Теория чисел

ДЗ 9

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Найдите все первообразные корни по модулю 22 на промежутке от -11 до 11.

Решение:

Заметим, что 3 является первообразным корнем, так как

$$3^{\frac{\varphi(22)}{11}} \not\equiv 1 \pmod{22}$$

$$3^{\frac{\varphi(22)}{2}} \not\equiv 1 \pmod{22}$$

Тогда $5 \equiv 3^3$ – первообразный корень, $9 \equiv 3^7 \pmod{22}$ – первообразный корень, $-7 \equiv 15 \equiv 3^9 \pmod{22}$ – первообразный корень. Всего корней $\varphi(\varphi(22)) = 4$. Мы их нашли.

Ответ:

-7,3,5,9

Задание 2

Найдите какой-нибудь первообразный корень по модулю 242.

Решение:

2 является первообразным корнем по модулю 11. Пусть $h = 2 + 11t$

$$t \not\equiv \frac{2^{11} - 2}{11} \pmod{11} \Rightarrow t \not\equiv 10 \pmod{11}$$

Значит как h можно взять $h = 2 + 11 \cdot 11$=123 – первообразный корень по модулю 11^2. Чтобы найти первообразный корень по модулю $242 = 2 \cdot 11^2$, берём нечётное из чисел 123, 123+121. Значит 123 первообразный корень по модулю 242.

Ответ:

123

Задание 3

Найти все целые числа g, лежащие в промежутке от 1 до 25, удовлетворяющие двум условиям:
а) g является первообразным корнем по модулю 5;
б) g не является первообразным корнем по модулю 25.

Решение:

Числа 2 и 3 являются первообразными корнями по модулю 5. Тогда из искомого промежутка под первое условие подходят числа 2,3,7,12,17,22,8,13,18,23. Они будут подходить под второе условие, если выполняется сравнение

$$g \equiv g^5 \pmod{25}$$

Из выше описанного набора подходят только числа 7, 18.

Ответ:

7, 18

Задание 4

Найдите количество решений сравнения $x^{21} \equiv 1 \pmod{29}$.

Решение:

Это сравнение разрешимо(есть корень 1), значит по обобщенному критерию Эйлера оно имеет ровно $(21, \varphi(29)) = 7$ решений.

Ответ:

7

Задание 5

Пусть $n \in \mathbb{N}$. Докажите, что для того, чтобы число Ферма $f_n = 2^{2^n} + 1$ было простым, достаточно выполнения сравнения

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

Решение:

Возведём обе части сравнения в квадрат. Получаем сравнение

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

Порядок должен делить $f_n - 1 = 2^{2^n}$, но при этом он не делит $\frac{f_n-1}{2} = 2^{2^n-1} \Rightarrow$ порядок равен $f_n - 1$. Порядок числа всегда делит $\varphi(f_n)$, то есть $f_n - 1 \mid \varphi(f_n)$. Такое возможно, только если $\varphi(f_n) = f_n - 1$. Значит f_n является простым.

Ответ:

ч.т.д