Seminar 6 10.11.2020

$\boxed{\text{Prb 7/ Lista 2}}$ Calculati 2019^{2019}, 2021^{2021} in $\mathbb{Z}_{100}$.

$2019^{2019} \equiv ?? \pmod{100}$ $\quad$ ($\bullet$ $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$)

$2019^{2019} \equiv 19^{2019} \pmod{100} \equiv (19^2)^{1009} \cdot 19 \pmod{100} \equiv (-39)^{1009} \cdot 19 \pmod{100}$

$19^2 \equiv 61 \equiv -39 \pmod{100}$

$\equiv ((-39)^2)^{504} \cdot (-39) \cdot 19 \pmod{100} \equiv 21^{504} \cdot (-39) \cdot 19 \pmod{100} \equiv$

$39^2 = 1521 \equiv 21 \pmod{100}$

$\equiv 41^{252} \cdot (-39) \cdot 19 \pmod{100} \equiv 81^{126} \cdot (-39) \cdot 19 \pmod{100} \equiv 19^{127} \cdot (-39) \pmod{100}$

$21^2 = 441 \equiv 41 \pmod{100}$ $\qquad$ $81 \equiv -19 \pmod{100}$

$\equiv (19^2)^{63} \cdot 19 \cdot (-39) \pmod{100} \equiv (-39)^{64} \cdot 19 \pmod{100} \equiv 21^{32} \cdot 19 \pmod{100}$

$\equiv 41^{16} \cdot 19 \pmod{100} \equiv 81^{8} \cdot 19 \pmod{100} \equiv -19^{9} \pmod{100} \equiv -(-39)^4 \cdot 19 \pmod{100}$

$\equiv -21^2 \cdot 19 \pmod{100} \equiv -41 \cdot 19 \pmod{100} \equiv -779 \pmod{100} \equiv 21 \pmod{100}$

$2019^{2019} \equiv 21 \pmod{100}$.

Exc Luați a, b de 4 cifre fiecare și c un număr de 2 cifre. Calculați $a^b \pmod{c}$. (Temă!)

Prb2 Fie $G=\{x\in\mathbb{R} \mid 0\le x<1\}$. Definim pe G legea $x*y=\{x+y\}$. ($\{x+y\}$ înseamnă partea fracționară a lui $x+y$). Arătați că $(G,*)$ este un grup abelian.

"$*$" asociativă #

$$(x*y)*z=\{x+y\}*z=\{\{x+y\}+z\}.$$

$$x*(y*z)=x*\{y+z\}=\{x+\{y+z\}\} \quad (*)$$

$\{x\}=x-[x]$

$$\{\{x+y\}+z\}=\{x+y\}+z-[\{x+y\}+z]=x+y-[x+y]+z-[x+y-[x+y]+z]=x+y+z-[x+y]-[\boxed{x+y+z}-[x+y]]=x+y+z-[x+y+z]=\{x+y+z\}$$

$$=x+y+z-\cancel{[x+y]}-[x+y+z]+\cancel{[x+y]}=x+y+z-[x+y+z]$$

Analog se arată că $(*)=\{x+y+z\}$ $\Rightarrow$ "$*$" e asociativă

"$*$" e evident com. ($\{x+y\}=\{y+x\} \Rightarrow x*y=y*x$)

$(\forall)x\in G$ $x*0=0*x=\{x\}=x$ deoarece $x\in[0,1)$. $\Rightarrow$ 0 este elem. neutru pt G în raport cu "$*$".

Fie $x, y \in G$ a.î. $x * y = 0 \Rightarrow \{x+y\} = 0 \Rightarrow$ $x+y \in \mathbb{Z}$
$x, y \in [0,1) \Rightarrow 0 \le x+y < 2$ $\Big| \Rightarrow x+y \in \{0,1\}$

$x+y=0 \Leftrightarrow x=y=0$ (0 este inversul lui 0)

Dacă $x+y=1 \Rightarrow y = 1-x$ (e inversul lui x, $(\forall)\, x \in G \setminus \{0\}$).

$\Rightarrow (G, *)$ este grup abelian.

<u>Prb 3</u> Arătați că subgrupurile lui $(\mathbb{Z}, +)$ sunt submulțimile $n\mathbb{Z}$, $n \in \mathbb{N}$.

Fie $H = n\mathbb{Z}$, $n \in \mathbb{N}$. $n=0 \Rightarrow 0\mathbb{Z} = \{0\} \rightarrow$ subgrupul trivial al lui $(\mathbb{Z}, +)$
$n=1 \Rightarrow 1\mathbb{Z} = \mathbb{Z}$

Fie $x, y \in H = n\mathbb{Z} \Rightarrow (\exists)\, k, l \in \mathbb{Z}$ a.î. $x = nk$, $y = nl \Rightarrow x - y = n(k-l) \in n\mathbb{Z} = H$.

$\Rightarrow H = n\mathbb{Z}$ este subgrup al lui $(\mathbb{Z}, +)$.

Fie $L \le (\mathbb{Z}, +)$ și presupun că $L \ne 0\mathbb{Z} = \{0\}$. $\Rightarrow (\exists)\, n_0 \in L \setminus \{0\}$ $(n_0 \in \mathbb{Z})$ $\overset{L \le (\mathbb{Z},+)}{\underset{\text{def}}{\Longrightarrow}}$ $-n_0 \in L$. Prin urmare, $L \cap \mathbb{N}^* \ne \emptyset$ și notez cu n cel mai mic număr natural nenul din $L \cap \mathbb{N}^*$.

Afirmație $L = n\mathbb{Z}$. Dem "$\supseteq$" Deoarece $n \in L$ și $L \le (\mathbb{Z}, +)$
$\Rightarrow n \cdot k \in L$ $(\forall)\, k \in \mathbb{Z}$

$\Rightarrow m\mathbb{Z} \subseteq L$

"$\subseteq$" Fie $t \in L \Rightarrow t \in \mathbb{Z}$ $\xrightarrow{m \in \mathbb{N}^*}$ $t = m \cdot c + r$ $\quad 0 \le r < m$

$m \cdot c \in L$ (deoarece $m \in L$) $\Big|$ $\xrightarrow{L \le (\mathbb{Z},+)}$ $\underbrace{t - mc}_{= r} \in L \Rightarrow$

$r \in L$

Deoarece m e cel mai mic ~~nr.~~ nat. nenul din L $\Big| \Rightarrow \boxed{r = 0} \Rightarrow t = mc \in m\mathbb{Z}$

$\Rightarrow L \subset m\mathbb{Z}$. $\boxtimes$

Prb 4 "Calculați" toate morfismele de grupuri dintre: $(\mathbb{Q},+)$ și $(\mathbb{Q},+)$; $(\mathbb{Q},+)$ și $(\mathbb{Z},+)$;

$(\mathbb{Z},+)$ și $(\mathbb{Z},+)$; $(\mathbb{Z},+)$ și $(\mathbb{Q},+)$; $(\mathbb{Z}_m,+)$ și $(\mathbb{Z}_n,+)$, unde $m, n \in \mathbb{N}$, $m,n \ge 2$. (Exc!)

$(\mathbb{Z}_3,+)$ și $(\mathbb{Z}_4,+)$;

Fie $f : (\mathbb{Z},+) \to (\mathbb{Z},+)$ morfism de grupuri $\Rightarrow f(x+y) \overset{(*)}{=} f(x)+f(y)$ $\quad (\forall)\, x,y \in \mathbb{Z}$

$(\Rightarrow f(0) = 0)$ $\quad f(2) = f(1+1) \overset{(*)}{=} f(1) + f(1) = 2f(1)$

Prin inducție după $n \in \mathbb{N}^*$ putem arăta că $f(n) = nf(1)$.

$n \in \mathbb{N}^* \rightsquigarrow \underbrace{f(0)}_{=0} = f(n-n) = f(n+(-n)) \overset{(*)}{=} f(n) + f(-n) \Rightarrow f(-n) = -f(n) = -nf(1)$ $\quad (\forall)\, n \in \mathbb{N}^*$

$\Rightarrow f(k) = k f(1)\ (\forall)\ k\in\mathbb{Z} \Rightarrow f$ este perfect determinat de $f(1)=a\in\mathbb{Z}$

$\Rightarrow$ toate morfismele de la $(\mathbb{Z},+)$ la $(\mathbb{Z},+)$ sunt de forma:

$f_a:(\mathbb{Z},+)\to(\mathbb{Z},+)\quad f_a(k) = ka\ (\forall)\ k\in\mathbb{Z}.$

$(a\in\mathbb{Z})$

Analog se poate arăta că $(\forall)$ morfism de la $(\mathbb{Z},+)$ la $(\mathbb{Q},+)$ este de forma g_a, cu $a\in\mathbb{Q}$ $\quad g_a:(\mathbb{Z},+)\to(\mathbb{Q},+)\quad g_a(m)=ma\ (\forall)\ m\in\mathbb{Z}$

Fie $h:(\mathbb{Q},+)\to(\mathbb{Q},+)$ un morfism de grupuri.

La fel ca mai sus se arată că $h(k)=k\,h(1)\ (\forall)\ k\in\mathbb{Z}.$

Fie $q\in\mathbb{Q}^* \Rightarrow q=\frac{a}{b}$ $\quad b\neq 0,\ a,b\in\mathbb{Z}\ \ (a,b)=1$

$b\,h(\tfrac{1}{b}) = h(b\cdot\tfrac{1}{b}) = h(\underbrace{\tfrac{1}{b}+\tfrac{1}{b}+\dots+\tfrac{1}{b}}_{b \text{ ori}}) = h(1) \Rightarrow h(\tfrac{1}{b}) = \tfrac{1}{b}h(1)$

h morfism

$h(q) = h(\tfrac{a}{b}) = h(\underbrace{\tfrac{1}{b}+\dots+\tfrac{1}{b}}_{a \text{ ori}}) = a\,h(\tfrac{1}{b}) = a\cdot\tfrac{1}{b}h(1) = \tfrac{a}{b}h(1) = q\,h(1)$

$(\forall)\ q\in\mathbb{Q}$

$\Rightarrow$ Orice morfism de grupuri de la $(\mathbb{Q},+)$ la $(\mathbb{Q},+)$ este de forma h_a, $a\in\mathbb{Q}$, unde $h_a:(\mathbb{Q},+)\to(\mathbb{Q},+)$ este $h_a(q)=aq\ (\forall)q\in\mathbb{Q}$.

Fie $f:(\mathbb{Q},+)\to(\mathbb{Z},+)$ un morfism de grupuri

Obs Între orice 2 grupuri există un morfism de grupuri, morfismul trivial, i.e. $\psi:(G_1,\cdot)\to(G_2,\cdot)$, $\psi(x)=1_{G_2}\ (\forall)x\in G_1$

Q Există morfisme netriviale?

Dacă $f:(\mathbb{Q},+)\to(\mathbb{Z},+)$ e morf. de grupuri $\Rightarrow$ $f=h_a$ cu $a\in\mathbb{Z}$ (deoarece $h_a(1)=a\in\mathbb{Z}$)

Morfismul trivial este h_0

Dacă $\boxed{a\neq 0}$ $\rightsquigarrow$ $f\left(\frac{1}{2a}\right)=h_a\left(\frac{1}{2a}\right)=a\cdot\frac{1}{2a}=\frac{1}{2}\notin\mathbb{Z}$

$\Rightarrow$ Nu există morfisme netriviale de la $(\mathbb{Q},+)$ la $(\mathbb{Z},+)$.

Pb Care din următoarele grupuri sunt izomorfe:

$(U_n,\cdot)$, $(\mathbb{Z}_n,+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\mathbb{Q}^*_+,\cdot)$, $(\mathbb{R}^*_+,\cdot)$?

Din motive de cardinal studiem (de $\exists$) izomorfism doar între grupurile din aceeași "grupă colorată".

Rezultă din problema anterioară că $(\mathbb{Z},+) \not\simeq (\mathbb{Q},+)$.

nu e izomorf.

$$(U_n,\cdot) \simeq (\mathbb{Z}_n,+)$$

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0,\dots,n-1\right\}$$

Moivre

Dc $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \Rightarrow U_n = \{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$, $1 = \varepsilon^n$

Moivre $(\cos\alpha + i\sin\alpha)^n = \cos(n\alpha) + i\sin(n\alpha)$

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}, \quad \hat{0} = n\cdot\hat{1}$$

Se arată ușor că $f : (U_n,\cdot) \to (\mathbb{Z}_n,+)$, $f(\varepsilon^j) = \hat{j}$ este un morfism de grupuri $(\forall)\ j = 0,\dots,n-1$.