§2. Cel mai mare divizor comun a două numere. Proprietăți

Fie $a, b \in \mathbb{Z}$

Definiție

Nr. c se num. divizor comun a nr. a și b, dacă $a \vdots c$ și $b \vdots c$ ($c \mid a$) și ($c \mid b$).

6; 15.

$\pm 1; \pm 3$

Definiție nr. $d \in \mathbb{Z}$ se numește cel mai mare divizor comun a nr. a și b, dacă verifică condițiile.

1) d - divizor comun a lui a și b
2) d - divizibil prin orice alt divizor comun al numerelor a și b.

6, 15

3, -3 - sunt cei m. mari d. com.

Teorema 1

Dacă d_1 și d_2 sunt cei mai mari divizori comuni ai nr. a și b, atunci $d_1 = d_2$ sau $d_1 = -d_2$.

Din faptul că d_1 este cel mai mare divizor comun al nr. a și b $\Rightarrow$ că d_1 este divizibil prin orice alt divizor al lui a și b în particular $d_1 \vdots d_2$

$d_1 : d_2 \Rightarrow d_1 = c_1 d_2$ (1) analog $\Rightarrow$

pt. d_2 obținem:

$d_2 : d_1 \Rightarrow d_2 = c_2 \cdot d_1$ (2)

$d_1 = c_1 c_2 d_1$

$d_1 (1 - c_1 c_2) = 0$. $\quad | d_1 \neq 0 \Rightarrow$

$c_1 c_2 = 1 \Leftrightarrow \begin{cases} c_1 = c_2 = 1 \\ c_1 = c_2 = -1 \end{cases} \Leftrightarrow \begin{cases} d_1 = d_2 \\ d_1 = -d_2 \end{cases}$ ▨

Dintre nr. d_1 și d_2, unul din ele este mai mare ca zero.

În continuare dl mai mare divizor comun al nr a și b îl vom nota astfel (a, b)

~~5~~ $(6, 15) = 3$.

~~3~~

Teorema 2

Dacă $a = bq + r$, atunci cel mai mare divizor comun ~~coincide~~ (a, b) cmmdc (b, r)

$(a, b) = (b, r)$

$(a, b) = d_1$

$(b, r) = d_2$ | $d_1 = d_2$ - ?

Din acea că:

1) $(a, b) = d_1 \Rightarrow a ; d_1$ și $\underline{b ; d_1} \overset{p.7.}{\Rightarrow} a ; d_1 \mid bq : d_1$

$\overset{p.2.5.}{\Rightarrow} \underbrace{(a - bq)}_{r} ; d_1 \Rightarrow \underline{r ; d_1} \Rightarrow d_1$ divizor comun al lui b și r. Deoarece d_2 este cmmdc al lui b și r $\Rightarrow d_2 : d_1$ (*)

2. $(b, r) = d_2 \Rightarrow b : d_2 \wedge r : d_2 \overset{p.t.}{\Rightarrow} (bq + r) : d_2$

$\wedge\ r : d_2 \Rightarrow a : d_2 \Rightarrow d_2$ - divizor comun a lui a, b, deoarece d_1 este CMMDC a lui a și b, $\Rightarrow$

$d_1 : d_2$ (**)

(*) și (**) $\Rightarrow d_1 = d_2$

$d_1 > 0$

$d_2 > 0$ ☐

§2. Algoritmul lui Euclid de aflare a CMMDC a două numere

Deoarece CMMDC $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ e suficient să studiem algoritmul de aflare a CMMDC (a, b) pt $a \geq 0$ și $b > 0$.

Pt. nr. a și b, conform T. împ. cu rest $\exists\ q$ și r din $\mathbb{Z}$, încît

(1) $a = bq + r$, $0 \leq r < b$.

Dacă $r = 0$, atunci $(a, b) = b$.

Dacă $r \neq 0$, pt. nr. b și r $\exists\ q_1, r_1 \in \mathbb{N}$, încît are loc

(2) $b = rq_1 + r_1$, $0 \leq r_1 < r$

Dacă $r_1 = 0$, $b = r q_1 \Rightarrow (b, r) = r \overset{T1}{=} (a, b)$

Dacă $r_1 \neq 0$, pt nr r și r_1 $\exists\ q_2, r_2$, încît va avea loc egalitatea

(3) $r = r_1 q_2 + r_2$, $0 \leq r_2 < r_1$

Dacă $r_2 = 0$, prin def.:

$(r, r_1) = r_1 \overset{T1}{=} (b, r) = (a, b)$.

Iar dacă $r_2 \neq 0$, pentru (r_1, r_2) vom $\exists$

$\exists q_3, r_3$ (4) $r_1 = r_2 q_3 + r_3$, cu $r_3 < r_2$

– – – – – – – – – –

Observăm că șirul de nr. $b, r, r_1, r_2, r_3 \ldots$ este un șir de nr. naturale, strict descrescător, de aici $\Rightarrow$ că $\exists$ așa un $n \in \mathbb{N}$, încît $r_n = 0$.

31.05.13.

(n) $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

(n+1) $r_{n-2} = r_{n-1} q_n + r_n$

$(r_{n-2}, r_{n-1}) = r_{n-1} \overset{T2}{=} (r_{n-3}, r_{n-2}) \overset{T2}{=}$

$\overset{T2}{=} (r_{n-4}, r_{n-3}) \overset{T2}{=} \ldots \overset{T2}{=} (r_3, r_2) \overset{T2}{=} (r_2, r_1) \overset{T2}{=}$

$\overset{T2}{=} (r_1, r) \overset{T2}{=} (b, r) \overset{T2}{=} (a, b)$ (descrescător)

$(a, b) = r_{n-1}$

Algoritmul descris mai sus poartă denumirea de Algoritmul lui Euclid.

C.M.M.D.C. = cel mai mare divizor comun

Exemplu

Utilizând algoritmul lui Euclid aflați C.M.M.D.C. al numerelor 948, și 216.

$(948, 216) = 12$.

948	216
864	4 = q
84	

rest. r_0

216	84
168	2 = q_1
48	

r_1

84	48
48	1 = q_2
36	

r_2

48	36
36	1 = q_3
12	

r_3

36	12
36	3 = q_4
0 =	r_4

C.M.M.D.C $(948; 216) = 12$.

§ 4. Reprezentarea liniară a celui mai mare divizor comun. Numere (reciproc) prime între ele

Fie $a, b \in \mathbb{Z}$, iar $d = (a, b)$ cel mai

Teorema

Pentru nr. a, b $\exists x, y \in \mathbb{Z}$, astfel încât $d = ax + by$ (liniară)

Pentru nr. a și b scriem algoritmul lui Euclid, de aflare a C.M.M.

a, b. (1) $a = bq + r$ $\quad d = r_{n-1}$

(2) $b =$

(3) $r = r_1 q_2 + r_2$

(4) $r_1 = r_2 q_3 + r_3$.

(n) $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

(n-1) $r_{n-2} = r_{n-1} q_n + r_n$

Din egalitatea (n) exprimăm:

r_{n-1} prin r_{n-3} și r_{n-2}

$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$

Ințelegând egalitatea (n-1), exprimăm:

r_{n-2} prin r_{n-4}, r_{n-3}

$r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$

Exprimăm succesiv r_{n-1} prin r_{n-5}, r_{n-4} ... r_2, r_1), ... r_1, r, r, b, a, b.

Notăm coeficientul obținut pe linia a prin x, iar coeficientul obținut pe linia b prin y. și obținem:

$r_{n-1} = ax + by$.

$d = ax + by$ ∎

Reprezentarea $d = ax + by$ se numește reprezentarea liniară a c.m.m.d.c

Observație.

Din egalitățile algoritmului lui Euclid, atunci când determinăm x și y se scriu doar ultimele împărțirilor, celelalte elemente să păstrează în forma generală

Exemplu

Aflați reprezentarea liniară a C.M.M.D.C a numerelor:

$(\overset{a}{\sim}112, \overset{b}{\sim}46) = 2$

112	46
92	2 = q
20 = r	

46	20
40	2 = q_1
= 6 = r_1	

20	6
18	3 = q_2
= 2 = r_2	

6	2
6	3
0	

$a = 2b + r$ $\quad b = 2r + r_1$ $\quad r = 3r_1 + r_2$

$d = r_2$; $d = 2$; $d = r_2 = r - 3r_1 =$
$= r - 3(b - 2r) = 7r - 3b =$
$= 7(a - 2b) - 3b = 7a - 17b.$

$d = 7a - 17b.$

Ver. $d = 4 \cdot 112 - 17 \cdot 46 = 2.$

$x = 7$; $y = -17.$

Definiție

Numerele întregi a și b se numesc prime între ele (sau reciproc) dacă $(a, b) = 1$

$(3,8) = 1 \quad (12,33) \neq 1$

$(4,9) = 1$

Teoremă:

Numerel $a, b \in \mathbb{Z}$ sunt prime între ele dacă și numai dacă există $x, y \in \mathbb{Z}$, astfel încât: $ax + by = 1$.

☑ Necesitatea

Fie a, b - prime între ele.
Conform algoritm. lui Euclid reprezentăm liniar (a, b), și obținem: $ax + by = 1$.

Suficiența

Fie că pentru numerele ~~$a x + by = 1$~~ a, b
Să adăugăm egalitatea $ax + by = 1$

$ax + by = 1 \mid (a, b) = 1$?

$(a,b) = d \Rightarrow a : d \wedge b : d \overset{P_2.7}{\Rightarrow} ax : d$ și $by : d \overset{P_2.5}{\Rightarrow}$
$(ax + by) : d \Rightarrow 1 : d \Rightarrow d = 1$.
În așa mod (a, b) - reciproc prime. ☒

Consecință Dacă $(a,b) : c$ și $(a,c) = 1 \Rightarrow b : c$.

☑ $ab : c$, $(a, c) = 1$ - repr. liniară

$ax + cy = 1 \mid \times b$.

$\underbrace{abx}_{:c} + \underbrace{bcy}_{:c} = b. \overset{P_2.5}{\Rightarrow} b : c$ ☒