ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Механико-математический факультет МГУ
1 поток 1 курса, осень 2026г.
Лекция 8: Кольцо классов вычетов. Полиномиальные сравнения по простому и составному модулям.

Кольцо классов вычетов $\mathbb{Z}$.

Для каждого целого числа a символом $\overline{a}$ будем обозначать класс вычетов по фиксированному модулю m, содержащий число a. Список всех классов вычетов по модулю m имеет вид $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. При $m = 7$ справедливы равенства $\overline{9} = \overline{2}$.

• На множестве классов вычетов по модулю m можно ввести **операции сложения, вычитания и умножения** по правилам

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} - \overline{b} = \overline{a-b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}. \tag{1}$$

• Так определённые операции не зависят от выбора представителей классов a и b и действительно являются операциями между классами вычетов.

Кольцо классов вычетов $\mathbb{Z}$.

Множество классов вычетов по модулю m с так определенными операциями является коммутативным кольцом – кольцом классов вычетов по модулю m. Оно обозначается $\mathbb{Z}/m\mathbb{Z}$. Все аксиомы кольца, а также коммутативность, легко проверяются с помощью аналогичных свойств целых чисел.

• Роль нулевого элемента этого кольца играет класс $\overline{0}$. Действительно, для любого элемента $\overline{a}$ имеем

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}, \qquad \overline{0} + \overline{a} = \overline{0 + a} = \overline{a}.$$

• Роль единичного элемента – класс вычетов $\overline{1}$:

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}, \qquad \overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}.$$

Кольцо классов вычетов $\mathbb{Z}$.

Проверка ассоциативности умножения выполняется так

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{a \cdot (bc)} = \overline{(ab) \cdot c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}.$$

• Доказательство дистрибутивности:

$$(\overline{a}+\overline{b})\cdot\overline{c} = \overline{a+b}\cdot\overline{c} = \overline{(a+b)\cdot c} = \overline{ac+bc} = \overline{ac}+\overline{bc} = \overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}.$$

Остальные аксиомы кольца проверяются столь же несложными преобразованиями.

• Обратимыми будут элементы $\overline{c}$ этого кольца с условием $(c, m) = 1$, т.е. классы вычетов, состоящие из чисел, взаимно простых с модулем m. В этом случае найдётся целое число b, удовлетворяющее сравнению $b \cdot c \equiv 1 \pmod{m}$ и, значит, будет выполнено равенство $\overline{b} \cdot \overline{c} = \overline{1}$.

Кольцо классов вычетов $\mathbb{Z}$.

В частности, если модуль $m = p$ есть простое число, то каждый класс вычетов, отличный от $\overline{0}$, обратим в кольце $\mathbb{Z}/p\mathbb{Z}$. Это значит, что кольцо классов вычетов по простому модулю есть поле. Для краткости мы будем обозначать его буквами $\mathbb{F}_p$.

• В кольце $\mathbb{Z}/m\mathbb{Z}$, вообще говоря, могут быть делители нуля. Например, при $m = 6$ имеем $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$.

• Пусть a – целое число, $d = (a, m)$, причем $1 < d < m$. Тогда с некоторыми целыми числами u, v выполняются равенства $a = du, m = dv$ и $av = udv = um \equiv 0 \pmod{m}$.

• Это значит, что $\overline{a} \cdot \overline{v} = \overline{0}$, причем $\overline{v} \neq \overline{0}$, т.е. $\overline{a}$ – делитель нуля в кольце $\mathbb{Z}/m\mathbb{Z}$.

Кольцо многочленов $\mathbb{F}_p[x]$.

Кольцо $\mathbb{F}_p[x]$ имеет много общего с кольцом целых чисел $\mathbb{Z}$. При любом простом p в кольце многочленов $\mathbb{F}_p[x]$ можно ввести понятия делимости, общего делителя и деления многочленов с остатком. При этом, как объяснялось раньше, можно работать только с многочленами, имеющими целые коэффициенты, заменяя их в сравнениях наименьшими неотрицательными или абсолютно наименьшими вычетами по модулю p. Степень остатка будет меньше степени делителя.

Кольцо многочленов $\mathbb{F}_p[x]$.

Степень остатка будет меньше степени делителя. Понижая таким способом степени многочленов, можно, вычислять наибольший общий делитель двух многочленов. Этот алгоритм подобен алгоритму для целых чисел и его также называют алгоритмом Евклида. Наибольший общий делитель многочленов $f(x)$ и $g(x)$ будет, как и для целых чисел, обозначаться символом $(f(x), g(x))$. Он определён с точностью до ненулевого множителя из поля $\mathbb{F}_p$.

Кольцо многочленов $\mathbb{F}_p[x]$.

Аналогом простых чисел в кольце $\mathbb{F}_p[x]$ служат неприводимые многочлены, т.е. многочлены, которые не возможно разложить в произведение двух многочленов меньшей степени. Они определены с точностью до ненулевого множителя из поля $\mathbb{F}_p$. Такой многочлен можно фиксировать однозначно, если выбрать его старший коэффициент равным 1. Каждый многочлен из кольца $\mathbb{F}_p[x]$ раскладывается в произведение неприводимых многочленов, притом единственным способом, если считать равными многочлены отличающиеся лишь множителями из поля $\mathbb{F}_p$.

Кольцо многочленов $\mathbb{F}_p[x]$.

Можно ввести понятие сравнимости многочленов по модулю $m(x) \in \mathbb{F}_p[x]$, полагая два многочлена $f(x), g(x) \in \mathbb{F}_p[x]$ сравнимыми, если разность $f(x) - g(x)$ делится на $m(x)$. Это свойство можно обозначать символом $f(x) \equiv g(x) \pmod{m(x)}$. Для таких сравнений выполняются свойства, подобные свойствам сравнений для чисел.

Следующее утверждение позволяет, не нарушая равносильности, понизить степень сравнения больше, чем теорема 18.

Теорема 19

Пусть $f(x)$ и $d(x)$ многочлены с целыми коэффициентами, причём, $d(x)$ есть наибольший общий делитель $f(x)$ и $x^p - x$ в кольце $\mathbb{F}_p[x]$. Тогда множества решений сравнений

$$f(x) \equiv 0 \pmod{p}, \qquad \text{и} \qquad d(x) \equiv 0 \pmod{p} \tag{2}$$

одинаковы.

• Делимость $d(x) \mid x^p - x$ в кольце $\mathbb{F}_p[x]$ означает, что все корни многочлена $d(x)$ содержатся среди корней многочлена $x^p - x$ и потому принадлежат полю $\mathbb{F}_p$, т.е. являются классами вычетов кольца $\mathbb{Z}$ по модулю p.

Доказательство.

Согласно условию в кольце $\mathbb{F}_p[x]$ выполняется равенство $f(x) = d(x) \cdot h(x)$, где $h(x) \in \mathbb{F}_p[x]$. Заменяя коэффициенты многочленов их наименьшими неотрицательными вычетами, мы можем не уменьшая общности считать, что $f(x), d(x), h(x) \in \mathbb{Z}[x]$, причём выполнено сравнение

$$f(x) \equiv d(x) \cdot h(x) \pmod{p}.$$

Доказательство.

Пусть для целого a выполняется сравнение $d(a) \equiv 0 \pmod{p}$. Тогда имеем $f(a) \equiv d(a)h(a) \equiv 0 \pmod{p}$. Таким образом, целое число a удовлетворяет первому из сравнений (2).

Подобно теореме 5 можно утверждать,что в кольце многочленов $\mathbb{F}_p[x]$ найдутся многочлены $\overline{u}(x), \overline{v}(x)$, удовлетворяющие равенству $\overline{f}(x)\overline{u}(x) + (x^p - x)\overline{v}(x) = \overline{d}(x)$.

• Заменяя эти многочлены соответствующими многочленами из кольца $\mathbb{Z}[x]$, получаем сравнение

$$d(x) \equiv f(x)u(x) + (x^p - x)v(x) \pmod{p}.$$

Доказательство.

Если для $a \in \mathbb{Z}$ выполнено сравнение $f(a) \equiv 0 \pmod{p}$, то согласно малой теореме Ферма имеем

$$d(a) \equiv f(a)u(a) + (a^p - a)v(a) \equiv 0 \pmod{p}.$$

Значит, a есть корень второго из сравнений (2). Теорема доказана.

Пример. Решим сравнение

$$x^3 - 2x - 3 \equiv 0 \pmod{17} \tag{3}$$

с помощью теоремы 19. Вычислим для этого наибольший общий делитель многочленов $x^3 - 2x - 3$ и $x^{17} - x$ в кольце $\mathbb{F}_{17}[x]$. Имеем в кольце $\mathbb{F}_{17}[x]$ сравнения по модулю многочлена $x^3 - 2x - 3$ (для краткости мы опускаем модуль в обозначениях)

$$\begin{aligned} x^3 &\equiv 2x + 3, \\ x^4 &\equiv 2x^2 + 3x, \\ x^8 &\equiv (2x^2 + 3x)^2 \equiv 2x + 2, \\ x^{16} &\equiv (2x + 2)^2 \equiv 4x^2 + 8x + 4, \\ x^{17} &\equiv x(4x^2 + 8x + 4) \equiv 8x^2 - 5x - 5. \end{aligned}$$

Таким образом, в соответствии с алгоритмом Евклида

$$(x^{17} - x, x^3 - 2x - 3) = (8x^2 - 6x - 5, x^3 - 2x - 3).$$

Продолжая алгоритм Евклида, находим

$$x^3 - 2x - 3 = (-2x + 7)(8x^2 - 6x - 5) - 4x - 2,$$
$$8x^2 - 6x - 5 = (4x + 2)(2x + 6).$$

И искомый наибольший общий делитель в кольце $\mathbb{F}_{17}[x]$ равен $4x + 2$ или $2x + 1$. В соответствии с теоремой 19 сравнение (3) имеет те же решения, что и сравнение $2x + 1 \equiv 0 \pmod{17}$. Последнее сравнение имеет единственное решение $x \equiv 8 \pmod{17}$.

Заметим, что в этом примере для вычисления остатка x^{17} по модулю $x^3 - 2x - 3$ использовался быстрый алгоритм возведения в степень, подобный числовому алгоритму. Он может использоваться и в других случаях при больших p.

• Далее в этом параграфе мы обсудим, как можно находить решения полиномиальных сравнений по простому модулю. Если модуль p не очень велик, это можно сделать перебором элементов какой-нибудь полной системы вычетов по модулю p.

Пример. Решить сравнение $x^2 + x + 1 \equiv 0 \pmod 7$. Многочлен $x^2 + x + 1$ при $x = -3, -2, -1, 0, 1, 2, 3$ принимает значения $7, 3, 1, 1, 3, 7, 13$ соответственно. Из них только значения в точках $-3, 2$ делятся на 7, так что сравнение имеет два решения $x \equiv -3 \pmod 7, x \equiv 2 \pmod 7$.

Алгоритм.

В общем случае сравнение имеет смысл сначала упростить, пользуясь теоремой 19. Далее будем предполагать, что такое упрощение выполнено и многочлен $f(x)$ есть делитель многочлена $x^p - x = x(x^{p-1} - 1)$ в кольце $\mathbb{F}_p[x]$, а точнее – делитель многочлена $x^{p-1} - 1$. Кроме того, будем предполагать, что $p \geq 3$.

Описываемый ниже алгоритм носит вероятностный характер и эффективен на практике. Он строит множество $\mathcal{M}$, состоящее из различных делителей многочлена $f(x)$ в кольце $\mathbb{F}_p[x]$. • При этом количество элементов в множестве $\mathcal{M}$ увеличивается до тех пор, пока оно не станет равным $n = \deg f(x)$.

Алгоритм.

Алгоритм рещения сравнений по простому модулю.
Данные: Многочлен $f(x) \in \mathbb{F}_p[x]$, $n = \deg f(x) \geq 2$, $f(x)|(x^{p-1} - 1)$.
Найти: Все корни многочлена $f(x)$.

1. Положить $\mathcal{M} = \{f(x)\}$.
2. Выбрать каким-либо способом элемент $c \in \mathbb{F}_p$.
3. Для каждого $u(x) \in \mathcal{M}$ с условием $\deg u(x) > 1$ выполнить следующие действия:
3.1. Если $u(c) = 0$, то исключить $u(x)$ из множества $\mathcal{M}$ и заменить его парой многочленов $x - c$ и $u(x)/(x - c)$.
3.2. Вычислить

$$d(x) = (u(x), (x - c)^{\frac{p-1}{2}} - 1).$$

Алгоритм.

3.3. Если $1 \leq \deg d(x) < \deg u(x)$, то исключить $u(x)$ из множества $\mathcal{M}$ и заменить его парой многочленов $d(x)$ и $u(x)/d(x)$.
3.4 Если $\#\mathcal{M} = n$, то алгоритм завершает работу. Множество $\mathcal{M}$ в этом случае состоит из всех многочленов вида $x - \gamma$, где $\gamma \in \mathbb{F}_P$ – корень многочлена $f(x)$.
4. Перейти к шагу 2.

Пример. Решим сравнение $x^3 + 2x + 1 \equiv 0 \pmod{17}$.

В начальный момент имеем $\mathcal{M} = \{x^3 + 2x + 1\}$. При $c = -1$ с помощью алгоритма возведения в степень в кольце $\mathbb{F}_{17}[x]$, как и в предыдущем примере, находим сравнения по модулю $x^3 + 2x + 1$

$$(x+1)^4 \equiv 4x^2 - 5x - 3, \qquad (x+1)^8 \equiv 3x^2 + 9x - 2$$

и

$$((x+1)^8 - 1, x^3 + 2x + 1) = x - 3.$$

Разделив многочлен $x^3 + 2x + 1$ на $x - 3$, получаем

$$x^3 + 2x + 1 = (x - 3)(x^2 + 3x - 6).$$

После этого множество $\mathcal{M}$ принимает вид $\mathcal{M} = \{x - 3, x^2 + 3x - 6\}$.

Точно так же при $c = 0$ находим

$$(x^8 - 1, x^2 + 3x - 6) = x + 8.$$

Разделив многочлен $x^2 + 3x - 6$ на $x + 8$, получаем

$$x^2 + 3x - 6 = (x + 8)(x - 5).$$

Множество $\mathcal{M}$ становится равным

$$\mathcal{M} = \{x - 3, x - 5, x + 8\}.$$

Множество решений данного сравнения имеет вид

$$x \equiv 3 \pmod{17}, \qquad x \equiv 5 \pmod{17}, \qquad x \equiv -8 \pmod{17}.$$

Следующее утверждение объясняет, почему алгоритм достаточно быстро находит решения сравнения.

Лемма 1

Пусть $u(x) \mid f(x), \deg u(x) \geq 2$. *Вероятность того, что при случайном выборе* $c \in \mathbb{F}_p$, *количество элементов в множестве* $\mathcal{M}$ *в пункте 3 алгоритма увеличится, не меньше* $\frac{1}{2}$.

Доказательство леммы.

Из условия леммы, поскольку $u(x)|(x^{p-1}-1)$ следует, что $u(x)$ имеет в поле $\mathbb{F}_p$ не менее двух корней, причём все его корни различны. Пусть γ_1, γ_2 – корни многочлена $u(x)$.

• Обозначим буквой $\mathcal{D}$ подмножество F_p, состоящее из элементов t, удовлетворяющих условиям

$$(t-\gamma_1)^{\frac{p-1}{2}} \neq (t-\gamma_2)^{\frac{p-1}{2}}.$$

Доказательство леммы.

По теореме Лагранжа многочлен $(x-\gamma_1)^{\frac{p-1}{2}} - (x-\gamma_2)^{\frac{p-1}{2}}$ имеет не более $\frac{p-3}{2}$ корней. Поэтому

$$\#\mathcal{D} \geq p - \frac{p-3}{2} = \frac{p+3}{2}.$$

• Докажем, что для каждого $c \in \mathcal{D}$ алгоритм увеличивает количество многочленов в множестве $\mathcal{M}$. Если $c = \gamma_1$ или $c = \gamma_2$, это, очевидно, будет сделано в пункте 3.1. Далее будем считать, что обе разности $c - \gamma_i$ отличны от нуля.
Каждый ненулевой элемент $b \in F_p$ согласно малой теореме Ферма удовлетворяет равенству

$$0 = b^{p-1} - 1 = (b^{\frac{p-1}{2}} - 1)(b^{\frac{p-1}{2}} + 1)$$

и, значит, удовлетворяет в точности одному из равенств $b^{\frac{p-1}{2}} = 1$ или $b^{\frac{p-1}{2}} = -1$.

Доказательство леммы.

Поскольку $c \in \mathcal{D}$, то

$$(c - \gamma_1)^{\frac{p-1}{2}} \neq (c - \gamma_2)^{\frac{p-1}{2}}$$

и, значит, одно из чисел γ_1, γ_2 будет корнем многочлена $(x - c)^{\frac{p-1}{2}} - 1$, а другое нет. Следовательно, в этом случае $1 \leq \deg d(x) < \deg u(x)$, т.е. $d(x)$ есть собственный делитель $u(x)$. Лемма доказана.

Из доказанной леммы следует, что алгоритм на каждом цикле увеличивает количество многочленов в множестве $\mathcal{M}$ с вероятностью

$$\frac{\#\mathcal{D}}{p} \geq \frac{p+3}{2p} > \frac{1}{2}.$$

Лемма доказана.

• Лемма 1 показывает, что при случайном выборе элемента $c \in F_p$, вероятность того, что величина $\#\mathcal{M}$ не увеличится после k повторений шагов 2 - 4 алгоритма, не превосходит 2^{-k}.

§6.6. Полиномиальные сравнения по составному модулю.

Рассмотрим сначала случай, когда модуль сравнения есть степень простого числа p, т.е. $m = p^k, k \geq 2$. Если $f(x)$ – многочлен с целыми коэффициентами и целое число a удовлетворяет сравнению $f(x) \equiv 0 \pmod{p^k}$, то $p^k | f(a)$. Но тогда $p | f(a)$, так что a удовлетворяет сравнению $f(x) \equiv 0 \pmod{p}$.

• Отсюда можно сделать два заключения.

1. *Если сравнение* $f(x) \equiv 0 \pmod{p}$ *не имеет решений, то ни при каком* $k \geq 2$ *сравнение* $f(x) \equiv 0 \pmod{p^k}$ *также не имеет решений.*

2. *Для каждого числа* a*, удовлетворяющего сравнению* $f(x) \equiv 0 \pmod{p^k}$ *найдется решение сравнения* $f(x) \equiv 0 \pmod{p}$*, которому принадлежит* a*.*

Таким образом решение сравнений по модулю равному степени простого числа p сводится во-первых к выяснению разрешимости сравнения по простому модулю p, и, в случае разрешимости, поиску решений по простому модулю. А во-вторых к поиску решений сравнения по модулю p^k, принадлежащих фиксированному решению по простому модулю.

• Первый шаг обсуждался в предыдущем параграфе. Второй шаг основан на следующем утверждении.

Теорема 20

Пусть $f(x)$ – многочлен с целыми коэффициентами и x_1 – целое число, удовлетворяющее условиям

$$f(x_1) \equiv 0 \pmod{p}, \qquad f'(x_1) \not\equiv 0 \pmod{p}.$$

Тогда при любом $k \geq 1$ существует единственное решение сравнения $f(x) \equiv 0 \pmod{p^k}$, принадлежащее классу вычетов $x \equiv x_1 \pmod{p}$.

Доказательство.

Докажем теорему с помощью индукции по степени модуля k. При $k = 1$ утверждение, очевидно, выполняется.

- Предположим утверждение теоремы справедливо для некоторого $k \geq 1$. Тогда существует единственное целое число a, удовлетворяющее условиям

$$f(a) \equiv 0 \pmod{p^k}, \quad 0 \leq a < p^k, \quad a \equiv x_1 \pmod{p}.$$

- Найдем все такие целые числа b, что

$$f(b) \equiv 0 \pmod{p^{k+1}}, \quad 0 \leq b < p^{k+1}, \quad b \equiv x_1 \pmod{p}. \tag{4}$$

$$f(a) \equiv 0 \pmod{p^k}, \quad 0 \le a < p^k, \quad a \equiv x_1 \pmod{p}.$$

Найдем все такие целые числа b, что

$$f(b) \equiv 0 \pmod{p^{k+1}}, \quad 0 \le b < p^{k+1}, \quad b \equiv x_1 \pmod{p}.$$

- Первое из условий на b влечёт $p^k | f(b)$ и, значит, наименьший неотрицательный вычет класса $b \pmod{p^k}$ равен a. Но тогда $b = a + p^k t$, с некоторым целым t, $0 \le t < p$.
- Многочлен

$$f(a + x) = c_0 + c_1 x + c_2 x^2 + \dots$$

имеет целые коэффициенты. Подставляя в это равенство $x = 0$, находим $c_0 = f(a)$. А дифференцируя это равенство и так же подставляя 0 вместо x, получаем $c_1 = f'(a)$.

$$f(a+x) = f(a) + f'(a)x + c_2x^2 + \ldots \tag{5}$$

• При $x = p^k t$ из (5) следует сравнение $f(b) \equiv f(a) + f'(a)p^k t \pmod{p^{k+1}}$. Так как $p^k | f(a)$ и $p^{k+1} | f(b)$, то разделив обе части сравнения на p^k, получим

$$0 \equiv \frac{f(a)}{p^k} + f'(a)t \pmod{p}.$$

• Учитывая теперь, что $a \equiv x_1 \pmod{p}$, заключаем, что $f'(a) \equiv f'(x_1) \pmod{p}$ и

$$f'(x_1)t + \frac{f(a)}{p^k} \equiv 0 \pmod{p}. \tag{6}$$

• Согласно условию теоремы $p \nmid f'(x_1)$, так что сравнение (6) разрешимо относительно t и имеет единственное решение.

Решив это сравнение, мы найдем единственное число $b = a + p^k t$, удовлетворяющее условиям (4). Это завершает шаг индукции и вместе с ним доказательство теоремы.

Приведённое доказательство позволяет находить решения сравнений по модулю, равному степени простого числа.

Конец 8-й лекции