ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 4

ВЗАИМНАЯ ПРОСТОТА И АРИФМЕТИЧЕСКИЕ ФУНКЦИИ

Цель лекции	Обосновать свойства взаимно простых чисел, понятие мультипликативности и формулу функции Эйлера; научиться работать с целой и дробной частями.
Результат обучения	Различать общую и попарную взаимную простоту; вычислять арифметические функции по разложению; корректно находить целую и дробную части отрицательных чисел.
Предварительная подготовка	Делимость, НОД, НОК, тождество Безу и единственность разложения на простые множители из лекций 1–3.

Аудиторная нагрузка: 1 академический час. Основное содержание занятия — критерий взаимной простоты, мультипликативность, функция Эйлера и целая часть. Дополнительные следствия, подсчёт делителей и задачи для самостоятельной работы расширяют материал занятия.

План лекции

1. Критерий взаимной простоты и основные свойства.
2. Попарная взаимная простота и наименьшее общее кратное.
3. Арифметические и мультипликативные функции.
4. Функция Эйлера и её вычисление.
5. Целая и дробная части действительного числа.
6. Подсчёт кратных и связь с криптографическими вычислениями.
7. Задачи для самостоятельного решения.

1 Взаимная простота

Целые числа a, b называются **взаимно простыми**, если $\gcd(a, b) = 1$. При вычислении НОД знаки аргументов несущественны. Например, 14 и 25 взаимно просты, хотя оба числа составные; 14 и 21 не взаимно просты, поскольку их НОД равен 7. Простота одного числа и взаимная простота пары — разные понятия.

Критерий Безу. Числа a, b взаимно просты тогда и только тогда, когда существуют целые u, v, для которых

$$au + bv = 1.$$

Доказательство. Если НОД равен 1, такое представление даёт тождество Безу, полученное в лекции 2. Обратно, любой общий положительный делитель a и b делит левую часть, а значит, делит 1. Поэтому общий положительный делитель только один — единица.

Например, $2 \cdot 25 - 7 \cdot 7 = 1$, следовательно, 25 и 7 взаимно просты. Для соседних целых $n, n + 1$ имеем $(n + 1) - n = 1$, поэтому они всегда взаимно просты. В частности, взаимная простота не требует положительности обоих аргументов: $\gcd(0,1) = 1$.

Если $g = \gcd(a, b) > 0$, то числа a/g и b/g взаимно просты. Достаточно разделить равенство $au + bv = g$ на g . Это свойство понадобится при правильном сокращении сравнений.

1.1 Сокращение в утверждении о делимости

Теорема. Если $a \mid bc$ и $\gcd(a, b) = 1$, то $a \mid c$.

Доказательство. Выберем u, v с $au + bv = 1$ и умножим равенство на c. Получим $acu + bcv = c$. Оба слагаемых слева делятся на a, откуда $a \mid c$.

Условие взаимной простоты существенно. Из $6 \mid 2 \cdot 3$ нельзя заключить, что $6 \mid 3$, поскольку 6 и 2 не взаимно просты. В сравнении по модулю это ограничение проявляется как запрет произвольного деления обеих частей.

1.2 Взаимная простота с произведением

Для положительных целых a, b, c справедливо равносильное утверждение

$$\gcd(a, bc) = 1 \quad \Leftrightarrow \quad \gcd(a, b) = \gcd(a, c) = 1.$$

Доказательство. Если a взаимно просто с bc, общий делитель a и одного из сомножителей также делил бы bc, поэтому он равен 1. Обратно, предположим взаимную простоту с каждым сомножителем. Если бы a и bc имели общий делитель больше 1, они имели бы общий простой делитель p. По лемме Евклида $p \mid b$ или $p \mid c$, что противоречит одной из двух гипотез.

Следствие: если a взаимно просто с каждым из $b_1, \dots, b_k$, то оно взаимно просто с их произведением. В частности, из $\gcd(a, b) = 1$ следует $\gcd(a^r, b^s) = 1$ для положительных целых r, s.

2 Общая и попарная взаимная простота

Для нескольких положительных целых различают два условия. **Общая взаимная простота** означает $\gcd(a_1, \dots, a_k) = 1$. **Попарная взаимная простота** означает $\gcd(a_i, a_j) = 1$ при любых $i \neq j$.

Попарная взаимная простота влечёт общую, но обратное неверно. У чисел 6, 10 и 15 нет общего простого делителя сразу для всех трёх, однако каждая пара имеет нетривиальный НОД:

$$\gcd(6,10,15) = 1, \qquad \gcd(6,10) = 2, \quad \gcd(6,15) = 3, \quad \gcd(10,15) = 5.$$

Теорема. Для попарно взаимно простых положительных чисел

$$\operatorname{lcm}(a_1, \dots, a_k) = a_1 \cdots a_k.$$

Доказательство. Для двух чисел пусть $a \mid N$ и $b \mid N$. Запишем $N = at$. Из $b \mid at$ и $\gcd(a, b) = 1$ следует $b \mid t$, значит, $ab \mid N$. Само ab является общим кратным, поэтому это НОК. Для нескольких чисел применяем индукцию: произведение уже рассмотренных чисел взаимно просто с очередным числом по свойству раздела 1.2.

Например, числа 4, 9 и 25 попарно взаимно просты, и их НОК равен $4 \cdot 9 \cdot 25 = 900$. Для 6, 10 и 15 НОК равен 30, тогда как произведение равно 900. Одного условия общего НОД, равного 1, для формулы произведения недостаточно.

Верно и обратное: для положительных a_i равенство НОК произведению возможно только при попарной взаимной простоте. Действительно, показатель любого простого в НОК — максимум его показателей в a_i, а в произведении — их сумма. Эти величины совпадают для всех простых только тогда, когда каждый простой встречается не более чем в одном из чисел.

3 Арифметические функции

Арифметическая функция — функция, определённая на положительных целых $\mathbb{N} = \{1,2,\dots\}$. Здесь достаточно функций с действительными значениями. Примеры: постоянная функция $f(n) = 1$, степенная функция $f_k(n) = n^k$ при фиксированном целом $k \geq 0$, число делителей и функция Эйлера.

Функция f называется **мультипликативной**, если $f(1) = 1$ и

$$f(mn) = f(m)f(n) \qquad \text{при } \gcd(m,n) = 1.$$

Если $f(1) = 1$ и равенство выполнено для любых положительных m, n, функцию называют **вполне мультипликативной**. Каждая вполне мультипликативная функция мультипликативна. Степенная функция $f_k(n) = n^k$ вполне мультипликативна, поскольку $(mn)^k = m^k n^k$.

Проверка нескольких чисел может опровергнуть мультипликативность, но не доказывает её для всех аргументов. Например, функция $f(n) = n + 1$ не удовлетворяет даже условию $f(1) = 1$, а при взаимно простых 2 и 3 также получаем $f(6) = 7 \neq f(2)f(3) = 12$.

3.1 Вычисление по простым степеням

Если функция мультипликативна и известно каноническое разложение $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, то

$$f(n) = \prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right).$$

Основание формулы — попарная взаимная простота различных простых степеней. При этом нельзя без дополнительного условия заменять $f(p^\alpha)$ на $f(p)^\alpha$: сомножители p и p не взаимно просты. Такая замена гарантирована только для вполне мультипликативной функции.

3.2 Число и сумма делителей

Пусть $\tau(n)$ — число положительных делителей, а $\sigma(n)$ — их сумма. Из канонического разложения следуют формулы

$$\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1), \qquad \sigma(n) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{\alpha_i}).$$

Каждый делитель однозначно имеет вид $p_1^{\beta_1} \cdots p_k^{\beta_k}$, где $0 \leq \beta_i \leq \alpha_i$. Независимый выбор показателей даёт формулу для количества. Раскрытие произведения геометрических сумм даёт по одному слагаемому на каждый делитель и доказывает формулу суммы.

При $\gcd(m,n) = 1$ множества простых оснований в разложениях m и n не пересекаются. Обе формулы поэтому показывают мультипликативность τ и σ. Но $\tau(4) = 3 \neq \tau(2)^2 = 4$, так что τ не вполне мультипликативна.

Например, $72 = 2^3 \cdot 3^2$. Следовательно, $\tau(72) = 4 \cdot 3 = 12$, а $\sigma(72) = (1 + 2 + 4 + 8)(1 + 3 + 9) = 195$. Для 1 единственный положительный делитель — 1, поэтому $\tau(1) = \sigma(1) = 1$.

4 Функция Эйлера

Функцией Эйлера называется число положительных целых, не превосходящих n и взаимно простых с n:

$$\varphi(n) = \#\{k \in \mathbb{N} : 1 \le k \le n,\ \gcd(k,n) = 1\}.$$

По этому определению $\varphi(1) = 1$. Для $n > 1$ само число n не учитывается; поэтому можно считать взаимно простые числа от 1 до $n-1$. Например, для 12 подходят 1, 5, 7, 11, откуда $\varphi(12) = 4$.

4.1 Простое число и его степень

Если p простое, все числа $1, \dots, p-1$ взаимно просты с ним, и $\varphi(p) = p - 1$. Для степени p^α единственная причина невзаимной простоты — делимость на p. Среди чисел от 1 до p^α таких чисел ровно $p^{\alpha-1}$. Следовательно,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1), \qquad \alpha \ge 1.$$

Например, $\varphi(16) = 16 - 8 = 8$. Это число взаимно простых с 16 чисел, а не количество простых до 16: функция $\pi(n)$ из предыдущей лекции считает другой набор.

4.2 Общая формула

Теорема. Если $n > 1$ и $p_1, \dots, p_k$ — все различные простые делители n, то

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

Доказательство через включения и исключения. Число взаимно просто с n тогда и только тогда, когда оно не делится ни на один из p_i. Среди $1, \dots, n$ имеется n/p_i кратных p_i. Из n нужно вычесть эти количества, затем вернуть числа, вычтенные дважды, снова вычесть пересечения троек и так далее:

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \cdots.$$

Все знаменатели здесь делят n: произведение различных простых делителей входит в его каноническое разложение. Если раскрыть произведение $n \prod_i (1 - 1/p_i)$, получится ровно эта чередующаяся сумма. Подстановка $n = \prod_i p_i^{\alpha_i}$ даёт вторую форму формулы.

Пример. Для $30 = 2 \cdot 3 \cdot 5$ имеем

$$\varphi(30) = 30 - 15 - 10 - 6 + 5 + 3 + 2 - 1 = 8.$$

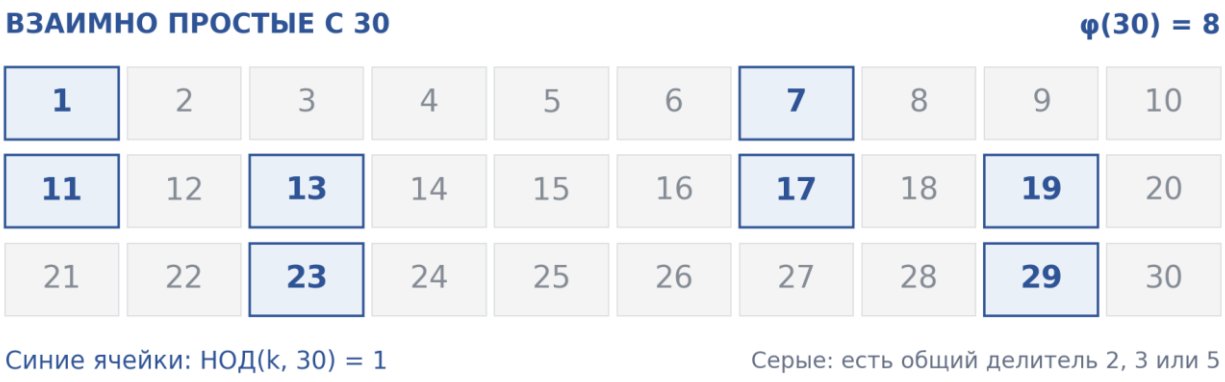


Рисунок 1. Числа 1, 7, 11, 13, 17, 19, 23 и 29 не делятся на 2, 3 или 5 и учитываются в функции Эйлера.

4.3 Мультипликативность и границы её применения

Если $\gcd(m,n)=1$, различные простые делители m и n образуют непересекающиеся наборы. Применяя общую формулу, получаем

$$\varphi(mn)=mn\prod_{p\mid m}(1-1/p)\prod_{q\mid n}(1-1/q)=\varphi(m)\varphi(n).$$

Следовательно, функция Эйлера мультипликативна. При этом она не вполне мультипликативна: $\varphi(4)=2$, тогда как $\varphi(2)\varphi(2)=1$. Ещё один пример: $\varphi(4\cdot 6)=\varphi(24)=8$, но $\varphi(4)\varphi(6)=4$.

В формуле произведение берётся по **различным** простым делителям. Для $360=2^3\cdot 3^2\cdot 5$ каждая поправка применяется один раз:

$$\varphi(360)=360(1-1/2)(1-1/3)(1-1/5)=96.$$

Для вычисления целыми числами можно начать с $y=n$ и для каждого различного простого делителя p выполнить $y\leftarrow y-y/p$. Каждое такое деление точное. В Python используют `y -= y // p`; повторять эту поправку по числу экземпляров одного и того же простого нельзя.

4.4 Сумма по делителям

Теорема. Для любого положительного n

$$\sum_{d\mid n}\varphi(d)=n.$$

Доказательство. Разобьём числа $k=1,\dots,n$ на группы по значению $g=\gcd(k,n)$. Для фиксированного делителя g запишем $k=gj$, $n=gm$. Тогда $1\le j\le m$ и $\gcd(j,m)=1$, то есть группа содержит $\varphi(m)=\varphi(n/g)$ чисел. Группы не пересекаются и вместе содержат все n чисел. Суммируя и заменяя делитель n/g на d, получаем утверждение.

Для $n=12$ делители равны 1, 2, 3, 4, 6, 12, поэтому сумма равна $1+1+2+2+2+4=12$. Это полезная проверка таблицы значений функции.

Дополнительное следствие: $\varphi(n)$ чётно при $n>2$. Подходящие числа разбиваются на пары $k,n-k$. Равенство $k=n-k$ возможно лишь при $k=n/2$, но для $n>2$ такое число не взаимно просто с n.

5 Целая и дробная части

Целая часть действительного x, обозначаемая $\lfloor x\rfloor$, — наибольшее целое, не превосходящее x. Это округление вниз, а не отбрасывание знаков после запятой. **Дробная часть** определяется равенством $\{x\}=x-\lfloor x\rfloor$. Всегда выполнено

$$x=\lfloor x\rfloor+\{x\},\qquad \lfloor x\rfloor\le x<\lfloor x\rfloor+1,\qquad 0\le\{x\}<1.$$

Например, $\lfloor 17/5\rfloor=3$ и $\{17/5\}=2/5$. Для отрицательного числа $-17/5=-3{,}4$ получаем $\lfloor -17/5\rfloor=-4$, $\{-17/5\}=3/5$. У целого числа дробная часть равна нулю.

5.1 Основные тождества

Для целого t из определения непосредственно следует

$$\lfloor x+t\rfloor=\lfloor x\rfloor+t,\qquad \{x+t\}=\{x\}.$$

Записав $x = r + \alpha$, $y = s + \beta$, где r, s целые и $0 \le \alpha, \beta < 1$, получаем

$$\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor.$$

Последнее слагаемое равно 0 или 1. Поэтому целая часть суммы не обязана равняться сумме целых частей. Например, при $x = 7/10$, $y = 8/10$ целая часть суммы равна 1, а сумма целых частей равна 0.

Если x не целое, то

$$\lfloor -x \rfloor = -\lfloor x \rfloor - 1, \qquad \{-x\} = 1 - \{x\}.$$

Для целого x вместо этого имеем $\lfloor -x \rfloor = -x$ и $\{-x\} = 0$. Особый случай целого аргумента нельзя пропускать.

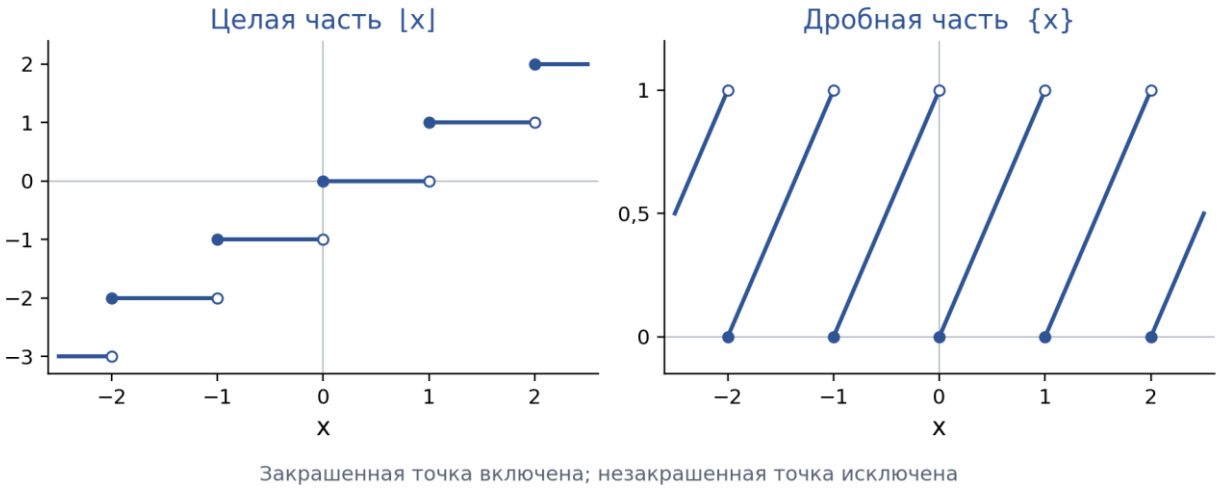


Рисунок 2. Целая часть постоянна на каждом интервале от целого числа до следующего; дробная часть на нём возрастает от 0 до 1, не достигая 1.

5.2 Деление с остатком

Пусть a — целое, $m > 0$ — целый модуль. Тогда единственное деление с неотрицательным остатком имеет вид

$$q = \lfloor a/m \rfloor, \qquad r = a - mq, \qquad 0 \le r < m.$$

Отсюда $\{a/m\} = r/m$. Например, $-17 = 5(-4) + 3$, поэтому частное равно -4, остаток 3, дробная часть $-17/5$ равна $3/5$.

В Python при положительном `m` этим формулам соответствуют `a // m` и `a % m`. Вызов `int(a / m)` сначала создаёт вещественное число и затем отбрасывает дробную часть к нулю; для отрицательного нецелого частного результат отличается от округления вниз. Для больших целых вычисление через вещественные числа может также потерять точность.

6 Применения формул

6.1 Количество кратных на целочисленном отрезке

Пусть L, U целые, $L \le U$, $d > 0$ целое. Число кратных d на отрезке от L до U включительно равно

$$\lfloor U/d \rfloor - \lfloor (L-1)/d \rfloor.$$

Доказательство. Для кратного jd условие имеет вид $L/d \le j \le U/d$. Наибольшее допустимое целое j равно $\lfloor U/d \rfloor$, а первое допустимое равно $\lfloor (L-1)/d \rfloor + 1$. Вычитание

границ и добавление единицы дают формулу. Это рассуждение одинаково работает при положительных и отрицательных концах отрезка.

На отрезке от -17 до 23 кратных 5 ровно $\lfloor 23/5 \rfloor - \lfloor -18/5 \rfloor = 4 - (-4) = 8$: это $-15, -10, -5, 0, 5, 10, 15, 20$.

6.2 Зачем функция Эйлера нужна в криптографии

Для произведения двух различных простых $n = pq$ формула принимает вид $\varphi(n) = (p-1)(q-1)$. Например, для $n = 5 \cdot 11 = 55$ получаем $\varphi(55) = 40$. Этот подсчёт будет использоваться при изучении теоремы Эйлера и RSA.

Различие простых существенно: для $n = 5^2$ следует использовать формулу простой степени, и $\varphi(25) = 20$, а не $(5-1)^2 = 16$. На этом этапе функция Эйлера описывает количество взаимно простых чисел; утверждения о степенях по модулю будут доказаны в соответствующей лекции.

7 Самостоятельная работа

1. С помощью алгоритма Евклида найдите целые u, v с $35u + 64v = 1$. Объясните, почему это доказывает взаимную простоту и позволяет сокращать множитель 35 в утверждении $64 \mid 35c$.
2. Сравните тройки $(6,10,15)$ и $(8,9,25)$: общий НОД, попарные НОД, НОК и произведение. Для какой тройки НОК равен произведению и почему?
3. Для 180 найдите $\varphi(180)$, $\tau(180)$ и $\sigma(180)$. Обоснуйте каждую формулу по разложению.
4. Вычислите $\varphi(8)$, $\varphi(9)$, $\varphi(72)$, а также $\varphi(6)$, $\varphi(12)$ и $\varphi(72)$. Объясните, почему в первой паре работает произведение значений, а во второй — нет.
5. Найдите целые и дробные части чисел $-23/6$, -4 и $19/7$. Проверьте тождества для изменения знака и для суммы $-23/6 + 19/7$.
6. Найдите число кратных 7 на отрезке от -50 до 50 включительно. Проверьте ответ перечислением.

Контрольные вопросы

1. Чем взаимная простота отличается от простоты каждого числа?
2. Как тождество Безу удостоверяет взаимную простоту?
3. Какое условие позволяет из $a \mid bc$ заключить $a \mid c$?
4. Почему общий НОД тройки, равный 1, не гарантирует попарной взаимной простоты?
5. Когда НОК нескольких положительных чисел равен их произведению?
6. Чем мультипликативность отличается от полной мультипликативности?
7. Почему достаточно знать значения мультипликативной функции на простых степенях?
8. Что считает функция Эйлера и почему $\varphi(1) = 1$?
9. Почему каждый различный простой делитель входит в формулу функции Эйлера один раз?
10. Почему $\varphi(mn) = \varphi(m)\varphi(n)$ требует взаимной простоты аргументов?
11. Почему целая часть $-3{,}4$ равна -4, а дробная часть равна 0,6?
12. Как целая часть связана с делением с остатком и подсчётом кратных?

Литература к теме

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии**. СПб.: Лань, 2020. §§ 3.1.2–3.1.3: критерий и свойства взаимной простоты; § 3.3.2: разложение и делители; § 4.3.1, с. 107–109: функция Эйлера.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory**. 2nd ed. Pearson Education, 2006. §§ 3.1–3.2: делимость и НОД; § 3.6: функция Эйлера и её применение.