ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 3

ПРОСТЫЕ ЧИСЛА И РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ

Цель лекции	Обосновать свойства простых чисел, единственность разложения и алгоритмы пробных делений и решета Эратосфена.
Результат обучения	Доказывать простоту или составность небольших чисел; строить каноническое разложение; объяснять границы циклов и проверять полноту результата.
Предварительная подготовка	Делимость и деление с остатком; НОД, взаимная простота и тождество Безу из лекций 1–2.

Аудиторная нагрузка: 1 академический час. Основу занятия составляют определения, доказательства теорем и разбор решета. Подробный анализ алгоритмов и задачи раздела 7 предназначены также для самостоятельного изучения и практической работы.

План лекции

1. Простые и составные числа, наименьший делитель.
2. Бесконечность множества простых чисел.
3. Основная теорема арифметики.
4. Проверка простоты и факторизация пробными делениями.
5. Решето Эратосфена и его корректность.
6. Объём вычислений и связь с криптографией.
7. Следствия, задачи и контрольные вопросы.

1 Простые и составные числа

Простым называется целое число $p > 1$, имеющее ровно два положительных делителя: 1 и p. Целое число $n > 1$ называется **составным**, если оно не является простым. У составного числа есть делитель d, удовлетворяющий $1 < d < n$, поэтому $n = de$, где $1 < d, e < n$.

Число 1 не относится ни к простым, ни к составным: у него один положительный делитель. В этой лекции простота определяется только для положительных чисел, больших 1; ноль и отрицательные целые также не являются простыми или составными. Для разложения отрицательного целого сначала выделяют множитель -1, а затем раскладывают его модуль.

Начало последовательности простых чисел:

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.$$

Число 2 — единственное чётное простое. Любое чётное $n > 2$ имеет нетривиальный делитель 2. Обратное утверждение для нечётных чисел неверно: 9, 15 и 21 нечётные, но составные.

1.1 Наименьший делитель и граница квадратного корня

Лемма 1. У любого целого $n > 1$ существует простой делитель.

Доказательство. Среди положительных делителей n, больших 1, выберем наименьший d. Такое множество непусто, поскольку содержит n. Если d составное, то $d = uv$ при $1 < u < d$. Тогда $u \mid d$ и $d \mid n$, откуда $u \mid n$, что противоречит минимальности d. Следовательно, d простое.

Лемма 2. Если $n > 1$ составное, то у него есть простой делитель $p \le \sqrt{n}$.

Доказательство. Представим $n = uv$ при $1 < u \le v$. Из $u \le v$ следует $u^2 \le n$, то есть $u \le \sqrt{n}$. По лемме 1 число u имеет простой делитель p. Тогда $p \mid n$ и $p \le u \le \sqrt{n}$.

Следствие. Число $n > 1$ простое тогда и только тогда, когда ни одно простое $p \le \sqrt{n}$ не делит n. Граница включается: число $121 = 11^2$ было бы ошибочно признано простым при проверке только $p < 11$.

Например, $9^2 < 97 < 10^2$. Для доказательства простоты 97 достаточно проверить простые 2, 3, 5 и 7. Остатки равны соответственно 1, 1, 2 и 6, поэтому 97 простое.

1.2 Делитель произведения

Лемма Евклида. Если простое p делит произведение ab, то $p \mid a$ или $p \mid b$.

Доказательство. Если $p \mid a$, утверждение уже выполнено. Иначе $\gcd(p, a) = 1$, поскольку у p нет положительных делителей, кроме 1 и p. По тождеству Безу существуют целые s, t с $ps + at = 1$. Умножим это равенство на b:

$$pbs + abt = b.$$

Оба слагаемых слева делятся на p, поэтому $p \mid b$. Последовательное применение леммы показывает: если простое делит произведение нескольких целых чисел, оно делит хотя бы один сомножитель.

Для составного делителя вывод может быть неверен: $6 \mid 2 \cdot 3$, но $6 \nmid 2$ и $6 \nmid 3$. Простота делителя — существенная гипотеза леммы.

2 Бесконечность множества простых чисел

Теорема Евклида. Простых чисел бесконечно много.

Доказательство от противного. Предположим, что все простые исчерпываются конечным списком $p_1, \dots, p_k$. Построим число

$$Q = p_1 p_2 \cdots p_k + 1.$$

По лемме 1 у $Q > 1$ есть простой делитель q. Если q совпадает с одним из p_i, он делит и Q, и произведение $p_1 \cdots p_k$. Тогда он делит их разность 1, что невозможно для простого числа. Значит, существует простой делитель, не входящий в предполагаемый полный список. Получено противоречие.

В доказательстве не утверждается, что само число Q обязательно простое. Например,

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

Здесь простые множители 59 и 509 отсутствуют в исходном списке. Для доказательства бесконечности достаточно существования нового простого делителя; формула «произведение плюс один» не является гарантированным генератором простых чисел.

Бесконечность множества простых совместима с наличием сколь угодно длинных промежутков составных чисел. Для заданного $m \geq 1$ числа

$$(m+1)!+2,\ (m+1)!+3,\ \ldots,\ (m+1)!+(m+1)$$

образуют m последовательных составных чисел: число $(m+1)!+j$ делится на j при $2 \leq j \leq m+1$ и больше j.

3 Основная теорема арифметики

Теорема. Любое целое число $n > 1$ представимо в виде произведения простых множителей. Такое представление единственно с точностью до перестановки сомножителей.

3.1 Существование разложения

Применим сильную индукцию по n. Для $n = 2$ утверждение очевидно. Предположим, что оно выполнено для всех целых от 2 до $n-1$. Если n простое, оно само является произведением из одного простого множителя. Если n составное, то $n = ab$ при $1 < a, b < n$. По предположению индукции a и b раскладываются на простые множители; объединяя эти разложения, получаем разложение n.

Существование разложения объясняет, почему процесс деления на простые множители может закончиться полным результатом. Оно само по себе ещё не означает, что такой результат единственен.

3.2 Единственность разложения

Пусть получены два представления

$$n = p_1 \cdots p_r = q_1 \cdots q_s,$$

в которых все множители простые. Число p_1 делит правую часть, поэтому по лемме Евклида оно делит некоторый q_j. Простота q_j даёт $p_1 = q_j$. Переставим множители так, чтобы совпавшие простые стояли первыми, и сократим их. Повторяем рассуждение для оставшихся произведений.

Нельзя исчерпать множители только с одной стороны: тогда с другой стороны осталось бы непустое произведение простых, равное 1. Следовательно, $r = s$, и после перестановки множители совпадают попарно.

Собрав одинаковые множители, получаем **каноническое разложение**:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \qquad p_1 < \cdots < p_k, \qquad \alpha_i \in \mathbb{N}.$$

Например, $360 = 2^3 \cdot 3^2 \cdot 5$. Число 1 удобно рассматривать как пустое произведение простых, равное 1. Включение единицы в множество простых позволило бы произвольно добавлять множители 1 и нарушило бы формулировку единственности.

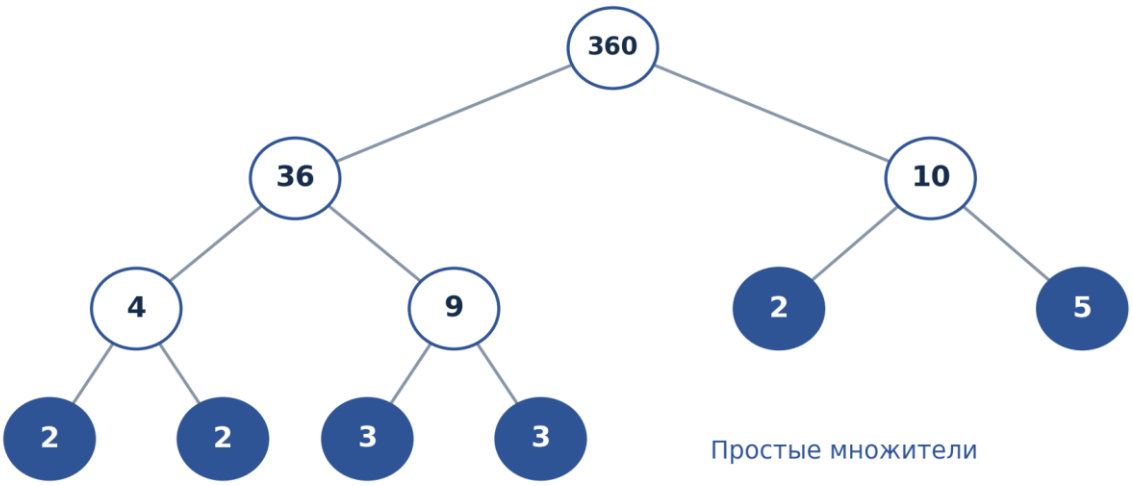


Рисунок 1. Промежуточные составные множители могут различаться, но набор простых листьев остаётся тем же.

3.3 Проверка полноты и следствия

Чтобы проверить предложенное разложение, нужны три условия: все основания простые, показатели — положительные целые и произведение степеней равно исходному числу. Одного совпадения произведения недостаточно: запись $360 = 4 \cdot 9 \cdot 10$ верна, но не является разложением на простые множители.

Если разложения a и b известны, добавим нулевые показатели для отсутствующих простых. Тогда

$$\gcd(a,b) = \prod_p p^{\min(\alpha_p,\beta_p)}, \qquad \operatorname{lcm}(a,b) = \prod_p p^{\max(\alpha_p,\beta_p)}.$$

Например, $360 = 2^3 \cdot 3^2 \cdot 5$, $252 = 2^2 \cdot 3^2 \cdot 7$. Отсюда НОД равен $2^2 \cdot 3^2 = 36$, а НОК — $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. Для вычисления НОД без готовых разложений по-прежнему применим алгоритм Евклида из лекции 2.

4 Пробные деления

4.1 Проверка одного числа на простоту

Для $n < 2$ ответ «не простое» следует из определения. Число 2 обрабатывается отдельно. Для $n > 2$ сначала проверяют делимость на 2, а затем нечётные кандидаты $d = 3,5,7,9,\ldots$, пока $d^2 \le n$. Найденный нетривиальный делитель доказывает составность; если цикл закончился без него, лемма 2 доказывает простоту.

Проверка всех нечётных кандидатов включает некоторые лишние деления, например на 9. Это сохраняет корректность и позволяет обойтись без заранее построенного списка простых. При ручном доказательстве можно проверять только простые кандидаты, если их список до нужной границы известен полностью.

Условие $d^2 \le n$ сравнивает целые числа. Оно избегает округления квадратного корня. В Python целые числа имеют произвольную точность; для получения самой границы используют точную функцию `math.isqrt(n)`.

4.2 Полная факторизация

Обозначим исходное число через n, а текущую неразложенную часть через R. Начинаем с $R = n$. Для очередного кандидата p извлекаем его **все возможные разы**, пока $p \mid R$, каждый раз заменяя R на R/p. Число извлечений даёт показатель степени.

После извлечения множителей границу проверяют по **текущему** R, а не только по исходному n. Если очередной кандидат удовлетворяет $p^2 > R$, то при $R > 1$ оставшееся число простое. Иначе у него был бы простой делитель не больше $\sqrt{R} < p$, который уже должен был быть извлечён.

При последовательном переборе 2 и всех нечётных кандидатов сохраняются два утверждения: исходное число равно произведению найденных множителей и R; у R нет простого делителя меньше текущего кандидата. Поэтому составной кандидат не может стать новым извлекаемым множителем.

Пример. Разложим 7560.

Этап	Выделенный множитель	Новая часть R
Начало	—	7560
Деление на 2 до отказа	2^3	945
Деление на 3 до отказа	3^3	35
Деление на 5	5	7
Простой остаток	7	1

Получаем $7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$. Проверка: $8 \cdot 27 \cdot 5 \cdot 7 = 7560$. Если остановить перебор раньше необходимой границы, оставшаяся часть не обязана быть простой: например, после удаления множителя 2 из 242 остаётся $121 = 11^2$.

5 Решето Эратосфена

5.1 Построение таблицы простых чисел

Решето решает задачу получения **всех** простых чисел, не превосходящих заданное N. Это другая задача, чем проверка одного числа. Создадим таблицу признаков для чисел от 0 до N. Числа 0 и 1 сразу исключим, а числа от 2 до N первоначально отметим как возможные простые.

Перебираем $p = 2,3, \ldots$, пока $p^2 \leq N$. Если число p ещё не вычеркнуто, исключаем его кратные

$$p^2,\ p^2 + p,\ p^2 + 2p, \ldots \leq N.$$

После окончания цикла все оставшиеся числа от 2 до N являются простыми. Если $N < 2$, результат — пустой список.

Почему начинаем с p^2? Любое кратное kp с $2 \leq k < p$ имеет простой делитель $q \mid k$, причём $q < p$. Поэтому оно уже было вычеркнуто при обработке q. Само простое p исключать нельзя. Начало с $2p$ тоже позволяет получить правильный результат, но выполняет дополнительные отметки.

5.2 Доказательство корректности

До обработки очередного кандидата p уже исключены все составные числа, имеющие простой делитель меньше p. Если невычеркнутое p было бы составным, оно имело бы простой делитель меньше p и было бы исключено ранее. Следовательно, каждое обрабатываемое невычеркнутое p действительно простое.

Алгоритм не вычёркивает простые: каждое отмечаемое число имеет вид $p(p+j)$ при $j \geq 0$ и потому составное. Обратно, у любого составного $n \leq N$ есть наименьший простой делитель $p \leq \sqrt{n} \leq \sqrt{N}$. При этом $n \geq p^2$, поэтому число n обязательно попадает в последовательность отметок для p. Значит, после завершения остаются ровно простые числа.

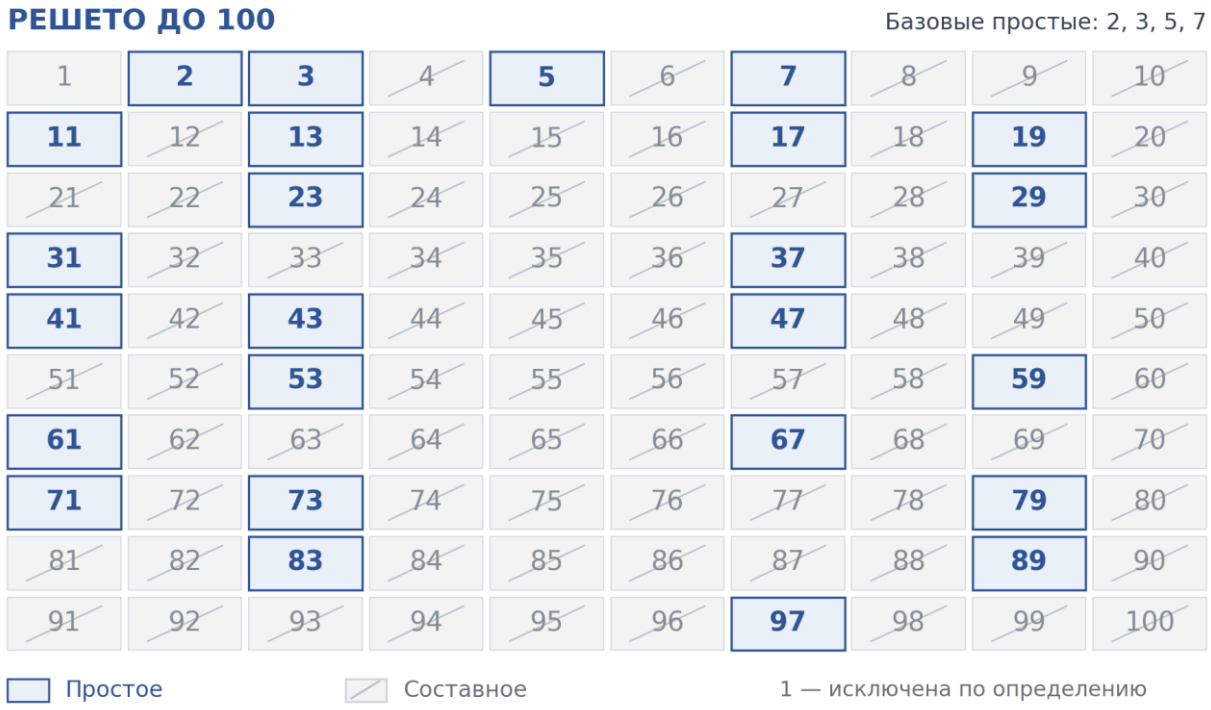


Рисунок 2. Для границы 100 достаточно обработать простые 2, 3, 5 и 7; остаются 25 простых чисел.

5.3 Пример и точный подсчёт отметок

Для $N = 60$ обрабатываются простые 2,3,5,7. Остаётся список

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59.$$

Введём $\pi(N)$ — число простых, не превосходящих N. Здесь $\pi(60) = 17$. Если считать каждое присваивание «вычеркнуто», включая повторные, для простого p число отметок равно

$$C_p(N) = \lfloor N/p \rfloor - p + 1 \qquad (p^2 \leq N).$$

Действительно, отмечаются числа kp при $k = p, p+1, \ldots, \lfloor N/p \rfloor$. Общее число отметок:

$$C(N) = \sum_{\substack{p \text{ простое} \\ p^2 \leq N}} (\lfloor N/p \rfloor - p + 1).$$

Для $N = 60$ получаем $29 + 18 + 8 + 2 = 57$ отметок. Различных составных чисел в диапазоне $[2,60]$ всего $60 - 1 - 17 = 42$. Число 30, например, отмечается при обработке 2, 3

и 5. Поэтому число присваиваний и число впервые исключённых чисел различаются. Начальное исключение 0 и 1 в $C(N)$ не включается.

6 Объём вычислений и связь с криптографией

6.1 Размер числа и длина его записи

В худшем случае проверка простоты пробными делениями требует порядка $\sqrt{n}$ проверок остатка. Если число нечётное и простое, перебор всех нечётных кандидатов выполняется до конца. Пропуск чётных кандидатов уменьшает количество проверок примерно вдвое, но не изменяет порядок роста.

Пусть двоичная запись n содержит ℓ бит. Тогда $2^{\ell-1} \le n < 2^{\ell}$, поэтому $\sqrt{n}$ имеет порядок $2^{\ell/2}$. Следовательно, число пробных делений растёт экспоненциально по длине входа. Даже оценка числа делений уже объясняет, почему этот учебный метод неудобен для больших криптографических чисел. Дополнительно нужно учитывать стоимость самих операций над длинными целыми.

Полная факторизация пробными делениями имеет такую же верхнюю оценку по порядку числа кандидатов. При наличии небольших множителей текущая часть R быстро уменьшается, и фактический объём работы может быть значительно меньше.

6.2 Оценка решета

Массив признаков занимает $O(N)$ памяти. Для числа отметок непосредственно получаем

$$C(N) \le N \sum_{j=2}^{\lfloor \sqrt{N} \rfloor} \frac{1}{j} = O(N \log N).$$

Это простая верхняя оценка, в которой сумма по простым заменена большей суммой по всем целым. Более точная классическая оценка решета — $O(N \log\log N)$ операций при $N \to \infty$; её вывод использует оценку суммы обратных простых. Для практической работы достаточно точной формулы $C(N)$ и понимания источника повторных отметок.

Счётчики пробных делений и отметок решета измеряют разные операции. По их значениям нельзя непосредственно заключить, во сколько раз одна программа быстрее другой. Выбор метода прежде всего зависит от задачи: проверить одно число, разложить его или построить таблицу простых.

6.3 Криптографический смысл

В RSA используется модуль $n = pq$, образованный произведением двух различных простых чисел. Например, $61 \cdot 53 = 3233$. Зная множители, произведение легко проверить. Восстановление множителей по одному произведению составляет задачу факторизации. Проверка простоты заданного кандидата и факторизация составного числа — разные вычислительные задачи; алгоритмы для больших чисел будут изучаться позднее.

Единственность разложения обеспечивает однозначность искомых простых множителей, но сама по себе не даёт быстрого способа их найти. Решето же требует хранения признаков для целого диапазона, поэтому подходит для построения таблиц умеренного размера.

7 Следствия и самостоятельная работа

7.1 Степени и дополнение до квадрата

Из основной теоремы арифметики следует: положительное число является полным квадратом тогда и только тогда, когда все показатели его канонического разложения чётны. Для k-й степени при $k \geq 2$ все показатели должны делиться на k.

Если $n = \prod p_i^{\alpha_i}$, то наименьшее положительное целое h, для которого nh — квадрат, имеет вид

$$h = \prod_{\alpha_i \text{ нечётно}} p_i.$$

Каждый нечётный показатель необходимо увеличить хотя бы на 1. Любой подходящий множитель обязан содержать все указанные простые, то есть делиться на h; поэтому найденное h минимально. Например, для $7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$ имеем $h = 210$ и $7560 \cdot 210 = 1260^2$.

7.2 Необходимое условие не является достаточным

Любое простое $p > 3$ имеет вид $6k - 1$ или $6k + 1$: остальные классы остатков по модулю 6 делятся на 2 или 3. Но числа 25 и 35 имеют такой вид и являются составными. Этот признак сокращает кандидатов, но не доказывает простоту.

Ещё один пример дают числа Мерсенна $M_t = 2^t - 1$. Если $t = ab$, где $a, b > 1$, то

$$2^{ab} - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)}).$$

Поэтому для простоты M_t необходимо, чтобы t было простым. Обратное неверно: 11 простое, но $2^{11} - 1 = 2047 = 23 \cdot 89$.

7.3 Задания для самостоятельного решения

1. Докажите простоту 101 и составность 221. Укажите достаточную границу проверки и найденные остатки или делитель.
2. Разложите 1470 и 980 на простые множители; найдите по показателям НОД и НОК и проверьте их алгоритмом Евклида.
3. Найдите наименьшее положительное h, для которого $540h$ — квадрат. Укажите этот квадрат и докажите минимальность h.
4. Постройте решето до 50. Найдите $\pi(50)$, число всех отметок от p^2 и количество различных составных чисел в $[2,50]$.
5. Используя факториал, постройте четыре последовательных составных числа и для каждого укажите нетривиальный делитель.

Контрольные вопросы

1. Почему 1 не является простым или составным числом?
2. Почему наименьший делитель числа, больший 1, обязательно прост?
3. Почему в проверке простоты достаточно границы $\sqrt{n}$ и почему она включается?
4. Где в лемме Евклида используется простота делителя?
5. Должно ли число «произведение простых плюс один» само быть простым?
6. Какие два утверждения содержит основная теорема арифметики?
7. Как проверяется полнота предложенного разложения?
8. Почему при факторизации нужно извлекать всю степень найденного простого?
9. При каком условии оставшаяся часть факторизации гарантированно простая?
10. Почему в решете отметки начинают с p^2, а цикл заканчивают при $p^2 > N$?
11. Чем число отметок решета отличается от количества составных чисел?
12. Почему число делений порядка $\sqrt{n}$ не даёт полиномиальной оценки по числу бит?

Литература к теме

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии**. СПб.: Лань, 2020. § 3.3, с. 91–96: свойства простых, основная теорема арифметики и решето.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory**. 2nd ed. Pearson Education, 2006. § 3.1.2: простые числа и единственность разложения.
3. Панкратова И. А. **Теоретико-числовые методы в криптографии**. 2009. § 3.1, с. 73–74: пробные деления и полнота факторизации.
4. Kraft D., Washington L. C. **An Introduction to Number Theory with Cryptography**. 2nd ed. CRC Press, 2018. §§ 2.2–2.3: бесконечность множества простых; разделы доступны в предоставленном ознакомительном фрагменте.