# Билет 57. Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_2 \geq \lambda_3$.

**Постулат Бертрана.** $\forall x \geq 2 \quad \exists$ простое $p : x < p < 2x$.
**Асимптотика** $\forall x \quad \exists p : p \in [x; x + O(x^{0,525})]$

**Неравенство Чебышёва** $\exists a, b \in \mathcal{R} : 0 < a < b$ (на самом деле, близкие к единице) : $\frac{ax}{ln(x)} \leq \pi(x) \leq \frac{bx}{ln(x)}$

**Def.** $\pi(x) = \sum\limits_{p \leq x} 1$ – количество простых чисел, не превышающих $x$

**Def.** $\theta(x) = \sum\limits_{p \leq x} ln(p)$

**Def.** $\psi(x) = \sum\limits_{(p,\alpha): p^\alpha \leq x} ln(p)$

**Теорема о равенстве нижних и верхних пределов (формулировка)**

Введем следующие обозначения:

$\lambda_1 = \overline{\lim\limits_{x \to \infty} \frac{\theta(x)}{x}}$

$\lambda_2 = \overline{\lim\limits_{x \to \infty} \frac{\psi(x)}{x}}$

$\lambda_3 = \overline{\lim\limits_{x \to \infty} \frac{\pi(x)}{x/ln(x)}}$

$\mu_1, \mu_2, \mu_3$ – соответствующие нижние пределы.

**Теорема:** $\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$
**Неравенство** $\lambda_2 \leq \lambda_3$

Зафиксируем $p$ и $x$. Тогда таких $\alpha$, что $p^\alpha < x$, ровно $[log_p x] = [\frac{ln(x)}{ln(p)}]$.

Тогда $\psi(x) = \sum\limits_{(p,\alpha): p^\alpha \leq x} ln(p) = \sum\limits_{p \leq x} [\frac{ln(x)}{ln(p)} ln(p) \leq \sum\limits_{(p,\alpha): p \leq x} ln(x) = ln(x) \sum\limits_{p \leq x} 1 = ln(x)\pi(x).$

$\frac{\psi(x)}{x} \leq \frac{\pi(x) ln(x)}{x} = \frac{\pi(x)}{x/ln(x)}$, т.е. $\lambda_2 \leq \lambda_3$

# Билет 58. Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_3 \leq \lambda_1$.

Зафиксируем некоторое $\gamma \in (0; 1)$.

$\theta(x) = \sum_{p \le x} ln(p) \ge \sum_{x^\gamma < p \le x} ln(p) > \sum_{x^\gamma < p \le x} ln(x^\gamma) = \gamma ln(x) \sum_{x^\gamma < p \le x} 1 = \gamma ln(x)(\pi(x) - \pi(x^\gamma)) \ge \gamma ln(x)(\pi(x) - x^\gamma)$.

Получаем неравенство:

$\frac{\theta(x)}{x} \ge \gamma(\frac{\pi(x)}{x/ln(x)} - \frac{x^\gamma}{x} ln(x))$. Перейдя к верхнему пределу, получим, что $\frac{\theta(x)}{x} \ge \gamma \frac{\pi(x)}{x/ln(x)}$, т.е. $\lambda_1 \ge \gamma \lambda_3 \forall \gamma \in (0;1)$. Значит, $\lambda_1 \ge \lambda_3$, и $\lambda_2 \ge \lambda_1 \ge \lambda_3$.

# Билет 59. Порядки(показатели) элементов в системах вычетов. Равенство $ord(g^l) = \frac{ord(g)}{gcd(l,ord(g))}$. Следствие: если есть порядок $k$, то есть порядки и всех делителей $k$.

**Порядки(показатели) элементов в системах вычетов**
Рассмотрим систему вычетов по модулю $m$.

**Def.** Пусть $gcd(g, m) = 1$. Тогда показатель $ord(g) = k$ – минимальное $k > 0, g^k \equiv 1$.

Если $gcd(g, m) \ne 1$, то рассматривать $ord(g)$ бессмысленно, т.к. оно равно $\infty$.

**Равенство** $ord(g^l) = \frac{ord(g)}{gcd(l,ord(g))}$

Обозначим $ord(g^l)$ за $s$, а $ord(g)$ за $k$. По определению порядка, $s$ – минимальное натуральное число такое, что $g^{ls} \equiv 1$. Заметим, что т.к. $k$ – минимальное число такое, что $g^k \equiv 1$, то $k|ls$. Значит, мы ищем минимальное $s$ такое, что $k|ls$, ведь если это верно, то несложно понять, что тогда $s$ – порядок $g^l$.

**Теперь сформулируем лемму:**

Пусть $a, b \in \mathcal{N}, s$ – минимальное натуральное число, такое что, $b|as$. Тогда $s = \frac{b}{gcd(a,b)}$.

**Доказательство:** $\frac{a}{gcd(a,b)}$ – целое, поэтому $\frac{ab}{gcd(a,b)} \vdots b$, то есть $\frac{b}{gcd(a,b)} \ge s$.

Пусть $a' = \frac{a}{gcd(a,b)}, b' = \frac{b}{gcd(a,b)}$).
Тогда т.к. $b|as$, то $b'|a's$, а в силу того, что $gcd(a', b') = 1$, то $b'|s \Rightarrow s \ge b'$. А т.к. $s \le b'$, то $s = b'$.

**Следствие: если есть порядок $k$, то есть порядки и всех делителей $k$.**
Пусть существует $ord(k) < \infty \pmod m$. Тогда $gcd(k, m) = 1$.

Значит, если $a|k$, то $gcd(a, m) = 1$. Тогда рассмотрим $m$ чисел: $a^1, \ldots, a^{m-1}$. Если среди них все различные, тогда среди них есть 1, т.к. остатков от деления на $m$, отличных от 0, ровно $m - 1$. В противном случае какие-то два различных числа равны, то есть $a^i \equiv a^{i+t} \pmod m$, где $t \ne 0$. Тогда $a^i(a^t - 1) \equiv 0 \pmod m$, а т.к. $gcd(a^i, m) = 1$, то $a^t \equiv 1 \pmod m$.