15 июля

Первообразные корни

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

Замечание1. Тем самым $a = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1} \pmod m$ – это ***все*** вычеты, взаимно простые с m.

Замечание2. Наличие первообразного корня в точности означает, что группа обратимых элементов по модулю m является *циклической.*

Упр1. Существует ли первообразный корень по модулю 8? По модулю 9?

Зад0. Пусть по модулю m существует первообразный корень. а) Сколько тогда существует элементов a, для которых $a^d \equiv 1 \pmod m$? б) Сколько имеется первообразных корней?

Зад1. а) Над $\mathbb{Z}_p$ (p – простое) многочлен степени d имеет не более d корней;

б) при $d|p-1$ уравнение $x^d = 1$ имеет ровно d корней;

в) если $d|p-1$, то обозначим через $f(d)$ количество вычетов показателя ровно d. Докажите, что $d = \sum\limits_{d'} f(d')$, где суммирование ведется по всем делителям d' числа d.

Теорема (Гаусс). Существует первообразный корень по модулю простого p.

Упр2. а) Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?

б) Покажите, что 2 – первообразный корень по модулю 29.

Упр3. Сколько корней над $\mathbb{Z}_p$ имеет уравнение $x^d = 1$? Как найти все решения этого уравнения, если известен первообразный корень?

Замечание3. По модулю m существует первообразный корень тогда и только тогда, когда m иммет вид $2, 4$, p^α, $2p^\alpha$, где $p > 2$ – простое число.

---

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

2. Докажите, что числа $1, 2, ..., p-1$ можно расставить по кругу так, что для любых трех последовательных a, b, c разность $b^2 - ac$ будет делиться на простое p.

3. Докажите, что для каждого n найдется такое m, что $2^m + 2008 \,\vdots\, 3^n$.

---

4. Найдите сумму для целых d (для отрицательных тоже)

$$\sum_{n=0}^{p-1} n^d \pmod p.$$

5. Многочлен $f(x) \in \mathbb{Z}_p[x]$ будем называть *перестановочным*, если значения $f(0), \ldots, f(p-1)$ попарно различны.

а) при каких d многочлен x^d будет перестановочным по модулю p?

б) по модулю 101 не существует перестановочного многочлена степени 100;

в) по модулю p не существует перестановочного многочлена степени $d > 1$, $d|p-1$.

6. $f(x) \in \mathbb{Z}[x]$, $f(0) = 0$, $f(1) = 1$. Простое число p таково, что для любого целого n остаток от деления $f(n)$ на p равен 0 или 1. Докажите, что $\deg(f) \geq p-1$. (Степень $p-1$, очевидно, бывает.)