Глава 2

Разпределение на простите числа.

2.1 Аритметични функции.

Аритметична функция се нарича всяка функция $f(n)$, която е дефинирана върху множеството от естествени числа. Например $f(n) = n!$ е една такава функция. По-долу ще разгледаме някои често използвани в теория на числата аритметични функции.

Дефиниция 2.1.1 *За всяко $n \in \mathbb{Z}$ с $\tau(\mathbf{n})$ се означава броят на положителните му делители, а със $\sigma(\mathbf{n})$ тяхната сума.*

Теорема 2.1.2 *Ако $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, $e_i \geq 1$, то*

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_s + 1).$$

Доказателство. Всеки положителен делител на n има вида $d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$, където $\delta_i \in S_i = \{0, 1, \ldots, e_i\}$. Твърдението следва от факта, че $|S_i| = e_i + 1$.

Теорема 2.1.3 *Ако $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $e_i \geq 1$, то*

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}.$$

Доказателство.

$$\begin{aligned} \sigma(n) &= \sum_{\substack{\delta_i \in S_i \\ 1 \leq i \leq k}} p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} \\ &= (1 + p_1 + \cdots + p_1^{e_1})(1 + p_2 + \cdots + p_2^{e_2}) \cdots (1 + p_k + \cdots + p_k^{e_k}) \\ &= \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1} \end{aligned}$$

Дефиниция 2.1.4 *Една аритметична функция $f : \mathbb{N} \to \mathbb{N}$ наричаме **мултипликативна**, ако $f(nm) = f(n)f(m)$ за всеки $(n, m) = 1$.*

Теорема 2.1.5 *Ако $f(n)$ е мултипликативна, то такава е и $F(n)$, където*

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

Доказателство. Нека $(n, m) = 1$. Да отбележим, че $d\,|\,mn$ тогава и само тогава, когато $d = d_1 d_2$, където $d_1|n$, а $d_2|m$. Тогава

$$F(nm) = \sum_{d|nm} f(d) = \sum_{d_1|n,\, d_2|m} f(d_1 d_2) = \sum_{d_1|n,\, d_2|m} f(d_1 d_2) = \sum_{d_1|n} f(d_1) \cdot \sum_{d_2|m} f(d_2).$$

Тъй като функциите $f(n) = 1$ и $f(n) = n$ са очевидно мултипликативни, то е в сила следното

Следствие 2.1.6 *Функциите $\tau(n)$ и $\sigma(n)$ са мултипликативни.*

Ясно е, че една мултипликативна функция се определя еднозначно от стойностите, които приема за n степен на просто число.

Упражнение 2.1.1 *Едно число n се нарича* ***съвършено****, ако $\sigma(n) = 2n$. Проверете, че 6, 28 и 496 са първите три съвършени числа.*

Упражнение 2.1.2 *Докажете, че ако $2^m - 1$ е просто, то $2^{m-1}(2^m - 1)$ е съвършено*

Упражнение 2.1.3 *Докажете, че ако $2^m - 1$ е просто, то m е също просто число.*

В сила е и следния резултат:

Теорема 2.1.7 *Ако n е четно съвършено число, то съществува m, такова че $2^m - 1$ е просто и $n = 2^{m-1}(2^m - 1)$.*

Доказателство. Нека $n = 2^e n_1$, където n_1 е нечетно. Съгласно Следствие 2.1.6 и Теорема 2.1.3 $2n = \sigma(n) = (2^{e+1} - 1)\sigma(n_1)$. Следователно

$$2^{e+1} n_1 = (2^{e+1} - 1)\sigma(n_1),$$

откъдето заключаваме, че

$$\sigma(n_1) = 2^{e+1} d \quad \text{и} \quad n_1 = d(2^{e+1} - 1),$$

за някое d. Ако $d \neq 1$, то 1 и d са различни делители на n_1 и тогава

$$\sigma(n_1) \geq n_1 + d + 1 + (2^{e+1} - 1) = 2^{e+1}(d + 1) > \sigma(n_1),$$

което е противоречие. Следователно $d = 1$, т.е. $n_1 = (2^{e+1} - 1)$ и $\sigma(n_1) = 2^{e+1}$. Тогава търсеното $m = e + 1$. Освен това $\sigma(n_1) = 2^m$ е възможно тогава и само тогава, когато 1 и $n_1 = (2^m - 1)$ са единствените делители на n_1, т.е. $(2^m - 1)$ е просто число.

Забележка 2.1 *Простите числата от вида $(2^m - 1)$ се наричат прости числа на Мерсен Първите от редицата такива числа се получават при $m = 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127$. Информация може да се намери на http://www.mersenne.org и http://www.utm.edu/research/primes/mersenne/index.html.*

Забележка 2.2 *Досега няма известни нечетни съвършени числа и това е нерешена задача с многовековна давнаст (поне от Евклид). Днес е известно, че ако съществуват нечетни съвършени числа, то те са по-големи от 10^{300} (Bent et al., 1991) и имат поне 47 прости делители (броени с кратностите) (Hare, 2004).*

Дефиниция 2.1.8 ***Функция на Ойлер*** *, $\varphi(n)$, се нарича функцията съпоставяща на всяко естествено число n броя на естествените числа, които не надминават и са взаимнопрости с n, т.е.*

$$\varphi(n) \stackrel{\text{def}}{=} |\{1 \le a \le n \mid (n, a) = 1\}|\,.$$

Теорема 2.1.9 *Ако $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ е разлагането на n на прости множители, то*

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}). \tag{2.1}$$

Доказателство. Доказателство, което ще дадем, се базира на добре известния и често употребяван в комбинаториката принцип за включване и изключване (Силвестър 1883 г.). За пълнота го формулираме.
Принцип за включване и изключване. *Нека E е множество, чиито $N = |E|$ елемента могат да притежават свойствата $P_1, P_2, \dots, P_k$. Нека $N_{i_1 \dots i_s}$ е броя на елементите на E, които притежават свойствата $P_{i_1}, \dots, P_{i_s}$. Тогава броят N_0 на всички елементи от E, които не притежават нито едно от свойствата P_i се дава с формулата*

$$N_0 = N - \sum_{i=1}^{k} N_i + \sum_{i,j} N_i N_j - \cdots + (-1)^k N_{12\dots k}.$$

Сега да пристъпим към доказателството на Теорема 2.1.9. Нека с P_i означим свойството едно число да е кратно на p_i. Елементите на $E = \{1, 2, \dots, n\}$, които не притежават нито едно от свойствата P_i са точно числата взаимнопрости с n. Тогава $N_i = n/p_i$ и по-общо $N_{i_1 \dots i_s} = n/(p_{i_1} \dots p_{i_s})$. Прилагайки принципа за включване и изключване получаваме

$$\varphi(n) = n\left(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i,j} \frac{1}{p_i p_j} + \cdots + (-1)^k \frac{1}{p_1 \cdots p_k}\right) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

Теорема 2.1.10 *Ако $(n, m) = 1$, то $\varphi(nm) = \varphi(n)\varphi(m)$.*

Доказателство. Мултипликативността на Ойлеровата функция следва веднага от Теорема 2.1.9, а нейно директно доказателство ще изложим в Глава 3. В такъв случай Теорема 2.1.10 заедно с лесно проверяемия факт $\varphi(p^k) = p^{k-1}(p-1)$ дават друго доказателство на формула (2.1).

Теорема 2.1.11 *Ако n е естествено число, то*

$$\sum_{d|n} \varphi(d) = n,$$

където сумирането се извършва по всички делители d на n.

Доказателство. Ако d е произволен делител на n, то има точно n/d негови кратни ненадминаващи n и това са

$$d,\ 2d,\ \dots,\ \frac{n}{d}\cdot d.$$

Най-големият общ делител $(kd,\, n) = d\cdot(k,\, n/d)$. Следователно $(kd,\, n) = d$ тогава и само тогава, когато $(k,\, n/d) = 1$. И така за точно $\varphi(n/d)$ числа $(kd,\, n) = d$. Но за всяко $a:\ 1 \le a \le n$, е в сила $(a, n) = d$, за някой делител d на n, т.е. $a = kd$, където $(k,\, n/d) = 1$. Следователно всяко такова число a попада в някоя от разгледаните групи и

$$\sum_{d|n} \varphi(\frac{n}{d}) = n.$$

Сега твърдението на теоремата следва от факта, че когато d пробягва всички делители на n същото прави и n/d.

Дефиниция 2.1.12 ***Функция на Мьобиус*** *наричаме функцията $\mu:\ \mathbb{N} \to \{0, 1, -1\}$ зададена с*

$$\mu(n) \overset{\text{def}}{=} \begin{cases} 1, & n = 1 \\ 0, & n \text{ се дели на точен квадрат} \\ (-1)^k, & n = p_1 \cdots p_k,\ \ p_i \text{ са различни прости числа.} \end{cases}$$

Лема 2.1.13

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$$

Доказателство. При $n = 1$ единственият делител е 1 и $\mu(n) = \mu(d) = 1$, т.е. твърдението е вярно. Нека $n > 1$ и $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Всеки делител d на n има вида $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, където $0 \le \alpha_j \le e_j$ са естествени числа. Ако $\alpha_j > 1$, то $\mu(d) = 0$. Следователно

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + \cdots + \mu(p_1 \dots p_k) \\ &= 1 - k + \binom{k}{2} + \cdots + \binom{k}{s}(-1)^s + \cdots + (-1)^k = (1-1)^k = 0. \end{aligned}$$

Теорема 2.1.14 *Ако $f(n)$ и $g(n)$ са две функции дефинирани за всяко естествено n и*

$$f(n) = \prod_{d|n} g(d), \tag{2.2}$$

то е изпълнено

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

Доказателство.

$$\prod_{d|n} f(d)^{\mu(\frac{n}{d})} = \prod_{d|n}\left(\prod_{s|d} g(s)\right)^{\mu(\frac{n}{d})} = \prod_{s|n}(g(s))^A,$$

където

$$A = \sum_{d\colon\, d|n,\, s|d} \mu\left(\frac{n}{d}\right).$$

Но за всяко s делящо n е изпълнено

$$\sum_{d\colon\, d|n,\, s|d} \mu\left(\frac{n}{d}\right) = \sum_{d=sd_1\colon\, d|n} \mu\left(\frac{n}{d}\right) = \sum_{d_1|\frac{n}{s}} \mu\left(\frac{n/s}{d_1}\right) = \sum_{\delta|\frac{n}{s}} \mu(\delta) = \begin{cases} 1, & s = n \\ 0, & s < n \end{cases},$$

където $\delta = \frac{n/s}{d_1} = \frac{n}{d}$. Следователно

$$\prod_{d|n} f(d)^{\mu(\frac{n}{d})} = g(n) \prod_{s|n,\, s<n} (g(s))^0 = g(n).$$

Теорема 2.1.15 *Ако $f(n)$ и $g(n)$ са две функции дефинирани за всяко естествено n и*

$$f(n) = \sum_{d|n} g(d), \tag{2.3}$$

то е изпълнено

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d).$$

Доказателство. Доказателството се получава с "логаритмуване" на доказателството на предходната теорема, т.е. заествайки произведението със сума, а степенуването с умножение.

Теореми 2.1.14 и 2.1.15 са известни под името *формули за обръщане*. Те показват, че две функции f и g, които са свързани с (2.2) или (2.3) се определят една друга еднозначно. Като следствие от Теорема 2.1.15 се получава друго доказателство на формулата за $\varphi(n)$ от Теорема 2.1.9. Наистина обръщайки равенството от Теорема 2.1.11 получаваме

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d = n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{i,j} \frac{n}{p_i p_j} + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

Преди да преминем по-нататък ще изложим някои от свойствата на функцията $\lfloor x \rfloor$.

Теорема 2.1.16 *Нека x, y са реални числа. В сила са следните свойства:*

(1) $\lfloor x+n \rfloor = \lfloor x \rfloor + n$ *за всяко* $n \in \mathbb{Z}$.

(2) $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ *или* $\lfloor x \rfloor + \lfloor y \rfloor + 1$.

(3) *Ако $n, m \in \mathbb{N}$, то броят на кратните на $m:\ 1 \leq km \leq n$, е равен на* $\lfloor n/m \rfloor$.

(4) $\left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor = \lfloor \frac{x+n}{m} \rfloor$ *за всяко $n, m \in \mathbb{Z},\ m > 0$. В частност* $\left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{b} \right\rfloor = \lfloor \frac{a}{b^2} \rfloor,\ b > 0$.

(5) $\lfloor x + \frac{1}{2} \rfloor$ *и* $-\lfloor -x + \frac{1}{2} \rfloor$ *са най-близкото до x цяло число. Ако съществуват две цели числа, които са най-близко до x, то първото е по-голямото, а второто по-малкото.*

(6) $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$ *и* $\lfloor \frac{1}{n} \lfloor nx \rfloor \rfloor$ *за всяко* $n \in \mathbb{N}$.

(7) *Броят на нечетните естествени числа $\leq n$ е* $\lfloor \frac{n+1}{2} \rfloor$.

Доказателство. Ще докажем (3) и (4), а другите свойства ще оставим за упражнение на читателя.
(3): Нека $n = mq + r,\ 0 \leq r < m$. Тогава $1,\ m,\ 2m,\ \ldots,\ qm$ са търсените кратни на m, т.е. те са точно q на брой. Но $q = \lfloor n/m \rfloor$.
(4): Нека $\lfloor x \rfloor + n = mq + r,\ 0 \leq r < m$, т.е. $\left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor = q$. Тогава $x + n = mq + r + \alpha < mq + r + 1$, където $0 \leq \alpha < 1$, което влече

$$q + \frac{r}{m} \leq \frac{x+n}{m} < q + \frac{r+1}{m} \leq q + 1.$$

Следователно

$$\left\lfloor \frac{x+n}{m} \right\rfloor = q = \left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor.$$

Теорема 2.1.17 *Нека $n \in \mathbb{Z}$ и p е просто число. Най-високата степен на p, която дели $n!$ се дава с формулата*

$$ord_p(n!) = \sum_{j=1}^{m} \left\lfloor \frac{n}{p^j} \right\rfloor,$$

където $p^m \leq n < p^{m+1}$.

Доказателство. Нека с a_i означим броят на числата измежду $1, 2, 3, \ldots, n$, които се делят на p^i. Всяко такова число се дели и на $p^j,\ 1 \leq j \leq i-1$, но приносът в $ord_p(n!)$ е i, а не 1. Следователно

$$ord_p(n!) = a_1 + a_2 + \cdots + a_m.$$

Но числата кратни на p^i са $p^i,\ 2p^i,\ \ldots,\ \lfloor \frac{n}{p^i} \rfloor p^i$. Следователно $a_i = \lfloor \frac{n}{p^i} \rfloor$, откъдето следва твърдението.
Да отбележим, че съгласно (4) на Теорема 2.1.16 $a_{i+1} = \lfloor \frac{a_i}{p} \rfloor$, което позволява лесно пресмятане на $ord_p(n!)$.

Упражнение 2.1.4 *Нека $a_1, a_2, \dots, a_k$ са две по две взаимнопрости естествени числа, т.е. $(a_i, a_j) = 1,\ i \neq j$. Докажете, че броят на естествените числа ненадминаващи x, които не се делят на никое от числата $a_1, a_2, \dots, a_k$ е равен на*

$$\lfloor x \rfloor - \sum_{j=1}^{k} \left\lfloor \frac{x}{a_j} \right\rfloor + \sum_{i,j} \left\lfloor \frac{x}{a_i a_j} \right\rfloor - \sum_{i,j,l} \left\lfloor \frac{x}{a_i a_j a_l} \right\rfloor + \cdots .$$

Упражнение 2.1.5 *Докажете, че най-високата степен на простото число p, която дели биномният коефициент $\binom{m+n}{n}$ е равна на броя на "преносите към следващия разряд" при събирането на m и n в p-ична бройна система.*

Забележка 2.3 *Навсякъде в текста по-нататък ще се придържаме към следните означения:*

$\log_a x$ *означава логаритъм от x при основа a.*

$\log x$ *означава логаритъм от x при основа 2.*

$\ln x$ *означава натурален логаритъм от x, т.е. при основа e.*

$\lg x$ *означава логаритъм от x при основа 10.*

Дефиниция 2.1.18 ***Функция на Манголдт*** *се нарича функцията дефинирана за всяко естествено n както следва:*

$$\Lambda(n) \stackrel{\text{def}}{=} \begin{cases} \ln p, & \text{ако } n = p^m,\ m \geq 1, \\ 0, & \text{в останалите случаи.} \end{cases}$$

Теорема 2.1.19 *В сила е равенството*

$$\sum_{d|n} \Lambda(d) = \ln n.$$

Доказателство. Нека $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Всеки делител d на n има вида $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, където $\alpha_j \geq 0$. Но $\Lambda(d) \neq 0$ тогава и само тогава, когато $d = p_i^{\alpha_i},\ 1 \leq \alpha_i \leq k_i$. Следователно

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{s} \sum_{j=1}^{k_i} \Lambda(p_i^{\alpha_i}) = \sum_{i=1}^{s} k_i \ln p_i = \ln n.$$

$\diamond$

Дефиниция 2.1.20 ***Функция на Чебишев*** *се нарича функцията дефинирана за всяко реално $x \geq 1$ чрез равенствата*

$$\theta(x) \stackrel{\text{def}}{=} \sum_{p \leq x} \ln p, \qquad \theta(1) \stackrel{\text{def}}{=} 0.$$

Теорема 2.1.21 *За всяко $x \geq 1$ е в сила* $\theta(x) < (4\ln 2)x$.

Доказателство. Разглеждаме биномния коефициент

$$\binom{2n}{n} = \frac{2n(2n-1)\dots(n+1)}{n!}.$$

Очевидно той се дели на всички прости числа $p:\ n < p \leq 2n$. От друга страна

$$\binom{2n}{n} < \sum_{j=1}^{2n} \binom{2n}{j} = (1+1)^{2n} = 4^n.$$

Следователно

$$\prod_{n<p\leq 2n} p < \binom{2n}{n} < 4^n.$$

Логаритмувайки получаваме

$$\sum_{n<p\leq 2n} \ln p < 2n \ln 2.$$

Но $\sum_{n<p\leq 2n} \ln p = \theta(2n) - \theta(n)$. Следователно

$$\theta(2n) - \theta(n) < 2n \ln 2.$$

Сумирайки за $n = 1, 2, \dots, 2^{m-1}$, където $2^{m-1} \leq x < 2^m$, получаваме

$$\theta(x) \leq \theta(2^n) < 2\ln 2 \cdot (2^{m-1} + \dots + 2 + 1) = 2\ln 2 \cdot (2^m - 1) < 4\ln 2 \cdot 2^{m-1}.$$

Следователно $\theta(x) < (4\ln 2)x$.

Теорема 2.1.22 *Съществува положителна константа c, така че $c.x < \theta(x)$ за всяко $x \geq 2$.*

Доказателство. Да разгледаме отново

$$\binom{2n}{n} = \frac{2n(2n-1)\dots(n+1)}{n!}.$$

Нека p е просто число и m_p е максималното естествено число, за което $p^{m_p} \leq 2n$. Съгласно Теорема 2.1.17

$$ord_p \binom{2n}{n} = \sum_{i=1}^{m_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right).$$

Но $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 0$ или 1. Следователно $ord_p \binom{2n}{n} \leq m_p$ и

$$\binom{2n}{n} \leq \prod_{p\leq 2n} p^{m_p}.$$

Вземайки предвид, че

$$\frac{(n+n)(n+n-1)\cdots(n+1)}{n!} \geq 2^n$$

можем да заключим, че

$$2^n \leq \prod_{p \leq 2n} p^{m_p}.$$

Логаритмувайки това неравенство получаваме

$$n \ln 2 \leq \sum_{p \leq 2n} m_p \ln p.$$

Тъй като $m_p = \left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor \leq \frac{\ln 2n}{\ln p}$ и $\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor = 1$ за $p > \sqrt{2n}$, то

$$n \ln 2 \leq \sum_{p \leq \sqrt{2n}} \left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor \cdot \ln p + \sum_{\sqrt{2n} < p \leq 2n} \ln p \leq \sum_{p \leq \sqrt{2n}} \frac{\ln 2n}{\ln p} \cdot \ln p + \theta(2n) - \theta(\sqrt{2n}).$$

Ако означим с K броя на простите числа $\leq \sqrt{2n}$, то $\theta(\sqrt{2n}) > K \ln 2$ и

$$n \ln 2 \leq K \ln 2n - K \ln 2 + \theta(2n) < \sqrt{2n} \ln n + \theta(2n).$$

Следователно

$$\theta(2n) \geq 2n \left(\frac{\ln 2}{2} - \frac{\ln n}{\sqrt{2n}} \right).$$

Но $\lim_{n \to \infty} \frac{\ln n}{\sqrt{n}} = 0$. Следователно за достатъчно големи n съществува константа $c_1 > 0$, такава че

$$\theta(2n) \geq c_1 \cdot 2n.$$

Ако $2n \leq x < 2(n+1)$, за достатъчно големи x е изпълнено

$$\theta(x) \geq \theta(2n) \geq c_1 \cdot 2n > c_1(x-2) \geq c_2 x.$$

В такъв случай можем да твърдим (вземайки минималната измежду краен брой константи), че съществува константа $c > 0$, такава че

$$\theta(x) > c \cdot x$$

за $x > 2$.

2.2 Разпределение на простите числа.

Теорема 2.2.1 *Съществуват безброй много прости числа.*

> ***Доказателство.*** Да допуснем, че $p_1, p_2, \ldots, p_n$ са всички прости числа. Разглеждаме числото $a = p_1 p_2 \cdots p_n + 1$. Ако числото a не е просто, то трябва да се дели на някое просто число p_i. Но тогава p_i ще дели 1, което е невъзможно. Следователпо a е просто число и очевидно е различно от $p_1, p_2, \ldots, p_n$. Полученото противоречие се дължи на допускането, че има само краен брой прости числа.

Следващата теорема показва, че може да се намери произволно голяма “дупка” между две последователни прости числа.

Теорема 2.2.2 *За всяко k съществуват поне k последователни числа, които не са прости.*

> ***Доказателство.*** Да разгледаме числата $(k+1)!+2$, $(k+1)!+3$, $\ldots$, $(k+1)!+k+1$. За всяко $l: \quad 2 \le l \le k+1$, числото $(k+1)!+l$ се дели на l. Следователно всички тези k числа са съставни.

Твърдение 2.2.3 *Всяко едно от множества естествени числа* $\{\, 4n-1 \mid n = 1, 2, \ldots \,\}$ *и* $\{\, 6n-1 \mid n = 1, 2, \ldots \,\}$ *съдържа безброй много прости числа.*

> ***Доказателство.*** Нека n е произволно естествено число. Разглеждаме $M = 4n! - 1$. То не може да има прости делители само от вида $4k+1$, защото произведението на две такива числа е пак число от същия вид: $(4k+1)(4l+1) = 4(4kl+k+l)+1$. Следователно M има поне един прост делител от вида $4k-1$ и този делител не може да бъде число ненадминаващо n (в противния случай ще дели 1). И така за всяко естествено n съществува просто число от вида $4k-1$, което е по-голямо от n. Оставяйки n да расте неограничено получаваме безброй много прости числа от вида $4k-1$.
> Доказателството на другото твърдение оставяме за упражнение на читателя.

Горните твърдения са частен случай на знаменитата теорема Дирихле за простите числа в аритметически прогресии:

Теорема 2.2.4 *Всяка аритметическа прогресия* $\{an+b \mid n = 1, 2, \ldots\}$, *с* $(a, b) = 1$ *съдържа безброй много прости числа.*

Целите и обемът на настоящото изложение, обаче, не позволяват да включим нейното доказателството.

Сега да се опитаме да дадем някои по-точни оценки за разпределението на простите числа. Да означим с $\pi(x)$ броя на всички прости числа ненадминаваши x, т.е.

$$\pi(x) \stackrel{\text{def}}{=} \{p \text{ прости} \mid 1 < p \le x\}$$

Следващите две теореми дават някои груби оценки за $\pi(x)$.

Теорема 2.2.5 $\pi(x) \geq \ln(\ln x)$ *за всяко* $x \geq 2$.

Доказателство. Да означим с p_n n-тото просто число. Тъй като никое от $p_1, p_2, \dots, p_n$ не делят $p_1 p_2 \cdots p_n + 1$, то $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$. Използвайки този факт по индукция можем да заключим, че $p_n < 2^{2^n}$. Наистина $p_1 < 2^{2^1}$, $p_2 < 2^{2^2}$ и от $p_n < 2^{2^n}$ следва, че

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 < 2^{2^1} 2^{2^2} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}}.$$

Но в такъв случай $\pi(2^{2^n}) \geq n$. Нека сега за дадено $x > 2$ цялото число n е избрано така, че $e^{e^{n-1}} < x \leq e^{e^n}$. За всяко $n > 3$ е в сила $e^{n-1} > 2^n$, откъдето при $x > e^e$ получаваме

$$\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(e^{2^n}) \geq n \geq \ln(\ln x).$$

При $x \leq e^e$ неравенството е очевидно.

Теорема 2.2.6 $\pi(x) \geq \dfrac{\ln x}{2 \ln 2}$.

Доказателство. Да положим $m = \pi(x)$ и да разгледаме множеството $S = \{p_1, p_2, \dots, p_m\}$ от всички прости числа $\leq x$. Нека с $f_S(x)$ означим броя на всички цели числа $n:\ 1 \leq n \leq x$, чиито прости делители се съдържат в S. При направения избор на S очевидно $f_S(x) = x$ (считаме x цяло). От друга страна като запишем произволно n във вида $n = t^2 s$, където s е свободно от квадрати естествено число можем да заключим, че $t \leq \sqrt{x}$, а s е произведение от прости числа образуващи подмножество на S. Следователно има най-много 2^m възможности за s - толкова колкото е броят на различните подмножества на S. Следователно $x = f_S(x) \leq 2^m \sqrt{x} = 2^{\pi(x)} \sqrt{x}$. Логаритмувайки получаваме търсеното неравенство.

В 1798 г. Льожандр публикува предположението, че

$$\pi(x) \approx \frac{x}{\ln x - 1,08366} \tag{2.4}$$

Тази формула дава доста добро приближение за x ненадминаващи 10^8, но с нарастването на x започва да се различава значително. В 1848 г. руският математик Чебишев доказва следните твърдения.

Теорема 2.2.7 *За всяко* $x \geq 2$ *е в сила*

$$\frac{\theta(x)}{\ln x} \leq \pi(x) \leq 2\frac{\theta(x)}{\ln x} + \sqrt{x}.$$

Доказателство.

$$\theta(x) = \sum_{p \leq x} \ln p \leq \pi(x) \cdot \ln x,$$

което дава лявото неравенство. От друга страна

$$\begin{aligned}\theta(x) &= \sum_{p\le x}\ln p = \sum_{p\le\sqrt{x}}\ln p + \sum_{p\ge\sqrt{x}}\ln p \ge \sum_{p\ge\sqrt{x}}\ln p \ge [\pi(x)-\pi(\sqrt{x})]\ln\sqrt{x}\\ &= \frac{1}{2}\ln x[\pi(x)-\pi(\sqrt{x})] \ge \frac{1}{2}\ln x[\pi(x)-\sqrt{x}]\end{aligned}$$

Следователно

$$2\frac{\theta(x)}{\ln x} \ge \pi(x)-\sqrt{x},$$

откъдето получаваме и дясното неравенство.

Теорема 2.2.8 *Съществуват константи A и B, такива че за всяко $x \ge 2$ е изпълнено:*

$$A\frac{x}{\ln x} < \pi(x) < B\frac{x}{\ln x}.$$

Доказателство. Съгласно Теорема 2.2.7 $\pi(x) \ge \frac{\theta(x)}{\ln x}$. Прилагайки Теорема 2.1.22 получаваме търсената оценка отляво. Аналогично от неравенствата

$$\pi(x) \le 2\frac{\theta(x)}{\ln x} + \sqrt{x} \quad \text{и} \quad \theta(x) < 4x\ln 2$$

дадени съответно в Теорема 2.2.7 и Теорема 2.1.21, и вземайки предвид, че $\sqrt{x} > \frac{1}{2}\ln x$ за $x \ge 1$ получаваме

$$\pi(x) < 8\ln 2\frac{x}{\ln x} + \frac{1}{2}\ln x\frac{2\sqrt{x}}{\ln x} < 8\ln 2\frac{x}{\ln x} + \frac{2x}{\ln x}$$

Следователно

$$\pi(x) < (2+8\ln 2)\frac{x}{\ln x}.$$

Следствие 2.2.9 $\displaystyle\lim_{x\to\infty}\frac{\pi(x)}{x} = 0.$

В 1851 г. Чебишев прецизира резултатите и показва, че за достатъчно големи x

$$(0,92\ldots)\frac{x}{\ln x} < \pi(x) \le (1,105\ldots)\frac{x}{\ln x}$$

Това представлява значителна стъпка към доказателството на така наречената ***Теоремата за простите числа***:

Теорема 2.2.10 $\displaystyle\lim_{x\to\infty}\frac{\pi(x)\ln x}{x} = 1.$

Тя е доказана през 1896 г. (почти едновременно и независимо един от друг) от Адамар и де ла Вале Пуасен използвайки свойствата на комплекснозначната дзета-функция на Риман, т.е. с аналитични методи. Доказателство без използване на комплексния анализ е получено чак в 1949 г. от Селберг и Ердьош (също независимо един от друг).

Следващата таблица дава представа за ръста на $\pi(x)$ и $x/\ln(x)$ в зависимост от x.

x	$\pi(x)$	$\lfloor x/\ln(x)\rfloor$	Льожандр	x	$\pi(x)$	$\lfloor x/\ln(x)\rfloor$	Льожандр
100	25	21	28,4	8 000	1007	890	1012
300	62	52	64,9	10^4	1 229	1 085	1 230
500	95	80	97,4	10^5	9 592	8 685	9 588
800	139	119	142,8	$6\cdot 10^5$	49 098	45 096	49 096
1 000	168	144	171,7	10^6	78 498	72 382	78 543
2 000	303	263	306,9	$5\cdot 10^6$	348 513	324 150	348 644
3 000	430	374	433,4	10^7	664 579	620 420	665 139
4 000	550	482	554,7	$5\cdot 10^7$	3 001 134	2 820 471	3 004 108
5 000	669	587	672,6	$6\cdot 10^7$	3 562 115	3 350 110	3 565 868
6 000	783	689	787,8	10^8	5 761 455	5 428 681	5 768 003

Да отбележим, че за горните стойности на x оценката (2.4) на Льожандр е много поточна. Това илюстрира добре, че теоремата за простите числа е асимптотически резултат, т.е. в сила е за много големи n.

2.3 Допълнителни задачи към Глава 2.

Задача 2.1 *Докажете, че ако n е съставно число, то $\varphi(n) \le n - \sqrt{n}$.*

Задача 2.2 *Докажете, че* $\displaystyle\sum_{(a,n)=1} a = \frac{1}{2} n\varphi(n)$.

Задача 2.3 *Нека p и q са прости числа. Да се намери n, ако $n = pq$ и $\varphi(n) = 120$.*

Задача 2.4 *Да се реши уравнението* $\varphi(n) = \dfrac{n}{2}$.

Задача 2.5 *С колко нули завършва (в десния край) числото 100! записано в десетична бройна система.*

Задача 2.6 *Нека $s(n)$ е сумата от цифрите на числото n записано в p-ична бройна система. Да се докаже, че $p^e \mid n!$, но p^{e+1} не дели $n!$, където* $e = \dfrac{n - s(n)}{p-1}$.

Задача 2.7 *За произволни естествено число n и реално число ξ докажете, че е в сила равенството*

$$\lfloor \xi \rfloor + \left\lfloor \xi + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor \xi + \frac{n-1}{n} \right\rfloor = \lfloor n\xi \rfloor.$$

Задача 2.8 *Докажете, че за всяко естествено число n,*

$$\sum_{(a,n)=1} e^{\frac{2\pi i a}{n}} = \mu(n).$$