SEMINAR 11: ARITMETICĂ ÎN INELELE $\mathbb{Z}$ ŞI $k[X]$ (I)

Începem în $\mathbb{Z}$, iar în a doua parte vedem aspecte aritmetice dintr-un inel $k[X]$, k fiind un corp comutativ fixat.

Depistarea efectivă a celui mai mare divizor comun pentru doi întregi a şi b, notat (a, b), e posibilă conform algoritmului lui Euclid (atribuit lui Euclid pentru că apare într-o formă geometrică în ale sale *Elemente*), aşa că, din nou, nu o să insistăm asupra acestei chesiuni. De exemplu:

1. Determinaţi $(1804, 328)$.

Soluţie. Efectuăm împărţiri cu rest până când şirul resturilor devine nul. Avem $1804 = 5 \cdot 328 + 164$, de unde $(1804, 328) = (328, 164)$. Continuăm: $328 = 2 \cdot 164 + 0$, de unde $(1804, 328) = 164$.

Observaţi că partea importantă de reducţie se bazează pe următorul fapt:

2. Din orice relaţie de forma $a = qb + r$ rezultă că $(a, b) = (b, r)$.

Soluţie. Fie u cu $u \mid a$ şi $u \mid b$, *i.e.* $a = su$, $b = tu$. Atunci $r = a-qb = su-qtu = (s-qt)u$, adică avem şi că $u \mid r$. Reciproc, Dacă $v \mid b$ şi $v \mid r$, $b = s'v$ şi $r = t'v$, atunci $a = qb+r = qs'v+t'v = (qs'+t)v$, *i.e* $v \mid a$. Cu alte cuvinte, mulţimea tuturor divizorilor comuni lui a şi b e tot una cu cea a tuturor divizorilor comuni lui b şi r; în particular, rezultă că $(a, b) = (b, r)$.

A doua parte importantă, cea care oferă finitudine algoritmului, e buna ordonare a lui $\mathbb{N}$.

Următoarea consecinţă am mai văzut-o în limbajul idealelor, însă insist asupra ei:

3. Fie $a, b \in \mathbb{Z}$ (nu ambii nuli, desigur). Atunci $d = (a, b)$ dacă şi numai dacă există $k, l \in \mathbb{Z}$ aşa încât $d = ka + lb$.

Soluţie. Suficienţa e evidentă. Pentru necesitate, fie $d = (a, b)$. Considerăm şirul de resturi succesive $|b| > r_1 > r_2 > \ldots > 0$, dat de aplicarea repetată a teoremei împărţirii cu rest:

$$\begin{aligned}
a &= q_1 b + r_1, \quad 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4, \quad 0 < r_4 < r_3 \\
&\cdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Deci $d = r_n$ (conform algoritmului). Din prima ecuaţie avem $r_1 = a - q_1 b$, aşa că r_1 e de forma $r_1 = k_1 a + l_1 b$ ($k_1 = 1, l_1 = -q_1$). Din următoarea egalitate obţinem $r_2 = b - q_2 r_1 = b - q_2(k_1 a + l_1 b) = (-q_2 k_1)a + (1 - q_2 l_1)b \overset{not}{=} k_2 a + l_2 b$. Continuând astfel, ajungem, într-un număr finit de paşi, la o reprezentare de forma $d = r_n = ka + lb$, adică concluzia.

Aţi văzut că dacă un număr prim p divide un produs ab, atunci $p \mid a$ sau $p \mid b$, şi vă spuneam că în cazul abstract (aritmetică într-un domeniu integru oarecare), acest rezultat e luat drept definiţie. Mai general:

4. Dacă un întreg r divide ab, iar r şi a sunt relativ prime, atunci trebuie să avem $r \mid b$.

Soluţie. Deoarece $(r, a) = 1$, există $k, l \in \mathbb{Z}$ aşa încât $kr + la = 1$ (cf. ex. 3), de unde $krb + lab = b$. Dar, conform ipotezei, există $s \in \mathbb{Z}$ aşa încât $ab = sr$, şi deci $b = krb + lsr = (kb + ls)r$, *i.e.* $r \mid b$.

V-am tot pomenit de problema centrală a aritmeticii: înţelegerea calitativă şi cantitativă a ecuaţiilor diofantice. Mai precis, dat un $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, problema e să înţelegem soluţiile întregi $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ ale ecuaţiei $F(x_1, \ldots, x_n) = 0$. O astfel de ecuaţie poate avea un număr finit sau un număr infinit de soluţii, sau nici una. Noi vedem aici doar cazul cel mai simplu, anume cel al ecuaţiilor diofantice liniare în două necunoscute (bine, cel mai simplu e $ax = c$, însă acest caz e trivial).

5. Daţi $a, b, c \in \mathbb{Z}$, să se rezolve, în $\mathbb{Z}$, calitativ şi cantitativ, ecuaţia $ax + by = c$.

Soluţie. Din nou, situaţia e lămurită de algoritmul lui Euclid. Mai întâi, am văzut că, notând $(a, b) = d$, există $k, l \in \mathbb{Z}$ aşa încât $ak + bl = d$. Astfel, dacă $c = d$, ecuaţia are soluţia $x = k$, $y = l$. Apoi, dacă c e un multiplu al lui d, *i.e.* $c = qd$, atunci $a(qk) + b(ql) = qd = c$, şi deci obţinem soluţia particulară $x \overset{not}{=} x^* = qk$, $y \overset{not}{=} y^* = ql$. Reciproc, dacă ecuaţia are o soluţie (x_0, y_0), atunci sigur avem $d \mid c$ (căci $d \mid a$ şi $d \mid b$, iar $c = ax_0 + by_0$). Aşadar, ecuaţia $ax + by = c$ are soluţie dacă şi numai dacă $(a, b) \mid c$ (asta-i partea calitativă).

Acum, presupunând că $d \mid c$, am văzut soluţia (x^*, y^*) şi observăm că dacă (x', y') e altă soluţie, atunci $x" = x' - x^*$, $y" = y' - y^*$ e soluţie a ecuaţiei omogene $ax + by = 0$. Astfel, dacă găsim soluţiile omogenizatei, atunci le găsim şi pe cele ale ecuaţiei iniţiale.

Pentru a depista soluţiile ecuaţiei $ax + by = 0$, împărţim cu d; deci avem de rezolvat ecuaţia $a'x + b'y = 0$, unde $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, sau $a'x = -b'y$. Dacă există o astfel de pereche (x, y), atunci avem că $b' \mid a'x$ şi $a' \mid b'(-y)$. Însă $(a', b') = 1$ (de ce?), aşa că $b' \mid x$ şi $a' \mid -y$ (cf. ex.4), adică $x = ub'$ şi $-y = va'$. Dar atunci $a'ub' = b'va'$, de unde $u = v \overset{not}{=} t$. Prin urmare, soluţiile ecuaţiei $ax + by = 0$ sunt $(x = \frac{b}{(a,b)}t, y = \frac{-a}{(a,b)}t)$, $t \in \mathbb{Z}$, şi deci soluţiile ecuaţiei $ax + by = c$ sunt $x = x^* + \frac{b}{(a,b)}t$, $y = y^* + \frac{-a}{(a,b)}t$, cu $t \in \mathbb{Z}$ oarecare, (x^*, y^*) fiind o soluţie particulară determinată cu algoritmul lui Euclid (aceasta este partea cantitativă).

Ca să fie limpede, vedem şi o ilustrare:

6. Să se studieze următoarele ecuaţii diofantice liniare:
(i) $3x + 6y = 22$
(ii) $7x + 11y = 13$

Soluţie. (i) Avem $(3, 6) = 3 \nmid 22$, aşa că ecuaţia nu are soluţii (cf. ex. 5).
(ii) Aceasta are soluţii: $(7, 11) = 1 \mid 13$. Procedăm exact ca în ex. 5.

Trebuie doar să determinăm o soluţie particulară. Avem

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

$(7, 11) = 1$, şi deci, parcurgând drumul invers,

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 \\ &= 2(11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7 \end{aligned}$$

Astfel, $7(-3) + 11 \cdot 2 = 1$, de unde $7(-39) + 11 \cdot 26 = 13$. Aşadar, obţinem soluţia particulară $x^* = -39$, $y^* = 26$, şi deci celelalte soluţii sunt $x = -39 + 11t$, $y = 26 - 7t$, cu $t \in \mathbb{Z}$ oarecare (cf. ex. 5).

Aţi văzut în curs demonstraţia faptului că, într-adevăr, există o infinitate de numere prime (e încă o situaţie în care putem cădea pradă "evidentului": amintiţi-vă discuţia asemănătoare legată de teorema fundamentală a aritmeticii, unde am văzut un sistem numeric în care unicitatea descompunerii eşua - sigur, exemplul era complet neinteresant, însă există). Există alte două demonstraţii ale acestui rezultat - una dată de Euler (care a fost crucială), iar alta dată de Pólya. O vedem, mai întâi, pe a doua, însă e imperativ să discutăm şi despre prima.

De-a lungul timpului, s-au făcut varii încercări de a găsi formule cât mai simple care să producă numere prime (nu neapărat pe toate). Printre acestea, se numără conjectura făcută de Fermat: "*Toate numerele de forma* $F(n) = 2^{2^n} + 1$ *sunt prime* ($n \in \mathbb{N}$)". Cel mai probabil, Fermat a afirmat acest lucru datorită experienţei (formulările multor rezultate din teoria numerelor sunt deduse prin experiment...): $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, $F(4) = 65537$ sunt toate prime. Însă conjectura e falsă, Euler arătând că are loc factorizarea $F(5) = 641 \cdot 6700417$. Mai sunt şi alte încercări de a genera numere prime. Spre exemplu, $f(n) = n^2 - n + 41$: pentru $n \in \{1, 2, \ldots, 40\}$, $f(n)$ e prim, însă $f(41) = 41^2$. Asemănător, expresia $f(n) = n^2 - 79n + 1601$ oferă numere prime pentru orice $n \in \{1, 2, \ldots, 79\}$, dar $f(80)$ nu e prim. Comportamentul numerelor prime e prea complicat şi nu se supune niciunei formule algoritmice. Abordarea numerelor prime s-a schimbat, instaurându-se punctul de vedere asimptotic...

În fine, avem nevoie de o anumită proprietate a numerelor Fermat F_n:

7. Pentru orice $m, n \in \mathbb{N}$, avem $(F_n, F_m) = 1$ ($m \neq n$, bineînţeles).

Soluţie. Să zicem că $m > n$ şi scriem $m = n + k$, $k > 0$. Fie d un divizor comun al lui F_n şi F_{n+k}. Notând $2^{2^n} = t$, avem că

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{t^{2^k} - 1}{t + 1} = t^{2^{k-1}} - t^{2^{k-2}} + \ldots - 1,$$

şi deci $F_n \mid F_{n+k} - 2$. Atunci $d \mid F_{n+k}$ şi $d \mid F_{n+k} - 2$, de unde $d \mid 2$. Deoarece numerele Fermat sunt impare, trebuie să avem $d = 1$. Cum d a fost ales arbitrar, avem concluzia.

Acum:

8. Mulţimea $\mathcal{P} = \{p \in \mathbb{N}; \text{p e prim}\}$ e infinită.

Soluţie (Pólya). Conform ex. 7, pentru orice $n \in \mathbb{N}$, fiecare dintre numerele $F_0, F_1, \ldots, F_n$ e divizibil printr-un număr prim diferit de 2 (posibil el însuşi) ce nu divide pe ceilalţi. Astfel, avem măcar n numere prime distincte (diferite de 2) până la F_n, şi cum n e oarecare, obţinem $card(\mathcal{P}) = \infty$.

Poate la prima vedere numerele Fermat nu impresionează. Însă, în general, un savuros misticism a învăluit mereu numerele. Iată o (posibilă) pastilă pentru tulburarea somnului de noapte:

<u>Teoremă</u> (Gauss). Un poligon regulat cu n laturi, $n \geq 3$, se poate construi cu rigla şi compasul dacă şi numai dacă $n = 2^k$, cu $k \geq 2$, sau $n = 2^k p_1 p_2 \ldots p_s$, cu $p_1, p_2, \ldots, p_s$ numere Fermat ce sunt prime, mutual distincte, şi $k \geq 0$.

Acum, ca să fie mai clară exprimarea "metode asimptotice" de mai devreme, se defineşte funcţia de interes $\pi : \mathbb{N}^* \longrightarrow \mathbb{N}$, $\pi(x) =$ numărul numerelor prime ce nu depăşesc x. Astfel, $\pi(1) = 0$, $\pi(2) = 1$, sau $\pi(20) = 8$. O primă mostră din cadrul acestei metode e următoarea estimare:

9. $\pi(x) \geq log\, log\, x$, oricare ar fi $x \geq 2$ (log notează singurul logaritm interesant în matematică, anume cel în baza e, unde e e numărul lui Euler).

Soluţie. Avem şi funcţia $P : \mathbb{N}^* \longrightarrow \mathbb{N}$, $P(n) =$ al n-lea număr prim $\overset{not}{=} p_n$. Evident, $\pi(P(n)) = n$, deci p şi π sunt inverse una alteia. Observăm că $p_{n+1} \leq F_n = 2^{2^n} + 1$ (conform soluţiei de la ex. 8, punându-l şi pe 2). Fie $x \geq 2$ fixat oarecare. Dacă $x > e^{e^3}$, atunci găsim un $n \geq 4$ aşa încât $e^{e^{n-1}} < x \leq e^{e^n}$ ($(2, \infty) \subseteq \bigcup\limits_n (e^{e^{n-1}}, e^{e^n}]$). Dar, deoarece $n \geq 4$, avem că $e^{n-1} > 2^n$, şi deci $e^{e^{n-1}} > 2^{2^n}$. Astfel, $\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(2^{2^n}) \geq \pi(p_n) = n$, ţinând cont de inegalitatea de mai sus ($p_n < p_{n+1}$, deci $p_n \leq 2^{2^n}$). Dar $log\, log\, x \leq log\, log\, e^{e^n} = n$ aşa că avem estimarea (cazul $2 \leq x \leq e^{e^3}$ e clar).

Însă această estimare este foarte slabă: de exemplu, pentru $x = 10^9$, se verifică faptul că inegalitatea oferă $\pi(x) \geq 3$, când în realitate, $\pi(x)$ depăşeşte 50000000 (!) De fapt, iată care este bijuteria:

<u>Teoremă</u> (Hadamard - de la Vallée Poussin).

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{log\, x}} = 1,$$

i.e. numărul primelor ce nu depăşesc x e asimptotic cu $\frac{x}{log\, x}$.

Deşi teorema a fost mai întâi conjecturată de Gauss (experimental), la vremea aceea matematica nu era suficient de dezvoltată aşa încât să se fi putut demonstra acest lucru. Abia la 100 de ani după formularea ei a venit şi demonstraţia, dată de Hadamard (1896), şi, separat, de către de la Vallée Poussin (1896), folosind metodele analizei complexe!

Aşadar, comportarea media e distribuţiei numerelor prime, *i.e.* ”$\frac{\pi(x)}{x}$ când $x \to \infty$”, se poate descrie cu ajutorul funcţiei logaritmice: lucru deloc evident, căci aparent nu e nicio legătură între funcţiile $\pi(x)$ şi $log\, x$ (gândiţi-vă numai că prima e discretă, iar a doua e continuă...)

Am notat cu $\mathcal{P}$ mulţimea numerelor prime. Spuneam că mai există o altă demonstraţie a infinitudinii numerelor prime, dată de Euler. Ideea e simplă şi încântătoare: considerăm seria $\sum\limits_{p \in \mathcal{P}} \frac{1}{p}$. Dacă ar fi un număr finit de prime, atunci această serie ar fi convergentă, aşa că infinitudinea primelor rezultă din:

10. (Euler) Seria $\sum\limits_{p \in \mathcal{P}} \frac{1}{p}$ diverge.

Soluţie. Pentru început, o scurtă pregătire. Pentru orice j considerăm funcţia N_j care asociază unui număr x numărul $N_j(x)$ al acelor numere n cu proprietatea că $n \leq x$ şi $p \nmid n$ dacă p e un număr prim mai mare strict decât p_j (al j-lea număr prim). Vrem să găsim o margine superioară pentru $N_j(x)$. Pentru un n cu proprietăţile de mai sus, scriem $n = n_1^2 m$, cu m liber de pătrate; deci m e de forma $m = 2^{\alpha_1} 3^{\alpha_2} \dots p_j^{\alpha_j}$, unde $\alpha_1, \dots, \alpha_j \in \{0, 1\}$. Deoarece avem 2^j alegeri posibile ale exponenţilor $\alpha_1, \dots, \alpha_j$, m poate lua cel mult 2^j valori diferite. Pentru cealaltă bucată din scrierea lui n avem $n_1 \leq \sqrt{n} \leq \sqrt{x}$, aşa că avem cel mult $[\sqrt{x}]$ valori diferite pe care le poate lua n_1. Prin urmare, $N_j(x) \leq 2^j \sqrt{x}$ $(*)$.

Acum să abordăm seria din enunţ. Presupunem că ar fi convergentă. Atunci, pentru $\varepsilon = \frac{1}{2}$, există $j \in \mathbb{N}$ aşa încât

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \dots < \frac{1}{2}$$

(din definiţia convergenţei). Pentru un prim fixat p, numărul acelor $n \leq x$ ce se divid prin p este cel mult egal cu $[\frac{x}{p}]$ $(1 \cdot p, 2 \cdot p, \dots$ şi $n \leq x)$, aşa că

$$x - N_j(x) \leq \frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \dots < \frac{1}{2}x$$

($N_j(x)$ e numărul acelor $n \leq x$ ce se divid măcar cu unul dintre primele $p_{j+1}, p_{j+2}, \dots$ conform definirii lui N_j). Astfel, ţinând cont şi de $(*)$, găsim că $\frac{1}{2}x < 2^j \sqrt{x}$, şi deci, $x < 2^{2j+2}$. Dar asta e absurd, căci j e fixat, iar x a fost ales oarecare; deci seria e divergentă.

Mai mult, Euler a mers mai departe considerând pentru orice $s \in \mathbb{R}$ seria $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$. Când are sens? Avem:

11. Seria $\sum\limits_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots$ e convergentă dacă şi numai dacă $s > 1$.

Soluţie. Folosim criteriul integral considerând funcţia $f : [1, \infty) \to \mathbb{R}$, $f(x) = \frac{1}{x^s}$. Acesta ne spune că $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ e convergentă dacă şi numai dacă integrala improprie $\int_1^{\infty} \frac{1}{x^s} dx$ e convergentă, adică dacă şi numai dacă $s > 1$ (calculaţi integrala). Observaţi că putem folosi criteriul integral:f e descrescătoare şi pozitivă.

Astfel, pentru $s > 1$ are sens funcţia continuă $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, numită funcţia zeta (a lui Riemann). Dar iată ce se relevă:

<u>Teoremă</u> (formula lui Euler). Pentru orice $s > 1$, avem

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

Apoi, odată ce Riemann a extins funcţia ζ la planul complex (deci a definit $\zeta(\sigma)$ cu $\sigma \in \mathbb{C} \setminus \{1\}$ - pentru că formula lui Euler sugerează o legătură profundă între comportamentul funcţiei ζ şi cel numerelor prime, iar ca legătura aceasta să fie dată la iveală trebuie să ne extindem de la $\mathbb{R}$ la $\mathbb{C}$), un nou domeniu a prins contur: *Teoria Analitică a Numerelor* (studiul numerelor prin metodele analizei matematice). De exemplu, formula spectaculoasă a lui Euler e exprimarea analitică a teoremei fundamentale a aritmeticii!

Revenind la infinitudinea primelor, o mică reformulare a acestui rezultat dă naştere la o întreagă linie de probleme. Reformularea e următoarea: de-a lungul şirului $1, 2, 3, 4, \ldots, n, \ldots$, există o infinitate de numere prime. Astfel văzută teorema, ne putem întreba acelaşi lucru pentru orice şir de numere naturale $(x_n)_n$: există o infinitate de numere prime în şirul $(x_n)_n$? De exemplu:

12. Şirul $(x_n)_n$, unde $x_n = 4n + 3$, conţine o infinitate de numere prime.

Soluţie. Ideea e să modificăm puţin argumentul original al lui Euclid. Presupunem că ar exista doar un număr finit de numere prime $p_1, \ldots, p_s$ care să fie de forma $4n + 3$. Atunci considerăm numărul $N = 4(p_1 \ldots p_s) - 1 = 4(p_1 \ldots p_s - 1) + 3$. Fie avem că N e prim, fie avem că N se descompune într-un produs de numere prime, dar dintre care nici unul nu poate fi $p_1, p_2, \ldots, p_s$ (altminteri unul dintre ele l-ar divide pe 1, absurd). Nici nu se poate ca toţi factorii primi ai lui N să fie de forma $4n + 1$ (N nu e de forma asta, iar $(4a + 1)(4b + 1) = 4(4ab + a + b) + 1 \overset{not}{=} 4c + 1$), aşa că măcar unul e de forma $4n + 3$, iar asta intră în contradicţie cu ce am lămurit mai devreme ($p_1, \ldots, p_s$ sunt presupuse a fi <u>toate</u> primele de forma $4n + 3$). Rămâne că N e prim, e de forma $4n + 3$ şi e diferit de $p_1, \ldots, p_s$ - contradicţie.

La fel se poate arăta că există o infinitate de prime de forma $4n+1$ sau $6n+5$. De fapt:

Teoremă (Dirichlet). Fie $a, b \in \mathbb{Z}$ relativ prime. Atunci există o infinitate de numere prime în progresia $(a+nb)_{n\in\mathbb{N}}$ (observaţi că dacă $(a,b) \neq 1$, atunci nu e nimic de discutat).

Aceasta a fost conjecturată de către Legendre şi demonstrată de către Dirichlet (pe urmele lui Euler), arătând că seria $\sum\limits_{p\equiv a\,(mod\,b)} \frac{1}{p}$ diverge folosind teoria seriilor Fourier în variantă discretă....

Sper că s-a conturat puţin o idee despre ce se întâmplă în $\mathbb{Z}$. De fapt, din toată partea elementară a teoriei numerelor, nu am vorbit nimic despre cel mai important rezultat - TEMĂ: Citiţi despre legea reciprocităţii pătratice.

Data viitoare ne mutăm în $k[X]$.