Divizibilitate.

Teorema (Teorema împărţirii cu rest)
Pentru orice două numere întregi a şi b cu $b \neq 0$, există $q, r \in \mathbf{Z}$ astfel încât $a = bq+r$ şi $0 \leq r < |b|$. In plus, q şi r sunt unicele cu aceste proprietăţi.

Numerele q şi r din Teorema împărţirii cu rest se numesc *câtul* şi, respectiv, *restul* împărţirii lui a la b. Ele se mai notează prin $a \ div \ b$ şi, respectiv, $a \ mod \ b$. |

Definitia 1. Relatia binara $| \subseteq \mathbf{Z} \times \mathbf{Z}$ data prin

$$a|b \quad \Leftrightarrow \quad (\exists c \in \mathbf{Z})(b = ac),$$

pentru orice $a, b \in \mathbf{Z}$, se numeste *relatia de divizibilitate* pe $\mathbf{Z}$.

Daca $a \ b$ atunci vom spune ca a *divide* b sau ca a *este divizor al lui* b sau ca b *se divide prin* a sau ca b *este multiplu al lui* a. Daca a nu divide b atunci vom mai scrie $a \nmid b$.

Propoziţie Fie $a, b, c \in \mathbf{Z}$. Atunci, au loc următoarele proprietăţi:

1. 0 divide doar 0;

2. a divide 0 si a;

3. 1 divide a;

4. $a|b$ daca si numai daca $a|-b$;

5. daca $a|b$ si $b|c$ atunci $a|c$;

6. daca $a|b+c$ si $a|b$ atunci $a|c$;

7. daca $a|b$ atunci $ac|bc$. Reciproc, daca $c \neq 0$ si $ac|bc$ atunci $a|b$;

8. daca $a|b$ si $a|c$ atunci $a|\beta b + \gamma c$ pentru orice $\beta, \gamma \in \mathbf{Z}$;

Definiţia 2. Un număr natural $p \geq 2$ este numar *prim* dacă singurii lui divizori pozitivi sunt 1 si p.

Definiţia 3. Fie $a_1, \ldots, a_m \in \mathbf{Z}$, unde $m \geq 2$. Spunem ca $a_1, \ldots, a_m$ sunt *prime intre ele* sau *relativ prime* sau *coprime* daca singurii divizori comuni ai acestor numere sunt 1 si -1.

Notam $(a_1, \ldots, a_m) = 1$ pentru a specifica faptul ca $a_1, \ldots, a_m$ sunt relativ prime.

Teorema 1 Fie $m \geq 2$ si $a_1, \ldots, a_m \in \mathbf{Z}$. Atunci $(a_1, \ldots, a_m) = 1$ daca si numai dacă există $\alpha_1, \ldots, \alpha_m \in \mathbf{Z}$ astfel încât $\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_m a_m = 1$.

Proprietatea 1. Fie $a_1,\dots, a_m, b \in \mathbf{Z}$ unde $m \geq 2$. Daca $(b, a_i) = 1$ pentru orice $1 \leq i \leq m$, atunci $(b, a_1 \cdots a_m) = 1$.

Demonstraţie Demonstram pentru $m = 2$, cazul general obţinându-se prin simpla inductie.
Conform Teoremei 1 există α_1, α_2, β_1 şi β_2 astfel încât $\alpha_1 a_1 + \beta_1 b = 1$ şi
$\alpha_2 a_2 + \beta_2 b = 1$. Deci $1 = 1.1 = (\alpha_1 a_1 + \beta_1 b)(\alpha_2 a_2 + \beta_2 b)$
$= \alpha_1\alpha_2 a_1 a_2 + b(\alpha_1 a_1 \beta_2 + \alpha_2 a_2 \beta_1 + \beta_1\beta_2 b)$,

ceea ce arata ca $(b, a_1 a_2) = 1$.
Pentru $m > 2$ se aplica inductia matematica.

Proprietatea 2. Fie $a_1,\dots, a_m, b \in \mathbf{Z}$, unde $m \geq 2$. Daca numerele $a_1,\dots, a_m$ sunt prime între ele două câte două şi fiecare din ele divide b, atunci produsul lor divide b.

Demonstraţie Demonstram pentru $m = 2$.
Deoarece $(a_1, a_2) = 1$, există α_1 şi α_2 astfel încât $\alpha_1 a_1 + \alpha_2 a_2 = 1$, iar de la $a_1 \mid b$ si $a_2 \mid b$ rezulta că există β_1 şi β_2 astfel încât $b = a_1\beta_1 = a_2\beta_2$.

Atunci, $b = a_1\beta_1 = a_1\beta_1 1 = a_1\beta_1(\alpha_1 a_1 + \alpha_2 a_2) = a_1\beta_1\alpha_1 a_1 + a_1 a_2 \alpha_2\beta_1$
$= a_2\beta_2\alpha_1 a_1 + a_1 a_2\alpha_2\beta_1 = a_1 a_2(\alpha_1\beta_2 + \alpha_2\beta_1)$,
ceea ce arata ca $a_1 a_2 | b$.
Pentru $m > 2$ se aplica inductia matematica.

Proprietatea 3. Fie $a_1,\dots, a_m, b \in \mathbf{Z}$, unde $m \geq 2$. Daca b este prim cu a_1 si b divide produsul $a_1 \cdots a_m$, atunci b divide produsul $a_2 \cdots a_m$.

Demonstraţie Deoarece $(b, a_1) = 1$ urmează că există α şi β astfel încât $\alpha a_1 + \beta b = 1$, iar de la $b | a_1 \cdots a_m$ urmează că există γ astfel încât $a_1 \cdots a_m = b\gamma$. Atunci,

$$a_2 \cdots a_m = 1 \cdot a_2 \cdots a_m = (\alpha a_1 + \beta b) a_2 \cdots a_m = \alpha a_1 \cdots a_m + \beta b a_2 \cdots a_m$$
$$= \alpha b\gamma + \beta b a_2 \cdots a_m = b(\alpha\gamma + \beta a_2 \cdots a_m),$$

ceea ce arata ca $b | a_2 \cdots a_m$.

Proprietatea 4. Fie $a_1,\dots, a_m, p \in \mathbf{Z}$, unde $m \geq 2$. Daca p este prim si p divide produsul $a_1 \cdots a_m$, atunci există i astfel încât p divide a_i.

Demonstratie Presupunem, prin contradictie ca *p nu divide* a_i, pentru orice i. Atunci, p este prim cu oricare din numerele a_i si deci, conform Prop.1 conduce la $(p, a_1 \cdots a_m) = 1$, ceea ce contrazice $p | a_1 \cdots a_m$.

Fie $n \geq 2$ un număr natural. Numim *descompunere* a lui n orice secvenţă finită de numere naturale $n_1,\dots, n_k$ $(k \geq 1)$ astfel încât $n = n_1 \cdots n_k$. Prin descompunerea numărului natural $n \geq 2$ in produs de puteri de numere prime vom intelege orice secventa de perechi de numere naturale

$(n_1, e_1),\ldots, (n_k, e_k)$ $(k \geq 1)$

astfel încât: $2 \leq n_1 < \cdots < n_k$; n_i numere prime, $e_i > 0$, pentru orice $1 \leq i \leq k$, si

$n = n_1^{e_1} n_2^{e_2} \ldots n_k^{e_k}$

De exemplu, $20 = 2^2 5$ Daca în descompunerea de mai sus numerele $n_1, \ldots, n_k$ sunt prime, atunci descompunerea lui n va fi numita *descompunere în factori primi*. Are loc:

Teorema 2. (Teorema fundamentala a aritmeticii)
Orice număr natural $n \geq 2$ poate fi descompus, în mod unic, într-un produs de puteri de factori primi.

Cel mai mare divizor comun (c.m.m.d.c.) si Cel mai mic multiplu comun (c.m.m.m.c.)

Definiţia 4. Fie $a_1, \ldots, a_n$ numere întregi diferite de 0, unde $n \geq 2$. Cel mai mare număr natural d cu proprietatea $d | a_i$, pentru orice $1 \leq i \leq n$ se numeste *cel mai mare divizor comun* al numerelor $a_1, \ldots, a_n$. Se noteaza $d = (a_1, \ldots, a_n)$

Teorema 3
Fie $a_1, \ldots, a_n$ numere întregi nu toate 0, unde $n \geq 2$. Atunci, exista numerele întregi $\alpha_1, \ldots, \alpha_n$ astfel încât $d = (a_1, \ldots, a_n) = \alpha_1 a_1 + \cdots + \alpha_n a_n$.

Definiţia 5. Fie $a_1, \ldots, a_n$ numere întregi nenule, unde $n \geq 2$. *Cel mai mic multiplu comun* al numerelor $a_1, \ldots, a_n$ este cel mai mic număr natural nenul m cu proprietatea $a_i | m$, pentru orice $1 \leq i \leq n$. Se noteaza $m = [a_1, \ldots, a_n]$.

Determinarea celui mai mare divizor comun a două numere - *Algoritmul lui Euclid* .

Fie $a \geq b \geq 0$:

- daca $a = b$ sau $b = 0$ atunci $(a, b) = a$;
- dacă $a > b > 0$

$a = b q_1 + r_1, \quad 0 < r_1 < b$
$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$
...
$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}$
$r_{n-1} = r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0,$

$r_n < r_{n-1} < r_{n-2} < \ldots\ldots < r_2 < r_1 < b$

Avem $(a, b) = (b, r_1) = \cdots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n$.

Algoritmul Extins al lui Euclid

Dacă fiecărui element x ce intervine în secvenţa de împărţiri de mai sus îi asociem un vector $V_x = (\alpha, \beta)$ ce furnizează combinatia liniara (in functie de a si b) a lui x, adica $d = \alpha a + \beta b$, atunci combinatia liniara a resturilor se poate determina prin:

$V_a = (1, 0)$ $V_b = (0,1)$
$a = bq_1 + r_1$ $V_{r_1} = V_a - q_1 V_b$
$b = r_1 q_2 + r_2$ $V_{r_2} = V_b - q_2 V_{r_1}$
$r_1 = r_2 q_3 + r_3$ $V_{r_3} = V_{r_1} - q_3 V_{r_2}$
...
$r_{n-2} = r_{n-1} q_n + r_n$ $V_{r_n} = V_{r_{n-2}} - q_n V_{r_{n-1}}$
$r_{n-1} = r_n q_{n+1}$

Congruente $\equiv$

Fie m un număr întreg. Definim pe $\mathbf{Z}$ relaţia binară $\equiv_m$, numită *relaţia de congruenţă modulo m* sau *congruenta modulo m*, prin: $a \equiv_m b \Leftrightarrow m|(a-b)$,

pentru orice $a, b \in \mathbf{Z}$. Daca $a \equiv_m b$ atunci vom spune ca a si b sunt *congruente modulo m*, notat prin $a \equiv b \bmod m$.

Proprietaţi Fie a, b, c, d, m şi m' numere întregi. Atunci, au loc următoarele proprietăţi:

1. $\equiv_m$ este relatie de echivalenta pe $\mathbf{Z}$;
2. $a \equiv_m b$ daca si numai daca $a \bmod m = b \bmod m$;
3. daca $a \equiv_m b$, atunci $(a, m) = (b, m)$;
4. daca $a \equiv_m b$ si $c \equiv_m d$ atunci $a + c \equiv_m b + d$, $a - c \equiv_m b - d$, $ac \equiv_m bd$;
5. dacă $ac \equiv_{mc} bc$ şi $c \neq 0$, atunci $a \equiv_m b$;
6. daca $ac \equiv_m bc$ si $d = (m, c)$, atunci $a \equiv_{m/d} b$;
7. daca $ac \equiv_m bc$ si $(m, c) = 1$, atunci $a \equiv_m b$;
8. daca $a \equiv_{mm'} b$, atunci $a \equiv_m b$ si $a \equiv_{m'} b$;
9. daca $a \equiv_m b$ si $a \equiv_{m'} b$, atunci $a \equiv_{[m, m']} b$;

Demonstratii

3. daca $a \equiv_m b$, atunci $(a, m) = (b, m)$;

Fie $d_a = (a,m)$ => $d_a|a$ si $d_a|m$
Fie $d_b = (b,m)$ => $d_b|b$ si $d_b|m$
$a \equiv_m b$ => m | a - b

$d_a | a - b, d_a | a \Rightarrow d_a | b \Rightarrow d_a | d_b$ deci $d_a \leq d_b$
$d_b | a - b, d_b | b \Rightarrow d_b | a \Rightarrow d_b | d_a$ deci $d_b \leq d_a$
deci $d_a = d_b \Rightarrow (a, m) = (b, m)$

6. daca $ac \equiv_m bc$ si $d = (m, c)$, atunci $a \equiv_{m/d} b$;

$ac \equiv_m bc \Rightarrow$ m | ac - bc <=> exista k astfel incat ac - bc = mk <=> c(a - b) = mk
$d = (m, c) \Rightarrow$ d | m si d | c deci exista x, y astfel incat c = dx si m = dy , (x, y) = 1.
Asadar dx(a - b) = dyk => x(a - b) = yk, (x, y) = 1 => y|$a - b$ => m/d | $a - b$ => $a \equiv_y b$ => $a \equiv_{m/d} b$.

9. daca $a \equiv_m b$ si $a \equiv_{m'} b$, atunci $a \equiv_{[m, m']} b$;
Presupunem că $a \equiv_m b$ şi $a \equiv_{m'} b$. Prima relaţie conduce la $m|(a - b)$ a doua la $m' | (a - b) \Rightarrow [m, m'] | (a - b)$.

Euatii diofantice liniare

Sunt ecuatii de forma ax + by = c

Ecuatia ax + by = c are solutie <=> gcd(a, b)|c

Solutia se calculeaza astfel:

1. Se aplica Algoritmul Extins al lui Euclid pentru a calcula gcd(a, b) = αa + βb;

2. c′ = c/gcd(a,b) ;

3. x = αc′; y = βc′.

Exercitiul 1 (Algoritmul Extins al lui Euclid).

Calculati d = gcd(a, b) si α, β *astfel incat d*= αa + βb, *unde:*

a) a = 27, b = 21*;*

$V_a = (1, 0)$ $V_b = (0,1)$

$27 = 1 \cdot 21 + 6$ $V_{r_1} = V_a - q_1 V_b = (1,0) - 1(0,1) = (1, -1)$

$21 = 3\cdot 6 + 3$ $\quad V_{r_2} = V_b - q_2 V_{r_1} = (0,1) - 3(1,-1) = (-3, 4)$
$6 = 3\cdot 2$

$\alpha = -3$ si $\beta = 4$

Deci $(27, 21) = 3 = -3\cdot 27 + 4\cdot 21$

b) a = 24, b = 39*;*

(24, 39) = (39, 24)

$V_a = (1, 0)$ $\quad V_b = (0,1)$

$39 = 1\cdot 24 + 15$ $\quad V_{r_1} = V_a - q_1 V_b = (1,0) - 1(0,1) = (1, -1)$
$24 = 1\cdot 15 + 9$ $\quad V_{r_2} = V_b - q_2 V_{r_1} = (0,1) - 1(1,-1) = (-1, 2)$
$15 = 1\cdot 9 + 6$ $\quad V_{r_3} = V_{r_1} - q_3 V_{r_2} = (1,-1) - 1(-1,2) = (2, -3)$
$9 = 1\cdot 6 + 3$ $\quad V_{r_4} = V_{r_2} - q_4 V_{r_3} = (-1,2) - 1(2,-3) = (-3, 5)$
$6 = 2\cdot 3$

(39, *24*) = 3 deci si $\alpha = 5$, $\beta = -3$

c) a = 47, b = 35
d) a = 25, b = 45

Exercitiul 2 (Ecuatii diofantice liniare). *Rezolvati ecuatiile:*

a) $24x + 7y = 8$*;*

$24 = 3\cdot 7 + 3$ $\quad V_{r_1} = V_a - q_1 V_b = (1,0) - 3(0,1) = (1, -3)$
$7 = 3\cdot 2 + 1$ $\quad V_{r_2} = V_b - q_2 V_{r_1} = (0,1) - 2(1,-3) = (-2, 7)$
$3 = 3\cdot 1$

$(24, 7) = 1$ $\quad \alpha = -2$, $\beta = 7$

deci $c' = 8/1 = 8$ si $x = \alpha c' = -16$ si $y = \beta c' = 56$

b) $12x + 39y = 18$*;*

$(12, 39) = (39, 12)$

$39 = 3\cdot 12 + 3$ $\quad V_{r_1} = V_a - q_1 V_b = (1,0) - 3(0,1) = (1, -3)$
$12 = 3\cdot 4$

$(12, 39) = (39, 12) = 3$ $\quad \alpha = -3$, $\beta = 1$

deci c' = 18/3 = 6 si x = αc′ = -18 si y = βc′ = 6

c) 28x + 18y = 16.
d) 12x + 9y = 6
e) 7x + 21y = 11

Notam $Z_m = Z/_{\equiv m}$ $\mathbf{Z}_m^* = \{a \in \mathbf{Z}_m | (a, m) = 1\}$

Calculul inversului modular

a ∈ $\mathbf{Z}_m$ are invers modulo m <=> (a,m) = 1.

1. Se calculeaza (a,m) = αa + βm;

2. Daca (a,m) = 1 atunci a^{-1} = α mod m.

Exercitiul 3 (Invers modular)

Calculati a^{-1} mod m, *unde:*
a) a = 35, m = 46

(35, 46) = (46, 35)

46 = 1·35 + 11 $V_{r_1} = V_a - q_1 V_b = (1,0) - 1(0,1) = (1, -1)$
35 = 3·11 + 2 $V_{r_2} = V_b - q_2 V_{r_1} = (0,1) - 3(1,-1) = (-3, 4)$
11 = 5·2 + 1 $V_{r_3} = V_1 - q_3 V_{r_2} = (1,-1) - 5(-3,4) = (-3, 4) = (16, -21)$
2 = 1·2

35^{-1} = -21 mod 46 = (46-21)mod 46 = 25 mod 46

b) a = 18, m = 23*;*

c) a = 21, m = 34.

d) a = 17, m = 42