Теорема Жигмонді

Теорема 1 (Жигмонді, Zsigmondy). Нехай a та n — цілі числа, більші за 1. Тоді існує простий дільник q числа $a^n - 1$, який не ділить жодне з чисел $a^i - 1$ для всіх натуральних i менших n, крім двох випадків:

- $n = 2$, $a = 2^s - 1$, де $s \geq 2$;
- $n = 6$, $a = 2$.

Таке число q називають **простим числом Жигмонді (Zsigmondy prime).**

Означення 1. Для $n \geq 1$ многочленом поділу кола називається многочлен Φ_n, такий що

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (x - \epsilon_i)$$

де ϵ_i — первісні корені n-ого степеню з одиниці.

Означення 2. Функцією Мебіуса називається функція $\mu(n)$, така що

- $\mu(n) = 0$, якщо $n = p^2 k$
- $\mu(n) = 1$, якщо $n = 1$
- $\mu(n) = (-1)^k$, якщо $n = p_1 p_2 \dots p_k$

План доведення

- Якщо $a > 1$, то $(a+1)^{\varphi(n)} > \Phi_n(a) > (a-1)^{\varphi}(n)$
- $\sum_{d|n} \mu(d) = 0$, якщо $n > 1$, $\sum_{d|n} \mu(d) = 1$, якщо $n = 1$
- Якщо $F : \mathbb{Z} \to \mathbb{Z}$ та $f : \mathbb{Z} \to \mathbb{Z}$ такі функції, що

  $$F(n) = \prod_{d|n} f(d)$$

  , то

  $$f(n) = \prod_{d|n} F(\frac{n}{d})^{\mu(d)}$$

  .
- Якщо n — натуральне число, то

  $$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

- Якщо n — натуральне число, то

  $$\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$$

- Нехай n — натуральне число, а p — просте. Тоді $\Phi_{pn}(X) = \Phi_n(X^p)$, якщо $p|n$ та $\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$, якщо $p \nmid n$

- Нехай $a > 1$ та $n = q^i r$, причому $i \geq 1$, q — просте, що не ділить r. Нехай $b = a^{q^{i-1}}$. Тоді

$$\Phi_n(a) > \left(\frac{b^q - 1}{b + 1}\right)^{\varphi(n)}$$

- Нехай $a > 1$ та $n > 1$ — натуральні числа. Нехай q є простим дільником $\Phi_n(a)$. Тоді якщо q не є простим Жигмонді для (a, n) тоді і тільки тоді, коли $q|n$. Причому, якщо q не є простим Жигмонді, то q — найбільший простий дільник n. Тоді $n = q^i r$ та $r|q - 1$, більше того, $q^2 \nmid \Phi_n(a)$, крім випадку, коли $q = n = 2$. Отже, якщо для пари (a, n) немає жодного простого Жигмонді, то $\Phi_n(a)$ — степінь q, а якщо $n > 2$, то $\Phi_n(a) = q$.

- Теорема Жигмонді

Задача 1. Нехай b, m, n — натуральні числа, такі що $b^n - 1$ та $b^m - 1$ мають однакову множину дільників. Доведіть, що $b + 1$ — степінь 2.