Lecție pentru clasa a VI-a sau a VII-a, Răzvan Mihăescu, clasa a VIII-a

Algoritmul lui Euclid

- pentru clasele a VI-a și a VII-a

Algoritmul lui Euclid constituie o metodă eficientă de a determina cel mai mare divizor comun a două numere. El este denumit după matematicianul grec Euclid care l-a descris în Cărțile VII și X din „Elementele".

Algoritmul lui Euclid cunoaște două variante:

- varianta cu scăderi repetate;
- varianta cu împărțiri repetate.

Teorema 1 (Algoritmul lui Euclid, varianta cu scăderi repetate):

Pornind de la numerele întregi pozitive a și b, se poate obține c.m.m.d.c. (a, b) prin înlocuirea repetată a numerelor a și b cu $|a-b|$ și $\min\{a, b\}$ până când cele două numere sunt egale, iar acela este c.m.m.d.c. (a, b).

Demonstrație: Mai întâi vom demonstra că:

$$\text{c.m.m.d.c.}(a,b) = \text{c.m.m.d.c.}(|a-b|, a) = \text{c.m.m.d.c.}(|a-b|, b).$$

Dacă c.m.m.d.c. $(a, b) = d$ atunci $d \mid a$ și $d \mid b$, de unde rezultă că $d \mid a-b \Rightarrow d \mid |a-b|$.

Din $d \mid a$ și $d \mid |a-b| \Rightarrow d \mid$ c.m.m.d.c. $(|a-b|, a) \overset{not}{=} d_1$ (1)

Din c.m.m.d.c. $(|a-b|, a) = d_1$, rezultă că $d_1 \mid a$ și $d_1 \mid |a-b|$. Relația $d_1 \mid |a-b|$ implică $d \mid -a+b \Rightarrow d \mid a-a+b = b$. Din $d_1 \mid a$ și $d_1 \mid b$, rezultă că: $d_1 \mid$ c.m.m.d.c. $(a, b) = d$. (2)

Din (1) și (2) $\Rightarrow d = d_1$. Analog se demonstrează că d_2 = c.m.m.d.c. $(|a-b|, b)$ este egal cu d.

În continuare vom demonstra că, prin înlocuirea repetată a numerelor a și b cu $|a-b|$ și $\min\{a, b\}$ se obține în final c.m.m.d.c. (a, b). Din c.m.m.d.c. (a, b) = cmmdc $(|a-b|, a)$ = = cmmdc $(|a-b|, b)$ rezultă că:

$$\text{cmmdc}(a, b) = \text{cmmdc}(|a-b|, \min\{a, b\}).$$

Dacă $a, b > 0$ atunci: $a > b$ sau $b \geq a$. Dacă $a > b$, atunci

$$a + b - |a-b| - \min\{a, b\} = a + b - (a-b) - b = b > 0$$

iar dacă $b \geq a$, atunci:

$$a + b - |a-b| - \min\{a, b\} = a + b - (b-a) - a = a > 0.$$

În ambele cazuri rezultă că $a + b > |a-b| + \min\{a, b\}$. (3)

Dacă $a = 0$, atunci:

$$a + b - |a-b| - \min\{a, b\} = b - b - 0 = 0.$$

iar dacă $b=0$, atunci:

$$a+b-|a-b|-\min\{a,b\} = a-a-0 = 0.$$

În ambele cazuri rezultă că:

$$a+b = |a-b| + \min\{a,b\} \qquad (4)$$

Din (3) și (4) $\Rightarrow$ după cel mult $a+b$ pași suma $a+b$ devine constantă. Suma de la un pas este egală cu suma de la pasul următor doar dacă $a=0$ sau $b=0$. Fie K ultimul pas în care $a_K \neq 0$ și $b_K \neq 0$ și $K+1$ primul pas în care $a_{K+1}=0$ sau $b_{K+1}=0$. Suma $a+b$ în pasul $K+1$ este egală cu $|a_K - b_K| + \min\{a_K, b_K\}$, de unde rezultă că sau $|a_K - b_K| = 0$ sau $\min\{a_K, b_K\} = 0$.

Dacă $\min\{a_K, b_K\} = 0$ atunci $a_K = 0$ sau $b_K = 0$, contradicție cu $a_K \neq 0$, $b_K \neq 0$. Așadar singura variantă posibilă este ca $a_K = b_K$. Astfel $\text{cmmdc}(a,b) = \text{cmmdc}(a_K, b_K) = a_K$.

Exerciții explicate:

1) Să se determine $\text{cmmdc}(50,80)$, utilizând algoritmul lui Euclid, varianta cu scăderi repetate.

Rezolvare: Aplicăm algoritmul lui Euclid, varianta cu scăderi repetate asupra numerelor 50 și 80.

Pasul 1. $a_1 = 50$ și $b_1 = 80 \Rightarrow$

$a_2 = |a_1 - b_1| = |50-80| = 30$

$b_2 = \min\{a_1, b_1\} = \min\{50, 80\} = 50$

Pasul 2. $a_2 = 30$ și $b_2 = 50 \Rightarrow$

$a_3 = |a_2 - b_2| = |30-50| = 20$ și

$b_3 = \min\{a_2, b_2\} = \min\{30, 50\} = 30$.

Pasul 3. $a_3 = 20$ și $b_3 = 30 \Rightarrow$

$a_4 = |a_3 - b_3| = |20-30| = 10$ și

$b_4 = \min\{a_3, b_3\} = \min\{20, 30\} = 20$.

Pasul 4. $a_4 = 10$ și $b_4 = 20 \Rightarrow$

$a_5 = |a_4 - b_4| = |10-20| = 10$ și

$b_5 = \min\{a_4, b_4\} = \min\{10, 20\} = 10$.

Cum $a_5 = b_5 = 10 \Rightarrow \text{cmmdc}(50,80) = \text{cmmdc}(a_5, b_5) = 10$.

2) Să se determine $\text{cmmdc}(81, 64)$, utilizând algoritmul lui Euclid, varianta cu scăderi repetate.

Rezolvare: Aplicăm algoritmul lui Euclid, varianta cu scăderi repetate asupra numerelor $a_1 = 81$ și $b_2 = 64$.

Pasul 1. $a_1 = 81$ și $b_1 = 64 \Rightarrow a_2 = |a_1 - b_1| = |81-64| = 17$ și $b_2 = \min\{a_1, b_1\} = \min\{81, 64\} = 64$.

Pasul 2. $a_2 = 17$ și $b_2 = 64 \Rightarrow a_3 = |a_2 - b_2| = |17 - 64| = 47$ și $b_3 = \min\{a_2, b_3\}$
$= \min\{17, 64\} = 17$.
Pasul 3. $a_3 = 47$ și $b_3 = 17 \Rightarrow a_4 = |a_3 - b_3| = |47 - 17| = 30$ și $b_4 = \min\{a_3, b_3\}$
$= \min\{47, 17\} = 17$.
Pasul 4. $a_4 = 30$ și $b_4 = 17 \Rightarrow a_5 = |a_4 - b_4| = |30 - 17| = 13$ și $b_5 = \min\{17, 30\}$
$= 17$
Pasul 5. $a_5 = 13$ și $b_5 = 17 \Rightarrow a_6 = |a_5 - b_5| = |13 - 17| = 4$ și $b_6 = \min\{a_5, b_5\}$
$= \min\{13, 17\} = 13$.
Pasul 6. $a_6 = 4$ și $b_4 = 13 \Rightarrow a_7 = |a_6 - b_6| = |4 - 13| = 9$ și $b_7 = \min\{a_6, b_6\} =$
$= \min\{4, 13\} = 4$.
Pasul 7. $a_7 = 9$ și $b_7 = 4 \Rightarrow a_8 = |a_7 - b_7| = |9 - 4| = 5$ și $b_8 = \min\{a_7, b_7\}$
$= \min\{9, 4\} = 4$.
Pasul 8. $a_8 = 5$ și $b_8 = 4 \Rightarrow a_9 = |a_8 - b_8| = |5 - 4| = 1$ și $b_9 = \min\{a_8, b_8\}$
$= \min\{5, 4\} = 4$.
Pasul 9. $a_9 = 1$, $b_9 = 4 \Rightarrow a_{10} = |a_9 - b_9| = |1 - 4| = 3$ și $b_{10} = \min\{a_9, b_9\}$
$= \min\{1, 4\} = 1$.
Pasul 10. $a_{10} = 3$ și $b_{10} = 1 \Rightarrow a_{11} = |a_{10} - b_{10}| = |3 - 1| = 2$ și $b_{11} = \min\{a_{10}, b_{10}\}$
$= \min\{3, 1\} = 1$.
Pasul 11. $a_{11} = 2$ și $b_{11} = 1 \Rightarrow a_{12} = |a_{11} - b_{11}| = |2 - 1| = 1$ și $b_{12} = \min\{a_{11}, b_{11}\}$
$= \min\{2, 1\} = 1$.
Cum $a_{12} = b_{12} = 1 \Rightarrow \text{cmmdc}(81, 64) = \text{cmmdc}(a_{12}, b_{12}) = 1$.

Temă: 1) Să se determine cmmdc (18, 12), utilizând algoritmul lui Euclid, varianta cu scăderi repetate.
2) Să se determine cmmdc (20, 30), utilizând algoritmul lui Euclid, varianta cu scăderi repetate.
3) Să se determine cmmdc (54, 24), utilizând algoritmul lui Euclid, varianta cu scăderi repetate.

Probleme rezolvate: 1) Să se demonstreze că pentru orice număr natural n fracția $\frac{21n+4}{14n+3}$ este ireductibilă.

Soluție: Este suficient să demonstrăm că $\text{cmmdc}(21n+4, 14n+3) = 1$.
Deci, $\text{cmmdc}(21n+4, 14n+3) = \text{cmmdc}(21n+4-(14n+3), 14n+3)$
$= \text{cmmdc}(7n+1, 14n+3) = \text{cmmdc}(7n+1, 14n+3-2(7n+1)) =$
$= \text{cmmdc}(7n+1, 1) = 1$.

2) Fie $n, p > 1$ numere întregi pozitive și p un număr prim. Știm că $n \mid p-1$ și $p \mid n^3-1$. Să se demonstreze că $4p-3$ este pătrat perfect.

VitoriOlimpici.ro

Soluție: Din $n \mid p-1 \Rightarrow (\exists)\ K \in \mathbb{Z}$ astfel încât $p-1 = nK \Leftrightarrow p = nK+1$. Din $n \mid p-1$ deducem că $p-1 \geq n \Leftrightarrow p \geq n+1$. De aici rezultă că cmmdc $(p, n-1) = 1$, deoarece p este număr prim. Din $p \mid n^3-1 = (n-1)(n^2+n+1)$ și din cmmdc $(p, n-1) = 1 \Rightarrow p \mid n^2+n+1 \quad | \cdot K$

$\Rightarrow p \mid Kn^2+Kn+K,\ K \in \mathbb{Z}$ și $p = nK+1$

$\Rightarrow nK+1 \mid Kn^2+Kn+K$.

Acum, cmmdc $(nK+1, Kn^2+Kn+n) =$ cmmdc $(nK+1, Kn^2+Kn+K-n(nK+1))$ $=$ cmmdc $(nK+1, Kn+K-n)$.

Cum $nK+1 \mid Kn^2+Kn+K \Rightarrow nK+1 \mid$ cmmdc $(nK+1, Kn^2+Kn+K)$ și astfel: $nK+1 \mid nK+K-n$

Aceasta înseamnă că $Kn+K-n = 0$ sau $Kn+K-n \geq nK+1 \Leftrightarrow K-n \geq 1$.

Prima relație este imposibilă, deoarece ar rezulta că $K(n+1) = n \Leftrightarrow K = \frac{n}{n+1} \in \mathbb{Z}$, imposibil când $n \in \mathbb{N}$ și $n \geq 1 \Rightarrow K-n \geq 1$. De asemenea, din $p = nK+1$ și $p \mid n^2+n+1 \Rightarrow nK+1 \leq n^2+n+1 \Rightarrow K \leq n+1 \Rightarrow K = n+1$

$\Rightarrow p = Kn+1 = (n+1)n+1 = n^2+n+1$.

Astfel, $4p-3 = 4(n^2+n+1)-3 = (2n+1)^2 =$ pătrat perfect q.e.d

Teorema 2 (Algoritmul lui Euclid, varianta cu împărțiri repetate):

Pornind de la numerele întregi pozitive a și b se poate obține cmmdc (a, b) efectuând următorii pași

1. Dacă $a < b$, atunci a se interschimbă cu b.
2. a se împarte la b obținându-se restul r. Dacă $r = 0$, atunci cmmdc $(a, b) = b$.
3. a ia valoarea lui b, iar b ia valoarea lui r. Se repetă pasul 1.

Demonstrație: Mai întâi vom demonstra că dacă $a, b, q, r \in \mathbb{Z}$ și $a = bq+r$, atunci cmmdc $(a, b) =$ cmmdc (b, r).

Fie $d =$ cmmdc (a, b) și $d_1 =$ cmmdc (b, r). Din $d \mid a \Rightarrow d \mid bq+r$. Dar $d \mid b \Rightarrow d \mid bq \Rightarrow d \mid bq+r-bq = r$. Din $d \mid b$ și $d \mid r \Rightarrow d \mid d_1$.

Din $d_1 \mid b$ și $d_1 \mid r \Rightarrow d_1 \mid bq+r = a$. Din $d_1 \mid b$ și $d \mid a \Rightarrow d_1 \mid d$

$\Rightarrow d = d_1 \Leftrightarrow$ cmmdc $(a, b) =$ cmmdc (b, r).

În continuare vom scrie pași prin care se obține cmmdc (a, b)

$a = bq_1 + r_1$, cmmdc $(a, b) =$ cmmdc (b, r_1)

$b = r_1 q_2 + r_2$, cmmdc $(b, r_1) =$ cmmdc (r_1, r_2)

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

$r_{n-1} = r_n q_{n+1}$, $cmmdc(r_{n-1}, r_n) = r_n$.

Prin urmare, rezultă că: $cmmdc(a,b) = cmmdc(b, r_1) = \ldots =$

$= cmmdc(r_{n-1}, r_n) = r_n$.

Exerciții explicate:

1. Să se determine $cmmdc(50,80)$, utilizând algoritmul lui Euclid, varianta cu scăderi repetate.

Rezolvare: Aplicăm algoritmul lui Euclid, varianta cu împărțiri repetate asupra numerelor 50 și 80. Notăm $a=50$ și $b=80$. Cum $a<b$, interschimbăm numerele a și b obținând noile valori $a=80$ și $b=50$.

$80 = 1 \cdot 50 + 30$
$50 = 1 \cdot 30 + 20$
$30 = 1 \cdot 20 + 10$
$20 = 2 \cdot 10 + 0$

Cum 10 este ultimul rest diferit de 0 $\Rightarrow cmmdc(50,80) = 10$.

2. Să se determine $cmmdc(81,64)$, utilizând algoritmul lui Euclid, varianta cu împărțiri repetate.

Rezolvare: Aplicăm algoritmul lui Euclid, varianta cu împărțiri repetate asupra numerelor 81 și 64. Notăm $a=81$ și $b=64$. Cum $a>b$, avem:

$81 = 1 \cdot 64 + 17$
$64 = 3 \cdot 17 + 13$
$17 = 1 \cdot 13 + 4$
$13 = 3 \cdot 4 + 1$
$4 = 4 \cdot 1 + 0$

Cel mai mare divizor comun este ultimul rest diferit de 0, adică 1.

Temă: 1) Să se determine $(18,12)$, utilizând algoritmul lui Euclid, varianta cu împărțiri repetate.

2) Să se determine $cmmdc(20,30)$, utilizând algoritmul lui Euclid, varianta cu împărțiri repetate.

3) Să se determine $cmmdc(54,24)$, utilizând algoritmul lui Euclid, varianta cu împărțiri repetate.

Problemă rezolvată: Să se determine cel mai mare divizor comun d al numerelor $a=1079$ și $b=741$ și să se găsească numerele întregi x și y astfel încât $xa+yb=d$.

Soluție: Pentru determinarea celui mai mare divizor comun d al numerelor a și b vom folosi algoritmul lui Euclid, varianta cu împărțiri

$1079 = 1 \cdot 741 + 338$
$741 = 2 \cdot 338 + 65$
$338 = 5 \cdot 65 + 13$
$65 = 5 \cdot 13 + 0$.

Cel mai mare divizor comun este ultimul rest diferit de 0, în acest caz 13. Pentru determinarea lui x și y vom parcurge ecuațiile în ordine inversă, substituind resturile și colectând termenii pe măsură ce facem aceste operații:

$$13 = 338 - 5 \cdot 65 = 338 - 5(741 - 2 \cdot 338) = 11 \cdot 338 - 5 \cdot 741 = 11(1079 - 741) - 5 \cdot 741 = 11 \cdot 1079 - 16 \cdot 741.$$

Am obținut faptul că:

$$11 \cdot 1079 - 16 \cdot 741 = 13.$$

Deci numerele $x = 11$ și $y = -16$ îndeplinesc relația $xa + yb = d$.

Corolarul 1 (Primul Corolar al algoritmului lui Euclid):

Pentru fiecare $a, b \in \mathbb{N}^*$ există $x, y \in \mathbb{Z}$ astfel încât $ax + by = \text{cmmdc}(a, b)$. Numărul $\text{cmmdc}(a, b)$ este cel mai mic întreg pozitiv pentru care astfel de x și y pot fi găsiți.

Demonstrație: Fie d cel mai mic întreg pozitiv care este o combinație liniară de a și b. Aceasta înseamnă că există întregii x și y astfel încât:

$$d = ax + by$$

Vom demonstra că $d \mid a$. Împărțind a la d rezultă că există numerele întregi q și r cu $0 \leq r < d$ astfel încât:

$$a = dq + r$$

Din $d = ax + by \Rightarrow r = a - dq \Rightarrow r = a - q(ax + by) \Rightarrow r = a - qax - qyb \Rightarrow r = (1 - qx)a + (-qy)b$.

Această relație implică faptul că r este o combinație liniară de a și b. Datorită faptului că $0 \leq r < d$ și că d este cel mai mic întreg pozitiv care poate fi scris ca o combinație liniară de a și b, deducem că $r = 0 \Rightarrow d \mid a$. Analog se demonstrează că $d \mid b$.

Rămâne să demonstrăm că d este cel mai mare divizor comun al numerelor a și b. Până acum am demonstrat că d este un divizor comun al numerelor a și b. Presupunem prin absurd că există $d' > d$ astfel încât $\text{cmmdc}(a, b) = d'$. Din relațiile $d' \mid a$ și $d' \mid b$ și $d = ax + by \Rightarrow d' \mid d \Rightarrow d' \leq d$, contradicție. Astfel d este cel mai mare divizor comun al numerelor a și b și cel mai mic întreg pozitiv care este o combinație liniară de a și b.

Exerciții explicate:

1) Să se precizeze dacă există numerele întregi x și y astfel încât $47x + 3y = 1$. În cazul în care există, să se dea un exemplu de astfel de numere.

Rezolvare: Din Primul Corolar al algoritmului lui Euclid rezultă că cel mai mic număr natural nenul n pentru care există $x, y \in \mathbb{Z}$ astfel încât $4x+3y=n$ este $n = \text{cmmdc}(4,3) = 1$. În consecință, există x și y astfel încât $4x+3y=1$. Două astfel de numere sunt $x=1, y=-1$

2) Să se precizeze dacă există numerele întregi x și y astfel încât $4x+2y=1$. În cazul în care există, să se dea un exemplu de astfel de numere.

Rezolvare: Din Primul Corolar al algoritmului lui Euclid rezultă că cel mai mic număr natural nenul n pentru care există x și y astfel încât $4x+2y=n$ este $n = \text{cmmdc}(4,2) = 2 > 1$. De aici rezultă că nu există $x, y \in \mathbb{Z}$ astfel încât $4x+2y=1$.

Temă: 1) Să se precizeze dacă există numerele întregi x și y astfel încât $27x+81y=27$. În cazul în care există, să se dea un exemplu de astfel de numere.

2) Să se precizeze dacă există numerele întregi x și y astfel încât $36x+216y=6$. În cazul în care există, să se dea un exemplu de astfel de numere.

3) Să se precizeze dacă există numerele întregi x și y astfel încât $125x+256y=1$. În cazul în care există, să se dea un exemplu de astfel de numere.

Probleme rezolvate:

1) Fie $m, n, s \in \mathbb{Z}$ astfel încât $m \mid ns$ și $\text{cmmdc}(m,n)=1$. Să se arate că $m \mid s$.

Soluție: Din Primul Corolar al algoritmului lui Euclid rezultă că există numerele întregi x și y astfel încât:

$$msx + nsy = \text{cmmdc}(m,n) = 1.$$

Înmulțind această relație cu s, rezultă că:

$$msx + nsy = s$$

Din $m \mid msx$ și $m \mid ns \Rightarrow m \mid snsy \Rightarrow m \mid msx + nsy$

$\Rightarrow m \mid s$ q.e.d.

2) Fie p și q două numere prime între ele. Demonstrați că există un singur număr întreg x care satisface simultan relațiile $x \equiv a \pmod p$ și $x \equiv b \pmod q$. (x este unic în modulo pq)

(Teorema chineză a resturilor)

Soluție: Din $\text{cmmdc}(p,q)=1$ și din Primul Corolar al algoritmului lui Euclid rezultă că există numerele întregi px și qy astfel încât:

$$pqx + qpy = 1$$

$\Rightarrow pq_x - 1 = -qy \Rightarrow pq_x \equiv 1 \pmod q$

Fie r_1 restul împărțirii lui q_x la $q \Rightarrow (\exists)\ k \in \mathbb{Z}$ astfel încât $q_x = qk + r_1$, $r \in \{0, 1, 2, \dots, q-1\}$. Din $pq_x \equiv 1 \pmod q \Rightarrow p(qk + r_1) \equiv 1 \pmod q$. Această relație se poate scrie sub forma echivalentă:

$$q \mid pqk + pr_1 - 1$$

Din $q \mid pqk \Rightarrow q \mid pr_1 - 1 \Leftrightarrow pr_1 \equiv 1 \pmod q$

Numărul r_1 cu proprietățile $r_1 \in \{0, 1, \dots, q-1\}$ și $pr_1 \equiv 1 \pmod q$ este inversul lui p modulo q și se notează sub forma:

$$r_1 = p^{-1} \pmod q$$

Asemănător se demonstrează că există numărul q_1 care este inversul lui q modulo p. Acest lucru se notează sub forma:

$$q_1 = q^{-1} \pmod p$$

Vom demonstra că $x = aqq_1 + bpr_1 \pmod{pq}$ satisface ambele ecuații: $\begin{cases} x \equiv aqq_1 + bpr_1 \equiv a \pmod p \\ x \equiv aqq_1 + bpr_1 \equiv b \pmod q \end{cases}$ evident.

În continuare demonstrăm că x este unic modulo pq. Presupunem prin reducere la absurd că mai există un număr întreg $x' \neq x$ din mulțimea $\{0, 1, \dots, pq-1\}$ astfel încât:

$$\begin{cases} x' \equiv a \pmod p \\ x' \equiv b \pmod q \end{cases}$$

Din $x \equiv a \pmod p$ și $x' \equiv a \pmod p \Rightarrow x - x' \equiv 0 \pmod p$. Analog, $x - x' \equiv 0 \pmod p$. Cum $(p, q) = 1 \Rightarrow x - x' \equiv 0 \pmod{pq} \Leftrightarrow x \equiv x' \pmod{pq}$

Cum $x, x' \in \{0, 1, 2, \dots, pq-1\}$ și $x \equiv x' \pmod{pq} \Rightarrow x = x'$, contradicție și cu aceasta problema este încheiată.

<u>Corolarul 2</u> (Al Doilea Corolar al algoritmului lui Euclid):

Pentru $a, m, n \in \mathbb{N}$ și $a > 1$ rezultă că:

$$\text{cmmdc}(a^m - 1, a^n - 1) = a^{\text{cmmdc}(m,n)} - 1.$$

<u>Demonstrație:</u> Dacă $m > n$, atunci:

$$\text{cmmdc}(a^n - 1, a^m - 1) = \text{cmmdc}(a^n - 1, a^m - 1 - a^{m-n}(a^n - 1)) =$$
$$= \text{cmmdc}(a^n - 1, a^{m-n} - 1).$$

Folosind aceeași procedură ca și în cazul Algoritmului lui Euclid, varianta cu scăderi repetate, pentru a demonstra că $\text{cmmdc}(m, n) = d$ rezultă că: $\text{cmmdc}(a^m - 1, a^n - 1) = a^d - 1$

<u>Exerciții explicate:</u>

1) Să se determine $\text{cmmdc}(2^6 - 1, 2^4 - 1)$

Rezolvare: Din al Doilea Corolar al algoritmului lui Euclid rezultă că: $\text{cmmdc}(2^6 - 1, 2^4 - 1) = 2^{\text{cmmdc}(6,4)} - 1 = 2^2 - 1 = 3$.

2) Să se determine $cmmdc(3^{18}-1, 3^{16}-1)$.

Rezolvare: Din al Doilea Corolar al algoritmului lui Euclid rezultă că: $cmmdc(3^{18}-1, 3^{16}-1) = 3^{cmmdc(18,16)}-1 = 3^2-1 = 8$.

Temă: 1) Să se determine $cmmdc(5^{20}-1, 5^{30}-1)$.

2) Să se determine $cmmdc(7^{35}-1, 7^{25}-1)$.

3) Să se determine $cmmdc(11^{14}-1, 11^{49}-1)$.

Problemă rezolvată: Cel mai mare divizor comun al numerelor $3^{50^{36}}-3$ și $3^{50^{30}}-3$ poate fi exprimat sub forma 3^x-3. Să se determine x.

Soluție: Din al Doilea Corolar al algoritmului lui Euclid rezultă că:

$cmmdc(3^{50^{36}}-3, 3^{50^{30}}-3) = 3\cdot[3^{cmmdc(50^{36}-1, 50^{30}-1)}-1]$

$\Rightarrow cmmdc(3^{50^{36}}-3, 3^{50^{30}}-3) = 3\cdot[3^{50^{cmmdc(50,30)}-1}-1] = 3(3^{50^6-1}-1)$

$\Rightarrow cmmdc(3^{50^{36}}-3, 3^{50^{30}}-3) = 3^{50^6}-3$

$\Rightarrow x = 50^6$.

Deși pare o metodă mai complicată și mai inutilă de aflare a celui mai mare divizor comun a două numere, algoritmul lui Euclid se dovedește a fi mai folositor în rezolvarea mai multor ecuații liniare diofantice, cum ar fi teorema chineză a resturilor (demonstrată anterior). În continuare, vom evidenția această idee prin două exerciții explicate:

1) Să se determine o soluție a sistemului de ecuații:

$$\begin{cases} x \equiv 2 \pmod{13} \\ x \equiv 3 \pmod{17} \end{cases}$$

Soluție: Mai întâi trebuie determinate numerele $13^{-1} \pmod{17}$ și $17^{-1} \pmod{13}$. Pentru aceasta putem utiliza Algoritmul lui Euclid. Începem cu calculul numărului $13^{-1} \pmod{17}$:

$17 = 13\cdot 1 + 4$

$13 = 4\cdot 3 + 1$

Astfel, numărul 1 poate fi scris sub forma: $1 = 13 - 4\cdot 3 = 13 - 3\cdot(17 - 13\cdot 1) = 13\cdot 4 - 3\cdot 17 \Rightarrow 17 \mid 13\cdot 4 - 1 \Leftrightarrow 13\cdot 4 \equiv 1 \pmod{17} \Rightarrow 13^{-1} \pmod{17} = 4$.

Folosind relația $1 = 13\cdot 4 - 3\cdot 17$ deducem asemenea că $13 \mid (-3)\cdot 17 - 1 \Leftrightarrow (-3)\cdot 17 \equiv 1 \pmod{13} \Rightarrow 17^{-1} \pmod{13} = -3$.

Conform Teoremei chineze a resturilor, rezultă că singura soluție pentru x modulo $13\cdot 17$ este:

$x = 2\cdot 17\cdot(-3) + 3\cdot 13\cdot 4 \pmod{13\cdot 17} \Leftrightarrow x = -102 + 156 \pmod{221}$

$\Leftrightarrow x = 54$

$\Rightarrow x = 54$ este o soluție a sistemului de ecuații dat.

2) Să se determine o soluție a sistemului de ecuații:

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

Soluție: Mai întâi trebuie determinate numerele $5^{-1} \pmod 7$ și $7^{-1} \pmod 5$. Pentru aceasta putem utiliza Algoritmul lui Euclid. Începem cu calculul $5^{-1} \pmod 7$:

$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$

Astfel, numărul 1 poate fi scris sub forma: $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5 \cdot 1) = 5 \cdot 3 - 2 \cdot 7 \Rightarrow 7 \mid 5 \cdot 3 - 1 \Leftrightarrow 5 \cdot 3 \equiv 1 \pmod 7 \Rightarrow 5^{-1} \pmod 7 = 3$.

Folosind relația $1 = 5 \cdot 3 - 2 \cdot 7 \Rightarrow 5 \mid (-2) \cdot 7 - 1 \Leftrightarrow (-2) \cdot 7 \equiv 1 \pmod 5$

$\Rightarrow 7^{-1} \pmod 5 = -2$.

Folosind Teorema chineză a resturilor, rezultă că singura soluție pentru x modulo $5 \cdot 7$ este:

$$x = 2 \cdot 7 \cdot (-2) + 3 \cdot 5 \cdot 3 \pmod{35} \Leftrightarrow x = -28 + 45 \pmod{35} \Leftrightarrow x = 17$$

$\Rightarrow x = 17$ este o soluție a sistemului de ecuații dat.

Temă: 1) Să se determine o soluție a sistemului de ecuații:

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod 9 \end{cases}.$$

2) Să se determine o soluție a sistemului de ecuații:

$$\begin{cases} x \equiv 7 \pmod{17} \\ x \equiv 5 \pmod{19} \end{cases}.$$

3) Să se determine o soluție a sistemului de ecuații:

$$\begin{cases} x \equiv 5 \pmod{100} \\ x \equiv 7 \pmod{101} \end{cases}.$$

Bibliografie:

- Magdaș Camelia, Moldovan Dorin – „Introducere în teoria numerelor", Gil.
- www.viitorolimpici.ro

Mihăescu Răzvan
Clasa a VIII-a
C.N. „Gh. Țițeica"
Dr. Tr. Severin, Prof. Streteu Daniel