# ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

## Лекция 7

## МАЛАЯ ТЕОРЕМА ФЕРМА И ТЕОРЕМА ЭЙЛЕРА

| | |
|---|---|
| **Цель лекции** | Обосновать теоремы Ферма и Эйлера и научиться применять их для вычисления обратных вычетов и понижения показателей степеней. |
| **Результаты обучения** | Проверять условия теорем; доказывать теорему Эйлера через приведённую систему; находить обратные элементы; вычислять большие степени; объяснять ограничения теста Ферма. |
| **Предварительная подготовка** | Сравнения, НОД, обратимые классы вычетов, функция Эйлера и её вычисление по простым делителям. |

**Аудиторная нагрузка:** 1 академический час. Доказательства и основные примеры предназначены для занятия; дополнительные пояснения и задачи — для закрепления. Во всей лекции модуль $m \geq 2$, основание $a$ целое. Если не оговорено иное, показатель степени — неотрицательное целое число.

## План лекции

1. Обратимые вычеты и умножение приведённой системы.
2. Теорема Эйлера: формулировка, доказательство, пример.
3. Малая теорема Ферма и её следствие.
4. Нахождение обратного вычета с помощью степеней.
5. Понижение показателей и условия его корректности.
6. Двоичное возведение в степень и криптографический смысл.

## 1 От обратимых вычетов к степеням

В предыдущем блоке установлено: класс $[a]$ обратим в кольце $\mathbb{Z}_m$ тогда и только тогда, когда $\gcd(a, m) = 1$. Обратимые классы образуют множество $U(m)$; его мощность равна $\varphi(m)$. Для вычислений будем выбирать их наименьшие неотрицательные представители.

Например, $U(10)$ представлено числами $1,3,7,9$, поэтому $\varphi(10) = 4$. Если последовательно умножать обратимый класс на себя, среди его степеней появится единица. Теорема Эйлера указывает общий показатель, при котором это обязательно произойдёт.

**Лемма.** Если $\gcd(a, m) = 1$, то умножение на $a$ переставляет элементы любой приведённой системы вычетов по модулю $m$.

**Доказательство.** Произведение двух обратимых классов обратимо. Далее, из $ar_i \equiv ar_j \pmod m$ следует $r_i \equiv r_j \pmod m$: можно умножить обе части на обратный к $a$ класс. Поэтому различные элементы системы переходят в различные обратимые классы. Их число не изменилось и равно $\varphi(m)$; значит, получена та же система в другом порядке.

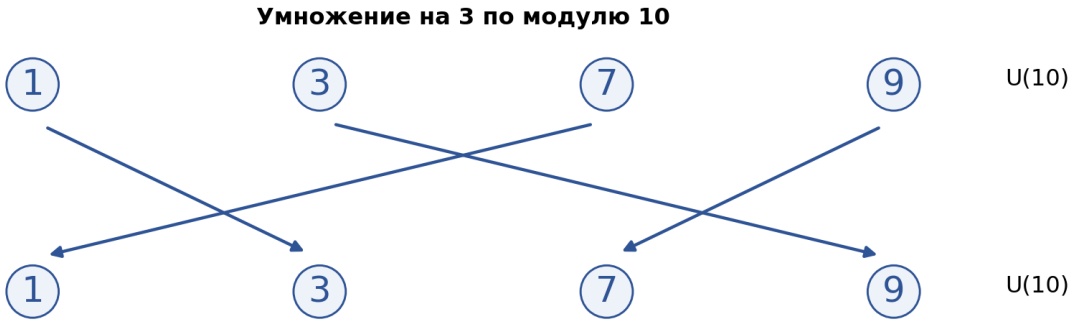



*Рисунок 1. Умножение на обратимый вычет сохраняет приведённую систему.*

Условие взаимной простоты существенно. При умножении тех же представителей на 2 получаем 2,6,4,8 — необратимые классы. Это уже не приведённая система по модулю 10.

## 2 Теорема Эйлера

**Теорема.** Для любого целого $a$ и натурального $m \geq 2$, таких что $\gcd(a, m) = 1$, выполняется

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

**Доказательство.** Обозначим представителей приведённой системы через $r_1, \dots, r_t$, где $t = \varphi(m)$. По лемме классы $ar_1, \dots, ar_t$ совпадают с исходными классами с точностью до порядка. Перемножим их:

$$\prod_{i=1}^{t} (ar_i) \equiv \prod_{i=1}^{t} r_i \pmod{m}.$$

Вынесение множителя $a$ из каждого сомножителя даёт

$$a^t P \equiv P \pmod{m}, \qquad P = \prod_{i=1}^{t} r_i.$$

Каждый $r_i$ взаимно прост с $m$, поэтому произведение $P$ тоже взаимно просто с $m$. Следовательно, $P$ обратимо, и обе части сравнения можно умножить на $P^{-1}$. Получаем $a^t \equiv 1 \pmod{m}$, что и требовалось доказать.

В доказательстве используется сокращение на **обратимое** произведение. Сокращать сравнение на произвольный ненулевой вычет нельзя: например, $2 \cdot 1 \equiv 2 \cdot 3 \pmod{4}$, но $1 \not\equiv 3 \pmod{4}$.

**Пример 1.** Для $m = 10$ и $a = 3$ произведение представителей равно $P = 1 \cdot 3 \cdot 7 \cdot 9 = 189$, причём $\gcd(189,10) = 1$. Из $3^4 P \equiv P \pmod{10}$ следует $3^4 \equiv 1 \pmod{10}$. Проверка: $3^4 = 81$.

**Пример 2.** Для $m = 40 = 2^3 \cdot 5$ имеем

$$\varphi(40) = 40(1 - 1/2)(1 - 1/5) = 16.$$

Поскольку $\gcd(7,40) = 1$, теорема гарантирует $7^{16} \equiv 1 \pmod{40}$. Однако показатель 16 не обязательно наименьший: уже $7^4 = 2401 \equiv 1 \pmod{40}$.

## 3 Малая теорема Ферма и её следствие

**Малая теорема Ферма.** Если $p$ — простое число и $p \nmid a$, то

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Доказательство.** Для простого $p$ все ненулевые классы обратимы, поэтому $\varphi(p) = p - 1$. Условие $p \nmid a$ равносильно $\gcd(a, p) = 1$. Подстановка этих сведений в теорему Эйлера даёт утверждение.

**Следствие.** Для простого $p$ и любого целого $a$ справедливо

$$a^{p} \equiv a \pmod{p}.$$

Если $p \nmid a$, умножаем сравнение из теоремы Ферма на $a$. Если $p \mid a$, обе части равны нулю по модулю $p$. Эти два случая охватывают все целые основания, включая отрицательные.

**Пример 3.** Для $p = 7$, $a = 14$ равенство $14^7 \equiv 14 \equiv 0 \pmod{7}$ верно. Но утверждение $14^6 \equiv 1 \pmod{7}$ неверно: левая часть равна 0. В двух формулировках различаются условия на основание.

**Пример 4.** Вычислим $5^{12345} \bmod 17$. Простота 17 и $17 \nmid 5$ позволяют использовать показатель 16. Делим показатель с остатком:

$$12345 = 771 \cdot 16 + 9, \qquad 5^{12345} \equiv 5^9 \pmod{17}.$$

Последовательные квадраты дают $5^2 \equiv 8$, $5^4 \equiv 13$, $5^8 \equiv 16 \pmod{17}$. Значит, $5^9 \equiv 16 \cdot 5 \equiv 12 \pmod{17}$. Здесь показатель сокращается по модулю 16, а значения степеней — по модулю 17.

### 3.1 Почему обратное утверждение неверно

Пусть $n > 1$, $1 < a < n$ и $\gcd(a, n) = 1$. Если $a^{n-1} \not\equiv 1 \pmod{n}$, то $n$ составное: при простом $n$ теорема Ферма была бы нарушена. Основание $a$ в этом случае называют свидетелем составности.

Если же сравнение выполнено, простота ещё не доказана. Например,

$$341 = 11 \cdot 31, \qquad 2^{10} = 1024 = 3 \cdot 341 + 1.$$

Поэтому $2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}$, хотя 341 составное. Это пример псевдопростого числа по основанию 2. Следовательно, успешная проверка одного такого сравнения не является критерием простоты. Если предварительно обнаружен НОД строго между 1 и $n$, составность уже установлена без возведения в степень.

## 4 Нахождение обратного вычета

### 4.1 Формулы Эйлера и Ферма

При $\gcd(a, m) = 1$ теорему Эйлера можно переписать как

$$a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}.$$

По определению обратного элемента отсюда следует

$$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}.$$

Если модуль $p$ прост и $p \nmid a$, то получаем частный случай

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

Обозначение $a^{-1}$ означает обратный **класс по указанному модулю**; оно не означает обычную дробь $1/a$. При $p = 2$ показатель $p - 2$ равен нулю. Для нечётного $a$ формула по-прежнему верна: единственный ненулевой класс равен единице и обратен самому себе.

**Пример 5.** Найдём обратный вычет к $a = -13$ по модулю 60. Сначала $a \equiv 47 \pmod{60}$ и $\gcd(47,60) = 1$. Поскольку $60 = 2^2 \cdot 3 \cdot 5$, имеем $\varphi(60) = 16$. Значит, достаточно вычислить $47^{15}$.

Последовательные квадраты по модулю 60: $47^2 \equiv 49$, $47^4 \equiv 1$, $47^8 \equiv 1$. Так как $15 = 8 + 4 + 2 + 1$, получаем

$$47^{15} \equiv 1 \cdot 1 \cdot 49 \cdot 47 \equiv 23 \pmod{60}.$$

Проверка исходного отрицательного числа: $(-13) \cdot 23 = -299 = 1 - 5 \cdot 60$. Искомый наименьший неотрицательный представитель равен 23.

### 4.2 Как выбрать способ вычисления

| Способ | Какие данные нужны | Как проверить результат $b$ |
|---|---|---|
| Расширенный алгоритм Евклида | Числа $a, m$; разложение $m$ не требуется | Проверить $ab \equiv 1 \pmod{m}$ |
| Теорема Эйлера | НОД 1 и известное $\varphi(m)$ | Вычислить $a^{\varphi(m)-1}$ и проверить произведение |
| Малая теорема Ферма | Простой модуль $p$ и $p \nmid a$ | Вычислить $a^{p-2}$ и проверить произведение |

Формула Эйлера особенно удобна, когда значение функции уже известно. Если разложение большого составного модуля неизвестно, сначала находить его лишь ради обратного элемента обычно не требуется: расширенный алгоритм Евклида получает обратный элемент непосредственно. При НОД больше 1 ни одна из степенных формул не создаёт обратного элемента — его не существует.

## 5 Понижение показателя степени

### 5.1 Основное правило и доказательство

Если $\gcd(a, m) = 1$ и $n = q\varphi(m) + r$, где $0 \le r < \varphi(m)$, то

$$a^n = (a^{\varphi(m)})^q a^r \equiv a^r \pmod{m}.$$

Таким образом, показатель можно заменить остатком от деления на $\varphi(m)$. Для простого модуля и ненулевого основания используется остаток по модулю $p - 1$. Если остаток показателя равен 0, получается $a^0 = 1$; условие обратимости уже гарантирует корректность такого перехода.

**Пример 6.** Вычислим $7^{2026} \bmod 40$. НОД равен 1, $\varphi(40) = 16$, $2026 = 126 \cdot 16 + 10$. Следовательно,

$$7^{2026} \equiv 7^{10} \equiv 7^8 \cdot 7^2 \equiv 1 \cdot 9 \equiv 9 \pmod{40}.$$

Мы использовали $7^2 \equiv 9$ и $7^4 \equiv 1 \pmod{40}$. Можно сразу сократить показатель по модулю 4, **после** проверки последнего равенства: $2026 \equiv 2 \pmod{4}$.

## 5.2 Наименьший период

Для обратимого класса наименьшее положительное $t$, при котором $a^t \equiv 1 \pmod m$, называется его порядком и обозначается $\mathrm{ord}_m(a)$. Существование такого $t$ следует из теоремы Эйлера. Любой показатель $N$ с $a^N \equiv 1$ делится на $t$: если $N = qt + r$, $0 \le r < t$, то $a^r \equiv 1$, а минимальность $t$ вынуждает $r = 0$.

В частности, $\mathrm{ord}_m(a)$ делит $\varphi(m)$. Степени можно сокращать по модулю этого меньшего периода. Например, $3 \not\equiv 1 \pmod 8$, но $3^2 \equiv 1 \pmod 8$. Поэтому порядок 3 по модулю 8 равен 2, хотя $\varphi(8) = 4$.

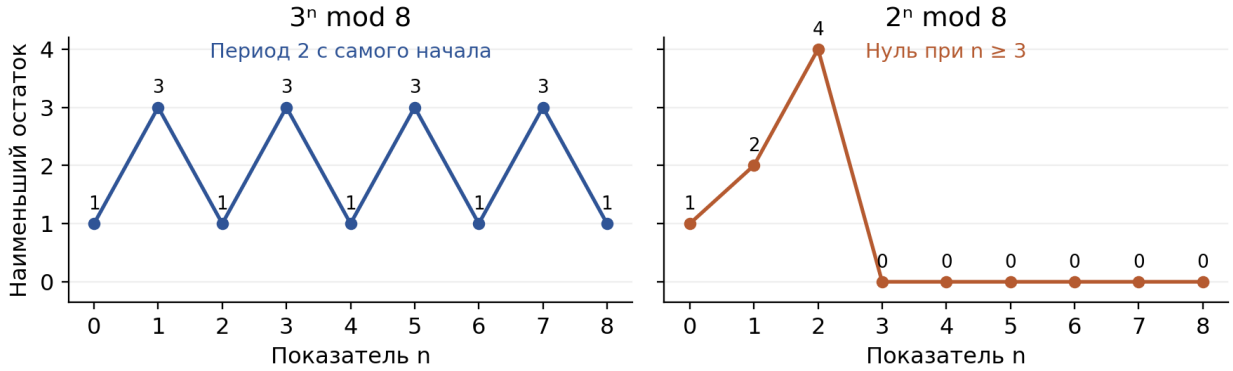



*Рисунок 2. У обратимого основания период начинается с единицы; у необратимого такой вывод делать нельзя.*

## 5.3 Необратимое основание и отрицательный показатель

Условие НОД 1 нельзя опускать. По модулю 8 значение $\varphi(8) = 4$, но для основания 2 ошибочное сокращение показателя дало бы

$$2^4 \not\equiv 2^{\,4 \bmod 4} = 2^0 \pmod 8, \qquad 0 \not\equiv 1 \pmod 8.$$

Если основание необратимо, неотрицательную степень всегда можно вычислять двоичным алгоритмом без применения теоремы Эйлера. Иногда помогают особенности конкретного основания: например, $6^2 \equiv 6 \pmod{15}$, поэтому $6^n \equiv 6 \pmod{15}$ при всех $n \ge 1$; это отдельное обоснование, а не применение теоремы Эйлера.

Отрицательная степень по модулю определяется только для обратимого класса: при $k > 0$ полагают $a^{-k} = (a^{-1})^k$. После такого определения сокращение целого показателя по периоду также корректно. Например, $7^{-1} \equiv 23 \pmod{40}$, а запись $2^{-1} \pmod 8$ не определяет обратимого вычета.

# 6 Как вычислять оставшуюся степень

Двоичное возведение в степень применимо к любому целому основанию, модулю $m \ge 2$ и показателю $n \ge 0$. Оно не требует взаимной простоты. Сначала устанавливают $R = 1$, $B = a \bmod m$, $e = n$. Пока $e > 0$, выполняют три действия в указанном порядке:

1. Если $e$ нечётно, заменить $R$ на $RB \bmod m$.
2. Заменить $B$ на $B^2 \bmod m$.
3. Заменить $e$ на целую часть $e/2$.

Когда $e = 0$, результат равен $R$. Объяснение даёт инвариант $RB^e \equiv a^n \pmod m$ перед каждой итерацией. При чётном $e = 2u$ произведение превращается в $R(B^2)^u$. При нечётном $e = 2u + 1$ оно превращается в $(RB)(B^2)^u$. Поэтому инвариант сохраняется в обоих случаях.

**Пример 7.** Вычисление $7^{13} \bmod 40$ без предварительного понижения показателя. В каждой строке показано состояние **после** полной итерации; первая строка — начальное состояние.

| **Состояние** | $e$ | $R$ | $B$ | **Действие с** $R$ |
|---|---|---|---|---|
| Начало | 13 | 1 | 7 | Пока без изменения |
| После шага 1 | 6 | 7 | 9 | $1 \cdot 7 \bmod 40 = 7$ |
| После шага 2 | 3 | 7 | 1 | Чётный показатель: $R$ прежнее |
| После шага 3 | 1 | 7 | 1 | $7 \cdot 1 \bmod 40 = 7$ |
| После шага 4 | 0 | 7 | 1 | $7 \cdot 1 \bmod 40 = 7$ |

Для положительного $n$ число итераций равно количеству его двоичных разрядов. На итерации нужно не более двух умножений по модулю, поэтому число модульных умножений имеет порядок $O(\log n)$. Это оценка количества операций, а не полная оценка битовой сложности: стоимость умножения зависит от размера модуля. В Python вычисление с теми же входами записывается как `pow(7, 13, 40)` и даёт 7.

## 7 Связь с криптографическими преобразованиями

Теоремы объясняют, почему степенное преобразование обратимых вычетов иногда можно обратить другой степенью. Пусть $\gcd(e, \varphi(m)) = 1$, а $d$ найден из $ed \equiv 1 \pmod{\varphi(m)}$. Тогда $ed = 1 + k\varphi(m)$ при подходящем целом $k$, и для обратимого $x$ выполняется

$$(x^e)^d = x^{ed} \equiv x \pmod{m}.$$

Например, при $m = 55$ значение функции равно 40. Показатель $e = 3$ имеет обратный $d = 27$ по модулю 40, поскольку $3 \cdot 27 = 81 \equiv 1 \pmod{40}$. Для $x = 7$ получаем $y = 7^3 \bmod 55 = 13$ и $y^{27} \bmod 55 = 7$.

Здесь основание и результат вычисляются по модулю 55, а взаимная обратимость **показателей** проверяется по модулю 40. Это математическая предпосылка изучения степенных криптосистем. Доказанное в этом разделе утверждение относится к $x \in U(m)$; для необратимых классов требуется отдельное рассуждение. Небольшие числа в примере служат только для разбора арифметики.

## 8 Закрепление и самостоятельная работа

1. Вычислите $3^{2027} \bmod 10$, объяснив, по какому модулю сокращён показатель.
2. Вычислите $5^{2026} \bmod 13$ с помощью малой теоремы Ферма и последовательных квадратов.
3. Найдите обратный вычет к 7 по модулю 40 и к $-7$ по модулю 23 с помощью степенных формул. Проверьте оба произведения.
4. Вычислите $6^{100} \bmod 15$. Объясните, почему сокращение показателя по модулю $\varphi(15)$ недопустимо; покажите отдельный контрпример на показателе 8.
5. Найдите $\mathrm{ord}_{21}(5)$ и затем $5^{2026} \bmod 21$. Сопоставьте найденный порядок с $\varphi(21)$.
6. Докажите, что число 341 проходит проверку Ферма по основанию 2, хотя является составным. Сформулируйте корректный вывод из успешной и неуспешной проверки.

## Контрольные вопросы

1. Какие классы входят в $U(m)$ и почему их количество равно $\varphi(m)$?
2. Почему умножение на взаимно простой с модулем элемент переставляет приведённую систему?
3. На каком основании в доказательстве Эйлера сокращается произведение представителей?
4. Сформулируйте малую теорему Ферма и объясните её связь с теоремой Эйлера.
5. Почему сравнение $a^p \equiv a \pmod p$ верно и при $p \mid a$?
6. Как получить формулы обратного вычета из теорем Эйлера и Ферма?
7. Почему показатель сокращают по модулю $\varphi(m)$, а не по модулю $m$?
8. Когда показатель можно сократить по модулю меньшего числа, чем $\varphi(m)$?
9. Что нарушается при применении теоремы Эйлера к необратимому основанию?
10. Какой инвариант обосновывает двоичное возведение в степень?
11. Почему успешная проверка Ферма не доказывает простоту?
12. В каком смысле используется отрицательная степень по модулю?

## Литература


1. Мартынов Л. М. **Алгебра и теория чисел для криптографии.** 2020. Раздел 4.3, особенно п. 4.3.2–4.3.3: приведённые системы, теоремы Эйлера и Ферма; §12.1 — связь с порядком конечной группы.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory.** 2nd ed. 2006. §3.5 — модульное возведение в степень; §3.6 — теоремы Ферма и Эйлера и понижение показателей.


Изложение, вычислительные примеры и иллюстрации подготовлены для данной дисциплины по предоставленным изданиям. Формулы и условия сформулированы явно, без воспроизведения опечаток сканированных источников.