CURS 6

Inel cât. Congruenţe modulo n. Teorema chineză a restului

Fie $(R,+,\cdot)$ un inel comutativ şi I un ideal al lui $(R,+,\cdot)$. Relaţia

$$x\rho_I y \;\Leftrightarrow\; y-x\in I \;\Leftrightarrow\; y\in x+I$$

este o echivalenţă pe R, numită **relaţia de echivalenţă determinată de** (sau **modulo**) I. (Într-adevăr, cum $x-x=0\in I$, $x\rho_I x$ pentru orice $x\in R$, iar dacă $x\rho_I y$, adică $y-x\in I$, atunci $x-y=-(y-x)\in I$, adică $y\rho_I x$. De asemenea, dacă $x\rho_I y$ şi $y\rho_I z$, adică $y-x\in I$ şi $z-y\in I$, atunci $z-x=(z-y)+(y-x)\in I$, deci $x\rho_I z$.)

Observăm că mulţimea tuturor elementelor echivalente modulo I cu un $x\in R$, adică clasa lui x, este $\rho_I\langle x\rangle = x+I$, iar mulţimea cât corespunzătoare este

$$R/I=\{x+I\mid x\in R\}=\{I,x+I,y+I,\dots\}.$$

Teorema 1. Fie $(R,+,\cdot)$ un inel comutativ şi I un ideal al lui $(R,+,\cdot)$.
1) Egalităţile

$$(x+I)+(y+I)=(x+y)+I \text{ şi } (x+I)(y+I)=xy+I \tag{1}$$

sunt independendente de alegerea reprezentanţilor şi definesc două operaţii binare pe R/I.
2) $(R/I,+,\cdot)$ este un inel comutativ în raport cu operaţiile $+$ şi $\cdot$ definite prin (1).
3) Aplicaţia canonică $p_I: R\to R/I$, $p_I(x)=x+I$ este un omomorfism unital de la inelul $(R,+,\cdot)$ în inelul $(R/I,+,\cdot)$.

Demonstraţie. (facultativă)
1) Într-adevăr, dacă $x'\in x+I$ şi $y'\in y+I$, există $u_1,u_2\in I$ cu $x'=x+u_1,\ y'=y+u_2$ şi atunci

$$x'+y'=(x+y)+(u_1+u_2),\ x'y'=xy+xu_2+u_1y+u_1u_2,$$

iar cum $u_1+u_2, xu_2, u_1y, u_1u_2\in I$ (şi, implicit, $xu_2+u_1y+u_1u_2\in I$),

$$x'+y'\in(x+y)+I \text{ şi } x'y'\in xy+I.$$

2) Verificarea faptului că $(R/I,+,\cdot)$ este un inel comutativ este un exerciţiu simplu. În acest inel elementul zero este clasa $I=0+I$ care are (şi pe) 0 din R ca reprezentant, opusa clasei $x+I$ este $-x+I$, iar unitatea lui R/I este clasa $1+I$. Vom demonstra, ca exemplu, distributivitatea lui $\cdot$ faţă de $+$ în R/I. Din (1) rezultă

$$(x+I)[(y+I)+(z+I)]=(x+I)(y+z+I)=x(y+z)+I=xy+xz+I=(xy+I)+(xz+I)=$$

$$=(x+I)(y+I)+(x+I)(z+I).$$

3) p_I este un omomorfism de inele deoarece pentru orice $x,y\in R$,

$$p_I(x+y)=(x+y)+I=(x+I)+(y+I)=p_I(x)+p_I(y),$$

$$p_I(xy)=xy+I=(x+I)(y+I)=p_I(x)\cdot p_I(y).$$

Iar cum $p_I(1)=1+I$, care e unitatea lui R/I, acest omomorfism este unital. □

Definiţia 2. Fie $(R,+,\cdot)$ un inel comutativ şi I un ideal al său. Inelul $(R/I,+,\cdot)$ construit mai sus se numeşte **inelul cât (factor) al inelului** $(R,+,\cdot)$ **în raport cu** (sau **modulo**) **idealul** I.

Exemplul 3. Inelele cât ale inelului $(\mathbb{Z},+,\cdot)$.
Am văzut în cursul 4 că $(\mathbb{Z},+,\cdot)$ este un domeniu de integritate cu ideale principale şi că mulţimea idealelor lui $(\mathbb{Z},+,\cdot)$ este $\{n\mathbb{Z}=(n)\mid n\in\mathbb{N}\}$. Prin urmare inelele cât ale lui $(\mathbb{Z},+,\cdot)$ sunt $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ cu $n\in\mathbb{N}$. Mai precis, $\mathbb{Z}_0=\{\{k\}\mid k\in\mathbb{Z}\}$, $\mathbb{Z}_1=\{\mathbb{Z}\}$ sunt (izomorfe cu) $\mathbb{Z}$ şi inelul nul, iar pentru $n\geq 2$ inelele $(\mathbb{Z}_n,+,\cdot)$ sunt chiar inelele de clase de resturi modulo n. Într-adevăr, în $\mathbb{Z}_0$ operaţiile definite în (1) se transcriu astfel

$$\{k\}+\{k'\}=\{k+k'\},\ \{k\}\{k'\}=\{kk'\}$$

şi $p_{0\mathbb{Z}}$ este izomorfism, adică $(\mathbb{Z},+,\cdot)\simeq(\mathbb{Z}_0,+,\cdot)$, iar în $\mathbb{Z}_1$ operaţiile definite în (1) devin

$$\mathbb{Z}+\mathbb{Z}=\mathbb{Z}\text{ şi }\mathbb{Z}\cdot\mathbb{Z}=\mathbb{Z}.$$

Dacă $n\in\mathbb{N}$, $n\geq 2$ atunci

$$x\rho_{n\mathbb{Z}}y\ \Leftrightarrow\ y-x\in n\mathbb{Z}\ \Leftrightarrow\ n\mid y-x\ \Leftrightarrow\ x\equiv y\,(\mathrm{mod}\,n),$$

prin urmare, $\mathbb{Z}/n\mathbb{Z}=\{\widehat{0},\widehat{1},\ldots,\widehat{n-1}\}=\mathbb{Z}_n$, cu $\widehat{i}=i+n\mathbb{Z}$, iar operaţiile definite în (1) se transcriu ca în exemplul 3 f) din cursul 4:

$$\widehat{i}+\widehat{j}=\widehat{i+j}\text{ şi }\widehat{i}\cdot\widehat{j}=\widehat{i\cdot j}.$$

Ele organizează pe $\mathbb{Z}_n$ ca un inel comutativ. Elementul nul din $\mathbb{Z}_n$ este $\widehat{0}$, iar elementul unitate este $\widehat{1}$. Dacă $n\geq 2$ este număr prim, atunci (şi numai atunci) inelul $\mathbb{Z}_n$ este un corp comutativ.

Profităm de ocazia ivită pentru a reaminti câteva proprietăţi ale congruenţelor modulo n:

Propoziţia 4. Fie $n\in\mathbb{N}$, $n\geq 2$ şi fie a, b, c, $d\in\mathbb{Z}$. Atunci:
1) $a\equiv b\,(\mathrm{mod}\,n)$ şi $c\equiv d\,(\mathrm{mod}\,n)\Rightarrow a+c\equiv b+d\,(\mathrm{mod}\,n)$ şi $ac\equiv bd\,(\mathrm{mod}\,n)$;
2) dacă $a\equiv b\,(\mathrm{mod}\,n)$ şi $k\in\mathbb{N}$, atunci $a^k\equiv b^k\,(\mathrm{mod}\,n)$, $a+c\equiv b+c\,(\mathrm{mod}\,n)$ şi $ac\equiv bc\,(\mathrm{mod}\,n)$;
3) $ac\equiv bc\,(\mathrm{mod}\,nc)\Rightarrow a\equiv b\,(\mathrm{mod}\,n)$;
4) $ac\equiv bc\,(\mathrm{mod}\,n)$ şi $(c,n)=1\Rightarrow a\equiv b\,(\mathrm{mod}\,n)$.

Observaţia 5. Proprietăţile 1) de mai sus exprimă chiar faptul că egalităţile (1) sunt independente de alegerea reprezentanţilor, iar 4) exprimă chiar faptul că în $\mathbb{Z}_n$ se poate simplifica cu orice clasă $\widehat{c}$ cu $(c,n)=1$ (lucru demonstrat în $\mathbb{Z}_n$ în cursul 4 dacă ţinem cont că elementele cu care se poate simplifica coincid cu non-divizorii lui zero).

Vom adăuga la lista de mai sus câteva proprietăţi celebre ale congruenţelor modulo n pe care le vom demonstra trecând prin inelul cât corespunzător.

Reamintim că pentru un omomorfism de inele $f:R\to R'$, $\mathrm{Ker}f=\{x\in R\mid f(x)=0\}$ este ideal al lui R şi $f(R)$ este subinel al lui R', iar **teorema întâi de izomorfism pentru inele** afirmă că *inelul cât $R/Kerf$ este izomorf cu inelul $f(R)$*.

Teorema 6. Dacă R este un domeniu cu ideale principale şi $a,b\in R$ sunt două elemente relativ prime, adică $(a,b)=1$, atunci inelele $R/(ab)$ şi $R/(a)\times R/(b)$ sunt izomorfe.

Demonstraţie. Se verifică uşor că

$$f : R \to R/(a) \times R/(b),\ f(x) = (x + (a), x + (b))$$

este omomorfism de inele. Vom aplica teorema întâi de izomorfism (pentru inele) lui f. În acest scop aflăm pe $\mathrm{Ker} f$ şi arătăm că f este surjectiv (adică $f(R) = R/(a) \times R/(b)$).

$$x \in \mathrm{Ker} f \Leftrightarrow (x + (a), x + (b)) = ((a), (b)) \Leftrightarrow x + (a) = (a) \text{ şi } x + (b) = (b) \Leftrightarrow x \in (a) \text{ şi } x \in (b).$$

Dar $(a, b) = 1$ implică $[a, b] = ab$ şi, astfel,

$$x \in (a) = aR \text{ şi } x \in (b) = bR \Leftrightarrow x \in aR \cap bR = [a, b]R = (ab)R = (ab),$$

ceea ce arată că $\mathrm{Ker} f = (ab)$.

Fie acum $(x_1 + (a), x_2 + (b)) \in R/(a) \times R/(b)$. Din $(a, b) = 1$ deducem că există $u, v \in R$ astfel încât $au + bv = 1$. Atunci $x_1 - x_2 = au(x_1 - x_2) + bv(x_1 - x_2)$, iar dacă notăm $u' = u(x_1 - x_2)$, $v' = v(x_1 - x_2)$, atunci $au' + bv' = x_1 - x_2$ sau, echivalent, $bv' + x_2 = x_1 - au'$. Luăm

$$x = bv' + x_2 = x_1 - au'.$$

Din definiţia lui f şi $au' \in aR = (a)$, $bv' \in bR = (b)$ rezultă

$$f(x) = (x_1 - au' + (a), bv' + x_2 + (b)) = (x_1 + (a), x_2 + (b)).$$

Deci omomorfismul f este surjectiv. Acum, din prima teoremă de izomorfism urmează că inelul cât $R/\mathrm{Ker} f = R/(ab)$ este izomorf cu $f(R) = R/(a) \times R/(b)$. □

Observaţia 7. Izomorfismul de inele care rezultă aplicând prima teoremă de izomorfism lui f este

$$\overline{f} : R/(ab) \to R/(a) \times R/(b),\ \overline{f}(x + (ab)) = (x + (a), x + (b)).$$

Corolarul 8. Fie $a, b \in \mathbb{N}^* \setminus \{1\}$ şi $(a, b) = 1$. Pentru orice $c, d \in \mathbb{Z}$ sistemul de congruenţe

$$\begin{cases} x \equiv c \pmod{a} \\ x \equiv d \pmod{b} \end{cases} \tag{2}$$

are o soluţie $x_0 \in \mathbb{Z}$ unică modulo ab, adică pentru orice soluţie x_0' a lui (2) avem $x_0' \equiv x_0 \pmod{ab}$.

Într-adevăr, dacă luăm $R = \mathbb{Z}$ rezultă că există o singură clasă $x_0 + (ab) \in \mathbb{Z}/(ab)$ astfel încât $\overline{f}(x_0 + (ab)) = (c + (a), d + (b))$, de unde urmează

$$(x_0 + (a), x_0 + (b)) = (c + (a), d + (b)).$$

Deci x_0 este o soluţie a sistemului (2).

Corolarul 8 este un caz particular al unei proprietăţi celebre:

Corolarul 9. (**Teorema chineză a resturilor**) Fie $n_1, \ldots, n_k \in \mathbb{N}$ o familie de numere naturale două câte două relativ prime cu $n_i \geq 2$ pentru toţi $i \in \{1, \ldots, k\}$. Oricare ar fi numerele $a_1, \ldots, a_k \in \mathbb{Z}$, sistemul

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

are soluţie unică modulo $n_1 n_2 \ldots n_k$.

Cum $(n_i, n_j) = 1$ pentru orice $i \neq j$, avem $(n_1 n_2 \cdots n_i, n_{i+1}) = 1$ pentru orice $i \in \{1, \ldots, k-1\}$. Rezultatul de mai sus se obţine aplicând inductiv corolarul 8.

Reamintim că elementele inversabile ale unui inel formează o parte stabilă a monoidului multiplicativ care este un grup în raport cu operaţia indusă. Cum definiţia **funcţiei lui Euler** $\varphi : \mathbb{N} \to \mathbb{N}$ este $\varphi(n)$ este numărul numerelor $i \in \mathbb{N}$ cu $i < n$ şi $(i, n) = 1$, iar elementele inversabile din inelul $\mathbb{Z}_n$ sunt clasele $\widehat{i}$ cu $(i, n) = 1$, rezultă imediat că $|U(\mathbb{Z}_n)| = \varphi(n)$ (adică $\varphi(n)$ este chiar ordinul grupului elementelor inversabile din $\mathbb{Z}_n$). Din teorema 6 mai deducem şi:

Corolarul 10. Dacă $m, n \in \mathbb{N}^*$ şi $(m, n) = 1$, iar φ este funcţia lui Euler, atunci

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{3}$$

Într-adevăr, din teorema 6 rezultă existenţa izomorfismului de inele $\overline{f} : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ menţionat şi în observaţia 7. Cum imaginile elementelor inversabile din domeniul unui omomorfism unital de inele sunt elemente inversabile ale codomeniului, restricţionând domeniul şi codomeniul lui $\overline{f}$ rezultă un izomorfism de grupuri multiplicative de la $(U(\mathbb{Z}_{mn}), \cdot)$ la $(U(\mathbb{Z}_m) \times U(\mathbb{Z}_n), \cdot)$. Prin urmare $|U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)|$, de unde rezultă (3).

Corolarul 11. Dacă $n \in \mathbb{N}$, $n \geq 2$ şi

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k},\ \alpha_1, \ldots, \alpha_k \in \mathbb{N}^* \tag{4}$$

este descompunerea lui n în factori primi distincţi, atunci

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1). \tag{5}$$

Într-adevăr, dacă $p \in \mathbb{N}$ este un număr prim şi $\alpha \in \mathbb{N}^*$, atunci numerele naturale strict mai mici decât p^α care sunt multipli de p sunt numerele mp cu $0 \leq m \leq p^{\alpha-1} - 1$. Rezultă că numărul acestor întregi este $p^{\alpha-1}$. Deci

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1). \tag{6}$$

Din (3), (4) şi (6) rezultă (5).

Să ne reamintim că o consecinţă a faptului că *ordinul oricărui subgrup al unui grup finit G este finit şi divide ordinul $|G|$ al grupului G* (**Teorema lui Lagrange**) este faptul că $a^{|G|} = 1$ pentru orice element a al grupului G. Astfel, rezultă:

Teorema 12. (**Teorema lui Euler**) Dacă $a \in \mathbb{Z}$ şi $(a, n) = 1$, atunci

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{7}$$

Demonstraţie. Din $(a, n) = 1$ rezultă $\widehat{a} \in U(\mathbb{Z}_n)$, de unde, conform consideraţiilor anterioare,

$$(\widehat{a})^{|U(\mathbb{Z}_n)|} = \widehat{1} \ \Leftrightarrow\ (\widehat{a})^{\varphi(n)} = \widehat{1},$$

ceea ce, în limbajul congruenţelor modulo n, se traduce prin (7). □

Corolarul 13. (**Teorema lui Fermat**) Dacă $p \in \mathbb{N}^*$ este un număr prim, $a \in \mathbb{Z}$ şi $p \nmid a$, atunci

$$a^{p-1} \equiv 1 \pmod{p}. \tag{8}$$

Într-adevăr, din ipoteză rezultă $\varphi(p) = p-1$ şi $(a,p) = 1$ de unde conform lui (7) urmează (8).

Observaţia 14. Menţionăm că relaţia (8) este echivalentă cu

$$a^p \equiv a \pmod{p}$$

care este adevărată şi în cazul $p \mid a$.

Teorema 15. (**Teorema lui Wilson**) Dacă $p \in \mathbb{N}$ este un număr prim, atunci

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{9}$$

Demonstraţie. Dacă $p = 2$ sau $p = 3$, evident (9) are loc. Să considerăm în continuare $p \geq 5$.

Întâi arătăm că în corpul $\mathbb{Z}_p$ avem

$$(\widehat{i})^{-1} = \widehat{i} \Leftrightarrow \widehat{i} = \widehat{1} \text{ sau } \widehat{i} = \widehat{p-1}. \tag{10}$$

Într-adevăr, din $\widehat{1} \cdot \widehat{1} = \widehat{1}$ şi $\widehat{p-1} \cdot \widehat{p-1} = (\widehat{p-1})^2 = p^2 \widehat{-2p} + 1 = \widehat{1}$ rezultă

$$(\widehat{1})^{-1} = \widehat{1} \text{ şi } (\widehat{p-1})^{-1} = \widehat{p-1}.$$

Invers, deoarece într-un corp nu există divizori ai lui zero avem

$$(\widehat{i})^{-1} = \widehat{i} \Leftrightarrow \widehat{i} \cdot \widehat{i} = \widehat{1} \Rightarrow (\widehat{i})^2 - \widehat{1} = \widehat{0} \Rightarrow (\widehat{i} - \widehat{1})(\widehat{i} + \widehat{1}) = \widehat{0} \Rightarrow \widehat{i} - \widehat{1} = \widehat{0} \text{ sau } \widehat{i} + \widehat{1} = \widehat{0}.$$

Înseamnă că $\widehat{i} = \widehat{1}$ sau $\widehat{i} = -\widehat{1} = \widehat{p-1}$, ceea ce completează demonstraţia echivalenţei (10).

Din faptul că p este prim impar urmează că submulţimea $M = \{\widehat{2}, \widehat{3}, \ldots, \widehat{p-2}\}$ a lui $\mathbb{Z}_p$ este nevidă şi conţine un număr par de clase, iar din (10) rezultă că pentru orice $\widehat{j} \in M$ avem $\widehat{j} \neq (\widehat{j})^{-1} \in M$. Aşadar, în produsul $\widehat{2} \cdot \widehat{3} \cdot \ldots \cdot \widehat{p-2}$ putem forma perechi de factori formate din clase care sunt una inversă celeilalte. Astfel, rezultă că în $\mathbb{Z}_p$ avem

$$\widehat{2} \cdot \widehat{3} \cdot \ldots \cdot \widehat{p-2} = \widehat{1}$$

de unde urmează

$$\widehat{2} \cdot \widehat{3} \cdot \ldots \cdot \widehat{p-2} \cdot \widehat{p-1} = \widehat{p-1} = -\widehat{1}$$

ceea ce implică $(\widehat{p-1})! + \widehat{1} = \widehat{0}$, sau, echivalent,

$$\widehat{(p-1)!} + 1 = \widehat{0},$$

ceea ce, în limbajul congruenţei modulo p se transcrie prin (9). □