Теория чисел

ДЗ 5

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Решите сравнение $x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod{54}$.

Решение:

Исходное сравнение равносильно системе

$$\begin{cases} x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod 2 \\ x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod{3^3} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 \pmod 2 \\ x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod{3^3} \end{cases}$$

Методом подъема решений решим второе сравнение

$$x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod 3 \Rightarrow \left[\begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 3 \end{array}\right.$$

Поднимаем 1

$$x = 1 + 3t$$

$$f(1+3t) \equiv 0 \pmod 9 \Leftrightarrow f(1) + 3tf'(1) \equiv 0 \pmod 9 \Leftrightarrow -12 + 3t \cdot (-2) \equiv 0 \pmod 9 \Leftrightarrow -3 + 3t \equiv 0 \pmod 9 \Leftrightarrow$$

$$\Leftrightarrow t \equiv 1 \pmod 3 \Rightarrow t = 3t_1 + 1 \Rightarrow x = 4 + 9t_1 \Rightarrow x \equiv 4 \pmod 9$$

$$f(4+9t_1) \equiv 0 \pmod{27} \Leftrightarrow f(4) + 9t_1 f'(4) \equiv 0 \pmod{27} \Leftrightarrow 9 + 9t_1 \cdot 1 \equiv 0 \pmod{27} \Leftrightarrow t_1 \equiv 2 \pmod 3 \Rightarrow$$

$$\Rightarrow t_1 = 2 + 3t_2 \Rightarrow x = 22 + 27t_2 \Rightarrow x \equiv 22 \pmod{27}$$

Поднимаем 2

$$x = 2 + 3t$$

$$f(2+3t) \equiv 0 \pmod 9 \Leftrightarrow f(2) + 3tf'(2) \equiv 0 \pmod 9 \Leftrightarrow 0 + 0 \equiv 0 \pmod 9 \Rightarrow t \equiv 0; 1; 2 \pmod 3$$

$$\Rightarrow \left[\begin{array}{l} x \equiv 2 \pmod 9 \\ x \equiv 5 \pmod 9 \\ x \equiv 8 \pmod 9 \end{array}\right.$$

Поднимаем 2

$$x = 2 + 9t$$

$$f(2+9t) \equiv 0 \pmod{27} \Leftrightarrow f(2) + 9tf'(2) \equiv 0 \pmod{27} \Leftrightarrow 9 + 9t \cdot 0 \equiv 0 \pmod{27}, \text{но } 9 \not\equiv 0 \pmod{27} \Rightarrow$$

не поднимается

Поднимаем 5

$$x = 5 + 9t$$

$$f(5+9t) \equiv 0 \pmod{27} \Leftrightarrow f(5) + 9tf'(5) \equiv 0 \pmod{27} \Leftrightarrow 0 + 9t \cdot 0 \equiv 0 \pmod{27} \Leftrightarrow$$

$$\Leftrightarrow t \equiv 0; 1; 2 \pmod 3 \Rightarrow x \equiv 5; 14; 23 \pmod{27}$$

Поднимаем 8

$$x = -1 + 9t$$

$$f(-1+9t) \equiv 0 \pmod{27} \Leftrightarrow f(-1) + 9tf'(-1) \equiv 0 \pmod{27} \Leftrightarrow 0 + 9t \cdot 0 \equiv 0 \pmod{27} \Leftrightarrow$$

$$\Leftrightarrow t \equiv 0; 1; 2 \pmod 3 \Rightarrow x \equiv 26; 8; 17 \pmod{27}$$

Итого, имеем систему

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv (22; 5; 14; 23; 26; 8; 17) \pmod{27} \end{cases}$$

Общее решение имеет вид $x = 27k + a \Rightarrow 27k + a \equiv 1 \pmod 2 \Rightarrow k + a \equiv 1 (\mathrm{mod}\, 2) \Rightarrow a$ и k разной четности.

1. $a = 22 \Rightarrow k = 2m + 1 \Rightarrow x = 27(2m + 1) + 22 = 54m + 49$
2. $a = 5 \Rightarrow k = 2m \Rightarrow x = 27(2m) + 5 = 54m + 5$
3. $a = 14 \Rightarrow k = 2m + 1 \Rightarrow x = 27(2m + 1) + 14 = 54m + 41$
4. $a = 23 \Rightarrow k = 2m \Rightarrow x = 27(2m) + 23 = 54m + 23$
5. $a = 26 \Rightarrow k = 2m + 1 \Rightarrow x = 27(2m + 1) + 26 = 54m + 53$
6. $a = 8 \Rightarrow k = 2m + 1 \Rightarrow x = 27(2m + 1) + 8 = 54m + 35$
7. $a = 17 \Rightarrow k = 2m \Rightarrow x = 27(2m) + 17 = 54m + 17$

Ответ:

$x \equiv 49, 5, 41, 23, 53, 35, 17 \pmod{54}$

Задание 2

Найдите количество решений сравнения $x^2 - 25 \equiv 0 \pmod{16^{19} \cdot 19^{91} \cdot 91^{16}}$

Решение:

Исходное сравение равносильно системе

$$\begin{cases} x^2 - 25 \equiv 0 \pmod{2^{76}} \\ x^2 - 25 \equiv 0 \pmod{19^{91}} \\ x^2 - 25 \equiv 0 \pmod{13^{16}} \\ x^2 - 25 \equiv 0 \pmod{7^{16}} \end{cases}$$

Заметим, что $25 \equiv 1 \pmod 8 \Rightarrow$ сравнение $x^2 - 25 \equiv 0 \pmod{2^{76}}$ имеет ровно 4 решения(общее утверждение доказано на семинаре). 19 не делит 25, 13 не делит 25, 7 не делит 25, значит сравнения $x^2 - 25 \equiv 0 \pmod{19^{91}}, x^2 - 25 \equiv 0 \pmod{13^{16}}, x^2 - 25 \equiv 0 \pmod{7^{16}}$ имеют ровно по два решения соответственно(общее утверждение доказано на семинаре). Значит всего $4 \cdot 2 \cdot 2 \cdot 2 = 32$ решения.

Ответ:

32

Задание 3

Пусть p —нечетное простое. Докажите, что количество решений сравнения

$$x^2 \equiv y^2 \pmod p$$

равно $2p-1$.

Решение:

Пусть $y^2 \equiv 0 \pmod p \Leftrightarrow y \equiv 0 \pmod p$, тогда сравнение $x^2 \equiv 0 \pmod p$ имеет единственное решение $x \equiv 0 \pmod p$. Далее считаем, что x и y не сравнимы с нулем по модулю p. У нас есть $p-1$ вариант зафиксировать вычет для y по модулю p. Для каждого такого вычета сравнение $x^2 \equiv y^2 \pmod p$ будет иметь ровно 2 решения, так как p не делит y. Имеем $2 \cdot (p-1) + 1 = 2p-1$ решений.

Ответ:

ч.т.д

Задание 4

Докажите, что сравнение $(x^2 - ab)(x^2 - bc)(x^2 - ac) \equiv 0 \pmod p$ разрешимо при любом простом p и любых $a, b, c \in \mathbb{Z}$.

Решение:

Это сравнение разрешимо, если хотя бы одна из скобок делится на p. Пусть это не так, тогда числа ab, bc, ac являются квадратичными невычетами. С одной стороны, $ab \cdot bc \cdot ac = a^2b^2c^2 = (abc)^2$ является квадратичным вычетом(так как это квадрат некоторого числа). Но $ab \cdot bc$ является квадратичным вычетом(произведение квадратичных невычетом–квадратичный вычет, доказано на лекции). Произведение квадратичного вычета и невычета также является квадратичным невычетом(следует из критерия Эйлера квадратичности вычета). Тогда $(ab \cdot bc) \cdot ac$ является квадратичным невычетом. Получили противоречие, значит среди ab, bc, ac есть квадратичный вычет, значит какая-то скобка кратна p.

Ответ:

ч.т.д

Задание 5

Вычислите сумму символов Лежандра

$$\text{а) } \sum_{x=0}^{58} \left(\frac{15x+79}{59} \right); \text{б) } \sum_{x=0}^{57} \left(\frac{15x+79}{59} \right)$$

Решение:

а) 59 не делит 15$\Rightarrow$ сумма нулевая(на семинаре нашли все возможные значения суммы $\sum\limits_{x=0}^{p-1} \left(\frac{ax+b}{p} \right)$)

б) $\sum\limits_{x=0}^{57} \left(\frac{15x+79}{59} \right) = \sum\limits_{x=0}^{58} \left(\frac{15x+79}{59} \right) - \left(\frac{15 \cdot 58+79}{59} \right) = 0 - \left(\frac{949}{59} \right) = -1$ $(949 \equiv 5 \pmod{59}$ – кв. вычет))

Ответ:

0;-1