1 Полиномиальные сравнения.

Определение. *Полиномиальным сравнением* будем называть сравнение вида $f(x) \equiv 0(mod\, n)$, где $f(x) \in \mathbb{Z}[x]$, то есть $f(x)$ - многочлен с целыми коэффициентами.

Замечание. Понятно, что от сравнения $f(x) \equiv g(x)(mod\, n)$, $f(x), g(x) \in \mathbb{Z}[x]$ можно перейти к полиномиальному сравнению $h(x) \equiv 0(mod\, n)$, где $h(x) = f(x) - g(x)$.

Пример. Рассмотрим случай $\deg f(x) = 1$. Тогда получаем полиномиальное сравнение $ax \equiv b(mod\, n)$, которое как известно разрешимо тогда и только тогда, когда $(n, a)|b$ и его решение может быть найдено с помощью Алгоритма Евклида.

Также рассмотрим случай $f(x) = x^2 - a$, тогда получаем полиномиальное сравнение $x^2 \equiv a(mod\, n)$, для разрешимости которого необходимо $\left(\frac{a}{n}\right) = 1$ и достаточно чтобы $\left(\frac{a}{p_i^{\alpha_i}}\right) = 1$, $i \in \overline{1,r}$, где $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ - каноническое разложение числа n.

1.1 Полиномиальное сравнение $ax^m \equiv b(mod\, n)$.

Рассмотрим сравнение $ax^m \equiv b(mod\, n)$, $(a, n) = (b, n) = 1$, где $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, p_i - нечётные простые, $\alpha_i \in \mathbb{N}$, $\alpha_0 \in \mathbb{N}_0$. Тогда данное сравнение эквивалентно следующей системе сравнений $ax^m \equiv b(mod\, 2^{\alpha_0})$, $ax^m \equiv b(mod\, p_i^{\alpha_i})$, $i \in \overline{1,r}$. Пусть $(\gamma, \gamma_0, \gamma_1, \ldots, \gamma_r)$ и $(\delta, \delta_0, \delta_1, \ldots, \delta_r)$ системы индексов a и b соответственно. То есть $a \equiv (-1)^{\gamma} 5^{\gamma_0} (mod\, 2^{\alpha_0})$, $a \equiv g_i^{\gamma_i} (mod\, p_i^{\alpha_i}), i \in \overline{1,r}$ и $b \equiv (-1)^{\delta} 5^{\delta_0} (mod\, 2^{\alpha_0})$, $b \equiv g_i^{\delta_i} (mod\, p_i^{\alpha_i}), i \in \overline{1,r}$, где g_i - первообразные корни по модулю $p_i^{\alpha_i}$.

Нетрудно видеть, что $(x, n) = 1$. Пусть $(\lambda, \lambda_0, \lambda_1, \ldots, \lambda_r)$ - система индексов числа x(в тех же первообразных корнях g_i, что и ранее приведённые системы a и b).

Рассмотрим сравнение $ax^m \equiv b(mod\, p_i^{\alpha_i})$. Оно равносильно тому, что индексы ax^m и b при основании g_i совпадают. То есть $\mathrm{ind}_{g_i}(ax^m) \equiv \mathrm{ind}_{g_i} a + m \cdot \mathrm{ind}_{g_i} x \equiv \gamma_i + m\lambda_i \equiv \delta(mod\, \varphi(p_i^{\alpha_i}))$.

Рассмотрим сравнение $ax^m \equiv b(mod\, 2^{\alpha_0})$, где $\alpha_0 > 1$. Используя аналогичные рассуждения получаем, что оно равносильно системе из двух сравнений $\gamma + m\lambda \equiv \delta(mod\, 2)$ и $\gamma_0 + m\lambda_0 \equiv \delta_0(mod\, 2^{\alpha_0 - 2})$. При $\alpha_0 = 0, 1$ сравнение $ax^m \equiv b(mod\, 2^{\alpha_0})$ очевидно верно

То есть исходное сравнение равносильно системе сравнений

$$\begin{cases} \gamma + m\lambda \equiv \delta(mod\, c) \\ \gamma_0 + m\lambda_0 \equiv \delta_0(mod\, c_0) \\ \gamma_i + m\lambda_i \equiv \delta_i(mod\, c_i), i \in \overline{1,r} \end{cases}$$

где $c_i = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$, $i \in \overline{1,r}$,

$$c = \begin{cases} 2, \alpha_0 \geq 2 \\ 1, \alpha = 0, 1 \end{cases}$$

$$c_0 = \begin{cases} 2^{\alpha_0 - 2}, \alpha_0 \geq 2 \\ 1, \alpha = 0, 1 \end{cases}$$

Из данной системы можно найти систему индексов $(\lambda, \lambda_0, \lambda_1 \ldots, \lambda_r)$ x по модулю n. Исходя из сравнений $x \equiv (-1)^{\lambda} 5^{\lambda_0} (mod\, 2^{\alpha_0})$, $x \equiv g_i^{\lambda_i} (mod\, p_i^{\alpha_i}), i \in \overline{1, r}$ находим x.

Замечание. Если $n = p^{\alpha}$ или $n = 2p^{\alpha}$, где p - нечётное простое, то можно дискретно логарифмировать сравнение $ax^m \equiv b(mod\, n)$ по основанию некоторого первообразного корня g_i и переходить к сравнению $y \cdot \mathrm{ind}_{g_i} a \equiv \mathrm{ind}_{g_i} b (mod\, p^{\alpha} - p^{\alpha - 1})$, где $y = \mathrm{ind}_{g_i} x$.

Замечание. Рассмотрим сравнение $ax^m \equiv b(mod\, n)$, где a и b не обязательно взаимнопросты с n. Тогда от него можно перейти к сравнению $cy^m \equiv d(mod\, k)$, $(c, k) = (d, k) = 1$(покажите самостоятельно).

Задача. Решить сравнение $7x^{17} \equiv 157(mod\, 1144)$.

Решение

Отметим, что $1144 = 2^3 \cdot 11 \cdot 13$. В прошлой лекции было показано, что системы индексов 7 и 157 по модулю 1144 равны $(1, 0, 7, 11)$ и $(1, 0, 8, 0)$ соответственно($g_1 = 2$,$g_2 = 2$). Пусть $(\lambda, \lambda_0, \lambda_1, \lambda_2)$ - соответствующая система индексов x по модулю 1144 при таких же первообразных корнях. Отметим, что $c = 1$, $c_0 = 2$, $c_1 = 8$, $c_2 = 12$. Тогда получаем систему:

$$\begin{cases} 1 + 17\lambda \equiv 0(mod\, 2) \\ 17\lambda_0 \equiv 1(mod\, 2) \\ 7 + 17\lambda_1 \equiv 8(mod\, 10) \\ 11 + 17\lambda_2 \equiv 0(mod\, 12) \end{cases}$$

Упрощаем данную систему:

$$\begin{cases} \lambda \equiv 1(mod\, 2) \\ \lambda_0 \equiv 1(mod\, 2) \\ 7\lambda_1 \equiv 1(mod\, 10) \\ 5\lambda_2 \equiv 1(mod\, 12) \end{cases}$$

Отсюда находим систему индексов числа x по модулю 1144: $(1, 1, 3, 5)$. Отсюда получаем следующую систему для нахождения x:

$$\begin{cases} x \equiv -5(mod\, 8) \\ x \equiv 8(mod\, 11) \\ x \equiv 32(mod\, 13) \end{cases}$$

Упрощая и используя китайскую теорему об остатках получаем, что $x \equiv 19(mod\, 1144)$. Таким образом $x = 19 + 1144k$.

Задача. Показать, что сравнение $x^8 \equiv 23(mod\, 41)$ не имеет решений.

Решение

Воспользуемся тем фактом, что 6 - первообразный корень по модулю 41. Дискретно прологарифмируем данное сравнение по основанию 6. Получаем, что $\text{ind}_6 x^8 \equiv \text{ind}_6 23 (mod\, 40)$. То есть $8\text{ind}_6 x \equiv \text{ind}_6 23 (mod\, 40)$. Таким образом разрешимость исходного сравнения равносильна тому что $8|\text{ind}_6 23$, но $\text{ind}_6 23 \equiv 36 (mod\, 40)$. Таким образом данное сравнение не разрешимо.

1.2 Общий случай полиномиального сравнения.

Предложение.(Многочлен Тейлора) Пусть $f(x) = \sum\limits_{k=0}^{m} a_i x^i$, где $a_i \in \mathbb{Z}$ и $a_m \neq 0$. Тогда для любого целого a

$$f(x) = \sum_{k=0}^{m} \frac{f^{(k)}(a)}{k!}(x-a)^k.$$

Пример. Пусть $f(x) = x^3 + 2x + 3$ и $a = 1$. Тогда $P(x) = (x-1)^3 + 3(x-1)^2 + 5(x-1) + 6$.

Пусть $f(x) = x^5 + 3$ и $a = -2$. Тогда $P(x) = 120(x+2)^5 - 8(x+2)^4 + 40(x+2)^3 - 80(x+2)^2 + 80(x+2) - 29$.

Рассмотрим произвольное полиномиальное сравнение $f(x) \equiv 0 (mod\, n)$. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ - каноническое разложение числа n. Тогда исходное сравнение равносильно системе полиномиальных сравнений $f(x) \equiv 0 (mod\, p_i^{\alpha_i})$, $i \in \overline{1,r}$. Решив каждое из них мы найдём решение исходного сравнения с помощью китайской теоремы об остатках, поэтому далее рассмотрим сравнение $f(x) \equiv 0 (mod\, p^{\alpha})$, p - простое.

Для начала рассмотрим сравнение $f(x) \equiv 0 (mod\, p)$. Используя малую теорему Ферма($a^p \equiv a (mod\, p)$) переходим к сравнению $g(x) \equiv 0 (mod\, p)$, где $\deg f < p$. Найдём все его решения: $x \equiv x_1 (mod\, p)$, $x \equiv x_2 (mod\, p), \ldots, x \equiv x_r (mod\, p)$.

Далее рассмотрим сравнение $f(x) \equiv 0 (mod\, p^2)$. Отметим, что исходя из решения предыдущего сравнения $x = x_i + tp$, $t \in \mathbb{Z}$. То есть данное сравнение эквивалентно $f(x_i + tp) \equiv 0 (mod\, p^2)$. Воспользуемся формулой Тейлора для многочлена $f(x_i + tp)(a = x_i,\, x = x_i + tp)$: $f(x_i) + tpf'(x_i) \equiv 0 (mod\, p^2)$, так как коэффициенты остальных мономов в многочлене Тейлора целые и будут кратны p^2. Далее переходим к сравнению по модулю p: $\frac{f(x_i)}{p} + tf'(x_i) \equiv 0 (mod\, p)$. Находим всевозможные решения относительно t: $t \equiv t_{i,j} (mod\, p), \ldots t, \equiv t_{i,s} (mod\, p)$.

Отметим, что если $p^2 | f(x_i)$ и $p | f'(x_i)$,то подходит любое $0 \leq t \leq p-1$. Если же $p^2 \not| f(x_i)$ и $p | f'(x_i)$, то таких t не существует и данное линейное сравнение не имеет решений, а значит исходное полиномиальное сравнение также не имеет решений и мы заканчиваем работу алгоритма. В противном случае для каждого x_i существует единственное(по модулю p) подходящее t.

Далее рассмотрим сравнение $f(x) \equiv 0 (mod\, p^3)$. Отметим, что исходя из решения предыдущего сравнения $x = x_i + t_{i,j}p + zp^2 = x_{i,j} + zp^2$, $z \in \mathbb{Z}$. То

есть данное сравнение эквивалентно $f(x_{i,j}+zp^2) \equiv 0(mod\, p^3)$. Воспользуемся формулой Тейлора для многочлена $f(x_{i,j}+zp^2)(a = x_{i,j},\, x = x_{i,j}+zp^2)$: $f(x_{i,j})+zp^2f'(x_{i,j}) \equiv 0(mod\, p^3)$, так как коэффициенты остальных мономов в многочлене Тейлора целые и будут кратны p^3. Далее переходим к сравнению по модулю p: $\frac{f(x_{i,j})}{p^2} + zf'(x_{i,j}) \equiv 0(mod\, p)$. Находим всевозможные решения относительно z либо показываем, что их не существует и завершаем работу алгоритма. Пусть решения существуют: $z \equiv z_{i,j,1}(mod\, p), \dots t, \equiv z_{i,j,s}(mod\, p)$.

Далее рассматриваем сравнение $f(x) \equiv 0(mod\, p^4)$, причём $x = x_{i,j} + z_{i,j,k}p^2 + up^3 = x_{i,j,k} + up^3$, $u \in \mathbb{Z}$. Используем аналогичные рассуждения и находим u. Повторяем данную операцию пока не дойдём до p^α.

Задача. Найти все решения полиномиального сравнения $16x^8 - 8x^7 + 9x^4 - 1 \equiv 0(mod\, 196)$.

Решение

Заметим, что $196 = 2^2 \cdot 7^2$. Тогда исходная система равносильна системе сравнений

$$\begin{cases} 16x^8 - 8x^7 + 9x^4 - 1 \equiv 0(mod\, 4) \\ 16x^8 - 8x^7 + 9x^4 - 1 \equiv 0(mod\, 7^2) \end{cases}$$

Упростим первое сравнение: $x^4 \equiv 1(mod\, 4)$. Нетрудно видеть, что отсюда следует $x \equiv \pm 1(mod\, 4)$.

Далее обозначим $f(x) = 16x^8 - 8x^7 + 9x^4 - 1$. Рассмотрим сравнение $f(x) \equiv 0(mod\, 7)$. Отметим, что $f(x) \equiv 2x^2 - x + 2x^4 - 1 \equiv 2x^4 + 2x^2 - x - 1 \equiv (16x^4 - 1) + (2x^2 - x) \equiv (2x - 1)(x + 8x^3 + 4x^2 + 2x + 1) \equiv (2x - 1)(x^3 + x^2 + 3x + 1) \equiv (2x - 1)((x - 1)^3 + 2)(mod\, 7)$. То есть $2x - 1 \equiv 0(mod\, 7)$ или $(x - 1)^3 + 2 \equiv 0(mod\, 7)$. Первое сравнение имеет единственное решение $x \equiv 4(mod\, 7)$, второе не имеет решений. Таким образом $x = 4 + 7t$, $t \in \mathbb{Z}$. Тогда по формуле Тейлора

$$f(4) + 7tf'(4) \equiv 28 + 14t \equiv 0(mod\, 49)$$

Это сравнение равносильно $2t \equiv 3(mod\, 7)$. То есть $t \equiv 5(mod\, 7)$. Тогда решениями сравнения $f(x) \equiv 0(mod\, 49)$ являются $x \equiv 39(mod\, 49)$. Тогда решение изначального сравнения может быть найдено исходя из следующих систем сравнений:

$$\begin{cases} x \equiv 1(mod\, 4) \\ x \equiv 39(mod\, 49) \end{cases}$$

$$\begin{cases} x \equiv -1(mod\, 4) \\ x \equiv 39(mod\, 49) \end{cases}$$

Используя китайскую теорему об остатках получаем, что $x \equiv 137(mod\, 196)$ либо $x \equiv 39(mod\, 196)$. Таким образом $x = 137 + 196k$ либо $x = 39 + 196k$.

2 Лемма Гензеля.

Определение. Пусть p - простое число. Через $v_p(a)$ обозначим функцию $v_p : \mathbb{Z} \to \mathbb{N}_0$ такую что $v_p(a)$ равно максимальной степени p делящей a.

Пример. Пусть $n = 1144$, $p = 11$, тогда $v_{11}(1144) = 1$. Аналогично $v_2(1144) = 3$ и $v_{131}(1144) = 1$. В тоже время $v_5(1144) = v_7(1144) = 0$.

Также $v_3(63) = 2$, $v_7(63) = 1$.

Замечание. Нетрудно видеть, что $v_p(ab) = v_p(a) + v_p(b)$. Отсюда также следует, что $v_p(a^k) = kv_p(a)$.

Предложение.(Лемма Гензеля для нечётного p). Пусть $p|(a-b)$ и $n \in \mathbb{N}$, тогда

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Следствие. Если $(p, n) = 1$ и $p|(a - b)$, то $v_p(a^n - b^n) = v_p(a - b)$.

Следствие. Пусть $p|(a + b)$ и n - нечётное, тогда

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n).$$

Предложение.(Лемма Гензеля для $p = 2$). Пусть $4|(a - b)$ и $n \in \mathbb{N}$, тогда

$$v_2(a^n - b^n) = v_2(b - b) + v_2(n).$$

Следствие. Если $(2, n) = 1$ и $4|(a - b)$, то $v_2(a^n - b^n) = v_2(a - b)$.

Следствие. Пусть $4|(a + b)$ и n - нечётное, тогда

$$v_2(a^n + b^n) = v_2(a + b) + v_2(n).$$

Задача. Определить, в какой степени 5 входит в разложение $7^{10000} - 2^{10000}$.

Доказательство

Используем лемму Гензеля для нечётного $p = 5$. Пусть $a = 7$ и $b = 2$. Тогда $5|(a - b)$. То есть

$$v_5(7^{10000} - 2^{10000}) = v_5(7 - 2) + v_5(10000) = 1 + 4 = 5.$$

Задача. Определить, в какой степени 5 входит в разложение $3^{10000} - 2^{10000}$.

Используем лемму Гензеля для нечётного $p = 5$. Пусть $a = 9 = 3^2$ и $b = 4 = 2^2$. Тогда $5|(a - b)$. То есть

$$v_5(3^{10000} - 2^{10000}) = v_5(9^{5000} - 4^{5000}) = v_5(9 - 4) + v_5(5000) = 1 + 4 = 5.$$

Задача. Доказать, что 2 является первообразным корнем по модулю 3^n.

Доказательство

Пусть δ - показатель которому принадлежит 2 по модулю 3^n. Отметим, что $\delta|\varphi(3^n) = 2 \cdot 3^{n-1}$. То есть $\delta = 3^k$ или $\delta = 2 \cdot 3^k$, где $k \in \{0, 1, 2, \ldots, n-1\}$. Отметим, что первый случай невозможен, так как тогда $2^{3^k} \equiv (-1)^{3^k} \equiv -1 (mod\, 3^n)$. Таким образом $\delta = 2 \cdot 3^k$.

Согласно определению $2^\delta \equiv 1(mod\, 3^n)$, то есть $2^{2\cdot 3^k} \equiv 4^{3^k} \equiv 1(mod\, 3^n)$. Это сравнение равносильно тому, что $v_3(4^{3^k} - 1) \geq n$. Используем лемму Гензеля:

$$v_3(4^{3^k} - 1) = v_3(4^{3^k} - 1^{3^k}) = v_3(3) + v_3(3^k) = k + 1.$$

То есть $k \geq n - 1$. А значит $\delta = 2 \cdot 3^{n-1} = \varphi(3^n)$ и 2 - первообразный корень по модулю 3^n.

3 Задачи для самостоятельного решения.

Задача 1

a)Решите сравнение $x^3 + 16x + 27 \equiv 0(mod\, 900)$.
b)Решите сравнение $x^{12} \equiv 25(mod\, 41)$.
Указание. 6 - первообразный корень по модулю 41.
c)Найдите максимальную степень 7 делящую $3^{7007} + 4^{7007}$.

Задача 2

Обозначим через $\omega(m, n) = |\{x^m \equiv 1(mod\, n) | 0 \leq x < n\}|$, то есть число решений сравнения $x^m \equiv 1(mod\, n)$ не превосходящих n.
a)Докажите, что $\omega(m, kl) = \omega(m, k)\omega(m, l)$, $(k, l) = 1$.
b)Вычислите $\omega(m, p^\alpha)$, где p - простое нечётное, $\alpha \in \mathbb{N}$.
c)Вычислите $\omega(m, 2^\alpha)$, $\alpha \in \mathbb{N}$.
d)Вычислите $\omega(m, n)$? если известно каноническое разложение n.
e)Покажите, что $\omega(m, n) | \varphi(n)$.
f**)Пусть $x^m \equiv 1(mod\, n)$. Покажите, что $x^{\omega(m,n)} \equiv 1(mod\, n)$.

Задача 3

Пусть k - натуральное число. Найдите все такие l, что $3^k | 2^l - 1$.