Елементи от теория на числата
част 2

доц. Евгения Великова

Февруари 2021

Най-голям общ делител

определение НОД

Нека $a, b \in \mathbb{Z}$ и поне едно от двете е различно от нула. Най-голямото естествено число d, което дели едновременно и двете числа ($d|a$ и $d|b$) се нарича техен **най-голям общ делител** и се отбелязва по следния начин $d = (a, b)$ или $d = \texttt{НОД}(a, b) = \texttt{GCD}(a, b)$

Свойства

- $(a, 0) = a$, за произволно $a \in \mathbb{N}$
- $(a, b) = (\pm a, \pm b)$

Теорема (Безу)

Нека $a, b \in \mathbb{Z}$, поне едно от тях е ненулево и $d = (a, b)$.
Съществуват цели числа $u, v \in \mathbb{Z}$, за които е изпълнено

$$d = (a, b) = au + bv \quad \textit{(Тъждество на Безу)}$$

Доказателство: Разглеждаме $M = \{xa + yb \mid x, y \in \mathbb{Z}\}$
Нека $d = au + bv \in M$ е **минималното положително число** от M.
Нека $t = ax + by \in M$ е произволно

$$\begin{array}{rcl} t & = & dq + r, \quad \text{където} \quad 0 \le r < d \\ r & = & t - dq = ax + by - (au + bv)q = a(x - uq) + b(y - vq) \ \in \ M \end{array}$$

$r \in M$ и $d > r \geq 0$, следователно $r = 0$, откъдето следва че $d|t$.
Получихме, че $d|a$ и $d|b$.

$$\left.\begin{array}{l} d_1|a \\ d_1|b \end{array}\right\} \Rightarrow d_1|\underbrace{(au + bv)}_{=d}, \text{ т.е. } d_1|d \ \Rightarrow \ d_1 \le d$$

свойства на НОД (2)

Ако $d = \text{НОД}(a, b)$, тогава d се дели на всеки общ делител на a и b.

Забележка: *Числата от тъждеството на Безу не са единствени. Ако $d = (a, b) = au + bv$, тогава за k- произволно е изпълнено*

$$d = au + bv = au + abk + bv - abk = a(u + bk) + b(v - ak)$$

Свойство

Нека a, b са ненулеви и $a = bq + r$, където $0 \leq r < b$, тогава

$$\text{Ако} \quad a = bq + r \ \Rightarrow (a, b) = (b, r).$$

Доказателство: Нека $d = (a, b)$ и $d_1 = (b, r)$

$$\left.\begin{array}{c} \left.\begin{array}{c} d|b \\ d|a \end{array}\right\} \Rightarrow d|\underbrace{(a - bq)}_{=r} \Rightarrow \left|\begin{array}{c} d|b \\ d|r \end{array}\right\} \Rightarrow d|d_1 \\ \hline \left.\begin{array}{c} d_1|b \\ d_1|r \end{array}\right\} \Rightarrow d_1|\underbrace{(bq + r)}_{=a} \Rightarrow \left|\begin{array}{c} d_1|b \\ d_1|a \end{array}\right\} \Rightarrow d_1|d \end{array}\right\} \Rightarrow d = d_1$$

Алгоритъм на Евклид за намиране на НОД

Зададени са a, b ненулеви цели числа

- **Стъпка 1:** Разделят се с частно и остатък
$$a = bq_1 + r_1, \quad \text{където } 0 \le r_1 < b, \quad \text{и} \quad (a, b) = (b, r_1)$$
  - ако $r_1 = 0$ следователно $b = (a, b)$ (край).
  - ако $r_1 \neq 0$,преминаваме към следващата стъпка.
- **Стъпка 2:** Разделя се b на r_1
$$b = r_1 q_2 + r_2, \quad \text{където } 0 \le r_2 < r_1, \quad \text{и} \quad (b, r_1) = (r_1, r_2)$$
  - ако $r_2 = 0$ следователно $r_1 = (a, b)$ (край).
  - ако $r_2 \neq 0$,преминаваме към следващата стъпка.
- ....
- **Стъпка** $k + 1$: Разделя се r_{k-1} на r_k
$r_{k-1} = r_k q_{k+1} + r_{k+1}, \quad \text{където } 0 \le r_{k+1} < r_k, \quad \text{и} \quad (r_{k-1}, r_k) = (r_k, r_{k+1})$
  - ако $r_{k+1} = 0$ следователно е намерен най-големият общ делител - последния ненулев остатък $r_k = (a, b)$ (край).
  - ако $r_{k+1} \neq 0$, преминаваме към следващата стъпка.

Алгоритъма е краен, защото $b > r_1 > r_2 > \ldots > r_k > r_{k+1} \ldots \ge 0$.

Пример

Да се пресметне най-големият общ делител на $a = 7293$ и $b = 3147$ и да се намери тъждеството на Безу за тях.

$$
\begin{array}{ccr}
7293{=}2.3147{+}999 & \Rightarrow & 3{=}20.3147 - 63.(7293 - 2.3147) = -63.a + 146.b \\
3147{=}3.999{+}150 & \Rightarrow & 3{=} - 3.999{+}20(3147{-}3.999){=}20.3147{-}63.999 \Uparrow \\
999{=}6.150 + 99 & \Rightarrow & 3{=}2.150{-}3.(999{-}6.150){=} - 3.999{+}20.150 \Uparrow \\
150{=}1.99 + 51 & \Rightarrow & 3{=}2(150{-}99){-}99{=}2.150{-}3.99 \Uparrow \\
99{=}1.51 + 48 & \Rightarrow & 3{=}51{-}(99{-}51){=}2.51{-}99 \Uparrow \\
51{=}1.48 + 3 & \Rightarrow & 3 = 51 - 48 \Uparrow \\
48{=}16.3 + 0 & \Rightarrow & \boxed{3 = (7293, 3147)}
\end{array}
$$

Взаимно прости числа

Определение

Ненулевите числа $a, b \in \mathbb{Z}$ се наричат **взаимно прости**, ако $(a, b) = 1$.

Твърдение

Нека $a, b \in \mathbb{Z}$ и $(a, b) = 1$, тогава е изпълнено

1. ако $a \mid bc$, следва че $a \mid c$;
2. ако $a \mid c$ и $b \mid c$, следва че $ab \mid c$;

Доказателство:

1. От $(a, b) = 1 \;\Rightarrow$ съществуват $u, v \in \mathbb{Z}$, за които $1 = au + bv$.
$$a|bc \;\Rightarrow\; a|\underbrace{cau + cbv}_{=c} \;\Rightarrow\; a|c$$
2. От $a|c \;\Rightarrow c = aq$.
$$\left.\begin{array}{r} b|c \\ c = aq \end{array}\right\} \Rightarrow\; b|aq \xrightarrow[(a,b)=1]{} b|q \Rightarrow\; q = bt \Rightarrow\; c = abt \Rightarrow\; ab|c.$$

Определение

Естественото число $p \in \mathbb{N}, \quad p > 1$ се нарича **просто число**, ако единствените естествени числа, които го делят са 1 и p.

$$p \text{ просто число } \Leftrightarrow \text{ ако от } \left| \begin{array}{l} x|p \\ x \in \mathbb{N} \end{array} \right\} \to x = 1 \text{ или } x = p.$$

Свойство

Всяко естествено число $n > 1$ е или просто или се дели на някакво просто число .

Доказателство: Ако допуснем, че n не е просто, следователно n се дели на някое число $t|n$, за което $1 < t < n$. Нека $k > 1$ е минималното число, което дели n и $1 < k < n$.
Ако $s < k$, такова че $s|k \Rightarrow s|n$ и от минималността на $k > 1$ следва че $s = 1$. Следователно k е просто число което дели n.

Решето на Ератостен

Решето на Ератостен - алгоритъм за получаване на простите числа, които са от 1 до N.

- Записват се числата от 2 до N и започвайки подред за всяко число k се прави следното:
    1. ако числото k не е задраскано се отбелязва като просто число и задраскваме всяко $k-$то число след него. След това се преминава към следващото число;
    2. ако числото k е задраскано, нищо не се прави и се преминава към следващото число;

В примера е показано как се определят простите числа < 50.

	$\boxed{2}$	$\boxed{3}$	$\cancel{4}$	$\boxed{5}$	$\cancel{6}$	$\boxed{7}$	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
$\boxed{11}$	$\cancel{12}$	$\boxed{13}$	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	$\boxed{17}$	$\cancel{18}$	$\boxed{19}$	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	$\boxed{23}$	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	$\boxed{29}$	$\cancel{30}$
$\boxed{31}$	$\cancel{32}$	$\cancel{33}$	$\cancel{34}$	$\cancel{35}$	$\cancel{36}$	$\boxed{37}$	$\cancel{38}$	$\cancel{39}$	$\cancel{40}$
$\boxed{41}$	$\cancel{42}$	$\boxed{43}$	$\cancel{44}$	$\cancel{45}$	$\cancel{46}$	$\boxed{47}$	$\cancel{48}$	$\cancel{49}$	$\cancel{50}$

Свойства на простите числа

Теорема на Архимед

Простите числа са безброй много.

Доказателство: Допускаме, че простите числа са краен брой и нека всички прости числа са $p_1, \ldots, p_k$.
Разглеждаме $a = 1 + p_1 \cdot \ldots \cdot p_1$

- a не е просто, защото не е измежду $p_1, \ldots, p_k$.
- $p_i \nmid a$ за $i = 1, \ldots, k$, следователно a не се дели на прости числа

Получихме противоречие $\Rightarrow$ допускането че простите числа са краен брой е грешно, следователно простите числа са безброй много.

Свойство

Ако p е просто число и a е произволно цяло число, тогава

$$(p, a) = \begin{cases} p, & \text{когато } \; p \mid a \\ 1, & \text{когато } \; p \nmid a \end{cases}$$

Свойства простите числа (2)

Твърдение

Ако p е просто число, което дели произведение на няколко цели числа, тогава p дели поне един от множителите.

$$\text{ако } p\text{-просто число и } \ p \mid a_1.\dots.a_s \ \Rightarrow \ \exists i : p \mid a_i$$

Доказателство: Индукция по s - броя на множителите.
Ако $s = 1$, тогава $p \mid a_1$ и няма какво да се доказва.
Допускаме, че твърдението е вярно за s множителя $a_1, \dots, a_s$.
Нека p - просто число и $p \mid a_1.\dots.a_s.a_{s+1}$. Тогава:

- ако $p \mid a_{s+1}$, следователно твърдението е изпълнено;
- ако $p \nmid a_{s+1}$, следователно $(p, a_{s+1}) = 1$ и

$$\left.\begin{array}{r} p \mid (a_1 \dots a_s)a_{s+1} \\ (p, a_{s+1}) = 1 \end{array}\right\} \Rightarrow \ p \mid a_1 \dots a_s.$$

Тогава от индукционно предположение следва, че p дели някой от множителите $a_1, \dots, a_s$.

Основна теорема на аритметиката

Всяко естествено число $n > 1$ може да се представи по "единствен начин"(с точност до пренареждане на множителите) като произведение на прости числа.

Доказателство: $\boxed{\exists}$ Индукция по n

- **База :** $n = 2$ - числото 2 е просто и считаме, че 2 е представено като "произведение"на един множител.
- **Индукционно предположение:** предполагаме, че е вярно за всички естествени k, където $1 < k < n$.
- **Индукционна стъпка:** Доказваме за n. Имаме два случая:
  - Ако n е просто число, тогава n е "произведение"на един множител.
  - Ако n е съставно число, тогава $n = a.b$, където $a < n, \quad b < n$. Прилагаме индукционното предположение и получаваме

$$\left.\begin{array}{r} a = p_1.\dots.p_s \\ b = q_1.\dots.q_t \\ p_i \;\; q_j \;\; - \text{ прости} \end{array}\right\} \Rightarrow \;\; n = a.b = p_1.\dots.p_s.q_1.\dots.q_t$$

Осн.Th. на аритметиката - доказателство (продълж.)

$\boxed{"!"}$ Да разгледаме n представено по два начина като произведение на прости числа $n = p_1.\dots.p_k$ и $n = q_1.\dots.q_s$, където p_i и q_j са прости.

$$p_1.\dots.p_k = q_1.\dots.q_s \quad \Rightarrow \quad p_k \mid q_1.\dots.q_s$$

Следователно p_k дели някой измежду множителите $q_1, \dots, q_s$.
Преномерираме ги, така че да е изпълнено $p_k \mid q_s$.
Числото q_s е просто, откъдето получаваме, че $p_k = q_s$.

$$(p_1 \dots .p_{k-1}).p_k = (q_1 \dots .q_{s-1}).p_k \ \Rightarrow \ p_1 \dots .p_{k-1} = q_1 \dots .q_{s-1}$$

Продължава се по същия начин.
Ако допуснем, че $k \neq s$ (например $k < s$) след k стъпки ще получим $1 = q_1.\dots.q_{s-k}$ - невъзможно е !
Следователно $s = k$ и след преномериране е изпълнено $p_i = q_i$ за $i = 1, \dots, k$

Функция на Ойлер

Функция на Ойлер-определение

Нека $n \in \mathbb{N}$, $\varphi(n)$ е броят на естествените числа, по-малки от n и взаимно прости с n. Приемаме, че $\varphi(1) = 1$.
Функцията, определена така се нарича **функция на Ойлер**.

$$\varphi : \mathbb{N} \to \mathbb{N}, \text{ където } \varphi(n) = \left|\{k \in \mathbb{N} \mid k < n, \quad (k, n) = 1\}\right|.$$

$\varphi(2) = 1$, $\varphi(3) = 2$ и $\varphi(5) = 4$.
Ако p е просто число, тогава p е взаимно просто с всички естествени числа, по-малки от него.

Свойство

Ако p е просто числото, тогава $\varphi(p) = p - 1$.

Функция на Ойлер (2)

$\varphi(4) = 2 = |\{1, 3\}|$, $\varphi(8) = 4 = |\{1, 3, 5, 7\}|$, $\varphi(9) = 6 = |\{1, 2, 4, 5, 7, 8\}|$

Свойство

Ако p е просто число и тогава $\varphi(p^k) = p^k - p^{k-1}$, където $k \in \mathbb{N}$.

Доказателство: p е просто число, следователно $(p^k, t) = 1 \Leftrightarrow p \nmid t$. Множеството от по-малките от p^k, които са взаимно прости с p^k е

$$M = \{t \in \mathbb{N} \mid t < p^k, \ \ (t, p^k) = 1\} = \{t \in \mathbb{N} \ \mid \ t < p^k, \ p \nmid t\}$$

$$M = \{1, 2, \ldots, p^k\} \setminus \{p, 2p, \ldots, p^{k-1}.p\}$$

Следователно $\varphi(p^k) = |M| = p^k - p^{k-1}$.

Примери: $\varphi(1024) = 512$, $\varphi(625) = 625 - 125 = 500$

Лема

Нека a, b са естествени числа и a, b са взаимно прости $(a, b) = 1$, тогава е изпълнено, че $t \in \mathbb{N}$ е взаимно просто с ab точно когато t е взаимно просто както с a, така и с b.

Доказателство: $\boxed{\Rightarrow}$ Нека $(t, ab) = 1$ и нека $d_1 = (t, a)$ и $d_2 = (t, b)$. Прилагаме теоремата на Безу

$$tu + abv = 1 \;\Rightarrow\; \begin{cases} d_1 \mid t, \quad d_1 \mid a \;\Rightarrow\; d_1 \mid 1 \;\Rightarrow\; d_1 = (t, a) = 1 \\ \\ d_2 \mid t, \quad d_2 \mid b \;\Rightarrow\; d_2 \mid 1 \;\Rightarrow\; d_2 = (t, b) = 1 \end{cases}$$

$\boxed{\Leftarrow}$ Имаме че $(t, a) = 1$ и $(t, b) = 1$. Написваме тъждествата на Безу $tu_1 + av_1 = 1$ и $u_2 t + v_2 b = 1$ и ги умножаваме

$$\begin{aligned} 1 &= (u_1 t + v_1 a).(u_2 t + v_2 b) \\ 1 &= (u_1 u_2 t + u_1 v_2 b + v_1 u_2 a)t + v_1 v_2 ab \end{aligned}$$

Следователно (t, ab) дели 1 и t е взаимно просто с ab.

Теорема

Нека a, b са естествени числа, които са взаимно прости $(a, b) = 1$. Тогава за функцията на Ойлер е изпълнено $\varphi(a.b) = \varphi(a).\varphi(b)$.

Доказателство: Търсим числа, които са едновременно взаимно прости с a и с b. Записваме всички числа в матрица

$$M = \begin{pmatrix} 1 & 2 & \dots & a \\ a+1 & a+2 & \dots & 2a \\ \dots & \dots & \dots & \dots \\ (b-1)a+1 & (b-1)a+2 & \dots & ba \end{pmatrix}, \quad c_k = \begin{pmatrix} k \\ a+k \\ \dots \\ (b-1)a+k \end{pmatrix}.$$

Числата от c_k дават равен остатък k при делене с a и $(sa+k, a)=(k, a)$.
$\Rightarrow$ или всички числа от c_k са взаимно прости с a или всички не са взаимно прости с a.
В първия ред имаме $\varphi(a)$ взаимно прости с a числа и $\Rightarrow$ всички взаимно прости с a числа от матрицата са върху $\varphi(a)$ стълба на M.

Делим числата от стълб c_k с частно и остатък

$$\left.\begin{array}{rcl} k & = & q_0 b + r_0 \\ a+k & = & q_1 b + r_1 \\ \ldots\ldots\ldots & & \ldots\ldots\ldots \\ (b-1)a+k & = & q_{b-1} b + r_{b-1} \end{array}\right., \quad 0 \le r_i < b, \quad \text{за} \quad i = 0, 1, \ldots, b-1.$$

Допускаме, че съществуват два равни остатъка, т.е. съществуват различни индекси i, j, за които $r_i = r_j$ и $0 \le i < j < b$.

$$\begin{array}{c} ja + k = q_j b + r_j \\ ia + k = q_i b + r_i \\ \hline (j-i)a = b(q_j - q_i) \end{array} \quad \Rightarrow \quad b \mid (j-i)a \xrightarrow[(a,b)=1]{} b \mid (j-i)$$

Получихме, че $b \mid (j-i)$, но $0 < j - i < b$, което е противоречие.
Следователно $\{r_0, r_1, \ldots, r_{b-1}\} = \{0, 1, \ldots, b-1\}$.
Получаваме, че във всеки стълб на M има по $\varphi(b)$ числа, които са взаимно прости с b.
Окончателно $\varphi(ab) = \varphi(a).\varphi(b)$.

пример

Да пресметнем $\varphi(40)$, $40 = 8.5$ и намираме $\varphi(40) = \varphi(8).\varphi(5) = 4.4 = 16$.

$$M = \begin{pmatrix} \boxed{1} & 2 & \boxed{3} & 4 & 5 & 6 & \boxed{7} & 8 \\ \boxed{9} & 10 & \boxed{11} & 12 & \boxed{13} & 14 & 15 & 16 \\ \boxed{17} & 18 & \boxed{19} & 20 & \boxed{21} & 22 & \boxed{23} & 24 \\ 25 & 26 & \boxed{27} & 28 & \boxed{29} & 30 & \boxed{31} & 32 \\ \boxed{33} & 34 & 35 & 36 & \boxed{37} & 38 & \boxed{39} & 40 \end{pmatrix}$$

Например $40 = 4.10$, но тези числа не са взаимно прости и затова нямаме равенство

$$\varphi(40) = 16 \neq \varphi(4).\varphi(10) = 2.4 = 8$$

формули за функцията на Ойлер

пресмятане на $\varphi(n)$

Нека $n > 1$ и нека $n = p_1^{k_1}.\dots.p_s^{k_s}$, където $p_1, \dots, p_s$ са различни прости числа и $k_i > 0$. Тогава са изпълнени следните равенства, които задават начини за пресмятане на функцията на Ойлер:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1}).\dots.\varphi(p_s^{k_s}) \\
\varphi(n) &= (p_1^{k_1} - p_1^{k_1-1}).\dots.(p_s^{k_s} - p_s^{k_s-1}) \\
\varphi(n) &= p_1^{k_1-1}.\dots.p_s^{k_s-1}(p_1 - 1).\dots.(p_s - 1) \\
\varphi(n) &= n(1 - \tfrac{1}{p_1}).\dots.(1 - \tfrac{1}{p_s})
\end{aligned}$$

Пример Да се пресметне функцията на Ойлер за 144000.
$144000 = 144.1000 = 12^2.10^3 = 2^7.3^2.5^3$

$$\varphi(144000) = 144000.(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 144000.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 38400$$