ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Механико-математический факультет МГУ
1 поток 1 курса, осень 2026г.
Лекция 9: Полиномиальные сравнения по составному модулю. Сравнения второй степени по простому модулю.

Напоминание.

Теорема 21

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 $x \equiv x_1 \pmod{p}$.

Напоминание.

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

Найдем все такие целые числа b, что

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

$b = a + p^{k-1}t$, с некоторым целым t, $0 \le t < p$.

$$f'(x_1)t + \frac{f(a)}{p^{k-1}} \equiv 0 \pmod{p}. \qquad (1)$$

• Согласно условию теоремы $p \nmid f'(x_1)$, так что сравнение (1) разрешимо относительно t и имеет единственное решение. Решив это сравнение, мы найдем единственное число $b = a + p^k t$, удовлетворяющее утверждению теоремы.

Алгоритм.

Данные: Простое нечётное число p и натуральное число m, многочлен $f(x) \in \mathbb{Z}$ с условием $f(x)|(x^p - x)$ в кольце $\mathbb{F}_p[x]$,
Найти все решения сравнения $f(x) \equiv 0 \pmod{p^m}$.

1. Положить $S_1 = \emptyset, S_2 = \emptyset$, $k = 1$. Найти все решения сравнения $f(x) \equiv 0 \pmod{p}$. Их наименьшие неотрицательные вычеты поместить в множество S_2.

2. Если множество S_1 пусто возможны два случая.

2.1. При $k = m$, алгоритм завершает свою работу. Представители всех решений данного сравнения лежат в множестве S_2.

2.2. При $k < m$ увеличить k на 1 и переместить все числа из множества S_2 в множество S_1.

Алгоритм.

3. Выбрать и исключить из S_1 какой-нибудь элемент a.

4. Найти $x_1 \equiv a \pmod{p}$ и решить сравнение

$$f'(x_1)t + \frac{f(a)}{p^{k-1}} \equiv 0 \pmod{p}. \qquad (2)$$

относительно неизвестного t.

4.1. Если $f'(x_1) \not\equiv 0 \pmod{p}$ и t_0 единственное в этом случае решение сравнения (2), то нужно поместить число $a + t_0 \cdot p^{k-1}$ в множество S_2. а затем перейти в п. 2.

4.2. Если $f'(x_1) \equiv 0 \pmod{p}$ и $\frac{f(a)}{p^{k-1}} \not\equiv 0 \pmod{p}$, сравнение (2) решений не имеет. В этом случае нужно перейти в п. 2.

4.3. Если $f'(x_1) \equiv 0 \pmod{p}$ и $\frac{f(a)}{p^{k-1}} \equiv 0 \pmod{p}$, сравнение (2) имеет p решений. Поместить в множество S_2 числа $a + t \cdot p^{k-1}$ при всех $t = 0, 1, 2, \ldots, p-1$. Затем перейти в п. 2.

Пример. Решить сравнение $x^3 - 3x^2 - 1 \equiv 0 \pmod{125}$.

Так как $125 = 5^3$, то $m = 3$, и для работы с алгоритмом положим

$$f(x) = x^3 - 3x^2 - 1, \qquad f'(x) = 3x^2 - 6x.$$

Решая сравнение $x^3 - 3x^2 - 1 \equiv 0 \pmod{5}$, находим его решения $x \equiv 2 \pmod{5}$, $x \equiv -1 \pmod{5}$.

После пункта 1 алгоритма имеем $S_1 = \emptyset$, $S_2 = \{2, -1\}$, $k = 1$ и далее после пункта 2.2 $S_1 = \{2, -1\}, S_2 = \emptyset$, $k = 2$.
Выбрав $a = 2$ имеем $f(2) = -5, f'(2) = 0$ и находим сравнение

$$-1 \equiv 0 \pmod{5}.$$

не имеющее решений. В этот момент алгоритм выходит из п. 4.2, и выполняются равенства $S_1 = \{-1\}$, $S_2 = \emptyset$, $k = 2$. Он должен перейти в п.2 и пропустив его, перейти в п.3, после которого получится $S_1 = \emptyset, S_2 = \emptyset, k = 2$ и $a = -1$, $x_1 = -1$.

Так как $f(-1) = -5, f'(-1) = 9$,находим сравнение

$$\frac{-5}{5} + 9 \cdot t \equiv 0 \pmod 5.$$

Из него следует, что $t = -1$ и новое значение $-1 + (-1) \cdot 5 = -6$, согласно п. 4.1 алгоритма должно быть помещено в множество S_2. Итак, находим $S_1 = \emptyset$, $S_2 = \{-6\}$ и после пункта 2.2 имеем $S_1 = \{-6\}$, $S_2 = \emptyset$, $k = 3$.
Так как $f(-6) = -325$ и $f'(-1) = 9$, приходим к сравнению

$$\frac{-325}{25} + 9 \cdot t \equiv 0 \pmod 5,$$

которое после сокращения на 5 даёт нам $t = 2$ и число которое должно быть занесено в множество S_2 имеет вид $-6 + 2 \cdot 25 = 44$. Отсюда следует $S_1 = \emptyset$, $S_2 = \{44\}, k = 3$ и
Ответ: $x \equiv 44 \pmod{125}$.

Перейдем теперь к решению сравнений по произвольному составному модулю.

Теорема 22

Пусть $f(x)$ – многочлен с целыми коэффициентами и $m_1 > 1, \ldots, m_k > 1$ – попарно взаимно простые числа. Множества целых чисел, удовлетворяющих сравнению

$$f(x) \equiv 0 \pmod{m_1 \cdots m_k} \tag{3}$$

и системе сравнений

$$f(x) \equiv 0 \pmod{m_1}, \quad \ldots, \quad f(x) \equiv 0 \pmod{m_k} \tag{4}$$

совпадают. Если при любом натуральном m символ $N(m)$ обозначает количество решений сравнения $f(x) \equiv 0 \pmod{m}$, то

$$N(m_1 \cdots m_k) = N(m_1) \cdots N(m_k).$$

Доказательство.

Пусть b – целое число, удовлетворяющее сравнению (3), т.е. $m_1 \cdots m_k | f(b)$. Тогда при любом $j, 1 \leq j \leq k$, выполняется $m_j | f(b)$ или $f(b) \equiv 0 \pmod{m_j}$. Значит, b удовлетворяет системе сравнений (4).

Докажем обратное утверждение. Если b удовлетворяет системе сравнений (4), то $m_j | f(b)$ при любом $j, 1 \leq j \leq k$. Числа $m_1, \ldots, m_k$ попарно взаимно просты, поэтому $m_1 \cdots m_k | f(b)$ и, значит, b удовлетворяет сравнению (3).

Пусть $a_1, \ldots, a_k$ – целые числа, удовлетворяющие сравнениям (4) соответственно. Согласно китайской теореме об остатках система сравнений

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_k \pmod{m_k} \tag{5}$$

разрешима, и целое число x_0, определенное в этой теореме, удовлетворяет системе (5). Тогда при любом j имеем $f(x_0) \equiv f(a_j) \equiv 0 \pmod{m_j}$, т.е. $m_j | f(x_0)$.
Поскольку числа $m_1, \ldots, m_k$ попарно взаимно просты, заключаем, что $m_1 \cdots m_k | f(x_0)$, т.е. x_0 удовлетворяет сравнению (3).

Если числа $a_1, \ldots, a_k$ независимо друг от друга пробегают множества представителей классов вычетов, состоящих из решений соответствующих сравнений (4), то по следствию 1 из китайской теоремы об остатках числа x_0, определённые в этой теореме, пробегают различные классы вычетов, состоящие из решений сравнения по модулю $m_1 \cdots m_k$. Эти классы вычетов, по доказанному состоят из чисел, удовлетворяющих сравнению (3). Значит, число решений этого сравнения не меньше, чем $N(m_1) \cdots N(m_k)$.

По доказанному выше каждое целое число b, удовлетворяющее сравнению (3) удовлетворяет системе сравнений (4) и потому при каждом j класс вычетов $b \pmod{m_j}$ есть решение сравнения $f(x) \equiv 0 \pmod{m_j}$. Это доказывает, что никаких решений, отличных от построенных $N(m_1) \cdots N(m_k)$ решений сравнение (3) не имеет.

Теорема 22 доказана.

Приведенное выше доказательство теоремы 22 позволяет находить решения сравнения (3) при составном модуле m.

А именно, если $m = p_1^{r_1} \cdots p_k^{r_k}$ – разложение в произведение различных простых чисел, то найдя числа, $a_1, \ldots, a_k$, удовлетворяющие сравнениям $f(x) \equiv 0 \pmod{p_j^{r_j}}$ при $1 \leq j \leq k$ и выбрав x_0 с помощью китайской теоремы об остатках, мы найдем некоторое решение $x_0 \pmod{m}$ сравнения (3).

Более того, так будут найдены все решения, если каждое из чисел $a_1, \ldots, a_k$ независимо будет пробегать все решения своего сравнения.

Пример.

Решить сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod{75}$.

Справедливо разложение $75 = 3 \cdot 5^2$. Сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod 3$ имеет два решения $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 3$. Сравнение $x^3 - x^2 + 2x + 1 \equiv 0 \pmod 5$ имеет единственное решение $x \equiv 3 \pmod 5$.

Для того, чтобы решить сравнение

$$x^3 - x^2 + 2x + 1 \equiv 0 \pmod{25} \tag{6}$$

представим x в виде $x = 3 + 5t$. Для вычисления t получаем $f(3) = 25$, $f'(3) = 23$ и, как это было указано выше, сравнение $\frac{25}{5} + 23 \cdot t \equiv 0 \pmod 5$. Таким образом, $t = 0$ и сравнение (6) имеет единственное решение $x \equiv 3 \pmod{25}$.

В соответствии с теорией для решения исходного сравнения нужно найти решения двух систем сравнений

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 3 \pmod{25}, \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod{25}. \end{cases}$$

Первая из них имеет решение $x \equiv 28 \pmod{75}$, а вторая $x \equiv 53 \pmod{75}$. Два найденных класса вычетов и составляют ответ к задаче.

§6.1 Сравнения второй степени по простому модулю.

Пусть p – простое нечётное число. Каждое сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad p \nmid a, \tag{7}$$

можно упростить, изменив его коэффициенты и сделав замену переменной.

Умножив обе части сравнения (7) на число $4a$, не делящееся на p, получим равносильное сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

Его можно переписать в виде $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ или в виде

$$y^2 \equiv D \pmod{p}, \tag{8}$$

где использованы обозначения $y = 2ax + b$ и $D = b^2 - 4ac$.

Сравнения второй степени по простому модулю

Так как $p \nmid 2a$, то сравнение

$$2ax + b \equiv y \pmod{p}$$

при любом целом y имеет единственное решение относительно x. Это устанавливает взаимно однозначное соответствие между решениями сравнения (7) относительно x и сравнения (8) относительно y.

Из сказанного следует, что в дальнейшем можно рассматривать лишь сравнения вида

$$x^2 \equiv a \pmod{p}. \tag{9}$$

Сравнения второй степени по простому модулю

По теореме Лагранжа сравнение $x^2 \equiv a \pmod{p}$ имеет не более двух решений.

Если это сравнение разрешимо и $a \not\equiv 0 \pmod{p}$, то число решений равно двум. Действительно, вместе с решением $x_0 \pmod{p}$ сравнение будет иметь решением и класс вычетов $-x_0 \pmod{p}$, причем эти классы вычетов различны.

В противном случае мы имели бы $x_0 \equiv -x_0 \pmod{p}$ и $p|x_0$. Но тогда $p|a$, что противоречит условию. Таким образом, при $a \not\equiv 0 \pmod{p}$ сравнение (9) либо не имеет решений, либо имеет два решения.

В случае $a \equiv 0 \pmod{p}$ сравнение имеет единственное решение $x \equiv 0 \pmod{p}$.

Сравнения второй степени по простому модулю

Установленное выше взаимно однозначное соответствие между множествами решений сравнений (7) и (8) позволяет утверждать, что и в общем случае при $p|D = b^2 - 4ac$ сравнение (7) имеет единственное решение. Если же $p \nmid D$, то сравнение (7) либо имеет два решения, либо не имеет их вовсе.

Легко проверить, что сравнение $x^2 \equiv -1 \pmod 3$ не имеет решений, а сравнение $x^2 \equiv -1 \pmod 5$ имеет два решения $x \equiv 2 \pmod 5$ и $x \equiv 3 \pmod 5$.

Сравнения второй степени по простому модулю

Целое число a, не делящееся на p, называется *квадратичным вычетом* по модулю p, если сравнение

$$x^2 \equiv a \pmod{p}.$$

имеет решение.

Если же это сравнение не имеет решений, число a называется *квадратичным невычетом* по модулю p.

Числа, сравнимые между собой, одновременно являются квадратичными вычетами или квадратичными невычетами.

Число -1 есть квадратичный невычет по модулю 3. Оно же является квадратичным вычетом по модулю 5.

Лемма 1.1

Любая приведенная система вычетов по модулю p содержит $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов. Целое число a, не делящееся на p будет квадратичным вычетов в том и только том случае, когда

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{10}$$

и квадратичным невычетом в том и только том случае, когда

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{11}$$

Доказательство

Пусть a – квадратичный вычет. Тогда с некоторым целым числом b, не делящимся на p, выполняется сравнение $b^2 \equiv a \pmod{p}$. Возводя обе части этого сравнения в степень $\frac{p-1}{2}$, и пользуясь малой теоремой Ферма, находим

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

Таким образом, каждый квадратичный вычет удовлетворяет сравнению $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$. Согласно теореме Лагранжа можно утверждать, что существует не более $\frac{p-1}{2}$ классов вычетов, состоящих из квадратичных вычетов.

Доказательство

Числа

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2, \tag{12}$$

очевидно, являются квадратичными вычетами.

Они не сравнимы друг с другом по модулю p. В противном случае нашлись бы два числа k_1, k_2, удовлетворяющие условиям

$$p|(k_1^2 - k_2^2) = (k_1 - k_2)(k_1 + k_2), \qquad 1 \leq k_2 < k_1 \leq \frac{p-1}{2}.$$

Но указанная делимость невозможна, ведь сумма $k_1 + k_2$ и разность $k_1 - k_2$ не делятся на p, они положительны, но меньше, чем $p - 1$.

Доказательство

Итак, существует ровно $\frac{p-1}{2}$ классов вычетов по модулю p, состоящих из квадратичных вычетов. Все они удовлетворяют сравнению (10).

Но тогда квадратичные невычеты составляют оставшиеся $\frac{p-1}{2}$ классов вычетом, состоящих из чисел, не делящихся на p, а каждая приведённая система вычетов по модулю p содержит ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов.

Если a – квадратичный невычет, то по доказанному $p \nmid a^{\frac{p-1}{2}} - 1$. По малой теореме Ферма имеем

$$p | a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Следовательно, $p | a^{\frac{p-1}{2}} + 1$ и, значит, выполнено сравнение (11).

□

Конец 9-й лекции