R: $x_1 = \frac{-7+17x_4}{11}$; $x_2 = \frac{5-20x_4}{11}$; $x_3 = \frac{3+32x_4}{11}$

$x_4 \in R$

Tema; Elemente din teoria divizibilităţii în inelul numerelor întregi

§ 1. Noţiunea de divizibilitate în inelul nr. întregi. Proprietăţi. Teorema împărţirii cu rest.

Fie $(Z, +, \cdot)$ inelul numerelor întregi

$(a, b)^{*} \in Z$.

Definiţie Vom spune că numărul a este divizibil b, dacă există un c, $c \cdot b = a$

$a \vdots b$ sau $(b | a)$

$15 \vdots 3$, $15 = 3 \cdot 5$.

$15 \not\vdots 4$

Proprietăţi

1. Pentru $\forall a \in Z$, avem că: $a \vdots a$ $(a \cdot 1 = a)$

Din (1) rezultă că relaţia este reflexivă.

2. Dacă $a \vdots b$ nu $\not\Rightarrow$ (rezultă) $b \vdots a$ $(8 \vdots 2 \Rightarrow 2 \not\vdots 8)$ relaţia nu este simetrică.

semnul opus.

3. Daca $a \vdots b$ si $b \vdots a \not\Rightarrow a = b$.
$(2 \vdots -(2)$, $(-2) \vdots 2$, $2 \neq -2)$
(nu-i antisimetrica)

4. Daca $a \vdots b$ si $b \vdots c \Rightarrow a \vdots c$

■ $a \vdots b \Rightarrow \exists c_1 \in \mathbb{Z};\ a = bc_1$
$b \vdots c \Rightarrow \exists c_2 \in \mathbb{Z};\ b = cc_2$
$\} a = c\underbrace{(c_2 c_1)}_{c_3} = cc_3$.

$\Rightarrow a \vdots c$
Relaţia de divizibilitate este tranzitivă. ■

5 Daca $a \vdots c$ şi $b \vdots c \Rightarrow (a \pm b) \vdots c$

■ $a \vdots c \Rightarrow a = cc_1$
$b \vdots c \Rightarrow b = cc_2$
$\Rightarrow a \pm b = c(c_1 \pm c_2) \Rightarrow$
$(a \pm b) \vdots c$. ■

6 Daca $(a \pm b) \vdots c \not\Rightarrow a \vdots c$ sau $b \vdots c$
$(3 + 7) \vdots 10$, $3 \not\vdots 10$, $7 \not\vdots 10$.

7 Daca $a \vdots b$, atunci pentru $\forall c \in \mathbb{Z} \Rightarrow$
$ac \vdots b$.
■ $a \vdots b \Rightarrow a = bc_1 \mid \cdot c$
$ac = b(cc_1) \Rightarrow ac \vdots b$

8. Dacă $ac \vdots b \not\Rightarrow a \vdots b$ sau $c \vdots b$
$(20 \cdot 2) \vdots 10$, $20 \vdots 10$, $2 \not\vdots 20$.
$(3 \cdot 5) \vdots 15$, $3 \not\vdots 15$, $5 \not\vdots 15$

9. Dacă $(a+b) \vdots c$ şi $b \vdots c$, atunci $\Rightarrow$
$a \vdots c$.

■ $(a+b) \vdots c \Rightarrow \overbrace{a+b}^{1} = cc_1$ $-$
scăderea

$b \vdots c \Rightarrow b = c c_2$

$a = c(c_1 - c_2) \Rightarrow a \vdots c$

10. Daca $a \vdots b \Leftrightarrow$ (echivalent) $\Leftrightarrow a \vdots (-b) \Leftrightarrow (-a) \vdots b \Leftrightarrow -a \vdots (-b)$

$\underline{a \vdots b} \Leftrightarrow a = bc \Leftrightarrow a = (-b)\cdot(-c) \Leftrightarrow \underline{a \vdots (-b)}$

$20 \vdots 5 \Leftrightarrow 20 \vdots (-5) \Leftrightarrow -20 \vdots 5 \Leftrightarrow -20 \vdots (-5)$

11. $\forall\, a \in \mathbb{Z},\ a \vdots 1,\ a = 1 \cdot a$

Teorema împărțirii cu rest.

Din def. relat. de divizibilitate rezulta ($\Rightarrow$) nu pentru $\forall$ a și b, a este divizibil cu b ($\forall\, a$ și b, $a \vdots b$)

Teoremă (T. împărț. cu rest.)

Pentru orice $\forall\, a, b \in \mathbb{Z}$, $b \neq 0$, există o singură pereche $q, r \in \mathbb{Z}$, astfel încît $a = bq + r$, unde $0 \leq r < |b|$

$\forall\, a, b \in \mathbb{Z},\ b \neq 0$
$\exists!\ q, r \in \mathbb{Z},\ a = bq + r,\ 0 \leq r < |b|$

Observăm ca dacă $b = 1$, are loc $a = 1 \cdot \underset{q}{a} + \underset{r}{0}$

(Vom lua $b \neq 1$) Vom demonstra teorema prin metoda inducției matematice

1. $a > 0,\ b > 0$ $\qquad M = \{a \in \mathbb{N}^* \mid a = bq + r,\ a < r < b\}$

(a) $1 \in M$, $a = 1$, $1 = b \cdot 0 + 1$, $0 \leq 1 < b$ $\qquad b \neq 1$

(b) Presupunem că $a \in M$, $a = bq + r$, $0 \leq r < b$

(c) Arătăm că $a + 1 \in M$.

$a+1=bq+r+1$

a_1• Dacă $r+1<b$, atunci notăm: $r+1=r_1$, atunci obținem

$a+1=bq+r_1$ (r_1-restul)

a_2• Dacă $r+1=b$, atunci obținem

$a+1=bq+b$.

$a+1=b\underbrace{(q+1)}_{cît}+\underset{rest}{0}$.

Din $(a_1, a_2) \Rightarrow a+1 \in M$

1) Din a, b, c în conformitate cu principiul inducției matematice, rezultă că $M=N^*$.

c.c.d.d.

Observăm că dacă $a=0$, $0=b\cdot\underset{cît}{0}+\underset{rest}{0}$.

$b\neq 0$, evident că are loc condiția dată.

În așa mod am demonstra teorema pentru numerele naturale

2) $a\geq 0$, $b\geq 0$, observăm că $a\geq 0$, $-b>0$.

pentru a și $(-b)$, în baza 1, avem

$a=(-b)\cdot q+r$, $0\leq r<|b|=-b$.

$a=b\underset{cît}{(-q)}\cdot\underset{rest}{r}$

③. $a < 0$, $b > 0$.

$-a > 0$, $b > 0$

$-a = b \cdot q + r$

$a = -bq - r = b\cdot(-q) - b + b - r =$

$b(-q-1) + \underbrace{b-r}_{r_1}$ deoare r este pozitiv nenegativ

$a = b(-q-1) + r_1$, $r_1 = b - r$.

$0 \le b - r < b$

④ $a < 0$, $b < 0$.

$a < 0$ $-b > 0$

conform cazului ③. obținem:

$a = (-b)q + r$.

$a = b(-q) + r$.

Existența lui q și r pentru orice $a, b \in \mathbb{Z}$, $b \neq 0$, este demonstrată.

Verificăm unicitatea pentru q și r.

Admitem că pentru a și b avem două descompuneri:

$a = bq_1 + r_1$

$a = bq_2 + r_2$

T.d. că $q_1 = q_2$?

$r_1 = r_2$ - ?

Dacă presupunem că ~~q~~ $r_1 = r_2$, atunci

$$a = bq_1 + r_1$$
$$- \quad a = bq_2 + r_2$$
$$b(q_1 - q_2) = 0.$$
$$q_1 - q_2 = 0.$$
$$q_1 = q_2$$

Admitem că $r_1 \neq r_2$

$$a = bq_1 + r_1$$
$$- \quad a = bq_2 + r_2$$
$$b(q_1 - q_2) + r_1 - r_2 = a$$

Atît r_1 cît și r_2 sunt ≥ 0 și mai mici decît $|b|$, e clar că diferența lor va fi mai mic ce b.

$$0 \leq r_1 < |b|$$
$$0 \leq r_2 < |b|$$
$$r_1 - r_2 < |b|$$

$$b(q_1 - q_2) = r_2 - r_1$$

$$r_2 - r_1 = b(q_1 - q_2) \Rightarrow (r_2 - r_1) \vdots b \Rightarrow$$

$$(r_1 - r_2) \vdots b \Rightarrow (r_1 - r_2) \vdots |b|$$

$$\left.\begin{matrix} (r_1 - r_2) \vdots |b| \\ (r_1 - r_2) < |b| \end{matrix}\right\} \text{contradicție}$$

astfel $r_1 = r_2 \Rightarrow q_1 = q_2$ (unicitatea) ∎