ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 15

Числа Кармайкла и алгоритмы арифметики

Тема 15 по рабочей программе: числа Кармайкла; алгоритмы определения простоты числа, умножения и возведения в степень. **Аудиторная нагрузка:** 1 академический час. Конспект содержит расширенные объяснения и доказательства для самостоятельного изучения.

Цель лекции: объяснить ограничения проверки Ферма и показать, как свойства остатков определяют корректность и трудоёмкость алгоритмов проверки простоты и целочисленной арифметики.

После изучения темы студент должен уметь: применять критерий Корсельта; различать псевдопростое число по одному основанию и число Кармайкла; объяснять раунд Миллера — Рабина; выполнять шаг умножения Карацубы и двоичное возведение в степень с подсчётом операций.

Предварительная подготовка: факторизация, НОД, китайская теорема об остатках, малая теорема Ферма, порядок элемента и первообразный корень по простому модулю; материал лекции 14 о проверке простоты.

План лекции

1. Псевдопростые числа и критерий Корсельта.
2. Числа Кармайкла в проверках Ферма и Миллера — Рабина.
3. Точные и вероятностные алгоритмы определения простоты.
4. Умножение в столбик и алгоритм Карацубы.
5. Двоичное возведение в степень: корректность и стоимость.

Распределение 45 минут: постановка задачи — 3 минуты; числа Кармайкла — 12; проверка простоты — 8; умножение — 9; возведение в степень — 11; вопросы — 2. Подробное доказательство критерия, полный перебор оснований и программные реализации выносятся также на самостоятельное изучение.

1 Почему обратное утверждение теоремы Ферма неверно

Для простого числа p и целого основания a, не делящегося на p, малая теорема Ферма утверждает:

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

Если для некоторого $n > 1$ это сравнение не выполняется, число составное. Но из выполнения сравнения простота не следует. **Псевдопростым по основанию** a называют составное число n, взаимно простое с a, для которого выполняется сравнение Ферма.

Пример 1. Число $341 = 11 \cdot 31$ составное, но $2^{10} = 1024 \equiv 1 \pmod{341}$. Поскольку 340 кратно 10, проверка Ферма по основанию 2 принимает 341. Здесь найдено основание, скрывающее составность; универсальное утверждение обо всех основаниях ещё не получено.

Определение. Число Кармайкла — составное положительное целое число n, для которого

$$a^{n-1} \equiv 1 \pmod{n} \qquad \text{при каждом } a \text{ с } \gcd(a,n) = 1.$$

Условие взаимной простоты обязательно. Например, 561 является числом Кармайкла, однако $3^{560} \bmod 561 = 375$. Основание 3 не входит в мультипликативную группу обратимых остатков: уже вычисление НОД обнаруживает делитель.

Перебирать все основания для больших чисел неудобно. Следующий критерий заменяет перебор проверкой свойств простых множителей. Он предполагает, что факторизация известна, поэтому сам по себе не служит быстрым способом получения этой факторизации.

2 Критерий Корсельта

Теорема. Составное число n является числом Кармайкла тогда и только тогда, когда выполнены два условия:

1. Число свободно от квадратов: никакой квадрат простого числа его не делит.
2. Для каждого простого делителя p числа n выполняется $p - 1 \mid n - 1$.

2.1 Достаточность

Пусть $n = p_1 \cdots p_r$, где простые множители различны, и каждый показатель $p_i - 1$ делит $n - 1$. Если основание взаимно просто с n, оно взаимно просто с каждым простым множителем. По теореме Ферма и условию делимости получаем

$$a^{n-1} = (a^{p_i-1})^{(n-1)/(p_i-1)} \equiv 1 \pmod{p_i}.$$

Следовательно, все различные простые множители делят разность $a^{n-1} - 1$. Их произведение тоже делит эту разность. Это требуемое сравнение по модулю n.

2.2 Необходимость: отсутствие квадратных делителей

Пусть n — число Кармайкла. Предположим, что p^e входит в его факторизацию с показателем $e \geq 2$, и обозначим $u = n/p$. Основание $a = 1 + u$ взаимно просто с n: по модулю каждого простого делителя оно равно 1. При этом u делится на p^{e-1}, но не на p^e.

В разложении бинома все слагаемые, содержащие квадрат или более высокую степень u, делятся на p^e. Поэтому

$$(1 + u)^{n-1} \equiv 1 + (n - 1)u \pmod{p^e}.$$

Число $n - 1$ не делится на p. Значит, линейное слагаемое не делится на p^e, и полученный остаток отличен от 1. Возникло противоречие с определением. Следовательно, повторных простых множителей нет.

2.3 Необходимость: делимость показателей

Зафиксируем простой делитель p и первообразный корень g по модулю p. Для $p = 2$ условие делимости очевидно. По китайской теореме об остатках можно выбрать целое a, равное g по модулю p и равное 1 по модулю остальных простых делителей. Оно взаимно просто с n.

Из определения числа Кармайкла следует $g^{n-1} \equiv 1 \pmod{p}$. Порядок первообразного корня равен $p - 1$, а порядок элемента делит любой показатель, дающий единицу. Таким образом, $p - 1$ делит $n - 1$. Необходимость обоих условий доказана.

2.4 Следствия и примеры

Следствие 1. Все числа Кармайкла нечётны. Если бы свободное от квадратов составное число было чётным, у него имелся бы нечётный простой делитель. Тогда чётное число $p-1$ должно было бы делить нечётное число $n-1$, что невозможно.

Следствие 2. Число Кармайкла имеет не менее трёх различных простых делителей. Для двух множителей $n=pq$, где $p<q$, условие $q-1 \mid pq-1$ влечёт $q-1 \mid p-1$. Это невозможно, поскольку $0<p-1<q-1$.

Таблица 1. Проверка условий критерия на характерных числах.

n	Факторизация	Проверка	Вывод
561	$3\cdot 11\cdot 17$	Кратности 1; все деления без остатка	Число Кармайкла
1729	$7\cdot 13\cdot 19$	Кратности 1; все деления без остатка	Число Кармайкла
341	$11\cdot 31$	340 не делится на 30	Не Кармайкла
169	13^2	Есть квадратный делитель	Не Кармайкла
97	97	Число простое	Не Кармайкла

Для 561 числа 2, 10 и 16 делят 560; для 1729 числа 6, 12 и 18 делят 1728. Оба числа свободны от квадратов и составны. Число 169 показывает, почему нельзя опускать первое условие, а число 97 — почему в формулировке необходимо слово «составное».

Ещё одна форма определения. Для числа Кармайкла выполняется

$$a^n \equiv a \pmod{n} \qquad \text{для каждого целого } a.$$

Действительно, по каждому простому делителю либо основание равно нулю, либо можно применить теорему Ферма. Затем сравнения объединяются по китайской теореме. Обратно, для взаимно простого основания можно сократить на его обратимый остаток. Здесь переход к формуле для всех оснований обоснован свободой от квадратов, а не незаконным сокращением необратимого элемента.

3 Как Миллер — Рабин обнаруживает числа Кармайкла

Пусть $n \geq 5$ нечётно. Записываем $n-1=2^s d$, где d нечётно. Для основания из диапазона от 2 до $n-2$ сначала проверяем НОД. Нетривиальный НОД сразу доказывает составность. В остальных случаях вычисляем цепочку

$$x_0 = a^d \bmod n, \qquad x_{j+1} = x_j^2 \bmod n.$$

Раунд пройден, если $x_0 = 1$ либо в цепочке с индексами от 0 до $s-1$ встретилось $n-1$. В иных случаях число составное. Возникновение единицы после остатка, отличного от обоих знаков единицы, позволяет завершить раунд с отрицательным ответом сразу.

Для простого модуля сравнение $z^2 \equiv 1$ имеет лишь два решения: 1 и -1. Действительно, простое число делит произведение $(z-1)(z+1)$, значит, делит один из множителей. В цепочке последовательных квадратов первая единица поэтому должна появиться либо сразу, либо вслед за -1. Именно это дополнительное условие усиливает проверку Ферма.

Пример 2. Для $n=561$ получаем $560=2^4\cdot 35$. При основании 2 цепочка имеет вид

$$263 \to 166 \to 67 \to 1 \pmod{561}.$$

Ни один остаток не равен 560, начальный остаток не равен 1. Число отвергается, хотя заключительное сравнение Ферма выполняется. Остаток 67 — нетривиальный квадратный корень из единицы. Из него получаем делители:

$$\gcd(67 - 1{,}561) = 33, \qquad \gcd(67 + 1{,}561) = 17.$$

Делитель 33 ещё составной. Свидетельство Миллера — Рабина иногда помогает найти множители таким способом, но не каждый отрицательный раунд обязательно предъявляет нетривиальный корень из единицы.

Почему корней больше двух? Для произведения трёх различных нечётных простых модулей каждый набор знаков единицы по этим модулям задаёт единственный остаток. Для 561 получается восемь корней: 1, 67, 188, 254, 307, 373, 494, 560. Это конкретное проявление китайской теоремы об остатках.

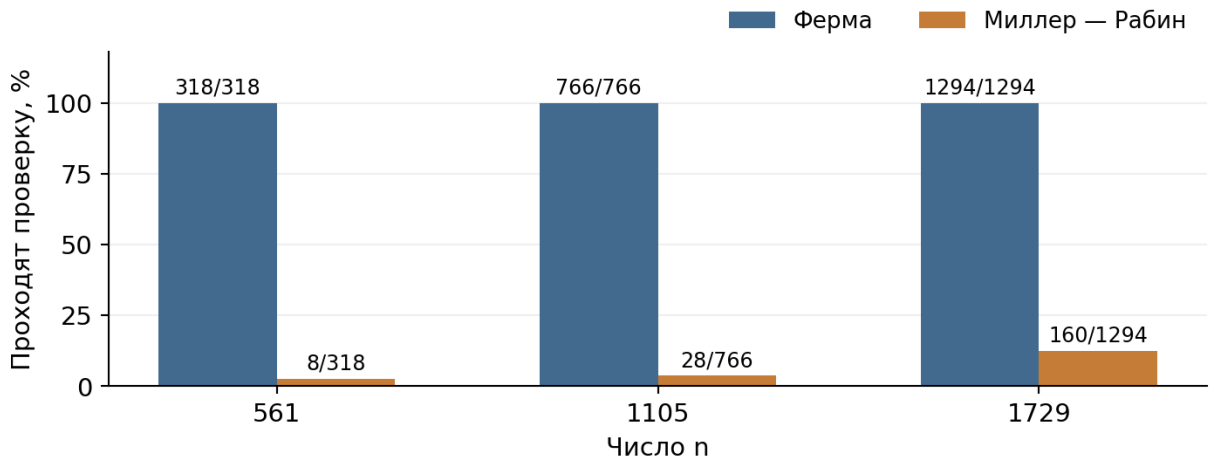


Рисунок 1. Точный перебор взаимно простых оснований от 2 до n − 2; над столбцами указаны количества прошедших и общее количество оснований.

В рисунке исключены тривиальные основания 1 и $n - 1$. Для 561 знаменатель равен $\varphi(561) - 2 = 318$: проверку Ферма проходят 318 оснований, сильную проверку — 8. Здесь показаны результаты полного конечного перебора, а не частоты случайной выборки.

4 Какие выводы дают алгоритмы проверки простоты

Для любого фиксированного нечётного составного числа доля оснований, пропускающих его в раунде Миллера — Рабина при равномерном выборе из диапазона от 2 до $n - 2$, не превосходит одной четверти. При независимых повторениях получаем

$$\Pr(\text{все } k \text{ раундов пройдены} \mid n \text{ составное}) \leq 4^{-k}.$$

Например, 40 независимых раундов дают верхнюю границу 2^{-80}. Основания должны выбираться заново и равномерно; повторение одного и того же основания не создаёт независимых проверок. Для заранее заданных оснований 2 и 3 эта общая вероятностная формула не является обоснованием результата.

Условная вероятность пропустить **заранее фиксированное составное число** не равна автоматически вероятности составности случайно сгенерированного кандидата после принятия. Во втором вопросе необходимо учитывать распределение кандидатов. Также нельзя смешивать знаменатель по всем разрешённым основаниям с подмножеством взаимно простых оснований рисунка 1.

Таблица 2. Характер результата разных подходов.

Метод	Результат	Особенность
Пробные деления	Точная простота или делитель	Перебор до квадратного корня; дорог для больших чисел
Проверка Ферма	Свидетельство составности либо прохождение	Числа Кармайкла проходят по всем взаимно простым основаниям
Миллер — Рабин	Составность либо прохождение раундов	Вероятностная граница при независимом равномерном выборе
Сертификат простоты	Доказательство при успешной проверке	Нужно проверить все условия сертификата; см. лекцию 14
AKS	Детерминированная проверка простоты	Полиномиальность по длине входа; обзор теоретического результата

Алгоритм AKS показывает, что простоту можно определить детерминированно за время, полиномиальное по двоичной длине числа. В данной теме используется только этот теоретический результат; полная конструкция и её доказательство выходят за пределы одного занятия. Проверка отдельного полиномиального сравнения без остальных условий AKS не заменяет алгоритм.

Проверка простоты, полная факторизация и распознавание числа Кармайкла — связанные, но разные задачи. Для применения критерия Корсельта в нашем практикуме факторизацию получают пробными делениями, поскольку числа небольшие.

5 Алгоритмы умножения

5.1 Умножение в столбик и длина входа

Если оба числа имеют не более L разрядов в фиксированной системе счисления, умножение в столбик вычисляет попарные произведения цифр и выполняет переносы. Получается $O(L^2)$ элементарных операций над цифрами; для двоичных чисел это квадратичная битовая оценка.

Разобьём числа на старшую и младшую части в основании B:

$$x = x_1 B + x_0, \qquad y = y_1 B + y_0.$$

Раскрытие скобок даёт четыре произведения частей. Простое рекурсивное применение этой формулы сохраняет квадратичный порядок трудоёмкости: уменьшение размера задачи компенсируется четырьмя рекурсивными вызовами.

5.2 Идея Карацубы

Средний коэффициент можно восстановить через сумму частей. Достаточно вычислить три произведения:

$$z_0 = x_0 y_0, \qquad z_2 = x_1 y_1, \qquad h = (x_0 + x_1)(y_0 + y_1).$$

После этого выполняются сложения, вычитания и разрядные сдвиги:

$$z_1 = h - z_0 - z_2, \qquad xy = z_2 B^2 + z_1 B + z_0.$$

Равенство следует непосредственно из раскрытия произведения, определяющего h. Для учебной рекурсивной версии индукцию проводят по наибольшему из двух множителей: при разбиении он уменьшается в каждой подзадаче, включая произведение сумм. Базовый

случай вычисляется непосредственно; меньшие произведения верны по предположению индукции; формула сборки возвращает нужный результат.

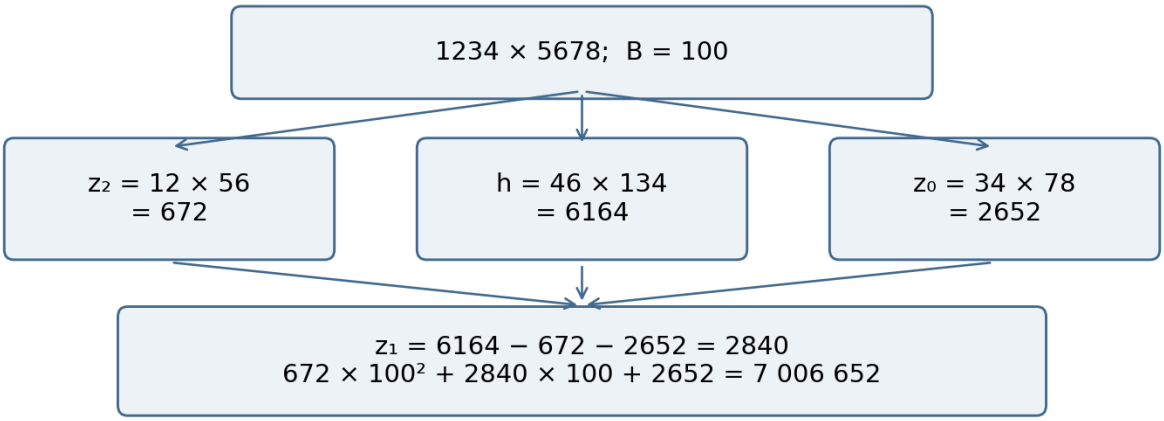


Рисунок 2. Разбиение на две части в основании 100 и сборка результата.

Для сбалансированного разбиения характерная рекуррентность имеет вид $T(L) = 3T(L/2) + O(L)$, если временно опустить округления. Она приводит к оценке

$$T(L) = O(L^{\log_2 3}) \approx O(L^{1.585}).$$

Суммы половин могут иметь на один разряд больше; эта поправка не меняет асимптотический порядок. Её учитывают при строгом анализе либо используют вариант с разностями. Для небольших чисел накладные расходы рекурсии могут превысить выигрыш, поэтому асимптотическая оценка не обещает ускорения каждого отдельного умножения.

Три произведения многозначных частей нельзя напрямую сравнивать с шестнадцатью произведениями отдельных цифр: это операции разного размера. В практикуме отдельно фиксируются уровень разбиения и выбранная единица подсчёта.

6 Двоичное возведение в степень по модулю

6.1 Алгоритм слева направо

Требуется найти остаток $a^e \bmod m$ при целых $e \geq 0$ и $m \geq 1$. Для положительного показателя выписываем двоичную запись, начинающуюся с единицы. Начальное значение — $r = a \bmod m$. Далее обрабатываем остальные биты слева направо: возводим текущий остаток в квадрат и, если очередной бит равен 1, дополнительно умножаем на основание. После каждой операции берём остаток по модулю.

Инвариант. После обработки двоичного префикса со значением v текущий остаток сравним с a^v. Добавление бита b меняет значение префикса на $2v + b$. Обновление алгоритма даёт

$$r_{\text{new}} \equiv r^2 a^b \equiv a^{2v+b} \pmod{m}.$$

Инвариант сохраняется. После последнего бита префикс равен всему показателю, поэтому результат верен. Для нулевого показателя сразу возвращается $1 \bmod m$; это также обрабатывает модуль 1. В учебной реализации отрицательные показатели отклоняются.

6.2 Пример и точное число операций

Пример 3. Вычислим $7^{181} \bmod 561$. Двоичная запись показателя — 10110101. Начальный остаток равен 7; дальнейшие вычисления приведены в таблице.

Префикс	Остаток квадрата	После обработки бита
1	—	7
10	49	49
101	157	538
1011	529	337
10110	247	247
101101	421	142
1011010	529	529
10110101	463	436

Получен остаток 436. Пусть t — длина двоичной записи положительного показателя, а $w(e)$ — число единичных битов. В описанной реализации начальная единица уже учтена присваиванием, поэтому

$$S = t - 1, \qquad M = w(e) - 1, \qquad S + M = t + w(e) - 2.$$

Здесь S — число возведений в квадрат, M — число дополнительных умножений на основание. Для показателя 181 получаем 7 квадратов и 4 дополнительных умножения, всего 11 операций вместо 180 при последовательном умножении с начальным значением a.

Формула относится именно к данной реализации. Алгоритм, начинающий с 1 и обрабатывающий все биты, может выполнять дополнительные операции. Для показателя $65537 = 2^{16} + 1$ наша схема выполняет 16 квадратов и одно умножение, всего 17 операций.

6.3 Стоимость модульной арифметики

Если модуль имеет L битов, остатки занимают не более L битов, но перед редукцией произведение может занимать до $2L$ битов. Обозначим через $C_{\mathrm{mod}}(L)$ стоимость умножения **вместе с получением остатка**. Тогда для показателя длины t оценка имеет вид

$$O(t\, C_{\mathrm{mod}}(L)).$$

При школьной арифметике умножение и деление с остатком имеют квадратичную стоимость. Для показателя длины порядка L получается $O(L^3)$ битовых операций; это же даёт стандартную оценку одного раунда Миллера — Рабина. Замена лишь умножения на Карацубу ещё не обосновывает улучшение всей оценки: необходимо учитывать и алгоритм редукции.

Модульная степень не требует взаимной простоты основания и модуля. Такая предпосылка появляется при сокращении показателя по теореме Эйлера. Нельзя произвольно заменять показатель его остатком по модулю m или применять теорему Ферма к составному модулю.

Упражнения для закрепления

1. Примените критерий Корсельта к числам 561, 341 и 169. Для каждого укажите решающее условие.

2. Для 1729 выполните раунд Миллера — Рабина по основанию 2. Если возник нетривиальный квадратный корень из единицы, извлеките делители через НОД.
3. Найдите все решения сравнения $z^2 \equiv 1 \pmod{561}$ и сопоставьте их тройкам знаков по модулям 3, 11 и 17.
4. Вычислите произведение 2345 и 6789 одним шагом Карацубы в основании 100. Покажите все три произведения и сборку.
5. Вычислите $5^{117} \bmod 97$ алгоритмом слева направо. Запишите цепочку остатков и точное число операций.
6. Объясните ошибку сокращения показателя по модулю самого модуля на примере $2^6 \bmod 5$. Сравните число операций для показателя 65537 в двоичной и последовательной схемах.

Контрольные вопросы

1. Чем число Кармайкла отличается от псевдопростого по одному основанию?
2. Почему в определении указаны составность и взаимная простота основания с модулем?
3. Какие условия содержит критерий Корсельта и где используется каждое из них?
4. Почему число Кармайкла не может быть чётным или произведением двух простых?
5. Что позволяет Миллеру — Рабину отвергнуть число, проходящее проверку Ферма?
6. При каких предпосылках верна оценка вероятности ошибки нескольких раундов?
7. В чём состоит теоретический результат AKS?
8. Как в алгоритме Карацубы четыре произведения заменяются тремя?
9. Каков инвариант двоичного возведения в степень и почему счётчик зависит от реализации?
10. Почему при оценке сложности нельзя забывать стоимость редукции по модулю?

Литература и источники

1. Katz J., Lindell Y. *Introduction to Modern Cryptography*. 2nd ed. CRC Press, 2015. Гл. 8, с. 307–310: проверка простоты и числа Кармайкла; приложение B, с. 553–555: модульная степень. Использовано предоставленное издание; точные счётчики в лекции относятся к указанной здесь реализации.
2. Trappe W., Washington L. C. *Introduction to Cryptography with Coding Theory*. 2nd ed. Pearson, 2006. § 3.13, упражнение 16, с. 105–106: число 1729; § 6.3, с. 176–179: проверка простоты. Использована предоставленная книга.
3. Shoup V. *A Computational Introduction to Number Theory and Algebra*. Version 2.1, 2008. § 10.1, теорема 10.2, с. 306: структура чисел Кармайкла. Текст на сайте автора.
4. Erickson J. *Algorithms*. 2019. § 1.9, с. 39–42: быстрое умножение. Глава на сайте автора. Соответствует тематике предоставленного русского издания «Алгоритмы» 2023 года; страницы указаны для английского оригинала.
5. Agrawal M., Kayal N., Saxena N. *PRIMES is in P*. Annals of Mathematics, 160 (2004), 781–793. Статья; исправление доказательства, 2019. Использован только результат о детерминированной полиномиальной проверке простоты.