Решетки, алгоритмы и современная криптография

Шокуров А.В, Кузюрин Н.Н, Фомин С.А

22 октября 2011 г.

Оглавление

Введение

0.1 Введение. История криптографии

Криптография занимается разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей. Предполагается, что имеется круг законных пользователей информации, а также незаконный пользователь (противник), стремящийся овладеть защищаемой информацией.

Криптография занимается методами преобразования информации, которые не позволили бы противнику извлечь ее из перехватываемых сообщений (зашифрованной информации). Предполагается, что обмен зашифрованными сообщениями происходит между законными пользователями A (Алиса) и B (Боб) информации по открытому каналу связи и противник (Ева) имеет возможность перехватить все или часть сообщений.

Вскрытие (взламывание) шифра — процесс получения защищаемой информации из зашифрованного сообщения без знания примененнного шифра.

Долгое время занятие криптографией было уделом чудаков-одиночек. Среди них были одаренные ученые, дипломаты, священнослужители. Этот период развития криптографии длился с незапамятных времен до начала XX века, когда появились первые шифровальные машины.

Многие из древних шифров принадлежат одному из двух типов: *шифру замены* и *шифру перестановки*.

Типичными примерами шифра замены являются *шифр Цезаря* и «пляшущие человечки» Артура Конан Дойля. Его математическое описание весьма просто. Пусть X, Y два алфавита, открытого и зашифрованного текстов

соответственно, состоящие из одинакового числа букв. Пусть $g : X \to Y$ — произвольное взаимно-однозначное отображение. Тогда шифр замены преобразует открытый текст $x_1x_2 \ldots x_n$ в шифртекст $g(x_1)g(x_2) \ldots g(x_n)$. В частности, в шифре Цезаря g заменяет каждую букву открытого текста на третью после нее в алфавите, причем алфавит считается круговым — после последней буквы идет первая и т. д.

Методы вскрытия такого шифра не представляют труда и описаны в известных рассказах «Золотой жук» Э. По и «Пляшущие человечки» А. Конан Дойля.

Шифр перестановки, как и следует из его названия, осуществляет перестановку букв в открытом тексте. Примером шифра перестановки является *шифр «Сцитала»,* известный со времен войны Спарты против Афин в V веке до н.э. Открытый текст разбивается на отрезки равной длины и каждый отрезок шифруется независимо. Если длина отрезка равна n и σ — некоторая перестановка множества $\{1, 2, \ldots, n\}$, то шифр перестановки отрезок открытого текста $x_1x_2 \ldots x_n$ переводит в отрезок шифртекста $x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma($
В настоящее время этот шифр также не представляет трудностей для вскрытия.

В общем случае можно сказать, что функция шифрования E (от английского слова encryption) ставит в соответствие каждому открытому тексту m шифртекст C (от английского слова cyphertext), т. е. $E(m) = C$. Функция дешифрования D (от английского слова decryption) ставит в соответствие каждому зашифрованному тексту C шифртекст m (от английского слова cyphertext), причем $D(E(m)) = m$.

Поскольку создание хорошего шифра дело весьма трудоемкое, то издавна в криптографии стали использовать идею *сменного ключа*. Под ключом понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. Например, в шифрах типа шифра Цезаря ключом является величина сдвига букв шифртекста относительно букв открытого текста, в шифрах перестановки — ключом является перестановка σ.

На протяжении многих веков среди специалистов не утихали споры о стойкости различных шифров и о возможности построения абсолютно стойкого шифра. Опыт говорит о том, что шифры, считавшиеся своими создателями абсолютно стойкими, вскрывались рано или поздно, а стойкость

шифра обычно переоценивается его разработчиками. В теоретической криптографии существуют два основных подхода к определению стойкости криптосистем: теоретико-информационный и теоретико-сложностной. При теоретико-информационном подходе предполагается, что противник не сможет получить никакой информации из перехватываемых им зашифрованных сообщений. Такая абсолютная стойкость, как показал еще К. Шеннон, является достижимой (например, в шифре Вернама), однако требует, чтобы длина ключа была не меньше длины передаваемого сообщения. Это жесткое ограничение заставляет использовать такие стойкие шифры исключительно для передачи редких и очень важных сообщений. Во всех остальных случаях, приходится обращаться к теоретико-сложностному подходу, к обсуждению которого мы и переходим.

В идеале, хорошо бы получить теоретические оценки стойкости шифра, что могло бы гарантировать невозможность вскрытия выбранного шифра, за период, скажем, 20 лет. Однако, существующий уровень развития теории сложности вычислений не дает нужных теорем, поскольку они относятся к нерешенной *проблеме получения нижних оценок вычислительной сложности задач*. Однако, на практике, для повышения обоснованности стойкости шифра это требование заменяется на требование включения в задачу вскрытия шифра *трудной математической задачи*.

Самыми известными на сегодняшний день вычислительно трудными задачами такого сорта являются проблема вычисления *дискретного логарифма и факторизация* (разложение на множители) целых чисел. Использование этих задач для построения шифров описано в последующих разделах, а пока мы закончим обсуждение теоретико-сложностной компоненты в криптографии.

Итак, для задач факторизации чисел (разложения на множители) и нахождения дискретного логарифма в настоящее время неизвестны эффективные (полиномиальные) алгоритмы, несмотря на то, что эти задачи интенсивно исследовались в последние 30 лет. Конечно, такой аргумент не должен нас вполне успокаивать, так как вся история науки (в частности, алгоритмическая теория чисел) показывает, что многие задачи, казавшиеся трудными, решаются затем достаточно просто. Ярким примером подобного результата является недавнее (в 2002 г.) открытие полиномиального детерминированного алгоритма проверки простоты числа, который будет

рассмотрен нами в дальнейшем.

Это явилось побудительным стимулом в криптографии к поиску других вычислительно трудных задач, на которых можно строить стойкие криптосистемы. Еще одним таким стимулом явились результаты Питера Шора о существовании полиномиальных алгоритмов решения задач дискретного логарифмирования и разложения числа на множители на так называемых квантовых вычислителях. Квантовая модель вычислений является вполне реалистичной, хотя споры о возможности создания квантого компьютера не утихают. Скорее это является «тревожным звонком», который может привести затем к построению эффективных алгоритмов решения указанных задач и на обычных моделях вычислений. Все это заставляет искать задачи, для которых неизвестны эффективные квантовые алгоритмы.

В целом можно констатировать, что больших успехов в таком поиске достигнуто не было. Однако, одна интересная задача была найдена, причем с теоретическим обоснованием ее труднорешаемости. Речь идет о результатах венгерского математика Миклоша Айтаи, опубликованных им в 1996 г., о трудности задачи поиска короткого вектора в решетке. Ему удалось доказать, что можно построить случайную решетку с коротким вектором в ней такую, что любой алгоритм нахождения этого вектора в данной случайной решетке можно конвертировать в эффективный алгоритм нахождения достаточно короткого вектора в *любой решетке*. Эти результаты положили начало новому направлению в криптографии, которое на Западе получило название «Lattice based cryptography».

Глава 1

Основные понятия криптографии и теории сложности

Связь с теорией чисел и теорией сложности.

1.1 Дискретный логарифм. Обмен ключами.

Напомним некоторые сведения из алгебры. Для любого простого числа p множество $\mathbf{Z}_p = \{0, 1, \ \ldots, p-1\}$ является полем с операциями умножения и сложения по модулю p. Известно, что $\mathbf{Z}_p^* = \mathbf{Z}_p - \{0\}$ образует циклическую группу по умножению. Любой порождающий элемент этой группы называется примитивным элементом.

Задача 1. *«Дискретный логарифм»*

Даны примитивный элемент g, $b \neq 0$, простое число p. Найти x такое, что

$$g^x \equiv b \pmod{p}.$$

Опишем сейчас применение дискретного логарифма для задачи формирования общего секретного ключа двумя пользователями (задача 2), связанными открытым (для противника) каналом связи.

Задача 2. *«Формирование секретного ключа»*

Абоненты A и B взаимодействуют по открытому каналу связи. Могут ли они, не имея вначале никакой секретной информации, организовать обмен так, чтобы в конце у них появлялся общий секретный ключ. Предполагается, что пассивный противник может перехватить все сообщения, которыми они обмениваются.

Диффи и Хеллман предложили решать эту задачу с помощью дискретного логарифма (алгоритм 1).

Алгоритм 1 Протокол выработки общего секретного ключа

1. A и B независимо друг от друга выбирают по одному натуральному числу X_A и X_B. Эти элементы они держат в секрете.

2. Каждый из них вычисляет новый элемент

$$Y_A \equiv a^{X_A} \pmod{p}, \qquad Y_B \equiv a^{X_B} \pmod{p},$$

   причем числа p и a считаются общедоступными. Потом они обмениваются этими элементами по каналу связи.

3. A получив Y_B и зная свой секретный элемент X_A вычисляет новый элемент

$$Y_B^{X_A} = (a^{X_B})^{X_A} \bmod p.$$

   Аналогично поступает B:

$$Y_A^{X_B} = (a^{X_A})^{X_B} \bmod p.$$

   После этого у A и B появился общий элемент $a^{X_A X_B} \bmod p$, который и объявляется общим ключом.

Задача А. *Противник знает p, a, a^{X_A}, a^{X_B}, но не знает X_A и X_B, и хочет узнать $a^{X_A X_B}$.*

Гипотеза Диффи-Хеллмана. Задача А — вычислительно трудна.

В настоящее время нет алгоритмов решения задачи А, более эффективных чем дискретное логарифмирование. А это — трудная математическая

задача.

1.2 Дискретный логарифм и криптосистема Эль Гамаля

Напомним сначала общее описание криптосистемы блочного шифрования. Открытый текст разрезается на куски одинаковой длины, которые шифруются независимо с помощью некоторого преобразования E следующим образом. Куску открытого текста m и ключу k ставится в соответствие зашифрованный текст $E(m,k)$. В криптосистемах вероятностного шифрования куску открытого текста m и ключу k ставится в соответствие зашифрованный текст $E(m,k,r)$, зависящий еще от строки r случайных бит, которая выбирается заново для каждой пары (m,k). Таким образом, в системах вероятностного шифрования одной и той же паре (m,k) соответствуют разные шифртексты.

Криптосистема Эль Гамаля является криптосистемой вероятностного шифрования, основанной на использовании дискретного логарифма. Пусть G — циклическая группа порядка p и g — ее порождающий элемент. В качестве секретного ключа криптосистемы выбирается случайный элемент x группы Z_{p-1}. Соответствующий открытый ключ вычисляется по формуле $y = g^x$. Криптограмма открытого текста $m \in G$ вычисляется с помощью функции шифрования

$$E(y,m) = (y^r m, g^r),$$

где r — случайный элемент группы Z_{p-1}, т. е. число r выбирается всякий раз заново, независимо и равновероятно.

Дешифрование криптограммы (c_1, c_2) выполняется следующим образом. Сначала вычисляется $c_2^x = g^{rx}$, откуда затем вычисляется $m = c_1/c_2^x$.

Стойкость шифра основана на трудности вычисления x по известному y, т. е. на трудности вычисления дискретного логарифма. Криптосистема Эль Гамаля является криптосистемой вероятностного шифрования. При этом одному открытому тексту соответствуют различные шифртексты. Ее функция шифрования гомоморфна относительно операции умножения от-

крытых текстов: криптограмма произведения может быть вычислена как произведение (попарное) криптограмм сомножителей.

Если $E(y, m_1) = (y^{r_1}m_1, g^{r_1})$ и $E(y, m_2) = (y^{r_2}m_2, g^{r_2})$, то $E(y, m_1m_2)$ можно получить в виде $(y^{r_1}y^{r_2}m_1m_2, g^{r_1}g^{r_2})$.

Функция шифрования криптосистемы Эль Гамаля обладает свойством ерандомизации. Криптограмму произведения, полученную в указанном выше виде, можно рандомизировать, выбрав случайное число r из Z_{p-1} и домножив первый элемент криптограммы на y^r, а второй — на g^r.

Таким образом будет получена криптограмма $(y^{r_1}y^{r_2}y^r m_1m_2, g^{r_1}g^{r_2}g^r)$, связь которой с исходными криптограммами «затемнена».

1.3 Односторонние функции

Трудности с обоснованием стойкости криптосистем привели к тому, что стали выделять некий примитив, существование которого позволяет строить стойкие криптосистемы. В качестве основного примитива в настоящее время рассматриваются односторонние функции.

Центральным понятием «новой криптографии», которая начала формироваться с конца 70-х годов XX века после исторической статьи Диффи и Хеллмана, является понятие односторонней функции. Не совсем строго односторонней называют эффективно вычислимую функцию, обратная к которой трудно вычислима. Итак,

Определение 1.3.1. ***Односторонней*** *называется функция $F : X \to Y$, обладающая двумя свойствами:*

1. *существует полиномиальный алгоритм вычисления значений $F(x)$;*
2. *не существует полиномиального алгоритма инвертирования функции F (т. е. вычисления обратной функции — решения уравнения $F(x) = y$ относительно x).*

Это не совсем формальное определение. Более формально свойство 2 формулируется так: любая полиномиальная вероятностная машина Тьюринга T по $y \in Y$ может найти x из уравнения $F(x) = y$ лишь с пренебрежимо малой вероятностью (меньше $\frac{1}{p(n)}$ для любого полинома $p(n)$, где

n — длина входа), т. е.

$$P\{F(T(F(x))) = F(x)\} < \frac{1}{p(n)}.$$

Здесь вероятность берется по равномерно распределенному $x \in X$ и случайным битам вероятностного алгоритма T. При этом рассматривается дополнительное ограничение на мощность X: считается, что она не превосходит некоторого полинома от мощности Y.

Вопрос о существовании односторонних функций пока открыт и является одним из центральных в теоретической криптографии и теории сложности. Однако есть функции, которые предположительно являются односторонними. Одна из них — *дискретный логарифм* (уже упоминавшийся в разделе **??**).

Как мы видели только что, требование трудности вычисления обратной к односторонней функции формулируется с использованием сложности на случайных исходных данных (а не в худшем случае, что более привычно в теории сложности). В связи с этим значительный интерес представляют задачи, в которых из сложности в худшем случае вытекает ее сложность в среднем. Дискретный логарифм обладает этим интересным свойством: если эта функция сложна в *худшем случае*, то сложна и *в среднем*. Доказательство этого свойства простое, и мы приведем его сейчас, предварительно дав более точную формулировку. Пусть $\mathbf{Z}_p^*$ обозначает мультипликативную группу поля $\mathbf{Z}_p$, g — ее примитивный элемент.

Теорема 1. *Пусть существует полиномиальный алгоритм A, который при случайном и равномерном выборе $b \in \mathbf{Z}_p^*$ правильно решает задачу дискретного логарифмирования на доле b не менее $1/n^{O(1)}$ (здесь n обозначает длину двоичной записи b).*

Тогда существует полиномиальный по n вероятностный алгоритм, который находит дискретный логарифм для всех b.

Доказательство. Построим новый вероятностный алгоритм B:

1. выберем x' случайно и равномерно из $\mathbf{Z}_{p-1}$
2. вычислим $g^{x'} \bmod p$

3. вычислим $b' = bg^{x'} \bmod p$.

Заметим, что величина $g^{x'} \bmod p$ равномерно распределена в $\mathbf{Z}_p^*$ (упражнение 1.3.1).

Тогда b' — случайный элемент, равномерно распределенный в $\mathbf{Z}_p^*$ (упражнение 1.3.2).

А далее все просто. Применим алгоритм A к b': при этом мы получим ответ с вероятностью не менее $1/n^{O(1)}$.

А по нему очень легко восстановить ответ для исходной задачи, т. е. найти дискретный логарифм b. Действительно, дискретный логарифм от b' по определению равен $x + x'$, т.к. $g^x g^{x'} = g^{x+x'}$. Но мы знаем x', поэтому легко можем найти x.

Далее используя стандартную технику усиления (амплификации, т. е. повторяя для данного b независимо эту процедуру полиномиальное число раз), можно сделать вероятность ошибки экспоненциально малой. □

Упражнение 1.3.1. Выберем x случайно и равномерно из $\mathbf{Z}_{p-1}$. Докажите, что величина $g^x \bmod p$ равномерно распределена в $\mathbf{Z}_p^*$.

Упражнение 1.3.2. Выберем x случайно и равномерно из $\mathbf{Z}_{p-1}$. Докажите, что для любого фиксированного $b \neq 0$ величина $b' = bg^x \bmod p$ равномерно распределена в $\mathbf{Z}_p^*$.

Дадим определение криптосистем с открытым ключом и посмотрим, почему для существования достаточно стойких криптосистем с открытым ключом *необходимо существование односторонних функций*.

Определение 1.3.2. *Криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей F, шифрования E и дешифрования D.*

Все эти алгоритмы предполагаются полиномиальными. Алгоритм генерации ключей известен всем: любой может подать ему на вход случайную строку r нужной длины и получить пару ключей (e, d), где e — открытый, а d — секретный ключ. По условию корректности криптосистемы для любого открытого текста m, алгоритма шифрования E_e и алгоритма дешифрования D_d должно выполняться соотношение: $D_d(E_e(m)) = m$.

Покажем, что F должна быть односторонней функцией, иначе система не будет стойкой. Предположим, что существует полиномиальный вероятностный алгоритм A, который инвертирует F с вероятностью не менее $1/p(n)$ для некоторого полинома $p(n)$, где n — длина открытого ключа e. Противник может подать на вход алгоритма A ключ e и получить с указанной вероятностью значение из прообраза r'. Далее ему остается только подать r' на вход алгоритма генерации ключей F и получить пару ключей (e, d'). По определению криптосистемы для любого открытого текста m должно выполняться $D_{d'}(E_e(m)) = m$. Таким образом, секретный ключ найден с вероятностью не менее $1/p(n)$ и, используя процедуру амплификации, эту вероятность можно сделать близкой к единице, запуская алгоритм полиномиальное число раз.

1.4 Система RSA и ее анализ

Еще одним новым понятием криптографии является понятие *функции с секретом*.

Определение 1.4.1. ***Функцией с секретом*** K *называется функция* $F_K : X \to Y$*, зависящая от параметра* K *и обладающая следующими свойствами:*

1. *при любом* K *существует полиномиальный алгоритм вычисления значений* $F_K(x)$*;*

2. *при неизвестном* K *не существует полиномиального алгоритма инвертирования* F_K*;*

3. *при известном* K *существует полиномиальный алгоритм инвертирования* F_K*.*

Существование таких функций также не доказано, но для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом.

Для них свойство 2 пока строго не доказано, но считается, что задача инвертирования эквивалентна некоторой давно изучаемой трудной (с алгоритмической точки зрения) математической задаче. Наиболее известной и популярной из них является теоретико-числовая функция, на которой построен шифр RSA.

Сначала приведем общую схему *криптосистемы с открытым ключом*.

1. Пользователь A, который хочет получать шифрованные сообщения, должен выбрать какую-нибудь функцию F_K с секретом K.

2. Он публикует описание функции F_K в качестве своего алгоритма шифрования. При этом значение секрета K он никому не сообщает и держит в секрете.

3. Пользователь B посылает пользователю A защищаемую информацию $x \in X$, вычисляя $y = F_K(x)$ и посылая y по открытому каналу пользователю A.

4. Поскольку A знает секрет K, то он умеет эффективно инвертировать F_K. Он вычисляет x по полученному y. Никто другой не знает K и, поэтому, в силу свойства 2 функции с секретом, не сможет за полиномиальное время по шифрованному сообщению $F_K(x)$ вычислить защищаемую информацию x.

Схема RSA устроена следующим образом (алгоритм 2).
Докажем сейчас однозначность декодирования.

Теорема 2. *Для всех* x

$$x^{ed} \equiv x \pmod{n}.$$

Доказательство. Имеем

$$ed \equiv 1 \pmod{\varphi(n)},$$

откуда получаем, что для некоторого k

$$ed = 1 + k(p-1)(q-1).$$

Алгоритм 2 Схема RSA

1. Выбирают два достаточно больших простых числа p и q (обычно около 100 десятичных знаков).

2. Находят $n = pq$.

3. Выбирают число e, взаимно-простое с $p-1$ и $q-1$:

$$\text{нод}(e, p-1) = \text{нод}(e, q-1) = 1.$$

   Здесь и далее нод(a, b) обозначает наибольший общий делитель чисел a и b.

4. Вычисляют функцию Эйлера $\varphi(n)$, равную числу натуральных чисел, не превосходящих n и взаимно-простых с ним по формуле:

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

5. Находят целое число d такое, что

$$de \equiv 1 \pmod{\varphi(n)}, \qquad 1 \le d < \varphi(n).$$

   Такое число существует и единственно, поскольку нод$(e, \varphi(n)) = 1$.

- Функция F_K, реализующая шифрование в схеме RSA устроена следующим образом:
$$F_K : \ x \to x^e \bmod n.$$

- Дешифрование осуществляется функцией

$$G(a) = a^d \bmod n.$$

Секретом является число p (или q) в разложении n на простые множители (или d).

Пусть $x \neq 0$. Малая теорема Ферма гласит, что $x^{p-1} \equiv 1 \pmod{p}$, откуда мы получаем, что

$$\begin{aligned} x^{ed} &\equiv x(x^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv x(1)^{k(q-1)} \pmod{p} \\ &\equiv x \pmod{p}. \end{aligned}$$

Если же $x = 0$, то тривиально имеем $x^{ed} \equiv x \pmod{p}$.

Аналогично рассматриваем соотношения по модулю q и получаем, что для всех x

$$x^{ed} \equiv x \pmod{q}.$$

Теперь остается применить китайскую теорему об остатках, которая гласит: для взаимно-простых чисел $r_1, \ldots, r_k$ любое число $0 \leq n < r_1 \cdot \ldots \cdot r_k$ однозначно восстанавливается по остаткам

$n \equiv n_1 \pmod{r_1}$, $n \equiv n_2 \pmod{r_2}$, ..., $n \equiv n_k \pmod{r_k}$.

По китайской теореме об остатках имеет место соотношение:

$$x^{ed} \equiv x \pmod{pq}.$$

□

Как осуществить шаги 1-5? Шаги 2 и 4 выполняются очевидным образом.

Шаг 1 выполняется с использованием эвристики: выбираются числа из некоторой арифметической прогрессии и проверяются на простоту эффективным (полиномиальным) алгоритмом. В силу силу гипотезы Крамера о том, что в любом интервале от n до $n + O(\log^2 n)$ при достаточно больших n есть простое число, число проверок на простоту можно ограничить полиномом от $\log n$. Шаг эвристический, поскольку гипотеза Крамера далека от того, чтобы быть доказанной, но на практике этот метод работает весьма эффективно.

Шаг 3 выполняется с использованием алгоритма Евклида.

Шаг 5 также выполняется с использованием алгоритма Евклида, точнее некоторого его обобщения. А именно, ищется решение сравнения

$$xe \equiv 1 \pmod{\varphi(n)},$$

что равносильно поиску целых решений (x, y) уравнения $ex + y\varphi(n) = 1$. Для последней задачи используется следующая модификация алгоритма Евклида.

Алгоритм решения уравнения $ax + by = 1$.

На чем основана стойкость системы RSA? Из изложенного выше видно, что единственным препятствием к нахождению секретного ключа d, позволяющего расшифровывать все сообщения, является незнание сомножителей p и q. Значит, если мы в состоянии эффективно разложить на множители $n = pq$, то система RSA не является стойкой. Для задачи факторизации чисел (разложения на множители) в настоящее время неизвестны эффективные (полиномиальные) алгоритмы, несмотря на то, что эта задача интенсивно исследовалась в последние 30 лет. Конечно, такой аргумент не должен нас вполне успокаивать, так как вся история науки (в частности, алгоритмическая теория чисел) показывает, что многие задачи, казавшиеся трудными, решаются затем достаточно просто. Ярким примером подобного результата является недавнее открытие полиномиального детерминированного алгоритма проверки простоты числа, который будет рассмотрен нами в дальнейшем.

Миклош Айтаи в 1996 г. доказал, что можно построить случайную решетку с коротким вектором в ней такую, что любой алгоритм нахождения этого вектора в данной случайной решетке можно конвертировать в эффективный алгоритм нахождения достаточно короткого вектора в *любой решетке*. Это по виду похоже на теорему 1 для дискретного логарифма, но там параметры p и g не были случайными, что оставляет слабости в интерпретациях сводимости от сложности «в среднем» к сложности «в худшем случае» для дискретного логарифма.

Эти результаты положили начало новому направлению в криптографии, которое на Западе получило название «Lattice based cryptography» и элементы которого мы предполагаем рассмотреть в данном курсе лекций.

В качестве подготовительного раздела мы рассматриваем основные факты из теории колец, полей и решеток, необходимые для описания криптосистем на решетках. Довольно удивительным образом оказывается, что многие из этих фактов необходимы и для доказательства корректности полиномиального алгоритма проверки простоты числа. Именно на этом до-

казательстве мы иллюстрируем ряд приложений алгебраической техники из теории колец полиномов.

В заключение данного раздела приведем пару упражнений, связанных с важными свойствами криптосистемы RSA.

Упражнение 1.4.1. Система RSA является мультипликативной в том смысле, что произведение кодов равно коду произведения

$$x^e y^e \pmod{n} \equiv (xy)^e \pmod{n}.$$

Используя этот факт докажите, что если противник имеет алгоритм расшифровки 1 процента сообщений случайно выбранных из $\mathbf{Z}_n$, то он может переработать его в вероятностный алгоритм расшифровки произвольного сообщения, закодированного кодом RSA, с большой вероятностью (аналогично теореме 1).

Упражнение 1.4.2. Докажите, что если противник найдет каким-либо образом секретный ключ d, то он сможет эффективно разложить число n на множители.

Этот факт означает, что нахождение секретного ключа в системе RSA на самом деле эквивалентно разложению n на множители.

1.5 Основные понятия теории сложности

План

1. Интуитивное понятие алгоритма и его сложности
2. Модель RAM. Однородная и логарифмическая сложность. Примеры с однородной сложностью (RSA и др.)
3. Полиномиальность и эффективность
4. Машины Тьюринга. Классы сложности
5. Теория NP-полноты
6. Схемы

1. Интуитивное понятие алгоритма и его сложности

Неформально, можно понимать алгоритм, как запись последовательности некоторых элементарных операторов, причем существуют однозначные правила интерпретации записи и выполнения этих операторов. Для того, чтобы формализовать это понятие, нужно определиться с субъектами этих операторов, и ввести некоторую модель интерпретатора.

В предыдущих разделах мы довольствовались качественным, интуитивным понятием «эффективного» алгоритма. Для построения же математической теории сложности алгоритмов, разумеется, необходимо строгое количественное определение меры эффективности.

Опыт, накопленный в теории сложности вычислений, свидетельствует, что наиболее удобным и адекватным способом сравнения эффективности разнородных алгоритмов является понятие *асимптотической сложности*, рассмотрению которого и посвящен настоящий параграф.

Первое, о чем следует договориться, — это выбор вычислительной модели, в которой конструируются наши алгоритмы. Оказывается, что как раз этот вопрос не имеет слишком принципиального значения для теории сложности вычислений, и тот уровень строгости, на котором мы работали в разделе **??** — число выполненных элементарных операций (или операторов на языке Python), оказывается почти приемлемым. Главная причина такого отношения к выбору модели состоит в том, что существуют весьма эффективные способы моделирования (или *трансляции программ* в более привычных терминах) одних естественных вычислительных моделей с помощью других. При этих моделированиях сохраняется класс эффективных алгоритмов и, как правило, алгоритмы более эффективные в одних

моделях оказываются более эффективными и в других.

Ниже мы рассмотрим три модели вычислений: модель RAM, машины Тьюринга и булевы схемы.

2. Модель RAM. Однородная и логарифмическая сложность. Примеры с однородной сложностью (RSA и др.)

Сначала рассмотрим модель, наиболее напоминающую современный компьютер, программируемый непосредственно в терминах инструкций процессора (или на языке Assembler): *random access machines (RAM)*[1], т. е. «машины с произвольным доступом к памяти».

RAM-машину составляют следующие компоненты (рис. 1.1).

- Конечная входная *read-only* лента, на которую записываются входные данные.

- Полубесконечная[2] выходная *write-only* лента, куда записывается результат работы машины.

- Бесконечное число регистров $r_0, r_1, r_2, \ldots$, каждый из которых может хранить произвольное целое число (изначально везде записаны нули). Регистр r_0 является выделенным и называется «сумматором» — этот регистр используется при арифметических операциях как накопитель, т. е. как второй операнд и место хранения результата.

- Программа, состоящая из конечного числа инструкций, каждая из которых содержит адрес и команду с операндом. Список команд приведен в таблице 1.1. Существенно, что в качестве операнда можно использовать как произвольный регистр, так и регистр, номер которого хранится в другом регистре — это так называемая косвенная адресация.

- Регистр-счетчик «PC» — указатель текущей команды.

[1] В теории сложности вычислений под *машинами* традиционно понимают single-purpose machines, т. е. машины, каждая из которых создана для решения какой-либо одной фиксированной задачи. В привычных терминах это скорее программы.

[2] Ограниченная с одной стороны и неограниченная с другой.

Машина последовательно, такт за тактом, выполняет команды, на которые указывает регистр «PC», читает входную ленту, изменяет значения регистров и записывает результат на выходную ленту.

Легко видеть, что высокоуровневые конструкции языков программирования, типа циклов, легко моделируются на ассемблере RAM-машин (см. рис. 1

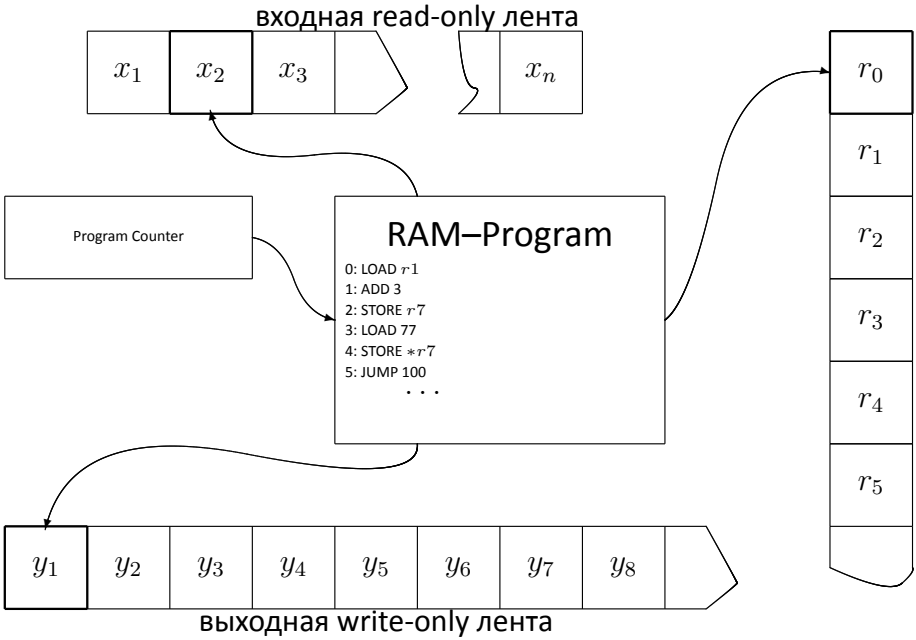


Рис. 1.1: RAM — машина с произвольным доступом

Переменные других типов (булевы, строки, структуры) тоже можно моделировать с помощью целых чисел и косвенной адресации.

Обратите внимание, что, несмотря на «примитивный ассемблер», RAM-машины потенциально мощней любых существующих компьютеров и физически нереализуемы, т.к. оперируют бесконечной памятью, где доступ к любой ячейке-регистру осуществляется мгновенно при выполнении соответствующей инструкции, и каждая ячейка этой памяти может содер-

Таблица 1.1: RAM-машина: Список команд

LOAD OP	$r_0 \leftarrow OP$	Загрузить операнд в сумматор.
STORE OP	$r_{OP} \leftarrow r_0$	Сохранить сумматор в регистре.
ADD OP	$r_0 \leftarrow r_0 + OP$	Прибавить операнд к сумматору.
SUB OP	$r_0 \leftarrow r_0 - OP$	Вычесть операнд из сумматора.
READ OP	$r_{OP} \leftarrow input$	Загрузить ячейку из входной ленты в r_{OP} и перейти к следующей.
WRITE OP	$OP \rightarrow output$	Записать OP в текущую ячейку выходной ленты и сдвиг к следующей.
JUMP OP	$PC \leftarrow OP$	Установить счетчик команд в OP.
JGTZ OP	$PC \leftarrow OP : r_0 > 0$	Установить счетчик команд в OP, если $r_0 > 0$.
JZERO OP	$PC \leftarrow OP : r_0 = 0$	Установить счетчик команд в OP, если $r_0 = 0$.
HALT		Остановить работу.

Операнд OP может быть:

- целым числом, например, 7, -1917;
- регистром, например, r_{12}, r_{34};
- значением регистра, указанного в другом регистре. Например, операнд $*r_{14}$ означает значение регистра, номер которого указан в регистре r_{14}.

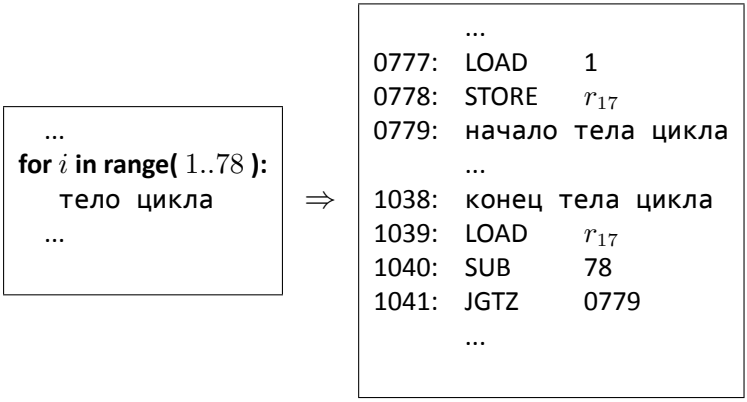


Рис. 1.2: Моделирование циклов для RAM

жать произвольное целое число (т. е. не ограничена по размеру). Но эта модель уже дает возможность вводить более или менее формальные определения времени выполнения программы (как число тактов до остановки машины) и соответственно сложности алгоритма.

Если мы будем принимать в расчет только число выполненных команд, то определим так называемые *однородные* меры сложности. В англоязычной литературе RAM с однородной мерой сложности называются *unit-cost RAM*.

Более реалистично было бы учитывать битовый размер операндов при выполнении каждой команды. Например, можно считать, что время выполнения каждой команды есть единица плюс величина пропорциональная сумме логарифмов значений операндов[3], если они есть (т. е. их суммарной битовой длине), а общее время работы программы на рассматриваемых входных данных — суммарное время выполнения всех индивидуальных команд. Таким образом, мы можем определить различные *логарифмические* меры сложности.

Очевидно, логарифмическая сложность всегда больше однородной. С другой стороны, обратите внимание, что определенная нами RAM-машина

[3]Более корректно логарифм брать от модуля операнда плюс 2, чтобы логарифм был положительным.

не включает в число основных операций умножение и деление, хотя в литературе такой вариант машин со случайным доступом часто рассматривается. Допустим, что однородное время работы некоторой машины с произвольным доступом к памяти *без умножения и деления* при работе на входных данных $x_1, \ldots, x_m$, битовая длина каждого из которых не больше n, равно t. Так как при выполнении любого индивидуального оператора максимальная битовая длина может возрасти не более чем на 1, в ходе выполнения всей программы встречаются лишь числа битовой длины не более $(t + n)$, и, стало быть, логарифмическая сложность превышает однородную не более чем в $2(t + n)$ раз. В частности (см. обсуждение в разделе **??**), с точки зрения эффективности однородная и логарифмическая сложности равносильны, и выбор одной из них в основном определяется внутренней спецификой рассматриваемой задачи.

Если же добавить умножение и деление к списку элементарных операций, то это исключит равносильность однородной и логарифмической сложности. Следующий известный способ быстро переполнить память карманного калькулятора (алгоритм 3) имеет однородную сложность $(t + 1)$ и логарифмическую порядка экспоненты — 2^t.

Алгоритм 3 Переполнение памяти из-за умножения

Вход: Натуральное t

```
R ← 2
for all i ∈ 1..t do
  R ← R × R
end for
```

Алгоритм 4 Простое вычисление $R_1 \cdot R_2$ на RAM

Вход: Натуральные R_1, R_2

Выход: $R_1 \times R_2$

```
R ← 0
for all i ∈ 1..R_1 do
  R ← R + R_2
end for
return R
```

Как показывает обсуждение в разделе **??**, этот алгоритм не может считаться эффективным с точки зрения логарифмической сложности (хотя и по совершенно другим причинам, нежели переборные алгоритмы), и, чтобы избежать неприятных эффектов такого рода, мы не включаем умножение (и тем более деление) в список основных операций.

В тех же случаях, когда умножение используется «в мирных целях», его в большинстве случаев можно промоделировать с помощью сложения очевидным образом (см. алгоритм 4).

В заключение можно отметить, что некоторые частные случаи модели RAM описывают популярные модели вычислений — *неветвящиеся* программы, булевы схемы[4], а сама модель RAM является основой модели, используемой в теории параллельных вычислений — PRAM[5].

3. Полиномиальность и эффективность

4. Машины Тьюринга. Классы сложности

Одной из самых простых и распространенных в теории сложности моделей является Машина Тьюринга, выполняющая элементарные и последовательные преобразования строк, т. е. наборов атомарных символов из некоторого алфавита (множества символов). В виде строк можно представить любой информационный объект — натуральное или рациональное число, матрицу, полином, граф и даже алгоритм. Машина Тьюринга — это простой автомат с минимумом правил, выполняющий преобразования строк, размещенных на одной или нескольких лентах.

Определение 1.5.1. ***Машина Тьюринга*** *— это набор* $T = \langle k, \Sigma, \Gamma, \alpha, \beta, \gamma \rangle$*, где*

- $k \geq 1$ *— число лент;*
- Σ *— алфавит лент,* $\star \in \Sigma$ *— символ-пробел;*
- Γ *— конечное множество состояний,* $S, Q \in \Gamma$ *— выделенные состояния: запуск машины и завершение работы;*

[4] Boolean circuits.

[5] Parallel RAM.

- α, β, γ — *произвольные отображения:*

$$\alpha : \Gamma \times \Sigma^k \to \Gamma,$$
$$\beta : \Gamma \times \Sigma^k \to \Sigma^k,$$
$$\gamma : \Gamma \times \Sigma^k \to \{-1, 0, 1\}^k.$$

т. е. отображение α задает новое состояние, отображение β — символы для записи на ленты, γ — перемещение головок.

Таким образом, машина Тьюринга задается таблицей команд размером $|\Sigma|^k \times |\Gamma|$, задающей правила работы машины в соответствии с функциями α, β, γ.

Под *входом* для МТ подразумевается набор из k слов (k-кортеж) из Σ^*, записанных справа от стартовых позиций на k лентах МТ. Обычно входные данные записывают только на первую ленту, и под входом x подразумевают k-кортеж $\langle x, \emptyset, \ \ldots, \emptyset \rangle$.

Результатом работы МТ на некотором входе X считается слово, записанное на последней ленте после остановки МТ (слова, записанные на остальных лентах, принято игнорировать).

Теперь можно ввести строгое определение вычислимости.

Определение 1.5.2. *Функция $f : N \to N$ является **вычислимой**, если существует такая машина Тьюринга* T*, что если на вход ей подать представленный в некоторой кодировке **x**, то*

1. *если функция f определена на **x**, и $f(\boldsymbol{x}) = \boldsymbol{y}$, то машина* T *останавливается на входе **x**, и на выходе у нее записано **y**;*

2. *если функция f не определена на **x**, то машина* T *зацикливается (не останавливается за любое конечное число шагов) на входе **x**.*

Аналогичным образом определяется понятие разрешимости и вычислимости для языков и других множеств[6].

[6]Обратите внимание, что в теории формальных языков (теории реализации языков программирования, теории автоматных языков и регулярных выражений) принято говорить, что язык распознается автоматом, если автомат останавливается на словах из этого языка и не останавливается на остальных. В теории сложности для распознавания языка требуется, чтобы распознающая машина Тьюринга останавливалась на всех словах.

Определение 1.5.3. *Множество S (язык L) является **разрешимым**, если существует такая машина Тьюринга* T*, что если на вход ей подать элемент $x \in S$ (слово $l \in L$), то она остановится и выведет «1».*

Иначе ($x \notin S$, $l \notin L$), T *останавливается и выводит «0».*

Если некоторая машина Тьюринга не «зависает» ни на одном из входных слов, то для нее можно определить *временную сложность в худшем случае*.

Определение 1.5.4. *Пусть $t : N \to N$. Машина Тьюринга* T *имеет **временную сложность** (time complexity) $t(n)$, если для каждого входного слова длины n* T *выполняет не больше $t(n)$ шагов до остановки. Также будем обозначать временную сложность машины Тьюринга* T*, как $time_T(n)$.*

Основываясь на лучшей временной сложности среди всех машин распознающих некоторый язык, можно определить следующие классы языков.

Определение 1.5.5. *Язык $L \subset \Sigma^*$ принадлежит классу $\mathcal{DTIME}(t(n))$, если существует машина Тьюринга* T*, разрешающая данный язык, и $\forall n$: $time_T(n) \leq t(n)$.*

Определение 1.5.6.

$$\mathcal{P} \equiv \cup_{k \geq 0} \mathcal{DTIME}(n^k).$$

Определение 1.5.7.

$$\mathcal{EXPTIME} \equiv \cup_{k \geq 0} \mathcal{DTIME}(2^{n^k}).$$

Аналогично временной сложности, можно определить *пространственную* (или *емкостную*) сложность, отражающую потребление алгоритмом «памяти», и ввести соответствующие классы сложности.

Определение 1.5.8. *k-ленточная машина Тьюринга (произвольное $k > 0$)* T *имеет **пространственную сложность** $s(n)$, если для любого входного слова длины n* T *просматривает не более $s(n)$ ячеек на всех рабочих лентах (исключая входную ленту).*

Определение 1.5.9. *Язык $L \subset \Sigma^*$ принадлежит классу $\mathcal{DSPACE}(s(n))$, если существует машина Тьюринга* T*, разрешающая данный язык, и пространственная сложность* T *не превосходит $s(n)$.*

Определение 1.5.10.

$$\mathcal{PSPACE} \equiv \cup_{k\geq 0}\mathcal{DSPACE}(n^k).$$

Алгоритмическая задача называется *труднорешаемой*, если для нее не существует полиномиального алгоритма.

5. Теория NP-полноты

Для анализа сложности переборных задач дискретной оптимизации используется теория $\mathcal{NP}$-полноты, основой которой является понятие *полиномиальной сводимости*.

Определение 1.5.11. *Задача разрешения P_1* ***полиномиально сводится*** *к задаче разрешения P_2, если*

- *существует полиномиально вычислимая функция $f : I_1 \to I_2$, (отображает входные данные I_1 для P_1 во входные данные $I_2 \equiv f(I_1)$ для задачи P_2),*
- *$\forall I_1$ совпадают ответы на вопросы «$P_1(I_1)$?» и «$P_2(f(I_1))$?».*

Далее, мы можем ввести класс задач, определяющий задачи переборной оптимизации.

Определение 1.5.12. *Язык $L \subseteq \Sigma^*$ принадлежит классу $\mathcal{NP}$, если существуют полиномиальная детерминированная машина Тьюринга* M *и полином $p(\cdot)$, такие, что*

$$L = \{x \in \Sigma^* : \exists\, y,\ |y| < p(|x|)\&\ \mathsf{M}(x, y) = 1\}.$$

Слово y называется обычно «подсказкой», «свидетелем» ($\mathcal{NP}$-*witness*), «доказательством» ($\mathcal{NP}$-*proof*).

С помощью полиномиальной сводимости из определения 1.5.12 «$\mathcal{NP}$/ДМТ» определим класс наиболее сложных переборных задач.

Определение 1.5.13. *Задача разрешения называется $\mathcal{NP}$-полной*[7]*, если*

- *она принадлежит классу $\mathcal{NP}$,*
- *произвольная задача из $\mathcal{NP}$ сводится к ней полиномиально (См. определение 1.5.11 «Сводимость по Карпу»).*

Класс $\mathcal{NP}$-полных задач обозначается $\mathcal{NPC}$.

Также, интерес представляет и класс-дополнение

$$\text{co}\mathcal{NP} \equiv \{L | \overline{L} \in \mathcal{NP}\},$$

состоящий из языков-дополнений к языкам из класса $\mathcal{NP}$ (не путать с теоретико-множественным дополнением к самому классу $\mathcal{NP}$).

[7] Чтобы не перегружать лекции излишней терминологией, мы будем называть в дальнейшем оптимизационную задачу $\mathcal{NP}$-*полной*, если $\mathcal{NP}$-полна соответствующая задача разрешения.

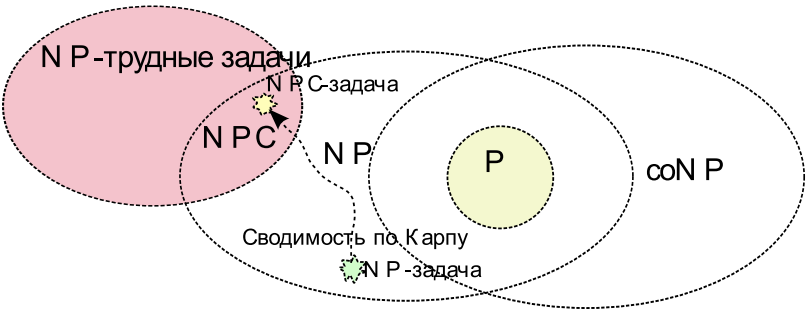


Рис. 1.4: Классы $\mathcal{NP}$, co$\mathcal{NP}$, $\mathcal{P}$, $\mathcal{NPC}$

Определение 1.5.14. *Класс сложности $\mathcal{RP}$ состоит из всех языков L, для которых существуют некий полином $p(\cdot)$ и полиномиальная МТ $\mathsf{M}(x,y)$, такая, что:*

$$\begin{aligned} x \in L &\Rightarrow \frac{|\{y : \mathsf{M}(x,y) = 1, |y| \leq p(|x|)\}|}{2^{p(|x|)}} \geq \frac{1}{2}, \\ x \notin L &\Rightarrow \forall y \quad \mathsf{M}(x,y) = 0. \end{aligned}$$

Определение 1.5.15. *Класс сложности co$\mathcal{RP}$ состоит из всех языков L, для которых существуют некий полином $p(\cdot)$ и полиномиальная МТ $\mathsf{M}(x,y)$,*

такая, что:

$$\begin{aligned} x \in L &\Rightarrow \forall y \quad \mathsf{M}(x,y) = 1, \\ x \notin L &\Rightarrow \frac{|\{y : \mathsf{M}(x,y) = 0, |y| \le p(|x|)\}|}{2^{p(|x|)}} \ge \frac{1}{2}. \end{aligned}$$

Определение 1.5.16.

$$\mathcal{ZPP} \equiv \mathcal{RP} \cap \mathsf{co}\mathcal{RP}.$$

Определение 1.5.17. ***Вероятностная машина Тьюринга*** *представляет собой детерминированную машину Тьюринга (см. опр. 1.5.1 «Машина Тьюринга»), имеющую дополнительно источник случайных битов, любое число которых, например, она может «заказать» и «загрузить» на отдельную ленту и потом использовать в вычислениях обычным для МТ образом.*

Определение 1.5.18. *Класс сложности $\mathcal{BPP}$ (Bounded-Probability Polynomial Time) состоит из всех языков L, для которых существует полиномиальная ВМТ* M*, такая, что:*

$$\begin{aligned} x \in L &\Rightarrow P[\mathsf{M}(x) = 1] \ge \frac{2}{3}, \\ x \notin L &\Rightarrow P[\mathsf{M}(x) = 0] \ge \frac{2}{3}. \end{aligned}$$

Определение 1.5.19. *Алгоритм называется C-**приближенным**, если при любых исходных данных он находит допустимое решение со значением целевой функции, отличающимся от оптимума не более чем в C раз.*

Определение 1.5.20. *Класс $\mathcal{APX}$ состоит из всех оптимизационных задач, для которых существуют полиномиальные приближенные алгоритмы с мультипликативной ошибкой, не превышающей некоторой абсолютной константы (см. определение 1.5.19 «C-приближенный алгоритм»).*

6. Булевы схемы

Схема (булева)[8] — это способ вычислить функцию $f : \{0,1\}^n \to \{0,1\}^m$.

Помимо исходных переменных $x_1, \ldots, x_n$, для которых вычисляется значение f, схема использует некоторое количество вспомогательных переменных $y_1, \ldots, y_s$ и некоторый набор (*базис*) булевых функций $\mathcal{F}$.

Схема S в базисе $\mathcal{F}$ определяется последовательностью *присваиваний* $Y_1, \ldots, Y_s$.

Каждое присваивание Y_i имеет вид

$$y_i := f_j(u_{k_1}, \ldots, u_{k_r}),$$

где $f_j(\cdot) \in \mathcal{F}$, а переменная u_{k_p} $(1 \le p \le r)$ — это либо одна из исходных переменных x_t $(1 \le t \le n)$, либо вспомогательная переменная y_l с меньшим номером $(1 \le l < i)$.

Таким образом, для каждого набора значений исходных переменных последовательное выполнение присваиваний, входящих в схему, однозначно определяет значения всех вспомогательных переменных. *Результатом вычисления* считаются значения последних m переменных $y_{s-m+1}, \ldots, y_s$.

Схема *вычисляет* функцию f, если для любых значений $x_1, \ldots, x_n$ результат вычисления — $f(x_1, \ldots, x_n)$.

Определение 1.5.21. *Схема называется **формулой**, если каждая вспомогательная переменная используется в правой части присваиваний только один раз.*

Обычные математические формулы именно так задают последовательность присваиваний: «внутри» формул не принято использовать ссылки на их части или другие формулы.

Схему можно также представлять в виде ориентированного ациклического графа, у которого

- вершины входной степени 0 (*входы*) помечены исходными переменными;

[8] В русскоязычной литературе часто используется термин — схемы из функциональных элементов.

- остальные вершины (*функциональные элементы*) помечены функциями из базиса;
- дуги помечены числами, указывающими номера аргументов;
- вершины выходной степени 0 (*выходы*) помечены переменными, описывающими результат работы схемы.

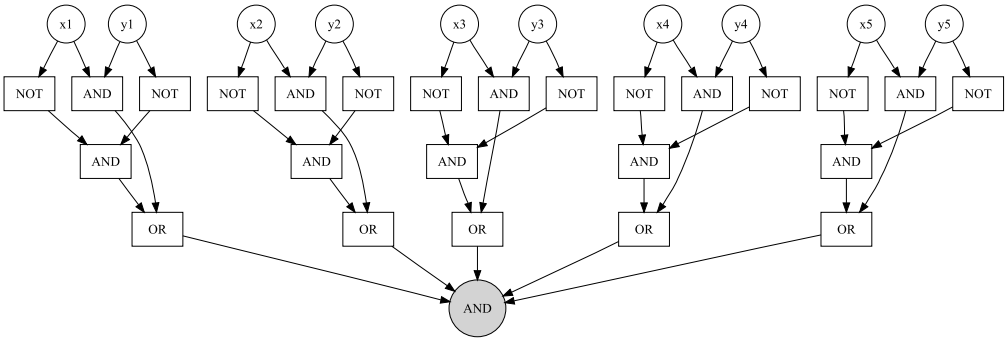


Рис. 1.5: Пример схемы: сравнение двух строк

Вычисление на графе определяется индуктивно: как только известны значения всех вершин $y_1, \ldots, y_{k_v}$, дуги из которых ведут в данную вершину v, вершина v получает значение $y_v = f_v(y_1, \ldots, y_{k_v})$, где f_v — базисная функция, которой помечена вершина.

При переходе к графу схемы мы опускаем *несущественные присваивания*, которые ни разу не используются на пути к выходным вершинам, так что они никак не влияют на результат вычисления.

Определение 1.5.22. *Базис называется **полным**, если для любой булевой функции f есть схема в этом базисе, вычисляющая f.*

Ясно, что в полном базисе можно вычислить произвольную функцию $f : \{0,1\}^n \to \{0,1\}^m$ (такую функцию можно представить как упорядоченный набор из m булевых функций).

Булева функция может быть задана таблицей значений. Приведем таблицы значений для трех функций

$$NOT(x) = \neg x,$$
$$OR(x_1, x_2) = x_1 \vee x_2,$$
$$AND(x_1, x_2) = x_1 \wedge x_2,$$

(*отрицание*, *дизъюнкция*, *конъюнкция*), образующих полный базис, который будем считать стандартным. В дальнейшем имеются в виду схемы именно в этом базисе, если явно не указано что-либо иное.

x	NOT
0	1
1	0

x_1	x_2	OR
0	0	0
0	1	1
1	0	1
1	1	1

x_1	x_2	AND
0	0	0
0	1	0
1	0	0
1	1	1

Конъюнкция и дизъюнкция определяются для произвольного числа n булевых переменных аналогичным образом: конъюнкция равна 1 только тогда, когда все аргументы равны 1, а дизъюнкция равна 0 только тогда, когда все аргументы равны 0. В стандартном базисе они очевидным образом вычисляются схемами (и даже формулами), содержащими $n - 1$ элементарных двухвходовых операций (конъюнкций или дизъюнкций).

Теорема 3. *Базис* $\{NOT, OR, AND\}$ *— полный.*

Доказательство. *Литералом* будем называть переменную или ее отрицание. Конъюнкцией литералов (это схема и даже формула) легко представить функцию $\chi_u(x)$, которая принимает значение 1 ровно один раз: при $x = u$. Если $u_i = 1$, включаем в конъюнкцию переменную x_i, если $u_i = 0$, то включаем в конъюнкцию $\neg x_i$.

Произвольная функция f может быть представлена в виде

$$f(x) = \bigvee_{u:f(u)=1} \chi_u(x). \tag{1.1}$$

В таком случае говорят, что f представлена в *дизъюнктивной нормальной форме* (ДНФ), т. е. как дизъюнкция конъюнкций литералов.[9]

Как уже говорилось, дизъюнкция нескольких переменных выражается формулой в стандартном базисе. □

Определение 1.5.23. ***Размером*** *схемы называется количество присваиваний в схеме.*

Определение 1.5.24. ***Глубиной*** *схемы называется максимальное число элементов на пути от входов к выходу.*

Определение 1.5.25. *Минимальный размер схемы в базисе $\mathcal{F}$, вычисляющей функцию f, называется* ***схемной сложностью*** *функции f в базисе $\mathcal{F}$ и обозначается $c_{\mathcal{F}}(f)$.*

Переход от одного полного конечного базиса к другому полному конечному базису меняет схемную сложность функций на множитель $O(1)$. Так что в асимптотических оценках выбор конкретного полного базиса неважен и поэтому будем использовать обозначение $c(f)$ для схемной сложности f в конечном полном базисе.

Каждый предикат f на множестве $\{0,1\}^*$ задает последовательность булевых функций $f_n\colon \{0,1\}^n \to \{0,1\}$ следующим образом (справа стоит предикат f):

$$f_n(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n).$$

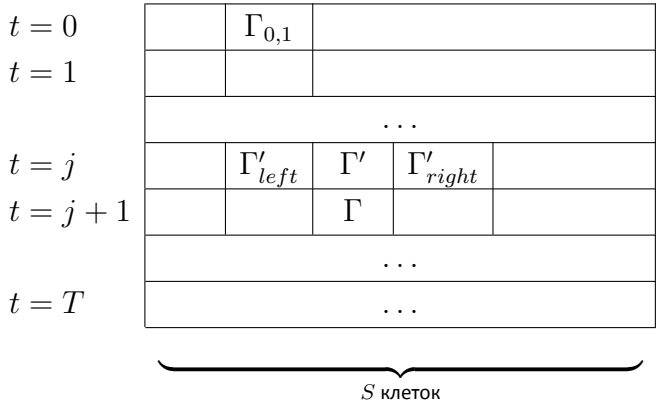
Определение 1.5.26. *Предикат f принадлежит классу* P/poly*, если*

$$c(f_n) = \mathrm{poly}(n).$$

Теорема 4. $P \subset \mathsf{P}/\mathrm{poly}$.

Доказательство. Если МТ работает за полиномиальное время, то и память, которую она использует, ограничена полиномом. Поэтому весь процесс вычисления на входном слове x длины n можно представить *таблицей вычисления* размера $T \times S$, где $T = \mathrm{poly}(n)$, $S = \mathrm{poly}(n)$.

[9] Далее нам еще потребуется и *конъюнктивная нормальная форма* (КНФ) — конъюнкция дизъюнкций литералов.



Строка с номером j таблицы задает состояние МТ после j тактов работы. Символы $\Gamma_{j,k}$, записанные в таблице, принадлежат алфавиту $\Sigma \times \{\emptyset \cup \mathcal{Q}\}$. Символ $\Gamma_{j,k}$ определяет пару (символ, записанный в k-й ячейке после j тактов работы; состояние управляющего устройства после j тактов работы, если головка находится над k-й ячейкой, в противном случае второй элемент пары — $\emptyset$). Для простоты также считаем, что если вычисление заканчивается при некотором входе за $T' < T$ тактов, то строки с номерами, большими T', повторяют строку с номером T'.

Построить схему, вычисляющую значения предиката на словах длины n, можно следующим образом. *Состояние каждой клетки таблицы* можно закодировать конечным (не зависящим от n) числом булевых переменных. Имеются *локальные правила согласования*, т. е. состояние каждой клетки Γ в строке ниже нулевой однозначно определяется состояниями клеток в предыдущей строке, лежащих непосредственно над данной (Γ'), левее данной (Γ'_{left}) и правее данной (Γ'_{right}). Каждая переменная, кодирующая состояние клетки Γ, есть функция от переменных, кодирующих состояния клеток Γ'_{left}, Γ', Γ'_{right}. Все эти функции могут быть вычислены схемами конечного размера. Объединяя эти схемы, получим схему, вычисляющую все переменные, кодирующие состояния клеток таблицы; размер этой схемы будет $O(ST) = O(n^{O(1)})$.

Осталось заметить, что переменные, кодирующие часть клеток нулевой строки, определяются входным словом, а переменные, кодирующие остальные клетки нулевой строки, являются константами. Чтобы узнать

результат вычисления, нужно определить символ, записанный в нулевой ячейке ленты в конце вычисления.

Без ограничения общности можно считать, что состояния клеток таблицы кодируются так, что одна из кодирующих переменных равна 1 только в том случае, когда в ячейке записана 1. Тогда значение этой переменной для кода $\Gamma_{T,0}$ и будет результатом вычисления. □

Класс P/poly шире класса P. Любой функции от натурального аргумента $\varphi(n)$ со значениями в $\{0,1\}$ можно сопоставить предикат f_φ по правилу $f_\varphi(x) = \varphi(|x|)$, где $|x|$ обозначает длину слова x. Ограничение такого предиката на слова длины n тождественно равно 0 или 1 (в зависимости от n). Схемная сложность таких функций ограничена константой. Поэтому все такие предикаты по определению принадлежат P/poly, хотя среди них есть и неразрешимые предикаты.

Справедливо следующее усиление теоремы.

Теорема 5. *f принадлежит P тогда и только тогда, когда*

1. $f \in$ P/poly*;*

2. *существует МТ, которая для входа n за время* poly(n) *строит схему вычисления f_n.*

Доказательство. $\Longrightarrow$ Данное в доказательстве теоремы 4 описание нетрудно превратить в МТ, которая строит схему вычисления f_n за полиномиальное по n время (схема f_n имеет простую структуру: каждая переменная связана с предыдущими одними и теми же правилами согласования).

$\Longleftarrow$ Столь же просто. Вычисляем размер входного слова. Затем строим по этому размеру схему $S_{|x|}$ вычисления $f_{|x|}$, используя указанную в условии 2) машину. После этого вычисляем $S_{|x|}(x)$ на машине, которая по описанию схемы и значениям входных переменных вычисляет значение схемы за полиномиальное от длины входа время. □

Упражнение 1.5.1. Пусть c_n есть максимум сложности $c(f)$ по всем булевым функциям f от n переменных. Докажите, что $1{,}99^n < c_n < 2{,}01^n$ при достаточно больших n.

Упражнение 1.5.2. Покажите, что любую функцию можно вычислить схемой глубины не более 3 из элементов NOT и из элементов AND и OR с произвольным числом входов.

Упражнение 1.5.3. Докажите, что если из схемы глубины $O(\log n)$, вычисляющей $f\colon \{0,1\}^n \to \{0,1\}^m$, выбросить все несущественные присваивания, то полученная схема имеет полиномиальный по $n+m$ размер.

Упражнение 1.5.4. Постройте схему, которая сравнивает два n-битовых числа и имеет размер $O(n)$, а глубину $O(\log n)$.

Упражнение 1.5.5.

1. Постройте схему сложения двух n-битовых чисел размера $O(n)$.
2. Тот же вопрос, если дополнительно потребовать, чтобы глубина схемы была $O(\log n)$.

Упражнение 1.5.6. Функция *MAJ* $\{0,1\}^n \to \{0,1\}$ равна 1 на двоичных словах, в которых число единиц больше числа нулей, и 0 — на остальных словах. Постройте схему, вычисляющую эту функцию, размер схемы должен быть линеен по n, глубина — $O(\log n \log\log n)$.

Упражнение 1.5.7. Постройте схему размера $\mathrm{poly}(n)$ и глубины $O(\log^2 n)$, которая проверяет, связаны ли путём две вершины в графе. Граф на m вершинах, которые помечены числами от 1 до m, задаётся $n = m(m-1)/2$ булевыми переменными. Переменная x_{ij}, где $i < j$, определяет, есть ли в графе ребро, соединяющее вершины i и j.

Упражнение 1.5.8. Пусть схема глубины 3 из элементов NOT и из элементов AND и OR с произвольным числом входов вычисляет сложение n битов по модулю 2 (функция $PARITY$). Покажите, что размер схемы не меньше c^n для некоторого $c > 1$.

Упражнение 1.5.9. Пусть $f_1, f_2, \ldots f_n, \ldots$ — последовательность булевых функций от $1, 2, \ldots n, \ldots$ аргументов. Покажите, что следующие два свойства равносильны:

1. существует последовательность вычисляющих эти функции формул, размер которых не превосходит полинома от n;

2. существует последовательность вычисляющих эти функции схем глубины $O(\log n)$ из элементов NOT, AND и OR (с двумя входами).

Упражнение 1.5.10. Докажите, что существует разрешимый предикат, который принадлежит P/poly, но не принадлежит P.

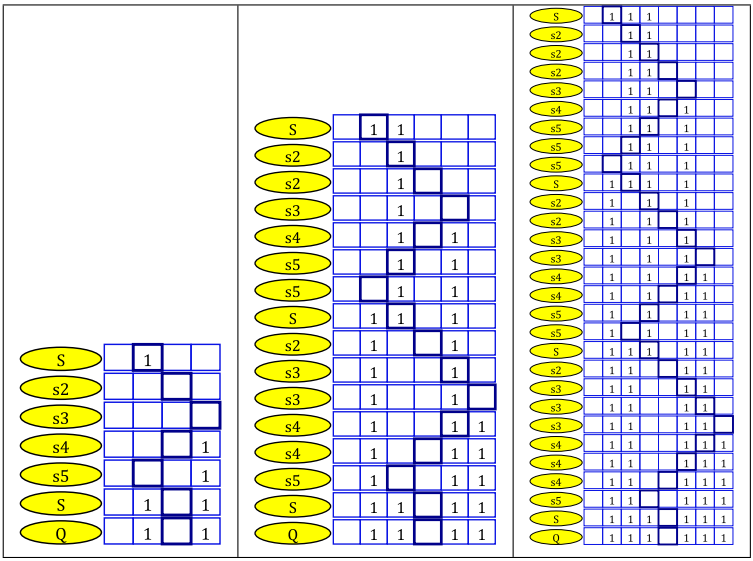


Рис. 1.3: Машина Тьюринга: удвоение строки

Глава 2

Необходимые сведения из теории колец, полей и решеток

2.1 Понятие кольца. Кольца с однозначным разложением на множители.

2.1.1 Кольца. Основные определения

Напомним некоторые определения.

Законом композиции называет отображение

$$M \times M \to M,$$

называемое умножением. Результат композиции называется произведением и обычно записывается как xy. Элемент $x \in M$ называется единицей, если для всех $y \in M$ выполняется равенство $xy = yx = y$ и обозначается символом e (в случае аддитивной операции $x + y$, для которой предполагается выполнение равенства $x+y = y+x$, такой элемент называется нулем и обозначается через 0). Операция называется ассоциативной, если для всех $x, y, z \in M$ выполняется равенство $x(yz) = (xy)z$. Операция называется коммутативной, если для всех $x, y \in M$ выполняется равенство $xy = yx$.

Моноидом называется множество M с ассоциативной операцией умножения, содержащее единицу. В частности, множество M не пусто.

Пусть имеется упорядоченный набор элементов $\{x_1, \ldots, x_n\}$, тогда определено их произведение $x_1 \cdot \ldots \cdot x_n$ (докажите это).

Упражнение 2.1.1. Пусть M — произвольное множество. Докажите, что определен моноид, состоящий из произведений $x_1 \cdot \ldots \cdot x_n$ элементов множества M. Как определяется единичный элемент в этом моноиде?

Определение 2.1.1. *Пусть M — моноид. Элемент $b \in M$ называется **правым обратным** для $a \in M$, если $ab = e$. Элемент $b \in M$ называется **левым обратным** для $a \in M$, если $ba = e$.*

Определение 2.1.2. *Моноид G называется **группой**, если для любого его элемента определен его правый обратный.*

Упражнение 2.1.2. Доказать, что правый обратный элемент единственный и является также левым обратным.

Определение 2.1.3. ***Кольцом** называется множество R с двумя законами композиции, называемыми, соответственно, сложением и умножением, такими что*

1. *множество R является коммутативной группой относительно сложения; нейтральный элемент обозначается через 0;*

2. *умножение ассоциативно[1];*

3. *умножение и сложение связаны законами **дистрибутивности**: $a(b+c) = ab + ac$ и $(b + c)a = ba + ca$.*

Определение 2.1.4. *Если в кольце (см. определение 2.1.4) имеется единичный элемент e относительно умножения, то такое кольцо называется **кольцом с единицей**.*

[1]Вообще бывают и неассоциативные кольца, например *кольца Ли*, но в этом курсе они рассматриваться не будут.

Упражнение 2.1.3. Приведите пример ассоциативного кольца без единицы. т. е. кольца в смысле определения 2.1.3 «Кольцо» но не удовлетворяющего определению 2.1.4 «Кольцо с единицей».

Определение 2.1.5. *Если в кольце (см. определение 2.1.4 «Кольцо с единицей») умножение коммутативно, то кольцо называется* ***коммутативным****.*

Приведем примеры различных колец.

$(\mathbb{Z}, +, \cdot)$ — кольцо *целых* чисел.

$(\mathbb{Q}, +, \cdot)$ — кольцо *рациональных* чисел.

$(\mathbb{R}, +, \cdot)$ — кольцо *вещественных* чисел.

$(\mathbb{C}, +, \cdot)$ — кольцо *комплексных* чисел.

$(\mathbb{Z}_n, +, \cdot)$ — кольцо *вычетов по модулю* n.

$\mathbb{A}[x]$ — кольцо многочленов над коммутативным кольцом $\mathbb{A}$.

$\mathbb{A}(x)$ — кольцо рациональных функций над кольцом $\mathbb{A}$.

Упражнение 2.1.4. Показать, что в общем случае $\mathbb{A}[x]$ не совпадает с кольцом функций, задаваемых многочленами над кольцом $\mathbb{A}$. (Указание: рассмотреть кольцо $A = \mathbb{Z}_p$, где p — простое.)

Рассмотрим еще пару нетривиальных примеров:

- Пусть S — множество, A — кольцо и $\mathcal{M}(S, A)$ — множество отображений из S в A. Тогда $\mathcal{M}(S, A)$ является кольцом, относительно операций, заданных формулами

$$(fg)(x) = f(x)g(x) \quad \text{и} \quad (f + g)(x) = f(x) + g(x)$$

при всех $x \in S$.

- Пусть M — аддитивная группа и $\mathrm{End}(M)$ — множество групповых гомоморфизмов M в себя. Это множество является кольцом относительно операций, заданных формулами

$$(fg)(x) = f(g(x)) \quad \text{и} \quad (f+g)(x) = f(x) + g(x)$$

при всех $x \in M$.

Упражнение 2.1.5. Докажите:

1. $0x = 0$.
2. при $1 = 0$ кольцо A состоит из одного 0.
3. $(-x)y = -(xy)$.
4. $(-x)(-y) = (xy)$.

Определение 2.1.6. *Подмножество $B \subset A$ называется подкольцом кольца A, если это множество является аддитивной группой относительно сложения, замкнуто относительно умножения, а для кольца с единицей содержит единицу.*

Очевидный пример подколец среди рассмотренных выше колец:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Упражнение 2.1.6. Рассмотрим кольцо вычетов $\mathbb{Z}_{10}$. Образуют ли элементы из $\mathbb{Z}_{10}$ кратные 5, подкольцо в $\mathbb{Z}_{10}$?

Упражнение 2.1.7. Описать все подкольца в кольце вычетов $\mathbb{Z}_n$ по модулю n.

Определение 2.1.7. *Если A — кольцо, то $U(A)$ — множество всех обратимых по умножению элементов в A, т. е. имеющих одновременно правый и левый обратный элемент (по умножению), называется* ***группой единиц***[2] *кольца A и обозначается через A^*.*

[2] Иногда называют *множеством обратимых элементов*.

Упражнение 2.1.8. Докажите, что группа единиц (см. определение 2.1.7 «Группа единиц»), является группой относительно операции умножения.

Примеры групп единиц:

1. $U(\mathbb{Z}) \equiv \mathbb{Z}^* = \{1, -1\}$.
2. $U(\mathbb{Q}) \equiv \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
3. $U(\mathbb{R}) \equiv \mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
4. $U(C[0,1]) = \{f \in C[0,1] \mid f(x) \neq 0 \, \forall x \in [0,1]\}$.

Определение 2.1.8. *Кольцо A, в котором $1 \neq 0$ и всякий ненулевой элемент обратим, называется **кольцом с делением** или **телом**.*

Определение 2.1.9. *Коммутативное кольцо с делением называется **полем** (см. определения 2.1.5 «Коммутативное кольцо» и 2.1.8 «Тело»).*

Примеры:

1. Полями являются кольца $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_2$.
2. $\mathbb{Z}$ не является полем.

Упражнение 2.1.9. Кольцо вычетов $\mathbb{Z}_n$ является полем (полем вычетов) тогда и только тогда, когда $n = p$, т. е. является простым числом.

2.1.2 Идеалы и гомоморфизмы колец

Определение 2.1.10. ***Левым идеалом*** *кольца A называется подмножество a в A являющееся аддитивной подгруппой группы A, и такое, что $Aa \subset a$.*

*Для **правого идеала** должно аналогично выполняться условие $aA \subset a$.*

*Подмножество, являющееся одновременно левым и правым идеалом называется **двусторонним идеалом** или просто **идеалом**.*

Приведем примеры идеалов:

1. Для любого кольца A идеалами будут $\{0\}$ и A.
2. Для любого $n \in \mathbb{Z}$, $\mathbb{Z}_n$ будет идеалом для $\mathbb{Z}$.
3. Для любого $a \in [0,1]$, $I_a = \{f \in C[0,1] \mid f(a) = 0\}$ будет идеалом для $C[0,1]$.

Определение 2.1.11. *Идеал порожденный одним элементом, называют **главным** (principal ideal):*

*Пусть A кольцо и $a \in A$, то $a = Aa$ — левый **главный** идеал, а элемент a называется **образующим** главного идеала a.*

*Аналогично AaA — **главный двусторонний идеал**.*

Очевидно, что в коммутативном кольце всякий левый или правый идеал является двусторонним.

Определение 2.1.12. *Коммутативное кольцо, в котором всякий идеал главный, называется **кольцом главных идеалов**.*

Упражнение 2.1.10. Доказать, что кольцо целых чисел является кольцом главных идеалов.

Определение 2.1.13. *Пусть a и b — идеалы в A.*

***Произведением идеалов** ab называется множество сумм*

$$x_1y_1 + \ \ldots + x_ny_n,$$

где $x_i \in a$ и $y_i \in b$.

Упражнение 2.1.11. Проверить, что ab является идеалом и что множество идеалов образует мультипликативный моноид, причем единичным элементом в нем является само кольцо. Этот последний идеал называется единичным и обозначается через (1). Если a и b — левые идеалы, то их произведение также является левым идеалом, и выполняется свойство ассоциативности умножения.

Упражнение 2.1.12. Если a и b — левые идеалы, то a + b (сумма аддитивных подгрупп — минимальная подгруппа, аддитивной группы кольца, содержащая группы a и b)— левый идеал. Аналогично для двусторонних

идеалов. Доказать, что идеалы образуют моноид относительно сложения идеалов. Доказать свойство дистрибутивности

$$\mathfrak{b}(\mathfrak{a}_1 + \ \ldots + \mathfrak{a}_n) = \mathfrak{b}\mathfrak{a}_1 + \ \ldots + \mathfrak{b}\mathfrak{a}_n.$$

Аналогично для умножения с другой стороны.

Однако заметим, что это множество не является кольцом.

Упражнение 2.1.13. Пусть $\{\mathfrak{a}_i\}_{i\in I}$ — семейство идеалов. Тогда их пересечение $\bigcap_{i\in I} \mathfrak{a}_i$ — также идеал.

Упражнение 2.1.14. Пусть $a_1, \ \ldots, a_n$ — элементы кольца A. Обозначим через $(a_1, \ \ldots, a_n)$ идеал, являющийся пересечением всех идеалов, содержащих эти элементы или левый идеал являющийся пересечением всех левых идеалов, содержащих эти элементы. Элементы $a_1, \ \ldots, a_n$ называются образующими этого идеала. Доказать, что этот идеал состоит из всех элементов кольца A, которые могут быть представлены в виде

$$x_1a_1 + \ \ldots x_na_n,$$

где $x_i \in A$.

Определение 2.1.14. *Отображение $f : A \to B$ колец называется **гомоморфизмом**, если выполняются соотношения*

$$\begin{array}{rclrcl} f(a+a') & = & f(a)+f(a'), & f(aa') & = & f(a)f(a'), \\ f(0) & = & 0, & f(1) & = & 1 \end{array}$$

для всех $a, a' \in A$.

*Его **ядром** называется ядро его аддитивного гомоморфизма, т. е. множество*

$$\ker f = \{a \in A \mid f(a) = 0\}.$$

Упражнение 2.1.15. Ядро гомоморфизма является идеалом (двусторонним).

Обратно, пусть задан идеал $\mathfrak{a} \subset A$. Тогда определено кольцо $A/\mathfrak{a}$, элементами которого являются смежные классы аддитивной группы кольца A. Умножение классов определяется формулой $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$.

Упражнение 2.1.16. Доказать, что определенное выше множество является кольцом. Определить гомоморфизм $f : A \to A/\mathfrak{a}$ и доказать, что $\ker f = \mathfrak{a}$.

Определение 2.1.15. *Пусть A кольцо и B его подкольцо. Пусть $S \subset A$. Обозначим через $B[S]$ пересечение всех подколец, содержащих B и S.*

Упражнение 2.1.17. Пусть элементы множеств B и S коммутируют. Докажите, что $B[S]$ состоит из элементов вида

$$\sum b_{i_1,\ldots,i_n} s_1^{i_1} \ldots s_n^{i_n},$$

где сумма пробегает некоторое множество наборов $(i_1, \ldots, i_n)$ целых чисел ≥ 0 $b_{i_1,\ldots,i_n} \in B, s_1 \ldots s_n \in S$.

Определение 2.1.16. *Если $A = B[S]$, то говорят что S является множеством* ***кольцевых образующих*** *для A над B. Если S конечно, то говорят, что A* ***конечно порождено как кольцо над*** *B.*

Упражнение 2.1.18. Пусть $f : B \to B'$ — гомоморфизм колец и $A = B[S]$. Докажите, что имеется не более одного продолжения этого гомоморфизма на кольцо A, имеющее предписанное задание на множестве S.

Пусть A — кольцо, $\mathfrak{a}$ — идеал и S подмножество в A. Если $S \subset \mathfrak{a}$, будем обозначать это как

$$S \equiv 0 \pmod{\mathfrak{a}}.$$

Пусть $x, y \in A$ и $x - y \in \mathfrak{a}$, будем обозначать это как

$$x \equiv y \pmod{\mathfrak{a}}.$$

Если $\mathfrak{a}$ — главный идеал, равный (a), то допустима запись

$$x \equiv y \pmod{a}.$$

Упражнение 2.1.19. Докажите, что любой биективный гомоморфизм колец является изоморфизмом колец, а образ кольца при гомоморфизме является подкольцом.

Упражнение 2.1.20. Пусть $f : A \to A'$ — гомоморфизм колец и $\mathfrak{a}'$ — идеал в A'. Докажите, что $f^{-1}(\mathfrak{a}') = \mathfrak{a}$ — идеал в A и определен инъективный гомоморфизм

$$A/\mathfrak{a} \to A/\mathfrak{a}'.$$

Определение 2.1.17. *Пусть A — кольцо. Элементы $x, y \in A$ называются **делителями нуля**, если $x \neq 0$, $y \neq 0$, а $xy = 0$.*

Примеры:

- В $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ нет делителей нуля.
- В кольце пар $\mathbb{Z} \times \mathbb{Z}$, с покомпонентным умножением, все элементы вида $(z_1, 0)$ или $(0, z_2)$, где $z_1, z_2 \in \mathbb{Z}$, будут делителями нуля $(0, 0)$.
- В кольце матриц 2×2 над полем $\mathbb{Q}$, будет, например, делитель нуля $\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$, т.к.

$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- В кольце $C[0, 1]$ непрерывных $[0, 1]$ функций с умножением-композицией, делителями нуля будут все нетождественно равные нулю функции, имеющие точки, где они равны нулю.

Определение 2.1.18. *Кольцо A называется **целостным**, если:*

- *оно коммутативно;*
- *в нем нет делителей нуля;*
- $1 \neq 0$.

Упражнение 2.1.21. Кольцо целых чисел $\mathbb{Z}$ целостное. Пусть $m > 1$ целое. Докажите, что кольцо $\mathbb{Z}/m\mathbb{Z}$ содержит делители нуля тогда и только тогда, когда m не простое.

Определение 2.1.19. *Факторкольцо $\mathbb{Z}/n\mathbb{Z}$ называется **кольцом целых чисел по модулю** n.*

2.1.3 Коммутативные кольца

В данном разделе далее термин кольцо будет означать коммутативное кольцо.

Определение 2.1.20. *Идеал $\mathfrak{p} \neq A$ кольца A называется **простым**, если из $xy \in \mathfrak{p}$ следует, что либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$.*

Упражнение 2.1.22. Докажите, что идеал $\mathfrak{p}$ простой тогда и только тогда, когда кольцо $A/\mathfrak{p}$ целостное (не имеет делителей нуля).

Упражнение 2.1.23. Пусть $p \in \mathbb{Z}$ — простое число и $\mathfrak{p} = (p)$ — главный идеал в $\mathbb{Z}$, порожденный числом p. Тогда идеал $\mathfrak{p}$ простой. Докажите это, используя основную теорему арифметики о единственности разложения на простые сомножители в кольце целых чисел.

Определение 2.1.21. *Идеал $\mathfrak{m}$ называется **максимальным**, если $\mathfrak{m} \neq A$ и не существует другого идеала $\mathfrak{a} \neq A$, содержащего $\mathfrak{m}$.*

Упражнение 2.1.24. Всякий максимальный идеал — простой.

Упражнение 2.1.25. Докажите, что идеал $\mathfrak{m}$ кольца A максимальный тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Пример. Пусть $\mathbb{Z}$ — кольцо целых чисел. Тогда всякий его идеал $\mathfrak{o}$ главный, т. е. $\mathfrak{o} = n\mathbb{Z}$. Этот идеал простой тогда и только тогда, когда $n = p$ простое. Кольцо $\mathbb{Z}/n\mathbb{Z}$ называется *кольцом целых чисел по модулю* n. Если $n = p$ простое, то это кольцо является полем и обозначается символом $\mathbb{F}_p$. В частности, мультипликативная группа поля $\mathbb{F}_p$ совпадает с группой отличных от нуля целых чисел по модулю p. Порядок группы единиц кольца $\mathbb{Z}/n\mathbb{Z}$ обозначается через $\varphi(n)$ и определяемая функция известна как φ -функция Эйлера. В частности, для простых p выполняется равенство $\varphi(p) = p - 1$.

Упражнение 2.1.26. Докажите равенство $x^{\varphi(n)} \equiv 1 \pmod{n}$ для всех целых x, взаимно простых с n.

Теорема 6. *«Китайская теорема об остатках»*

Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при всех $i \neq j$. Для любого семейства элементов $x_1, \ldots, x_n$ кольца A существует такой элемент $x \in A$, что $x \equiv x_i \pmod{\mathfrak{a}_i}$ при всех i.

Следствие. Пусть A — кольцо и $\mathsf{a}_1, \ldots, \mathsf{a}_n$ — такие идеалы, что $\mathsf{a}_i + \mathsf{a}_j = A$ при всех $i \neq j$. Пусть

$$f : A \to \prod_{i=1}^{n} A/\mathsf{a}_i$$

— гомоморфизм кольца A, индуцированное проекциями A на A/a_i для каждого сомножителя. Тогда ядро гомоморфизма f есть $\bigcap\limits_{i=1}^{n} \mathsf{a}_i$ и f сюръективно, что приводит к изоморфизму

$$A/\bigcap \mathsf{a}_i \xrightarrow{\approx} \prod A/\mathsf{a}_i.$$

Упражнение 2.1.27. Докажите китайскую теорему об остатках и ее следствие.

Упражнение 2.1.28. Пусть $m = \prod\limits_i p_i^{r_i}$ — разложение на простые сомножители числа m. Докажите, что тогда имеет место изоморфизм колец

$$\mathbb{Z}/m\mathbb{Z} \approx \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

В частности, для мультипликативной группы кольца имеется изоморфизм

$$(\mathbb{Z}/m\mathbb{Z})^* \approx \prod_i \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^*.$$

Поэтому для функции Эйлера справедливо равенство

$$\varphi(m) = \prod_i \varphi\left(p_i^{r_i}\right).$$

Упражнение 2.1.29. Пусть p — простое число и r — целое число ≥ 1. Докажите индукцией по r, что

$$\varphi\left(p^r\right) = (p-1)p^{r-1}.$$

Пусть A кольцо и e его единичный элемент. Тогда определен гомоморфизм колец

$$\lambda : \mathbb{Z} \to A,$$

для которого $\lambda(n) = ne$ и его ядро является главным идеалом, порожденным некоторым целым неотрицательным числом n.

Тогда определен инъективный гомоморфизм колец $\mathbb{Z}/n\mathbb{Z} \to A$. Поэтому, если кольцо A целостное, то кольцо $\mathbb{Z}/n\mathbb{Z}$ — целостное и число n простое или $n = 0$. Если $n = 0$, то кольцо A содержит подкольцо $\mathbb{Z}$, обычно отождествляемое с $\mathbb{Z}$. В этом случае говорят, что A имеет *характеристику* 0. Если же $n = p$ — простое, то кольцо A содержит в качестве подкольца поле $\mathbb{F}_p$ и в этом случае говорят, что что A имеет *характеристику* p.

Характеристика поля Q обозначается как char Q.

В частности, каждое поле K имеет характеристику 0 или $p > 0$. В первом случае поле K содержит в качестве подполя поле рациональных чисел, а во втором случае изоморфный образ поля $\mathbb{F}_p$.

В обоих случаях это поле будет называться *простым полем* содержащимся в K и его обычно отождествляют с $\mathbb{Q}$ или F_p.

Примеры:

- char $\mathbb{Q} = 0$, char $\mathbb{R} = 0$;
- char $\mathbb{Z}_p = p$ (для простого числа p).

Под простым кольцом в целостном кольце A будем понимать либо кольцо целых чисел $\mathbb{Z}$, если A имеет характеристику 0, либо F_p, если A имеет характеристику p.

2.1.4 Факториальные кольца

Определение 9. Элемент $a \neq 0$ кольца A называется *неприводимым*, если он не является единицей и если из равенства $a = bc$, где $b, c \in A$, следует, что b или c — единица кольца A. Неприводимые элементы, отличающиеся умножением на единицу будем называть эквивалентными.

Задача 20. Пусть $a \neq 0$ — некоторый элемент в A, и пусть главный идеал (a) простой. Тогда элемент a неприводимый.

Определение 10. Нормой в кольце A называется мультипликативная функция $N : A \to \mathbb{R}_+$, равная нулю только на нулевом элементе кольца.

Пример. Приведем контрпример к обратному утверждению предыдущей задачи. Полагаем

$$A = \mathbb{Z}[X]/(X^2+5) \approx \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}.$$

Докажем, что элемент $3 \in A$ неприводим. Для этого введем норму в кольце A формулой $N\left(x+y\sqrt{-5}\right) = x^2+5y^2$. Тогда $N(3) = 9$. Если элемент $3 \in A$ не является неприводимым, то существуют a и b, такие что $N(a) \neq 1$, $N(b) \neq 1$ и $ab = 3$. Тогда $9 = N(3) = N(ab) = N(a)N(b)$. Следовательно, $N(a) = 3$. Но это невозможно ввиду определения нормы. Имеем далее

$$A/(3) = \mathbb{Z}[X]/(X^2+5,\ 3) = \mathbb{F}_3[X]/(X^2+5) = \mathbb{F}_3[X]/(X^2-1).$$

Тогда в кольце $A/(3)$ выполняется равенство $(X-1)(X+1) = 0$, причем $X-1 \neq 0$ и $X+1 \neq 0$ в кольце $A/(3)$. Поэтому кольцо $A/(3)$ не целостное, т. е. идеал (3) не является простым.

Определение 11. Кольцо называется *факториальным* (или кольцом с однозначным разложением на множители), если оно целостное и всякий ненулевой элемент кольца имеет единственное разложение на неприводимые элементы. Единственность понимается с точностью до перестановок сомножителей и замен неприводимых множителей эквивалентными.

Определение 12. Пусть A — целостное кольцо и $a, b \in A$, $ab \neq 0$. Будем говорить, что a *делит* b, и записывать это формулой $a|b$, если существует элемент $c \in A$, для которого $ac = b$. Элемент $d \in A$, $d \neq 0$, называется *наибольшим общим делителем* (сокращенно НОД) элементов a и b, если $d|a$, $d|b$ и если любой элемент $e \in A$, $e \neq 0$, делящий и a и b, делит также d.

Предложение 1. Пусть A — целостное кольцо главных идеалов и $a, b \in A,\ a, b \neq 0$. Если $(a, b) = (c)$, то c — наибольший общий делитель элементов a и b.

Задача 21. Доказать предложение 1.

Теорема 1. Всякое целостное кольцо A главных идеалов факториально.

Доказательство. Докажем вначале, что всякий ненулевой элемент имеет разложение на неприводимые множители. Обозначим через S множество ненулевых главных идеалов, образующие которых не имеют разло-

жения на неприводимые множители. Пусть $S \neq \emptyset$. Пусть $(a_1) \in S$. Рассмотрим произвольную возрастающую цепочку

$$(a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} (a_n) \underset{\neq}{\subset} \ldots$$

идеалов из S. Докажем, что эта цепочка конечна. Действительно, объединение идеалов этой цепочки является идеалом в A, а согласно условию теоремы этот идеал главный, скажем равен (a). Тогда a лежит в некотором идеале (a_n) и

$$(a_n) \subset (a) \subset (a_n).$$

Следовательно, $(a) = (a_n)$, и цепочка обрывается на члене (a_n). Поэтому, любой идеал в A, содержащий идеал (a_n), имеет образующую, допускающую разложение на неприводимые множители.

Заметим теперь, что элемент a_n приводимый, иначе он имел бы разложение на неприводимые множители. Следовательно, $a_n = bc$, где ни b, ни c не являются единицами. Тогда $(a_n) \underset{\neq}{\subset} (b)$ и $(a_n) \underset{\neq}{\subset} (c)$, и, следовательно, b и c имеют разложения на неприводимые сомножители. Тогда произведение этих разложений дает разложение a_n на неприводимые множители, вопреки тому, что S не пусто.

Докажем единственность. Вначале докажем, что если p — неприводимый элемент в A, $a, b \in A$, $p|ab$, то $p|a$ или $p|b$. Действительно, если $p \nmid a$, то НОД элементов p и a равен 1 и, следовательно, по предыдущему предложению

$$1 = xp + ya$$

для некоторых $x, y \in A$. Тогда $b = bxp + yab$, а поскольку $p|ab$, то из этого равенства получаем, что $p|b$.

Предположим, что некоторый элемент a имеет два разложения

$$a = p_1 \ldots p_r = q_1 \ldots q_s.$$

Тогда p_1 делит произведение, стоящее справа. Следовательно, по доказанному выше p_1 делит один из его сомножителей, причем после их перестановки можно считать, что это q_1. Тогда $q_1 = p_1 u_1$, где u_1 единица. Сокращая на p_1 получаем

$$p_2 \ldots p_r = u_1 q_2 \ldots q_s.$$

Повторяя процедуру $r-1$ раз завершаем доказательство единственности разложения.

Если A факториальное кольцо, то всякий неприводимый элемент p порождает простой идеал (p). Поэтому в факториальном кольце неприводимые элементы будем называть *простыми*.

Используя разложение на простые сомножители, легко находить значения наибольших общих делителей пар элементов кольца. Элементы $a, b \in A$ называются *взаимно простыми* если $(a,b) = (1)$.

2.1.5 Кольца многочленов

Определение 13. Пусть A — кольцо. Кольцом многочленов $A[X]$ над кольцом A называется множество конечных сумм вида

$$p(X) = \sum_{i=0}^{\infty} a_i X^i,$$

где только конечное число элементов $a_n \in A$ не равно нулю. Сложение и умножение определяются формулами

$$\begin{aligned} \left(\sum_{i=0}^{\infty} a_i X^i\right) + \left(\sum_{i=0}^{\infty} b_i X^i\right) &= \sum_{i=0}^{\infty} (a_i + b_i) X^i \\ \left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_i X^i\right) &= \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) X^i \end{aligned}$$

Степенью ненулевого многочлена $p(X) = \sum\limits_{i=0}^{\infty} a_i X^i$ называется число n, такое, что $a_n \neq 0$ и $a_m = 0$ при $m > n$ и обозначается $\deg p(X)$. Полагаем $\deg 0 = -\infty$. Тривиально проверяется, что

$$\begin{aligned} &\deg(fg) = \deg f + \deg g \\ &\deg(f+g) \leq (\deg f, \deg g). \end{aligned}$$

Выполняя деление «столбиком» получаем

Предложение 2. В кольце многочленов над полем определено деление с остатком. А именно, для любых многочленов $f, g \in K[X]$ существуют многочлены $q, r \in K[X]$, такие что $\deg r < \min\{\deg f, \deg g\}$ и

$$f(X) = q(X)g(X) + r(X).$$

В кольце многочленов над произвольным кольцом определено деление с остатком на многочлен со старшим коэффициентом равным единице.

Следствие. Если $f(a) = 0$ для некоторого $a \in A$, то существует такой многочлен $g(X)$, для которого выполняется равенство $f(X) = (X - a)g(X)$.

Доказательство. В силу предыдущего предложения имеем $f(X) = (X - a)g(X) + r(x)$. Поскольку степень многочлена $X - a$ равна единице, то степень остатка r не меньше единицы. Следовательно, остаток является элементом кольца A. Тогда выполняется равенство $f(a) = (a - a)g(a) + b$ и, следовательно, $b = 0$, т. е. $f(X) = (X - a)g(X)$.

При этом степень многочлена $g(X)$ на единицу меньше степени многочлена $f(X)$.

Теорема 2. Кольцо многочленов над полем является кольцом главных идеалов.

Доказательство. Рассмотрим произвольный идеал а $\neq 0$ в кольце $K[X]$ над полем K. Пусть $g(X)$ — ненулевой многочлен минимальной степени в этом идеале. Пусть $f(X) \in$ а. Разделим многочлен f на многочлен g с остатком. Получим $f(X) = q(X)g(X) + r(X)$, причем степень многочлена $r(X)$ меньше степени многочлена $g(X)$. Поскольку а — идеал, элемент $r \in$ а, а поскольку его степень меньше степени многочлена $g(X)$, то этот многочлен равен нулю. Следовательно, $f(X) \in (g(X))$, т. е. $(g(X)) =$ а. Следовательно, все идеалы кольца $K[X]$ главные.

Следствие. Кольцо многочленов над полем факториально.

2.1.6 Однозначность разложения на простые множители в кольце многочленов

Для доказательства однозначности разложения на простые множители в кольце многочленов нам потребуются некоторые новые понятия.

Конструкция Гротендика. Пусть A — кольцо без делителей нуля. Рассмотрим отношение $\sim$ на множестве пар $(a, b) \in A \times A^*$, заданное правилом

$$(a, b) \sim (c, d) \;\Leftrightarrow\; ad = bc.$$

Легко проверить, что $\sim$ является отношением эквивалентности на множестве таких пар. Определим операции сложения и умножения на таких парах

$$(a, b) + (c, d) = (ad + bc, bd), \quad (a, b)(c, d) = (ab, cd).$$

Из определения следует, что при замене пар эквивалентными, результаты операций остаются эквивалентными. Следовательно, определены операции на множестве классов эквивалентности $A \times A^*/\sim$ и это множество является полем. Полученное поле называется полем частных кольца A. Пара $(a, b) \in A \times A^*$ называется дробью, $a \in A$ — числителем, а элемент $b \in A^*$ — знаменателем этой дроби может быть записана также в виде $\dfrac{a}{b}$. Имеется инъективный гомоморфизм колец $i : A \to K$, заданный формулой $i(a) = (a, 1)$.

Задача 22. Доказать, что в факториальном кольце каждый элемент его кольца частных K может быть представлен в виде (a, b), где НОД$(a, b) = 1$ и такое представление единственно с точностью до умножения числителя и знаменателя на единицу кольца A. Такое представление называется несократимым.

Определение 14. Пусть A факториальное кольцо и K — его поле частных. Пусть $a \in K$, $a \neq 0$ и p — простой элемент кольца A. Тогда существует такое целое число r, что

$$a = p^r b,$$

где $b \in K$ и p не делит ни числитель, ни знаменатель несократимого представления для b. Это число r называется *порядком* элемента a в p и обозначается через $r = \mathrm{ord}_h a$. Порядок элемента $a = 0$ в p полагаем равным $+\infty$.

Если $a, a' \in K$ и $aa' \neq 0$, то

$$\mathrm{ord}_p(aa') = \mathrm{ord}_p(a) + \mathrm{ord}_p(a').$$

Определение 15. Пусть $f(X) \in K[X]$ — многочлен одной переменной

$$f(X) = a_0 + a_1 X + \ \ldots + a_n X^n.$$

Для $f = 0$ полагаем $\mathrm{ord}_p f = +\infty$. Если $f \neq 0$, то считаем по определению

$$\mathrm{ord}_p f = \min \mathrm{ord}_p a_i,$$

где минимум берется по тем i, для которых $a_i \neq 0$.

Элемент $up^{\mathrm{ord}_p f}$, где u — единица в A, называется p*-содержанием* многочлена f. *Содержанием* f будем называть выражение

$$\prod p^{\mathrm{ord}_p f},$$

заданное с точностью до умножения на единицу и будем обозначать через $\mathrm{cont}(f)$.

Если $b \in K$, $b \neq 0$, то $\mathrm{cont}(bf) = b\,\mathrm{cont}(f)$. Следовательно,

$$f(X) = cf_1(X),$$

где $c = \mathrm{cont}(f)$ и $f_1(X)$ имеет содержание 1. В частности, все коэффициенты многочлена f_1 лежат в A и их НОД равен 1.

Лемма Гаусса. Пусть A — факториальное кольцо, K — его поле частных, $f, g \in K[X]$ — многочлены от одной переменной. Тогда

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g).$$

Доказательство. Достаточно доказать, что если $f, g \in K[X]$ имеют содержание 1, то и их произведение имеет содержание 1. Для этого достаточно проверить, что для каждого простого p выполняется равенство $\mathrm{ord}_p(fg) = 1$. Пусть

$$\begin{aligned} f(X) &= a_n X^n + \ \ldots + a_0, \quad a_n \neq 0 \\ g(X) &= b_n X^n + \ \ldots + b_0 \quad\ \ b_n \neq 0. \end{aligned}$$

Пусть r — наибольшее целое число, такое, что $0 \leq r \leq n$ и $p \nmid a_r$. . Пусть s — наибольшее целое число, такое, что $0 \leq s \leq n$ и $p \nmid a_s$. Такие r, s определены, поскольку $\mathrm{ord}_p(f) = \mathrm{ord}_p(g) = 1$. Коэффициент при X^{r+s} в произведении $f(X)g(X)$ равен

$$c = a_0 b_{r+s} + \ \ldots a_r b_s + \ \ldots + a_{r+s} b_0.$$

Все слагаемые, кроме $a_r b_s$, делятся на p, а $p \nmid a_r b_s$. Поэтому $p \nmid c$. Следовательно, $\mathrm{ord}_p(fg) = 1$.

Следствие. Пусть $f(X) \in A[X]$ имеет в $K[X]$ разложение $f(X) = g(X)h(X)$. Если $c_g = \mathrm{cont}(g)$, $c_h = \mathrm{cont}(h)$ и $g = c_g g_1$, $h = c_h h_1$, то

$$f(X) = c_g c_h g_1(X) h_1(X)$$

и $c_g c_h$ — элемент из A.

В доказательстве нуждается только последнее утверждение. Оно следует из соотношения

$$\mathrm{cont}(f) = c_g c_h \mathrm{cont}(g_1 h_1) = c_g c_h.$$

Теорема 3. Пусть A факториальное кольцо. Тогда кольцо многочленов $A[X]$ факториально. Его простыми элементами являются либо простые элементы из кольца A, либо многочлены из $A[X]$, неприводимые в $K[X]$ и имеющие содержание 1.

Доказательство. Пусть A — факториальное кольцо и K его поле частных. Пусть $f \in A[X] \subset K[X]$. Тогда существует разложение этого многочлена на простые сомножители в кольце $K[X]$

$$f(X) = c \cdot p_1(X) \ldots p_r(X),$$

где $c \in A$ и $p_1(X) \ldots p_r$ — многочлены из $A[X]$, неприводимые в $K[X]$. Выделив их содержания, можно без ограничений общности, считать, что содержание p_i равно 1 для каждого i. Тогда $c = \mathrm{cont}(f)$. Поэтому существование разложения на множители доказано. Единственность разложения следует из единственности разложения в кольце $K[X]$ и предыдущего следствия.

Следствие 1. Многочлен степени n имеет не более n различных корней.

Следствие 2. Пусть A — факториальное кольцо. Тогда кольцо многочленов от n переменных $A[X_1, \ldots, X_n]$ факториально. Его единицами являются в точности единицы из A, а простыми элементами — либо простые элементы из A, либо многочлены, которые неприводимы в $K[X]$ и имеют содержание 1.

Теорема 4. Пусть k — поле. Всякая конечная мультипликативная подгруппа U в k циклическая.

Доказательство. Представим группу U как произведение подгрупп $U(p)$ по всем простым p, где $U(p)$ — группы порядка степени p. Достаточно доказать, что $U(p)$ циклическая для каждого p. Пусть a — элемент из $U(p)$ максимального периода p^k. Тогда $x^{p^k} = 1$ для всех $x \in U(p)$. Поэтому все элементы из $U(p)$ являются корнями многочлена

$$X^{p^k} - 1.$$

Циклическая группа, порожденная a, содержит p^k элементов. Если эта группа не совпадает с $U(p)$, то многочлен имеет более чем p^k различный корней, что противоречит полученному выше следствию.

2.1.7 Кратные корни

Определение. Дифференцированием в кольце многочленов $A[X]$ называется отображение

$$D : A[X] \to A[X],$$

определяемое формулой

$$D(a_n X^n + \ \ldots + a_0) = n a_n X^{n-1} + \ \ldots + a_1.$$

Используется также обозначение $D(f(X)) = f'(X)$.

Теорема 5. Выполняются соотношения

1. $(f + g) = f' + g'$,
2. $(fg)' = f'g + fg'$,
3. Если $a \in A$, то $(af)' = af'$,
4. $((x - a)^m)' = m(x - a)^{m-1}$ при $m \geq 1$.

Определение 16. Пусть K — поле, $f \in K[X]$ и a — его корень в K. Тогда

$$f(X) = (X - a)^m g(X),$$

где $g(X)$ — многочлен, взаимно простой с $X-a$. Число m называется кратностью корня a в f. Если $m>1$, то a называется *кратным корнем*.

Теорема 6. Пусть $f \in K[X]$, где K — поле. Элемент $a \in K$ является кратным корнем многочлена f тогда и только тогда, когда $f'(a)=0$.

Доказательство. Пусть $a \in K$ является кратным корнем многочлена f. Тогда $f(X)=(X-a)^m g(X)$ при некотором $m>1$. Тогда

$$f'(X)=m(X-a)^{m-1}g(X)+(X-a)^m g'(X)$$

и

$$f'(a)=m(a-a)^{m-1}g(a)+(a-a)^m g'(a)=0.$$

Пусть теперь $f'(a)=0$. Тогда $f(X)=(X-a)^m g(X)$, где $g(a)\neq 0$ и $m>0$. Тогда

$$0=f'(a)=m(a-a)^{m-1}g(a)+(a-a)^m g'(X)=m(a-a)^{m-1}g(a).$$

Следовательно,

$$0=m(a-a)^{m-1}g(a),$$

что возможно только при $m>1$.

2.2 Поля

2.2.1 Расширения полей

Пусть F — поле. Если F — подполе поля E, то поле E будем называть *расширением* поля F. Можно рассматривать E как векторное пространство над F. В зависимости от размерности этого векторного пространства будем назвать расширение E над F *конечным* или *бесконечным*.

Элемент $\alpha \in E$ поля расширения называется *алгебраическим* над F, если существуют $a_0, \ldots, a_n \in F$ $n \geq 1$, не все равные 0 и такие, что

$$a_0+a_1\alpha+\ldots+a_n\alpha^n=0.$$

Для алгебраического элемента $\alpha \neq 0$ всегда можно считать, что $a_0 \neq 0$ (иначе сократим на подходящую степень α. Это условие эквивалентно тому, что гомоморфизм полей

$$F[X] \to E,$$

тождественный на F и преобразующий X в α, имеет ненулевое ядро. Поскольку кольцо многочленов над полем является кольцом главных идеалов, это ядро будет порождено некоторым многочленом $p(X) \in F[X]$ со старшим коэффициентом, равным единице. Тогда имеет место изоморфизм

$$F[X]/(p(X)) \approx F[\alpha],$$

а поскольку кольцо $F[\alpha]$ — целостное (как подкольцо поля), то многочлен $p(X)$ неприводим. Будем обозначать такой многочлен через $\mathrm{Irr}(\alpha, F, X)$.

Расширение E поля F называется *алгебраическим*, если всякий элемент из E алгебраичен над F.

Предложение 1. Всякое конечное расширение E поля F алгебраично над F.

Доказательство. Пусть $\alpha \in E$, $\alpha \neq 0$. Степени

$$1, \alpha, \ \ldots, \alpha^n$$

не могут быть линейно независимыми над F для всех целых n, поскольку размерность E над F конечна. Линейное соотношение между степенями показывает алгебраичность элемента α над F.

Обратное утверждение неверно. Пример бесконечномерного алгебраического расширения — множество всех алгебраических чисел над полем рациональных чисел $\mathbb{Q}$.

Если E — расширение поля F, то размерностью этого расширения называется

$$[E : F] = \dim_F(E).$$

Предложение 2. Пусть $F \subset E$ — расширения поля k. Тогда

$$[E : k] = [E : F][F : k].$$

Если $\{x_i\}_{i \in I}$ — базис поля F над k и $\{y_j\}_{j \in J}$ — базис поля E над F, то $\{x_i y_j\}_{(i,j) \in I \times J}$ — базис поля E над k.

Следствие. Расширение $E \supset F \supset k$ конечно над k тогда и только тогда, когда E конечно над F и F конечно над k.

Задача 1. Докажите предложение 2 и выведите следствие. Указание: докажите линейную независимость предложенного варианта базиса.

Башней полей называется последовательность расширений

$$F_1 \subset F_2 \subset \ \ldots \subset F_n.$$

Башня *конечна*, тогда и только тогда, когда каждый ее этаж конечен.

Пусть k — поле, E — его расширение и $\alpha \in E$. Обозначим через $k(\alpha)$ наименьшее подполе в E, содержащее k и α. Оно изоморфно полю частных кольца $k[\alpha]$ и состоит из всех дробей вида $f(\alpha)/g(\alpha)$, где $g(\alpha) \neq 0$.

Предложение 3. Пусть элемент α алгебраичен над k. Тогда $k(\alpha) = k[\alpha]$ и поле $k(\alpha)$ конечно над k. Выполняется равенство $[k(\alpha) : k] = \deg \mathrm{Irr}(\alpha, F, X)$.

Задача 2. Доказать предложение 3. Указание: воспользуйтесь утверждением о возможности представления наибольшего общего делителя двух элементов евклидова кольца как их линейной комбинации.

Определение 1. Пусть E, F — расширения поля k. Если E и F содержатся в некотором поле L. Наименьшее подполе в L, содержащее E и F, называется *композитом* полей E и F в L и обозначается через EF. Отметим, что композит полей определен лишь в случае задания вложений полей в общее поле.

Пусть k — подполе в E и $\alpha_1, \ \ldots, \alpha_n$ — элементы из E. Обозначим через $k(\alpha_1, \ \ldots, \alpha_n)$ — наименьшее подполе в E, содержащее k и $\alpha_1, \ \ldots, \alpha_n$. Его элементами являются дроби

$$\frac{f(\alpha_1, \ \ldots, \alpha_n)}{g(\alpha_1, \ \ldots, \alpha_n)},$$

где f, g — многочлены с коэффициентами из k. Заметим, что E можно представить как объединение всех подполей $k(\alpha_1, \ \ldots, \alpha_n)$ по всем конечным подсемействам элементов из E. Поле E называется *конечно порожденным* над k, если существует конечное семейство $\alpha_1, \ \ldots, \alpha_n$ элементов из E, такое, что

$$E = k(\alpha_1, \ \ldots, \alpha_n).$$

Непосредственно из определений следует

Предложение 4. Всякое конечное расширение E поля k конечно порождено.

Предложение 5. Пусть $E = k(\alpha_1, \ \ldots, \alpha_n)$ — конечно порожденное расширение поля k, причем все α_i алгебраичны над k. Тогда E — конечное алгебраическое расширение поля k.

Указание: Для доказательства рассмотрите башню полей

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ \ldots \subset k(\alpha_1, \ \ldots, \alpha_n).$$

Предложение 6. Для алгебраических расширений выполняются свойства:

1. Пусть $k \subset F \subset E$ — башня полей. Расширение $k \subset E$ алгебраическое тогда и только тогда, когда расширения $k \subset F$ и $F \subset E$ алгебраические.

2. Если $k \subset F$ алгебраическое расширение и $k \subset E$ произвольное расширение, причем E и F лежат в общем поле, то $F \subset FE$ — алгебраическое расширение.

3. Если $k \subset F$ и $k \subset E$ — алгебраические расширения, причем E и F лежат в общем поле, то $k \subset FE$ — алгебраическое расширение.

Доказательство. Пусть $k \subset F \subset E$ — башня полей. Пусть E алгебраично над k. Тогда непосредственно из определения следует алгебраичность расширений $k \subset F$ и $F \subset E$. Обратно, пусть расширения $k \subset F$ и $F \subset E$ алгебраичны. Пусть $\alpha \in E$. Тогда при некоторых $a_0, \ \ldots, a_n \in F$ и $a_n \neq 0$ выполняется соотношение

$$a_n\alpha^n + \ \ldots + a_0 = 0.$$

Пусть $F_0 = k(a_n, \ \ldots, a_0)$. Тогда в силу предложения 5 расширение F_0 конечно над k и α алгебраичен над F_0. Рассматривая башню

$$k \subset F_0 = k(a_n, \ \ldots, a_0) \subset F_0(\alpha),$$

каждый этаж которой конечен, заключаем, что расширение $F_0(\alpha)$ конечно над k и, следовательно, элемент α алгебраичен над k.

Утверждение 2 предложения 6 вытекает из того, что композит FE можно представить как объединение полей $F(\alpha_1, \ \ldots, \alpha_n)$, по всем конечным семействам $\alpha_1, \ \ldots, \alpha_n$ элементов поля E, являющихся алгебраическими элементами над полем k и, следовательно, алгебраическими элементами над полем F.

Последнее утверждение является следствием двух первых. Для этого достаточно рассмотреть башню

$$k \subset F \subset EF.$$

2.2.2 Алгебраическое замыкание

Задача 3. Гомоморфизм полей всегда является вложением.

Пусть E и F — расширения поля k. Вложение полей $\sigma : F \to E$ называется гомоморфизмом над полем k, если ограничение $\sigma : k \to E$ является тождественным отображением $\sigma : k \to k \subset E$. Гомоморфизм поля в себя называется автоморфизмом, если этот гомоморфизм является изоморфизмом.

Лемма 1. Пусть E — алгебраическое расширение поля k, и $\sigma : E \to E$ вложение поля в себя над полем k. Тогда σ — автоморфизм.

Доказательство. Достаточно доказать его сюръективность. Пусть $\alpha \in E$ и $p(X)$ — его неприводимый многочлен над k. Обозначим через E' подполе в E, порожденное всеми корнями многочлена $p(X)$, лежащими в E. Тогда E' — конечно порождено над k и, следовательно, является конечным расширением над k. Кроме того, каждый корень многочлена $p(X)$, лежащий в поле E при вложении σ преобразуется также в корень того же многочлена и, следовательно, определяет вложение E' в себя. Поскольку $\sigma : E' \to E'$ является также гомоморфизмом конечномерных векторных пространств над k, то этот гомоморфизм является изоморфизмом. Следовательно, элемент α лежит в образе гомоморфизма σ.

Лемма 2. Пусть $E_1,\ E_2$ — расширения поля k, содержащиеся в некотором большем поле E, и пусть $\sigma : E \to L$ — вложение полей. Тогда $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.

Эта лемма вытекает из предыдущей.

Предложение 6. Пусть k —поле и f — многочлен из $k[X]$ степени ≥ 1. Существует расширение E поля k, в котором f имеет корень.

Следствие. Пусть k — поле и $f_1,\ \ldots, f_n\ k[X]$ — многочлены степеней ≥ 1. Существует расширение E поля k, в котором каждый f_i имеет корень.

Задача 4. Доказать предложение 6 и его следствие.

Определение 2. Поле L называется алгебраически замкнутым, если всякий многочлен из $L[X]$ степени ≥ 1 имеет в L корень.

Теорема 1. Для всякого поля k существует алгебраически замкнутое поле L, содержащее поле k в качестве подполя.

Доказательство. Построим расширение $k \subset E_1$, в котором всякий многочлен из $k[X]$ степени ≥ 1 имеет корень. Каждому многочлену $f \in k[X]$

степени ≥ 1 сопоставим символ X_f. Пусть S — множество таких символов X_f. Рассмотрим кольцо многочленов $k[S]$ и его идеал, порожденный многочленами $f(X_f)$. Покажем, что этот идеал не совпадает с единичным. Если это не так, то при некоторых $g_i \in k[S]$

$$g_1 f_1(X_{f_1}) + \ \ldots + g_n f_n(X_{f_n}) = 1$$

Многочлены $g_1, \ \ldots, g_n$ зависят только от конечного числа переменных, скажем $X_{f_1}, \ \ldots, X_{f_N}$. Тогда соотношение можно представить как

$$\sum_{i=1}^{n} g_i(X_{f_1}, \ \ldots, X_{f_N}) f_1(X_{f_i}) = 1.$$

Пусть теперь F — конечное расширение, в котором каждый многочлен $f_1, \ \ldots, f_n$ имеет корень, скажем α_i корень многочлена f_i в F. Положим $\alpha_i = 0$ при $i > n$. Подставив α_i вместо X_i в полученное соотношение, получим равенство $0 = 1$. Следовательно, предположение о том, что идеал единичный неверно.

Пусть теперь m — максимальный идеал, содержащий идеал, порожденный всеми многочленами $f(X_f)$. Тогда $k[S]/\mathsf{m}$ — поле и имеется каноническое отображение

$$\sigma : k[S] \to k[S]/\mathsf{m}.$$

Тогда многочлен $f \in k[X]$ степени ≥ 1 имеет в расширении $k \subset k[S]/\mathsf{m}$ корень, равный X_f.

По индукции можно построить такую последовательность полей

$$E_1 \subset E_2 \subset E_3 \subset \ \ldots \subset E_n \subset \ \ldots,$$

что каждый многочлен из $E_n[X]$ степени ≥ 1 имеет корень в E_{n+1}. Обозначим через E объединение всех таких полей. Тогда E — алгебраически замкнутое поле. (Докажите это.)

Следствие 1. Для всякого поля k существует расширение $\bar{k}$, алгебраическое над k и алгебраически замкнутое.

Доказательство. Пусть E — алгебраически замкнутое расширение поля k, и пусть $\bar{k}$ — объединение всех подрасширений из E, алгебраических над k. Тогда $\bar{k}$ алгебраично над k. (Докажите.)

Следствие 2. Пусть L алгебраически замкнутое поле и $f \in L[X]$. Тогда существуют $c \in L$ и $\alpha_1, \ \ldots, \alpha_n$, такие, что

$$f(X) = c(X - \alpha_1) \ \ldots (X - \alpha_n).$$

Коэффициент $c \in L$ совпадает со старшим коэффициентом многочлена $f \in L[X]$. В частности, если коэффициенты многочлена f лежат в подполе k поля L, то $c \in k$.

Предложение 7. Пусть $\sigma : k \to L$ — вложение поля k в алгебраически замкнутое поле L. Пусть $\alpha \in L$ — алгебраический элемент, $E = k(\alpha)$ и $p(X) = \mathrm{Irr}(\alpha, k, X)$. Число всевозможных продолжений вложения σ на $k(\alpha)$ равно числу различных корней многочлена p.

Задача 5. Докажите предложение 7.

Теорема 2. Пусть k — поле, E — его алгебраическое расширение и $\sigma : k \to L$ — вложение k в алгебраически замкнутое поле L. Тогда существует продолжение σ до вложения E в L. Если E алгебраически замкнуто и L алгебраично над σk, то любое такое продолжение σ будет изоморфизмом поля E на L.

Доказательство теоремы основывается на лемме Цорна, о существовании максимального элемента в индуктивно упорядоченном множестве.

Следствие. Пусть k — поле и $E, \ E'$ — алгебраические расширения над k. Пусть $E, \ E'$ алгебраически замкнуты. Тогда существует изоморфизм

$$\tau : E \to E'$$

поля E на E', индуцирующий тождественное отображение на k.

Следовательно, алгебраически замкнутое алгебраическое расширение определено однозначно с точностью до изоморфизма. Всякое такое расширение будет называться *алгебраическим замыканием* поля k и обозначаться через $\bar{k}$.

Предложение 8. Пусть k — бесконечное поле. Тогда любое алгебраическое расширение над k имеет ту же мощность, что и k.

Доказательство следует из оценки мощности расширения E_1 в конструкции доказательства теоремы 1 и построения алгебраического расширения как объединения счетного семейства таких множеств, а также конструкции из следствия для алгебраического замыкания.

Примеры.

1. Поле $\mathbb{C}$ является алгебраически замкнутым. Это следует, например, из основной теоремы алгебры.

2. Подполе поля $\mathbb{C}$, состоящее из всех чисел, алгебраических над $\mathbb{Q}$, есть алгебраическое замыкание $\overline{\mathbb{Q}}$ поля $\mathbb{Q}$. В частности, из предыдущего предложения следует, что $\overline{\mathbb{Q}} \neq \mathbb{C}$.

Пусть задан многочлен $f \in k[X]$ степени ≥ 1. *Полем разложения* K многочлена f называется такое расширение K поля k, в котором многочлен f разлагается на линейные множители

$$f(X) = c(X - \alpha_1) \ldots (X - \alpha_n),$$

где $\alpha_i \in K$ и $K = k(\alpha_1, \ldots, \alpha_n)$.

Из теоремы единственности разложения на простые сомножители в кольце многочленов следует единственность поля разложения с точностью до изоморфизма.

2.2.3 Конечные поля

Пусть F — конечное поле из q элементов. Имеется гомоморфизм колец

$$\mathbb{Z} \to F,$$

преобразующий 1 в 1, ядром которого не может быть 0, и, следовательно, является главным идеалом, порожденным простым числом p, поскольку F не имеет делителей 0. Следовательно, F имеет характеристику p и содержит поле, изоморфное $\mathbb{F}_p = \mathbb{Z}/(p)$.

Заметим, что единственным автоморфизмом поля $\mathbb{F}$ является тождественный. Поэтому можно отождествить поле $\mathbb{F}$ с соответствующим подполем поля F. Тогда F — векторное пространство над $\mathbb{F}$, причем в силу конечности поля его размерность конечна. Пусть $\omega_1, \ldots, \omega_n$ — базис для F над $\mathbb{F}$. Тогда всякий элемент из F однозначно представляется в виде

$$a_1\omega_1 + \ldots + a_n\omega_n,$$

где $a_i \in \mathbb{F}$. Следовательно, $q = p^n$.

Мультипликативная группа F^* имеет порядок $q-1$. Поэтому элементы $\alpha \in F^*$ являются корнями уравнения $X^{q-1}-1=0$. Следовательно, для всех элементов из F выполняется соотношение

$$X^q - X = 0.$$

Следовательно, многочлен $X^q - X$ имеет q различных корней в F и, следовательно, разлагается в F на линейные множители

$$X^q - X = \prod_{\alpha \in F}(X-\alpha).$$

Поэтому F — поле разложения для многочлена $X^q - X$. Но как было доказано выше, поле разложения определено однозначно с точностью до изоморфизма. Следовательно, если конечное поле из q элементов существует, то $q = p^n$ и совпадает с полем разложения многочлена $X^{p^n} - X$ над $\mathbb{F}$.

Докажем, что поле разложения многочлена $X^{p^n} - X$ над $\mathbb{F}$ совпадает с множеством корней многочлена $X^{p^n} - X$ в замыкании $\overline{\mathbb{F}}$. Действительно, пусть $\alpha,\ \beta$ — корни. Тогда

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$

откуда $\alpha+\beta$ — корень. Далее

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

и, следовательно, $\alpha\beta$ — корень. Отметим, что 0 и 1 также корни уравнения $X^{p^n} - X$. Если $\beta \neq 0$, то

$$\left(\beta^{-1}\right)^{p^n} - \beta^{-1} = \left(\beta^{p^n}\right)^{-1} - \beta^{-1} = 0,$$

следовательно, β^{-1} — корень. Наконец,

$$(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}\beta^{p^n} + \beta.$$

При нечетном p выполняется равенство $(-1)^{p^n} = -1$ и, следовательно, $-\beta$ — корень. Если $p = 2$, то $-\beta = \beta$ — корень. Утверждение о корнях доказано.

Производная многочлена $X^{p^n} - X$ равна

$$(X^{p^n} - X)' = p^n X^{p^n-1} - 1 = -1.$$

Следовательно, все корни многочлена $X^{p^n} - X$ различные и, следовательно, он имеет p^n различных корней. Следовательно, его поле разложения содержит ровно p^n различных элементов. Итак, доказана

Теорема 3. Для всякого простого числа p и всякого целого числа $n \geq 1$ существует поле порядка p^n, обозначаемое символом $\mathbb{F}_{p^n}$, однозначно определенное как подполе в алгебраическом замыкании $\overline{\mathbb{F}}$. Это поле разложения многочлена

$$X^{p^n} - X,$$

и его элементы — корни этого многочлена. Всякое конечное поле изоморфно одному и только одному из подполей $\mathbb{F}_{p^n}$.

Следствие. Пусть $\mathbb{F}_q$, где $q = p^n$, — конечное поле и $m \geq 1$ — целое число. В фиксированном алгебраическом замыкании $\overline{\mathbb{F}}_q$ существует одно и только одно расширение степени m, и этим расширением является поле $\mathbb{F}_{q^m}$.

Задача 6. Выведите следствие.

Пусть $q = p^n$ и $\mathbb{F}_q$ — конечное поле из q элементов. Рассмотрим отображение Фробениуса

$$\varphi : \mathbb{F}_q \to \mathbb{F}_q,$$

заданное формулой $\varphi(x) = x^p$. Это отображение является гомоморфизмом и его ядро равно 0, поскольку $\mathbb{F}_q$ — поле. Следовательно, этот гомоморфизм инъективен, а ввиду конечности поля является изоморфизмом. Заметим, что этот изоморфизм оставляет неподвижным поле $\mathbb{F}_q$.

Теорема 4. Группа автоморфизмов поля $\mathbb{F}_q$ является циклической группой порядка n с образующей φ.

Доказательство. Пусть G — группа, порожденная элементом φ. Выполняется равенство $\varphi^n = \mathrm{id}$, поскольку $\varphi^n(x) = x^{p^n} = x$ для всех $x \in \mathbb{F}_q$. Пусть d — период φ. Имеем $\varphi^d(x) = x^{p^d}$ для всех $x \in \mathbb{F}_q$. Следовательно, всякий элемент $x \in \mathbb{F}_q$ является корнем уравнения

$$X^{p^d} - X = 0.$$

Это уравнение имеет не более p^d корней. Следовательно, $d \geq n$, откуда $d = n$.

Согласно предложению 7 число автоморфизмов не превосходит n. Следовательно, $\mathbb{F}_q$ не может иметь других автоморфизмов, кроме тех, что содержатся в G.

2.2.4 Корни из единицы

Пусть k — поле. Элемент $\zeta \in k$ называется *корнем из единицы* в k, если для некоторого $n \geq 1$ выполняется соотношение $\zeta^n = 1$. Заметим, что если характеристика поля равна p, то уравнение

$$X^{p^m} = 1$$

имеет только один корень, равный 1.

Пусть целое число $n > 1$ взаимно просто с характеристикой поля k . Тогда многочлен

$$X^n - 1$$

не имеет кратных корней, поскольку его производная nX^{n-1} обращается в нуль только при $X = 0$. Следовательно, в алгебраическом замыкании поля k, в поле $\bar{k}$, многочлен $X^n - 1$ имеет n различных корней, являющихся корнями из единицы. Они образуют группу, а эта группа, как было доказано выше, является циклической. Образующие этой группы называются *примитивными*, или *первообразными*, корнями n -й степени из единицы.

Обозначим через U_n группу всех корней n-й степени из единицы в $\bar{k}$. Пусть m, n взаимно простые числа, тогда

$$U_{mn} \approx U_n \times U_n.$$

Докажем, что пересечение групп $U(n)$ и $U(m)$ состоит только из 1. Пусть это не так и пересечение содержит $x \neq 1$. Из взаимной простоты элементов m и n следует, что при некоторых целых a, b выполняется равенство $1 = am + bn$. Тогда

$$x = x^{am+bn} = 1.$$

Следовательно, $U_m \times U_n = U_m U n = U_{mn}$.

Теорема 5. Для всякого примитивного корня n-й степени из единицы ζ

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

Доказательство. Пусть $f(X)$ — неприводимый многочлен элемента ζ над $\mathbb{Q}$. Тогда $f(X)$ делит многочлен $X^n - 1$, поэтому $X^n - 1 = f(X)h(X)$, где f, g имеют старший коэффициент 1. Тогда по лемме Гаусса эти многочлены целочисленные.

Пусть p простое, не делящее n. Докажем, что ζ^p корень многочлена $f(X)$. Если это не так, то ζ^p корень многочлена $h(X)$ и, следовательно, ζ — корень многочлена $h(X^p)$. Поэтому многочлены $f(X)$ и $h(X^p)$ имеют нетривиальный общий делитель, а поскольку многочлен $f(X)$ — неприводимый, то

$$h(X^p) = f(X)g(X),$$

причем (доказывается как и выше) многочлен $g(X)$ целочисленный. Тогда из равенства

$$h(X^p) \equiv h(X)^p \pmod{p}$$

следует, что

$$h(X)^p \equiv f(X)g(X) \pmod{p}.$$

Следовательно, в кольце $\mathbb{F}_p[X]$ многочлены $f(X)$ и $h(X)$ имеют нетривиальный общий множитель и в этом кольце выполняется равенство $X^n - 1 = f(X)g(X)$ и, следовательно, многочлен $X^n - 1 \in \mathbb{F}_p[X]$ имеет кратные корни. Но это невозможно. Действительно, производная этого многочлена равна nX^{n-1} и, следовательно, не обращается в нуль в корнях из единицы, поскольку n и p взаимно простые. Следовательно, ζ^p корень многочлена $f(X)$.

Поскольку ζ^p — тоже примитивный корень n-й степени их единицы и любой примитивный корень можно получить последовательным возведением ζ в простые степени с показателями, не делящими n (поскольку группа корней из единицы циклическая), то все примитивные корни из единицы являются корнями многочлена f, который поэтому имеет степень $\geq \varphi(n)$.

Докажем, что степень f не превосходит $\varphi(n)$. Если это не так, существует такое s, имеющее нетривиальный общий множитель с n, такое, что ζ^s

корень многочлена f. Тогда соответствие $\zeta \mapsto \zeta^s$ определяет автоморфизм полей

$$\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta).$$

Пусть $q \geq 0$ наименьшее целое, такое, что $qs \equiv 0 \pmod{n}$. Тогда $q < n$ и

$$\zeta^q \to \zeta^{sq} = \zeta^{nl} = 1.$$

Следовательно, $\zeta^q = 1$, что противоречит примитивности корня ζ. Поэтому $\deg f(X) \leq n$. Учитывая доказанное неравенство $\deg f(X) \geq n$, получаем равенство $\deg f(X) = n$. Теорема доказана.

Пусть ζ_n обозначает произвольный примитивный корень степени n из единицы.

Следствие. Если $n, m \in \mathbb{N}$ — взаимно простые числа, то

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

Доказательство. Заметим, что ζ_n и ζ_m лежат в поле $\mathbb{Q}(\zeta_{nm})$, поскольку ζ_{nm}^n — примитивный корень m-й степени из единицы, а $\zeta_m\zeta_n$ — примитивный корень степени mn из единицы. Следовательно,

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m\zeta_n).$$

Теперь утверждение следствия вытекает из мультипликативности функции Эйлера $\varphi(mn) = \varphi(m)\varphi(n)$.

Исследуем разложение на множители многочлена $X^n - 1$. Пусть характеристика поля равна 0. Имеем

$$X^n - 1 = \prod_{\omega}(X - \omega),$$

где произведение берется по всем корням n-й степени из единицы. Сгруппируем члены, соответствующие корням из единицы, имеющим одинаковый период. Пусть

$$f_d(X) = \prod_{\text{период } \omega = d} (X - \omega).$$

Тогда

$$X^n - 1 = \prod_{d|n} f_d(X).$$

Из доказанной выше теоремы следует, что $f_d(X) = \mathrm{Irr}(\zeta_d, \mathbb{Q}, X)$. Этот многочлен можно вычислить также с помощью рекуррентной формулы

$$f_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} f_d(X)}.$$

и очевидного равенства $f_1(X) = X - 1$.

Многочлен $f_n(X)$ называется *n-м круговым (cyclotomic) многочленом*, или *многочленом деления круга* на n частей.

Все сказанное выше относится также к разложению многочленов $X^n - 1$ для степеней n, взаимно простым с характеристикой поля. В частности при p и n взаимно простых, определены n-круговые многочлены над $\mathbb{F}_p$.

Пусть $f_n(X) = \prod h(X)$ — разложение n-го кругового многочлена на неприводимые множители в алгебраическом замыкании $\overline{\mathbb{F}}_p$ поля $\mathbb{F}_p$. Положим $k = o_p(r)$ — порядок элемента p в группе единиц $\mathbb{Z}_r^*$ кольца $\mathbb{Z}_r$. Докажем, что $\deg h = k$. Пусть $\deg h = s$. Поскольку многочлен h неприводим, определено конечное расширение степени s, поля $\mathbb{F}_p$, являющееся конечным полем из p^s элементов. Согласно теореме 4 группа автоморфизмов этого поля состоит из s элементов, являющимися автоморфизмами Фробениуса. Пусть ζ — корень многочлена h. Этот корень, согласно определению многочлена h, имеет период r, т. е. $\zeta^r = 1$ и $\zeta^t \neq 1$ при $1 < t < r$. Пусть $p^s \equiv t (\mathrm{mod} r)$ и $0 < t < r$. Тогда по теореме 4 $\zeta^{p^s} = \zeta$. Следовательно, $\zeta^t = \zeta^{p^s} = \zeta$. Следовательно, $t = 1$. Поэтому $k = s$.

2.3 Основные понятия теории решеток. Критерий полноты решетки. Лемма Минковского

2.3.1 Введение в решетки

Вначале напомним некоторые результаты из теории групп.

Определение 1. Элементы $\alpha_1, \ \ldots, \alpha_n$ аддитивной абелевой группы M называется системой образующих группы, рассматриваемой как $\mathbb{Z}$-модуль, если любой элемент $\alpha \in M$ можно представить в виде $\alpha = c_1\alpha_1 + \ \ldots +$

$c_n\alpha_n$, где $c_i \in \mathbb{Z}$. Система образующих называется базисом, если такое представление единственно.

Определение 2. Элемент a аддитивной абелевой группы M называется элементом конечного порядка, если $ca = 0$ при некотором $c \in \mathbb{Z}$.

Теорема 1. Если абелева группа без элементов конечного порядка имеет конечную систему образующих, то она имеет и базис. Число элементов базиса является инвариантом группы.

Доказательство. Пусть $\alpha_1, \ \ldots, \alpha_n$ — произвольная система образующих. Заметим, что при замене одной образующей на новую, полученную добавлением к ней другой, умноженной на произвольное целое число, снова получится система образующих. Действительно, пусть $\alpha_1' = \alpha_1 + k\alpha_2$. Тогда для любого $\alpha \in M$ имеем

$$\alpha = c_1\alpha_1 + \ \ldots + c_n\alpha_n = c_1\alpha_1' + (c_2 - kc_1)\alpha_2 + \ \ldots + c_n\alpha_n.$$

Если элементы $\alpha_1, \ \ldots, \alpha_n$ линейно независимы, то они образуют базис M. Допустим теперь, что они линейно зависимы, т. е. выполняется соотношение

$$c_1\alpha_1 + \ \ldots + c_n\alpha_n = 0$$

при некоторых одновременно не равных нулю целых $c_1, \ \ldots, c_n$. Выберем среди ненулевых элементов коэффициент c_i с наименьшим абсолютным значением. Без ограничения общности можно считать, что это c_1. Пусть не все коэффициенты c_i делятся на c_1, например, $c_2 = c_1q + c'$, где $0 < c' < |c_1|$. Перейдем к новой системе образующих $\alpha_1' = \alpha_1 + q\alpha_2, \ \ldots, \alpha_n$. Тогда будет выполняться соотношение

$$c_1\alpha_1' + c'\alpha_2 + \ \ldots + c_n\alpha_n = 0,$$

причем $0 < c' < |c_1|$. Продолжим данную процедуру до тех пор пока через конечное число шагов (не более $|c_1|$) не получим соотношение

$$k_1\beta_1 + k_2\beta_2 + \ \ldots + k_n\beta_n = 0$$

с целыми коэффициентами k_i, в котором один из коэффициентов, например, k_1 является делителем остальных. Сократив последнее выражение на k_1, получим

$$\beta_1 + l_2\beta_2 + \ \ldots + l_n\beta_n = 0$$

с целыми $l_2,\ \ldots, l_n$. Следовательно, $\beta_2,\ \ldots, \beta_n$ — система образующих группы M. Повторив это рассуждение конечное число раз, получим базис группы.

Инвариантность числа элементов базиса следует из инвариантности размерности векторного пространства $M \otimes \mathbb{Q}$.

Напомним, что $M \otimes \mathbb{Q} = M \times \mathbb{Q}/\sim$, где отношение $\sim$ задается формулой

$$(k\alpha, r) \sim (\alpha, kr),$$

где $k \in \mathbb{Z}$.

Пусть $\omega_1,\ \ldots, \omega_m$ и $\omega'_1,\ \ldots, \omega'_m$ — два базиса модуля M. Тогда матрица перехода одного базиса в другой целочисленная. Поскольку их произведения являются единичными матрицами, определители матриц замены базиса равны ± 1. Следовательно, эти преобразования являются унимодулярными матрицами порядка m.

Теорема 2. В абелевой группе M без элементов конечного порядка и с конечной системой образующих всякая подгруппа N также имеет конечное число образующих и, следовательно, имеет базис. При этом для любого базиса $\omega_1,\ \ldots, \omega_m$ группы M для N существует базис вида

$$\begin{array}{lllllll}
\eta_1 & = & c_{11}\omega_1 + & c_{12}\omega_2 + & \ldots + & c_{1k}\omega_k + & \ldots + c_{1m}\omega_{1m}, \\
\eta_2 & = & & c_{22}\omega_2 + & \ldots + & c_{2k}\omega_k + & \ldots + c_{1m}\omega_{2m}, \\
\ldots & \ldots & \ldots\ldots & \ldots\ldots\ldots & & \ldots\ldots\ldots\ldots\ldots\ldots & , \\
\eta_k & = & & & & c_{1k}\omega_k + & \ldots + c_{1m}\omega_{1m},
\end{array}$$

Определение 3. Решеткой называется конечно порожденная подгруппа группы $\mathbb{R}^n$. Если ранг группы равен n, то решетка называется полной, в противном случае — неполной. Базис группы называется в этом случае базисом решетки.

Замечание. В силу теорем 1 и 2 число k из определения 3 задается решеткой однозначно и называется рангом группы M. Следовательно, ранг группы равен рангу матрицы, строками которой являются координаты образующих, или же ранг матрицы, строками которой являются попарные произведения образующих векторов.

В векторном пространстве $\mathbb{R}^n$ определены скалярное произведение и норма.

Определение 4. Подгруппа G группы $\mathbb{R}^n$ называется дискретной, если в шаре $U(r) = \{x \in \mathbb{R}^n \mid \|x\| < r\}$ радиуса r имеется только конечное число элементов группы G.

Лемма 1. Решетка является дискретной группой.

Доказательство. Выберем базис $b_1, \ldots, b_k$ в решетке. Дополним этот базис до базиса в векторном пространстве $\mathbb{R}^n$, содержащем решетку. Пусть это базис $b_1, \ldots, b_n$. Тогда существует ненулевой элемент $x \in \mathbb{R}^n$, ортогональный векторам $b_2, \ldots, b_n$. Положим $f_1 = \frac{x}{(x,b_1)}$. Заметим, что знаменатель согласно определению элемента x не может равняться нулю и $(f_1, b_j) = \delta_{1j}$. Аналогично определяются элементы f_i, причем выполняются равенства $(f_i, b_j) = \delta_{ij}$.

Пусть z — элемент решетки длины меньшей r. Тогда

$$z = a_1 b_1 + \ldots + a_n b_n$$

при целых $a_1, \ldots, a_n$, причем $a_k = (z, f_k)$ по определению векторов f_k. Тогда согласно неравенству Коши

$$|a_k| = |(z, f_k)| \leq \|z\|\|f_k\| < r\|f_k\|.$$

Следовательно, ввиду целочисленности коэффициентов a_k, в шаре радиуса r лежит конечное число элементов решетки.

Определение 5. Пусть $b_1, \ldots, b_k$ — базис решетки. Основным параллелепипедом решетки называется множество

$$T = \{x \in \mathbb{R}^n \mid x = c_1 b_1 + \ldots + c_k b_k, 0 \leq c_i < 1\}.$$

Объем основного параллелепипеда называется детерминантом решетки.

Лемма 2. Детерминант решетки не зависит от базиса.

Доказательство. Дополним базис решетки до базиса векторного пространства $\mathbb{R}^n$ взаимно ортогональными векторами единичной длины $b_{k+1}, \ldots, b$ ортогональными подпространству, порожденному векторами $b_1, \ldots, b_k$. Тогда объем основного параллелепипеда на базисе $b_1, \ldots, b_k$ равен объему основного параллелепипеда на базисе $b_1, \ldots, b_n$. Пусть $f_1, \ldots, f_k$ другой базис решетки. Тогда его можно пополнить теми же векторами $b_{k+1}, \ldots, b_n$ до базиса в $\mathbb{R}^n$. Преобразование базиса $b_1, \ldots, b_k$ в базис $f_1, \ldots, f_k$ продолжается до унимодулярного преобразования базиса $b_1, \ldots, b_n$ в базис $f_1, \ldots, f_k, b_{k+1}, \ldots, b_n$.

Объем основного параллелепипеда равен абсолютной величине определителя, строками которого являются координаты базисных векторов,

$$\begin{vmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{vmatrix}.$$

Поскольку базисы связаны унимодулярными преобразованиями, соответствующие объемы равны.

Лемма 3. Если T — основной параллелепипед полной решетки M, то имеется разбиение

$$\mathbb{R}^n = \bigcup_{z \in M} z + T,$$

причем $z + T \cap w + T = \emptyset$ при $z \neq w$.

Упражнение. Доказать лемму 3.

Лемма 4. Пусть M — решетка. Для любого $r > 0$ множество $N = \{z \in M \mid z + T \cap U(r) \neq \emptyset\}$ конечно.

Доказательство. Пусть $b_1, \ \ldots, b_n$ — базис решетки M. Положим

$$d = \|b_1\| + \ \ldots + \|b_n\|.$$

Пусть $x = z + t \in U(r)$, где $z \in M$ и $t \in T$. Тогда

$$\|t\| = \|\alpha_1 b_1 + \ \ldots + \alpha_n b_n\| \leq \alpha_1 \|b_1\| + \ \ldots + \alpha_n \|b_n\| < d$$

и

$$\|z\| = \|x - t\| \leq \|x\| + \|b_n\| < r + d,$$

т. е. множество N лежит в шаре радиуса $r + d$ и, следовательно, согласно лемме 1 конечно.

Лемма 5. Подгруппа $M \subset \mathbb{R}^n$, множество элементов которой дискретно, является решеткой.

Доказательство. Пусть $L \subset \mathbb{R}^n$ — минимальное линейное пространство, содержащее группу M. Выберем в L базис $b_1, \ \ldots, b_m$ из элементов группы M и построим решетку M_0 с этим базисом. Тогда M_0 — подгруппа в M. Покажем, что индекс этой группы конечен. Для этого достаточно

проверить, что факторгруппа M/M_0 состоит из конечного числа элементов. Согласно лемме 3 элементы факторгруппы однозначно представляются элементами группы M, лежащими в главном параллелепипеде решетки M_0, а решетка лежит в шаре конечного радиуса. Поскольку группа M дискретна, согласно лемме 4 число таких элементов конечно. Следовательно доказано, что группа M конечно порождена и, поэтому является решеткой.

Из лемм 1 и 5 вытекает

Следствие. Подгруппа $M \subset \mathbb{R}^n$ является решеткой тогда и только тогда, когда она дискретна.

Лемма 6. Пусть $b_1, \ \ldots, b_m$ базис решетки M. Тогда ее детерминант равен квадратному корню из определителя

$$\begin{vmatrix} (b_1, b_1) & \cdots & (b_1, b_m) \\ \cdots & \cdots & \cdots \\ (b_m, b_1) & \cdots & (b_m, b_m) \end{vmatrix}.$$

Доказательство. Согласно доказательству лемме 2 детерминант решетки равен абсолютной величине определителя матрицы

$$D = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix},$$

где $b_1, \ \ldots, b_m$, а $b_{m+1}, \ \ldots, b_n$ — его ортогональное продолжение. Поэтому, детерминант равен квадратному корню из квадрата определителя матрицы D и, следовательно, равен квадратному корню из определителя мат-

рицы DD', где $'$ — операция транспонирования. Имеем

$$
\begin{aligned}
DD' &= \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ \cdots & \cdots & \cdots \\ b_{1n} & \cdots & b_{nn} \end{pmatrix} \\
&= \begin{pmatrix} (b_1, b_1) & \cdots & (b_1, b_n) \\ \cdots & \cdots & \cdots \\ (b_n, b_1) & \cdots & (b_n, b_n) \end{pmatrix} \\
&= \begin{pmatrix} (b_1, b_1) & \cdots & (b_1, b_m) & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (b_m, b_1) & \cdots & (b_m, b_m) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{pmatrix} \\
&= \begin{pmatrix} (b_1, b_1) & \cdots & (b_1, b_m) \\ \cdots & \cdots & \cdots \\ (b_m, b_1) & \cdots & (b_m, b_m) \end{pmatrix}.
\end{aligned}
$$

2.3.2 Критерий полноты решетки. Теорема Минковского

Теорема 3. Решетка M в линейном пространстве L полна тогда и только тогда, когда в L существует ограниченное множество U, сдвиги которого на векторы из M полностью заполняют все пространство L.

Доказательство. Если решетка M полная, то в качестве U можно взять любой ее основной параллелепипед (лемма 3).

Пусть теперь решетка M неполная, и пусть U — произвольное ограниченное подмножество в L. Тогда существует $r > 0$, при котором $\|x\| < r$ для любого $x \in U$. Пусть $L_0 \subset L$ — подпространство, порожденное решеткой M. Поскольку решетка неполная, то L_0 — собственное подпространство и, следовательно, существует вектор $y \in L$, имеющий длину больше r и ортогональный подпространству L_0. Покажем, что y не покрывается сдвигами множества U. Пусть это не так, тогда при некоторых $u \in U$,

$z \in M$ выполняется равенство $y = u+z$. Тогда согласно неравенству Коши-Буняковского

$$\|y\|^2 = (y, y) = (y, u) \leq \|y\| \cdot \|u\| < r\|y\|,$$

откуда $\|y\| < r$.

Теорема 4 (лемма Минковского о выпуклом теле). Пусть в n -мерном пространстве $\mathbb{R}^n$ заданы полная решетка M, объем основного параллелепипеда которой равен Δ, и ограниченное центрально симметричное выпуклое множество X с объемом $v(X)$. Если $v(X) > 2^n\Delta$, то множество X содержит по крайней мере одну отличную от нуля точку решетки M.

Доказательство. Докажем вначале, что если множество $Y \subset \mathbb{R}^n$ таково, что все его сдвиги $Y_z = Y + z$ на векторы z из решетки M не пересекаются, то $v(Y) \leq \Delta$. Рассмотрим основной параллелепипед T решетки M и рассмотрим пересечения $Y \cap T_{-z}$. Тогда по лемме 3

$$v(Y) = \sum_{z \in M} v(Y \cap T_{-z}),$$

причем по лемме 4 в этой сумме только конечное число слагаемых не равно нулю. Сдвиг множества $Y \cap T_{-z}$ на вектор z равен $Y_z \cap T$, поэтому $v(Y \cap T_{-z}) = v(Y_z \cap T)$. Следовательно,

$$v(Y) = \sum_{z \in M} v(Y_z \cap T).$$

Поскольку все Y_z попарно не пересекаются, то сумма правой части не больше $v(T)$. Следовательно, $v(X) \leq v(T) = \Delta$.

Рассмотрим теперь множество $\frac{1}{2}X$, получающееся из X сжатием в два раза. Тогда из условия теоремы следует, что $v\left(\frac{1}{2}X\right) = \frac{1}{2^n}v(X) > \Delta$. Если бы все сдвиги множества $\frac{1}{2}X$ на элементы решетки попарно не пересекались бы, то по доказанному выше должно было бы выполняться неравенство $v\left(\frac{1}{2}X\right) \leq \Delta$. Но это не так. Следовательно, существуют $z_1, z_2 \in M$,

для которых множества $\frac{1}{2}X + z_1$ и $\frac{1}{2}X + z_2$ имеют непустое пересечение. Следовательно,

$$\frac{1}{2}x' + z_1 = \frac{1}{2}x'' + z_2, \quad x', x'' \in X.$$

Тогда

$$z_1 - z_2 = \frac{1}{2}x'' - \frac{1}{2}x' = \frac{1}{2}x'' + \frac{1}{2}(-x').$$

Поскольку множество X центрально симметрично и выпукло, то разность $z_1 - z_2 \in M$ лежит также и в X.

Теорема 5 (Неравенство Адамара). Пусть $det(\Lambda)$ детерминант решетки и $b_1, \ldots, b_n$ — ее базис. Справедливо неравенство

$$det(\Lambda) \leq ||b_1|| \cdot \ \ldots \cdot ||b_n||,$$

где $||\cdot||$ — евклидова норма, т. е. $||x|| = \sqrt{x^T x}$.

Доказательство. Пусть $b_1, \ \ldots, b_n$ — базис решетки. Рассмотрим процедуру ортогонализации базиса:

$$b_1^* = b_1, b_2^* = b_2 - \frac{(b_1, b_2)}{(b_1, b_1^*)}b_1^*, \ \ldots, b_n^* = b_n - \sum_{k=1}^{n-1} \frac{(b_n, b_k^*)}{(b_k^*, b_k^*)}b_k^*.$$

Выполняются неравенства $\|b_k^*\| \leq \|b_k\|$. Тогда

$$det(\Lambda) = \|b_1^*\| \cdot \ \ldots \cdot \|b_n^*\| \leq ||b_1|| \cdot \ \ldots \cdot ||b_n||$$

Из доказательства следует, что неравенство Адамара достигается в том и только в том случае, когда $b_1, \ \ldots, b_n$ — ортогональны. Однако не всякая решетка имеет ортогональный базис. Классическая теорема Эрмита (1850 г.) утверждает, что для каждого n существует такое число $c(n)$, что в любой n-мерной решетке Λ можно выбрать базис $b_1, \ \ldots, b_n$, для которого

$$||b_1|| \cdot \ \ldots \cdot ||b_n|| \leq c(n) \cdot det(\Lambda).$$

Эрмит показал, что можно положить $c(n) = (4/3)^{n(n-1)/4}$. Минковский улучшил эту оценку до $c(n) = 2^n/V_n \sim (2n/e\pi)^{n/2}$, где V_n — объем единичного n-мерного шара. Однако для всех этих оценок неизвестны полиномиальные алгоритмы отыскания соответствующих базисов. Ловас предложил полиномиальный алгоритм отыскания базиса с константой $c(n) = 2^{n(n-1)/4}$, получивший название метода приведения базиса.

Определение. Пусть $B_m(0,r)$ — открытый шар радиуса r в пространстве $\mathbb{R}^n$ и Λ — решетка. Определим последовательность минимумов $\lambda_1,\ \ldots, \lambda_n$ формулой

$$\lambda_i(\Lambda) = \inf\{r|\ \dim(\textbf{span}(\Lambda \cap B_m(0,r))) \geq i\}.$$

Теорема 6 (Вторая теорема Минковского). Существуют независимые векторы решетки, для которых выполняется неравенство

$$||b_1|| \cdot\ \ldots \cdot ||b_n|| \leq \frac{2^n}{V_n} \cdot det(\Lambda).$$

Доказательство. Пусть $x_1,\ \ldots, x_n$ — линейно независимые векторы решетки, для которых достигаются минимальные значения $\lambda_1,\ \ldots, \lambda_n$ и предположим, что $\prod_{i=1}^{n} \lambda_i > \frac{2^n}{V_n} \cdot det(\Lambda)$. Пусть векторы x_i^* получены с помощью процедуры ортогонализации Грамма-Шмидта. Рассмотрим преобразование

$$T\left(\sum_{i=1}^{n} c_i x_i^*\right) = \left(\sum_{i=1}^{n} \lambda_i c_i x_i^*\right).$$

Пусть $S = B_m(0,1) \cap \textbf{span}(\Lambda)$ — n-мерный шар в $\textbf{span}(\Lambda)$. Тогда

$$\begin{array}{rcl} \textbf{vol}(T(S)) & = & (\prod_i \lambda_i)\, \textbf{vol}(S) \\ & > & \frac{2^n}{V_n} \cdot det(\Lambda) \textbf{vol}(S) \\ & = & 2^n \textbf{vol}(\Lambda). \end{array}$$

Следовательно, по теореме Минковского в $T(S)$ имеется ненулевая точка решетки y. Следовательно, существует точка $x \in S$, для которой $T(x) = y$. Из определения S следует, что $\|x\| < 1$. Выполняются равенства

$$\begin{array}{rcl} x & = & \sum_{i=1}^{n} c_i x_i^* \\ y & = & \sum_{i=1}^{n} \lambda_i c_i x_i^*. \end{array}$$

Поскольку $y \neq 0$ при некотором i выполняется неравенство $c_i \neq 0$. Пусть k — максимальное значение такого i, при котором $c_i \neq 0$ и k' — минимальное значение индекса, при котором $\lambda_{k'} = \lambda_k$. Отметим, что элемент

y линейно независим от $x_1, \ \ldots, x_{k'}$, поскольку $(x_k^*, y) = \lambda_k c_k \|x_k^*\|^2 \neq 0$ и элемент x_k^* ортогонален $x_1, \ \ldots, x_{k'}$. Покажем теперь, что $\|y\| < \lambda_k$. Действительно,

$$\begin{aligned} \|y\|^2 &= \left\| \sum_{i \leq k} \lambda_i c_i x_i^* \right\|^2 \\ &= \sum_{i \leq k} \lambda_i^2 c_i^2 \, \|x_i^*\|^2 \\ &\leq \sum_{i \leq k} \lambda_k^2 c_i^2 \, \|x_i^*\|^2 \\ &= \lambda_k^2 \left\| \sum_{i \leq k} c_i x_i^* \right\|^2 \\ &= \lambda_k^2 \|x\|^2 < \lambda_k^2. \end{aligned}$$

Полученное неравенство противоречит определению k'-го последовательного минимума $\lambda_{k'}$.

Следствие. Для первого минимума λ_1 выполняется неравенство

$$\lambda_1 \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{det(\Lambda)}.$$

2.4 Применение алгебры. Полиномиальный алгоритм проверки простоты чисел

2.5 Полиномиальная детерминированная проверка простоты

Проблема проверки простоты натурального числа является одной из древнейших и классических задач теории чисел.

Неэффективные тесты (типа решета Эратосфена) были известны еще до нашей эры.

С развитием теории алгоритмов возник вопрос о существовании эффективных (полиномиальных) алгоритмов проверки простоты числа, которые за полиномиальное от длины входа ($\lceil \log(n+1) \rceil$ для числа n, заданного в двоичной системе) проверяют, является ли n простым числом.

Мы описываем ниже модифицированный алгоритм проверки простоты, предложенный в 2002 г. тремя индийскими математиками. Более точно, мы опираемся на статьи [AKS02; AKS04].

Некоторые определения и обозначения

Определение 2.5.1. *Через* НОД(a, n) *обозначим наибольший общий делитель (НОД) чисел* a *и* n.

Определение 2.5.2. *Пусть* НОД$(r, n) = 1$. *Тогда* $o_r(n)$ *— **порядок** n **по модулю** r: минимальное натуральное k такое, что*

$$n^k = 1 \pmod r.$$

*Через $\varphi(r)$ обозначается **функция Эйлера**, равная числу взаимно простых с r чисел, не превосходящих r.*

Определение 2.5.3. *Через Z_n обозначим кольцо целых чисел по модулю n, а через F_p — конечное поле из p элементов, где p — простое число. Через $Z_n[X]$ обозначим кольцо многочленов с коэффициентами из Z_n, а через $F_p[X]$ — кольцо многочленов с коэффициентами из F_p.*

Определение 2.5.4. *Напомним, что для простого p и неприводимого в F_p многочлена $h(x)$ степени d, $F_p[X]/(h(X))$ — конечное поле порядка p^d. Мы будем пользоваться обозначением*

$$f(X) \equiv g(X) \pmod{h(X), n}$$

для обозначения уравнения $f(X) = g(X)$ в кольце $Z_n[X]/(h(X))$.

Идея и основная лемма

Лемма 1. *Пусть a — целое число, n — натуральное, $n \geq 2$ и* НОД$(a, n) = 1$. *Тогда n простое тогда и только тогда, когда*

$$(X + a)^n = X^n + a \pmod n.$$

Доказательство. Заметим, что если $0 < i < n$, то коэффициент при X^i в $(X + a)^n - (X^n + a)$ равен $\binom{n}{i} a^{n-i}$.

Рассмотрим два случая.

1. n — простое. Тогда $\binom{n}{i} \bmod n = 0$ и все коэффициенты равны нулю.

2. n — составное. Рассмотрим его простой делитель q и пусть k — максимальная степень такая, что n делится на q^k. Тогда q^k не является делителем $\binom{n}{q}$ и взаимно просто с a^{n-q} (докажите это в качестве упражнения). Следовательно, коэффициент при X^q не равен нулю $(\bmod n)$.

□

Что дает нам эта лемма? На первый взгляд ничего, т.к. вычисление левой части тождества требует вычисления n коэффициентов в худшем случае. Однако она дала идею нового простого вероятностного теста на простоту, которая и привела к построению детерминированного полиномиального алгоритма проверки простоты числа. В некотором смысле можно рассматривать этот результат как *дерандомизацию соответствующего вероятностного алгоритма проверки специального тождества*.

Основная идея дерандомизации — заменить основное тождество на другое:

$$(X + a)^n = X^n + a \,(\bmod\, X^r - 1, n),$$

для некоторого специального r, ограниченного полиномом от $\log n$. К сожалению, в таком виде этому тождеству будут удовлетворять и некоторые составные числа. Ключевая идея авторов алгоритма заключалась в проверке данного тождества для целой серии значений a, число которых ограничено полиномом от $\log n$.

Им удалось показать, что данной серии тождеств удовлетворяют только простые числа, и, таким образом, построить детерминированный полиномиальный алгоритм проверки простоты произвольного натурального числа. На вход алгоритма подается число n, записанное в двоичной системе, а результатом алгоритма является 1, если n — простое, и 0, если n — составное.

Алгоритм 5 Полиномиальный алгоритм проверки простоты

Вход: целое $n > 1$.

Выход: целое 1 — если простое, и 0, если n — составное.

1. **if** ($n = a^b$ для $a \in N$ и $b > 1$) **return** 0.
2. Найти наименьшее r такое, что $o_r(n) > \log^2 n$.
3. **for** $a = 1$ **to** r
   do if $1 < \text{НОД}(a, n) < n$ **return** 0.
4. **if** $n \leq r$, return 1.
5. **for** $a = 1$ to $\lfloor \sqrt{\varphi(r)} \log n \rfloor$ **do**
   if $(X + a)^n \neq X^n + a \pmod{X^r - 1, n}$ **return** 0.
6. **return** 1.

Время работы

Покажем, что алгоритм 5 полиномиален.

Приведем без доказательства известный факт из теории чисел.

Лемма 2. *Обозначим через* ***LCM(****m****)*** *наименьшее общее кратное первых m натуральных чисел. Тогда* ***LCM(****m****)*** *не меньше 2^m при $m \geq 7$.*

Лемма 3. *Существует $r \leq \max(3, \lceil \log^5 n \rceil)$, такое, что $o_r(n) > \log^2 n$.*

Доказательство. При $n = 2$ значение $r = 3$ тривиально удовлетворяет всем условиям. Предположим, что $n > 2$.

Тогда $\lceil \log^5 n \rceil > 10$, и мы можем воспользоваться леммой 2.

Пусть $r_1, r_2, \ldots, r_t$ — все числа, такие, что $o_{r_i}(n) \leq \log^2 n$, а $q_1, \ldots, q_k$ — делители n. Пусть M — множество, состоящее из элементов r_i, q_j и всевозможных произведений $r_i q_j$. Каждое из чисел множества M должно делить произведение

$$n \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) < n^{\log^4 n} \leq 2^{\log^5 n}.$$

По лемме наименьшее общее кратное первых $\lceil \log^5 n \rceil$ натуральных чисел не меньше $2^{\lceil \log^5 n \rceil}$, и, следовательно, существует число $s \leq \lceil \log^5 n \rceil$, такое, что $s \notin M$. Если НОД$(s, n) = 1$, то все доказано. Если же НОД$(s, n) > 1$, то, поскольку s не делит n и НОД$(s, n) = q_j$ при некотором j, то $r = \frac{s}{\text{НОД}(s,n)} = \frac{s}{q_j} \neq r_i$ ни при каком i, и, следовательно, $o_r(n) > \log^2 n$.

□

Упражнение 2.5.1. Покажите, что шаг 1 можно выполнить за полиномиальное время.

Из леммы 3 вытекает, что шаги 2–5 выполнимы за полиномиальное время.

Отсюда получаем следующую теорему.

Теорема 7. *Алгоритм 5 полиномиален.*

Упражнение 2.5.2. Для каких n можно исключить шаг 4 из алгоритма 5?

Корректность

То, что для простого n алгоритм выдает 1, очевидно следует из описания алгоритма.

Нам надо доказать, что если алгоритм выдает 1, то n является простым числом (т. е. если число составное, то сработает какая-либо из «проверок» алгоритма, и алгоритм вернет 0).

Итак, допустим, число n — составное, но шаги 1 и 3 его не выявили. Рассмотрим последний «фильтр» — самый содержательный шаг алгоритма, шаг 5, внимательно.

Поскольку $o_r(n) > 1$ (кстати, почему?), должно существовать простое p, делящее n, такое, что $o_r(p) > 1$ (заметим, что если n — простое, то $p = n$). Зафиксируем числа p и n. Пусть также $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$.

На шаге 5 алгоритма проверяется l уравнений. Поскольку по нашему предположению алгоритм не выдает 0, то для любого $0 \leq a \leq l$

$$(X + a)^n = X^n + a \ (\text{mod } X^r - 1, n),$$

откуда следует

$$(X+a)^n = X^n + a \pmod{X^r - 1, p}.$$

С другой стороны, из основной леммы 1 следует, что

$$(X+a)^p = X^p + a \pmod{X^r - 1, p}.$$

Из двух предыдущих равенств следует, что

$$(X+a)^{n/p} = X^{n/p} + a \pmod{X^r - 1, p}.$$

Упражнение 2.5.3. Докажите этот факт, используя тождество

$$(X+a)^p \equiv X^p + a^p \pmod{p}.$$

Доказательство. Отметим, что

$$\mathbb{Z}[X]/(X^r - 1, p) = \mathbb{F}_p[X]/(X^r - 1).$$

Пусть

$$(X+a)^{n/p} - X^{n/p} - a = q(X) \in \mathbb{F}_p[X].$$

Тогда в кольце $\mathbb{F}_p[X]$ выполняется равенство

$$\left((X+a)^{n/p} - X^{n/p} - a\right)^p = (q(X))^p.$$

Возводя в степень p в кольце $\mathbb{F}_p[X]$ левую часть равенства, получим

$$\left((X+a)^{n/p} - X^{n/p} - a\right)^p = (X+a)^n - (X^{n/p} + a)^p = \\ = (X+a)^n - (X^n + a).$$

Следовательно, в кольце $\mathbb{F}_p[X]$ выполняется равенство

$$(X+a)^n - (X^n + a) = (q(X))^p.$$

С другой стороны, по условию задачи в кольце $\mathbb{F}_p[X]$ выполняется равенство

$$(X+a)^n - (X^n + a) = s(X)(X^r - 1).$$

Следовательно, в кольце $\mathbb{F}_p[X]$ выполняется равенство

$$s(X)(X^r - 1) = (q(X))^p.$$

Заметим, что многочлен $X^r - 1 \in \mathbb{F}_p[X]$ не имеет кратных корней в его поле разложения. Действительно, его производная равна rX^{r-1}, а согласно условию $o_r(p) > 1$ и, следовательно, НОД$(r, p) = 1$. Поэтому $r \neq 0$ в кольце $\mathbb{Z}_p$, и равенство rX^{r-1} возможно только при $X = 0$. Но $X = 0$ не является корнем многочлена $X^r - 1$, что и означает простоту его корней. Тогда из теоремы единственности разложения на множители в кольце многочленов $\mathbb{F}_p[X]$ следует, что многочлен $q(X)$ делится на многочлен $X^r - 1$, т. е. $q(X) = q_1(X)(X^r - 1)$. Следовательно, в кольце $\mathbb{F}_p[X]$ выполняется равенство

$$(X + a)^{n/p} - X^{n/p} - a = q(X) = q_1(X)(X^r - 1),$$

т. е. выполняется равенство

$$(X + a)^{n/p} - X^{n/p} - a = q_1(X)(X^r - 1) \equiv 0 \ (\text{mod } X^r - 1, p).$$

□

Определение 2.5.5. *Для полинома $f(X)$ натуральное число m* ***принадлежит*** *множеству $I[f(X)]$, если*

$$f(X)^m = f(X^m) \ (\text{mod } X^r - 1, p).$$

Лемма 4. *Множество $I[f(X)]$ замкнуто относительно умножения. Если $m_1,\ m_2 \in I[f(X)]$, то $m_1 \cdot m_2 \in I[f(X)]$.*

Доказательство. Поскольку $m_1 \in I[f(X)]$, то

$$[f(X)]^{m_1 \cdot m_2} \equiv [f(X^{m_1})]^{m_2} \pmod{X^r - 1, p}.$$

Поскольку $m_2 \in I[f(X)]$, то заменяя X на X^{m_1}, имеем

$$[f(X^{m_1})]^{m_2} \equiv f(X^{m_1 \cdot m_2}) \pmod{X^{m_1 r} - 1, p} \equiv$$
$$\equiv f(X^{m_1 \cdot m_2}) \pmod{X^r - 1, p},$$

поскольку $X^r - 1$ является делителем многочлена $X^{m \cdot r} - 1$.

Из этих двух соотношений получаем

$$[f(X)]^{m_1 \cdot m_2} \equiv f(X^{m_1 \cdot m_2}) \pmod{X^r - 1, p}.$$

□

Лемма 5. *Если* $m \in I[f(X)]$ *и* $m \in I[g(X)]$, *то*

$$m \in I[f(X) \cdot g(X)].$$

Доказательство. Имеем

$$[f(X) \cdot g(X)]^m = [f(X)]^m \cdot [g(X)]^m = \\ = f(X^m) \cdot g(X^m) \pmod{X^r - 1, p}.$$

Определим два множества, играющие ключевую роль в доказательстве корректности алгоритма:

$$I = \left\{ \left(\frac{n}{p} \right)^i \cdot p^j \mid i, j \geq 0 \right\},$$

$$P = \left\{ \prod_{a=0}^{l} (X + a)^{e_a} \mid e_a \geq 0 \right\}.$$

□

Простым следствием лемм 4 и 5 является

Лемма 6. *Для любого* $m \in I$ *выполнено* $m \in I[P]$.

Определим теперь две группы, связанные с введенными выше двумя множествами. Пусть G обозначает мультипликативную группу всех вычетов чисел из I по модулю r. Тогда G является подгруппой мультипликативной группы Z_r^*, поскольку, как отмечено выше, НОД$(n, r) =$ НОД$(p, r) = 1$. Пусть $t = |G|$ — число элементов группы G. Группа G порождается элементами n и p по модулю r и, поскольку, $o_r(n) > \log^2 n$, то $t > \log^2 n$.

Воспользуемся далее некоторыми известными фактами из теории конечных полей.

Факт 1. Мультипликативная группа любого конечного поля циклическая.

Факт 2. Для любого поля F существует его алгебраическое замыкание $\overline{F}$.

Факт 3. Рассмотрим расширение поля $\mathbb{F}_p$, полученное присоединением всех корней многочлена $X^r - 1$. Имеем $\mathbb{F}_p \subset \mathbb{F}_p(\alpha_1, \ \ldots, \alpha_r) \subset \overline{\mathbb{F}_p}$.

Факт 4. Возьмем мультипликативную подгруппу расширенного поля, состоящую из корней многочлена $X^r - 1$. Эта группа циклическая (из факта 1, как подгруппа циклической группы). Она содержит примитивный элемент α (r-й корень из единицы, порождающий всю циклическую группу). Тогда $\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) = F$.

Возьмем минимальный многочлен элемента α над полем $\mathbb{F}_p$ и обозначим его $h(X)$. Этот многочлен неприводим в $F_p[X]$ и имеет степень $o_r(p)$ (см. [ЛН88]). Такой многочлен всегда существует, если НОД$(p, r) = 1$, причем его степень $o_r(p) > 1$. Пусть H обозначает множество всех вычетов многочленов из P по модулю $h(X)$ и p.

Упражнение 2.5.4. Доказать, что фактор-множество H является группой.

Группа H порождается элементами $X, X+1, X+2,$ ..., $X+l$ в поле $F = \mathbb{F}_p[X]/(h(X))$ и является подгруппой мультипликативной группы поля F.

Следующие две леммы дают нижнюю и верхнюю оценку размера группы H.

Лемма 7. $|H| \geq \binom{t+l}{t-1}$.

Доказательство. Заметим сначала, что X — примитивный r-й корень из единицы в F (см. факт 4 выше).

Покажем теперь, что любые два различных многочлена в множестве P степени меньше, чем t, соответствуют различным элементам H. Пусть $f(X)$ и $g(X)$ — такие многочлены из P. Предположим $f(X) = g(X)$ в поле F, и пусть $m \in I$. Имеем $[f(X)]^m = [g(X)]^m$ в F. Поскольку $m \in I[f]$, $m \in I[g]$, и $h(X)$ является делителем $X^r - 1$, получаем, что в поле F выполнено

$$f(X^m) = g(X^m).$$

Отсюда вытекает, что X^m является корнем многочлена $Q(Y) = f(Y) - g(Y)$ для любого $m \in G$. Поскольку НОД$(m, r) = 1$ (т.к. G — подгруппа Z_r^*), любое такое X^m является примитивным r-м корнем из единицы. Следовательно, должно быть $|G| = t$ различных корней многочлена $Q(Y)$ в поле F. Однако степень $Q(Y)$ меньше t в силу выбора f и g. Это противоречие доказывает, что $f(X) \neq g(X)$ в F.

Заметим, что $i \neq j$ в F_p для $1 \leq i \neq j \leq l$, поскольку $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor < \sqrt{r} \log n < r$, и $p > r$.

Значит все элементы X, $X + 1$, $X + 2$, ..., $X + l$ различны в поле F. Также, поскольку степень h больше единицы, $X + a \neq 0$ в F для всех a, $0 \leq a \leq l$. Значит, существует не менее $l + 1$ различных полиномов первой степени в H. Отсюда вытекает, что существует не менее $\binom{t+l}{t-1}$ различных полиномов степени $< t$ в H. □

Лемма 8. *Если n не является степенью p, то*

$$|H| \leq n^{\sqrt{t}}.$$

Доказательство. Рассмотрим следующее подмножество множества I:

$$I_1 = \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \;\middle|\; 0 \leq i, j \leq \left\lfloor \sqrt{t} \right\rfloor \right\}.$$

Если n не является степенью простого числа, то

$$|I_1| = (\lfloor \sqrt{t} \rfloor + 1)^2 > t.$$

Поскольку $|G| = t$, по крайней мере два числа из I_1 должны быть равны по модулю r. Пусть это будут m_1 и m_2 и $m_1 > m_2$. Имеем

$$X^{m_1} = X^{m_2} \ (\text{mod } X^r - 1).$$

Пусть $f(X) \in P$. Тогда

$$\begin{aligned} [f(X)]^{m_1} &= f(X^{m_1}) \ (\text{mod } X^r - 1, p) = \\ &= f(X^{m_2}) \ (\text{mod } X^r - 1, p) = \\ &= [f(X)]^{m_2} \ (\text{mod } X^r - 1, p). \end{aligned}$$

Отсюда вытекает, что в поле F

$$[f(X)]^{m_1} = [f(X)]^{m_2}.$$

Следовательно, $f(X) \in H$ является корнем многочлена $Q_1(Y) = Y^{m_1} - Y^{m_2}$ в поле F. Поскольку $f(X)$ — произвольный элемент H, многочлен $Q_1(Y)$ имеет не менее $|H|$ различных корней в поле F. Однако степень многочлена $Q_1(Y)$ равна

$$m_1 \leq \left(\frac{n}{p} \cdot p\right)^{\lfloor\sqrt{t}\rfloor} \leq n^{\lfloor\sqrt{t}\rfloor}.$$

Это доказывает, что $|H| \leq n^{\lfloor\sqrt{t}\rfloor}$. □

Завершающей является лемма, основанная на сравнении нижней и верхней оценок из лемм 7 и 8.

Лемма 9. *Если алгоритм выдает ПРОСТОЕ, то n является простым числом.*

Доказательство. Предположим алгоритм выдает ПРОСТОЕ. Из леммы 7 вытекает, что для $t = |G|$ и $l = \lfloor\sqrt{\varphi(r)}\log n\rfloor$:

$$\begin{aligned}
|H| \geq \binom{t+l}{t-1} &= \frac{1}{(l+1)!} \cdot t \cdot \ \ldots \cdot (t+l) \geq \\
&\geq \frac{1}{(l+1)!} \cdot (\lfloor\sqrt{t}\log n\rfloor + 1) \cdot \ \ldots \cdot (\lfloor\sqrt{t}\log n\rfloor + l + 1) \\
&\qquad (\text{ поскольку } t > \sqrt{t}\log n) = \\
&= \binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{\lfloor\sqrt{t}\log n\rfloor} \geq \binom{2\lfloor\sqrt{t}\log n\rfloor + 1}{\lfloor\sqrt{t}\log n\rfloor} \\
&\qquad (\text{ поскольку } l = \lfloor\sqrt{\varphi(r)}\log n\rfloor \geq \lfloor\sqrt{t}\log n\rfloor) > \\
&> 2^{\lfloor\sqrt{t}\log n\rfloor + 1} \geq n^{\sqrt{t}},
\end{aligned}$$

поскольку $\lfloor\sqrt{t}\log n\rfloor > \lfloor\log^2 n\rfloor \geq 1$) и $\binom{2m+1}{m} > 2^{m+1}$ при $m \geq 1$.

По лемме 8 $|H| \leq n^{\sqrt{t}}$, если n не степень p. Следовательно, $n = p^k$ для некоторого $k > 0$. Если $k > 1$, то алгоритм выдаст 0 на шаге 1. Значит, $n = p$. □

Окончательно получаем следующую теорему.

Теорема 8. *Алгоритм выдает ПРОСТОЕ* $\Longleftrightarrow$ n *— простое.*

Глава 3

Алгоритмические аспекты теории решеток и их применение в криптографии

3.1 Кратчайший ненулевой вектор решетки. Ближайший вектор к заданному вектору решетки. Приближенные алгоритмы. Алгоритм Ловаса

Цель настоящей лекции — рассказать об LLL-алгоритме (Lenstra, Lenstra, Lovasz) нахождения в произвольной решетке L в Z^n приведенного базиса с детерминантом $\leq 2^{n(n-1)/4}(\det(\Lambda))^{1/n}$. В качестве следствия из него получается алгоритм нахождения в произвольной решетке L вектора длины не более $2^{(n-1)/4}sh(L)$.

Метод приведения базиса позволяет получать оценки в важной задаче отыскания короткого ненулевого вектора в решетке. Вопрос о нахождении короткого вектора в решетке был сформулирован еще Дирихле в 1842 г. в форме проблемы совместных диофантовых приближениях. Теорема Минковского о выпуклом центрально симметричном теле (1896 г.) также дает оценку длины кратчайшего ненулевого вектора. Для случая евклидо-

вой нормы, когда выпуклое тело является сферой, она дает оценку длины кратчайшего вектора вида $sh(\Lambda) \leq c\sqrt{n}(\det(\Lambda))^{1/n}$, $\det(\Lambda)$ — детерминант решетки Λ. Доказательства теорем Дирихле и Минковского являются неконструктивными и не дают никаких способов построения коротких векторов в решетке.

Кратчайший вектор приведенного базиса позволяет получить оценку длины короткого ненулевого вектора вида

$$||b|| \leq 2^{(n-1)/4}(det(\Lambda))^{1/n}.$$

К настоящему времени сложностной статус задачи поиска кратчайшего вектора в решетке SVP (shortest vector problem) установлен в смысле доказательства ее $\mathcal{NP}$-полноты. Не совсем ясно обстоит дело с эффективными приближенными алгоритмами. Более исследована близкая задача CVP (closest vector problem), нахождения для заданной решетки и вектора a ближайшего к нему вектора решетки b, т. е. минимизирующего $||b - a||$. Ее $\mathcal{NP}$-полнота была доказана еще в 1981 г.

3.1.1 Некоторые задачи на решетках

Последовательные минимумы могут определятся относительно любой нормы.

Через $sh(\Lambda)$ будем обозначать длину кратчайшего ненулевого вектора решетки Λ. Очевидно, что $sh(\Lambda) = \lambda_1$. В качестве следствия второй теоремы Минковского выше была получена оценка сверху для кратчайшего вектора решетки вектора

$$\lambda_1 \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{det(\Lambda)}.$$

Оценка снизу для кратчайшего вектора решетки дается следующей теоремой.

Теорема. Пусть B — базис решетки и B^* — соответствующий ортогональный базис, полученный с помощью процедуры ортогонализации Грамма-Шмидта. Тогда

$$\lambda_1 \geq \min_j \|b_j^*\| > 0.$$

Задача. Докажите эту теорему. **Указание.** Докажите, что для целочисленного вектора x выполняется неравенство

$$\|Bx\| \geq \|b_i\|, \text{ где } i = \max\{i|x_i \neq 0\}.$$

В настоящее время неизвестен ни один полиномиальный алгоритм нахождения кратчайшего вектора в решетке. Задачу нахождения кратчайшего вектора в решетке будем именовать SVP (Shortest Vector Problem). Более того, не известен ни один такой алгоритм для получения такого вектора в границах, заданных оценкой Минковского

$$Bx \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{det(\Lambda)},$$

или даже более грубой оценкой

$$Bx < n^c \cdot \sqrt[n]{det(\Lambda)}.$$

Другой важной задачей на решетках является задача нахождения ближайшего вектора CVP (Closest Vector Problem).

Соответственно могут рассматриваться три следующие задачи для CVP и SVP:

- Задача поиска ближайшего или наикратчайшего вектора решетки.
- Задача определения минимума расстояния до ближайшего вектора или длины наикратчайшего вектора решетки.
- Задача проверки: для заданного рационального $r > 0$, определить, существует ли вектор решетки, находящийся на расстоянии не более r или имеющий длину не более r.

3.1.2 Алгоритм Гаусса

Вначале исследуем двумерные решетки.

Определение 1. Пусть a, b — базис решетки. Этот базис называется приведенным относительно нормы $\|\cdot\|$, если выполняются неравенства

$$\|a\|, \|b\| \leq \|a + b\|, \|a - b\|.$$

Лемма 1. Рассмотрим три точки на прямой: x, $x+y$ и $x+\alpha y$, где $\alpha \in (1,\infty)$. Для любой нормы $\|\cdot\|$ из неравенства $\|x\| \le \|x+y\|$ следует, что $\|x+y\| \le \|x+\alpha y\|$, а из неравенства $\|x\| < \|x+y\|$ следует, что $\|x+y\| < \|x+\alpha y\|$.

Доказательство. Положим $\delta = 1/\alpha$. Тогда

$$x+y = (1-\delta)x + \delta(x+\alpha y).$$

Тогда согласно неравенству треугольника имеем

$$\|x+y = \|(1-\delta)\|x\| + \delta\|x+\alpha y\|.$$

Поскольку при $\|x\| < \|x+y\|$ выполняется неравенство

$$(1-\delta)\|x\| + \delta\|x+\alpha y\| < (1-\delta)\|x+y\| + \delta\|x+\alpha y\|,$$

то, комбинируя полученные неравенства, получаем

$$\|x+y\| < (1-\delta)\|x+y\| + \delta\|x+\alpha y\|.$$

Преобразуя последнее неравенство, получаем

$$\delta\|x+y\| < \delta\|x+\alpha y\|.$$

Поскольку $\delta > 0$, из полученного неравенства следует, что $|x+y\| < \|x+\alpha y\|$.

Следующая теорема дает простой критерий проверки минимальности базиса.

Теорема 1. Пусть a, b — базис решетки и λ_1, λ_2 последовательные минимумы решетки. Тогда базис a, b приведен в том и только том случае, если нормы векторов a и b равны значениям λ_1 и λ_2 соответственно.

Доказательство. Достаточность. Пусть $\|a\| = \lambda_1$ и $\|b\| = \lambda_2$. Без ограничения общности можно считать, что $\|a\| \le \|b\|$. Пусть базис не является приведенным. Тогда выполняется одно из двух неравенств $\|a \pm b\| < \|b\|$. Тогда для одного из базисов $(a, a \pm b)$ выполняется неравенство $\|a \pm b\| < \lambda_2$, противоречащее определению последовательных минимумов решетки.

Необходимость. Пусть базис приведен.

Определение 2. Базис называется a, b вполне упорядоченным, если выполняются неравенства $\|a\| \le \|a - b\| < \|b\|$.

Обобщенный алгоритм Гаусса:

$$\textbf{if } \|a\| > \|b\| \textbf{ then } (a, b) := (b, a)$$

$$\textbf{if } \|a - b\| > \|a + b\| \textbf{ then } b := -b$$

$$\textbf{if } \|b\| \le \|a - b\| \textbf{ then return}(a, b)$$

$$\textbf{if } \|a\| \le \|a - b\| \textbf{ then go to}(loop)$$

$$\textbf{if } \|a\| = \|b\| \textbf{ then return } (a, a - b)$$

$$\textbf{let } (a, b) := (b - a, b)$$

(loop):

$$\mu \in \mathbb{Z} | \ \|b - \mu a\| \le \|b - \mu' a\| \ \forall \mu' \in \mathbb{Z}$$

$$(a, b) := (a, b - \mu a,)$$

$$\textbf{if } \|a - b\| > \|a + b\| \textbf{ then let } b := -b$$

$$(a, b) := (b, a)$$

$$\textbf{if } (a, b) \textit{ приведенный } \textbf{then return } (a, b) \textbf{ else go to } (loop)$$

Отметим, что при первом обращении к циклу (loop) базис всегда вполне упорядочен. Необходимо убедиться, что после окончания каждого цикла базис остается вполне упорядоченным или определяется приведенный базис).

Сначала опишем эффективную процедуру нахождения значения μ, при котором значение $\|b - \mu a\|$ минимально.

Лемма 2. Пусть $\| \cdot \|$ — эффективно вычисляемая норма и векторы a, b таковы, что $\|b\| > \|b - a\|$. Тогда можно эффективно определить целое число μ, для которого значение $\|b - \mu a\|$ минимально. Более того, число μ удовлетворяет неравенствам $1 \le \mu \le \lceil 2\|b\|/\|a\| \rceil$.

Доказательство. Положим $c = \lceil 2\|b\|/\|a\| \rceil$. Тогда согласно неравенству треугольника

$$\|b - ca\| \ge c\|a\| - \|b\| \ge \|b\|,$$

и, следовательно, по лемме 1 выполняется неравенство $\|b - ca\| \le \|b - (c+1)a\|$. Заметим, что согласно условию леммы последнее неравенство не выполняется при $c = 0$. Используя процедуру бинарного поиска, находим эффективно на отрезке $[1, c]$ такое целое число μ, являющееся локальным минимумом для функции $\|b - \mu a\|$, для которого

$$\|b - (\mu - 1)a\| > \|b - \mu a\| \le \|b - (\mu + 1)a\|.$$

Тогда по лемме 1 для всех $k \ge \mu + 1$ выполняются неравенства

$$\|b - \mu a\| \le \|b - (\mu + 1)a\| \le \|b - ka\|.$$

Аналогично, при $k \le \mu - 1$ выполняются неравенства

$$\|b - \mu a\| < \|b - (\mu - 1)a\| \le \|b - ka\|.$$

Лемма 3. В начале каждого цикла итераций в алгоритме Гаусса базис (a, b) вполне упорядочен.

Доказательство. На первом цикле утверждение очевидно. После нахождения числа μ получаем два вектора $a' = \pm(b - \mu a)$ и $b' = a$. После второго шага итерации выполняется неравенство $\|a' - b'\| \le \|a' + b'\|$. Согласно определению μ выполняются соотношения

$$\|a' + b'\| \ge \|a' - b'\| = \| \pm \|(b - \mu a) - a\| = \|b - (\mu \pm 1)a)\| \ge \|a'\|.$$

Если $\|b'\| \le \|a' - b'\|$, то базис (a', b') приведен. В противном случае $\|b'\| > \|a' - b'\| \ge \|a'\|$ и базис (a', b') вполне упорядочен.

Теорема 2. Алгоритм Гаусса заканчивает работу за конечное число шагов. Число итераций в алгоритме Гаусса для базиса (a, b) не превосходит $2 + \log_2(\|a\| + \|b\|)$.

Пусть k — число итераций в алгоритме Гаусса и (a_k, a_{k+1}) вполне упорядоченный базис в начале первой итерации. На каждой из итераций получаем вполне упорядоченный базис (a_i, a_{i+1}), до тех пор пока не получим приведенный базис (a_1, a_2). Тогда справедлива следующая

Лемма 4. При $i \ge 3$ выполняется неравенство $\|a_i\| < \frac{1}{2}\|a_{i+1}\|$.

Доказательство. Рассмотрим последовательность векторов $(a_{i-1}, a_i, a_{i+1}) = (a, b, c)$. Тогда выполняются неравенства $\|a\| < \|b\| < \|c\|$ и при некотором целом $\mu > 1$ и $\varepsilon = \pm 1$ выполняется равенство $a = \varepsilon(c - \mu b)$. Тогда $c = \varepsilon a + \mu b$. Докажем, что $\|c\| > 2\|b\|$.

- Пусть $\mu = 1$. Тогда выполняется неравенство $\|c - b\| = \|a\| < \|b\|$, противоречащее вполне упорядоченности базиса (a, b). Следовательно, $\mu \neq 1$.

- Пусть $\varepsilon = -1$, $\mu = 2$. Тогда $\|c-b\| = \|-a+b\|$. Поскольку базис (a, b) вполне упорядочен, выполняется неравенство $\|a - b\| < \|b\|$ и, следовательно, $\|c-b\| < \|b\| < \|c\|$, что противоречит упорядоченности базиса (b, c).

- Пусть $\varepsilon = -1$, $\mu > 2$. Тогда, учитывая неравенство $\|a\| < \|b\|$, получим

$$\|c\| = \| - a + \mu b\| \geq \mu\|b\| - \|a\| > \mu\|b\| - \|b\| = (\mu - 1)\|b\| \geq 2\|b\|.$$

- Пусть $\varepsilon = 1$, $\mu \geq 2$. Поскольку базис (a, b) вполне упорядочен, выполняется неравенство $\|b - a\| < \|b\|$. Тогда, по лемме 1, выполняется неравенство $\|b\| < +a\|$, а из упорядоченности базиса (a, b) следует неравенство $\|a\| \leq \|b-a\|$. Поэтому $\|a\| < \|b+a\|$, и, следовательно, используя лемму 1, получим

$$\|a\| \leq \|a + b\| < \|a + 2b\| \leq \|a + \mu b\| = \|c\|.$$

  Итак, доказано неравенство $\|c\| = \|a + \mu b\| \geq \|2b + a\|$. Для доказательства леммы достаточно проверить выполнение неравенства $\|2b + a\| > 2\|b\|$.

  Используя неравенство $\|a - b\| < b$ (свойство упорядоченности базиса (a, b)), из неравенства треугольника получаем

$$\|2b - a\| \leq \|b\| + \|b - a\| < \|b\| + \|b\| = 2\|b\|.$$

  Воспользовавшись леммой 1, получаем

$$\|2b - a\| < \|2b\| = \|2b - a + a\| < \|2b - a + 2a\| = \|2b + a\|.$$

Лемма доказана.

Воспользовавшись леммой, получаем, что при $i \geq 3$ выполняется неравенство $\|a_i\| \geq 2^{i-3}\|a_3\|$. В частности, для любых базисных векторов a, b выполняется неравенство

$$2^{k-2} \leq 2^{k-2}\|a_3\| \leq \|a_{k+1}\| \leq \|a\| + \|b\|.$$

Следовательно, $k \leq 2 + \log_2(\|a\| + \|b\|)$.

Полученное неравенство доказывает теорему 2. Следовательно, для любой эффективно вычисляемой нормы $\|\cdot\|$ алгоритм Гаусса полиномиален относительно входов (a, b).

3.1.3 LLL-алгоритм

Вначале напомним процесс ортогонализации Грамма-Шмидта. Пусть $b_1, \ldots, b_n$ — базис. Тогда ортогональные векторы b_i^* определяются формулами

$$\begin{aligned} b_i^* &= b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \\ \mu_{i,j} &= \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}. \end{aligned}$$

Определение 1. Базис $B = (b_1, \ldots, b_n) \in \mathbb{R}^{m \times n}$ называется LLL-приведенным относительно параметра $\frac{1}{4} < \delta < 1$, если

1. $\mu_{ij} \leq 1/2$ при $i > j$, где μ_{ij} — коэффициенты Грамма-Шмидта,
2. для любой последовательной пары векторов b_i, b_{i+1} выполняется неравенство
$$\delta\|\pi_i(b_i)\|^2 \leq \|\pi_i(b_{i+1})\|^2,$$
где π_i — проекция на оболочку $\mathbf{span}(b_i^*, b_{i+1}^*, \ldots, b_n^*)$. Иначе это условие задается соотношением
$$\delta\|b_i^*\|^2 \leq \|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 = \|b_{i+1}^*\|^2 + \mu_{i+1,i}^2 \|b_i^*\|^2.$$

При $\delta = 1$ получаем, что при $i = 1, \ldots, n-1$ двумерные базисы $(\pi_i(b_i), \pi_i(b_{i+1}))$ вполне приведенные.

Теорема 1. Пусть $b_1, \ldots, b_n$ — приведенный базис решетки L. Тогда

1. $\det L \le \prod_{i=1}^{n} \|b_i\| \le \left(\frac{4}{4\delta-1}\right)^{n(n-1)/4} \det L$,
2. $\|b_j\| \le \left(\frac{4}{4\delta-1}\right)^{(i-1)/2} \|b_i^*\|$ при $1 \le j \le i \le n$,
3. $\|b_1\| \le \left(\frac{4}{4\delta-1}\right)^{(n-1)/4} (\det L)^{1/n}$,
4. если $x \ne 0$ — элемент решетки, то $\|b_1\| \le \left(\frac{4}{4\delta-1}\right)^{(n-1)/2} \|x\|$,
5. если векторы решетки $x_1, \ldots, x_t$ — линейно независимы, то $\|b_j\| \le \left(\frac{4}{4\delta-1}\right)^{(n-1)/2} \max\{\|x_1\|, \ldots, \|x_t\|\}$ при $1 \le j \le t$.

Доказательство. Согласно определению приведенного базиса выполняется неравенство

$$\|b_{i+1}^*\|^2 \ge \left(\delta - \mu_{i+1,i}^2\right) \|b_i^*\|^2 \ge \left(\delta - \frac{1}{4}\right) \|b_i^*\|^2$$

для всех $1 \le i < n$. Следовательно, для всех $1 \le j \le i < n$ выполняется неравенства $\|b_j^*\| \le \left(\frac{4}{4\delta-1}\right)^{i+1-j} \|b_{i+1}^*\|^2$. Введем обозначение $\tau = \frac{4}{4\delta-1}$. Тогда ввиду ограничения на параметр δ, получаем, что $\tau > \frac{4}{3}$. Поэтому

$$\begin{aligned}
\|b_{i+1}\| &= \|b_{i+1}^*\|^2 + \sum_{j=1}^{i} \mu_{i+1,j} \|b_j^*\|^2 \\
&\le \|b_{i+1}^*\|^2 + \sum_{j=1}^{i} \frac{1}{4} \cdot \left(\frac{4}{4\delta-1}\right)^{i+1-j} \|b_{i+1}^*\|^2 \\
&= \|b_{i+1}^*\|^2 + \sum_{j=1}^{i} \frac{1}{4} \cdot \tau^{i+1-j} \|b_{i+1}^*\|^2 \\
&= \left(1 + \frac{1}{4}\tau \frac{\tau^i - 1}{\tau - 1}\right) \cdot \|b_{i+1}^*\|^2 \\
&\le \tau^i \cdot \|b_{i+1}^*\|^2,
\end{aligned}$$

т.к. $\left(1 + \frac{1}{4}\tau \frac{\tau^i - 1}{\tau - 1}\right) \le \tau^i$ при $\tau > \frac{4}{3}$.

Следовательно,

$$\|b_j\|^2 \le \tau^{j-1} \|b_j^*\|^2 \le \tau^{i-1} \|b_i^*\|^2$$

при $1 \le j \le i \le n$. Формула 2 теоремы доказана.

Из полученного неравенства выводим

$$\prod_{i=1}^{n} \|b_i\|^2 \le \prod_{i=1}^{n} \tau^{i-1} \prod_{i=1}^{n} \|b_i^*\| = \tau^{n(n-1)/2} \cdot (\det L)^2.$$

Поскольку первая половина неравенства 1 представляет собой, доказанное ранее неравенство Адамара, соотношение 1 доказано.

Для доказательства соотношения 3 воспользуемся соотношениями 2. Перемножая соотношения

$$\|b_1\| \le \tau^{\frac{i-1}{2}} \|b_i^*\|,$$

получим

$$\|b_1\|^n \le \prod_{i=1}^{n} \left(\tau^{\frac{i-1}{2}} \|b_i^*\| \right) = \tau^{\frac{n(n-1)}{4}} \cdot \det L.$$

Соотношение 3 доказано.

Докажем соотношение 4. Поскольку x — вектор решетки, имеют место разложения

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r_i' b_i^*,$$

причем все $r_k \in \mathbb{Z}$. Пусть k — максимальное целое, для которого $r_k \ne 0$. Тогда из определения процесса ортогонализации выполняется равенство $r_k = r_i'$, и в частности $\|r_k\| = \|r_i'\| \ge 1$. Воспользовавшись соотношением 3, получаем

$$\tau^{n-1}\|x\| \ge \tau^{n-1}\|r_i'\|^2\|b_i^*\|^2 \ge \tau^{i-1}\|b_i^*\|^2 \ge \|b_1\|^2.$$

Соотношение 4 доказано.

Докажем соотношение 5. Выразим векторы x_i через элементы базиса b_i

$$x_j = \sum_{i=1}^{n} r_{i,j} b_i, \;\; r_{i,j} \in \mathbb{Z}.$$

Для каждого j обозначим через $k(j)$ наибольшее целое число k, для которого $r_{k,j} \ne 0$. Перенумеруем векторы x_j так, чтобы $k(1) \le k(2) \le \;\; \ldots k(t)$.

Тогда для всех $1 \le j \le t$ выполняются неравенства $\|x_j\|^2 \ge \|b^*_{k(j)}\|^2$. Выполняется неравенство $j \le k(j)$ для всех $1 \le j \le t$, поскольку векторы $x_1, \ldots, x_t$ линейно независимы. Воспользовавшись этим неравенством и уже доказанным соотношением 2, получаем

$$\|b_j\|^2 \le \tau^{k(j)-1} \cdot \|b^*_{k(j)}\|^2 \le \tau^{n-1} \cdot \|b^*_{k(j)}\|^2 \le \tau^{n-1} \cdot \|x_j\|^2.$$

Утверждение 5 теоремы доказано.

Из утверждения 4 теоремы 1 получаем

Следствие 1. Если $B = (b_1, \ldots, b_n) \in \mathbb{R}^{m\times n}$ — δLLL-приведенный базис с $\delta \in (1/4, 1)$, то $\|b_1\| \le \left(2/\sqrt{4\delta - 1}\right)^{n-1} \lambda_1$. В частности, если $\delta = 1/4 + (3/4)^{n/(n-1)}$, то $\|b_1\| \le \left(2/\sqrt{3}\right)^n \lambda_1$.

LLL-алгоритм.

Вход: Базис решетки $B = (b_1, \ldots, b_n) \in \mathbb{Z}^{m\times n}$

Выход: LLL-приведенный базис решетки.

(loop):

for $i = 1, \ldots, n$
  for $j = i-1, \ldots, 1$
    $b_i := b_i - c_{i,j} b_j$ где $c_{i,j} = \lfloor (b_i, b_j)/(b_j, b_j) \rceil$
if $\delta \|\pi_i(b_i)\|^2 > \|\pi_i(b_{i+1})\|^2$ для некоторого i
then swap(b_i, b_{i+1}) **go to** (loop)
else B — выход

Отметим, что выполняемые в алгоритме преобразования переводят базис решетки в базис той же решетки. Поэтому, если алгоритм заканчивает работу, то в результате получается приведенный базис решетки. Поэтому , достаточно доказать, что алгоритм заканчивает выполнение за конечное число шагов и оценить их число, а также сложность выполнения каждого шага. Для этого введем несколько новых определений.

Определим числа целые d_i формулами

$$d_i = \begin{vmatrix} (b_1, b_1) & \cdots & (b_1, b_i) \\ \cdots & \cdots & \cdots \\ (b_i, b_1) & \cdots & (b_i, b_i) \end{vmatrix}.$$

Очевидно, числа d_i можно интерпретировать как квадраты детерминантов решеток $b_1, \ldots, b_i$ и, следовательно, выполняются равенства

$$d_i = \prod_{j=1}^{n} \|b_j^*\|^2.$$

В силу п.4 доказанной теоремы такая решетка содержит ненулевой вектор x, удовлетворяющий неравенству

$$\|x\|^2 \le \left(\frac{4}{4\delta - 1}\right)^{(i-1)/2} d_i^{1/i}.$$

Введем также обозначение

$$D = \prod_{j=1}^{n-1} d_i.$$

Заметим, что если в процессе выполнения алгоритма не выполняется перестановка векторов, то величины d_i, являющиеся детерминантами базисов соответствующих решеток не изменяется. Следовательно, и величина D в этом случае остается неизменной.

Рассмотрим теперь шаг алгоритма, на котором выполняется перестановка двух соседних элементов базиса. А именно, пусть векторы $b_1, \ldots, b_i$ определяют приведенный базис в решетке **span**$(b_1, \ldots, b_i)$, порожденной этими векторами. Пусть также векторы $b_1, \ldots, b_{i+1}$ представляют базис, для которого выполняется условие 1, но не выполняется условие 2 определения δLLL-приведенности. Тогда согласно **LLL**-алгоритму выполняется перестановка векторов b_i и b_{i+1}, т. е. выполняется переход к базису $\tilde{b}_1, \ldots, \tilde{b}_n$, в котором

$$\tilde{b}_k = \begin{cases} b_k & \text{при} \quad k \ne i,\ k \ne i+1 \\ b_{k+1} & \text{при} \quad k = i \\ b_{k-1} & \text{при} \quad k = i+1 \end{cases}$$

Посмотрим, как изменится при этом значение величины D. Отметим, что значения d_k при $k \ne i$ остаются неизменными, поскольку соответствующие решетки не меняются. Меняется только решетка из первых i элементов базиса. Запишем соответствующее преобразование базиса

$$(\tilde{b}_1, \ldots, \tilde{b}_i) = (b_1, \ldots, b_{i-1}, b_{i+1}).$$

Тогда при $0 < j < i$ выполняется

$$\tilde{b}_j^* = b_j^*$$

и

$$\tilde{\mu}_{i,j}^* = \frac{\tilde{b}_i, \tilde{b}_j^*)}{(\tilde{b}_j^*, \tilde{b}_j^*)} = \frac{b_{i+1}, \tilde{b}_j^*)}{(\tilde{b}_j^*, \tilde{b}_j^*)} = \mu_{i+1,j}.$$

Поэтому

$$\begin{aligned}\tilde{b}_i^* &= \tilde{b}_i - \sum_{j=1}^{i-1} \tilde{\mu}_{i,j} b_j^* = b_{i+1} - \sum_{j=1}^{i-1} \mu_{i+1,j} b_j^* \\ &= b_{i+1} - \sum_{j=1}^{i} \mu_{i+1,j} b_j^* + \mu_{i+1,i} b_i^* = b_{i+1}^* + \mu_{i+1,i} b_i^*,\end{aligned}$$

т. е. $\tilde{b}_i^* = b_{i+1}^* + \mu_{i+1,i} b_i^*$. Поскольку для пары векторов b_i и b_{i+1}, .

3.2 Результаты Айтаи о сложности поиска короткого вектора в случайной решетке

Цель настоящей лекции — дать формулировку результатов Айтаи о случайном классе решеток в Z^n, элементы которых порождаются с коротким вектором в нем, таком, что если имеется вероятностный алгоритм нахождения короткого вектора в случайной решетке из данного класса с вероятностью не менее $1/2$, тогда имеется также вероятностный алгоритм, решающий следующие три задачи в *любой* решетке в Z^n с вероятностью экспоненциально близкой к 1:

(P1) Найти длину кратчайшего ненулевого вектора в n-мерной решетке приближенно с точностью до полиномиального фактора (по n);

(P2) Найти кратчайший ненулевой вектор в n-мерной решетке L, в которой кратчайший вектор **v** единственный в том смысле, что любой другой вектор с длиной не более $n^c||\mathbf{v}||$, параллелен **v**, где c достаточно большая абсолютная константа;

(P3) Найти базис $\mathbf{b}_1, \ldots, \mathbf{b}_n$ в n-мерной решетке L, с длиной определенной как $\max_{i=1}^n ||\mathbf{b}_i||$, кратчайший с точностью до полиномиального фактора (по n).

Получены следующие следствия:

a) существует односторонняя функция;

b) для любого фиксированного $0 < \varepsilon < 1/2$ существует полиномиально вычислимая функция $r(m)$ с $m^{\varepsilon} \leq \log r(m) \leq m^{2\varepsilon}$ такая, что рандомизированная задача «СУММА ПОДМНОЖЕСТВ»:

$$\sum_{i=1}^{m} a_i x_i \equiv b \pmod{r(m)},$$

$x_i \in \{0, 1\}$, для $i = 1, \ldots, m$, не имеет вероятностного полиномиального алгоритма решения, где a_i, $i = 1, \ldots, m$, и b выбираются случайно и равномерно из интервала $[1, r(m)]$.

Напомним, некоторые результаты из теории решеток. Вопрос о нахождении короткого вектора в решетке был сформулирован еще Дирихле в 1842 г. в форме проблемы о совместных диофантовых приближениях. Теорема Минковского о выпуклом центрально симметричном теле (1896 г.) также дает оценку длины кратчайшего ненулевого вектора. Для случая евклидовой нормы, когда выпуклое тело является сферой, она дает оценку $sh(L) \leq c\sqrt{n}(\det L)^{1/n}$, $\det L$ — детерминант решеки L. Доказательства теорем Дирихле и Минковского являются неконструктивными и не дают никаких способов построения коротких векторов в решетке.

Определим сейчас случайный класс решеток, который мы будем рассматривать. Мы будем рассматривать решетки как векторы с целочисленными коэффициентами, более того вектора будут определены по модулю некоторого целого числа q, так что если векторы когруентны по модулю q, то они оба либо принадлежат решетке, либо оба не принадлежат.

Пусть набор векторов $\nu = [u_1, \ldots, u_m]$, где $u_i \in \mathbf{Z}^n$. Тогда $\Lambda(\nu, q)$ — определяется как решетка всех последовательностей целых $h_1, \ldots, h_m$ таких, что

$$\sum_{i=1}^{m} h_i u_i \equiv 0 \pmod{q}$$

Выбор параметров q и m осуществляется следующим образом. Они будут зависеть от двух абсолютных констант c_1, c_2. При заданном n положим $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$.

Определим теперь параметр λ в решетке $\Lambda(\lambda, q)$. Выберем случайные независимые векторы $v_1, \ldots, v_{m-1}$ равномерно на множестве всех векторов $(x_1, \ldots, x_n) \in \mathbf{Z}^n$, с $0 \leq x_i < q$. Независимо от этого случайного выбора выберем также последовательность случайных бит $\delta_1, \ldots, \delta_{m-1}$, где каждое δ_i выбирается случайно и равномерно из множества $\{0, 1\}$.

Определим

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

с дополнительным ограничением, что каждая компонента v_m является целым числом из интервала $[0, q-1]$.

Пусть $\lambda = (v_1, \ldots, v_m)$. Чтобы подчеркнуть зависимость λ от n, c_1, c_2 мы будем писать λ_{n,c_1,c_2}. По теореме Дирихле для достаточно больших c_1, всегда существует вектор короче, чем n.

Определение 3.2.1. *Если v — кратчайший ненулевой вектор в решетке $L \subseteq \mathbf{R}^n$, и $\alpha > 1$ то скажем, что v является α-единственным, если для любого $w \in L$, из неравенства $||w|| \leq \alpha||v||$ вытекает, что вектора v и w — параллельны.*

Теорема 9. *Существуют абсолютные константы c_1, c_2, c_3 такие, что верно следующее. Предположим, что имеется вероятностный полиномиальный алгоритм A, который, получая на вход случайную переменную λ_{n,c_1,c_2} с вероятностью не менее $1/2$ выдает ненулевой вектор решетки $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$ длины не более n. Тогда имеется также вероятностный алгоритм B со следующими свойствами. Если линейно независимые векторы $a_1, \ldots, a_n \in \mathbf{Z}^n$ даны как вход, то алгоритм B за время полиномиальное от $\sigma = \sum_{i=1}^n size(a_i)$, выдает $z, u, (d_1, \ldots, d_n)$ такие, что с вероятностью более $1 - 2^{-\sigma}$ выполнены три требования:*

(1.1) если v — кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то

$$z \leq ||v|| \leq n^{c_3} z;$$

(1.2) если v n^{c_3}-единственный кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то $u = v$ или $u = -v$;

(1.3) $d_1, \ldots, d_n$ является базисом, причем $\max_{i=1}^n ||d_i|| \leq n^{c_3} bl(L)$.

Односторонние функции. Определим одностороннюю функцию f следующим образом. Для любого натурального n определим $f = f^{(n)}$. Пусть $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$, c_1, c_2 — даны в теореме. Областью определения f будет множество всех последовательностей $v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}$, где каждое v_i, является n-мерным вектором $(x_1, \ldots, x_n) \in \mathbf{Z}^n$, причем $0 \le x_i < q$, и каждое δ_i есть 0 или 1.

Предположим теперь, что $x = (v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}) \in \mathrm{domain}(f)$. Положим

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

с дополнительным ограничением, что каждая компонента v_m является целым числом из интервала $[0, q-1]$. Теперь положим

$$f(x) = (v_1, \ldots, v_{m-1}, v_m).$$

Посмотрим выполнено ли определение односторонней функции. Предположим, что

$$y = (v_1, \ldots, v_m) = f(x),$$

где x — случайный элемент $\mathrm{domain}(f)$. Это означает, что y является случайной переменной λ_{n,c_1,c_2}. Следовательно, если есть алгоритм инвертирования f на y, то есть алгоритм, который находит x' такое, что $f(x') = y$, то этот алгоритм находит также короткий ненулевой вектор в $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$. Следовательно, из теоремы вытекает, что если хотя бы одна из трех проблем трудна в худшем случае (не имеет полиномиального вероятностного алгоритма), то f — односторонняя функция.

3.3 Алгоритмическая сложность задач нахождения короткого вектора в решетках

Цель настоящей лекции — дать формулировку результатов Айтаи о случайном классе решеток в Z^n, элементы которых порождаются с коротким вектором в нем, таком, что если имеется вероятностный алгоритм нахождения короткого вектора в случайной решетке из данного класса с веро-

ятностью не менее $1/2$, тогда имеется также вероятностный алгоритм, решающий следующие три задачи в *любой* решетке в Z^n с вероятностью экспоненциально близкой к 1:

(P1) Найти длину кратчайшего ненулевого вектора в n-мерной решетке приближенно с точностью до полиномиального фактора (по n);

(P2) Найти кратчайший ненулевой вектор в n-мерной решетке L, в которой кратчайший вектор **v** единственный в том смысле, что любой другой вектор с длиной не более $n^c||\mathbf{v}||$, параллелен **v**, где c достаточно большая абсолютная константа;

(P3) Найти базис $\mathbf{b}_1, \ldots, \mathbf{b}_n$ в n-мерной решетке L, с длиной определенной как $\max_{i=1}^{n} ||\mathbf{b}_i||$, кратчайший с точностью до полиномиального фактора (по n).

Получены следующие следствия:

a) существует односторонняя функция;

b) для любого фиксированного $0 < \varepsilon < 1/2$ существует полиномиально вычислимая функция $r(m)$ с $m^{\varepsilon} \leq \log r(m) \leq m^{2\varepsilon}$ такая, что рандомизированная задача «СУММА ПОДМНОЖЕСТВ»:

$$\sum_{i=1}^{m} a_i x_i \equiv b \pmod{r(m)},$$

$x_i \in \{0, 1\}$, для $i = 1, \ldots, m$, не имеет вероятностного полиномиального алгоритма решения, где a_i, $i = 1, \ldots, m$, и b выбираются случайно и равномерно из интервала $[1, r(m)]$.

Напомним, некоторые результаты из теории решеток. Вопрос о нахождении короткого вектора в решетке был сформулирован еще Дирихле в 1842 г. в форме проблемы о совместных диофантовых приближениях. Теорема Минковского о выпуклом центрально симметричном теле (1896 г.) также дает оценку длины кратчайшего ненулевого вектора. Для случая евклидовой нормы, когда выпуклое тело является сферой, она дает оценку $sh(L) \leq c\sqrt{n}(\det L)^{1/n}$, $\det L$ — детерминант решеки L. Доказательства теорем Дирихле и Минковского являются неконструктивными и не дают никаких способов построения коротких векторов в решетке.

Определим сейчас случайный класс решеток, который мы будем рассматривать. Мы будем рассматривать решетки как векторы с целочислен-

ными коэффициентами, более того вектора будут определены по модулю некоторого целого числа q, так что если векторы когруентны по модулю q, то они оба либо принадлежат решетке, либо оба не принадлежат.

Пусть набор векторов $\nu = [u_1, \ldots, u_m]$, где $u_i \in \mathbf{Z}^n$. Тогда $\Lambda(\nu, q)$ — определяется как решетка всех последовательностей целых $h_1, \ldots, h_m$ таких, что

$$\sum_{i=1}^{m} h_i u_i \equiv 0 \pmod{q}$$

Выбор параметров q и m осуществляется следующим образом. Они будут зависеть от двух абсолютных констант c_1, c_2. При заданном n положим $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$.

Определим теперь параметр λ в решетке $\Lambda(\lambda, q)$. Выберем случайные независимые векторы $v_1, \ldots, v_{m-1}$ равномерно на множестве всех векторов $(x_1, \ldots, x_n) \in \mathbf{Z}^n$, с $0 \leq x_i < q$. Независимо от этого случайного выбора выберем также последовательность случайных бит $\delta_1, \ldots, \delta_{m-1}$, где каждое δ_i выбирается случайно и равномерно из множества $\{0, 1\}$.

Определим

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

с дополнительным ограничением, что каждая компонента v_m является целым числом из интервала $[0, q-1]$.

Пусть $\lambda = (v_1, \ldots, v_m)$. Чтобы подчеркнуть зависимость λ от n, c_1, c_2 мы будем писать λ_{n,c_1,c_2}. По теореме Дирихле для достаточно больших c_1, всегда существует вектор короче, чем n.

Определение 3.3.1. *Если v — кратчайший ненулевой вектор в решетке $L \subseteq \mathbf{R}^n$, и $\alpha > 1$ то скажем, что v является α-единственным, если для любого $w \in L$, из неравенства $||w|| \leq \alpha||v||$ вытекает, что вектора v и w — параллельны.*

Теорема 10. *Существуют абсолютные константы c_1, c_2, c_3 такие, что верно следующее. Предположим, что имеется вероятностный полиномиальный алгоритм A, который, получая на вход случайную переменную*

λ_{n,c_1,c_2} с вероятностью не менее $1/2$ выдает ненулевой вектор решетки $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$ длины не более n. Тогда имеется также вероятностный алгоритм B со следующими свойствами. Если линейно независимые векторы $a_1, \ldots, a_n \in \mathbf{Z}^n$ даны как вход, то алгоритм B за время полиномиальное от $\sigma = \sum_{i=1}^{n} size(a_i)$, выдает $z, u, (d_1, \ldots, d_n)$ такие, что с вероятностью более $1 - 2^{-\sigma}$ выполнены три требования:

(1.1) если v — кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то

$$z \leq ||v|| \leq n^{c_3} z;$$

(1.2) если v n^{c_3}-единственный кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то $u = v$ или $u = -v$;

(1.3) $d_1, \ldots, d_n$ является базисом, причем $\max_{i=1}^{n} ||d_i|| \leq n^{c_3} bl(L)$.

Односторонние функции. Определим одностороннюю функцию f следующим образом. Для любого натурального n определим $f = f^{(n)}$. Пусть $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$, c_1, c_2 — даны в теореме. Областью определения f будет множество всех последовательностей $v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}$, где каждое v_i, является n-мерным вектором $(x_1, \ldots, x_n) \in \mathbf{Z}^n$, причем $0 \leq x_i < q$, и каждое δ_i есть 0 или 1.

Предположим теперь, что $x = (v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}) \in \mathrm{domain}(f)$. Положим

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

с дополнительным ограничением, что каждая компонента v_m является целым числом из интервала $[0, q-1]$. Теперь положим

$$f(x) = (v_1, \ldots, v_{m-1}, v_m).$$

Посмотрим выполнено ли определение односторонней функции. Предположим, что

$$y = (v_1, \ldots, v_m) = f(x),$$

где x — случайный элемент $\mathrm{domain}(f)$. Это означает, что y является случайной переменной λ_{n,c_1,c_2}. Следовательно, если есть алгоритм инвертирования f на y, то есть алгоритм, который находит x' такое, что $f(x') = y$,

то этот алгоритм находит также короткий ненулевой вектор в $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$. Следовательно, из теоремы вытекает, что если хотя бы одна из трех проблем трудна в худшем случае (не имеет полиномиального вероятностного алгоритма), то f — односторонняя функция.

Глава 4

Некоторые криптосистемы на решетках

4.1 NTRU

Рассмотрим кольцо $\mathbb{Z}[X]/(X^N-1)$. Элементы этого кольца можно отождествить с многочленами с целыми коэффициентами степени не выше $N-1$. Сложение определяется по-компонентно. Умножение задается формулой

$$\sum_{k=0}^{N-1} a_k X^k \sum_{k=0}^{N-1} b_k X^k = \sum_{k=0}^{N-1} \left(\sum_{i+j \equiv k \pmod N} a_i b_j \right) X^k.$$

Операции в кольце многочленов $\mathbb{Z}_q[X]/(X^N-1)$ определяются так же, как и в кольце $\mathbb{Z}[X]/(X^N-1)$ с той лишь разницей, что операции над коэффициентами выполняются в кольце $\mathbb{Z}_q$. В этом кольце имеется группа единиц.

Задача Если q — простое, то $\mathbb{Z}_q$ — поле, тогда многочлены $f(X) \in \mathbb{Z}_q[X]/(X^N-1)$, для которых НОД$(f(X), X^N-1) = 1$, лежат в группе единиц и обратный элемент можно найти с помощью алгоритма Евклида. Доказать, что этот алгоритм имеет сложность $\mathcal{O}(N^2 \log q)$.

Пусть теперь $q = p^t$, где p простое и многочлены $f(X) \in \mathbb{Z}_q[X]/(X^N-1)$ такие, что НОД$(f(X), X^N-1) = 1$. С помощью алгоритма Евклида най-

дем многочлены $u, v, c \in \mathbb{Z}_q[X]/(X^N - 1)$, для которых

$$u * f + v * (X^N - 1) = 1 - pc.$$

Поэтому $u * f = 1$ в $\mathbb{Z}_q[X]/(X^N - 1)$. Имеем также

$$\begin{aligned}
(1 + pc) * u * f &= 1 - p^2c^2 \\
(1 + p^2c^2) * (1 + pc) * u * f &= 1 - p^4c^4 \\
&\vdots \\
(1 + p^{2^{s-1}}c^{2^{s-1}}) * \ \ldots * (1 + p^2c^2) * (1 + pc) * u * f &= 1 - p^{2^s}c^{2^s}
\end{aligned}$$

в кольце $\mathbb{Z}[X]/(X^N - 1)$. При $2^s \geq t$ имеем

$$(1 + p^{2^{s-1}}c^{2^{s-1}}) * \ \ldots * (1 + p^2c^2) * (1 + pc) * u * f = 1 \mod q$$

и, следовательно,

$$f^{-1} = (1 + p^{2^{s-1}}c^{2^{s-1}}) * \ \ldots * (1 + p^2c^2) * (1 + pc) * u.$$

4.1.1 Описание NTRU-шифрования

Обозначения. В дальнейшем описании системы шифрования NTRU будут использоваться следующие обозначения:

- n — размерность кольца многочленов, используемого при шифровании.
- p — натуральное число, участвующее в процессе шифрования и дешифрования.
- q — натуральное число, участвующее в процессе шифрования и дешифрования, а также при определении открытого ключа.
- k — секретный параметр, от которого зависит стойкость относительно некоторого типа атак.
- d_1 — распределение коэффициентов многочлена f, составляющего часть секретного ключа.

- d_2 — распределение коэффициентов случайного многочлена g, участвующего при формировании открытого ключа.
- d_3 — количество коэффициентов, равных 1 и -1 в случайном многочлене g.
- f — многочлен в кольце $\mathbb{Z}[X]/(X^n - 1)$.
- f_p — приведенный многочлен f в кольце $\mathbb{Z}[X]/(p, X^n - 1)$.
- f_q — приведенный многочлен g в кольце $\mathbb{Z}[X]/(q, X^n - 1)$.
- $\mathcal{L}_1$ — множество многочленов в $\mathbb{Z}[X]/(X^n - 1)$ с распределением коэффициентов по закону d_1.
- g — многочлен в кольце $\mathbb{Z}[X]/(q, X^n - 1)$.
- $\mathcal{L}_2$ — множество многочленов в $\mathbb{Z}[X]/(X^n - 1)$ с распределением коэффициентов по закону d_2.
- $\mathcal{L}_3$ — множество многочленов в $\mathbb{Z}[X]/(X^n - 1)$ с распределением коэффициентов по закону d_3.
- f_p^{-1} — обратный к f_p в $\mathbb{Z}[X]/(p, X^n - 1)$.
- f_q^{-1} — обратный к f_q в $\mathbb{Z}[X]/(q, X^n - 1)$.
- h — открытый ключ, многочлен в $\mathbb{Z}[X]/(q, X^n - 1)$.
- r — случайный многочлен в $\mathbb{Z}[X]/(q, X^n - 1)$, используемый для шифрования.
- m — исходный текст, многочлен в $\mathbb{Z}[X]/(p, X^n - 1)$.
- e — шифртекст, многочлен в $\mathbb{Z}[X]/(q, X^n - 1)$.
- G — порождающая функция.
- H — хэш функция.

Элементы кольца $R = \mathbb{Z}[X]/(X^n - 1)$ будем представлять многочленом или вектором вида

$$f = \sum_{i=0}^{n-1} f_i X^i = [f_0, f_1, \ \ldots, f_{n-1}].$$

Произведение в этом кольце описывается формулой

$$f * g = [f_0, f_1, \ \ldots, f_{n-1}] * [g_0, g_1, \ \ldots, g_{n-1}] = [h_0, h_1, \ \ldots, h_{n-1}],$$

где

$$h_k = \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{n-1} f_i g_{n+k-i}.$$

В кольцах $R_p = R/(p)$ и $R_q = R/(q)$ коэффициенты многочленов представляются остатками в диапазонах $[0, p-1]$ и $[0, q-1]$.

Рассмотрим также множество многочленов $\mathcal{P}_p(N)$, элементы которого представляются в виде

$$g = \sum_{i=0}^{N-1} g_i X^i = [g_0, g_1, \ \ldots, g_{N-1}], \text{ где } g_p \in \left(-\frac{p}{2}, \frac{p}{2}\right].$$

Функции G и H определяют отображения

$$G : \mathcal{P}_p(N) \longrightarrow \mathcal{P}_p(N) \text{ и } H : \mathcal{P}_p(N) \times \mathcal{P}_p(N) \longrightarrow \mathcal{P}_p(K),$$

легко вычислимые, нелинейные и случайные. Стойкость NTRU-шифрования существенно зависит от выбора функций G, H и параметра k и оценивается величиной p^k.

Генерация ключа. Выбираем два случайных многочлена $f \in \mathcal{L}_1$ и $g \in \mathcal{L}_2$, причем для многочлена f существуют обратные элементы f_p^{-1} и f_q^{-1} в кольцах $R_p = R/(p)$ и $R_q = R/(q)$. С вероятностью близкой к единице случайный многочлен f удовлетворяет этому условию. Обратные элементы f_p^{-1} и f_q^{-1} строятся с помощью алгоритма Евклида.

Затем вычисляется многочлен h в $R_q = R/(q)$

$$h \equiv p f_q^{-1} * g \mod q.$$

Открытым ключом шифрования объявляется многочлен h и числа q и p. Секретным ключом является многочлен f.

Шифрование. Открытый текст m находится в множестве $\mathcal{P}_p(n-k)$. Выбирается случайный многочлен $r \in \mathcal{L}_3$. Зашифрованный текст e получается из по формуле

$$e \equiv r * h + [m + H(m, [r * h]_p)X^{n-k} + G([r * h]_p)]_p \mod q,$$

где $[a]_p \equiv a \mod p$ и $[a]_p \in \mathcal{P}_p(n-1)$.

Дешифрация. Пусть e — шифртекст и f — секретный ключ.

Сначала вычислим многочлен a по формуле

$$a \equiv f * e \mod q,$$

причем коэффициенты многочлена a находятся в интервале от $-q/2$ до $q/2$. Рассматривая многочлен a как многочлен с целыми коэффициентами, вычислим многочлен $t \in R_p$ по формуле

$$t = f_p^{-1} * a \mod p.$$

Далее вычисляем

$$b \equiv e - t \mod p \quad \text{и} \quad c \equiv t - G(b) \mod p,$$

а затем представляем c как

$$c = c' + c''X^{n-k}, \text{ где } \deg(c') < n-k \text{ и } \deg(c') < k.$$

Затем сравниваем c'' и $H(c', b)$. Если значения совпадают, то c' — результат дешифрации. Если эти значения не совпадают, то шифртекст считается недопустимым.

4.1.2 Выбор параметров.

Определим ширину элемента $f \in R$ формулой

$$|f|_\infty = \max_{0 \le i \le n-1} \{f_i\} - \min_{0 \le i \le n-1} \{f_i\}.$$

Норма определяется формулой

$$|f|_2 = \left(\sum_{i=0}^{n-1}(f_i - \bar{f})^2\right)^{1/2}, \text{ где } \bar{f} = \frac{1}{n}\sum_{i=0}^{n-1} f_i.$$

Предложение. Для любого $\varepsilon > 0$ существуют константы $\gamma_1, \gamma_2 > 0$, зависящие от ε и N, такие, что для случайно выбранных $f, g \in R$, с вероятностью большей $1 - \varepsilon$ выполняется неравенство

$$\gamma_1 |f|_2 |g|_2 \le |f * g|_\infty \le \gamma_2 |f|_2 |g|_2.$$

Пространство сообщений определяется как $\mathcal{L}_m = \mathcal{P}_p(n-k)$. Положим

$$\mathcal{L}(d_1, d_2) = \{f \in R : f_i \in \{-1, 0, 1\}, \sum_{i=0}^{n-1} |f_i| = d_1 + d_2, \sum_{i=0}^{n-1} f_i = d_1 - d_2.\}$$

Тогда

$$\mathcal{L}_1 = \mathcal{L}(d_1, d_1 - 1), \ \mathcal{L}_2 = \mathcal{L}(d_2, d_2), \ \mathcal{L}_3 = \mathcal{L}(d_3, d_3).$$

Тогда

$$|f|_2 = \sqrt{2d_1 - 1 - n^{-1}}, \ |g|_2 = \sqrt{2d_2}, \ |r|_2 = \sqrt{2d_3}.$$

Критерий существования дешифрации. Положим

$$m' = [m + H(m, [r * h]_p)X^{n-k} + G([r * h]_p)]_p \, .$$

Для однозначности процесса дешифрования должно выполняться условие

$$|f * m' + pr * g|_\infty < q/2.$$

Это выполняется при

$$|f * m'|_\infty \le q/4, \ |pr * g|_\infty < q/4.$$

Это выполнено в силу предложения при

$$|f|_2 |m|_2 \approx q/4\gamma_2, \quad |r|_2 |g|_2 \approx q/4\gamma_2.$$

Для $N = 167$ и $N = 503$ $\gamma_2 \approx 0.27$ и $\gamma_2 \approx 0.17$.

Если ширина $f * e$ больше $q/2$, приводим произведение в интервале $(0.q/2)$ или $(-q/2, 0)$.

Если ширина $f * e$ в некотором выбранном интервале не превосходит $q/2$, то имеются допустимые сдвиги интервала на величины $\pm q$. Выбор подходящего (допустимого) значения осуществляется с помощью проверки значения хэш-функции.

4.1.3 Дешифрование.

Дешифрация. Пусть e — шифртекст и f — секретный ключ.

Сначала вычислим многочлен a по формуле

$$a \equiv f * e \mod q,$$

причем коэффициенты многочлена a находятся в интервале от $-q/2$ до $q/2$. Рассматривая многочлен a как многочлен с целыми коэффициентами, вычислим многочлен $t \in R_p$ по формуле

$$t = f_p^{-1} * a \mod p.$$

Далее вычисляем

$$pr * g = a - f * t.$$

Тогда

$$r * h \equiv f_q^{-1} * (pr * g) \mod q.$$

Положим

$$b \equiv e - t \mod p \quad \text{и} \quad c \equiv t - G(b) \mod p,$$

а затем представляем c как

$$c = c' + c'' X^{n-k}, \text{ где } \deg(c') < n - k \text{ и } \deg(c') < k.$$

Затем сравниваем c'' и $H(c', b)$. Если значения совпадают, то c' — результат дешифрации. Если эти значения не совпадают, то шифртекст считается недопустимым.

4.1.4 Атаки.

Рассмотрим следующую матрицу размера $2n \times 2n$

$$\begin{pmatrix} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-1} \\ 0 & \alpha & \cdots & 0 & h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix}$$

Пусть решетка L порождается строками этой матрицы. Тогда вектор $\tau = (\alpha f, g)$ — элемент решетки L. Детерминант решетки равен $\det L = q^n \alpha^n$. Математическое ожидание размера наикратчайшего вектора решетки размерности N с детерминантом D находится с вероятностью близкой к единице в диапазоне

$$\left(D^{1/N} \sqrt{\frac{N}{2\pi e}}, D^{1/N} \sqrt{\frac{N}{\pi e}} \right).$$

Следовательно, в нашем случае ($N = 2n$ и $D = q^n \alpha^n$) ожидаемая длина наикратчайшего вектора больше (но не существенно) величины

$$s = \sqrt{\frac{n \alpha q}{\pi e}}.$$

Наибольший шанс определить вектор τ, с помощью алгоритмов нахождения минимальных элементов решетки, — максимизировать отношение $s/|\tau|_2$.

Глава 5

Обзор современных результатов по алгоритмическим аспектам теории решеток

Предметный указатель

Список иллюстраций

Список алгоритмов

Bibliography

[AKS02] M. Agrawal, N. Kayal, and N. Saxena. *PRIMES is in P*. English. 2002. URL: http://citeseer.ist.psu.edu/article/agrawal02primes.html.

[AKS04] M. Agrawal, N. Kayal, and N. Saxena. “PRIMES is in P”. English. In: *Annals of Mathematics* 160 (2004), pp. 781–793.

[ЛН88] Р. Лидл and Г. Нидеррайтер. *Конечные поля*. russian. М. Мир, 1988.