

## Многочлены деления круга

**Определения.** Пусть  $\xi_n$  — примитивный корень степени  $n$  из 1. Многочленом деления круга порядка  $n$  называется многочлен

$$\Phi_n(x) = \prod_{\substack{(k,n)=1 \\ 0 \leq k < n}} (x - \xi_n^k).$$

Функцией Мёбиуса называется функция  $\mu: \mathbb{N} \rightarrow \mathbb{Z}$ , определённая по следующему правилу: если  $n = 1$ , то  $\mu(n) = 1$ ; если  $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ , где  $p_i$  — различные простые числа, то  $\mu(n) = (-1)^k$ ; если  $n$  делится на квадрат простого, то  $\mu(n) = 0$ .

**Основные свойства многочленов деления круга.**

1. Докажите, что  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ .
2. Докажите, что коэффициенты  $\Phi_n(x)$  — целые числа.
3. Докажите, что на коэффициенты  $a_i$  многочлена  $\Phi_n(x)$  при всех  $0 \leq k \leq \varphi(n)$  выполнено соотношение  $a_k = a_{\varphi(n)-k}$  (т. е. многочлен  $\Phi_n(x)$  «симметричен»).
4. Докажите, что  $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$ .
5. Пусть  $p$  — простое. Докажите, что если  $n$  кратно  $p$ , то  $\Phi_{np}(x) = \Phi_n(x^p)$ , и что если  $n$  не кратно  $p$ , то  $\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$ .
6. Пусть  $(m, n) = 1$ . Тогда  $\Phi_n(x^m) = \prod_{d|m} \Phi_{nd}(x)$ .

**Многочлены круга в  $\mathbb{Z}_p[x]$ .**

7. Пусть  $P(x) \in \mathbb{Z}_p[x]$ . Докажите, что существует неконстантный  $Q(x) \in \mathbb{Z}_p[x]$  такой, что  $Q^2(x) | P(x)$ , тогда и только тогда, когда  $(P'(x), P(x)) \neq 1$ .
8. Докажите, что если  $n$  не делится на простое число  $p$ , то в разложении многочлена  $\Phi_n(x)$  на неприводимые множители в  $\mathbb{Z}_p[x]$  нет кратных множителей.
9. Пусть  $m$  и  $n$  различны и не делятся на  $p$ . Докажите, что  $(\Phi_n(x), \Phi_m(x)) = 1$  в  $\mathbb{Z}_p[x]$ .
10. Пусть  $n$  не делится на простое  $p$ . Докажите, что показатель числа  $a$  по модулю  $p$  равен  $n$  тогда и только тогда, когда  $\Phi_n(a) \equiv 0 \pmod{p}$ .
11. (Частный случай теоремы Дирихле) Докажите, что для любого натурального  $n$  существует бесконечно много простых чисел вида  $nk + 1$ .

**12. Теорема.** Многочлены  $\Phi_n(x)$  неприводимы в  $\mathbb{Z}[x]$ .

Эту теорему сложно доказать самостоятельно. Вот вам план. Промежуточная цель — доказать, что минимальный многочлен для примитивного корня  $\xi_n$  обладает корнем  $\xi_n^p$ , где  $p$  не делит  $n$ . Предположив противное и рассмотрев разложение  $\Phi_n(x^p)$  на неприводимые в  $\mathbb{Z}_p[x]$ , придите к противоречию с задачей 8.