Естествени числа

Дефиниция:
Дефинираме множеството от естествените числа $\mathbb{N}$ по следния начин:

1. $1 \in \mathbb{N}$ - т.е 1 е естествено число;
2. $k \in \mathbb{N} \Rightarrow k+1 \in \mathbb{N}$ - т.е ако k е естествено число, то и $k+1$ е естествено число.

Такива определения, се наричат *определения по индукция*. По дискретна математика правихме подобни дефиниции (спомнете си дефиницията за кореново дърво).

Цели числа

За целите числа($\mathbb{Z}$) знаем, че са надмножество на $\mathbb{N}$, т.е. $\mathbb{Z} \supset \mathbb{N}$.
Бинарни операции в $\mathbb{Z}$ са събиране, изваждане и умножение.
Делението не е бинарна операция за $\mathbb{Z}$!

Твърдение 1: Припомнете си, че всяко ограничено отдолу (отгоре) подмножество U на естествените числа има най-малък (най-голям) елемент.
Т.е ако $\exists a \in \mathbb{Z} : \forall b \in U \Rightarrow a \leq b$ (ако a ограничава U отдолу), то
$\exists b_0 \in U : \forall b \in U \Rightarrow b_0 \leq b$ (съществува елемент, вече от U, който е по-малък или равен на всички елементи на U).

Твърдение 2: Ако $a = bc$, където $b, c \in \mathbb{Z}$ и $b \neq 0, c \neq 0$, то
$|a| \geq |b|$ и $|a| \geq |c|$

Делимост на цели числа

Теорема*(Деление с частно и остатък)*:

Нека $a, b \in \mathbb{Z}$ и $b \neq 0$. Тогава съществуват единствени $q, r \in \mathbb{Z}$, такива че a може да се престави по следния начин:
$a = bq + r$ и $0 \leq r < |b|$.

Доказателство:
1. Съществуване ($\exists$)
Разглеждаме множеството $M = \{a + bs | s \in \mathbb{Z}\}$.
Вземаме неговото подмножество $M^+ = \{x | x \in M \& x \geq 0\} \neq \varnothing$ (т.е филтрирахме M и взехме само неотрицателните).
M^+ е ограничено отдолу от нулата $\Longrightarrow \exists r \in M^+$, такова че за $\forall x \in M^+ \Rightarrow r \leq x$ (от твърдение 1).
Тъй като $r \in M^+$ и $M^+ \subset M \Longrightarrow r = a + bs_1$.

Допускаме, че $r \geq |b| \Rightarrow r - |b| \in M^+$, което е противоречие с това, че r е минимален в M^+, понеже $b \neq 0$, т.е. $0 < |b|$ и $0 \leq r - |b| < r$.
$\Longrightarrow \exists r : \ 0 \leq r < |b|$, такова че $a = -bs_1 + r = b(-s_1) + r$. Тук, ако положим $q = -s_1$, получаваме $a = bq + r$.
q наричаме *частно*, а r - *остатък*.

2. Единственост (!)
Допускаме, че
$a = bq_1 + r_1, \ 0 \leq r_1 < |b|$
$a = bq_2 + r_2, \ 0 \leq r_2 < |b|$
Изваждаме двете равенства и получаваме, че $b(q_1 - q_2) = r_2 - r_1$.
И тъй като $|r_2 - r_1| < |b|$ и от твърдение 2 $\Longrightarrow q_1 - q_2 = 0$, т.е. $q_1 = q_2$ и $r_1 = r_2$.

Следствие:
Не чак толкова очевидното следствие от предната теорема е, че всяко естествено число c може да се представи по единствен начин в q-ична бройна система.
Т.е ако $c \in \mathbb{N}$ и $q \in \mathbb{N}, \ q > 1$, то
$c = c_k q^k + c_{k-1} q^{k-1} + \ldots + c_1 q + c_0$, където $0 \leq c_i < q$ за $i = \overline{0, k}$

Доказателство:
Следствието се доказва индуктивно:
От теоремата $\Rightarrow c = a_1 q + r_1$, ако $a_1 < q$, тогава това е търсеното представяне ($a_1 = c_1$ и $r_1 = c_0$),
иначе $a_1 = a_2 q + r_2$ и $r_2 = c_1$.

Дефиниция*(Делимост)*:

Нека $a \in \mathbb{Z}, a \neq 0$. Казваме, че a **дели** b, когато $b = at, \ t \in \mathbb{Z}$.

Записваме a/b или $b \vdots a$ (b се дели на a)

Свойства на делимостта

За $a \in \mathbb{Z}, a \neq 0$:

1. $a/\pm a$
2. $a/0$
3. $a/b \& b/a \Longrightarrow |b| = |a| \iff a = \pm b$
4. $a/b \& b/c \Longrightarrow a/c$
5. $a/b \Longrightarrow \pm a/\pm b$
6. $a/b_1 \& a/b_2 \Longrightarrow a/k_1 b_1 + k_2 b_2$, където $k_1, k_2 \in \mathbb{Z}$
7. $a/b \& b \neq 0 \Longrightarrow |a| \leq |b|$

Дефиниция*(най-голям общ делител (НОД))*:

Най-голям общ делител на две цели числа $a, b \in \mathbb{Z}$, поне едно от които не е нула ($a \neq 0$ или $b \neq 0$), наричаме цялото число $d \in \mathbb{Z}$, за което са изпълнени следните свойства:

1. d/a и d/b.
2. d е максималното с това свойство.
2'. Ако d_1/a и d_1/b, то d_1/d.

Отбелязваме НОД$(a, b) = (a, b) = d$[1][2]

Забележка: 2. и 2'. са еквиваленти, когато знаем, че в даденото множество има "хубава" наредба (т.е. за всеки два елемента можем да кажем кой е по-големият/по-малкият или са равни). Но при пръстените (които ще изучаваме в бъдеще) явно няма "хубава" наредба и 2. е по-вървежно ;)

Теорема*(съществуване и единственост на НОД)* a.k.a Теорема на Безу:

Нека $a, b \in \mathbb{Z}$ като $a \neq 0$ или $b \neq 0$. Тогава $\exists! d = (a, b)$ и
$d = ua + vb$, където $u, v \in \mathbb{Z}$[3] (тъждество на Безу).

Доказателство:
Разглеждаме множеството $M = \{xa + yb | x, y \in \mathbb{Z}\}$.
Вземаме неговото подмножество $M^+ = \{z \in M | z > 0\} \neq \varnothing$.
$M^+ \subset \mathbb{N} \implies \exists d$ - минимален елемент в M^+.

$d = x_1 a + y_1 b \ > 0$

Нека $c \in M$. Тогава $c = x_2 a + y_2 b$ (от дефиницията на M).
От друга страна, ако използваме теоремата за деление с частно и остатък за c и d получаваме
$c = dq + r,\ 0 \leq r < |d| = d$
Сега да използваме двете представяния на c:
$x_2 a + y_2 b = c = dq + r = (x_1 a + y_1 b)q + r$
От тук получихме формула за r : $r = (x_2 - x_1 q)a + (y_2 - y_1 q)b$.
Очевидно $r \in M$ и е неотрицателно (от ТДЧО[4]). Също така $r < d$ следователно не е от M^+ (защото d е минимален елемент) и остана $r = 0$. Така получихме, че d/c.

Ще докажем, че d е НОД на a, b:

1. Ако $c \in M \Rightarrow d/c$. Сега понеже $a, b \in M$ имаме $d/a \& d/b$, т.е d е техен общ

делител.
2. Нека d_1 е произволен общ делител на a, b. Тогава $d_1/a \& d_1/b$, следователно $d_1/\underbrace{x_1 a + y_1 b}_{d}$. Т.е получихме, че d_1/d

Следователно, по дефиниция за НОД : $d = (a, b)$

Алгоритъм на Евклид за намиране на НОД

Дадено: $a, b \in \mathbb{Z},\ a, b \neq 0$.

Резултат: $d =$ НОД(a, b).

Процедура:

От теоремата за деление с частно и остатък $\Longrightarrow\ a = bq_1 + r_1$, $0 \leq r_1 < |b|$.

Първо ще докажем, че НОД(a, b) = НОД(b, r_1).
Нека $d_1 = (a, b)$ и $d_2 = (b, r_1)$.

От $d_1 =$НОД$(a, b) \Rightarrow\ d_1|a$ и $d_1|b\ \Longrightarrow\ d_1|(a - bq_1)\ \Rightarrow\ d_1|r_1$

$\Longrightarrow\ d_1|d_2$ (1)

От $d_2 =$НОД$(b, r_1) \Rightarrow\ d_2|b$ и $d_2|r_1\ \Longrightarrow\ d_2|(bq_1 + r_1)\ \Rightarrow\ d_2|a$

$\Longrightarrow\ d_2|d_1$ (2)

От (1) и (2) $\Longrightarrow\ d_1 = d_2$.

До тук: $a = bq_1 + r_1$ и $(a, b) = (b, r_1)$

Ako $r_1 = 0\ \Rightarrow\ d = b$ - търсеният НОД.
Иначе (ако $r_1 \neq 0$), то $b = r_1 q_2 + r_2,\ 0 \leq r_2 < r_1$ като $(b, r_1) = (r_1, r_2)$.

Отново, ако $r_2 = 0\ \Rightarrow\ d = r_1$;
иначе: процесът се повтаря.

Знаем, че за НОД(a, b) можем да получим минимум 1, т.е. процесът е краен.

На k-та стъпка имаме:
$r_{k-1} = r_k q_{k+1} + r_{k+1},\ 0 \leq r_{k+1} < r_k$ и $(r_{k-1}, r_k) = (r_k, r_{k+1})$.

$|b| > r_1 > r_2 > \ldots > r_{k-1} > r_k > \ldots \geq 0$

На $(k+1)$-ва стъпка получаваме следното:
$r_k = r_{k+1} q_{k+2} + 0$ и $(r_k, r_{k+1}) = (r_{k+1}, 0) = r_{k+1}$

Тъй като $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{k-1}, r_k) = (r_k, r_{k+1}) = r_{k+1}$.

НОД$(a, b) = r_{k+1}$. $\square$

По обратните стъпки на алгоритъма на Евклид, можем да получим и тъждеството на Безу ($d = ua + vb$).

Получихме, че:
$d = r_{k+1} = r_{k-1} - q_{k+1} r_k$
От теоремата за деление с частно и остатък знаем, че $r_k = r_{k-2} - r_{k-1} q_k$
И при заместване на r_k в горното равенство получаваме $d = u_{k-1} r_{k-1} + v_{k-1} r_{k-2}$,
където u_{k-1} и v_{k-1} са коефициентите, получени при приведението.
Така при следващата стъпка получаваме, че $d = u_{k-2} r_{k-2} + v_{k-2} r_{k-3}$.
Тъй като и този процес е краен, след известен брой стъпки, ще получим $d = ua + vb$. $\square$

Пример за намиране на НОД по алгоритъма на Евклид и намиране тъждеството на Безу:

Нека $a = 321$ и $b = 123$.

$a = 2b + 75$
$b = 1 * 75 + 48$
$75 = 1 * 48 + 27$
$48 = 1 * 27 + 21$
$27 = 1 * 21 + 6$
$21 = 3 * 6 + 3$
$6 = 2 * 3 + 0$
$\Rightarrow (a, b) = 3$

НОД$(321, 123) = 3$
$3 = 21 - 3 * 6 = 21 - 3 * (27 - 21) = 4 * 21 - 3 * 27 = 4 * (48 - 27) - 3 * 27 =$
$= 4 * 48 - 7 * 27 = 4 * 48 - 7 * (75 - 48) = 11 * 48 - 7 * 75 = 11 * (b - 75) - 7 * 75 =$
$= 11b - 18 * 75 = 11b - 18 * (a - 2b) = -18a + 47b$
В този случай $u = -18$ и $v = 47$.

Footnotes

1. Държа също да отбележа, че както и да смятате НОД на две цели числа не може (а и не трябва) да се получи число, което е по-малко от 1.
С други думи: най-малкият най-голям общ делител на две произволни цели числа е най-малко 1.
Не че някога ще се налага да се доказва, но е хубаво да се знае. Твърдението следва почти непосредствено от дефиницията и от свойствата на делимостта.
И междудругото възникна спорът колко е НОД(0, 0). Малко се затормозява човек с такива подробности.
2. за в бъдеще ще отбелязваме НОД или само с кръгли скоби - (a, b) или със английското му наименование - $gcd(a, b)$ (greatest common divisor). За математическите означения е прието да се използват английки/гръцки букви.
3. u и v не са единствени.
4. теорема за деление с частно и остатък - писна ми да го пиша :)

page revision: 129, last edited: 24 Jun 2009, 13:37 (1473 days ago)

Unless stated otherwise Content of this page is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License