Домашнее задание на 21.02 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 $x^2 \equiv 219 \pmod{383}$2 Найдём символ Лежандра:

$$\left(\frac{219}{383}\right) = \left(\frac{383}{219}\right) \cdot (-1)^{\frac{218 \cdot 382}{4}} = -\left(\frac{383}{219}\right) = -\left(\frac{64}{219}\right) = -\left(\frac{2^6}{219}\right) = -\left(\frac{2}{219}\right)^6$$

$$= -\left((-1)^{\frac{219^2-1}{8}}\right)^6 = -(-1)^{219^2-1} = -1$$

Ответ: неразрешимо

№2 Рассмотрим:

$$\left(\frac{5}{p}\right) = (-1)^{\frac{4(p-1)}{4}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

При $p = \pm 1 \pmod 5$:

$$\left(\frac{p}{5}\right) = 1$$

При $p = \pm 2 \pmod 5$:

$$\left(\frac{p}{5}\right) = -1$$

Получаем, что:

$$\left(\frac{5}{p}\right) = \begin{cases} 1, \text{ при } p \equiv \pm 1 \pmod 5 \\ -1, \text{ при } p \equiv \pm 2 \pmod 5 \end{cases}$$

№3 Модуль $128 \cdot 151 \cdot 199$ раскладывается на взаимно простые множители:

$$2^7,\ 151,\ 199$$

Получаем систему:

$$\begin{cases} x^2+2x+72=0 \pmod{2^7} \\ x^2+2x+72=0 \pmod{151} \\ x^2+2x+72=0 \pmod{199} \end{cases} \Leftrightarrow \begin{cases} (x+1)^2=-71 \pmod{2^7} \\ (x+1)^2=-71 \pmod{151} \\ (x+1)^2=-71 \pmod{199} \end{cases}$$

У первого сравнения, очевидно, 2 решения, а для остальных найдём символы Лежандра:

$$\left(\frac{-71}{151}\right)=\left(\frac{80}{151}\right)=\left(\frac{2^4\cdot 5}{151}\right)=\left(\frac{2}{151}\right)^4\cdot\left(\frac{5}{151}\right)=$$

$$=\left(\frac{2}{151}\right)^4\cdot\left(\frac{5}{151}\right)=\left(\frac{5}{151}\right)=\left(\frac{151}{5}\right)(-1)^{\frac{150\cdot 4}{4}}=1$$

$$\left(\frac{-71}{199}\right)=\left(\frac{128}{199}\right)=\left(\frac{2^7}{199}\right)=\left(\frac{2}{199}\right)=1$$

Следовательно, у второго и третьего сравнения по 2 решения. Итоговое количество решений:

$$2\times 2\times 2=8$$

Ответ: 8

№4 Чтобы доказать, что для простого числа Ферма $f_n=2^{2^n}+1$ выполняется сравнение $3^{(f_n-1)/2}\equiv -1 \pmod{f_n}$, воспользуемся критерием Эйлера.

Для простого p и целого a, не делящегося на p, верно:

$$a^{(p-1)/2}\equiv\left(\frac{a}{p}\right) \pmod{p},$$

где $\left(\frac{a}{p}\right)$ — символ Лежандра. Подставим $a = 3$ и $p = f_n$:

$$3^{(f_n-1)/2} \equiv \left(\frac{3}{f_n}\right) \pmod{f_n}$$

Докажем, что $\left(\frac{3}{f_n}\right) = -1$

$$\left(\frac{3}{f_n}\right) = \left(\frac{f_n}{3}\right)(-1)^{\frac{f_n-1}{2}} = \left(\frac{2^{2^n}+1}{3}\right)(-1)^{2^{2^n-1}} = \left(\frac{2^{2^n}+1}{3}\right) =$$

$$= \left(\frac{(-1)^{2^n}+1}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

Следовательно:

$$3^{\frac{f_n-1}{2}} \equiv -1 \pmod{f_n}$$

ч.т.д.

№5 Пусть p и $q = 2p+1$ — простые числа, причём $p \equiv 3 \pmod 4$. Требуется доказать, что число Мерсенна $M_p = 2^p - 1$ простое только при $p = 3$.

Подставим $p = 3$:

$$q = 2 \cdot 3 + 1 = 7 \text{ (простое)}$$

$$M_3 = 2^3 - 1 = 8 - 1 = 7 \text{ (простое)}$$

Условие выполнено.

Покажем, что для $p > 3$ число M_p составное:

Так как $q = 2p+1$ — простое, применим малую теорему Ферма к 2 по модулю q:

$$2^{q-1} \equiv 1 \pmod{q}.$$

Поскольку $q-1=2p$, получаем:

$$2^{2p} \equiv 1 \pmod{q}.$$

Это означает, что $2^p \equiv \pm 1 \pmod{q}$.

1) Если $2^p \equiv 1 \pmod{q}$:

   Тогда $2^p - 1 \equiv 0 \pmod{q}$, то есть q делит M_p.

   Так как $q = 2p+1$ и $p > 3$, то $q < M_p$, следовательно, M_p составное.

2) Если $2^p \equiv -1 \pmod{q}$:

   Возведём в квадрат:

$$(2^p)^2 = 2^{2p} \equiv 1 \pmod{q}.$$

   Это совпадает с малой теоремой Ферма, но для $p \equiv 3 \pmod{4}$ выполняется следующее:

   - $p = 4k+3$, тогда $q = 2(4k+3)+1 = 8k+7$
   - Число 2 является квадратичным вычетом по модулю q, так как $q \equiv 7 \pmod{8}$ (по теореме с лекции). По критерию Эйлера:

$$2^{\frac{q-1}{2}} \equiv 1 \pmod{q}.$$

     Подставляя $\frac{q-1}{2} = 4k+3$, получаем:

$$2^{4k+3} \equiv 1 \pmod{q}.$$

     Но $2^{4k+3} = 2^p$, поэтому $2^p \equiv 1 \pmod{q}$. Это сводится к первому случаю, где q делит M_p, делая его составным

   Следовательно, M_p простое только при $p = 3$