ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 2

НОД, НОК И АЛГОРИТМ ЕВКЛИДА

Цель лекции	Обосновать алгоритм Евклида, получить линейное представление НОД и оценить число делений.
Результат обучения	Находить НОД и НОК; строить таблицу расширенного алгоритма; проверять тождество Безу; объяснять завершение и сложность вычислений.
Предварительная подготовка	Делимость целых чисел, линейные комбинации и теорема о делении с остатком из лекции 1.

Аудиторная нагрузка: 1 академический час. Разделы 1–5 и формулировка теоремы Ламе составляют основу занятия. Подробное доказательство оценки и приложения раздела 7 предназначены также для самостоятельного изучения и практической работы.

План лекции

1. Наибольший общий делитель и взаимно простые числа.
2. Алгоритм Евклида: идея, корректность и пример.
3. Тождество Безу и расширенный алгоритм Евклида.
4. Следствия из тождества Безу.
5. Наименьшее общее кратное.
6. Число шагов и теорема Ламе.
7. Линейное уравнение и обратный элемент как приложения.

1 Наибольший общий делитель

Пусть $a, b \in \mathbb{Z}$ и хотя бы одно из чисел отлично от нуля. **Наибольший общий делитель** $\gcd(a, b)$, или $\text{НОД}(a, b)$, — наибольшее положительное целое число, которое делит и a, и b. Множество положительных общих делителей непусто, поскольку содержит 1, и конечно: любой такой делитель не превосходит модуля ненулевого числа из пары.

Например, общие положительные делители 18 и 30 — числа 1, 2, 3 и 6, поэтому $\gcd(18,30) = 6$. Числа называются **взаимно простыми**, если их НОД равен 1. Взаимная простота не означает, что каждое число простое: $\gcd(8,15) = 1$.

Из определения непосредственно следуют равенства

$$\gcd(a, b) = \gcd(b, a) = \gcd(|a|, |b|), \qquad \gcd(a, 0) = |a| \quad (a \neq 0).$$

У пары $(0,0)$ нет наибольшего положительного общего делителя. Для единообразия программ **отдельно принимаем соглашение** $\gcd(0,0) = 0$. Доказательства, в которых требуется положительный НОД или деление на него, относятся к парам, не равным $(0,0)$.

В криптографических вычислениях НОД нужен, например, для проверки возможности обратного умножения по модулю. Его можно вычислять делениями с остатком, не раскладывая исходные числа на простые множители. Именно этот путь реализует алгоритм Евклида.

2 Алгоритм Евклида

2.1 Почему можно заменить пару чисел

Лемма. Для любых целых a, b, q справедливо

$$\gcd(a, b) = \gcd(b, a - qb).$$

Доказательство. Если $d \mid a$ и $d \mid b$, то $d \mid (a - qb)$. Обратно, если $d \mid b$ и $d \mid (a - qb)$, то $d \mid \big((a - qb) + qb\big) = a$. Поэтому две пары имеют одно и то же множество общих делителей и одинаковый НОД. Для пары нулей равенство согласуется с принятым соглашением.

Выберем q как частное при делении положительного a на положительное b. Тогда $a = qb + r$, $0 \le r < b$, и лемма даёт

$$\gcd(a, b) = \gcd(b, r).$$

Новое второе число меньше прежнего. На этом уменьшении основано завершение алгоритма.

2.2 Алгоритм и доказательство корректности

Сначала заменим исходные числа модулями. Пока второе число b не равно нулю, вычисляем остаток $r = a \bmod b$ и **одновременно** заменяем пару (a, b) на (b, r). Когда второе число станет нулём, возвращаем первое.

Инвариант — утверждение, которое сохраняется после каждого шага: НОД текущей пары равен НОД исходной пары. Лемма доказывает сохранение инварианта. **Завершение** следует из строгого убывания неотрицательных вторых компонентов. В конце получаем пару $(g, 0)$, её НОД равен g. Следовательно, возвращается НОД исходных чисел.

Не следует смешивать два утверждения: уменьшение остатков доказывает завершение, а сохранение НОД доказывает правильность ответа.

2.3 Пример: НОД чисел 240 и 46

Шаг	Деление с остатком	Новый остаток
1	$240 = 5 \cdot 46 + 10$	10
2	$46 = 4 \cdot 10 + 6$	6
3	$10 = 1 \cdot 6 + 4$	4
4	$6 = 1 \cdot 4 + 2$	2
5	$4 = 2 \cdot 2 + 0$	0

Последний **ненулевой** остаток равен 2, поэтому $\gcd(240,46) = 2$. Последнее деление с нулевым остатком тоже считаем шагом: в примере выполнено пять делений. Числа 240 и 46 не являются взаимно простыми.

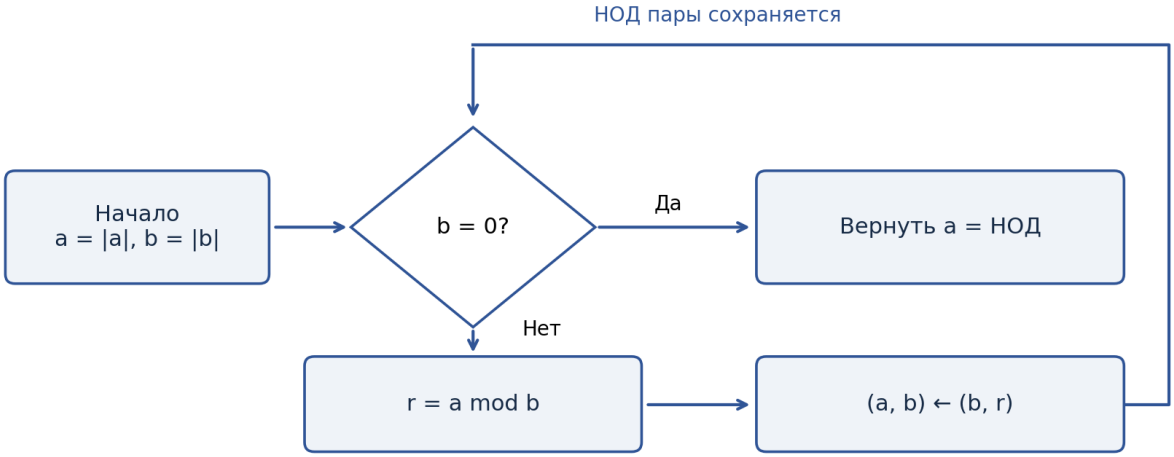


Рисунок 1. Остаток становится новым делителем; значение НОД сохраняется.

3 Тождество Безу и расширенный алгоритм

3.1 Линейное представление НОД

Теорема Безу. Если $g = \gcd(a, b) > 0$, то существуют целые s, t, для которых

$$as + bt = g.$$

Доказательство. Исходные числа уже являются линейными комбинациями: $a = 1 \cdot a + 0 \cdot b$, $b = 0 \cdot a + 1 \cdot b$. Каждый следующий остаток получается вычитанием целого кратного предыдущего остатка из предшествующего. Поэтому он также является целой линейной комбинацией a и b. Последний ненулевой остаток равен g, что и даёт нужное представление. Переход к модулям не мешает доказательству: знак можно включить в коэффициент.

Коэффициенты s, t называются **коэффициентами Безу**. Они не единственны. В общем случае неверно требовать, чтобы оба коэффициента были положительными.

Для примера из раздела 2 последовательно подставим выражения остатков снизу вверх:

$$2 = 6 - 4 = 6 - (10 - 6) = 2 \cdot 6 - 10,$$

$$2 = 2(46 - 4 \cdot 10) - 10 = 2 \cdot 46 - 9 \cdot 10,$$

$$2 = 2 \cdot 46 - 9(240 - 5 \cdot 46) = -9 \cdot 240 + 47 \cdot 46.$$

Итак, $s = -9$, $t = 47$. Проверка: $-2160 + 2162 = 2$. Обратная подстановка удобна для небольших примеров; расширенный алгоритм сразу вычисляет коэффициенты на каждом шаге.

3.2 Табличная форма расширенного алгоритма

Для положительных a, b положим

$$r_{-1} = a, \quad r_0 = b, \qquad (s_{-1}, t_{-1}) = (1,0), \quad (s_0, t_0) = (0,1).$$

На шаге $i \geq 1$, пока $r_{i-1} > 0$, вычисляем

$$q_i = \lfloor r_{i-2} / r_{i-1} \rfloor, \qquad r_i = r_{i-2} - q_i r_{i-1},$$

$$s_i = s_{i-2} - q_i s_{i-1}, \qquad t_i = t_{i-2} - q_i t_{i-1}.$$

У всех трёх столбцов одна и та же схема обновления: «предпредыдущее значение минус частное, умноженное на предыдущее». Сохраняется инвариант $r_i = as_i + bt_i$.

i	q_i	r_i	s_i	t_i
-1	—	240	1	0
0	—	46	0	1
1	5	10	1	-5
2	4	6	-4	21
3	1	4	5	-26
4	1	2	-9	47
5	2	0	23	-120

Ответ берём из строки $i = 4$, содержащей последний ненулевой остаток. Нулевая строка подтверждает завершение, но её коэффициенты выражают ноль, а не НОД.

Например, в строке $i = 2$ получаем $240(-4) + 46 \cdot 21 = 6$. Такая проверка каждой строки позволяет быстро найти арифметическую ошибку. Для исходной пары $(-240,46)$ соответствующие коэффициенты Безу равны 9 и 47.

4 Следствия из тождества Безу

Критерий взаимной простоты. Числа a, b взаимно просты тогда и только тогда, когда $as + bt = 1$ для некоторых целых s, t. Необходимость даёт теорема Безу. Для достаточности заметим, что любой общий делитель a, b делит левую часть, а значит, делит 1.

Сокращение на НОД. Если $g = \gcd(a, b) > 0$, то $\gcd(a/g, b/g) = 1$. Действительно, деление равенства Безу на g даёт $(a/g)s + (b/g)t = 1$.

Лемма о взаимно простом множителе. Если $\gcd(a, b) = 1$ и $a \mid bc$, то $a \mid c$. Умножим $as + bt = 1$ на c: $asc + btc = c$. Оба слагаемых слева делятся на a, следовательно, $a \mid c$.

Условие взаимной простоты существенно: $6 \mid 3 \cdot 4$, но $6 \nmid 4$. Эта лемма далее понадобится при работе со сравнениями и разложениями чисел.

5 Наименьшее общее кратное

Для ненулевых a, b **наименьшее общее кратное** $\operatorname{lcm}(a, b)$, или $\text{НОК}(a, b)$, — наименьшее положительное число, делящееся и на a, и на b. Для нулевых аргументов отдельно принимаем соглашение $\operatorname{lcm}(a, 0) = \operatorname{lcm}(0, a) = 0$, включая $a = 0$.

Теорема. Если $a, b \neq 0$ и $g = \gcd(a, b)$, то

$$\operatorname{lcm}(a, b) = \frac{|ab|}{g}, \qquad \gcd(a, b)\operatorname{lcm}(a, b) = |ab|.$$

Доказательство. Положим $A = |a|/g$, $B = |b|/g$; тогда $\gcd(A, B) = 1$. Число $L = gAB$ делится на $|a| = gA$ и на $|b| = gB$. Пусть $M > 0$ — другое общее кратное. Запишем $M = gAk$. Из $gB \mid M$ следует $B \mid Ak$. По лемме из раздела 4 имеем $B \mid k$, поэтому $gAB \mid M$. Следовательно, L — наименьшее положительное общее кратное.

Пример. Для 240 и 46 НОД равен 2. Поэтому

$$\operatorname{lcm}(240,46) = (240/2) \cdot 46 = 5520.$$

Проверка: $5520/240 = 23$, $5520/46 = 120$. В программе сначала делят на НОД и затем умножают; все операции должны оставаться целочисленными. Случай $(0,0)$ обрабатывают до вычисления частного, чтобы не получить деление на ноль.

Для трёх и более чисел НОД и НОК вычисляют последовательно: например, $\gcd(a,b,c) = \gcd(\gcd(a,b),c)$. Не следует подменять взаимную простоту нескольких чисел попарной: $\gcd(6,10,15) = 1$, хотя любая пара из этих чисел имеет НОД больше 1.

6 Число шагов и теорема Ламе

6.1 Числа Фибоначчи и медленное уменьшение остатков

Рассмотрим положительные входы, упорядоченные так, что $a > b > 0$. Пусть выполнено n делений, **включая последнее деление с нулевым остатком**. В обозначениях раздела 3 имеем $r_{n-1} = g$, $r_n = 0$.

Определим числа Фибоначчи: $F_1 = F_2 = 1$, $F_{k+2} = F_{k+1} + F_k$. Их начало: $1,1,2,3,5,8,13,21,34,55,89,144$.

В последнем делении частное не меньше 2, поэтому $r_{n-2} \geq 2g$. Двигаясь назад по равенствам Евклида и учитывая $q_i \geq 1$, получаем нижние границы $g, 2g, 3g, 5g, 8g, \ldots$. Отсюда

$$b \geq F_{n+1}g, \qquad a \geq F_{n+2}g.$$

Границы достигаются для пары (F_{n+2}, F_{n+1}): все частные, кроме последнего, равны 1, а последнее равно 2. Поэтому соседние числа Фибоначчи дают наименьшие положительные входы, требующие заданного числа делений.

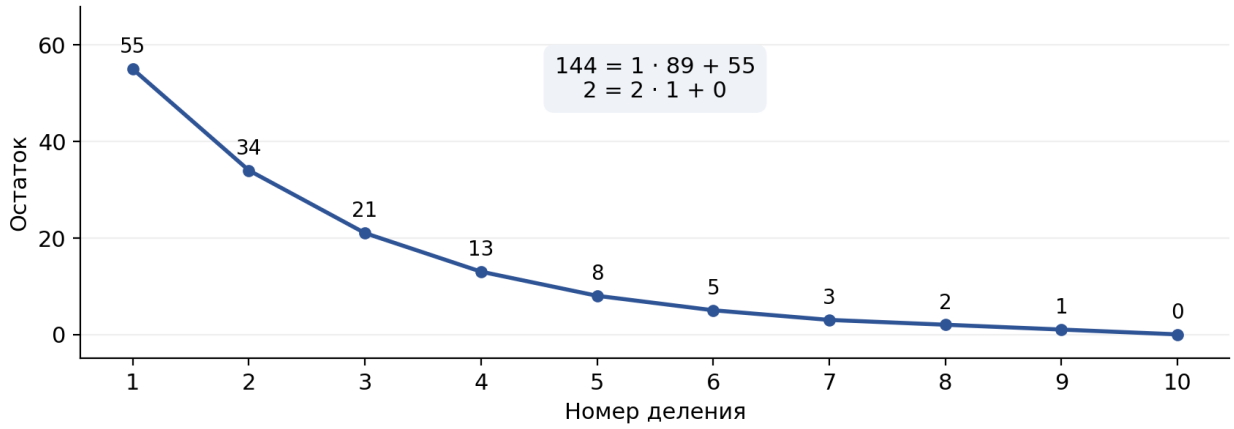


Рисунок 2. Для пары (144, 89) получаем 10 делений: остатки 55, 34, 21, 13, 8, 5, 3, 2, 1, 0.

6.2 Формулировка и доказательство оценки

Теорема Ламе. Если меньшее положительное число b имеет d десятичных цифр, алгоритм Евклида выполняет не более $5d$ делений.

Доказательство. Положим $\varphi = (1 + \sqrt{5})/2$. Из $\varphi^2 = \varphi + 1$ индукцией получаем $F_{n+1} \geq \varphi^{n-1}$. База: $F_2 = 1$, $F_3 = 2 \geq \varphi$; переход повторяет рекуррентное соотношение Фибоначчи. Следовательно,

$$\varphi^{n-1} \leq F_{n+1} \leq b < 10^d.$$

Так как $\log_\varphi 10 < 5$, имеем $n - 1 < 5d$. Число n целое, поэтому $n \le 5d$. Если исходные положительные числа равны, достаточно одного деления, и оценка также верна.

Для пары $(240,46)$ число 46 имеет две цифры: верхняя граница равна 10, фактически нужно 5 делений. Для $(144,89)$ та же граница равна 10 и достигается. Теорема даёт верхнюю оценку, а не точное число шагов для каждой пары.

Число делений имеет порядок $O(1 + \log b)$, то есть растёт не быстрее линейной функции длины записи меньшего числа. Это **оценка числа арифметических операций**, а не утверждение о постоянной стоимости каждого деления. При анализе времени работы с большими целыми дополнительно учитывают стоимость арифметики над многозначными числами.

7 Приложения тождества Безу

7.1 Линейное уравнение в целых числах

Для $a, b > 0$ уравнение $ax + by = c$ имеет целочисленное решение тогда и только тогда, когда $g = \gcd(a, b)$ делит c. Необходимость очевидна: g делит оба слагаемых. Для достаточности умножим равенство $as + bt = g$ на целое число c/g:

$$x_0 = s(c/g), \qquad y_0 = t(c/g).$$

Все решения имеют вид

$$x = x_0 + (b/g)k, \qquad y = y_0 - (a/g)k, \qquad k \in \mathbb{Z}.$$

Подстановка подтверждает, что любая такая пара — решение. Обратно, для двух решений $a(x - x_0) = -b(y - y_0)$. После деления на g и применения леммы о взаимно простом множителе получаем $(b/g) \mid (x - x_0)$; это и даёт указанную форму всех решений.

Пример. Для $240x + 46y = 14$ имеем $g = 2$, $s = -9$, $t = 47$. Одно решение: $x_0 = -63$, $y_0 = 329$. При $k = 3$ получаем более компактное решение $(6, -31)$: $1440 - 1426 = 14$. Уравнение $240x + 46y = 15$ решений не имеет, поскольку $2 \nmid 15$.

7.2 Обратное умножение по модулю

При $m > 1$ число u называется обратным к a по модулю m, если остаток au при делении на m равен 1. Это записывают как $au \equiv 1 \pmod m$. Полная теория сравнений будет изучаться далее; здесь достаточно определения через остаток.

Из равенства $as + mt = 1$ следует, что $u = s \bmod m$ — обратный элемент. Обратно, из $au = 1 + mq$ получается линейное представление единицы. Поэтому обратный существует **ровно при** $\gcd(a, m) = 1$; его единственного представителя выбирают в диапазоне $0 \le u < m$.

Для $a = 17, m = 3120$ расширенный алгоритм даёт

$$17(-367) + 3120 \cdot 2 = 1.$$

Отсюда $u = (-367) \bmod 3120 = 2753$. Проверка: $17 \cdot 2753 = 46801 = 15 \cdot 3120 + 1$. Такие вычисления используются при построении ключей RSA; устройство RSA и выбор параметров будут рассмотрены в последующих темах.

Для 240 по модулю 46 обратного нет: любое число вида $240u + 46v$ чётно и не может равняться 1. Нельзя просто взять коэффициент Безу по модулю, не проверив сначала, что НОД равен 1.

8 Закрепление и самостоятельная работа

1. Найдите НОД и НОК чисел 252 и 198. Выпишите все деления и представьте НОД как линейную комбинацию исходных чисел.
2. Докажите, что при $a \neq 0$ из $a \mid b$ следует $\gcd(a, b) = |a|$. Каков в этом случае НОК, если $b \neq 0$?
3. Решите в целых числах уравнение $35x + 22y = 1$. Найдите обратный к 35 по модулю 22.
4. Проверьте алгоритм для пары $(89, 55)$ и сопоставьте число делений с парой $(144, 89)$.
5. Докажите: если $as + bt = g > 0$, $g \mid a$ и $g \mid b$, то $g = \gcd(a, b)$. Почему без двух условий делимости одного равенства недостаточно?

Контрольные вопросы

1. Как определяется НОД? Какие соглашения приняты для нулевых аргументов?
2. Почему пары (a, b) и $(b, a - qb)$ имеют одинаковые общие делители?
3. Чем доказательство завершения алгоритма отличается от доказательства его корректности?
4. Какой остаток является НОД и почему нельзя брать последнюю нулевую строку?
5. В чём состоит тождество Безу? Единственны ли его коэффициенты?
6. Какой инвариант сохраняется в расширенном алгоритме Евклида?
7. Почему после деления обоих чисел на их НОД получаются взаимно простые числа?
8. Как связаны НОД, НОК и произведение исходных чисел?
9. Какую роль играют числа Фибоначчи в оценке числа делений?
10. Что именно оценивает теорема Ламе? Какой шаг обязательно включается в счёт?
11. Когда уравнение $ax + by = c$ разрешимо в целых числах?
12. При каком условии существует обратный к a по модулю $m > 1$?

Литература к теме

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии**. СПб.: Лань, 2020. §§ 3.1–3.2, с. 85–91: алгоритм Евклида, линейное представление НОД, взаимная простота и НОК.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory**. 2nd ed. Pearson Education, 2006. §§ 3.1.3–3.2: НОД, алгоритм Евклида и решение линейного уравнения.
3. Панкратова И. А. **Теоретико-числовые методы в криптографии**. 2009. § 1.6, с. 20–22: варианты алгоритма Евклида и бинарный алгоритм — для дополнительного чтения.

Нумерация источников в этой лекции локальная. Для самостоятельной подготовки вначале прочитайте §§ 3.1–3.2 Мартынова, затем воспроизведите таблицу расширенного алгоритма без обращения к готовому решению.