ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 11

Сравнения высших степеней и поднятие корней

Тема 11. Сравнения высших порядков. Сведение к сравнениям по модулям степеней простых чисел. Поднятие решения по модулю простого числа до решения по модулю его степени.

Объём: 1 академический час. **Цель:** научиться описывать все корни многочлена по составному модулю через корни по простым степеням и понимать, почему при поднятии корень может продолжиться единственным способом, разветвиться или исчезнуть.

После изучения темы студент должен уметь вывести формулу одного шага поднятия, различать простой и особый корень, обосновать полноту найденного множества решений и восстановить решение по китайской теореме об остатках. Используются делимость, производная многочлена, обратный элемент и КТО. Раздел 5 предназначен также для самостоятельного изучения и практической работы 11.

1 От общего модуля к простым степеням

Пусть $f(x) = c_0 + c_1 x + \cdots + c_d x^d$ — многочлен с целыми коэффициентами, а $m \geq 2$. Решить сравнение $f(x) \equiv 0 \pmod{m}$ означает найти все классы вычетов x по модулю m, при подстановке которых значение многочлена делится на m. В качестве ответов будем выбирать представителей $0 \leq x < m$.

Название «сравнение высшей степени» относится к степени многочлена. Степень простого числа в модуле — другой параметр: например, $x^3 - 1 \equiv 0 \pmod{7^2}$ имеет степень 3 и модуль, являющийся второй степенью простого числа.

Пусть известно каноническое разложение модуля:

$$m = \prod_{i=1}^{r} p_i^{e_i}.$$

Теорема 1. Решения $f(x) \equiv 0 \pmod{m}$ взаимно однозначно соответствуют наборам решений $f(x_i) \equiv 0 \pmod{p_i^{e_i}}$. Поэтому число решений по модулю m равно произведению чисел решений по простым степеням.

Доказательство. Если m делит $f(x)$, каждое $p_i^{e_i}$ также делит $f(x)$. Обратно, из делимости $f(x)$ на все попарно взаимно простые множители следует делимость на их произведение. КТО устанавливает взаимно однозначное соответствие между классом x по модулю m и набором его остатков по простым степеням. Многочлен сохраняет сравнимость аргументов, поэтому КТО применима к любому выбранному набору местных корней. Если хотя бы одно местное множество пусто, исходное сравнение неразрешимо. ■

Таким образом, общий алгоритм состоит из разложения модуля, решения сравнений по простым модулям, последовательного поднятия до нужных степеней и объединения корней по КТО. Само разложение большого числа может оказаться трудной частью задачи; в учебных примерах оно дано или легко находится.

2 Корни по простому модулю

При простом p кольцо $\mathbb{Z}/p\mathbb{Z}$ является полем. Ненулевой многочлен степени d над полем имеет не более d различных корней. Если a — корень, то многочлен делится на $x - a$; последовательное выделение линейных множителей доказывает утверждение индукцией по степени.

Здесь «ненулевой» означает, что после приведения коэффициентов по модулю p хотя бы один коэффициент отличен от нуля. Если все коэффициенты делятся на p, каждый из p классов является корнем. Если старший коэффициент обнуляется, степень нужно определить заново.

Для составного модуля ограничение числом d уже неверно: сравнение $x^2 \equiv 1 \pmod 8$ имеет четыре корня — 1, 3, 5 и 7. Причина состоит в наличии делителей нуля: из произведения, равного нулю по модулю 8, нельзя заключить, что один из множителей равен нулю.

Корень a по модулю p называется **простым**, если $f'(a) \not\equiv 0 \pmod p$. Корень с $f'(a) \equiv 0 \pmod p$ назовём **особым**. Для поднятия важен именно остаток производной, а не её значение как целого числа.

3 Один шаг поднятия и лемма Гензеля

3.1 Вывод линейного условия

Пусть a уже является корнем по модулю p^k, где $k \geq 1$. Все классы по модулю p^{k+1}, которые сводятся к a, имеют единственный вид

$$b = a + tp^k, \qquad 0 \leq t < p.$$

Для многочлена с целыми коэффициентами раскрытие каждого одночлена по биному даёт тождество

$$f(a + h) = f(a) + hf'(a) + h^2 Q(a, h),$$

где Q — некоторый многочлен с целыми коэффициентами. При $h = tp^k$ последний член делится на p^{2k}, а значит, и на p^{k+1}, поскольку $2k \geq k + 1$. Поэтому

$$f(a + tp^k) \equiv f(a) + tp^k f'(a) \pmod{p^{k+1}}.$$

Поскольку p^k делит $f(a)$, частное $f(a)/p^k$ является целым. Обозначим

$$c \equiv \frac{f(a)}{p^k} \pmod p, \qquad d \equiv f'(a) \pmod p.$$

Тогда условие поднятия принимает вид

$$c + td \equiv 0 \pmod p.$$

Деление здесь выполняется над целыми числами до перехода к остатку. Нельзя сначала заменить $f(a)$ нулём по модулю p^k, а затем пытаться извлечь из этого нуля частное.

3.2 Три возможных исхода

Первый случай: $d \not\equiv 0 \pmod p$. Обратный элемент d^{-1} существует, и ровно один класс $t \equiv -cd^{-1} \pmod p$ даёт корень следующего уровня.

Второй случай: $d \equiv 0$ и $c \not\equiv 0 \pmod p$. Линейное условие невозможно; данный корень не имеет продолжений.

Третий случай: $d \equiv c \equiv 0 \pmod{p}$. Подходит любое t от 0 до $p-1$; корень имеет ровно p продолжений. Однако на следующем уровне часть этих продолжений может исчезнуть.

Теорема 2 — конечная форма леммы Гензеля. Каждый простой корень по модулю p имеет единственное продолжение до корня по модулю p^e для любого целого $e \geq 1$.

Доказательство. На каждом шаге новый корень сравним с прежним по модулю p. Поэтому остаток производной остаётся ненулевым. Первый случай даёт существование и единственность следующего корня; индукция завершает доказательство. ■

Полнота алгоритма. Любой корень по модулю p^{k+1} после редукции является корнем по модулю p^k и единственным образом записывается как $a + tp^k$ с каноническим представителем a. Если на каждом уровне обработать все найденные корни и все допустимые t, ни один корень не будет пропущен. Разные родители не могут породить один класс следующего уровня.

4 Примеры простого и особого корня

4.1 Два простых корня

Решим $x^2 \equiv 6 \pmod{125}$. По модулю 5 получаем корни 1 и 4. Производная $2x$ в обоих случаях ненулевая, поэтому каждый корень имеет единственную цепочку продолжений.

При $a = 1$, $k = 1$ имеем $c = -1 \equiv 4$, $d = 2$. Условие $4 + 2t \equiv 0 \pmod{5}$ даёт $t = 3$ и новый корень $1 + 3 \cdot 5 = 16$ по модулю 25. Для него на следующем шаге $c = (16^2 - 6)/25 = 10 \equiv 0$, поэтому $t = 0$ и корень остаётся равным 16 по модулю 125.

При $a = 4$, $k = 1$ получаем $c = 2$, $d = 3$, $t = 1$ и корень 9 по модулю 25. Затем $c = (9^2 - 6)/25 = 3$, $d = 3$, откуда $t = 4$ и корень $9 + 4 \cdot 25 = 109$.

$$R_1 = \{1,4\}, \qquad R_2 = \{9,16\}, \qquad R_3 = \{16,109\}.$$

Проверка: $16^2 - 6 = 250 = 2 \cdot 125$ и $109^2 - 6 = 11875 = 95 \cdot 125$. Единственность поднятия каждого из двух начальных корней доказывает полноту ответа.

4.2 Разветвление с последующим исчезновением ветвей

Решим $x^2 \equiv 25 \pmod{125}$. По модулю 5 существует только корень 0. Для него $c = -5 \equiv 0$ и $d = 0$, поэтому по модулю 25 получаются все пять корней: 0, 5, 10, 15 и 20.

Запишем такой корень как $a = 5u$, где $u = 0,1,2,3,4$. На переходе от 25 к 125 имеем $c = u^2 - 1 \pmod{5}$ и $d = 0$. Продолжение возможно только при $u = 1$ или $u = 4$, то есть для родителей 5 и 20. Каждый из них порождает пять корней:

$$x = 5 + 25t \quad \text{или} \quad x = 20 + 25t, \qquad t = 0,1,2,3,4.$$

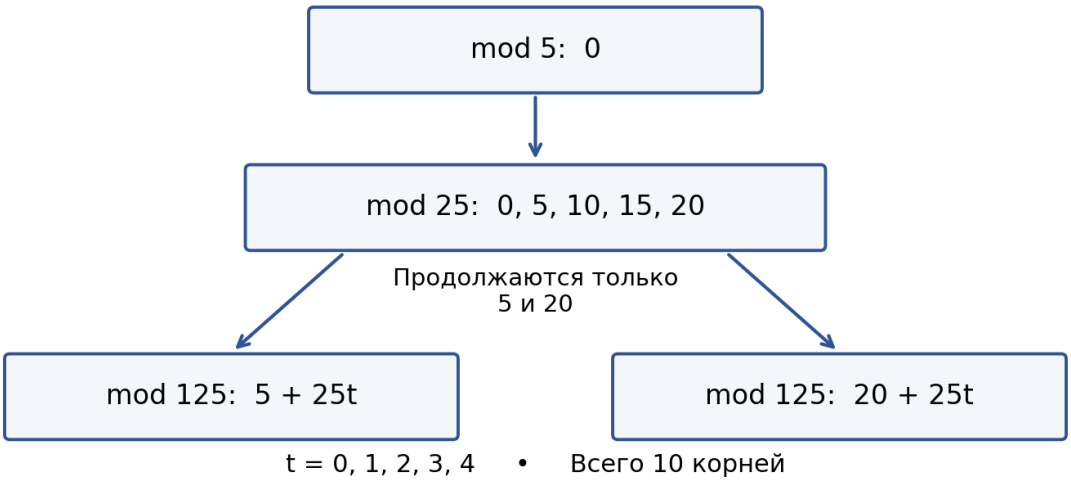


Рисунок 1 — Особый корень порождает пять ветвей, но далее продолжаются только две

Всего получено десять классов: 5, 20, 30, 45, 55, 70, 80, 95, 105 и 120. Утверждение «квадратное сравнение имеет не более двух корней» здесь неприменимо, поскольку модуль составной.

5 Квадратные сравнения по нечётной простой степени

Для ненулевого целого a обозначим через $v_p(a)$ показатель наибольшей степени p, делящей a. Рассмотрим $x^2 \equiv a \pmod{p^e}$ при нечётном простом p. Сначала приведём a к остатку от 0 до $p^e - 1$.

Случай $a = 0$. Делимость x^2 на p^e равносильна делимости x на $p^{\lceil e/2 \rceil}$. Поэтому

$$x = tp^{\lceil e/2 \rceil}, \qquad 0 \le t < p^{\lfloor e/2 \rfloor}.$$

Число корней равно $p^{\lfloor e/2 \rfloor}$. Например, по модулю $3^5 = 243$ сравнение $x^2 \equiv 0$ имеет девять корней, кратных 27.

Случай $a \neq 0$. Пусть $v = v_p(a) < e$. Если сравнение разрешимо, то $v_p(x^2) = v$: иначе сумма $a + p^e z$ не могла бы иметь тот же показатель делимости, что и a. Следовательно, v должен быть чётным. При нечётном v решений нет.

Пусть $v = 2s$ и $a = p^{2s}u$, где $p \nmid u$. Тогда $x = p^s y$ и

$$y^2 \equiv u \pmod{p^{e-2s}}.$$

Если u не является квадратом по модулю p, решений нет. Если является, имеются два ненулевых корня по модулю p; их производные $2y$ обратимы, и каждый единственным образом поднимается до модуля p^{e-2s}. Для каждого такого корня z получаем

$$x = p^s(z + tp^{e-2s}), \qquad 0 \le t < p^s.$$

Эти классы различны по модулю p^e, поэтому всего их $2p^s$. Дополнительный параметр возникает потому, что y рассматривается по модулю p^{e-s}, а уравнение определяет его лишь по модулю p^{e-2s}.

Для примера $a = 25$, $p = 5$, $e = 3$ имеем $s = 1$, $u = 1$ и число корней $2 \cdot 5 = 10$, что совпадает с деревом на рисунке 1. При $p = 2$ этот вывод для ненулевого a использовать нельзя: производная $2y$ всегда чётна. Само пошаговое условие $c + td \equiv 0 \pmod 2$ остаётся верным.

6 Объединение местных решений

Решим $x^2 \equiv 6 \pmod{2375}$, где $2375 = 125 \cdot 19$. По модулю 125 корни уже найдены: 16 и 109. По модулю 19 корни равны 5 и 14. Каждая из четырёх пар даёт один корень по КТО.

Положим $x = a + 125t$. Так как $125 \equiv 11 \pmod{19}$ и $11^{-1} \equiv 7 \pmod{19}$, для местного корня b получаем $t \equiv 7(b - a) \pmod{19}$. Пары (16,5), (16,14), (109,5) и (109,14) дают соответственно 2266, 641, 1734 и 109. Ответ в возрастающем порядке:

$$x \equiv 109,\ 641,\ 1734,\ 2266 \pmod{2375}.$$

Для сравнения $x^2 \equiv 6 \pmod{875}$ с $875 = 125 \cdot 7$ корней нет: число 6 не является квадратом по модулю 7. Наличие корней по одному простому множителю ещё не решает задачу для всего модуля.

7 Закрепление и самостоятельная работа

Задачи

1. Решите $x^2 \equiv 2 \pmod{49}$. Для обоих начальных корней выпишите a, c, d, t и результат поднятия.
2. Решите $x^2 \equiv 9 \pmod{81}$. Найдите все корни и обоснуйте их количество через показатель делимости.
3. Опишите все решения $x^2 \equiv 0 \pmod{243}$ одной формулой и перечислите их.
4. Докажите неразрешимость $x^2 \equiv 45 \pmod{125}$ двумя способами: через показатель делимости и через один неудачный шаг поднятия.
5. Найдите все решения $x^2 \equiv 1 \pmod{175}$ с помощью местных корней и КТО.
6. Решите $x^3 \equiv 1 \pmod{49}$. Объясните, почему найденные три корня исчерпывают все решения.

Контрольные вопросы

1. Что является неизвестным в сравнении многочлена и как принято записывать полный ответ?
2. Почему разложение модуля позволяет перейти к простым степеням?
3. При каких условиях число корней ограничено степенью многочлена?
4. Что называют простым корнем по модулю простого числа?
5. Почему достаточно рассмотреть $a + tp^k$ при $0 \le t < p$?
6. Почему при выводе условия поднятия исчезают члены начиная с квадратичного?
7. Почему величина $f(a)/p^k$ должна вычисляться до взятия остатка?
8. При каких условиях корень имеет ноль, одно или p продолжений?
9. Почему простой корень остаётся простым на следующих уровнях?
10. Почему при нечётном $v_p(a) < e$ квадратное сравнение неразрешимо?
11. Сколько корней имеет $x^2 \equiv 0 \pmod{p^e}$?
12. Как проверить полноту ответа для составного модуля?

Литература

1. Мартынов Л. М. Алгебра и теория чисел для криптографии. 2020. Глава 7, материал о сравнениях; § 7.7 о квадратных вычетах. Используется предоставленный экземпляр.
2. Trappe W., Washington L. C. Introduction to Cryptography with Coding Theory. 2nd ed. 2006. §§ 3.4 и 3.9 о КТО и квадратных корнях по модулю целого числа.
3. Conrad K. Hensel’s Lemma. § 2, Theorem 2.1 и доказательство последовательного поднятия. Авторский конспект.

Изложение и учебные примеры составлены для данного курса. Лемма Гензеля здесь используется в конечной форме; введение p-адических чисел не требуется.