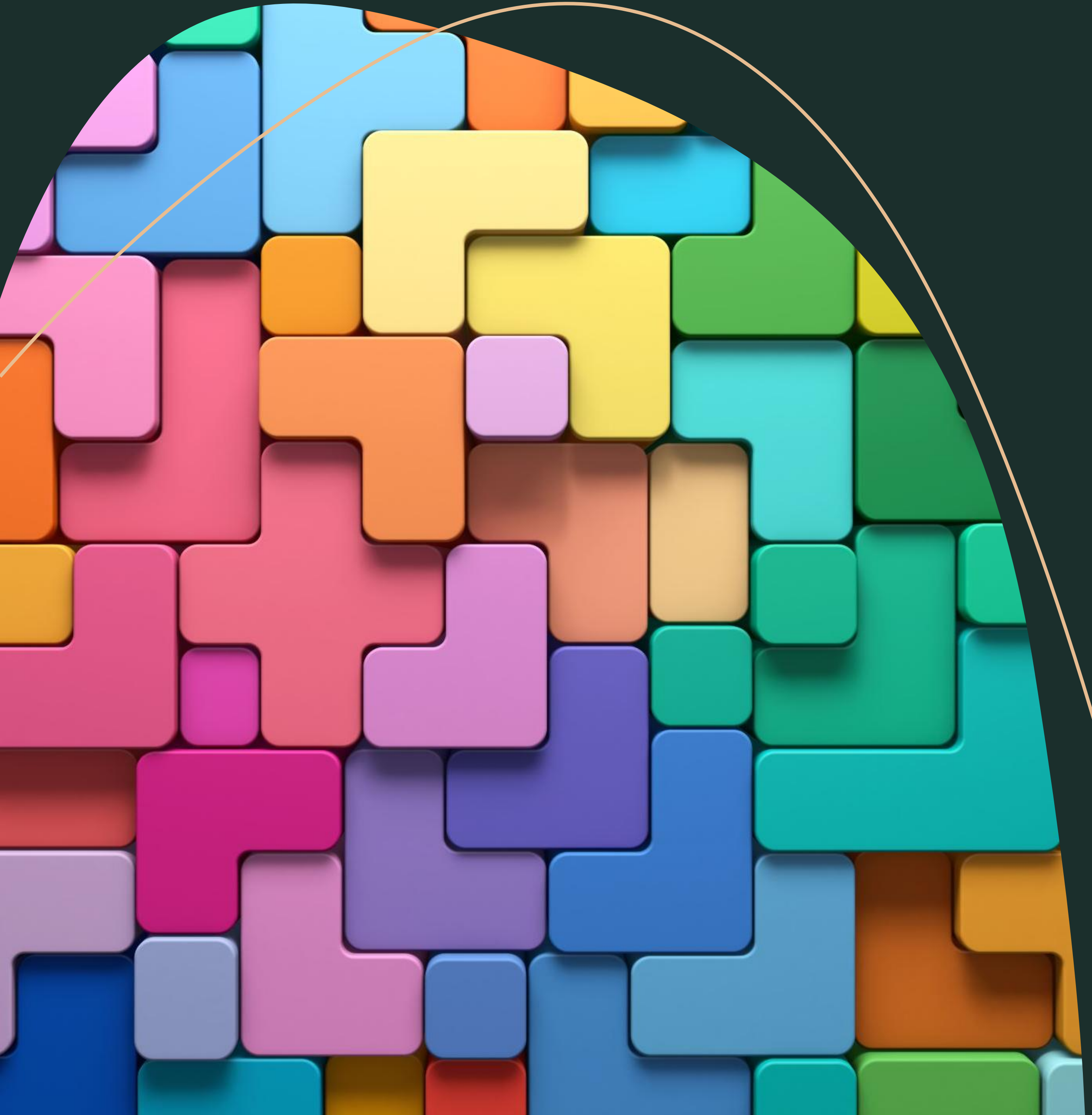
SESIUNEA DE COMUNICĂRI MATEMATICE 9 DECEMBRIE 2023



Divizibilitatea unui număr natural cu numere prime

Student: Bianca Borodescu
Profesor coordonator:
Conf.Univ.dr. Gabriela Badea

Știm că:

Un număr este divizibil cu 2 $\Leftrightarrow$ are ultima cifră pară.

Un număr este divizibil cu 5 $\Leftrightarrow$ are ultima cifră 0 sau 5.

Însă pentru celelalte numere prime nu avem un ***„test al ultimei cifre”*** pentru a concluziona divizibilitatea.

Ce ne propunem?

În această problemă vom oferi un test <u>recursiv</u> pentru divizibilitate bazat pe ultima cifră.

Scopul nostru este să găsim o modalitate de a trece de la un număr cu d cifre (în baza 10), la un număr cu d-1 cifre, astfel încât acesta să rămână divizibil cu numărul prim inițial.

Acest fapt a fost demonstrat cu ajutorul următoarei teoreme:

Teoremă: Fie $n \in \mathbb{N}^*$, iar p este un număr prim, altul decât 2 sau 5. Fie u și r ultima cifră a lui p, respectiv n. Atunci:

$$p \mid n \Leftrightarrow p \mid \left[\frac{n}{10}\right]\text{-}ar\,, \text{ unde:}$$

$$a = \begin{cases} \dfrac{up-1}{10}, & dacă\ u = 1\ sau\ 9 \\ \dfrac{(10-u)\cdot p-1}{10}, & dacă\ u = 3\ sau\ 7 \end{cases} \qquad (1)$$

În plus, dacă $0 < a < p$, atunci a este unic.

Observăm că $\left[\frac{n}{10}\right] - \boldsymbol{ar}$, are un număr de cifre mai mic cu 1 decât numărul de cifre al lui n. Astfel obținem un număr mult mai mic decât n căruia să îi testăm divizibilitatea cu numărul prim.

Exemple:

Ex1: Fie $p=13$ și $n=897$ Vrem să testăm dacă p | n.

$$\downarrow \qquad\qquad \downarrow$$

$$u=3 \qquad\qquad r=7$$

Pentru $u = 3$ avem: $a = \frac{(10-u)\cdot p-1}{10}$ $\quad a = \frac{(10-3)\cdot 13-1}{10} = \frac{7\cdot 13-1}{10} = \frac{90}{10} = 9$

Pentru $r = 7$ avem: $\left[\frac{n}{10}\right] - ar = \left[\frac{897}{10}\right] - 9 \cdot 7 = 89 - 63 = 26$

$26 = 13 \cdot 2 \implies 13 \mid 26 \overset{th}{\Rightarrow} 13 | 897$

De ce spunem că acest test este recursiv?

Ex2: Fie p=71 și n=18 389 Vrem să testăm dacă p | n.

$$\downarrow \qquad \downarrow$$

u=1 r=9

Pentru $u = 1$ avem: $a = \frac{up-1}{10}$ $a = \frac{1\cdot 71-1}{10} = \frac{70}{10} = 7$

Pentru $r = 9$ avem: $\left[\frac{n}{10}\right] - ar = \left[\frac{18\,389}{10}\right] - 7 \cdot 9 = 1838 - 63 = 1775$

Numărul încă este prea mare pentru a verifica divizibilitatea. Așa că aplicăm algoritmul încă o dată, deoarece testul este <u>recursiv</u> (îl putem aplica de câte ori este nevoie).

Noul n: $n=1775$

$\downarrow$

$r=5$

a=7 (calculat anterior)

Pentru $r = 5$ avem:

$$\left[\frac{n}{10}\right] - ar = \left[\frac{1775}{10}\right] - 7 \cdot 5 = 177 - 35 = 142$$

$$142 = 71 \cdot 2 \implies 71 \mid 142 \overset{th}{\Rightarrow} 71 \mid 1775 \overset{th}{\Rightarrow} 71 \mid 18\,389$$

Ex3: Fie $p=67$ și $n=2815$

$$\begin{array}{cc} \downarrow & \downarrow \\ u=7 & r=5 \end{array}$$

Pentru $u = 7$ avem: $a = \frac{(10-u)\cdot p-1}{10}$ $\quad a = \frac{(10-7)\cdot 67-1}{10} = \frac{201-1}{10} = \frac{200}{10} = 20$

Pentru $r = 5$ avem: $\left[\frac{n}{10}\right] - ar = \left[\frac{2815}{10}\right] - 20 \cdot 5 = 281 - 100 = 181$

$67 \cdot 2 = 134$

$67 \cdot 3 = 201 \implies 67 \nmid 181 \overset{th}{\Rightarrow} 67 \nmid 2815$

Ex4: Fie p=67 și n=2814

$$\begin{array}{cc} p=67 & n=2814 \\ \downarrow & \downarrow \\ u=7 & r=4 \end{array}$$

Pentru $u = 7$ avem: $a = \frac{(10-u)\cdot p-1}{10}$ $\quad a = \frac{(10-7)\cdot 67-1}{10} = \frac{201-1}{10} = \frac{200}{10} = 20$

Pentru $r = 4$ avem: $\left[\frac{n}{10}\right] - ar = \left[\frac{2814}{10}\right] - 20 \cdot 4 = 281 - 80 = 201$

$$201 = 67 \cdot 3 \Longrightarrow 67 \mid 201 \overset{th}{\Rightarrow} 67 \mid 2814$$

Ex5: Fie $p=29$ și $n=15\,631$

$$\downarrow \qquad \downarrow$$

$u=9 \qquad r=1$

Pentru $u = 9$ avem: $a = \frac{u \cdot p - 1}{10}$ $\qquad a = \frac{9 \cdot 29 - 1}{10} = \frac{261-1}{10} = \frac{260}{10} = 26$

Pentru $r = 1$ avem: $\left[\frac{n}{10}\right] - ar = \left[\frac{15\,631}{10}\right] - 26 \cdot 1 = 1563 - 26 = 1537$

Noul n: $n=1537 \Rightarrow r=7$

$$\left[\frac{n}{10}\right] - ar = \left[\frac{1537}{10}\right] - 26 \cdot 7 = 153 - 182 = -29$$

Cum $29 \mid -29 \overset{th}{\Rightarrow} 29 \mid 1537 \overset{th}{\Rightarrow} 29 \mid 15\,631$

Teoremă: Fie $n \in \mathbb{N}^*$, iar p este un număr prim, altul decât 2 sau 5.

Fie u și r ultima cifră a lui p, respectiv n. Atunci:

$$p \mid n \Leftrightarrow p \mid \left[\frac{n}{10}\right]\text{-}ar\text{, unde:}$$

$$a = \begin{cases} \dfrac{up-1}{10}, & dacă\ u = 1\ sau\ 9 \\ \dfrac{(10-u)\cdot p-1}{10}, & dacă\ u = 3\ sau\ 7 \end{cases} \qquad (1)$$

În plus, dacă $0 < a < p$, atunci a este unic.

Demonstrația teoremei:

Cum r este cifra unităților a lui n,

atunci putem scrie $n=10q+r$, unde $0\leq r \leq 9$.

Analog, cum u este cifra unităților a lui p,

scriem p ca fiind: $p=10t+u$, unde $u\in \{1,3,7,9\}$

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$

Observăm că $q=\left[\frac{n}{10}\right]$ si ne propunem să găsim $x\in \mathbb{Z}$ astfel încât $p \mid n \Leftrightarrow p \mid (q+x)$

,,$\Leftarrow$"

Dacă $p \mid (q+x)$, atunci $p \mid (10q+10x)$ și folosind relația: $10q=n-r$

obținem: $p \mid (n-r+10x)$

Dar c.m.m.d.c $(10, p) = 1$

Rezultând congruența: $\mathbf{10x \equiv r \pmod{p}}$, care are soluție unică modulo p, *care satisface relația*: $p \mid (10x-r)$ (2) $\Rightarrow p \mid n$.

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$

Propoziția 1:

Congruența: $ax \equiv c \pmod{m}$ are soluții $\Leftrightarrow$ c.m.m.d.c $d = (a, m)$ îl divide pe c.

Demonstrație:

Fie $\overline{x_0} \in \mathbb{Z}_m$, $x_0 \in \mathbb{Z}$, o soluție a congruenței date. Atunci $ax_0 \equiv c \pmod{m}$ și deci

$m \mid ax_0 - c$, adică $\exists$ un $y_0 \in \mathbb{Z}$ astfel că: $ax_0 - c = my_0$. Deoarece $d \mid a$ și $d \mid m$, rezultă:

$d \mid ax_0 - my_0 = c$.

Reciproc să presupunem că: $d \mid c$. Se știe că, există x_0', y_0' numere întregi, astfel încât:

$ax_o' + my_o' = d$. Luând $c' = \frac{c}{d} \in \mathbb{Z}$, avem $c = dc' = a(x_0' \cdot c') + m(y_0' \cdot c')$ și deci:

$a(x_0' \cdot c') \equiv c \pmod{m}$, ceea ce arată că $\overline{x_0' c'} \in \mathbb{Z}_m$ este o soluție a concurenței date.

Remarcă:

Numărul soluțiilor congruenței: $ax \equiv c \pmod{m}$

Fie $d = (a,m)$ și să presupunem că: $d \mid c$. Atunci, dacă $m' = \frac{m}{d} \in \mathbb{Z}$, iar $\overline{x_0}$ este o soluție a congruenței: $ax \equiv c \pmod{m}$, avem că:

$$\overline{x_0}\ ,\ \overline{x_0 + m'}, \overline{x_0 + 2m'}\ \ldots\ ,\ \overline{x_0 + (d-1)m'}$$

Sunt toate soluțiile congruenței și numărul acestor soluții este egal cu d.

Cum r este cifra unităților a lui n,

atunci putem scrie $n=10q+r$, unde $0\leq r \leq 9$.

Analog, cum u este cifra unităților a lui p,

scriem p ca fiind: $p=10t+u$, unde $u\in \{1,3,7,9\}$

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$$

Observăm că $q=\left[\frac{n}{10}\right]$ si ne propunem să găsim $x\in \mathbb{Z}$ astfel încât $p \mid n \Leftrightarrow p \mid (q+x)$

„$\Leftarrow$"

Dacă $p \mid (q+x)$, atunci $p \mid (10q+10x)$ și folosind relația: $10q=n-r$

obținem: $p \mid (n-r+10x)$

Dar c.m.m.d.c $(10, p) = 1$

Rezultând congruența: $\mathbf{10x \equiv r \pmod{p}}$, care are soluție unică modulo p, *care satisface relația*: $p \mid (10x-r)$ (2) $\Rightarrow p \mid n$.

„$\Rightarrow$"

Reciproc presupunem $p \mid n$ sau $p \mid (10q+r)$ $(n=10q+r)$ și folosind **(2) : $\boldsymbol{p \mid (10x\text{-}r)}$** avem relația:

Dacă $x \mid a$ și $x \mid b \Rightarrow x \mid a \pm b$

$$p \mid (10q+r+10x\text{-}r) \Rightarrow p \mid (10q+10x) \Rightarrow p \mid 10(q+x)$$

Dacă $p \mid a \cdot b$ și $p \nmid a \Rightarrow p \mid b$

$$p \mid 10(q+x) \Rightarrow p \mid (q+x).$$

Prin urmare, x pe care-l căutăm satisface **(2)**. Pentru a-l găsi observăm că $\exists!\, a$ cu $0 < a < p$ astfel încât:

$$10a \equiv \text{-}1 \pmod{p} \quad |\cdot(\text{-}r) \quad \Rightarrow \quad 10(\text{-}ar) \equiv r \pmod{p}$$

de unde rezultă că valoarea lui x este **x = -ar**

$x = -ar$

Pentru a determina valoarea lui *a* folosim relația: $\mathbf{10a \equiv -1 \pmod{p}}$

și scriem: $10a + 1 = pk$, $k \in \mathbb{Z}$ (evident, $k \neq 10$)

Din $\mathbf{0 < a < p} \Rightarrow \frac{1}{p} < k < 10 + \frac{1}{p}$, $\forall p$ nr. prim și $p \notin \{2; 5\}$

$k \neq 10$ $\Rightarrow$ $0 < k < 10$

Observație:

$\mathbf{0 < a < p}$ și $\mathbf{10a+1=pk}$, $k \in \mathbb{Z}$

$$\Longrightarrow \frac{10a+1}{p} = k \iff \frac{10a}{p} + \frac{1}{p} = k \iff \frac{1}{p} = k - \frac{10a}{p} \iff \frac{1}{p} < k \quad (3)$$

Acum avem:

$\mathbf{0 < a < p}$ și $\mathbf{k=\frac{10a+1}{p}}$, $k \in \mathbb{Z}$ $\Longrightarrow$

$$\Longrightarrow k = \frac{10a+1}{p} < \frac{10p+1}{p} = \frac{10p}{p} + \frac{1}{p} = 10 + \frac{1}{p} \Longrightarrow k < 10 + \frac{1}{p} \quad (4)$$

Din (3) si (4) $\Longrightarrow \frac{1}{p} < k < 10 + \frac{1}{p}$

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$

Dacă u=1 (ultima cifră a lui p), atunci din

$pk \equiv 1 \pmod{10}$ și $0 < k < 10 \Rightarrow$ k=1 și în consecință $a=\frac{p-1}{10}$

Dacă u=9, atunci din $pk \equiv 1 \pmod{10}$ și $0 < k < 10 \Rightarrow$ k=9 și în consecință

$$a=\frac{up-1}{10}$$

Dacă u=3, atunci din $pk \equiv 1 \pmod{10}$ și $0 < k < 10 \Rightarrow$ k=7 și în consecință $a=\frac{7p-1}{10}$

(5)

Dacă u=7, atunci din $pk \equiv 1 \pmod{10}$ și $0 < k < 10 \Rightarrow$ k=3 și în consecință $a=\frac{3p-1}{10}$

(6)

Din (5) și (6) $\Rightarrow$ **a**= $\mathbf{\frac{(10-u)p-1}{10}}$

Bibliografie:

- Mehdi Hassani, Tests for divisibility by prime numbers, „THE MATHEMATICAL GAZETTE", Volume 103, Issue 558, November 2019, pg. 494-495, (https://www.cambridge.org/core)
- C.Năstăsescu, C.Niță, C.Vraicu, „ARITMETICĂ ȘI ALGEBRĂ", Editura Didactică și pedagogică, R.A. București, Decembrie 1993, pg. 160-161.

Mulțumesc pentru atenție!