Домашнее задание на 07.02 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 Рассмотрим сравнение $x^3 - 17x^2 - 7x + 11 \equiv 0 \pmod{54}$.

Модуль $54 = 2 \cdot 3^3$. Решим систему сравнений по модулям 2 и 27.

1) По модулю 2:

   Подстановка $x = 0$ и $x = 1$:

$$x \equiv 0 \pmod 2 : 1 \not\equiv 0 \pmod 2$$

$$x \equiv 1 \pmod 2 : 0 \equiv 0 \pmod 2$$

   Решение: $x \equiv 1 \pmod 2$

2) По модулю 27:

   Сначала решаем по модулю 3:

$$x^3 - 2x^2 + 2x + 2 \equiv 0 \pmod 3$$

   Проверка $x = 0, 1, 2$:

$$x \equiv 1 \pmod 3 \text{ и } x \equiv 2 \pmod 3 \text{ — решения}$$

   Подъем решений до модуля 9:

   Для $x \equiv 1 \pmod 3$:

$$x \equiv 4 \pmod 9$$

   Для $x \equiv 2 \pmod 3$:

$$x \equiv 2 \pmod 9$$

   Подъем до модуля 27:

$x \equiv 4 \pmod 9$ даёт

$$x \equiv 13 \pmod{27}$$

$x \equiv 2 \pmod 9$ не даёт решений.

Объединение решений:

$$\begin{cases} x \equiv 1 \pmod 2, \\ x \equiv 13 \pmod{27}. \end{cases} \implies x \equiv 13 \pmod{54}$$

Ответ: $x \equiv 13 \pmod{54}$

№2 Рассмотрим сравнение

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

Модуль раскладывается:

$$N = 2^{76} \cdot 19^{91} \cdot 7^{16} \cdot 13^{16}$$

Количество решений равно произведению количеств решений по каждому простому множителю:

1) Для 2^{76}:

   Уравнение $x^2 \equiv 25 \pmod{2^{76}}$. Так как $25 \equiv 1 \pmod 8$, количество решений — 4.

2) Для 19^{91}, 7^{16}, 13^{16}:

   Уравнение $x^2 \equiv 25 \pmod{p^k}$ имеет два решения ($x \equiv 5$ и $x \equiv -5 \pmod{p^k}$), так как $5 \not\equiv -5 \pmod{p^k}$

Итоговое количество решений:

$$4 \cdot 2 \cdot 2 \cdot 2 = 32$$

Ответ: 32

№3 Рассмотрим сравнение $x^2 \equiv y^2 \pmod{p}$, где p — нечётное простое число. Перепишем его в виде:

$$(x - y)(x + y) \equiv 0 \pmod{p}.$$

Так как p - простое, то:

$$\begin{cases} x \equiv y \pmod{p} \\ x \equiv -y \pmod{p} \end{cases}$$

1) Количество пар для $x \equiv y \pmod{p}$:

   Для каждого $x \in \{0, 1, 2, ..., p-1\}$ существует ровно один $y \equiv x \pmod{p}$. Таким образом, количество таких пар равно p.

2) Количество пар для $x \equiv -y \pmod{p}$:

   Для каждого $x \in \{0, 1, 2, ..., p-1\}$ существует ровно один $y \equiv -x \pmod{p}$. Количество таких пар также равно p.

Пара $(0, 0)$ удовлетворяет обоим условиям. Таким образом, она учтена дважды. Чтобы получить количество уникальных решений, вычтем 1 повторяющуюся пару.

Итоговое количество решений:

$$p + p - 1 = 2p - 1.$$

Что и требовалось доказать.

№4 Рассмотрим сравнение

$$(x^2 - ab)(x^2 - bc)(x^2 - ac) \equiv 0 \pmod{p}$$

Для его разрешимости необходимо, чтобы хотя бы одно из уравнений:

$$x^2 \equiv ab \pmod{p}, \quad x^2 \equiv bc \pmod{p}, \quad x^2 \equiv ac \pmod{p}$$

имело решение. Рассмотрим два случая.

1) Случай 1:

   Хотя бы одно из чисел a, b, c делится на p.

   Пусть, например, $a \equiv 0 \pmod{p}$. Тогда:

$$ab \equiv 0 \pmod{p}$$

$$ac \equiv 0 \pmod{p}$$

   Уравнения $x^2 \equiv 0 \pmod{p}$ имеют решение $x \equiv 0 \pmod{p}$. Таким образом, в этом случае сравнение разрешимо.

2) Случай 2:

   Все числа a, b, c не делятся на p.

   В этом случае a, b, c обратимы, а значит и ab, bc, ac обратимы. Покажем, что хотя бы один из

$$ab, bc, ac$$

   является квадратичным вычетом.

   Предположим противное: все три элемента ab, bc, ac — квадратичные невычеты. Тогда их произведение:

$$(ab)(bc)(ac) = a^2b^2c^2 = (abc)^2$$

Квадрат любого элемента является квадратичным вычетом, поэтому $(abc)^2$ — вычет. Однако произведение трёх невычетов вычисляется как:

$$\text{невычет} \cdot \text{невычет} \cdot \text{невычет} = (\text{вычет}) \cdot \text{невычет} = \text{невычет}.$$

Получаем противоречие: $(abc)^2$ одновременно является вычетом и невычетом. Следовательно, предположение неверно, и хотя бы один из элементов ab, bc, ac — квадратичный вычет. Соответствующее уравнение $x^2 \equiv \text{вычет} \pmod{p}$ имеет решение.

В обоих случаях сравнение $(x^2 - ab)(x^2 - bc)(x^2 - ac) \equiv 0 \pmod{p}$ разрешимо. Таким образом, утверждение доказано для любого простого p и любых $a, b, c \in \mathbb{Z}$.

№5 а) $\sum_{x=0}^{58} \left(\frac{15x+79}{59}\right)$

Символ Лежандра $\left(\frac{15x+79}{59}\right)$ преобразуется к $\left(\frac{15x+20}{59}\right)$, так как $79 \equiv 20 \pmod{59}$.

Коэффициент 15 взаимно прост с 59, поэтому $15x+20$ пробегает все вычеты по модулю 59 при $x = 0, 1, \ldots, 58$.

Сумма символов Лежандра по всем $a \pmod{59}$ (включая 0) равна 0. Это следует из того, что количество квадратичных вычетов и невычетов одинаково, и их вклады взаимно сокращаются.

Ответ: 0

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

Так как верхний предел $x = 57$, а при $x = 58$ выражение $15x+20$ даёт $5 \pmod{59}$, нужно посчитать $\left(\frac{5}{59}\right)$.

$$\left(\frac{5}{59}\right) = 1 \text{ т.к. } 5 \equiv 64 \equiv 8^2 \pmod{59}$$

Получается, что:

$$\sum_{x=0}^{57}\left(\frac{15x+79}{59}\right)=\sum_{x=0}^{58}\left(\frac{15x+79}{59}\right)-\left(\frac{5}{59}\right)=0-1=-1$$

Ответ: -1