Теория чисел

ДЗ 6

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Пользуясь свойствами символа Лежандра, выясните, разрешимо ли сравнение

$$x^2 \equiv 219 \pmod{383}$$

Решение:

Вычислим символ Лежандра $\left(\dfrac{219}{383}\right)$

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right) = 1 \cdot \left(\frac{383}{73}\right) \cdot (-1)^{\frac{383-1}{2} \cdot \frac{73-1}{2}} = \left(\frac{18}{73}\right) = \left(\frac{9}{73}\right) \cdot \left(\frac{2}{73}\right) = 1 \cdot 1 = 1$$

$$\Rightarrow \text{ разрешимо}$$

Ответ:

разрешимо

Задание 2

Пусть p —простое число, $p > 5$. Докажите, что

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

Решение:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{p}{5}\right) = \begin{cases} 1, \text{ если } p \equiv \pm 1 \pmod 5 \Big(\text{из свойств для } \left(-\frac{1}{p}\right)\Big) \\ -1, \text{ если } p \equiv \pm 2 \pmod 5 \Big(\text{из свойств для } \left(\frac{2}{p}\right)\Big) \end{cases}$$

Ответ:

ч.т.д

Задание 3

Найдите количество решений сравнения

$$x^2 + 2x + 72 \equiv 0 \pmod{128 \cdot 151 \cdot 199}$$

Решение:

$$x^2 + 2x + 72 \equiv 0 \pmod{128 \cdot 151 \cdot 199} \iff (x+1)^2 \equiv -71 \pmod{2^7 \cdot 151 \cdot 199}$$

Это сравнение равносильно системе

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

Пользуясь задачей 4 из 5 семинара, первое сравнение разрешимо, так как $-71 \equiv 1 \pmod 8$, при этом оно имеет ровно 4 решения. Выясним, разрешимо ли второе и третье сравнение, для этого вычислим соответстующие символы Лежандра.

$$\left(\frac{-71}{151}\right) = \left(\frac{80}{151}\right) = \left(\frac{2^4}{151}\right) \cdot \left(\frac{5}{151}\right) = 1 \cdot 1 = 1$$

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

Так как эти сравнения разрешимы, то по задаче 3 из 5 семинара они имеют по два решения. Значит всего 16 решений.

Ответ:

16

Задание 4

Пусть $n \in \mathbb{N}$. Докажите, что если число Ферма $f_n = 2^{2^n} + 1$ является простым, то

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

Решение:

По критерию Эйлера:

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

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

$$\left(\frac{3}{f_n}\right) = \left(\frac{f_n}{3}\right) \cdot (-1)^{\frac{3-1}{2} \cdot \frac{f_n-1}{2}} = \left(\frac{f_n}{3}\right) (\text{так как } f_n \equiv 1 \pmod{4})$$

Исследуем f_n по модулю 3

$$2^2 \equiv 1 \pmod{3} \Rightarrow (2^2)^{2^{n-1}} \equiv 1 \pmod{3} \Rightarrow 2^{2^n} \equiv 1 \pmod{3} \Rightarrow f_n = 2^{2^n} + 1 \equiv 1 + 1 \equiv 2 \pmod{3}$$

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

Ответ:

ч.т.д

Задание 5

Пусть p, q —простые числа, причём $q = 2p + 1, p \equiv 3 \pmod 4$. Докажите, что число Мерсенна $M_p = 2^p - 1$ является простым числом только при $p = 3$.

Решение:

$p = \frac{q-1}{2}$, при этом $2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \equiv (-1)^{\frac{q^2-1}{8}} \equiv (-1)^{\frac{4p^2+4p+1-1}{8}} \equiv (-1)^{\frac{p\cdot(p+1)}{2}} \equiv 1 \pmod q$(так как $p + 1 \equiv 0 \pmod 4$). $M_p = 2^{\frac{q-1}{2}} - 1 \equiv 0 \pmod q$, но M_p должно быть простым, значит $2^{\frac{q-1}{2}} = q$, откуда $q = 7 \Rightarrow p = 3$.

Ответ:

ч.т.д