.$$

Отсюда имеем, что

$$\bar{\varepsilon} = \frac{N(\varepsilon)}{\varepsilon} = -\varepsilon + \mathrm{Sp}(\varepsilon) \in \mathbf{F}$$

является целым числом в $\mathbf{F}$. Далее, поскольку $N(\varepsilon) = \varepsilon\bar{\varepsilon} = \pm 1$, число ε будет делителем единицы. ◁

3. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — мнимое квадратичное поле ($D < 0$). Тогда множество всех единиц этого поля является конечной циклической группой порядка w, причем

$$w = \begin{cases} 6, & \text{если} \quad D = -3, \\ 4, & \text{если} \quad D = -1, \\ 2 & \text{в остальных случаях.} \end{cases}$$

▷ По утверждению задачи 3 целое число ε является единицей тогда и только тогда, когда $N(\varepsilon) = \pm 1$. Целое число ε можно представить в виде $\varepsilon = r + s\rho$, где r и s — целые рациональные числа.

Пусть $D \equiv 2$ или $\equiv 3 \pmod 4$. Тогда $\rho = \sqrt{D}$ и

$$0 < N(s + r\rho) = r^2 - Ds^2 = 1.$$

Рассмотрим сначала случай $D = -1$. Уравнение $r^2 + s^2 = 1$ имеет четыре решения $(r, s) = (\pm 1, 0), (0, \pm 1)$, которым отвечают единицы ± 1, $\pm i$ и число i является образующей группы четвертого порядка.

Пусть $|D| > 1$. Тогда $s = 0$, поскольку в противном случае $1 = r^2 - Ds^2 \geqslant |D| > 1$. Следовательно, в этом случае имеется только две единицы ± 1.

Пусть, теперь, $D \equiv 1 \pmod 4$. Тогда $\rho = \frac{1+\sqrt{D}}{2}$ и $N(r + s\rho) = r^2 + rs + s^2\frac{1-D}{4}$.

Рассмотрим сначала случай $D = -3$. Тогда уравнение $0 < N(r + s\rho) = r^2 + rs + s^2 = 1$ в целых r и s имеет 6 решений $(r, s) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)$. Этим решениям отвечают единицы

$$\pm 1, \quad \pm i, \quad \omega = \frac{1 - \sqrt{D}}{2}, \quad -\omega.$$

Число $-\omega = \frac{-1+\sqrt{D}}{2}$ является первообразным корнем 6-й степени из единицы и образующей группы единиц.

Пусть $|D| \geqslant 4$. Тогда $s = 0$, поскольку в противном случае при $|D| > 4$ имеем

$$N(r + s\rho) = r^2 + rs + s^2\frac{1-D}{4} \geqslant \frac{-D}{4} = \frac{|D|}{4} > 1,$$

и при $D = -4$

$$N(r + s\rho) = r^2 + rs + s^2\frac{5}{4} \geqslant \frac{5}{4} > 1.$$

Следовательно, уравнение $N(r+s\rho) = \pm 1$ имеем два решения $(r, s) = (\pm 1, 0)$. Им отвечают единицы ± 1. ◁

4. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — вещественное квадратичное поле ($D > 0$). Тогда существует нетривиальная единица этого поля, отличная от ± 1.

▷ Докажем сначала, что для любого натурального числа m существует ненулевое целое число α из поля $\mathbf{F}$ такое, что

$$|\alpha| < 1/m, \quad |N(\alpha)| < 1 + \sqrt{D}.$$

Любое целое число α можно представить в виде $\alpha = x + y\rho$ с целыми рациональными числами x и y. По лемме Дирихле целое число x и натуральное число y, не превосходящее m, такие, что $|\alpha| = |x + y\rho| < 1/m$. Так как $y \neq 0$, то и $\alpha \neq 0$.

Далее оценим сопряженное число к α. Имеем цепочку соотношений

$$\bar{\alpha} = x + y\bar{\rho} = (x + y\rho) + y(\bar{\rho} - \rho) = \alpha + y\sqrt{D}.$$

Следовательно,

$$|\bar{\alpha}| \leqslant |\alpha| + |y|\sqrt{D} \leqslant \frac{1}{m} + m\sqrt{D}.$$

Таким образом, находим

$$|N(\alpha)| = |\alpha\bar{\alpha}| < \frac{1}{m^2} + \sqrt{D} < 1 + \sqrt{D}.$$

Отсюда получим, что существует бесконечно много целых $\alpha \neq 0$ и таких, что $|N(\alpha)| < 1 + \sqrt{D}$. Поэтому найдется натуральное число $m < 1 + \sqrt{D}$ такое, что для бесконечного множества целых $\alpha \neq 0$ выполняется равенство $|N(\alpha)| = m$.

Далее разобьем все числа $\alpha = x + y\rho$ на классы вычетов по модулю m следующим образом: в один класс попадут все числа α с одинаковыми остатками при делении на m чисел x и чисел y, т.е.

для любой пары чисел $(r, s), 0 \leqslant r, s < m$, в один класс попадут числа с условием $x \equiv r \pmod m, y \equiv s \pmod m$. Таких классов будет ровно m^2. Для чисел α, β из одного класса имеем $\alpha \equiv \beta \pmod m$.

Отсюда находим, что найдутся два различных ненулевых целых α, β, удовлетворяющие условиям

$$|N(\alpha)| = |N(\beta)| = m, \alpha \equiv \beta \pmod m.$$

Домножив последнее сравнение на $\bar{\beta}$, получим

$$\alpha\bar{\beta} \equiv N(\beta) \equiv 0 \pmod m,$$

т.е. $\alpha\bar{\beta} = m\varepsilon$ при некотором целом ε из bfF.

Разделим последнее равенство на $N(\beta)$. Имеем $\frac{\alpha}{\beta} = \pm\varepsilon$. Поскольку $|N(\alpha)| = |N(\beta)|$, находим $N(\varepsilon) = \pm 1$. По утверждению задачи 3 целое число ε является единицей кольца целых поля $\mathbf{F}$ тогда и только тогда, когда $N(\varepsilon) = \pm 1$.

Таким образом число ε является единицей, причем нетривиальной, поскольку $\alpha \neq \pm\beta$. ◁

Нетривиальные единицы поля $\mathbf{F}$ можно объединить в группы по четыре: $\varepsilon, \bar{\varepsilon}, -\varepsilon, -\bar{\varepsilon}$. Тогда одна из них будет удовлетворять условию $\varepsilon > 1$. Наименьшую среди нетривиальных единиц ε_1 с условием ε_1 назовем основной единицей поля $\mathbf{F}$.

5. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — вещественное квадратичное поле ($D > 0$). Тогда группа единиц кольца целых этого поля $\mathbf{F}$ есть прямое произведение группы второго порядка, состоящей из единиц ± 1 и бесконечной циклической группы.

Другими словами, существует ε_1 — основная единица поля $\mathbf{F}$ такая, что для любой единицы ε кольца целых поля $\mathbf{F}$ найдутся целые числа $\nu = 0, 1$ и n имеет место представление

$$\varepsilon = (-1)^\nu \varepsilon_1^n.$$

▷ Без ограничения общности можно считать, что $\varepsilon > 1$, поскольку в противном случае ее следует заменить на одну из единиц вида $\pm\varepsilon^{\pm 1}$.

Далее, найдется единственное натуральное число n такое, что

$$\varepsilon_1^n \leqslant \varepsilon < \varepsilon_1^{n+1}.$$

Отсюда имеем

$$1 \leqslant \frac{\varepsilon}{\varepsilon_1^n} < \varepsilon_1,$$

что в силу минимальности $\varepsilon_1 > 1$ возможно только, если $\varepsilon = \varepsilon_1^n$. Таким образом найдено искомое представление $\varepsilon = (-1)^\nu \varepsilon_1^n$, где $\nu = 0, 1$ и n — любое целое рациональное число. ◁

Отметим, что при $D = 2$ основная единица поля $\mathbf{Q}(\sqrt{2})$ равна $\varepsilon_1 = 1 + \sqrt{2}$ и ее норма $N(\varepsilon_1) = \varepsilon_1\bar{\varepsilon_1}$ равна $N(\varepsilon_1) = 1^2 - 2 \cdot 1^2 = -1$,
при $D = 3$ имеем $\varepsilon_1 = 2 + \sqrt{3}$, $N(\varepsilon_1) = 1$,
при $D = 5$ имеем $\varepsilon_1 = \frac{1+\sqrt{5}}{2}$, $N(\varepsilon_1) = -1$.

Перейдем к приложению теории квадратичных полей к распознаванию простоты натуральных чисел.

Пусть многочлен $\lambda^2 - P\lambda + Q$ с целыми коэффициентами P, Q неприводим над полем рациональных чисел $\mathbf{Q}$, и пусть a и $b = \bar{a}$ — корни этого многочлена, при этом число b будет сопряженным числу a. Тогда по теореме Виета имеем $a + b = P, ab = Q$.

При $n \geqslant 0$ определим две последовательности

$$U_n = \frac{a^n - b^n}{a - b}, V_n = a^n + b^n.$$

Очевидно, имеем $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a + b = P$. Последовательности $\{U_n\}, \{V_n\}, n \geqslant 0$, называются последовательностями Люка.

6. При $m \geqslant n \geqslant 0$ справедливы следующие соотношения

$$U_{m+n} = U_m V_n - Q^n U_{m-n}, \quad V_{m+n} = V_m V_n - Q^n V_{m-n};$$
$$U_{m+1} = PU_m - QU_{m-1}, \quad U_0 = 0, \quad U_1 = 1;$$
$$V_{m+1} = PV_m - QV_{m-1}, \quad V_0 = 2, \quad V_1 = P;$$
$$U_{2n} = U_n V_n, \quad U_{2n+1} = U_{n+1}V_n - Q^n;$$
$$V_{2n} = V_n^2 - 2Q^n, \quad V_{2n+1} = V_{n+1}V_n - PQ^n.$$

Пусть, далее, $n = h2^s$, $(h, 2) = 1$, $s \geqslant 0$. Тогда

$$U_n = U_h V_h V_{2h} \dots V_{2^{s-1}h},$$
$$V_n = V_{2^s h} = V_{2^{s-1}h}^2 - 2Q^{2^{s-1}h}, \dots, V_{2h} = V_h^2 - 2Q^h.$$

▷ Искомые тождества проверяются непосредственными вычислениями

$$U_{m+n} = \frac{a^{m+n} - b^{m+n}}{a - b} = \frac{(a^m - b^m)(a^n + b^n)}{a - b} -$$
$$- \frac{(ab)^n(a^{m-n} - b^{m-n})}{a - b} = U_m V_n - Q^n U_{m-n},$$
$$V_{m+n} = a^{m+n} + b^{m+n} = (a^m + b^m)(a^n + b^n) -$$
$$-(ab)^n(a^{m-n} + b^{m-n}) = V_m V_n - Q^n V_{m-n}.$$

Положим в этих равенствах $n = 1$. Получим

$$U_{m+1} = (a + b)U_m - abU_{m-1} = PU_m - QU_{m-1},$$

$$V_{m+1} = (a+b)V_m - abV_{m-1} = PV_m - QV_{m-1}.$$

Следовательно, $\{U_n\}$, $\{V_m\}$ — рекуррентные последовательности второго порядка. Поскольку первые два члена этих последовательностей целые числа, они будут целочисленными последовательностями.

Положим, теперь, $m = n$. Имеем

$$U_{2n} = U_n V_n, \quad V_{2n} = V_n^2 - 2Q^n.$$

Если положим $m = n+1$, то получим

$$U_{2n+1} = U_{n+1}V_n - Q^n, \quad V_{2n+1} = V_{n+1}V_n - PQ^n.$$

Наконец, применяя последовательно, найденные выше тождества, имеем

$$U_n = U_{2^s h} = U_{2^{s-1}h}V_{2^{s-1}h} = \ldots = U_h V_h V_{2h} \ldots V_{2^{s-1}h},$$
$$V_n = V_{2^s h} = V_{2^{s-1}h}^2 - 2Q^{2^{s-1}h}, \ldots, V_{2h} = V_h^2 - 2Q^h. \triangleleft$$

7. Пусть p — нечетное простое число, $N = 2^p - 1$, и пусть задана последовательность $s_1 = 4, s_{k+1} = s_k^2 - 2$ при $k \geqslant 1$. Тогда для простоты числа N необходимо и достаточно, чтобы $s_{p-1} \equiv 0 \pmod N$.

$\triangleright$ *Необходимость.* Дано, что $N = 2^p - 1$ — простое число. Покажем, что $s_{p-1} \equiv 0 \pmod N$. Сначала докажем, что многочлен $P(x) = x^2 - 2^{(p+1)/2}x - 1$ является неприводимым над полем $\mathbf{F}_N$. Так как квадратичный многочлен $ax^2 + bx + c$ будет неприводимым над $\mathbf{F}_N$ тогда и только тогда, когда его дискриминант $\Delta = b^2 - 4ac$ не будет квадратичным вычетом по модулю N, то имеем

$$\Delta = (2^{(p+1)/2})^2 - 4(-1) \equiv (2^{p+1} - 2) + 2 + 4 \equiv 6 \pmod N.$$

Следовательно,

$$\left(\frac{\Delta}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{3}{N}\right).$$

Находим

$$\left(\frac{2}{N}\right) = +1,$$

поскольку $(2^{(p+1)/2})^2 \equiv 2 \pmod N$.

Из квадратичного закона взаимности символа Лежандра имеем

$$\left(\frac{3}{N}\right) = (-1)^{(N-1)/2}\left(\frac{N}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

поскольку $N = 2^p - 1 = (3-1)^p - 1 \equiv 1 \pmod 3$.

Таким образом, $\left(\frac{\Delta}{N}\right) = -1$, и многочлен $P(x)$ неприводим над $\mathbf{F}_N$.

Пусть a и b — корни многочлена $P(x)$. Положим $V(2^k) = a^{2^k} + b^{2^k}$. Имеем, что для любого натурального числа k сумма $V(2^k) \in \mathbf{F}_N$. Докажем индукцией по k, что

$$s_k \equiv V(2^k) \pmod N.$$

При $k = 1$ утверждение справедливо, так как

$$V(2) = a^2 + b^2 = (a+b)^2 - 2ab = (2^{(p+1)/2})^2 - 2(-1) \equiv 4 \pmod N.$$

Предположим утверждение верно при $k = m$, т.е. $s_m \equiv V(2^m) \pmod N$. Докажем справедливость утверждения при $k = m+1$. Имеем

$$s_{m+1} = s_m^2 - 2 \equiv (a^{2^m} + b^{2^m})^2 - 2 =$$
$$= a^{2^{m+1}} + b^{2^{m+1}} + 2a^{2^m}b^{2^m} - 2 \equiv V(2^{m+1}) \pmod N.$$

Следовательно, $s_p \equiv V(2^p) \equiv a^{N+1} + b^{N+1} \equiv -2 \pmod N$, так как $a^{N+1} \equiv b^{N+1} \equiv ab \equiv -1 \pmod N$. Поскольку $s_p = s_{p-1}^2 - 2$, получим $s_{p-1} \equiv 0 \pmod N$.

Достаточность. Предположим противное, т.е. N — составное число и q — наименьший простой делитель N. Тогда $3 \leqslant q \leqslant \sqrt{N}$. Так как $s_{p-1} \equiv 0 \pmod N$, то $s_{p-1} \equiv 0 \pmod q$. Тогда из $s_{p-1} \equiv V(2^{p-1}) \pmod q$ имеем цепочку сравнений

$$a^{2^{p-1}} + b^{2^{p-1}} \equiv 0 \,(\mathrm{mod}\, q), a^{2^p} + (ab)^{2^{p-1}} \equiv 0 \,(\mathrm{mod}\, q), a^{2^p} \equiv -1 \,(\mathrm{mod}\, q).$$

Число a принадлежит полю $\mathbf{F}_{q^2}$, порядок a равен 2^{p+1} и он делит порядок q^2-1 мультипликативной группы поля $\mathbf{F}_{q^2}$, т.е. $2^{p+1} \mid q^2-1$. Последнее невозможно, поскольку $2^{p+1} > n, q^2 \leqslant n$. Это противоречие доказывает, что N — простое число. ◁

8. Пусть $N \geqslant 2$ — натуральное число, $N+1 = \prod\limits_{q \mid N+1} q^{\alpha_q}$ — каноническое разложение числа $N+1$ на простые сомножители, и пусть найдется последовательность Люка U_n с условием $(2QD, N) = 1$, такая, что

$$U_{N+1} \equiv 0 \pmod N,$$

и для любого $q \mid N+1$ выполняется условие

$$(U_{(N+1)/q}, N) = 1.$$

Тогда число N является простым.

▷ Будем рассуждать от противного. Пусть N — составное число и p — наименьший простой делитель числа N. Тогда из условия задачи следует, что $U_{N+1} \equiv 0 \pmod p$ и для любого простого $q \mid N$ выполняется соотношение $U_{(N+1)/q} \not\equiv 0 \pmod p$. Буквой d обозначим наименьшее натуральное число такое, что $U_d \equiv 0 \pmod p$. ◁

§ 11. Разложение вещественных квадратичных иррациональностей в непрерывную дробь. Теорема Эйлера – Лагранжа

Пусть θ — иррациональное число из поля $\mathbf{Q}(\sqrt{D})$. Тогда имеем $\theta = r + s\sqrt{D}$, $r, s \in \mathbf{Q}$, $s \neq 0$. Число θ удовлетворяет однозначно определенному квадратному уравнению вида $a\theta^2 - b\theta - c = 0$ с целыми рациональными взаимно простыми коэффициентами a, b, c и $a > 0$. Поскольку $\theta \in \mathbf{Q}(\sqrt{D})$, его дискриминант равен $b^2 + 4ac = m^2 D$ для некоторого натурального числа m. Число θ называется принадлежащим дискриминанту $m^2 D$. Оно имеет вид

$$\theta = \frac{b \pm m\sqrt{D}}{2a} = \frac{2c}{-b \pm m\sqrt{D}}.$$

Назовем иррациональное число θ приведенным, если $\theta > 1$ и для сопряженного числа θ' справедливо неравенство $-\frac{1}{\theta'} > 1$, т.е. имеем $\theta > 1$, $-1 < \theta' < 0$.

Далее имеем

$$\theta' = \frac{-b \mp m\sqrt{D}}{2a} = \frac{2c}{b \mp m\sqrt{D}}.$$

Следовательно, по теореме Виета получим

$$\frac{b}{a} = \theta + \theta' > 0,\ b > 0; \quad \frac{c}{a} = \theta\theta' = \frac{b^2 - m^2 D}{4a^2} < 0.$$

Отсюда находим $0 < b < m\sqrt{D}$. Поэтому для приведенного числа θ справедливы соотношения

$$\theta = \frac{b + m\sqrt{D}}{2a} = \frac{2c}{-b + m\sqrt{D}} > 1, -1 < \theta' < 0.$$

Тем самым коэффициенты многочлена удовлетворяют неравенствам

$$0 < b < m\sqrt{D}, \quad \frac{-b + m\sqrt{D}}{2} < a, c < \frac{b + m\sqrt{D}}{2}.$$

Это показывает, что a, b, c — натуральные числа с условием $0 < a, b, c < m\sqrt{D}$, т.е. приведенных чисел данного дискриминанта $m^2 D$ существует конечное число.

1. Пусть иррациональное число θ принадлежит дискриминанту $m^2 D$. Тогда этому дискриминанту принадлежат все остатки θ_n разложения числа θ в непрерывную дробь. Более того, начиная с некоторого номера все остатки θ_n будут приведенными числами.

▷ Для справедливости первого утверждения достаточно доказать, что вместе с числом θ дискриминанту $m^2 D$ принадлежит и число θ_1, определяемое соотношением $\theta = a_1 + \frac{1}{\theta_1}$. Подставим вместо θ его

выражение $a_1 + \frac{1}{\theta_1}$ в квадратное уравнение $a\theta^2 - b\theta - c = 0$. Получим относительно новой переменной θ_1 квадратное уравнение

$$(aa_1^2 - ba_1 - c)\theta_1^2 - (b - 2aa_1)\theta_1 + a = 0.$$

Его коэффициенты будут взаимно простыми числами, а дискриминант этого уравнения равен

$$(b - 2aa_1)^2 - 4a(aa_1^2 - ba_1 - c) = b^2 + 4ac = m^2 D.$$

Первое утверждение доказано. Перейдем к доказательству второго утверждения. По определению непрерывной дроби имеем, что $\theta_{n+1} > 1$. Докажем, что, начиная с некоторого номера n, справедливо неравенство $-1/\theta'_{n+1} > 1$.

При $n > 1$, исходя из равенства

$$\theta = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}},$$

получим

$$-\frac{1}{\theta'_{n+1}} = \frac{q_n\theta' - p_n}{q_{n-1}\theta' - p_{n-1}} = \frac{q_n}{q_{n-1}} - \frac{(-1)^n}{q_{n-1}\left(q_{n-1}\theta' - p_{n-1}\right)}.$$

Отсюда при $n > 1$ находим

$$-\frac{1}{\theta'_{n+1}} - 1 = \frac{1}{q_{n-1}}\left((q_n - q_{n-1}) - \frac{(-1)^n}{q_{n-1}\left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)}\right).$$

Далее, при $n \to \infty$ имеем

$$\frac{(-1)^n}{q_{n-1}\left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)} \to 0,$$

поскольку

$$\lim_{n\to\infty} A_n = \theta' - \theta \neq 0,$$

где $A_n = \left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)$.

Следовательно, существует номер n_0 такой, что для всех $n > n_0$ выполняется неравенство $|A_n| \leqslant 1/2$. Поэтому для всех $n > n_0$ имеем

$$-\frac{1}{\theta'_{n+1}} - 1 \geqslant \frac{q_n - q_{n-1} - 0,5}{q_{n-1}} > 0.$$

Тем самым доказано, что, начиная с некоторого номера, все остатки θ_n разложения числа θ в непрерывную дробь являются приведенными числами. ◁

2. (Эйлер – Лагранж). Пусть $\theta > 1$ — вещественная квадратичная иррациональность. Тогда, начиная с некоторого номера, разложение

в непрерывную дробь числа θ будет периодичным. Более того, если θ является приведенным числом, то это разложение будет чисто периодическим.

▷ Пусть иррациональное число $\theta > 1$ принадлежит дискриминанту m^2D. Тогда по утверждению предыдущей задачи этому дискриминанту принадлежат все остатки θ_n разложения числа θ в непрерывную дробь, причем, начиная с некоторого номера n_0, все они будут приведенными числами. Количество приведенных чисел, принадлежащих данному дискриминанту, конечно. Поэтому найдутся натуральные числа $k \geqslant 1$ и $l \geqslant n_0$ такие, что $\theta_l = \theta_{l+k}$. Тогда имеем

$$\theta = [a_0, a_1, \ldots, a_{l-1}, \theta_l] = [a_0, a_1, \ldots, a_{l-1}, a_l, \ldots, a_{l+k-1}, \theta_{l+k}].$$

Отсюда следует, что разложение числа θ в непрерывную дробь будет иметь период $k \geqslant 1$ с непериодической начальной частью этого разложения длины l.

Докажем теперь вторую часть утверждения. Пусть l является минимальным номером, при котором $\theta_l = \theta_{l+k}$. Предположим, что $l \geqslant 1$, т.е. разложение числа θ не чисто периодическая непрерывная дробь. Поскольку θ — приведенное иррациональное число, имеем $\theta > 1$, $-\frac{1}{\theta'} > 1$.

Далее, из определения непрерывной дроби находим

$$\theta_{l-1} = a_{l-1} + \frac{1}{\theta_l}, \quad \theta_{l+k-1} = a_{l+k-1} + \frac{1}{\theta_{l+k}}.$$

Следовательно,

$$-\frac{1}{\theta'_l} = a_{l-1} + (-\theta'_{l-1}), \quad -\frac{1}{\theta'_{l+k}} = a_{l+k-1} + (-\theta'_{l+k-1}).$$

Так как θ — приведенное число, то a_{l-1} и a_{l+k-1} будут целыми частями соответственно чисел $-1/\theta'_l$ и $-1/\theta'_{l+k}$, а $-\theta_{l-1}$ и $-\theta_{l+k-1}$ — остатками этих чисел. Поскольку $\theta'_l = \theta'_{l+k}$, имеем $a_{l-1} = a_{l+k-1}$ и $\theta'_{l-1} = \theta'_{l+k-1}$. Стало быть, $\theta_{l-1} = \theta_{l+k-1}$. Последнее равенство противоречит минимальности выбранного номера l. Таким образом доказано, что $l = 0$ и приведенное иррациональное число θ разлагается в чисто периодическую непрерывную дробь. ◁

3. Пусть вещественное число $\theta > 1$ разлагается в периодическую непрерывную дробь. Тогда θ — квадратичная иррациональность. Кроме того, если непрерывная дробь числа θ — чисто периодическая, то θ — приведенное число. Более того, пусть число θ разлагается в чисто периодическую непрерывную дробь следующего вида

$$\theta = \overline{[a_1, \ldots, a_k]},$$

тогда число $-1/\theta'$ разлагается в чисто периодическую непрерывную дробь вида

$$-\frac{1}{\theta'} = [\overline{a_k, \ldots, a_1}].$$

▷ Докажем первое утверждение. Пусть k — период непрерывной дроби числа $\theta > 1$. Тогда существует целое число l (длина предпериода) такое, что для всех номеров n с условием $n \geqslant l$ остатки непрерывной дроби удовлетворяют равенствам $\theta_{n+k} = \theta_n$. Пользуясь формулой для выражения числа через остаток непрерывной дроби, найдем

$$\theta = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}} = \frac{\theta_{n+k} p_{n+k-1} + p_{n+k-2}}{\theta_{n+k} q_{n+k-1} + q_{n+k-2}} = \frac{\theta_n p_{n+k-1} + p_{n+k-2}}{\theta_n q_{n+k-1} + q_{n+k-2}}.$$

Следовательно, θ_n удовлетворяет квадратному уравнению

$$\frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}} = \frac{\theta_n p_{n+k-1} + p_{n+k-2}}{\theta_n q_{n+k-1} + q_{n+k-2}}.$$

Таким образом из равенства

$$\theta = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}}$$

имеем, что число θ является квадратичной иррациональностью.

Докажем теперь второе утверждение. Поскольку непрерывная дробь для числа θ является чисто периодической с периодом, равным k, имеем

$$\theta = [a_0, a_1, \ldots, a_{k-1}, \theta].$$

Отсюда получим

$$\theta = \frac{\theta p_{k-1} + p_{k-2}}{\theta q_{k-1} + q_{k-2}}, \quad q_{k-1}\theta^2 - (p_{k-1} - q_{k-1})\theta - p_{k-2} = 0.$$

Коэффициенты последнего квадратного уравнения — целые взаимно простые числа. Его дискриминант равен

$$(p_{k-1} - q_{k-1})^2 + 4q_{k-1}p_{k-2} > 0.$$

Следовательно, вещественное число $\theta > 1$ является квадратичной иррациональностью.

Покажем, что θ является приведенным числом. Из равенства

$$-\frac{1}{\theta'_k} = a_{k-1} + (-\theta'_{k-1}),$$

найденного при решении предыдущей задачи, получим

$$-\frac{1}{\theta'_k} = \left[a_{k-1}, \ldots, a_0, -\frac{1}{\theta'}\right].$$

Таким образом из условия $\theta_k = \theta$ следует, что число $-1/\theta'$ удовлетворяет уравнению

$$-\frac{1}{\theta'} = \left[a_{k-1}, \dots a_0, -\frac{1}{\theta'}\right],$$

тем самым доказано, что θ — приведенное число. ◁

§ 12. Разложение квадратного корня из натурального числа в непрерывную дробь

1. Разложить число $\sqrt{31}$ в непрерывную дробь. Доказать, что

$$\left|\sqrt{31} - \frac{1520}{273}\right| < \frac{1}{273 \cdot 2885} < \frac{1}{7 \cdot 10^5}.$$

▷ Имеем $5^2 < 31 < 6^2$. Следовательно, $a_0 = 5$. Далее получим

$$\sqrt{31} = 5 + (\sqrt{31} - 5) = 5 + \frac{6}{\sqrt{31} + 5},$$

$$\frac{\sqrt{31}+5}{6} = 1 + \frac{\sqrt{31}-1}{6} = 1 + \frac{5}{\sqrt{31}+1}, \quad a_1 = 1,$$

$$\frac{\sqrt{31}+1}{5} = 1 + \frac{\sqrt{31}-4}{5} = 1 + \frac{3}{\sqrt{31}+4}, \quad a_2 = 1,$$

$$\frac{\sqrt{31}+4}{3} = 3 + \frac{\sqrt{31}-5}{3} = 3 + \frac{2}{\sqrt{31}+5}, \quad a_3 = 3,$$

$$\frac{\sqrt{31}+5}{2} = 5 + \frac{\sqrt{31}-5}{2} = 5 + \frac{3}{\sqrt{31}+5}, \quad a_4 = 5,$$

$$\frac{\sqrt{31}+5}{3} = 3 + \frac{\sqrt{31}-4}{3} = 3 + \frac{5}{\sqrt{31}+4}, \quad a_5 = 3,$$

$$\frac{\sqrt{31}+4}{5} = 1 + \frac{\sqrt{31}-1}{5} = 1 + \frac{6}{\sqrt{31}+1}, \quad a_6 = 1,$$

$$\frac{\sqrt{31}+1}{6} = 1 + \frac{\sqrt{31}-5}{6} = 1 + \frac{1}{\sqrt{31}+5}, \quad a_7 = 1,$$

$$\sqrt{31} + 5 = 10 + (\sqrt{31} - 5) = 10 + \frac{6}{\sqrt{31}+5}, \quad a_8 = 10.$$

Таким образом приходим для числа $\sqrt{31}$ к периодической непрерывной дроби с периодом, равным 8. В понятных обозначениях имеем

$$\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}].$$

Схематически предыдущие действия можно изобразить в виде следующей таблицы для неполных частных a_n, числителей p_n и знаменателей q_n подходящих дробей числа $\sqrt{31}$.

n		0	1	2	3	4	5	6	7	8
a_n		5	1	1	3	5	3	1	1	10
p_n	1	5	6	11	39	206	657	863	1520	16063
q_n	0	1	1	2	7	37	118	155	273	2885

При $n \geqslant 1$ для вычисления числителей p_n и знаменателей q_n подходящих дробей использована следующая формула задачи 2 § 9:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}, \quad p_{-1} = 1, \quad q_{-1} = 0.$$

Из утверждений задач 2 § 9 и 10 § 9 находим

$$\frac{p_7}{q_7} = \frac{1520}{273}, \quad \left|\sqrt{31} - \frac{1520}{273}\right| < \frac{1}{273 \cdot 2885} < \frac{1}{7 \cdot 10^5}. \qquad \triangleleft$$

2. Для того чтобы алгебраическое число $\alpha > 1$ имело следующее разложение в непрерывную дробь

$$\alpha = [b, \overline{a_1, \ldots, a_{k-1}, 2b}] = [b, \overline{a_{k-1}, \ldots, a_1, 2b}],$$

где $b, a_1, \ldots, a_{k-1}$ — натуральные числа, необходимо и достаточно, чтобы число α было квадратным корнем из рационального числа, большего 1 и не являющегося точным квадратом.

▷ *Необходимость.* Пусть α имеет указанное выше разложение в непрерывную дробь. Тогда для остатка находим

$$\frac{1}{\alpha - b} = [\overline{a_1, \ldots, a_{k-1}, 2b}].$$

Отсюда по утверждению задачи 3 § 9 получим

$$-\alpha' + b = [\overline{2b, a_{k-1}, \ldots, a_1}].$$

Следовательно,

$$-\alpha' = [b, \overline{a_1, \ldots, a_{k-1}, 2b}] = \alpha.$$

Таким образом имеем, что $\alpha'^2 = \alpha^2 = a$ — рациональное число, причем $a > b \geqslant 1$ и a не является квадратом.

Достаточность. Дано, что число $\alpha = \sqrt{a}$, где $a > 1$ — рациональное число и не является точным квадратом. Положим $b = [\sqrt{a}] \geqslant 1$. Для остатка $\theta = \frac{1}{\alpha - b}$ имеем неравенство $\theta > 1$. Покажем, что число θ будет приведенным числом. Это следует из следующей цепочки соотношений

$$\alpha' = -\alpha, \quad \alpha - b = \frac{1}{\theta}, \quad -\frac{1}{\theta'} = -\alpha' + b = \alpha + b > 2b > 1.$$

Тогда по утверждению задачи 3 § 9 находим

$$\theta = [\overline{a_1, \ldots, a_k}], \quad -\frac{1}{\theta'} = [\overline{a_k, \ldots, a_1}].$$

Далее имеем

$$\left[-\frac{1}{\theta'}\right] = [\alpha + b] = [\alpha] + b = 2b, \quad a_k = 2b.$$

Следовательно,

$$-\frac{1}{\theta'} = [\overline{2b, a_{k-1}, \ldots, a_1}], \quad \theta = [\overline{a_1, \ldots, a_{k-1}, 2b}].$$

Таким образом

$$\alpha = -\frac{1}{\theta'} - b = [b, \overline{a_{k-1}, \ldots, a_1, 2b}], \quad \alpha = b + \theta = [b, \overline{a_1, \ldots, a_{k-1}, 2b}].$$

Эти равенства дают искомые разложения числа α в непрерывную дробь. ◁

§ 13. Вычисление основной единицы вещественного квадратичного поля

1. Пусть θ — приведенное число из $\mathbf{F} = \mathbf{Q}(\sqrt{D})$, т.е. $\theta > 1$ и $-\frac{1}{\theta'} > 1$, принадлежащее определителю m^2D, и пусть $\theta = [\overline{a_0, \ldots, a_{k-1}}]$ — чисто периодическое разложение в непрерывную дробь числа θ, имеющее период $k \geqslant 1$. Пусть, далее, p_{k-2}/q_{k-2} и p_{k-1}/q_{k-1} — последние перед повторением периода подходящие дроби числа θ. Тогда $\varepsilon = q_{k-1}\theta + q_{k-2}$ будет нетривиальной единицей кольца дискриминанта m^2D с условиями $\varepsilon > 1$ и $N(\varepsilon) = (-1)^k$. Кроме того, эту единицу можно представить в виде

$$\varepsilon = \frac{u + vm\sqrt{D}}{2},$$

где целые рациональные числа u и v определяются следующим образом

$$u = p_{k-1} + q_{k-2}, \quad v = (q_{k-1}, p_{k-1} - q_{k-2}, p_{k-2}).$$

▷ По утверждению задачи 6 § 9 получим

$$\theta = \frac{p_{k-1}\theta + p_{k-2}}{q_{k-1}\theta + q_{k-2}},$$

поскольку разложение в чисто периодическую дробь числа θ имеет период k и $\theta_k = \theta$. Следовательно, найдется число ε из $\mathbf{F}$ такое, что выполняется пара равенств

$$\varepsilon\theta = p_{k-1}\theta + p_{k-2}, \quad \varepsilon = q_{k-1}\theta + q_{k-2}.$$

Имеем цепочку равенств

$$\theta = \frac{\varepsilon - q_{k-2}}{q_{k-1}}, \quad \varepsilon\frac{\varepsilon - q_{k-2}}{q_{k-1}} = p_{k-1}\frac{\varepsilon - q_{k-2}}{q_{k-1}} + p_{k-2},$$

$$\varepsilon^2 - \varepsilon(p_{k-1} + q_{k-2}) + p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = 0.$$

Поскольку $p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k$, для числа ε находим уравнение

$$\varepsilon^2 - \varepsilon(p_{k-1} + q_{k-2}) + (-1)^k = 0.$$

По утверждению задачи 2 § 10 число ε является единицей поля $\mathbf{F}$ с нормой $N(\varepsilon) = (-1)^k$. Далее имеем явное выражение для $\varepsilon = q_{k-1}\theta + q_{k-2}$. Отсюда следует, что $\varepsilon > 1$.

С другой стороны, число θ удовлетворяет квадратному уравнению

$$\theta(q_{k-1}\theta + q_{k-2}) = p_{k-1}\theta + p_{k-2},$$

т.е. уравнению вида

$$q_{k-1}\theta^2 - (p_{k-1} - q_{k-2})\theta - p_{k-2} = 0.$$

Пусть v — наибольший общий делитель чисел $q_{k-1}, p_{k-1} - q_{k-2}$ и p_{k-2}. Положим

$$q_{k-1} = av, p_{k-1} - q_{k-2} = bv, p_{k-1} = cv, (a, b, c) = 1, p_{k-1} + q_{k-2} = u.$$

Тогда уравнение для числа θ примет вид

$$a\theta^2 - b\theta - c = 0.$$

Как и раньше, для приведенного числа θ находим

$$\theta = \frac{b + m\sqrt{D}}{2a}.$$

Следовательно,

$$\varepsilon = q_{k-1}\theta + q_{k-2} = q_{k-1}\frac{b + m\sqrt{D}}{2a} + q_{k-2} =$$

$$= q_{k-1}\frac{bv + vm\sqrt{D}}{2av} + q_{k-2} = \frac{u + vm\sqrt{D}}{2}. \quad \triangleleft$$

2. Каждая единица $\varepsilon > 1$, принадлежащая дискриминанту m^2D и имеющая форму

$$\varepsilon = \frac{u + v\sqrt{D}}{2}$$

с натуральными числами u и v, представляется в виде

$$\varepsilon = q\theta + q',$$

где q и q' — знаменатели двух соседних подходящих дробей в разложении приведенного числа θ дискриминанта m^2D в непрерывную дробь.

▷ Возьмем любую единицу $\varepsilon = \frac{u+vm\sqrt{D}}{2} > 1$ с целыми рациональными числами $u \geqslant 1$ и $v \geqslant 1$.

Пусть число θ удовлетворяет уравнению $a\theta^2 - b\theta - c = 0$ с целыми коэффициентами a, b, c и дискриминантом $b^2 + 4ac = m^2D$.

Положим

$$p = \frac{u+bv}{2}, \quad q = av, \quad p' = cv, \quad q' = \frac{u-bv}{2}.$$

Рациональные числа p, q, p', q' будут целыми, поскольку числа ε и $a\theta$ являются целыми в поле $\mathbf{F} = \mathbf{Q}(\sqrt{D})$. Кроме того, имеем

$$pq' - p'q = \frac{u^2 - (b^2+4ac)v^2}{4} = \frac{u^2 - v^2m^2D}{4} = N(\varepsilon).$$

Отсюда следует, что дроби p/q и p'/q' будут несократимы.

Так как набор чисел $q, p-q', p'$ пропорционален набору a, b, c, то число θ удовлетворяет уравнению

$$q\theta^2 - (p-q')\theta - p' = 0$$

или

$$\theta = \frac{p\theta + p'}{q\theta + q'}.$$

Как и раньше, из условия, что θ — приведенное число, имеем

$$b < m\sqrt{D}, \quad 2a - b < m\sqrt{D} < 2a + b.$$

Далее, используя условие $\varepsilon > 1$, находим

$$q' = \frac{a-bv}{2} > \frac{a-vm\sqrt{D}}{2} = \varepsilon' = \frac{N(\varepsilon)}{\varepsilon} > \begin{cases} 0, & \text{если } N(\varepsilon) = 1, \\ -1, & \text{если } N(\varepsilon) = -1, \end{cases}$$

$$q - q' = \frac{-u + (2a+b)v}{2} > \frac{-u + vm\sqrt{D}}{2} = -\varepsilon' =$$
$$= -\frac{N(\varepsilon)}{\varepsilon} > \begin{cases} -1, & \text{если } N(\varepsilon) = 1, \\ 0, & \text{если } N(\varepsilon) = -1, \end{cases}$$

$$p - q = \frac{u - (2a-b)v}{2} > \frac{u - vm\sqrt{D}}{2} = \varepsilon' =$$
$$= \frac{N(\varepsilon)}{\varepsilon} > \begin{cases} 0, & \text{если } N(\varepsilon) = 1, \\ -1, & \text{если } N(\varepsilon) = -1. \end{cases}$$

Следовательно,

$$0 < q' \leqslant q, \quad \frac{p}{q} > 1, \quad \text{если } N(\varepsilon) = 1,$$

$$0 \leqslant q' < q, \quad \frac{p}{q} \geqslant 1, \quad \text{если } N(\varepsilon) = -1.$$

Разложим число p/q в непрерывную дробь

$$\frac{p}{q} = [a_0, a_1, \ldots, a_k] = \frac{p_k}{q_k},$$

причем число k будет четным или нечетным в соответствии с равенством $N(\varepsilon) = (-1)^k$.

Покажем, что $\frac{p_{k-1}}{q_{k-1}} = \frac{p'}{q'}$. Имеем соотношения

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^k = N(\varepsilon), \quad 0 \leqslant q_{k-1} \leqslant q_k,$$

причем равенство имеет место в первом неравенстве только при $k = 1$, а во втором, — быть может, только при $k = 2$.

Таким образом,

$$p_k(q_{k-1} - q') - q_k(p_{k-1} - p') = 0,$$

что возможно только при $q_{k-1} = q'$, иначе несократимая дробь p_k/q_k была представлена дробью с меньшим знаменателем $|q_{k-1} - q'|$, а это невозможно. Следовательно, $p_{k-1} = p'$, $q_{k-1} = q'$.

Из равенств

$$\theta = \frac{p\theta + p'}{q\theta + q'} = \frac{p_k\theta + p_{k-1}}{q_k\theta + q_{k-1}}$$

имеем

$$\theta = [a_0, a_1, \ldots, a_k, \theta],$$

а натуральные числа $a_0, \ldots, a_k$ являются неполными частными разложения числа θ в непрерывную дробь, причем они могут представлять собой несколько периодов в этом разложении θ. Следовательно, получим

$$v = (q_k, p_k - q_{k-1}, p_{k-1}), \quad u = p_k + q_{k-1},$$

или $q_k = cv$, $p_k - q_{k-1} = bv$, $p_{k-1} = cv$. Эти соотношения по доказательству утверждения предыдущей задачи определяют $\varepsilon = q_k\theta + q_{k-1}$ по разложению числа θ в непрерывную дробь. ◁

Вычислим основную единицу поля $\mathbf{F} = \mathbf{Q}(\sqrt{D})$. Дискриминант этого поля равен d,

$$d = \begin{cases} D, & \text{если } D \equiv 1 \pmod 4, \\ 4D, & \text{если } D \equiv 2, 3 \pmod 4. \end{cases}$$

Базисом кольца целых чисел этого поля являются числа 1 и ρ, где

$$\rho = \begin{cases} \frac{1+\sqrt{D}}{2} = \frac{1+\sqrt{d}}{2}, & \text{если } D \equiv 1 \pmod 4, \\ \sqrt{D} = \frac{0+\sqrt{d}}{2}, & \text{если } D \equiv 2,3 \pmod 4. \end{cases}$$

Для наименьшего положительного дискриминанта $d = D = 5$ базисное число ρ имеет следующее разложение в чисто периодическую непрерывную дробь

$$\rho = \frac{1+\sqrt{5}}{2} = [\overline{1}]$$

с периодом 1. Числители p_n и знаменатели q_n подходящих дробей удовлетворяют при $n \geqslant 1$ рекуррентным формулам вида

$$\begin{cases} p_{n+1} = p_n + p_{n-1}, \\ q_{n+1} = q_n + q_{n-1}, \end{cases}$$

причем $p_0 = p_1 = 1$, $q_0 = 0$, $q_1 = 1$.

Схематически разложение числа ρ в непрерывную дробь представим в виде следующей таблицы для неполных частных a_n, числителей p_n и знаменателей q_n подходящих дробей этого числа.

n		0	1	2	3	4	5	6	7	8	...
a_n		1	1	1	1	1	1	1	1	1	...
p_n	1	1	2	3	5	8	13	21	34	55	...
q_n	0	1	1	2	3	5	8	13	21	34	...

Заметим, что в данном случае при $n \geqslant 0$ имеем $p_n = q_{n+1}$. Любое решение $u = u_n, v = v_n$ уравнения Пелля $u^2 - 5v^2 = 1$ по утверждению предыдущей задачи представляется в виде

$$\rho^n = \frac{u_n + v_n\sqrt{5}}{2},$$

где $\rho = \frac{1+\sqrt{5}}{2}$ — основная единица поля $\mathbf{Q}\sqrt{5}$ и

$$u_n = p_n + q_{n-1} = q_{n+1} + q_{n-1},$$
$$v_n = (q_n, p_n - q_{n-1}, p_{n-1}) = (q_n, q_n, q_n) = q_n.$$

3. Пусть ρ — базисное число квадратичного поля дискриминанта d, отличного от пяти. Тогда число

$$\rho^* = \frac{1}{\rho - a_0}$$

является приведенным, где $a_0 = [\rho]$.

▷ Имеем $\rho > 1$, $\rho^* > 1$. Для величины $-1/\rho^{*'}$ находим

$$-\frac{1}{\rho^{*'}} = a_0 - \rho' =$$

$$= \begin{cases} a_0 - \frac{1-\sqrt{D}}{2} = a_0 + \rho - 1 > 2a_0 - 1 \geqslant 1, & \text{если } D \equiv 1 \pmod 4, \\ a_0 + \sqrt{D} > 2a_0 \geqslant 2, & \text{если } D \equiv 2, 3 \pmod 4, \end{cases}$$

т.е. $-1/\rho^{*'} > 1$. Таким образом, число ρ^* будет приведенным. ◁

4. Найти основную единицу поля $\mathbf{Q}(\sqrt{31})$.

▷ В этом случае базисное число $\rho = \sqrt{31}$. Из утверждения задачи 1,XII получим разложение в периодическую непрерывную дробь с периодом 8 следующих чисел

$$\rho = \sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}],$$

$$\rho^* = \frac{5 + \sqrt{31}}{6} = [\overline{1, 1, 3, 5, 3, 1, 1, 10}].$$

Представим в виде таблицы при $0 \leqslant n \leqslant 7$ значения неполных частных a_n, числители p_n и знаменатели q_n подходящих дробей числа ρ^*. Имеем

n		0	1	2	3	4	5	6	7
a_n		1	1	3	5	3	1	1	10
p_n	1	1	2	7	37	118	155	273	2885
q_n	0	1	1	4	21	67	88	155	1638

Используя утверждения задач 1–3, получим

$$u_1 = 2885 + 155 = 2 \cdot 1520, v_1 = (1638, 2730, 273) = 273.$$

Следовательно, основная единица ε_1 равна

$$\varepsilon_1 = 1520 + 273\sqrt{31}.$$ ◁

§ 14. Теорема П. Л. Чебышёва о попадании простых чисел в интервалы (постулат Бертрана)

Далее докажем известную теорему П. Л. Чебышёва о том, что при $x > 1$ на промежутке $[x, 2x)$ лежит хотя бы одно простое число. Пусть, как и раньше в VI, $\psi(x) = \sum\limits_{n \leqslant x} \Lambda(n)$ обозначает функцию Чебышёва, $\theta(x) = \sum\limits_{p \leqslant x} \ln p$,

$$\Lambda(n) = \begin{cases} \ln p, & \text{если } \quad n = p^r, \\ 0, & \text{в противном случае,} \end{cases}$$

где p обозначает простое число, n, r — натуральные числа.

1. При $x \geqslant 1$ справедливы равенства

$$T(x) = \sum_{n \leqslant x} \ln n = \sum_{n \leqslant x} \psi(x/m),$$

$$T(x) - 2T(x/2) = \sum_{n\leqslant x} (-1)^{n-1}\psi(x/n).$$

▷ Поскольку $\ln n = \sum\limits_{d|n} \Lambda(d)$, имеем

$$T(x) = \sum_{n\leqslant x}\sum_{d|n}\Lambda(d) = \sum_{d\leqslant x}\Lambda(d)\sum_{\substack{n\leqslant x\\ n=md}} 1 =$$

$$= \sum_{d\leqslant x}\Lambda(d)\sum_{m\leqslant x/d} 1 = \sum_{m\leqslant x}\sum_{d\leqslant x/m}\Lambda(d) = \sum_{m\leqslant x}\psi(x/m).$$

Отсюда получим

$$T(x)-2T(x/2) = \sum_{n\leqslant x}\psi(x/n)-2\sum_{n\leqslant x/2}\psi(x/(2n)) = \sum_{n\leqslant x}(-1)^{n-1}\psi(x/n).\triangleleft$$

Приведем следующий признак сходимости ряда, принадлежащий Лейбницу. Пусть задана невозрастающая последовательность $\{a_n\}$, $n \geqslant 1$, неотрицательных чисел, стремящаяся к нулю при $n \to \infty$. Тогда справедливы неравенства

$$a_1 - a_2 \leqslant \sum_{n=1}^{\infty}(-1)^{n-1}a_n \leqslant a_1 - a_2 + a_3.$$

2. При $x \geqslant 1$ имеем

$$\psi(x) - \psi(x/2) \leqslant T(x) - 2T(x/2) \leqslant \psi(x) - \psi(x/2) + \psi(x/3).$$

▷ Поскольку функция $\psi(x)$ не отрицательна и не убывает, и $\psi(x) = 0$ при $0 < x < 2$, по признаку Лейбница и по утверждению предыдущей задачи следуют искомые неравенства. $\triangleleft$

3. Для любого натурального числа m справедливы неравенства

$$\frac{1}{2\sqrt{m}} \leqslant 2^{-2m}\binom{2m}{m} < \frac{1}{\sqrt{2m+1}}.$$

▷ Проведем индукцию по m. При $m = 1$ утверждение справедливо, поскольку $\frac{1}{2} = 2^{-2}\binom{2}{1} < \frac{1}{\sqrt{3}}$. Предположим, что оно справедливо при $m = k$. Докажем, что оно верно при $m = k + 1$. По предположению индукции имеем цепочку соотношений

$$\frac{1}{2\sqrt{m}}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2} \leqslant 2^{-2m}\binom{2m}{m}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2} =$$

$$= 2^{-2m-2}\binom{2m+2}{m+1} < \frac{1}{\sqrt{2m+1}}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2}.$$

Следовательно, достаточно доказать, что выполняются неравенства

$$\frac{1}{2\sqrt{m+1}} \leqslant \frac{1}{2\sqrt{m}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2},$$

$$\frac{1}{\sqrt{2m+1}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2} < \frac{1}{2m+3}.$$

Первое из них является следствием того, что $2m+1 \geqslant 2\sqrt{m(m+1)}$, т.е. $4m^2+4m+1 \geqslant 4m^2+4m$, а второе следует из того, что $2m+2 > \sqrt{(2m+1)(2m+3)}$, т.е. $4m^2+8m+4 > 4m^2+8m+3$.◁

4. При $x \geqslant 1$ имеем неравенство

$$\psi(x) < x \ln 4.$$

▷ Проведем индукцию по параметру x. Сначала проверим справедливость неравенства при $1 \leqslant x < 17$. При $1 \leqslant x < 2$ оно, очевидно, справедливо. При $2 \leqslant x < 4$ имеем

$$\psi(x) \leqslant \ln 2 + \ln 3 < 2 \ln 4 \leqslant x \ln 4.$$

При $4 \leqslant x < 7$ находим

$$\psi(x) \leqslant 2 \ln 2 + \ln 3 + \ln 5 = \ln 60 < 3 \ln 4 < x \ln 4.$$

Пусть $7 \leqslant x < 11$. Тогда имеем

$$\psi(x) \leqslant 3 \ln 2 + 2 \ln 3 + \ln 5 + \ln 7 = \ln 2520 < 6 \ln 4 < x \ln 4.$$

Пусть, теперь, $11 \leqslant x < 13$. Тогда

$$\psi(x) \leqslant 3 \ln 2 + 2 \ln 3 + \ln 5 + \ln 7 + \ln 11 = \ln 27720 < 10 \ln 4 < x \ln 4.$$

Пусть, наконец, $13 \leqslant x < 17$. Тогда получим

$$\psi(x) \leqslant 4 \ln 2 + 2 \ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 =$$

$$= \ln 720720 < 12 \ln 4 < x \ln 4.$$

Предположим, что утверждение справедливо при $17 \leqslant x < y$. Докажем, что оно верно при $y \leqslant x < y+2$. Пусть $[y] = n$, т.е. $n \leqslant y < n+1$, где n — целое число. Возможны два случая: 1) $n = 2m$ — четное число и 2) $n = 2m-1$ — нечетное число. Рассмотрим сначала случай 1). Имеем $2m \leqslant y < 2m+1 < 2m+2 \leqslant y+2$. Пусть $x \in [y, 2m+1)$. Тогда из утверждения задачи 2 и предположения индукции получим

$$\psi(x) = \psi(2m) < \ln \binom{2m}{m} + \psi(m) < 2m \ln 4 - \ln \sqrt{2m-1} \leqslant x \ln 4.$$

Пусть, теперь, $x \in [2m+1, 2m+2)$. Тогда, вновь используя утверждение задачи 2 и предположение индукции, находим

$$\psi(x) \leqslant \psi(2m+2) < (2m+2) \ln 4 - \ln \sqrt{2m+1} < (2m+1) \ln 4 \leqslant x \ln 4,$$

поскольку $\ln 4 < \ln\sqrt{17} \leqslant \ln\sqrt{2m+1}$.

Пусть, наконец, $x \in [2m+2, y)$. Тогда из тех же соображений, что и раньше, имеем

$$\psi(x) = \psi(2m+2) < \ln\binom{2m+2}{m+1} + \psi(m+1) <$$

$$< (2m+2)\ln 4 - \ln\sqrt{2m+1} \leqslant x \ln 4.$$

Случай 1) полностью рассмотрен.

Рассмотрим, теперь, случай 2). Имеем $2m-1 \leqslant y < 2m < 2m+1 \leqslant y+2 < 2m+2$. Пусть $x \in [y, 2m)$. Тогда из утверждения задачи 2 и предположения индукции получим

$$\psi(x) < \psi(2m) < \ln\binom{2m}{m} + \psi(m) <$$

$$< 2m\ln 4 - \ln\sqrt{2m-1} \leqslant (2m-1)\ln 4 \leqslant x \ln 4,$$

поскольку $\ln 4 = \ln\sqrt{16} \leqslant \ln\sqrt{2m-1}, 16 \leqslant [y] = 2m-1$.

Пусть, теперь, $x \in [2m, 2m+1)$. Тогда, вновь используя утверждение задачи 2 и предположение индукции, находим

$$\psi(x) \leqslant \psi(2m) < (2m)\ln 4 - \ln\sqrt{2m} \leqslant 2m \ln 4 \leqslant x \ln 4.$$

Пусть, наконец, $x \in [2m+1, y)$. Тогда из тех же соображений, что и раньше, имеем

$$\psi(x) = \psi(2m+2) < \ln\binom{2m+2}{m+1} + \psi(m+1) <$$

$$< (2m+2)\ln 4 - \ln\sqrt{2m+3} \leqslant (2m+1)\ln 4 \leqslant x \ln 4.$$

Этим завершается рассмотрение случая 2). ◁

5. Пусть m — натуральное число. Тогда имеем

$$\theta(2m) - \theta(m) \geqslant \frac{\ln 4}{3} m - \ln\sqrt{4m} - \sqrt{2m}\ln 4.$$

▷ Используя утверждения задач 2 и 4, находим

$$\psi(2m) - \psi(m) > \ln\binom{2m}{m} - \psi(\frac{2m}{3}) \geqslant$$

$$\geqslant m\ln 4 - \ln\sqrt{4m} - \frac{2m}{3}\ln 4 = \frac{\ln 4}{3} m - \ln\sqrt{4m}.$$

Далее, имеем $\psi(2m) - \psi(m) = \theta(2m) - \theta(m) + r_m$, где

$$r_m = \sum_{\substack{m < p^\alpha \leqslant 2m \\ \alpha \geqslant 2}} \ln p.$$

Поскольку $\alpha \geqslant 2$, в сумму r_m входят простые числа p с условием $p \leqslant \sqrt{2m}$, причем в силу условия $m < p^\alpha \leqslant 2m$ при каждом фиксированном простом числе p в эту сумму r_m может входить не более одной степени данного числа. Следовательно,

$$r_m \leqslant \theta(\sqrt{2m}) \leqslant \psi(\sqrt{2m}) \leqslant \sqrt{2m}\ln 4.$$

Отсюда следует искомое неравенство. ◁

6. Пусть $m \geqslant 2^8$ — натуральное число. Тогда справедливо неравенство

$$\pi(2m) - \pi(m) \geqslant \sqrt{m/2}.$$

▷ Из утверждения задачи 5 при любом натуральном числе m имеем неравенство

$$\pi(2m) - \pi(m) = \sum_{m<p\leqslant 2m} 1 \geqslant \frac{\theta(2m) - \theta(m)}{\ln 2m} \geqslant$$

$$\geqslant \frac{m\ln 4}{3\ln 2m} - \frac{\ln\sqrt{4m}}{\ln 2m} - \frac{\sqrt{2m}\ln 4}{\ln 2m} = f_1(m).$$

Далее, при $m \geqslant 2^8$ оценим $f_1(m)$ снизу. Получим

$$f_1(m) = \frac{m\ln 4}{3\ln 2m} - \frac{1}{2} - \frac{\ln 2}{2\ln 2m} - \frac{\sqrt{2m}\ln 4}{\ln 2m} \geqslant \frac{m\ln 4}{3\ln 2m} - \frac{5}{9} - \frac{2\sqrt{2m}}{9} = f(m).$$

Покажем, что при $m \geqslant 2^8$ функция $g(m) = f(m) - \sqrt{m/2}$ будет положительной. При $m = 2^8$ имеем

$$g(2^8) = \frac{2^8\ln 4}{3\ln 2^9} - \frac{5}{9} - \frac{2\sqrt{2^9}}{9} - \sqrt{2^7} = \frac{2^9 - 15 - 312\sqrt{2}}{27} > \frac{29}{27} > 0.$$

Найдем производную функции $g(x)$. Имеем

$$g'(x) = \frac{\ln 4}{3}\frac{\ln 2x - 1}{(\ln 2x)^2} - \frac{13}{18\sqrt{2x}}.$$

Поскольку при $x \geqslant 2^8$ справедливо неравенство $\ln 2x - 1 \geqslant \frac{7}{9}\ln 2x$, получим

$$g'(x) \geqslant \frac{7\ln 4}{27\ln 2x} - \frac{13}{18\sqrt{2x}} = g_1(x).$$

При $x > e^2$ функция $\sqrt{x}/\ln x$ является возрастающей, поэтому при $x \geqslant 2^8$ имеем

$$\sqrt{2x}g_1(x) \geqslant \frac{224\sqrt{2}}{243} - \frac{13}{18} > 0.$$

Следовательно, при $x \geqslant 2^8$ функция $g(x)$ возрастающая и $g(x) > 0$. Это и доказывает искомое неравенство. ◁

7. Пусть n — натуральное число. Тогда при $x \geqslant 2n^2$ на отрезке $[x, 2x]$ лежит по крайней мере n различных простых чисел.

▷ Положим $m = [x] \geqslant 2^8$. Имеем теоретико-множественное включение $[m+1, 2m] \subset [x, 2x]$. Следовательно, все простые числа, находящиеся на отрезке $[m+1, 2m]$, будут принадлежать и отрезку $[x, 2x]$. В силу утверждения задачи 6 при $m \geqslant 2^8$ на отрезке $[m+1, 2m]$ не менее $\sqrt{m/2}$ различных простых чисел. Поскольку при $x \geqslant 2n^2$ справедливы неравенства $\sqrt{x/2} \geqslant \sqrt{m/2} \geqslant n$, при $x \geqslant \max\{2^8, 2n^2\}$ на отрезке $[x, 2x]$ находится по крайней мере n различных простых чисел.

Осталось доказать утверждение задачи при $2 \leqslant x < 2^8$. Разобьем этот промежуток на промежутки вида $I_n = [2n^2, 2(n+1)^2)$, где $1 \leqslant n \leqslant 11$. Используя таблицы простых чисел, проверяем, что если $x \in I_n$, то на отрезке $[x, 2x]$ находится по крайней мере n различных простых чисел. Например, при $n = 1$ имеем $I_1 = [2, 8)$. Рассматривая x в промежутках $2 \leqslant x < 3$, $3 \leqslant x < 5$, $5 \leqslant x < 7$ и $7 \leqslant x < 8$, видим, что $3 \in [x, 2x]$ при $x \in [2, 3)$, $5 \in [x, 2x]$ при $x \in [3, 5)$, $7 \in [x, 2x]$ при $x \in [5, 7)$, $11 \in [x, 2x]$ при $x \in [7, 8)$. ◁

Экзаменационные вопросы

I. Алфавитное кодирование

1. Понятие алфавита и слова в алфавите. Кодирование сообщения. Алфавит сообщений. Алфавит кодирования. Однозначное кодирование.

2. Схема, задающая алфавитное кодирование. Примеры схем, задающих однозначное и неоднозначное кодирование. Префикс слова и определение схемы, обладающей свойством префикса. Достаточное условие взаимно однозначного кодирования.

II. Помехоустойчивость

1. Многоразрядный код. Расстояние Хемминга. Неравенство треугольника. Теорема об исправлении ошибок в кодах с любым заданным расстоянием.

2. Пример множества 5-разрядных двоичных кодов, в которых исправляется одна возможная ошибка. Способ построения множества 5-разрядных двоичных кодов, имеющих кодовое расстояние, равное 3.

III. Передача сообщения по каналу без шума

1. Пример построения кода Фано в случае 4-х буквенного алфавита сообщений и 2-х буквенного алфавита кодирования. Средняя длина кодового слова. Общая схема построения кода Фано, построение таблицы.

2. Бинарное дерево для двоичного кода Фано. Необходимое и достаточное условия существования префиксного кода заданного объема и с заданным набором длин слов. Неравенство Крафта – МакМиллана. Необходимое условие существования однозначно декодируемого кода. Две теоремы об оценке средней длины кодовых слов. Теорема о минимальной длине префиксного кода

3. Построение оптимального кода Хафмена. Пример.

IV. Способы защиты информации

1. Защита информации с помощью перестановки. Маршрутные перестановки. Шифры вертикальной замены. Решетка Кардано.

2. Защита информации с помощью шифра замены. Система Цезаря и система Цезаря с ключевым словом. Блочные и поточные шифры замены. Примеры блочных шифров замены: шифры Плейфера и Хилла.

V. О симметричных шифрах

VI. О шифровании с открытым ключом

VII. Конечные поля. Циклические коды

1. Конечные поля. Неприводимые многочлены над конечным полем.

2. Циклические коды.

VIII. Рекуррентные соотношения. Производящие функции

1. Примеры рекуррентных соотношений.

2. Последовательность Фибоначчи.

3. Линейные рекуррентные уравнения второго порядка.

4. Линейные рекуррентные уравнения произвольного порядка.

5. Рекуррентные соотношения в кольцах вычетов.

IX. Арифметический подход к искажению знаков в шифрах простой замены и Виженера

1. Примеры шифров со “сжатием” алфавита.

2. Метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного.

3. Метод искажения знаков в шифре простой замены с помощью возведения в квадрат.

4. Комбинированный метод искажения частот появления знаков в шифре простой замены.

5. Анализ методов искажения знаков в шифре простой замены.

6. Применение китайской теоремы об остатках к шифру Виженера.

7. Арифметический вариант шифра Виженера.

Литература

[1] Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. — М.: Гелиос АРВ, 2002. — 480 с.

[2] Архипов Г. И., Садовничий В. А., Чубариков В. Н. Лекции по математическому анализу. Изд. 6-е. — М.: Дрофа, 2008, 640 с.

[3] Аршинов М. Н., Садовский Л. Е. Коды и математика. — М.: Наука, Гл. ред. физ.-мат. лит., 1983 (Библитечка "Квант". Вып. 30).

[4] Бабаш А.В., Шанкин Г.П. Криптография. — М.: СОЛОН-ПРЕСС, 2007. — 511 с.

[5] Баричев С. Криптография без секретов (http://www.artelecom.ru/library/books/swos/index/html) — 44 с.

[6] Bach E., Shallit J. Algorithmic number theory, Volume I: Efficient algorithms. — Massachusetts, MIT Press 1996.

[7] Брассар Ж. Современная криптология. — М.: ПОЛИМЕД, 1999. — 176 с.

[8] Ван-дер-Варден Б. Л. Алгебра. Пер. с нем. — М.: Наука, 1976, 648 с.

[9] Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. 2-е изд., доп. — М.: МЦНМО, 2006. — 336 с.

[10] Виноградов И. М. Основы теории чисел. — М.: Наука, Гл. ред. физ.-мат. лит., 1983.

[11] Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Дрофа., 2004.

[12] Грин Д., Кнут Д. Математические методы анализа алгоритмов. — М.: Мир, 1987.

[13] Davenport H. A remark on a continued fractions // Michigan Math. J., 1964. **11**, 343–344.

[14] Diffie W., Hellman M E. New directions in cryptography // IEEE Trans. of Inf. Theory. 1976, IT-22.

[15] Dickson L. E. History of the theory of numbers. — Carnegie Inst. of Washington, 1919. Reprinted by Chelsea Publishing, New York, 1971.

[16] El Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Trans. on Inf. Theory, IT-31. 1985, 469–472.

[17] Жельников В. Криптография от папируса до компьютора. — М.: ABF, 1996. — 335 с.
[18] Земор Ж. Курс криптографии. — М.–Ижевск: НИЦ “Регулярная и хаотическая динамика”; Институт компьютерных исследований, 2006. — 256 с.
[19] Kahn D. The Codebreakers. — N.-Y., 1967.
[20] Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах // ДАН СССР. 1962, т. 145, №2, с.293–294.
[21] Кнут Д. Э. Искусство программирования. Т.II. 3-е изд.: Пер. с англ. — Москва – Санкт-Петербург – Киев: Издат.дом “Вильямс”, 2000, 832 с.
[22] Коблиц Н. Курс теории чисел и криптографии. — М.: Научное изд-во “ТВП”, 2001.
[23] Колмогоров А. Н. Три подхода к понятию информации // Проблемы передачи информации, 1965, т. 1, с.3–11.
[24] Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001.
[25] Маховенко Е. Б. Теоретико-числовые методы в криптографии. — М.: “Телиос АРВ”, 2006.
[26] Miller J. C. P., Wheeler D. J. Large prime numbers // Nature, 1951. **168**. 838.
[27] Минеев М. П., Чубариков В. Н. Задача об искажении частоты появления знаков в шифре простой замены// Математические вопросы кибернетики, 2007, вып. 16, с.242–245.
[28] Минеев М. П., Чубариков В. Н. Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН, 2008, т. 420, №6, с.736–738.
[29] Минеев М. П., Чубариков В. Н. К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН, 2009, т. 426, №1, с.6–8.
[30] Молдовян А. А., Молдовян Н. А.,Советов Б. Я. Криптография. — СПб.: Изд-во “Лань”, 2001. — 224 с.
[31] Нечаев В. И. Элементы криптографии (Основы теории защиты информации): Учеб. пос. для ун-тов и пед. вузов — М.:Высш.шк., 1999. — 109 с.
[32] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ. — М.: Мир, 1976, 594 с.
[33] Поздняков С. Н., Рыбин С. В. Дискретная математика. — М.: Изд. центр “Академия”., 2008. — 447 с.
[34] Полиа Г., Сегё Г. Задачи и теоремы из анализа. Пер. с нем. Изд. 3-е. Ч. I, II. — М.: Наука, 1978.

[35] Постникова Л. П. Тригонометрические суммы и теория сравнений по простому модулю. Уч. пос. — М.: Изд-во МГПИ, 1973, 186 с.

[36] Постников М. М. Основы теории Галуа. — М.: ГИФМЛ, 1963, 220 с.

[37] Райзер Г. Дж. Комбинаторная математика. Пер. с англ. — М.: Мир, 1966, 154 с.

[38] Riesel H. Prime numbers and computers methods for factorization (Progress in mathematics; vol.57). — Boston; Basel; Stuttgart: Birkhäuser, 1985. — pp.464.

[39] Rivest R. L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Criptosystems // Comm. of the ACM, Feb. 1978, v.21, №2, pp.120–126.

[40] Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996. — 318 с.

[41] Серпинский В. Что мы знаем и чего не знаем о простых числах. — М.: ГИФМЛ, 1963.

[42] Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида–Маллера // Дискретная математика, 1994, т.6, вып.2, с.3–20.

[43] Сингх С. Книга шифров: тайная история шифров и их расшифровки. — М.: АСТ: Астрель, 2007. — 447 с.

[44] Холл М. Комбинаторика. Пер. с англ. — М.: Мир, 1970, 424 с.

[45] Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002.

[46] Чмора А. Л. Современная прикладная криптография. 2-е изд., стер. — М.: Гелиос АРВ, 2002. — 256 с.

[47] Чубариков В. Н. Элементы арифметики. — М.: Изд-во Механико-математического ф-та МГУ, 2007. — 96 с.

[48] Шеннон К. Работы то теории информации и кибернетике. Пер. с англ. — М.: ИЛ, 1963, с.243–332.

Оглавление

Предисловие 3

Глава I. Введение 7
§ 1. Понятие информации и ее кодирование 7
§ 2. Основные задачи теории кодирования 9
§ 3. Алфавитное кодирование 10
§ 4. О помехоустойчивости 14
§ 5. Об увеличении скорости передачи информации 17
§ 6. О защите информации 19
§ 7. О симметричных шифрах 20
§ 8. О шифровании с открытым ключом 21

Глава II. Префиксные коды. Коды Шеннона и Гилберта–Мура 23
§ 1. Префиксные коды. Неравенство Крафта – МакМиллана 23
§ 2. Теорема о минимальной длине префиксного кода 25

Глава III. Конечные поля. Циклические коды 28
§ 1. Конечные поля. Неприводимые многочлены 28
§ 2. Циклические коды 34

Глава IV. Рекуррентные соотношения. Производящие функции 39
§ 1. Рекуррентные соотношения 39
§ 2. Последовательность Фибоначчи 41
§ 3. Линейные рекуррентные уравнения второго порядка . . 44
§ 4. Линейные рекуррентные уравнения произвольного порядка 44
§ 5. Рекуррентные соотношения первого порядка в кольцах вычетов 46
§ 6. Рекуррентные соотношения в конечных полях 49

Глава V. Арифметический подход к искажению знаков в шифрах простой замены и Виженера 55
§ 1. Введение 55
§ 2. Метод искажения знаков в шифре простой замены . . . 57
§ 3. Метод искажения знаков в шифре простой замены . . . 60
§ 4. Комбинированный метод искажения частот 62
§ 5. Анализ методов искажения знаков 63
§ 6. Применение китайской теоремы об остатках 65
§ 7. Арифметический вариант шифра Виженера 67

Глава VI. Асимметричные шифры 69
§ 1. Введение 69
§ 2. Задача о рюкзаке 72
§ 3. Рюкзачная система шифрования 74
§ 4. Система шифрования RSA 77
§ 5. Хэш-функции 82

Глава VII. Задачи по теории чисел 85
§ 1. Квадратичные вычеты и невычеты по простому модулю 85
§ 2. Извлечение квадратного корня по простому модулю . . 109
§ 3. Символ Якоби 110
§ 4. Извлечение квадратного корня по составному модулю . 113
§ 5. Целая часть квадратного корня 119
§ 6. Символ Кронекера 121
§ 7. Простейшие теоремы о распределении простых чисел . 129
§ 8. Распознавание простых и составных чисел 131
§ 9. Непрерывные (цепные) дроби 141
§ 10. Арифметика квадратичных полей 155
§ 11. Разложение квадратичных иррациональностей 163
§ 12. Разложение квадратного корня в непрерывную дробь . 167
§ 13. Вычисление основной единицы 169
§ 14. Теорема П. Л. Чебышёва (постулат Бертрана) 174

Экзаменационные вопросы 180

Литература 182

Минеев Михаил Петрович
Чубариков Владимир Николаевич

Лекции по арифметическим вопросам криптографии

Издательство «Попечительский совет Механико-математического факультета МГУ им. М. В. Ломоносова»

Подписано в печать 01.09.2010.
Формат 60×90 1/16. Усл. печ. л. 11,75.
Тираж 500 экз. Заказ 15.

Отпечатано с оригинал-макета на типографском оборудовании механико-математического факультета МГУ