# Семинар 8

# Полиномиальные сравнения
# Символы Лежандра
# Первообразные корни

***Полиномиальные сравнения***

**8.1.** Пользуясь малой теоремой Ферма или теоремой Эйлера, решите сравнения:

а) $x^5 + x^2 + x + 1 \equiv 0 \pmod 3$;
б) $x^{100} + x + 1 \equiv 0 \pmod 5$;
в) $x^{239} + x^{97} + 2 \equiv 0 \pmod{45}$.

**8.2.** При помощи китайской теоремы об остатках решите сравнения:

а) $x^2 + 2x + 5 \equiv 0 \pmod{15}$;
б) $x^3 + 8x - 2 \equiv 0 \pmod{21}$;
в) $x^6 + x + 5 \equiv 0 \pmod{105}$.

**8.3.** Используя метод подъёма решения решите сравнения:

а) $x^4 + 7x + 4 \equiv 0 \pmod{27}$;
б) $9x^2 + 11x + 2 \equiv 0 \pmod{64}$;
в) $x^2 + 7x + 5 \equiv 0 \pmod{125}$;
г) $x^3 + 2x + 3 \equiv 0 \pmod{25}$;
д) $x^2 + x + 4 \equiv 0 \pmod{81}$;
е) $x^3 + x - 10 \equiv 0 \pmod{27}$;
ж) $x^2 + 7x + 4 \equiv 0 \pmod{108}$;
з) $x^3 + 4x + 1 \equiv 0 \pmod{225}$;
и) $x^3 + 2x + 3 \equiv 0 \pmod{75}$.

**8.4.** Решите системы сравнений:

а) $\begin{cases} x^2 + x \equiv 0 \pmod 9 \\ x^3 \equiv 2 \pmod{125} \end{cases}$;
б) $\begin{cases} x \equiv 3 \pmod 7 \\ x^2 \equiv 44 \pmod{7^2} \\ x^3 \equiv 111 \pmod{7^3} \end{cases}$.

**8.5.** Докажите, что для любого простого $p$ сравнение $x^2 + y^2 + 1 \equiv 0 \pmod p$ разрешимо.

**8.6.** Докажите, что уравнение $x^2 - y^3 = a$ не имеет решений в целых $x, y$ для
а) $a = -5$;
б) $a = 7$;
в) $a = (2b)^3 - 1$, где $b$ — нечётное целое число **(Теорема Лебега)**.

**8.7.** Пусть $\alpha \geqslant 3$. Докажите, что нечётное $a$ является квадратичным вычетом по модулю $2^\alpha$ тогда и только тогда, когда $a \equiv 1 \pmod 8$.

***Символы Лежандра***

**8.8.** Вычислите значения символа Лежандра:

а) $\left(\dfrac{111}{541}\right)$; б) $\left(\dfrac{529}{601}\right)$; в) $\left(\dfrac{2108}{2003}\right)$; г) $\left(\dfrac{19525}{1847}\right)$.

**8.9.** Выясните, разрешимы ли сравнения:

а) $x^2 \equiv 68 \pmod{113}$;
б) $x^2 \equiv 219 \pmod{383}$;
в) $x^2 + 7x + 45 \equiv 0 \pmod{409}$;
г) $5x^2 + 11x - 91 \equiv 0 \pmod{379}$.

**8.10.** Докажите, что для любого простого $p$ сравнение $(x^2 - 11)(x^2 - 17)(x^2 - 187) \equiv 0 \pmod p$ разрешимо.

**8.11.** Найдите все простые числа $p$, для которых разрешимо сравнение $x^2 - 2 \equiv 0 \pmod p$. Докажите, что существует бесконечно много простых чисел вида $8n - 1$.

**8.12.** Найдите все простые числа $p$, для которых разрешимо сравнение $x^2 + 2 \equiv 0 \pmod p$. Докажите, что существует бесконечно много простых чисел вида $8n + 3$.

**8.13.** Пусть $p, q$ — простые числа, причём $q = 2p + 1$, $p \equiv 3 \pmod 4$, $p > 3$. Докажите, что число $2^p - 1$ является составным.

**8.14.** Пусть $p$ — простое число, $p > 3$. Не используя квадратичный закон взаимности, вычислите символ Лежандра $\left(\frac{3}{p}\right)$. Для этого докажите равносильность следующих трёх утверждений:

а) $\left(\frac{-3}{p}\right) = 1$;

б) сравнение $x^2 + x + 1 \equiv 0 \pmod{p}$ разрешимо;

в) $p \equiv 1 \pmod{3}$.

**8.15.** Докажите, что если $p$ — нечётное простое число, $a, b$ — целые числа, $p \nmid a$, то

$$\sum_{n=1}^{p} \left(\frac{an+b}{p}\right) = 0.$$

**8.16* Тест Пепина.** Докажите, что число Ферма $f_n = 2^{2^n} + 1$ является простым тогда и только тогда, когда выполняется сравнение

$$3^{(f_n-1)/2} \equiv -1 \pmod{f_n}.$$

***Символы Якоби***

**8.17.** Решите задачу 8.8, пользуясь свойствами символа Якоби.

**8.18.** Выясните, разрешимы ли сравнения:

а) $x^2 \equiv 17 \pmod{21}$;

б) $x^2 \equiv 19 \pmod{35}$;

в) $x^2 \equiv 70 \pmod{187}$.

**8.19.** Пусть $P$ — нечётное натуральное число, отличное от квадрата. Докажите, что существует такое целое $a$, что $\left(\frac{a}{P}\right) = -1$.

**8.20.** Пусть $P$ — такое же, как в предыдущей задаче. Докажите, что ровно половина приведённых вычетов по модулю $P$ удовлетворяет соотношению $\left(\frac{a}{P}\right) = -1$.

**8.21.** Обобщите на случай произвольного нечётного знаменателя задачу 8.15.

***Первообразные корни***

**8.22.** Пусть $n \in \mathbb{N}$, $n \geqslant 2$. Сколько существует первообразных корней по модулю $n$?

**8.23.** Найдите первообразные корни по модулям 9, 18, 25, 27, 41, 49, 50, 81, 125, 243, 250, 343.

**8.24.** Решите сравнения:

а) $3^x \equiv 2 \pmod{17}$;

б) $2^x \equiv 11 \pmod{25}$;

в) $2^x \equiv 11 \pmod{21}$;

г) $x^3 \equiv 11 \pmod{17}$;

д) $x^{119} \equiv 2 \pmod{19}$;

е) $x^7 \equiv 17 \pmod{33}$.

***Резерв***

**8.25.** Пусть $p$ — простое число, $m$ — натуральное. Докажите, что

$$\sum_{x=1}^{p} x^m \equiv \begin{cases} -1 \pmod{p}, & \text{если } p-1 \mid m, \\ 0 \pmod{p}, & \text{если } p-1 \nmid m. \end{cases}$$

**8.26.** Пусть $p$ — простое число, $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, $\deg f < n(p-1)$. Докажите, что

$$\sum_{\substack{1 \leqslant x_i \leqslant p \\ 1 \leqslant i \leqslant n}} f(x_1, \ldots, x_n) \equiv 0 \pmod{p}.$$

**8.27.** Пусть $p$ — простое число, $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, $\deg f < n - 1$. Докажите, что число решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ в $(\mathbb{Z}_p)^n$ делится на $p$.

**8.28.** Пусть $p$ — простое число, $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ — однородный многочлен, $\deg f < n$. Докажите, что сравнение $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ имеет ненулевое решение.