# Елементи от теория на числата
# част 1

доц. Евгения Великова

Февруари 2021

# Аксиоми на Пеано

*„Бог е създал целите числа, всичко останало е дело на човека"*

*Леополд Кронекер*

## аксиоми на Пеано

$\mathbb{N} \neq \emptyset$ и $\sigma : \mathbb{N} \Rightarrow \mathbb{N}$

1. $\sigma(a) \in \mathbb{N}, \forall a \in \mathbb{N}$
2. $1 \neq \sigma(x), \forall\, x \in \mathbb{N}$
3. метод на математическата индукция- ако за $M \subseteq \mathbb{N}$, е изпълнено
   - $1 \in M$
   - ако $a \in M$,следователно $\sigma(a) \in M$

   тогава $M = \mathbb{N}$

$$a + 1 = \sigma(a), \quad a + \sigma(b) = \sigma(a + b) \qquad a.1 = a, \quad a.(b + 1) = a.b + a$$

$$a + b = \underbrace{\sigma(\ldots(\sigma}_{b}(a))) \qquad a.b = \underbrace{a + \ldots + a}_{b}$$

# Цели числа

Числото нула (0) - неутрално относно събирането

$$a + 0 = a, \quad \text{за произволно число } a, \quad a.0 = 0$$

Отрицателните цели числа - за всяко естествено число има отрицателно цяло число, чиято сума е равна на нула.

$$\mathbb{N}^- = \{-a | a \in \mathbb{N}\}, \quad \text{където } -a + a = a + (-a) = 0 \Rightarrow -(-a) = a.$$

Множеството на целите числа се състои от естествените числа, заедно с нулата както и заедно с отрицателните цели числа

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{N}^-$$

Действията събиране и умножение се продължават до действия в множеството на целите числа.

# основни свойства на събирането и умножението

## Свойства на "+"и на "."

1. $a + b = b + a, \quad \forall a, b \in \mathbb{Z}$ - комутативност на събирането;
2. $a + (b + c) = (a + b) + c, \quad \forall a, b, c \in \mathbb{Z}$ - асоциативност на събирането;
3. $a + 0 = a, \quad \forall a \in \mathbb{Z}$ - неутрален елемент относно събирането;
4. $a + (-a) = 0, \forall a \in \mathbb{Z}$
5. $a.b = b.a, \quad \forall a, b \in \mathbb{Z}$ - комутативност на умножението;
6. $a.(b.c) = (a.b).c, \quad \forall a, b, c \in \mathbb{Z}$ - асоциативност на умножението;
7. $a.(b + c) = a.c + b.c, \quad \forall a, b, c \in \mathbb{Z}$ - дистрибутивност;
8. $1.a = a, \forall a \in \mathbb{Z}$ - единицата е неутрален елемент относно умножението.

Изваждането е обратно действие на събирането
$a - b$ е това число $x$, което изпълнява уравнението $b + x = a$.
$a - b = a + (-b)$

# "$>$"и "$<$"при целите числа

$\mathbb{Z}$ е наредено множество

$$a, b \in \mathbb{Z} \Rightarrow \left| \begin{array}{l} \textit{изпълнено е} \\ \textit{точно едно} \\ \textit{от трите} \end{array} \right| \left\{ \begin{array}{l} a < b \\ a = b \\ a > b \end{array} \right. .$$

## Свойства

1. Ако е изпълнено $a < b$ и $b < c$, следователно $a < c$ ;
2. Ако $a < b$, следователно $a + c < b + c$;
3. Ако $a_1 < b_1$ и $a_2 < b_2$, следователно $a_1 + a_2 < b_1 + b_2$;
4. Ако $a < b$ и $c > 0$, следователно $a.c < b.c$;
5. Ако $a < b$ и $c < 0 \Rightarrow \ a.c > b.c$;
6. ако $a \geq 1, \ b \geq 1$, следователно $a \leq ab$ и $b \leq ab$

$$|a| = \begin{cases} a, & \text{когато } a \geq 0 \\ -a, & \text{когато } a < 0 \end{cases}$$

# минимален (максимален) елемент при подмн-ва на $\mathbb{Z}$

## Ограничени отгоре множества

За подмножествата $M \subset \mathbb{Z}$ от цели числа, които са ограничени отгоре е изпълнено, че съдържат максимален елемент, т.е.

$$\left.\begin{array}{r} M \subset \mathbb{Z}, \quad \text{такова че} \\ \exists\ t : x < t, \forall x \in M \end{array}\right\} \Rightarrow \quad \exists\ a \in M, \text{за което} \quad x \leq a, \forall x \in M$$

$$(M - \quad \textit{ограничено отгоре}) \qquad\qquad (a - \quad \textit{максимален елемент})$$

## Ограничени отдолу множества

Ограничените отдолу множества имат минимален елемент

$$\left.\begin{array}{r} T \subset \mathbb{Z}, \quad \text{такова че} \\ \exists\ u : u < x, \forall x \in T \end{array}\right\} \Rightarrow \quad \exists\ b \in T, \text{за което} \quad b \leq x, \forall x \in T$$

$$(T - \quad \textit{ограничено отдолу}) \qquad\qquad (b - \quad \textit{минимален елемент})$$

## Теорема

Нека $a, b \in \mathbb{Z}$ и $b \neq 0$. Съществуват единствени $q, r \in \mathbb{Z}$, за които

$$a = b.q + r, \quad \text{където} \quad 0 \leq r < |b|.$$

$q$ - частно, а $r$ - остнатък при разделяне $a$ на $b$.

*Доказателство:*

$\boxed{\exists}$ Разглеждаме следното множество $M = \{a + b.t \mid t \in \mathbb{Z}\}$ и подмножеството му $M^{(\geq 0)} = \{c = a + bt \in M \mid t \in \mathbb{Z} \;\text{ и }\; c \geq 0\}$

$M^{(\geq 0)}$ е ограничено отдолу

минимален елемент на $M^{(\geq 0)}$ е $r \in M^{(\geq 0)}$ и нека $r = a + bt_0 \geq 0$.

Допускаме че $r \geq |b|$. От него вадим $|b|$ и получаваме $r_1 < r$, $r_1 \in M$

$$r_1 = r - |b| = a + bt_0 \pm b \in M, \quad \text{и } r_1 \geq 0 \;\Rightarrow r_1 \in M^{(\geq 0)}$$

Получихме противоречие с избора на $r$, следователно $0 \leq r < |b|$.

$$r = a + bt_0 \;\Rightarrow\; a = b(-t_0) + r, \;\; 0 \leq r < |b|.$$

$\boxed{!}$ Нека да са изпълнени две равенства:

$$\left.\begin{array}{lll} a = bq_1 + r_1, & \text{и} & 0 \le r_1 < |b| \\ a = bq_2 + r_2, & \text{и} & 0 \le r_2 < |b| \end{array}\right\} \Rightarrow |r_1 - r_2| < |b|$$

Изваждаме и получаваме

$$0 = b(q_1 - q_2) + (r_1 - r_2) \quad \Rightarrow |r_1 - r_2| = |b|.|q_1 - q_2|$$

Допускаме, че $|q_1 - q_2| \neq 0$,

$$|r_1 - r_2| = |b|.|(q_1 - q_2)| \ge |b|$$

от една страна $|r_1 - r_2| < |b|$, а от друга $|r_1 - r_2| \ge |b| \Rightarrow$ противоречие
Получихме $q_1 - q_2 = 0$ и $r_1 - r_2 = 0$, следователно $q_1 = q_2$ и $r_1 = r_2$
Частното и остатъка при разделяне $a$ на $b$ са единствени.

## Следствие

Нека $a, b \in \mathbb{N}$ и $b > 1$. Съществуват единствени $a_0, \ldots, a_k$, за които
$a = a_0 + a_1 b + \ldots + a_k b^k$, където $0 \le a_i < b, \forall i$ и $a_k \neq 0$
$a = \overline{a_k a_{k-1} \ldots a_0}_{\ (b)}$ - е в позиционна бройна система с основа $b$

*Доказателство:* Получаваме търсеното представяне постъпково:

Начална стъпка: $a = b.q_0 + a_0$

- Ако $q_0 = 0 \Rightarrow$ получили сме представянето $a = \overline{a_0}_{\ (b)}$.
- Ако $q_0 > 0$ имаме $a = b.q_0 + a_0 \rightarrow$ стъпка 1.

Стъпка $s$: Имаме $a = b^s q_{s-1} + b^{s-1} a_{s-1} + \ldots + b^0 a_0$

Пресмятаме $q_{s-1} = b.q_s + a_s$ и получаваме $a_s$, където $0 \le a_s < b$,
$a = b^s(b.q_s + a_s) + b^{s-1} a_{s-1} + \ldots + b^0 a_0 = b^{s+1} q_s + b^s a_s + b^{s-1} a_{s-1} + \ldots + b^0 a_0$

- Ако $q_s = 0 \Rightarrow a_s \neq 0$ и сме получили $a = \overline{a_s a_{s-1} \ldots a_0}_{\ (b)}$.
- Ако $q_s > 0 \rightarrow$ стъпка с номер $s + 1$.

Винаги е изпълнено $0 \le q_s < q_{s-1}$ и има краен брой стъпки
$a = b^k a_k + b^{k-1} a_{k-a} + \ldots + b a_1 + a_0 = \overline{a_k a_{k-1} \ldots a_0}_{\ (b)}$

# Пример

Да се представи 2657 в бройни системи с основи 8 и 7.

- $2657 = 332.8 + 1$, получаваме че $a_0 = 1$;
- $332 = 41.8 + 4$, получаваме че $a_1 = 4$;
- $41 = 5.8 + 1$, получаваме че $a_2 = 1$;
- $5 = 0.8 + 5$, получаваме че $a_3 = 5$

$$2657 = 5.8^3 + 1.8^2 + 4.8 + 1 = \overline{5141}_{(8)}$$

- $2657 = 379.7 + 4 \;\Rightarrow\; r_0 = 4$;
- $379 = 54.7 + 1 \;\Rightarrow\; r_1 = 1$;
- $54 = 7.7 + 5 \;\Rightarrow\; r_2 = 5$;
- $7 = 1.7 + 0 \;\Rightarrow\; r_3 = 0$;
- $1 = 0.7 + 1 \;\Rightarrow\; r_4 = 1$;

$$2657 = \overline{10514}_{(7)} = 1.7^4 + 5.7^2 + 1.7 + 4.$$

## Определение

Нека $a, b$ са цели числа и $b \neq 0$. Казваме, че $b$ дели $a$, когато съществува цяло число $q \in \mathbb{Z}$, такова че $a = bq$. Когато $b$ дели $a$ записваме $b \mid a$.

$b$ дели $a$ точно когато се получава остатък нула при разделяне $a$ на $b$ с частно и остатък.

- ***Забележка***: *Друг начин за отбелязване на b дели a, е* $a \vdots b$ *и се изговаря като "a се дели на b".*
- ***Забележка***: *Ако числото b не дели числото a, това ще го отбелязваме по следния начин* $b \nmid a$

# Свойства на делимостта

1. $\pm 1 \mid a, \ \forall a \in \mathbb{Z}$;
2. $b \mid 0, \ \forall b \in \mathbb{Z}$;
3. ако $b \mid a \ \Rightarrow -b \mid a$;
4. ако $b \mid a$ и $a \mid c \ \Rightarrow b \mid c$;
5. ако $b \mid a$ и $a \mid b \ \Rightarrow a = \pm b$;
6. $b \mid a \ \Rightarrow \ b \mid (a + kb), \ k \in \mathbb{Z}$
7. ако $b \mid a \ \Rightarrow \ b \mid ka$, където $k \in \mathbb{Z}$;
8. ако $b \mid a_1$ и $b \mid a_2 \ \Rightarrow \ b \mid (k_1 a_1 + k_2 a_2)$, където $k_1, k_2 \in \mathbb{Z}$;
9. ако $b \mid a$ и $a \neq 0 \ \Rightarrow |b| \leq |a|$;

**св-во 5:** Ако $b \mid a \ \rightarrow \ a = bq$ и от $a \mid b \ \rightarrow b = a.u$. Получаваме, че $b = a.u = bqu \Rightarrow qu = 1, \Rightarrow q = \pm 1$ и $a = \pm b$.

**св-во 8:** Ако $b \mid a_1$ и $b \mid a_2 \ \Rightarrow$

$$\left.\begin{aligned} a_1 &= q_1 b \\ a_2 &= q_2 b \end{aligned}\right\} \Rightarrow k_1 a_1 + k_2 a_2 = (q_1 a_1 + q_2 a_2) b \ \Rightarrow \ b \mid (k_1 a_1 + k_2 a_2).$$

# Пример

### признак за делене на седем

*"Числото $n$ се дели на 7 тогава и само тогава, когато числото $t$ се дели на 7, като $t$ се получава по следния начин - от числото $n$ премахнем последната цифра и от полученото извадим премахнатата последна цифра умножена по 2."*

$$7|(10x + y) \Leftrightarrow 7|(x - 2y)$$

$$\begin{aligned} \text{Ако} \quad 7|(10x+y) \quad &\Rightarrow \quad 7|(3x+y) \Rightarrow \\ &\Rightarrow \quad 7|5(3x+y) \ \text{ т.е. } \ 7|(x+14x+7y-2y) \Rightarrow \\ &\Rightarrow \quad 7|(x-2y) \end{aligned}$$

Аналогично може да се получи:

$$\begin{aligned} \text{Ако} \quad 7|(x-2y) \quad &\Rightarrow \quad 7|3(x-2y) \Rightarrow \\ &\Rightarrow \quad 7|(3x-6y+7(x+y)) \Rightarrow \\ &\Rightarrow \quad 7|(10x+y) \end{aligned}$$