Ecuatii Congruentiale

O ecuaţie congruenţiala liniara, de necunoscuta x, este o ecuatie de forma

(1) $ax \equiv b \bmod m$ unde $a, b \in \mathbf{Z}$

<=> $ax - b \equiv 0 \bmod m$ <=> m / $ax - b$ <=> exista y astfel incat $ax - b = my$

<=> $ax + (-m)y = b$

(1) se reduce la a determina o pereche (x, y) de numere întregi astfel încât

$$ax + (-m)y = b$$

(1) are solutie <=> (a,m) / b

Teorema 1. Fie $a, b, m \in \mathbf{Z}$ cu $m \geq 2$. Atunci, ecuatia $ax \equiv b \bmod m$ are solutii in **Z** daca si numai daca $(a, m) \mid b$. In plus, daca ecuatia are solutii, atunci ea are exact (a, m) solutii in $\mathbf{Z}_m$ de forma

$$x_i = (x_0 + im/(a, m)) \bmod m,$$

unde x_0 este o soluţie (arbitrară dar fixată) a acestei ecuaţii şi $0 \leq i < (a, m)$.

Exercitiul 1 Rezolvati ecuatiile:

a) $5x \equiv 25 \bmod 10$;

a = 5, b = 25, m = 10 (5, 10) = 5 | 25 => ecuatia are (5, 10) = 5 solutii in $\mathbf{Z}_{10} = \{0,1,2,...,9\}$

$5x \equiv 25 \bmod 10$ <=> $5x - 25 \equiv 0 \bmod 10$ => $10 \mid 5x - 25$ => $x_0 = 1$ deci

$x_0 = 1$
$x_1 = (1 + 10/5) \bmod 10 = 3$
$x_2 = (1 + 20/5) \bmod 10 = 5$
$x_3 = (1 + 30/5) \bmod 10 = 7$
$x_4 = (1 + 40/5) \bmod 10 = 9$

b) $35x \equiv 2 \bmod 3$;

a = 35, b = 2, m = 3 (35, 3) = 1 | 2 => ecuatia are o solutie in $\mathbf{Z}_3 = \{0,1,2\}$

$35x - 2 \equiv 0 \bmod 3$; $x_0 = 1$

c) $21x \equiv 3 \bmod 5$

a = 21, b = 3, m = 5 (21, 5) = 1 => ecuatia are o solutie in $\mathbf{Z}_5 = \{0,1,2,3,4\}$

$21x - 3 \equiv 0 \bmod 5$; $x_0 = 3$

d) $15x \equiv 2 \bmod 7$

$a = 15, b = 2, m = 7$ $(15,7) = 1 \Rightarrow$ ecuatia are o solutie in $\mathbf{Z}_7 = \{0,1,2,3,..., 6\}$
$x_0 = 2$

e) $14x \equiv 6 \bmod 18$;

$a = 14, b = 6, m = 18$ $(14,18) = 2 \Rightarrow$ ecuatia are 2 solutii in $\mathbf{Z}_{18} = \{0,1,2,..., 17\}$
$x_0 = 3$,

$$x_i = (x_0 + im/(a, m)) \bmod m,$$

$x_1 = (3 + 18/2) \bmod 18 = 12$

Observatie: $x_2 = (3 + 36/2) \bmod 18 = 3 = x_0$

f) $25x \equiv 15 \bmod 40$;

$a = 25, b = 15, m = 40$ $(25,40) = 5 \Rightarrow$ ecuatia are 5 solutii in $\mathbf{Z}_{40} = \{0,1,2,...,39\}$
$x_0 = 7$,

$x_1 = (7 + 40/5) \bmod 40 = 15$
$x_2 = (7 + 80/5) \bmod 40 = 23$
$x_3 = (7 + 120/5) \bmod 40 = 31$
$x_4 = (7 + 160/5) \bmod 40 = 39$

g) $18x \equiv 12 \bmod 42$;

$a = 18, b = 12, m = 42$ $(18,42) = 6 \Rightarrow$ ecuatia are 6 solutii in $\mathbf{Z}_{42} = \{0,1,2,...,41\}$
$x_0 = 3$

$x_1 = (3+ 42/6) \bmod 42 = 10$
$x_2 = (3 + 84/6) \bmod 42 = 17$
$x_3 = (3 + 126/6) \bmod 42 = 24$
$x_4 = (3 + 168/6) \bmod 42 = 31$
$x_5 = (3 + 210/6) \bmod 42 = 38$

Teorema chineză a resturilor

Teorema 2 (Teorema chineza a resturilor). Fie $k \in N$, $m_1, \ldots, m_k$ numere relativ prime ıntre ele. Atunci, pentru orice $b_1, \ldots, b_k \in Z$, urmatorul sistem de ecuatii are o unica solutie modulo $m = m_1 \cdot m_2 \cdot \cdot \cdot m_k$:

$x \equiv b_1 \bmod m_1$
$x \equiv b_2 \bmod m_2$
. . .
$x \equiv b_k \bmod m_k$

Solutia este obtinuta astfel:

1) Se calculeaza $m = m_1 \cdot \cdot \cdot m_k,$ si $c_i = m/m_i = m_1 \cdot \cdot \cdot m_{i-1}m_{i+1} \cdot \cdot \cdot m_k$
2) Se calculeaza o solutie x_i a ecuatiei $c_i\, x \equiv b_i \bmod m_i$, pentru fiecare i
3) Se calculeaza solutia $x = (c_1x_1 + . . . + c_kx_k) \bmod m$

Exercitiul 2.

Rezolvati sistemul:
$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 5$
$x \equiv 2 \bmod 7$

1) $m = m_1\, m_2\, m_3 = 3{\cdot}5{\cdot}7{=}105$

2) $c_1 = 35,\quad c_2 = 21,\quad c_3 = 15$

$35\, x \equiv 2 \bmod 3,\quad x_1 = 1,$

$21\, x \equiv 3 \bmod 5,\quad x_2 = 3,$

$15\, x \equiv 2 \bmod 7,\quad x_3 = 2,$

$x = (35 + 63 + 30) \bmod 105 = 23$

Exercitiul 3.

Rezolvati sistemul:

$x \equiv 1 \bmod 4$
$x \equiv 2 \bmod 9$
$x \equiv 3 \bmod 11$
$x \equiv 11 \bmod 13$

m = 5148, c1 = 1287, c2 = 572, c3 = 468, c4 = 396,
x1 = 3, x2 = 4, x3 = 6, x4 = 4, x = 245

Exercitiul 4.

Rezolvati sistemul:

$x \equiv 2 \bmod 5$
$x \equiv 1 \bmod 2$
$x \equiv 2 \bmod 3$

1) $m = m_1\, m_2\, m_3 = 5 \cdot 2 \cdot 3 = 30$

$c_1 = 6, \quad c_2 = 15, \quad c_3 = 10$

$6\, x \equiv 2 \bmod 5, \quad x_1 = 2,$

$15\, x \equiv 1 \bmod 2, \quad x_2 = 1,$

$10\, x \equiv 2 \bmod 3, \quad x_3 = 2,$

$x = (12 + 15 + 20) \bmod 30 = 47 \bmod 30 = 17$

Exercitiul 5.

Rezolvati sistemul:
$x \equiv 4 \bmod 3$
$x \equiv 6 \bmod 11$
$x \equiv 2 \bmod 5$

1) $m = m_1\, m_2\, m_3 = 3 \cdot 11 \cdot 5 = 165$

2) $c_1 = 55, \quad c_2 = 15, \quad c_3 = 33$

$55x \equiv 4 \bmod 3, \quad x_1 = 1,$

$15\, x \equiv 6 \bmod 11, \quad x_2 = 7,$

$33\, x \equiv 2 \bmod 5, \quad x_3 = 4,$

$x = (55 + 105 + 132) \bmod 165 = 127$

Exercitiul 6.

Rezolvati sistemul:
$x \equiv 3 \bmod 4$
$x \equiv 1 \bmod 5$
$x \equiv 2 \bmod 3$

1) $m = m_1\, m_2\, m_3 = 3 \cdot 4 \cdot 5 = 60$
2) $c_1 = 15, \quad c_2 = 12, \quad c_3 = 20$

$15x \equiv 3 \bmod 4, \quad x_1 = 1,$

$12x \equiv 1 \bmod 5, \quad x_1 = 3,$

$20x \equiv 2 \bmod 3, \quad x_1 = 1,$

$x = (15 + 36 + 20) \bmod 60 = 11$

Reziduuri patratice

Definitia 1. Fie p un numar prim, $p > 2$, $a \in \mathbf{Z}$, ai. p nu divide a. a se numeste *rest quadratic modulo p* (reziduu patratic modulo p) daca ecuatia $x^2 \equiv a \bmod p$ are cel putin o solutie.

Daca p nu divide a si a nu este reziduu patratic modulo p, atunci a se numeste non-reziduu patratic modulo p.

Exemple.
1. 8 este rest quadratic modulo 17 deoarece ecuatia $x^2 \equiv 8 \bmod 17$ are solutia $x = 5$.

2. 2 si 4 sunt resturi quadratice modulo 7 deoarece ecuatia $x^2 \equiv 2 \bmod 7$ are solutia $x = 3$ si ecuatia $x^2 \equiv 4 \bmod 7$ are solutia $x = 5$.

3. Este 3 rest quadratice modulo 5? Nu, ecuatia $x^2 \equiv 3 \bmod 5$ nu are solutie in Z_5.

Simbolul Legendre

Definitia 2. Fie $a \in \mathbf{Z}$, p un numar prim, $p > 2$, se defineste simbolul lui Legendre al numarului **a** relativ la numarul prim **p**, notat **(a/p)** numarul

$$(a/p) = \begin{cases} 0, & \text{daca p divide a,} \\ 1, & \text{daca p nu divide a si a este rest quadratic modulo p,} \\ -1, & \text{daca p nu divide a si a nu este rest quadratic modulo p;} \end{cases}$$

Reguli de calcul si Proprietatile simbolului lui Legendre.

1. $a \equiv_p b$ atunci $(a/p) = (b/p)$

2. $(ab/p) = (a/p)(b/p)$

3. $(a/p) = (a \bmod p/p)$

4. (1/p) = 1 pentru orice numar prim p.

Exercitiul 7.

Fie p un număr prim. Ecuaţia $x^2 \equiv 1 \bmod p$ are exact 2 soluţii în $\mathbf{Z}_p$, şi anume
x = 1 şi x = p − 1. In adevăr,

$$
\begin{aligned}
x^2 \equiv 1 \bmod p &\Leftrightarrow p|x^2 - 1\\
&\Leftrightarrow p|(x-1)(x+1)\\
&\Leftrightarrow p|x-1 \text{ sau } p|x+1\\
&\Leftrightarrow x \equiv 1 \bmod p \text{ sau } x \equiv -1 \bmod p.
\end{aligned}
$$

4. $(a/p) = a^{(p-1)/2} \bmod p$

5. $(2/p) = (-1)^{(p\char`^2 -1)/8}$

6. (Teorema reciprocitatii) Fie p, q doua numere prime distincte, p,q > 2, atunci

$$(q/p)(p/q) = (-1)^{(p-1)/2(q-1)/2} = (-1)^{(p-1)(q-1)/4}$$

Exercitiul 8.

Calculati simbolurile lui Legendre pentru

1. (7/5)

(7/5) = -1 deoarece ecuatia ecuatia $x^2 \equiv 7 \bmod 5$ nu are solutie in $\mathbf{Z}_5=\{0,1,2,3,4\}$

2. (4/5) = (2/5)(2/5) = 1; Obs. (2/5) = -1

3. (9/5) = (3/5)(3/5) = 1; Obs. (3/5) = -1

4. (19/5) = (19 mod 5/5) = (4/5) = 1

5. (21/5) = (21 mod 5/5) = (1/5) = 1

6. (102/37) = (102 mod 37/37) = (28/37) = (4/37) (7/37) = 1(7/37) aplicam Th de reciprocitate p = 7, q = 37

$(7/37)(37/7) = (-1)^{(p-1)/2(q-1)/2}$ = + 1 => (7/37) = (37/7) = (37mod 7/7) = (2/7) = 1

deci (102/37) = 1.

7. (3/103) = aplicam Th de reciprocitate p = 3, q = 103

(3/103)(103/3) = $(-1)^{(p-1)/2(q-1)/2}$ = -1 => (3/103) = - (103/3)

(103/3) = (103 mod 3/3) = (1/3) = 1 => (3/103) = - 1.

8. (2015/41) = (2015 mod 41/41) = (6/41) = (2/41)(3/41)

(2/41) = 1,

(3/41)(41/3) = +1 (Teorema de reciprocitate) => (3/41) = (41/3) = (41 mod 3/3) = (2/3) = -1

(2/3) = - 1, deci (2015/41) = -1

(2/p) = $(-1)^{(p\char`^2 -1)/8}$ => (2/41) = 1 si (2/3) = - 1

9. (2055/41) = (2055 mod 41/41) = (5/41) (Teorema de reciprocitate)

(5/41) (41/5) = $(-1)^{2.20}$ = 1 deci

(5/41) = (41/5) = (1/5) = 1

Simbolul Jacobi
Fie a $\in \mathbf{Z}$ si n > 0 un numar impar, se defineste simbolul lui Jacobi al numarului a, notat (a/n) numarul

$$(a/n) = \begin{cases} 1, \text{ daca } n = 1 \\ (a/n_1)^{e1}(a/n_2)^{e2} \ldots (a/n_k)^{ek} \end{cases}$$

unde $n = n_1^{e_1} n_2^{e_2} \ldots n_k^{e_k}$ este descompunerea lui n in produs de puteri de factori primi.

Exercitiul 9.

Calculati simbolurile lui Jacobi pentru

1. (15/81)= (15/3)^4= 0

2. (294/105) = (294/5) (294/3) (294/7) = 0

3. (35/531) = (35/3)^2 (35/59) = (5/59) (7/59) = 1
deoarece

(35/3)^2 = 1

(5/59) (59/5) = 1 => (5/59) = (59/5) = (4/5) = 1

(7/59) (59/7) = -1 => (7/59) = - (59/7) = - (3/7) = 1

Functia lui Euler

Reamintim că $\mathbf{Z}_m^* = \{a \in \mathbf{Z}_m | (a, m) = 1\}$, pentru orice $m \geq 1$. Funcţia φ ce asociază fiecărui număr $m \geq 1$ cardinalul mulţimii $\mathbf{Z}_m^*$ este numită *funcţia lui Euler*.

Proprietati 1. $\varphi(1) = 1$ şi $\varphi(p) = p\text{-}1$, pentru orice număr prim p.

2. $\varphi(ab) = \varphi(a)\varphi(b)$, pentru orice $a, b \geq 1$ prime intre ele;

3. $\varphi(p^e) = (p^e - p^{e-1})$

2. Dacă a este un număr natural a cărui descompunere în factori primi este $a = p^{e1} p^{e2} \ldots p^{e_n}$, atunci $\varphi(a) = (p^{e1} - p^{e1-1})(p^{e2} - p^{e2-1}) \ldots (p^{e_n} - p^{e_n-1})$

Teorema lui Euler

Fie $m \geq 1$. Atunci, $a^{\varphi(m)} \equiv 1 \; mod \; m$, pentru orice $a \in \mathbf{Z}_m^*$.

Consecinta Fie $m \geq 1$. Atunci $a^{\varphi(m)} \equiv 1$ mod m, pentru orice $a \in Z$ cu $(a, m)= 1$.

Teorema lui Fermat

Daca p este un numar prim, $p \geq 2$, atunci

1. $a^{p-1} \equiv 1$ mod p pentru orice $a \in Z$ cu p nu divide a
2. $a^p \equiv a$ mod p pentru orice $a \in Z$.