Домашнее задание на 28.02 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 $x^2 \equiv 3 \pmod{143}$

Найдём символ Якоби:

$$\left(\frac{3}{143}\right) = \left(\frac{143}{3}\right) \cdot (-1)^{\frac{142 \cdot 2}{4}} = \left(\frac{2}{3}\right) \cdot (-1)^{71} = -2 \pmod 3 = 1$$

Следовательно, сравнение разрешимо.

№2 $x^2 \equiv 3 \pmod{119}$

Найдём символ Якоби:

$$\left(\frac{3}{119}\right) = \left(\frac{3}{17}\right) \cdot \left(\frac{3}{7}\right) = 3^8 \pmod{17} \cdot 3^3 \pmod 7 = (-1) \cdot (-1) = 1$$

Следовательно, сравнение разрешимо

№3 Мы знаем, что:

$$\sum_{n=1}^{1001} \left(\frac{n}{1001}\right) = \sum_{n=1}^{499} \left(\frac{n}{1001}\right) + \left(\frac{500}{1001}\right) + \left(\frac{501}{1001}\right) + \sum_{n=502}^{1001} \left(\frac{n}{1001}\right) = 0$$

В силу симметрии символа Якоби ($\left(\frac{n}{1001}\right) = \left(\frac{1001-n}{1001}\right)$) это сводится к:

$$2\sum_{n=1}^{499} \left(\frac{n}{1001}\right) + 2\left(\frac{500}{1001}\right) = 0 \Leftrightarrow \sum_{n=1}^{499} \left(\frac{n}{1001}\right) = -\left(\frac{500}{1001}\right)$$

Найдём правую часть:

$$-\left(\frac{500}{1001}\right) = -(\left(\frac{500}{7}\right) \cdot \left(\frac{500}{11}\right) \cdot \left(\frac{500}{13}\right)) = -(\left(\frac{3}{7}\right) \cdot \left(\frac{5}{11}\right) \cdot \left(\frac{6}{13}\right)) =$$

$= -(3^3 \pmod 7) \cdot 5^5 \pmod{11} \cdot 6^6 \pmod{13}) = -((-1)\cdot 1 \cdot (-1)) = -1$

Ответ: -1

№4 Пусть P — нечётное число, $P \geqslant 3$. Требуется доказать, что символ Лежандра $\left(\frac{2}{P}\right) = (-1)^{\left[\frac{P+1}{4}\right]}$. Известно, что $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$. Достаточно показать, что показатели степени совпадают по модулю 2, т.е.:

$$\frac{P^2-1}{8} \equiv \left[\frac{P+1}{4}\right] \pmod 2.$$

Так как P - нечётное достаточно рассмотреть только два случая в зависимости от остатка P при делении на 4:

1) $P = 4k+1$, где $k \in \mathbb{Z}$

Вычислим показатель для символа Лежандра:

$$\frac{P^2-1}{8} = \frac{(4k+1)^2-1}{8} = \frac{16k^2+8k}{8} = 2k^2+k.$$

Целая часть:

$$\left[\frac{P+1}{4}\right] = \left[\frac{4k+2}{4}\right] = [k+0.5] = k.$$

По модулю 2:

$$2k^2+k \equiv k \pmod 2, \quad k \equiv k \pmod 2.$$

2) $P = 4k+3$, где $k \in \mathbb{Z}$

Вычислим показатель для символа Лежандра:

$$\frac{P^2-1}{8} = \frac{(4k+3)^2-1}{8} = \frac{16k^2+24k+8}{8} = 2k^2+3k+1.$$

Целая часть:

$$\left[\frac{P+1}{4}\right] = \left[\frac{4k+4}{4}\right] = [k+1] = k+1.$$

По модулю 2:

$$2k^2 + 3k + 1 \equiv k+1 \pmod 2, \quad k+1 \equiv k+1 \pmod 2.$$

В обоих случаях показатели степени совпадают по модулю 2, следовательно:

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = (-1)^{\left[\frac{P+1}{4}\right]}.$$

№5 Пусть $P = 4ab - 1$, где $a, b \in \mathbb{N}$. Предположим, что сравнение $x^2 \equiv -a \pmod P$ разрешимо. Тогда существует $x \in \mathbb{Z}$, такое что:

$$x^2 + a \equiv 0 \pmod P \implies x^2 + a = kP \quad \text{для некоторого } k \in \mathbb{Z}.$$

Подставляя $P = 4ab - 1$, получим:

$$x^2 + a = k(4ab - 1) \implies x^2 + a + k = 4abk.$$

Рассмотрим это равенство по модулю 4. Поскольку квадрат любого числа по модулю 4 равен 0 или 1, левая часть $x^2 + a + k$ может быть:

$0 + a + k \equiv a + k \pmod 4$, если $x^2 \equiv 0 \pmod 4$

$1 + a + k \equiv a + k + 1 \pmod 4$, если $x^2 \equiv 1 \pmod 4$

Правая часть $4abk \equiv 0 \pmod 4$. Следовательно:

Если $x^2 \equiv 0 \pmod 4$, то $a + k \equiv 0 \pmod 4$

Если $x^2 \equiv 1 \pmod 4$, то $a + k \equiv 3 \pmod 4$

Далее, умножим исходное сравнение $x^2 \equiv -a \pmod P$ на $4b$:

$$4bx^2 \equiv -4ab \pmod P.$$

Так как $4ab = P + 1$, подставляем:

$$4bx^2 \equiv -(P+1) \equiv -1 \pmod{P}.$$

Получаем:

$$(2x)^2 \cdot b \equiv -1 \pmod{P} \implies m^2 \equiv -4b \pmod{P}, \quad \text{где } m = 2x.$$

Рассмотрим символ Лежандра $\left(\frac{-4b}{P}\right)$. Поскольку $P \equiv 3 \pmod 4$, имеем:

$$\left(\frac{-1}{P}\right) = -1, \quad \left(\frac{4}{P}\right) = 1.$$

Таким образом:

$$\left(\frac{-4b}{P}\right) = \left(\frac{-1}{P}\right) \cdot \left(\frac{4}{P}\right) \cdot \left(\frac{b}{P}\right) = -1 \cdot \left(\frac{b}{P}\right).$$

Если сравнение $m^2 \equiv -4b \pmod{P}$ разрешимо, то $\left(\frac{-4b}{P}\right) = 1$, откуда:

$$-1 \cdot \left(\frac{b}{P}\right) = 1 \implies \left(\frac{b}{P}\right) = -1.$$

Применим квадратичный закон взаимности для $\left(\frac{b}{P}\right)$. Поскольку $P \equiv -1 \pmod{b}$, то:

$$\left(\frac{b}{P}\right) = \left(\frac{-1}{b}\right) \cdot (-1)^{\frac{(b-1)(P-1)}{4}}.$$

Учитывая $P = 4ab - 1$, получаем:

$$\frac{(b-1)(4ab-2)}{4} = \frac{(b-1)(2ab-1)}{2}.$$

Если b нечетно, $b - 1$ четно, и выражение сводится к $(-1)^{(b-1)/2}$. Тогда:

$$\left(\frac{b}{P}\right) = (-1)^{(b-1)/2} \cdot (-1)^{(b-1)/2} = 1.$$

Это противоречит $\left(\frac{b}{P}\right) = -1$. Аналогичное противоречие возникает для $\left(\frac{a}{P}\right)$.