Tipurile subgrupurilor finite din $GL_2(\mathbb{Z})$

Gabriel DOSPINESCU[1]

Studiul care urmează este o continuare a celui început în [**1**]. Cu acel prilej am demonstrat o serie de rezultate care ne-au permis să găsim majorări pentru ordinele subgrupurilor finite ale lui $GL_n(\mathbb{Z})$.

Ne-am bazat pe o teoremă de mare profunzime, cunoscută sub numele de *Lema lui Serre*. De fapt, rezultatul a fost obţinut de *Minkowski* şi extins de *Selberg*, drept pentru care îl vom numi în cele ce urmează *Lema lui Selberg*.

Ne-a mai rămas, din planul nostru, să demonstrăm că în $GL_2(\mathbb{Z})$ există exact nouă tipuri de grupuri finite (până la un izomorfism). Am adus deja în discuţie marea teoremă *Jordan-Zassenhaus*, care asigură că în $GL_n(\mathbb{Z})$ există un număr finit de clase de conjugare ale subgrupurilor finite, rezultat mult mai puternic şi mai greu de demonstrat decât ceea ce am numit noi "versiunea slabă" a teoremei *Jordan-Zassenhaus*. De asemenea, pentru $n \geq 3$, studiul subgrupurilor lui $GL_n(\mathbb{Z})$ devine foarte laborios şi complicat; de exemplu, in [**2**] se demonstrează că există 73 de clase de conjugare ale subgrupurilor finite din $GL_3(\mathbb{Z})$. Chiar studiul claselor de conjugare ale subgrupurilor finite din $GL_2(\mathbb{Z})$ este dificil (de altfel, in finalul articolului vom discuta problema conjugării subgrupurilor ciclice ale lui $GL_2(\mathbb{Z})$).

Teorema 5. *Există exact nouă clase de izomorfism ale subgrupurilor finite ale lui* $GL_2(Z)$.

Demonstraţie. Desigur, aici considerăm şi subgrupurile triviale. Deja ştim (din teorema 2) că ordinul oricărui subgrup finit al lui $GL_2(\mathbb{Z})$ divide pe 24; prin urmare, ordinul unui subgrup finit al lui $GL_2(\mathbb{Z})$ poate fi doar unul dintre numerele: 1, 2, 3, 4, 6, 8, 12 sau 24.

Să observăm că şapte clase de izomorfism se găsesc destul de repede. Într-adevăr, subgrupuri cu un element sau două se găsesc fără probleme, cu trei elemente putem lua subgrupul generat de $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, pentru patru elemente putem alege subgrupul generat de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (izomorf cu $\mathbb{Z}_4$) şi subgrupul format din matricile I_2, $-I_2$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ şi $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$), iar pentru şase elemente putem lua subgrupul generat de $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ (izomorf cu $\mathbb{Z}_6$) şi subgrupul generat de matricile $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ şi $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (izomorf cu grupul S_3 al permutărilor de grad 3). Mai mult, teoremele de structură ale grupurilor cu cel mult şase elemente arată că acestea sunt singurele posibilităţi pentru subgrupurile lui $GL_2(\mathbb{Z})$ cu cel mult 6 elemente. Ne mai rămâne să dovedim că există câte o singură clasă de izomorfism pentru subgrupuri din $GL_2(\mathbb{Z})$ cu 8 elemente şi tot una pentru cele cu 12 elemente.

Un subgrup abelian cu opt elemente al lui $GL_2(\mathbb{Z})$ (ca, de altfel, orice subgrup abelian cu opt elemente) ar trebui să fie izomorf cu $\mathbb{Z}_8$, cu $\mathbb{Z}_2 \times \mathbb{Z}_4$, sau cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

[1] Student, École Normale Supérieure, Paris

Cum orice element din $GL_2(\mathbb{Z})$ are ordinul 2, 3, 4, sau 6 (nu şi 8), nu există subgrup al lui $GL_2(\mathbb{Z})$ izomorf cu $\mathbb{Z}_8$.

Acum să facem câteva observaţii generale despre matricile de ordin 2, 3 sau 4 din $GL_2(\mathbb{Z})$. În primul rând se poate stabili (chiar cu mijloace elementare, fără a folosi adică noţiuni ca polinom caracterisitic, valori proprii, etc) că orice matrice de ordin 2 este fie $-I_2$, fie are forma $\begin{pmatrix} x & y \\ z & -x \end{pmatrix}$, cu x, y, z numere întregi astfel încât $x^2 + yz = 1$. O matrice A de ordinul patru trebuie să verifice polinomul $X^4 - 1$, deci (fiind cu elemente numere întregi) trebuie să aibă valorile proprii ± 1 sau $\pm i$; cum $A^2 \neq I_2$, rămâne a doua variantă, deci $A^2 = -I_2$ şi $A = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$, cu x, y, z numere întregi astfel încât $x^2 + yz = -1$. În sfârşit, argumente asemănătoare conduc la concluzia că, dacă A are ordinul 3, atunci valorile sale proprii sunt ε şi ε^2 (ε fiind o rădăcină cubică diferită de 1 a unităţii), deci A are urma -1 şi determinantul 1 şi $A = \begin{pmatrix} x & y \\ z & -1-x \end{pmatrix}$, cu x, y, z numere întregi astfel încât $x^2 + x + 1 + yz = 0$.

Acum să presupunem că există în $GL_2(\mathbb{Z})$ un subgrup izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ şi să privim elementele lui ca matrici complexe. Fiind de ordinul al doilea, ele sunt diagonalizabile şi, deoarece ele comută două câte două, există o bază comună de diagonalizare. În acea bază, matricile din G sunt diagonale şi au pe diagonala principală valorile lor proprii care sunt ± 1 (căci toate, cu excepţia identităţii, au ordinul 2). Astfel s-ar obţine existenţa a opt matrici de ordinul al doilea cu ± 1 pe diagonala principală şi 0 în rest, evident absurd (acest argument funcţionează în general: ordinul maxim al unui subgrup al lui $GL_n()$ care are toate elementele de ordinul 2 – desigur, cu excepţia elementului neutru – este 2^n; ceea ce furnizează şi o demonstraţie elegantă a faptului că, pentru $m \neq n$, $GL_m(\mathbb{Z})$ nu este izomorf cu $GL_n(\mathbb{Z})$, o problemă greu de rezolvat altfel).

Existenţa unui subgrup al lui $GL_2(\mathbb{Z})$ izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_4$ ar implica şi existenţa a două matrici $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, de ordinul al doilea şi $B = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$, de ordinul 4, cu a, b, c, x, y, z numere întregi, $a^2 + bc = 1$ şi $x^2 + yz = -1$, care comută: $AB = BA$. Condiţia aceasta (de comutativitate) ne dă sistemul $bz = cy$, $ay = bx$, $az = cx$. Presupunerea că un element, oricare, al celor două matrici este nul conduce la o contradicţie (de exemplu, $a = 0$ implică $bc = 1$ şi $yz = -1$ şi acestea contrazic $bz = cy$). Dacă sunt nenule, a şi b sunt prime între ele, la fel x şi y; de aceea, din $ay = bx$ rezultă $a = \pm x$ şi $b = \pm y$, apoi obţinem şi $c = \pm z$ (semnele corespund), deci $A = \pm B$, evident o contradicţie. De altfel, se constată uşor că, tot pe această cale, se poate obţine şi afirmaţia demonstrată mai sus: orice subgrup al lui $GL_2(\mathbb{Z})$ format numai din elemente de ordin 2 (cu excepţia elementului neutru) are cel mult patru elemente; desigur, în cazul general nu se poate proceda aşa.

Un subgrup necomutativ cu opt elemente este izomorf fie cu grupul diedral, fie cu cel al cuaternionilor. Un subgrup al lui $GL_2(\mathbb{Z})$ cu opt elemente, izomorf cu grupul diedral, este cel generat de matricile $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ şi $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (omitem de fiecare dată verificările, acestea fiind imediate). Ne mai rămâne să demonstrăm că $GL_2(\mathbb{Z})$ nu

are subgrupuri izomorfe cu grupul cuaternionilor.

Presupunem că există un asemenea subgrup; asta ar însemna, de fapt, că există matricile $A, B \in GL_2(\mathbb{Z})$, astfel încât $AB = B^3A$, $A^2 = B^2$, $B^4 = I_2$ şi ordinul lui B este 4; cum am văzut, asta înseamnă că $A^2 = B^2 = -I_2$, ceea ce duce şi la $AB = -BA$. Rezultă existenţa unor numere întregi a,b, c, x, y, z astfel încât $a^2 + bc + 1 = x^2 + yz + 1 = 0$ şi astfel încât $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ şi $B = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$. Egalitatea $AB = -BA$ implică şi $2ax + bz + cy = 0$; eliminând c, z din primele două relaţii şi folosind-o pe a treia, rezultă $(bx - ay)^2 + b^2 + y^2 = 0$, deci $b = y = 0$, ceea ce, evident, conduce la contradicţie.

Să ne îndreptăm acum atenţia asupra subgrupurilor cu 12 elemente ale lui $GL_2(\mathbb{Z})$; considerăm mai întâi un asemenea subgrup G neabelian. Să presupunem că printre numerele $x_2, \ldots, x_q$ nu apare şi 1; cum $(2 - (-1))(2 - 0) = 6$ şi cum $12 \mid (2 - x_2) \cdots (2 - x_q)$, trebuie să avem $x_q = -2$. Deci există $a, b \in$, cu $a + b = 10$ astfel încât $12 | 2^k + a \cdot 0^k + b \cdot (-1)^k + (-2)^k$, oricare ar fi k număr natural. Este clar că trebuie să avem atunci $b = 0$, iar alegerea $k = 2$ conduce iarăşi la o contradicţie. Astfel că trebuie să existe o matrice $A \in G$ cu urma egală cu 1.

Fie u, v valorile proprii ale matricii A (care verifică $u + v = 1$). Cum $A^{12} = I_2$, u şi v au modulul 1, deci $\dfrac{1}{uv} = \dfrac{1}{u} + \dfrac{1}{v} = \overline{u} + \overline{v} = \overline{u + v} = 1$. Din $u + v = uv = 1$ rezultă $u^3 = v^3 = -1$, deci $A^3 = -I_2$, adică A are ordinul 6. Să mai considerăm $B \in G - \{A^k \mid 0 \leq k \leq 5\}$ şi să observăm că vom avea atunci $G = \{A^k \mid 0 \leq k \leq 5\} \cup \{BA^k \mid 0 \leq k \leq 5\}$ şi că $AB = BA^5$. Într-adevăr, este clar (din modul în care l-am ales pe B) că există $k \geq 0$ astfel încât $AB = BA^k$, ceea ce înseamnă că matricile $A^k = B^{-1}AB$ şi A sunt similare, deci au aceleaşi valori proprii. Atunci mulţimile $\{u^k, \frac{1}{u^k}\}$ şi $\{u, \frac{1}{u}\}$ coincid, ceea ce duce imediat la posibilităţile $k \equiv 1 \pmod 6$ sau $k \equiv 5 \pmod 6$. Cum G este neabelian rămâne $k \equiv 5 \pmod 6$ şi $AB = BA^5$. Aceasta se mai scrie (ţinând cont de $A^2 - A + I_2 = 0_2$, adică de teorema *Cayley-Hamilton*) $AB + BA = B$, iar de aici obţinem $\operatorname{tr}(B) = 2\operatorname{tr}(AB)$. Cum matricile de ordin 3 sau 6 au urma impară, B trebuie să aibă ordinul 2 sau 4. Să presupunem că B ar avea ordinul 4; ca mai sus va rezulta că $B^2 = -I_2$. Un scurt moment de reflecţie arată existenţa unor numere întregi a, b, c, x, y, z astfel încât $a^2 + bc + 1 = x^2 + yz + 1 = 0$ şi $A = \begin{pmatrix} x & y \\ z & 1 - x \end{pmatrix}$, $B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Atunci, din $AB + BA = B$, după un mic calcul obţinem relaţia $u^2 - u + 1 + \left(\dfrac{y}{b}\right)^2 = 0$ ($u = \dfrac{ay}{b} - x$), egalitate evident imposibilă. Astfel rezultă că B are ordinul 2, deci singurul subgrup necomutativ de ordin 12 din $GL_2(\mathbb{Z})$ ar putea fi cel diedral. Şi nici nu e greu să arătăm că există în $GL_2(\mathbb{Z})$ un subgrup izomorf cu D_6: este cel generat de matricile: $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ şi $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$.

În fine, să presupunem că G ar fi un subgrup abelian cu 12 elemente al lui $GL_2(\mathbb{Z})$. După cum am amintit (v. mai sus problema de olimpiadă), ordinul oricărei matrici din $GL_2(\mathbb{Z})$ poate fi doar 1, 2, 3, 4 sau 6; prin urmare G ar putea fi izomorf (din cele două tipuri de grupuri comutative, adică $\mathbb{Z}_{12}$ şi $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$) doar cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ (deoarece $\mathbb{Z}_{12}$ este generat de un element de ordin 12).

Să zicem că ar fi în $GL_n(\mathbb{Z})$ un subgrup izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$; acesta conţine mai mult de un element de ordin 2 (prin urmare şi o matrice de ordin 2 diferită de $-I_2$) , precum şi elemente de ordin trei, deci atunci ar exista matricile $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, de ordin 2 ($a, b, c \in \mathbb{Z}$, $a^2 + bc = 1$) şi $B = \begin{pmatrix} x & y \\ z & -1-x \end{pmatrix}$ de ordin 3 ($x, y, z \in \mathbb{Z}$, $x^2+x+1+yz = 0$) astfel încât $AB = BA$. Obţinem relaţiile $bz = cy$, $2ay = b(2x+1)$ şi $2az = c(2x+1)$; vedem imediat că de aici s-ar obţine, dacă am presupune $a = 0$, că $b = c = 0$, imposibil. De aceea $a \neq 0$ şi putem exprima $y = \dfrac{b(2x+1)}{2a}$ şi $c = \dfrac{c(2x+1)}{2a}$; înlocuim în $x^2 + x + 1 + yz = 0$, mai ţinem seama şi de $bc = 1 - a^2$ şi ajungem iar la o evidentă contradicţie: $3a^2 + (2x+1)^2 = 0$; deci $GL_2(\mathbb{Z})$ nu are subgrupuri comutative cu 12 elemente.

Ne-a mai rămas să demonstrăm că nu există subgrupuri cu 24 de elemente în $GL_2(\mathbb{Z})$. Din păcate, oricât ne-am străduit, nu am reuşit să găsim o astfel de demonstraţie care să utilizeze ideile de mai sus. Se poate însă arăta acest fapt, trecând la un nivel superior al edificiului matematic. Avem, mai întâi

Teorema 6. *Orice subgrup finit al lui $GL_n(\mathbb{Z})$ este conjugat cu un subgrup al lui $O_n(\mathbb{R})$.*

Demonstraţie. Prin $O_n(\mathbb{R})$ înţelegem grupul matricilor ortogonale din $GL_n(\mathbb{Z})$. G fiind subgrupul finit despre care este vorba în enunţ, vom defini un nou produs scalar pe $\mathbb{R}^n$ (unde elementele se consideră ca vectori coloană) prin

$$\langle x, y\rangle_* = \sum_{g\in G} \langle gx, gy\rangle,$$

unde $\langle \cdot, \cdot \rangle$ este produsul scalar obişnuit din $\mathbb{C}^n$. Deoarece fiecare matrice din G este inversabilă, se verifică uşor faptul că şi $\langle \cdot, \cdot \rangle_*$ este un produs scalar, precum şi că

$$\langle gx, gy\rangle_* = \langle x, y\rangle_*, \quad \forall x, y \in \mathbb{C}^n,$$

adică orice element din G este izometrie faţă de acest nou produs scalar. Prin urmare, matricile din G sunt matrici ortogonale într-o bază ortonormală relativ la acest produs, ceea ce reprezintă (reformulată) concluzia lemei. Acum putem demonstra

Teorema 7. *Orice subgrup finit al lui $GL_2(\mathbb{Z})$ este fie ciclic, fie diedral.*

Demonstraţie. Fie, iar, G un subgrup finit al lui $GL_2(\mathbb{Z})$, pe care, conform teoremei anterioare îl putem considera direct subgrup al lui $O_2(\mathbb{R})$, şi fie H intersecţia lui G cu $SO_2(\mathbb{R})$, adică cu grupul (matricilor) rotaţiilor lui $\mathbb{R}^2$ (matrici ortogonale cu determinantul 1). Indicele lui H în G este cel mult egal cu 2 (deoarece, pentru orice $x, y \in G$, xy^{-1} este o matrice ortogonală care are determinantul 1 sau -1). În plus, H este un grup ciclic, deoarece este un grup finit de rotaţii şi se arată uşor că orice asemenea grup este generat de o rotaţie a sa de unghi minim (tot aşa cum se arată că orice subgrup al lui $\mathbb{Z}$ este generat de un element al său de modul minim).

Acum, dacă intersecţia H are indicele 1 în G, evident vom avea $G = H$, deci G este ciclic. Dacă indicele este 2, considerăm un element $s \in G - H$, care trebuie să fie o simetrie faţă de o dreaptă ce trece prin origine. Se verifică atunci cu uşurinţă (fie prin calcul, fie – recurgând la interpretarea geometrică – pe un desen) că $srs = r^{-1}$,

r fiind generatorul lui H. Cum s^2 este identitatea şi G este generat de s şi de r (indicele lui H în G fiind 2) obţinem imediat că, în acest caz, G este diedral.

În fine, Teorema 5 rezultă din nou, sub forma:

Teorema 8. *Orice subgrup finit al lui $GL_2(\mathbb{Z})$ are cel mult 12 elemente şi există doar o clasă de izomorfism a subgrupurilor lui $GL_2(\mathbb{Z})$ cu 12 elemente.*

Demonstraţie. Totul rezulta din teorema anterioara si vesnica observatie ca matricile din $GL_2(\mathbb{Z})$ au ordin 1, 2, 3, 4 sau 6. Evident, teorema 7 implică şi faptul că există doar 9 tipuri de clase de izomorfism pentru subgrupurile lui $GL_2(\mathbb{Z})$, dar noi ne-am străduit mai sus (şi nu am reuşit în totalitate) să arătăm că se poate obţine acelaşi rezultat şi pe cale "elementară".

Terminăm acest articol ţinându-ne o promisiune: stabilirea claselor de conjugare ale matricilor de ordin 3, 4, 6 din $GL_2(\mathbb{Z})$. Nu vom trata cazul matricilor de ordin 2, din simplul motiv că necesită o cu totul altă metodă. Vom folosi fără demonstraţie un rezultat clasic de geometria numerelor, anume faimoasa teoremă a lui Minkowski: orice mulţime convexă, simetrică în raport cu originea şi de arie strict mai mare decât 4 din $\mathbb{R}^2$ conţine măcar un punct laticial nenul. Vom începe cu următoarea aplicaţie directă a teoremei lui Minkowski, care se va dovedi crucială în studiul claselor de conjugare ale matricilor de ordin finit:

Lema 1. *a) Dacă a, b, c sunt numere întregi astfel încât $bc = a^2 + 1$, atunci ecuaţia $\left|cx^2 - 2axy + by^2\right| = 1$ are soluţii în numere întregi.*

b) Dacă $bc = a^2 + a + 1$, atunci ecuaţia $\left|cx^2 - (2a+1)xy + by^2\right| = 1$ are soluţii întregi.

Demonstraţia este uşoară dacă folosim teorema lui Minkowski şi foarte grea altfel. Ideea este următoarea (vom rezolva doar a), punctul b) fiind absolut identic): dacă considerăm A mulţimea punctelor (x, y) din plan pentru care $\left|cx^2-2axy+by^2\right| < 2$, un calcul imediat arata ca A are aria strict mai mare decat 4. Într-adevăr, putem în mod evident presupune $b, c > 0$ şi atunci condiţia se scrie $z^2 + t^2 < 2$, unde $z = x\sqrt{c} - \frac{a}{\sqrt{c}}y$ şi $t = \frac{y}{\sqrt{c}}$. Deci A este imaginea cercului de arie 2π prin aplicatia liniara $(z, t) \to (\frac{z+at}{\sqrt{c}}, \sqrt{c}t)$. Or, aceasta aplicaţie conservă ariile, căci matricea asociată are determinantul 1. Deci A are aria $2\pi > 4$ si totul rezultă acum din teorema lui Minkowki: A conţine un punct laticial nenul (x, y) şi pentru acest punct, mereu în ipoteza $b, c > 0$, avem în mod evident $\left|cx^2 - 2axy + by^2\right| = 1$. Cum am spus, b) urmează exact aceeaşi cale de demonstraţie, deci rămâne în seama cititorului.

Acum putem începe să studiem conjugarea matricilor de ordin 3, 4, 6. Mai precis, vom demonstra următoarea:

Teorema 9. *Există exact o clasă de conjugare in $GL_2(\mathbb{Z})$ pentru matricile de ordin 3 din $GL_2(\mathbb{Z})$. Aceeaşi concluzie este valabilă pentru matricile de ordin 4 şi pentru cele de ordin 6.*

Demonstraţie. Dacă $A \in GL_2(\mathbb{Z})$ este de ordin 3, respectiv 6, am văzut în timpul studiului tipului de izomorfism al subgrupurilor finite că $A^2 + A + I_2 = O_2$ şi $A^2 - A + I_2 = O_2$, respectiv. Să considerăm o matrice A de ordinul 3. Am văzut

că A se poate scrie sub forma $\begin{pmatrix} a & -b \\ c & -1-a \end{pmatrix}$ unde $a, b, c \in \mathbb{Z}$ verifică $a^2 + a + 1 = bc$. Aplicând lema, rezultă că există un vector nenul $e = (x, y)$ astfel încât $|\det(e, Ae)| = 1$ (aici (e, Ae) este matricea care are prima coloană egală cu e şi pe cea de-a doua cu Ae): un calcul imediat arată că de fapt condiţia $|\det(e, Ae)| = 1$ este echivalentă cu $\left|cx^2 - (2a+1)xy + by^2\right| = 1$. Aceasta înseamnă că (e, Ae) este o bază a lui $\mathbb{Z}^2$, în sensul că matricea (e, Ae) este în $GL_2(\mathbb{Z})$. Or, $A(Ae) = A^2e = -Ae - e$, deci în această bază matricea lui A este exact $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Am arătat astfel că elementele de ordin 3 sunt toate conjugate între ele. Cu exact aceleaşi argumente se arată că elementele de ordinul 4, respectiv 6 au aceeaşi proprietate.

Cititorul ar putea să se întrebe în acest moment: de ce am inclus ultimul rezultat în acest articol? Răspunsul este simplu: cum în tot articolul am oscilat între algebră şi teoria numerelor şi cum am început cu algebra, preferăm să terminăm cu teoria numerelor. Şi, într-adevar, din ultima teoremă obţinem câteva rezultate foarte frumoase din acest domeniu. Să luăm, de exemplu, iarăşi cazul matricilor de ordin 3. Am văzut ca pentru o astfel de matrice, scrisă sub forma $\begin{pmatrix} a & -b \\ c & -1-a \end{pmatrix}$, putem găsi $P \in GL_2(\mathbb{Z})$ astfel încât $A = P^{-1}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}P$. Scriind $P = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, un scurt calcul arată că există $\epsilon = \det P \in \{-1, 1\}$ astfel încât

$$a = \epsilon(yz - xy - zt),\ b = \epsilon(y^2 - yt + t^2) \quad \text{şi}$$
$$c = \epsilon(z^2 - xz + x^2),\ d = \epsilon(zt - xt + xy),$$

unde $xt - yz = \epsilon$. Aceasta este deci soluţia generală a ecuaţiei $a^2 + a + 1 = bc$ în numere întregi. Încercaţi să demonstraţi aceasta prin alte mijloace şi veţi vedea avantajele acestei metode. Să mai subliniem un rezultat, deloc banal, care se poate obţine de aici. Să presupunem că p este un număr prim de forma $3k + 1$ şi să luăm u o rădăcină primitivă modulo p. Notând $x = u^{\frac{p-1}{3}}$, obţinem imediat că $x \neq 1$ şi $x^3 = 1$, deci $x^2 + x + 1 = 0$ (lucrăm in $\mathbb{Z}/p\mathbb{Z}$). Aceasta arată existenţa unui număr întreg a pentru care $p \mid a^2 + a + 1$. Din cele observate anterior, rezultă că p se poate scrie sub forma $x^2 - xy + y^2$ pentru nişte numere întregi x şi y. Am arătat astfel că orice număr prim de forma $3k + 1$ poate fi exprimat ca $x^2 - xy + y^2$ (cu x, y întregi). Evident, lucrând cu matricile de ordin 4, ajungem cu aceleaşi argumente la frumoasa teoremă a lui Fermat: orice număr prim de forma $4k + 1$ se scrie ca suma a două pătrate de numere întregi.

Încheiem aici scurta noastră vizită în lumea subgrupurilor lui $GL_2(\mathbb{Z})$, nu înainte de a sugera cititorului temerar un studiu al claselor de izomorfism ale subgrupurilor finite ale lui $GL_3(\mathbb{Z})$.

Bibliografie

1. **G. Dospinescu** - *Câteva proprietăţi ale subgrupurilor finite din $GL_n(\mathbb{Z})$*, Recreaţii Matematice 1/2006.
2. **Ken-Ichi Tahara** - *On the finite subgroups of $GL_3(\mathbb{Z})$*, Nagoya Math. Journal.