Теория чисел

ДЗ 8

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Найдите все первообразные корни по модулю 11, лежащие на интервале от 0 до 11.

Решение:

2 - корень($\mathrm{ord}_{11} 2 = \varphi(11)$)$\Rightarrow$ 6 тоже корень как обратный вычет. $(3, \varphi(11)) = 1 \Rightarrow 2^3 -$ корень и 7 тоже корень как обратный вычет. Всего существует $\varphi(\varphi(11)) = 4$ корня, мы их нашли.

Ответ:

2,6,7,8

Задание 2

Докажите, что число -2 является первообразным корнем по модулю каждого простого числа вида $2p+1$, где p — тоже простое, $p \equiv -1 \pmod 4$.

Решение:

Покажем, что -2 является первообразным корнем. Так как показатель является делителем $\varphi(2p+1) = 2p$, проверим, что:

$$\begin{cases} (-2)^2 \not\equiv 1 \pmod{2p+1} \\ (-2)^p \not\equiv 1 \pmod{2p+1} \end{cases}.$$

Первое сравнение верно, так как $2p+1 > 5, 4+1 = 5 \not\equiv 0\ (2p+1)$.
Второе сравнение докажем от противного. Пусть $(-2)^p \equiv 1 \pmod{2p+1}$. Тогда для $q = 2p+1$ имеем $(-2)^{\frac{q-1}{2}} \equiv 1 \pmod q \Rightarrow \left(\frac{-2}{q}\right) = 1$ по критерию Эйлера. С другой стороны:

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{2}{q}\right) = (-1)^p \cdot (-1)^{\frac{q^2-1}{8}} = -1 \cdot (-1)^{\frac{4p^2+4p}{8}} = -1 \cdot (-1)^{\frac{p\cdot(p+1)}{2}} = -1 (\text{так как } 4 \mid p+1).$$

Получили противоречие, значит второе сравнение верно, значит =2 является первообразным корнем.

Ответ:

ч.т.д

Задание 3

Пусть P – произведение всех положительных первообразных корней по модулю 79. Докажите, что $P \equiv 1 \pmod{79}$.

Решение:

Пусть, g – первообразный корень, тогда все числа вида $g^k, (k, \varphi(79)) = 1$ тоже первообразные корни. Тогда

$$P = g^{\sum_{\substack{1<k<78 \\ (k,78)=1}} k} = g^{78 \cdot \frac{\varphi(78)}{2}} = g^{936}$$

Значение суммы такое, так как все числа, взаимопростые с 78, делятся на пары вида $n, 78 - n$, всего пар $\frac{\varphi(78)}{2} = 12$. Заметим, что $g^{78} \equiv 1 \pmod{79} \Rightarrow \left(g^{78}\right)^{12} \equiv 1^{12} \pmod{79} \Rightarrow g^{936} \equiv 1 \pmod{79} \Rightarrow P \equiv 1 \pmod{79}$.

Ответ:

ч.т.д

Задание 4

Пусть g — первообразный корень по модулю m и пусть $k \in \mathbb{N}$. Докажите, что

$$\operatorname{ord}_m\left(g^k\right) = \frac{\varphi(m)}{(k, \varphi(m))}.$$

Решение:

Пусть d такое наименьшее число, что

$$\left(g^k\right)^d \equiv 1 \pmod{m} \Rightarrow \varphi(m) \mid kd(\text{Теорема 22 из лекции})$$
$$\Rightarrow kd \equiv 0 \pmod{\varphi(m)}$$

Тогда $k = (k, \varphi(m)) \cdot k', \varphi(m) = (k, \varphi(m)) \cdot m', (k', m') = 1 \Rightarrow$

$$\Rightarrow (k, \varphi(m)) \cdot k' \cdot d \equiv 0 \pmod{(k, \varphi(m)) \cdot m'}$$

$$\Rightarrow k' \cdot d \equiv 0 \pmod{m'} \Longleftrightarrow d \equiv 0 \pmod{m'} \Rightarrow d = m' = \frac{\varphi(m)}{(k, \varphi(m))}$$

Что и требовалось доказать.

Ответ:

ч.т.д