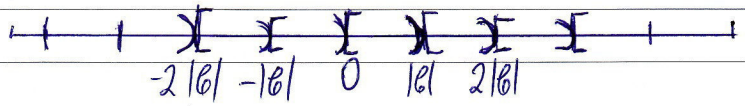
ЗА	Каспарян	24.02.13

Деление на цели числа с частно и остатък - Най-голям общ делител, най-малко общо кратно. Основна теорема на аритметиката

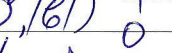
Т за деление с частно и остатък
За произволни цели числа a и b $(\forall a, b \in \mathbb{Z}\ b \neq 0)$ съществуват еднозначно определени $q, r \in \mathbb{Z}$ т.че $a = bq + r$ и $0 \leq r \leq |b|$
Казваме че q е частното, а r - остатъкът при деление на a със b

Док:



Разглеждаме покритието $\mathbb{R} = \bigcup [z|b|, z|b| + |b|)$ с непресичащи се $z \in \mathbb{Z}$ интервали. Числото $a \in \mathbb{Z} \subset \mathbb{R}$ попада в един от тези интервали т.е. съществува $z \in \mathbb{Z}$, $z|b| \leq a \leq z|b| + |b|$
Нека $\text{sign}(b) = \begin{cases} 1 & \text{за } b > 0 \\ -1 & \text{за } b < 0 \end{cases}$. Тогава $|b| = \text{sign}(b) \cdot b$ и ако $q = z\,\text{sign}(b) \in \mathbb{Z}$ то $qb \leq zqb + |b|$. Оттук $0 \leq r := a - qb \leq |b|$, $r \in \mathbb{Z}$

Единственост
Ако $a = bq + r = bq' + r'$ за $q, q', r, r' \in \mathbb{Z}$, $0 \leq r, r' \leq |b|$ то $b(q - q') = r' - r$. Допускането $q \neq q'$ води до $|r' - r| = |b||q - q'| \geq |b|$ защото $|q - q'| \geq 1$ и $|b| > 0$. Това противоречи на $r, r' \in [0, |b|)$ $|r - r'| < |b|$ и доказва $q = q'$, $r' = r$



Определение за делене на цели числа

Цялото число $b \neq 0$ дели цялото число $a \in \mathbb{Z}$ ако съществува $c \in \mathbb{Z}$ със $bc = a$

Свойства на делимостта

1) Рефлексивност
$\forall a \in \mathbb{Z}$ дели себе си
Ако в дели а тогава в/а
2) Антисиметричност
Ако а дели в и в дели а за $a, b \in \mathbb{Z} \setminus \{0\}$ то $b = \pm a$
Док:
По определение съществуват цели числа $c_1, c_2 \in \mathbb{Z}$ т.че $b = ac_1$ и $a = bc_2 \Rightarrow b = (bc_2)c_1 = b(c_1c_2)$ и след почленно делене с $b \neq 0$ имаме $c_1c_2 = 1$. Това е в сила само $c_1 = c_2 = \pm 1$
3) Транзитивност
Ако $a, b, c \in \mathbb{Z}$ $a \neq 0$, $b \neq 0$, a/b, b/c то a/c
Док:
По определение съществуват $q_1, q_2 \in \mathbb{Z}$ със $b = aq_1$ и $c = bq_2$. Следователно $c = (aq_1)q_2 = a(q_1q_2)$ със $q_1q_2 \in \mathbb{Z}$ и a/c
Релацията в множеството $\mathbb{Z}$ е подмножество на $\mathbb{Z} * \mathbb{Z}$
Делимостта на цели числа е релация
Ако една релация е рефлексивна, антисиметрична и транзитивна, казваме че тя е частична наредба
Делимостта на цели числа е частична наредба
Релация на еквивалентност е рефлексивна, симетрична и транзитивна релация. Релациите на еквивалентност разбиват съответните множества в непресичащи се класове на еквивалентност т.е. $Ca = \{x \in X / a \sim x\}$
Ако съществува $x \in Ca \cap Cb$ то $x \sim a$, $x \sim b \Rightarrow a \sim b$ и за $\forall y \in Cb$, $y \sim b$ води до $y \sim a$ и $y \in Ca$. Оттук $Cb \subseteq Ca$. Аналогично $Ca \subseteq Cb$ и $Ca = Cb$
Деф:
Ако $a_1 - a_n$ са едновременно нулеви цели числа, то най-голямият общ делител (НОД) d се бележи $d = (a_1 .. a_n)$ е (i) общ делител (ОД) и (ii) всеки общ делител d_1 на $a_1 - a_n$ дели d
Ако съществува, НОД на $a_1 - a_n$ е единствен със точност до знак. По-точно ако d и δ са НОД-ли

на $a_1 \dots a_n$ то d/δ защото δ е НОД а d е общ делител на $a_1 \dots a_n$

обратно

δ делим d понеже d е НОД а δ е общ делител на $a_1 \dots a_n$. От d/δ и $\delta/d \Rightarrow \delta = \pm d$ по Св. 2

Деф

Ако НОД d на група ненулеви числа $a_1 \dots a_n$ е равен на ± 1, казваме че $a_1 \dots a_n$ са взаимно прости $d = (a_1 \dots a_n) = \pm 1$

Лема

Ако $a_1 \dots a_n \in \mathbb{Z}$ са едновременно нулеви и $d = (a_1 \dots a_n)$ (НОД), то $\frac{a_1}{d}, \frac{a_2}{d} \dots \frac{a_n}{d} \in \mathbb{Z}$ са взаимно прости

Док:

Достатъчно е да проверим че общите делители на $\frac{a_1}{d} \dots \frac{a_n}{d}$ са $c = \pm 1$. Наистина ако $c/\frac{a_i}{d}$ за $\forall 1 \le i \le n$ то съществуват числа $q_i \in \mathbb{Z}$ т.ч. $cq_i = \frac{a_i}{d}$. Оттук $(cd)q_i = a_i$ и cd е ОД на $a_1 \dots a_n$. Следователно cd/d защото d е НОД на $a_1 \dots a_n$. Но съгласно $c \in \mathbb{Z}$, което $d \in \mathbb{Z}$ дели cd, от където $cd = \pm d$. След последно деление с $d \neq 0$ имаме $c = \pm 1$

Деф НОК

Ако $a_1 \dots a_n \in \mathbb{Z} \setminus \{0\}$ то НОК $m = [a_1 \dots a_n]$ на $a_1 \dots a_n$ е такова общо кратно което дели $\forall$ ОК на $a_1 \dots a_n$

Ако m и μ са НОК-ни на $a_1 \dots a_n$, то m/μ, защото m е НОК а μ е общо кратно на $a_1 \dots a_n$

Аналогично μ/m и $\mu = \pm m$

Лема (i) !

Ако $a_1 \dots a_n \in \mathbb{Z}$ са едновременно нулеви, то НОД на $(a_1 \dots a_{n-1}, a_n) = \pm((a_1 \dots a_{n-1}), a_n)$

(ii)

Ако $a_1 \dots a_n \in \mathbb{Z} \setminus \{0\}$ то НОК $[a_1 \dots a_{n-1}, a_n] = \pm[[a_1 \dots a_{n-1}], a_n]$

Док (i)

Означаваме $d := (a_1 \dots a_n)$, $d_1 := (a_1 \dots a_{n-1})$, $\delta := (d_1, a_n)$ и доказваме че $\delta = \pm d$. От една страна, d/a_n и d/a_i за $\forall 1 \le i \le n-1$, от където d е ОД на $a_1 \dots a_{n-1}$

и $d/d_1 = (a_1 \dots a_{n-1})$. Следователно d е ОД на d_1 и a_n
т.е. $d/\delta = (a_1 \dots a_n)$. От друга страна δ/a_n. От
δ/d_1 и d_1/a_i за $\forall 1 \le i \le n-1 \Rightarrow \delta/a_i$ за $\forall 1 \le i \le n-1$
Следователно δ е ОД на $a_1 \dots a_{n-1}, a_n$ и δ/d. От
d/δ и δ/d получаваме че $\delta = \pm d$

(ii)

Ако $m = [a_1 \dots a_n]$, $m_1 = [a_1 \dots a_{n-1}]$ и $\mu = [m_1, a_n]$, то
тогава че $\mu = \pm m$

Заб.

Предишната лема свежда намирането на НОД или НОК на n числа към намирането на НОД или НОК на две числа

Например:

$(a_1 \dots a_4) = \pm((a_1 \dots a_3), a_4) = \pm(((a_1, a_2), a_3) a_4)$

Алгоритъм на Евклид за намирането на НОД на 2 числа $a, b \in \mathbb{Z}$ $b \neq 0$

(при $a \neq 0, b \neq 0$ нека $|b| \le |a|$)

делим последното с частно и остатък

$$a = bq_1 + r_1, \quad 0 < r_1 < |b|$$
$$b = r_1 q_2 + r_2 \quad 0 < r_2 < |r_1|$$
$$r_1 = r_2 q_3 + r_3 \quad 0 < r_3 < |r_2|$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n \quad 0 < r_n < |r_{n-1}|$$
$$r_{n-1} = r_n q_{n+1}$$

r_n е общ делител на a и b защото $\dagger\ r_n/r_{n-1} \Rightarrow$
$r_n/r_{n-2} \Rightarrow \dots \Rightarrow r_n/b \Rightarrow r_n/a$

$\dagger \forall$ ОД d_1 на a и b дели r_n, защото $d_1/r_1 \Rightarrow d/r_2 \Rightarrow \dots \Rightarrow d/r_n$

III

Това доказва че $(a,b) = \pm$ на НОД

$r_n \in \mathbb{Z}a + \mathbb{Z}b$ защото $r_n \in \mathbb{Z}r_{n-1} + \mathbb{Z}r_{n-2} \Rightarrow$
$r_n \in \mathbb{Z}r_{n-2} + \mathbb{Z}r_{n-3} \Rightarrow \ldots \Rightarrow r_n \in \mathbb{Z}r_1 + \mathbb{Z}r_2 \Rightarrow$
$r_n \in \mathbb{Z}r_1 + \mathbb{Z}b \Rightarrow r_n \in \mathbb{Z}a + \mathbb{Z}b$

Следствие от Алгоритъма на Евклид за намиране на НОД на (a,b) е следното твърдение на Безу

За произволни неедновременно нулеви $a,b \in \mathbb{Z}$ съществуват $u,v \in \mathbb{Z}$ т.че НОД$(a,b) = au + bv$

Следствие 1 от Твърдение на Безу
Ако $a, b_1, b_2 \in \mathbb{Z}$ $a \neq 0$, $(a,b_1) = \pm 1$ и $a \mid b_1 b_2$, то $a \mid b_2$

Док:
Умножаваме почленно твърдението на Безу
$1 = au + b_1 v$ със $u,v \in \mathbb{Z}$ за a и b_1 с b_2 и получаваме $b_2 = ab_2u + b_1b_2v$. От $a \mid ab_2u$ и $a \mid b_1b_2v \Rightarrow a \mid b_2$

Следствие 2 от Твърдението на Безу
Ако $a_1, a_2, b \in \mathbb{Z}$, $a_1 \neq 0$, $a_2 \neq 0$, $(a_1,a_2) = \pm 1$, $a_1 \mid b$, $a_2 \mid b$ то $a_1a_2 \mid b$

Док:
По определение от $a_1 \mid b$ следва съществуването на $c \in \mathbb{Z}$ с $a_1c = b$ - Сега $a_2 \mid a_1c$ и $(a_1,a_2) = 1$ дава $a_2 \mid c$ по следствие 1 от Твърдението на Безу. По-точно съществува $s \in \mathbb{Z}$, т.че $a_2s = c$ откъдето $b = a_1c = a_1(a_2s) = (a_1a_2)s$ със $s \in \mathbb{Z}$ и $a_1a_2 \mid b$

Лема
Ако $a,b \in \mathbb{Z} \setminus \{0\}$ то $[a,b](a,b) = \pm ab$

Док
Да означим $d := (a,b)$, $m := [a,b]$ и да докажем че $dm = \pm ab$. От една страна $\frac{ab}{m} \in \mathbb{Z}$ и $\frac{ab}{m} \mid d$
По-точно ab е общо кратно на a и b откъдето $m \mid ab$ и $\frac{ab}{m} \in \mathbb{Z}$. От $a = \left(\frac{ab}{m}\right)\left(\frac{m}{b}\right)$ с $\frac{m}{b} \in \mathbb{Z}$ и от $b = \left(\frac{ab}{m}\right)\left(\frac{m}{a}\right)$ с $\frac{m}{a} \in \mathbb{Z} \Rightarrow \frac{ab}{m}$ е ОД на a и b, така че $\frac{ab}{m} \mid d$. следователно съществува $c \in \mathbb{Z}$ с $\frac{ab}{m}c = d$
От друга страна $\frac{ab}{d} \in \mathbb{Z}$ и $m \mid \frac{ab}{d}$ така че съществува $s \in \mathbb{Z}$ със $sm = \frac{ab}{d}$. Накрая

iii

$\frac{ab}{d} = \left(\frac{a}{d}\right)b = \frac{ab}{d} = b\left(\frac{a}{d}\right)$ с цели $\frac{b}{d}$ и $\frac{a}{d}$ са вида $\frac{ab}{d}$ е ОК на a и b. Следователно $m = [a,b]/\frac{ab}{d}$. От $\frac{ab}{m}e = d$ и $ms = \frac{ab}{d}$ чрез умножаване $\frac{dm}{e} = ab = dms$. Следователно $dm\left(s - \frac{1}{e}\right) = 0$ и $(d \neq 0, m \neq 0)$ и $s = \frac{1}{e}$. Целите числа e и s със $se = 1$ са $s = e = \pm 1$ т. е.

$$ab = dms = \pm dm$$