Серия 11. Первообразные корни

Определение. Если $(a, m) = 1$ и показатель a по модулю m равен $\varphi(m)$, то a называется первообразным корнем по модулю m.

Замечание. Тем самым $1 = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$ – это все вычеты по модулю m, взаимно простые с m.

Упражнение. Существует ли первообразный корень по модулю 8? По модулю 9?

1. Пусть m — такое натуральное число, что по его модулю существует первообразный корень, и пусть d — произвольное натуральное число.
(a) Сколько существует вычетов a, для которых $a^d \equiv 1 \pmod m$?
(b) Сколько существует первообразных корней по модулю m?

2. Пусть p – простое.
(a) Докажите, что при $d \mid p-1$ многочлен $x^d - 1 \in \mathbb{F}_p[x]$ имеет ровно d корней.
(b) Докажите, что для любого натурального n справедливо $\sum_{d|n} \varphi(d) = n$.
(c) Докажите, что для любого $d \mid p-1$ есть ровно $\varphi(d)$ вычетов, показатель которых по модулю p равен d. В частности, существует первообразный корень по модулю p.

3. Пусть p – простое, $p > 2$.
(a) Докажите, что если a – первообразный корень по модулю p, то либо a, либо $a+p$ является первообразным корнем по модулю p^2.
(b) Пусть a – первообразный корень по модулю p^2. Докажите, что a является первообразным корнем по модулю p^α при любом натуральном α.

Упражнение. 1. Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?
2. Покажите, что 2 – первообразный корень по модулю 29.

Замечание. По модулю m существует первообразный корень тогда и только тогда, когда m имеет вид $2, 4, p^\alpha, 2p^\alpha$, где $p > 2$ – простое.

4. Решите уравнение $1 + x + \ldots + x^6 \equiv 0 \pmod{29}$.

5. Докажите, что для любого n найдётся такое m, что $2^m + 2020$ делится на 3^n (здесь m, n – натуральные).

6. Пусть n — натуральное число. Обязательно ли найдётся такое простое p, что все натуральные числа, являющиеся первообразным корнем по модулю p, будут больше n?
Замечание: при решении этой задачи могут возникнуть вопросы «можно ли использовать такой-то факт». Скорее всего, ответ будет «да».

7. Известно, что число $2^{32}+1$ раскладывается на простые множители как $641 \cdot 6700417$. Докажите, что существует натуральное k такое, что для любого натурального n число $k2^n + 1$ будет составным.

8. Пусть p — простое число. Докажите, что существует такое простое число q, что при любом целом n число $n^p - p$ не делится на q.

[ЦПМ, кружок по математике, 10 класс] Афризонов Д., Тихонов Ю., Юргин Г.
[*2019–2020*] группа: 10-1 и 10-2 *21 ноября 2019 г.*

Серия 11. Первообразные корни

Определение. Если $(a, m) = 1$ и показатель a по модулю m равен $\varphi(m)$, то a называется первообразным корнем по модулю m.

Замечание. Тем самым $1 = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$ – это все вычеты по модулю m, взаимно простые с m.

Упражнение. Существует ли первообразный корень по модулю 8? По модулю 9?

1. Пусть m — такое натуральное число, что по его модулю существует первообразный корень, и пусть d — произвольное натуральное число.
(a) Сколько существует вычетов a, для которых $a^d \equiv 1 \pmod m$?
(b) Сколько существует первообразных корней по модулю m?

2. Пусть p – простое.
(a) Докажите, что при $d \mid p-1$ многочлен $x^d - 1 \in \mathbb{F}_p[x]$ имеет ровно d корней.
(b) Докажите, что для любого натурального n справедливо $\sum_{d|n} \varphi(d) = n$.
(c) Докажите, что для любого $d \mid p-1$ есть ровно $\varphi(d)$ вычетов, показатель которых по модулю p равен d. В частности, существует первообразный корень по модулю p.

3. Пусть p – простое, $p > 2$.
(a) Докажите, что если a – первообразный корень по модулю p, то либо a, либо $a+p$ является первообразным корнем по модулю p^2.
(b) Пусть a – первообразный корень по модулю p^2. Докажите, что a является первообразным корнем по модулю p^α при любом натуральном α.

Упражнение. 1. Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?
2. Покажите, что 2 – первообразный корень по модулю 29.

Замечание. По модулю m существует первообразный корень тогда и только тогда, когда m имеет вид $2, 4, p^\alpha, 2p^\alpha$, где $p > 2$ – простое.

4. Решите уравнение $1 + x + \ldots + x^6 \equiv 0 \pmod{29}$.

5. Докажите, что для любого n найдётся такое m, что $2^m + 2020$ делится на 3^n (здесь m, n – натуральные).

6. Пусть n — натуральное число. Обязательно ли найдётся такое простое p, что все натуральные числа, являющиеся первообразным корнем по модулю p, будут больше n?
Замечание: при решении этой задачи могут возникнуть вопросы «можно ли использовать такой-то факт». Скорее всего, ответ будет «да».

7. Известно, что число $2^{32}+1$ раскладывается на простые множители как $641 \cdot 6700417$. Докажите, что существует натуральное k такое, что для любого натурального n число $k2^n + 1$ будет составным.

8. Пусть p — простое число. Докажите, что существует такое простое число q, что при любом целом n число $n^p - p$ не делится на q.