Увод в Теория на числата

Иво Стратев

19 февруари 2018 г.

Съдържание

Под число ще разбираме цяло число, освен ако изрично не е оказано от кое числово множество е даден елемент.

1 Делимост на цели числа

Определение 1. Делимост.
Казваме, че ненулевото число a дели числото b (или b се дели на a), ако съществува число c, такова че $b = ac$. Числото a наричаме *делител* на b, а b - *кратно* на a.
За да отебележим, че a дели b ще използваме означението $a \mid b$. Напротив за да отебележим, че a не дели b ще използваме означението $a \nmid b$. означението $a \nmid b$.

1.1 Основни свойства

1. $\forall a,\ b \in \mathbb{Z}\ :\ a \mid b \implies \pm a \mid \pm b$

2. $\forall a \in \mathbb{Z}\ :\ a \neq 0 \implies a \mid a\ (a = 1.a)$

3. $\forall a,\ b \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \neq 0 \implies |a| \leq |b|$

   Доказателство. Нека $a,\ b \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \neq 0$

   $\implies \exists c \in \mathbb{Z}\ :\ c \neq 0\ \wedge\ b = ac \implies |b| = |ac| = |a||c|$

   $\implies |a| \leq |b|\ (c \neq 0 \implies |c| > 0)$ □

4. $\forall a \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \mid a \implies a = \pm b$

   Доказателство. Нека $a,\ b \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \mid a$

   $\implies a \neq 0\ \wedge\ b \neq 0 \implies |a| \leq |b| \wedge |b| \leq |a| \implies |a| = |b| \implies a = \pm b$ □

5. $\forall a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \mid c \implies a \mid c$

   Доказателство. Нека $a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b\ \wedge\ b \mid c$

   $\implies \exists u,\ v \in \mathbb{Z}\ :\ b = ua\ \wedge c = vb \implies c = vua = (vu)a \overset{vu \in \mathbb{Z}}{\implies} a \mid c$ □

6. $\forall a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b\ \wedge\ a \mid c \implies a \mid (b \pm c)$

   Доказателство. Нека $a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b\ \wedge\ a \mid c$

   $\implies \exists u,\ v \in \mathbb{Z}\ :\ b = ua\ \wedge c = va$

   $\implies b \pm c = ua \pm va = (u \pm v)a = (vu)a \overset{u \pm v \in \mathbb{Z}}{\implies} a \mid (b \pm c)$ □

7. $\forall a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b \implies a \mid cb$

   Доказателство. Нека $a,\ b,\ c \in \mathbb{Z}\ :\ a \mid b \implies \exists z \in \mathbb{Z}\ :\ b = za$

   $\implies cb = cza = (cz)a \overset{cz \in \mathbb{Z}}{\implies} a \mid cb$ □

8. $\forall a \in \mathbb{Z},\ n \in \mathbb{N}^+,\ b_1,\ \ldots,\ b_n \in \mathbb{Z},\ c_1,\ \ldots,\ c_n \in \mathbb{Z}\ :\ a \mid b_1,\ \ldots,\ a \mid b_n$

   $$\implies a \,\Big|\, \left(\sum_{i=1}^{n} c_i b_i\right)$$

   Доказателство. Нека $a \in \mathbb{Z},\ n \in \mathbb{N}^+,\ b_1,\ \ldots,\ b_n \in \mathbb{Z},\ c_1,\ \ldots,\ c_n \in \mathbb{Z}\ :$ $a \mid b_1,\ \ldots,\ a \mid b_n \implies \exists z_1,\ \ldots,\ z_n \in \mathbb{Z}\ :\ \forall i \in \{1,\ \ldots,\ n\}\ b_i = z_i a$

   $$\implies \sum_{k=1}^{n} c_k b_k = \sum_{k=1}^{n} c_k (z_k a) = \sum_{k=1}^{n} (c_k z_k) a = \left(\sum_{k=1}^{n} c_k z_k\right) a$$
   $$\implies a \,\Big|\, \left(\sum_{k=1}^{n} c_k b_k\right)\ (\forall i \in \{1,\ \ldots,\ n\}\ c_i z_i \in \mathbb{Z}) \qquad \square$$

9. $\forall a,\ b,\ c \in \mathbb{Z}\ :\ a \mid (b + c)\ \land\ a \mid b \implies a \mid c$

   Доказателство. Нека $a,\ b,\ c \in \mathbb{Z}\ :\ a \mid (b + c)\ \land a \mid b$

   $$\implies \exists u,\ v \in \mathbb{Z}\ :\ b + c = ua\ \land b = va$$

   $$\implies c = ua - b = ua - va = (u - v)a \stackrel{u-v \in \mathbb{Z}}{\implies} a \mid c \qquad \square$$

1.2 Теорема за деление с частно и остатък

Теорема 1. (Теорема за деление с частно и остатък)
$\forall a,\ b \in \mathbb{Z}\ :\ a \neq 0\ \exists!\ q,\ r \in \mathbb{Z}\ :\ b = qa + r\ \land\ 0 \leq r < |a|$

Доказателство. (*Единственост*)
Нека $a,\ b \in \mathbb{Z}\ :\ a \neq 0$ и нека

$$q_1,\ r_1 \in \mathbb{Z}\ :\ b = q_1 a + r_1\ \land\ 0 \leq r_1 < |a|$$

$$q_2,\ r_2 \in \mathbb{Z}\ :\ b = q_2 a + r_2\ \land\ 0 \leq r_2 < |a|$$

Тогава

$$0 = b - b = q_1 a + r_1 - (q_2 a + r_2) = (q_1 - q_2)a + (r_1 - r_2)$$

$$\implies r_2 - r_1 = (q_1 - q_2)a \iff r_2 - r_1 = 0 \iff q_1 - q_2 = 0$$

$$\iff r_2 = r_2\ \land\ q_1 = q_2$$

$\square$

Доказателство. (*Съществуване*)
Ще разгледаме четирите възможни случаи в зависимост от знаците на двете числа.

1. $a > 0\ \land\ b \geq 0$

   Ако $b < a$, то полагаме $q = 0$ и $r = b$.

   В противен случай нека $q \in \mathbb{N}$ е най-голямото със свойството:
   $qa \leq b < (q + 1)a$. Тогава

$0 = qa - qa \leq b - qa < (q+1)a - qa = a = |a|$
следователно полагаме $r = b - qa$.

2. $a > 0 \;\wedge\; b < 0$
Нека $t \in \mathbb{N}$ е най-голямото със свойството:
$ta < |b| \leq (t+1)a$. Тогава нека положим $q = -(t+1)$
Тогава

$$-(q+1)a < |b| \leq -qa \;|\; -1 \implies$$

$$(q+1)a > b \geq qa \;|\; -qa \implies$$

$$a > b - qa \geq 0 \implies 0 \leq b - qa < |a|$$

Полагаме $r = b - qa$

3. $a < 0 \;\wedge\; b \geq 0$

Ако $b < |a|$, то полагаме $q = 0$ и $r = b$.

В противен случай нека $t \in \mathbb{N}$ е най-голямото със свойството:
$t|a| \leq b < (t+1)|a|$. Тогава полагаме $q = -t$ и $qa = -ta = t|a|$
$0 = t|a| - t|a| \leq b - t|a| < (t+1)|a| - t|a| = |a|$
следователно полагаме $r = b - t|a| = b - qa$.

4. $a < 0 \;\wedge\; b < 0$
Нека $t \in \mathbb{N}$ е най-голямото със свойството:
$t|a| < |b| \leq (t+1)|a|$. Тогава нека положим $q = t+1$
Тогава

$$t|a| < |b| \leq (t+1)|a| \;|\; -1 \implies$$

$$(q-1)a > b \geq qa \;|\; +qa \implies$$

$$-a > b - qa \geq 0 \implies 0 \leq b - qa < |a|$$

Полагаме $r = b - qa$

□

1.3 Следствия

Следствие 1. $\forall a,\ b \in \mathbb{Z} \;:\; a \neq 0 \quad a \mid b \iff \exists!\, q \in \mathbb{Z} \;:\; b = qa + 0$

Следствие 2. Нека $n \in \mathbb{N}^+$. Тогава от всеки n последователни числа точно едно се дели на n.

Доказателство. Нека $n \in \mathbb{N}^+$ и нека $z \in Z$ е произволно число. Нека $\forall i \in \{0,\ \ldots,\ n-1\}\ a_i = z + i$. Прилагаме теоремата за деление с частно и остатък за z и получаваме $\exists!\, q,\ r \in \mathbb{Z} \;:\; z = qn + r \;\wedge\; 0 \leq r < n$. Ако $r = 0$ то тогава $a_0 = z + 0 = z = qn \implies n \mid a_0$. Ако $r \neq 0 \implies r > 0 \implies$
$\forall i \in \{0,\ \ldots,\ n-1\}\ a_i = qn + r + i \implies$
$a_{n-r} = qn + r + (n-r) = qn + n = (q+1)n \implies n \mid a_{n-r}$
Следователно $\exists k \in \{0,\ \ldots,\ n-1\} \;:\; n \mid a_k$ □

Следствие 3. Нека $n \in \mathbb{N}^+$. Тогава
$\forall a_1,\ \dots,\ a_{n+1} \in \mathbb{Z}\ \exists i \neq j \in \{1,\ \dots,\ n+1\}\ :\ n \mid (a_i - a_j)$

Доказателство. Нека $n \in \mathbb{N}^+,\ a_1,\ \dots,\ a_{n+1} \in \mathbb{Z}$. Прилагаме теоремата за деление с частно и остатък и получаваме
$\forall k \in \{1,\ \dots,\ n+1\}\ \exists!\ q_k,\ r_k \in \mathbb{Z}\ :\ a_k = q_k n + r_k\ \wedge\ 0 \leq r_k < n$. Нека да дефинираме функцията $\forall k \in \{1,\ \dots,\ n+1\}\ f(k) = r_k$, тоест
$f = \{(k,\ r_k) \mid k \in \{1,\ \dots,\ n+1\}\}$. Очевидно домейнът на f е множеството $\{1,\ \dots,\ n+1\}$, а нейният ко-домейн е множеството $\{0,\ \dots,\ n-1\}$. Очевидно домейнът има един елемент повече от ко-домейна, тогава f не е инекция следователно $\exists i \neq j \in \{1,\ \dots,\ n+1\}\ :\ f(i) = f(j) \implies$
$a_i - a_j = q_i n + r_i - (q_j n + r_j) = (q_i - q_j)n + (r_i - r_j) = (q_i - q_j)n + 0 \implies n \mid (a_i - a_j)$ □

1.4 Теорема за запис в p-ична бройна система

Теорема 2. Нека $p \geq 2$ е фиксирано естествено число. Тогава
$\forall z \in \mathbb{Z}\ \exists!\ n,\ c_0,\ \dots,\ c_n \in \mathbb{N}\ :\ z = \sum_{k=0}^{n} c_k p^k\ \wedge\ \forall i \in \{0,\ \dots,\ n\}\ 0 \leq c_i < p \wedge c_n > 0$

Доказателство. (*Съществуване*) Нека $z \in \mathbb{Z}$ е произволно.

Ако $z < p$, то $n = 0$ и $c_0 = z$.

Ако $z \geq p$ прилагаме теоремата за деление с частно и остатък и получаваме $z = q_1 p + c_0\ \wedge\ 0 \leq c_0 < p$ и освен това $z > q_1$. Ако $q_1 < p$, то полагаме $c_1 = q_1$ и получаваме представянето $z = c_1 p + c_0$. Ако пък $q_1 \geq p$ прилагаме теоремата за деление с частно и остатък за q_1 и p и получаваме $q_1 = q_2 p + c_1\ \wedge\ 0 \leq c_1 < p$ и $q_1 > q_2$, $z = q_2 p^2 + c_1 p + c_0$. Ако $q_2 < p$, полагаме $c_2 = q_2$ и получаваме търсеното представяне. Ако $q_2 \geq p$ продължаваме да прилагаме теоремата за деление с частно и остатък. Тъй като на всяка стъпка получаваме $z > q_1 > q_2 > \dots$ и тези числа са естествени, то този процес ще спре и за някое $n \in \mathbb{N}$ ще получим $q_{n-1} = q_n p + c_{n-1} \wedge 0 \leq c_{n-1} < p \wedge q_n < p$. Тогава полагаме $c_n = q_n$ и получаваме търсеното представяне $z = \sum_{k=0}^{n} c_k p^k$. □

Доказателство. (*Единственост*) Нека $z \in \mathbb{Z}$ е произволно.
Допускаме, че $z = \sum_{k=0}^{n} c_k p^k = \sum_{j=0}^{m} b_j p^j$, където
$\forall i \in \{0,\ \dots,\ n\}\ 0 \leq c_i < p\ \wedge\ c_n > 0$ и $\forall j \in \{0,\ \dots,\ m\}\ 0 \leq b_j < p\ \wedge\ b_m > 0$.
Следователно $0 \leq c_0 - b_0 < |p|$ От равенствата следва

$$0 = z - z = \sum_{k=0}^{n} c_k p^k - \sum_{j=0}^{m} b_j p^j = \left(\sum_{k=1}^{n} c_k p^{k-1} - \sum_{j=0}^{m} b_j p^{j-1} \right) p + (c_0 - b_0)$$

$$p \mid 0\ \wedge\ p \left| \left(\sum_{k=1}^{n} c_k p^{k-1} - \sum_{j=0}^{m} b_j p^{j-1} \right) \right. \implies p \mid (c_0 - b_0) \iff c_0 = b_0$$

Следователно $\frac{z - c_0}{p} = \sum_{k=1}^{n} c_k p^{k-1} = \sum_{j=1}^{m} b_j p^{j-1} = \frac{z - b_0}{p}$. Повтаряме горните стъпки и така получаваме, че $m = n$ и $\forall i \in \{0,\ \dots,\ n\}\ b_i = c_i$ □
С това теоремата е доказана. Записът от теоремата на числото a, се нарича *запис на a в p-ична бройна система* или *p-ичен запис на числото a*. Числото

p се нарича основа на бройната система, а числата $c_0, \ldots, c_n$ - *p-ични цифри в записа на числото a*. Така при фиксирано p всяко число се записва с краен брой символи. При $p = 10$ това са символите $\{-, 0, \ldots, 9\}$, при $p = 2$ символите са $\{-, 0, 1\}$.

1.5 Задачи