Домашнее задание на 14.03 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 Найдём $\varphi(22)$:

$$\varphi(22) = 10$$

g - первообразный корень по модулю 22 тогда и только тогда, когда:

$$\forall q \mid 10: \quad g^{\frac{10}{q}} \not\equiv 1 \pmod{22}$$

То есть:

$$\begin{cases} g^5 \not\equiv 1 \pmod{22} \\ g^2 \not\equiv 1 \pmod{22} \end{cases}$$

Подставим каждое значение из приведённой системы вычетов:

$$g \in \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9\}$$

Таким образом, подходят только:

$$g \in \{-3, -5, 7, -9\}$$

Они и являются первообразными корнями.

Ответ: $-3, -5, 7, -9$

№2 Найдём первообразный корень по модулю $242 = 2 \cdot 11^2$.

1) Для начала найдём первообразный корень по модулю 11:

   g - первообразный корень по модулю 11 тогда и только тогда, когда:

$$\forall q \mid 10: \quad g^{\frac{10}{q}} \not\equiv 1 \pmod{11}$$

То есть:
$$\begin{cases} g^5 \not\equiv 1 \pmod{11} \\ g^2 \not\equiv 1 \pmod{11} \end{cases}$$

Найдём первое удовлетворяющее условию значение из набора:

$$g \in \{1, 3 \ldots, 9\}$$

Таким образом:

$$g = 7 \text{ - первообразный корень}$$

2) g_1 -первообразный корень по модулю 11^α если:

$$\begin{cases} g_1 = g \pmod{11} \\ g_1^{10} \not\equiv 1 \pmod{121} \end{cases}$$

g_1 лежит в наборе:
$$g_1 \in \{7, 18\}$$

Проверим 7:
$$7^{10} \not\equiv 1 \pmod{121}$$

Это верно, следовательно:

$$7 \text{ — п.к. по модулю } 11^\alpha$$

В частности:
$$7 \text{ — п.к. по модулю } 121$$

3) g_2 -первообразный корень по модулю $2 \cdot 11^\alpha$ если:

$$\begin{cases} (g_2, 2) = 1 \\ g_2 \equiv g_1 \pmod{121} \end{cases}$$

Это выполняется для

$$g_2 = 7$$

Следовательно,

$$7 \text{ — п.к. по модулю } 2 \cdot 11^\alpha$$

В частности:

$$7 \text{ — п.к. по модулю } 242$$

Ответ: 7

№3 Найдём $\varphi(5)$:

$$\varphi(5) = 4$$

g - первообразный корень по модулю 5 тогда и только тогда, когда:

$$\forall q \mid 4: \quad g^{\frac{4}{q}} \not\equiv 1 \pmod 5$$

То есть:

$$g^2 \not\equiv 1 \pmod 5$$

Подставим каждое значение из приведённой системы вычетов:

$$g \in \{1, 2, 3, 4\}$$

Таким образом, подходят только:

$$g \in \{2, 3\}$$

Они и являются первообразными корнями по модулю 5.

то есть:

$$2 \pmod 5 \quad \text{и} \quad 3 \pmod 5 \text{ — п.к.}$$

Следовательно под условие пункта a) подходят числа из набора:

$$g' \in \{2, 7, 12, 17, 22, 3, 8, 13, 18, 23\}$$

Чтобы они не являлись первообразными корнями по модулю 25 для каждого g' должно выполняться:

$$\exists q \mid 16: \quad g'^{\frac{16}{q}} \equiv 1 \pmod{25}$$

То есть:

$$g'^8 \equiv 1 \pmod{25}$$

Подставив каждое число, получается, что подходят только:

$$\{7, 18\}$$

Ответ: $7, 18$

№4 Пусть g - первообразный корень по модулю 29. Тогда x можно представить как

$$g^k, \quad k \in \{0, 1, \dots 27\} \text{ по модулю 28}$$

Найдём количество решений сравнения:

$$g^{21k} \equiv 1 \pmod{29}$$

Чтобы сравнение выполнялось, нужно, чтобы:

$$21k \equiv 0 \pmod{28} \Leftrightarrow 3k \equiv 0 \pmod{4} \Leftrightarrow k \equiv 0 \pmod{4}$$

$$\Leftrightarrow k = 4m \quad m \in \mathbb{Z}$$

Следовательно, так как $k \in \{0, 1, \dots 27\}$, то всего решений:

$$0 \leqslant 4m < 28 \Leftrightarrow 0 \leqslant m < 7 \implies 7 \text{ решений}$$

Ответ: 7

№5 Докажем, что число Ферма $f_n = 2^{2^n} + 1$ простое при условии

$$3^{(f_n-1)/2} \equiv -1 \pmod{f_n},$$

Показатель числа 3 по модулю f_n — это наименьшее натуральное число k, такое что

$$3^k \equiv 1 \pmod{f_n}.$$

Из условия $3^{(f_n-1)/2} \equiv -1 \pmod{f_n}$ следует, что:

Возведя обе части в квадрат:

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

Значит, показатель числа 3 делит $f_n - 1$.

Однако

$$3^{(f_n-1)/2} \not\equiv 1 \pmod{f_n}$$

Поэтому показатель не делит $\frac{f_n-1}{2}$

Следовательно, показатель числа 3 равен $f_n - 1$.

- Если f_n простое, то по малой теореме Ферма

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

  и показатель числа 3 может достигать $f_n - 1$.

- Если f_n составное, то функция Эйлера $\varphi(f_n)$ будет меньше $f_n - 1$, так как у составного числа есть делители, отличные от 1 и самого числа.

- Показатель числа 3 должен делить $\varphi(f_n)$. Но если $\varphi(f_n) < f_n - 1$, то показатель $f_n - 1$ не может быть делителем $\varphi(f_n)$. Это противоречие.

Единственный случай, когда показатель числа 3 равен $f_n - 1$, возможен только если f_n простое. Таким образом, условие

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

гарантирует простоту числа Ферма f_n.