ASUPRA PROBLEMEI 27388

ION BĂETU[1)]

Abstract. This note establishes a more general frame for the contents of the problem 27388 from Gazeta Matematică.

Keywords: order of an element in a group, unities of the group $U(\mathbb{Z}_n)$
MSC: 20K01

În nota de faţă ne propunem să prezentăm un rezultat care constituie o extindere a unei probleme, propusă de domnii profesori *Mihai Piticari* şi *Vladimir Cerbu* în G.M.-B nr. 5 /2017. Iată enunţul problemei.

Fie $n \geq 2$ un număr natural. Să se arate că următoarele afirmaţii sunt echivalente:

a) $x^2 = \widehat{1}$, *oricare ar fi x inversabil în $\mathbb{Z}_n$.*

b) *n divide* 504.

Desigur, se cunoaşte că mulţimea $U(\mathbb{Z}_n)$ a elementelor inversabile ale inelului $\mathbb{Z}_n$, $n \geq 2$, formează un grup multiplicativ cu $\varphi(n)$ elemente. În particular, dacă n este prim, inelul $\mathbb{Z}_n$ este un corp, deci grupul $U(\mathbb{Z}_n)$ este ciclic, având $n-1$ elemente.

Pentru început, vom enunţa şi demonstra o proprietate utilă de izomorfism şi anume:

Teorema 1. *Fie $t \geq 2$ un număr natural şi numerele naturale nenule $n_1, n_2, \ldots, n_t$, două câte două prime între ele. Atunci grupul $U(\mathbb{Z}_{n_1 n_2 \ldots n_t})$ este izomorf cu grupul $U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2}) \times \ldots \times U(\mathbb{Z}_{n_t})$.*

Demonstraţie. Pentru orice $i \in \{1, 2, \ldots, t\}$ şi orice $x \in \mathbb{Z}$, notăm cu $\widehat{x}_i$ clasa lui x în inelul $\mathbb{Z}_{n_i}$. Dacă $x, y \in \mathbb{Z}$, cum $xy \in \mathbb{Z}$, obţinem $(\widehat{xy})_i = \widehat{x}_i \widehat{y}_i$, $\forall i \in \{1, 2, \ldots, t\}$. Fie $n = n_1 n_2 \ldots n_t$. Arătăm că funcţia

$$\widehat{x} \in U(\mathbb{Z}_n) \mapsto (\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_t) \in U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2}) \times \ldots \times U(\mathbb{Z}_{n_t})$$

este bine definită şi, totodată, reprezintă un izomorfism de grupuri.

Într-adevăr, pentru orice $x \in U(\mathbb{Z}_n)$ rezultă $(x, n_1 n_2 \ldots n_t) = (x, n) = 1$, de unde $(x, n_i) = 1$. Astfel $\widehat{x}_i \in U(\mathbb{Z}_{n_i})$, $i = 1, 2, \ldots, t$, adică $(\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_t) \in$ $\in U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2}) \times \ldots \times U(\mathbb{Z}_{n_t})$. Mai mult, dacă $\widehat{x} = \widehat{y}$, atunci n divide $x - y$ şi n_i divide n, deci n_i divide $x - y$, adică $\widehat{x}_i = \widehat{y}_i$, $i = 1, 2, \ldots, t$. Atunci $f(\widehat{x}) = (\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_t) = (\widehat{y}_1, \widehat{y}_2, \ldots, \widehat{y}_t) = f(\widehat{y})$, ceea ce înseamnă că funcţia f este bine definită.

Avem $f(\widehat{x}\widehat{y}) = f(\widehat{xy}) = (\widehat{xy}_1, \widehat{xy}_2, \ldots, \widehat{xy}_t) = (\widehat{x}_1\widehat{y}_1, \widehat{x}_2\widehat{y}_2, \ldots, \widehat{x}_t\widehat{y}_t) =$ $= (\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_t)(\widehat{y}_1, \widehat{y}_2, \ldots, \widehat{y}_t) = f(\widehat{x})f(\widehat{y})$, deci f este un morfism de grupuri.

Pentru orice $\widehat{x} \in \mathrm{Ker} f$ avem $(\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_t) = (\widehat{0}_1, \widehat{0}_2, \ldots, \widehat{0}_t)$, de unde n_i divide x, $i = 1, 2, \ldots, t$. Întrucât numerele $n_1, n_2, \ldots, n_t$ sunt, două

[1)] Profesor, Colegiul Naţional „M. Eminescu“, Botoşani.

câte două, prime între ele, rezultă că n divide x, adică $\widehat{x} = \widehat{0}$. Aşadar $\mathrm{Ker}f = \{\widehat{0}\}$, deci f este injectivă. Atunci $|\mathrm{Im}f| = |U(\mathbb{Z}_n)| = \varphi(n) = \varphi(n_1)\varphi(n_2)\ldots\varphi(n_t) = |U(\mathbb{Z}_{n_1}) \times U(\mathbb{Z}_{n_2}) \times \ldots \times U(\mathbb{Z}_{n_t})|$, deci codomeniul lui f şi $\mathrm{Im}f$ au acelaşi număr de elemente. Astfel funcţia f este şi surjectivă, deci bijectivă. □

Propoziţia 2. *Fie $n \geq 2$ un număr natural şi q un divizor prim al numărului n. Atunci există în $U(\mathbb{Z}_n)$ un element de ordin q, dacă q^2 divide n, sau un element de ordin $q-1$, dacă q^2 nu divide n.*

Demonstraţie. Dacă q^2 divide n, atunci q divide $\varphi(n)$, deci, conform teoremei lui *Cauchy*, există în $U(\mathbb{Z}_n)$ un element de ordin q.

În caz contrar, fie $m = \dfrac{n}{q}$. Întrucât $(m, q) = 1$, grupurile $U(\mathbb{Z}_q) \times U(\mathbb{Z}_m)$ şi $U(\mathbb{Z}_n)$ sunt izomorfe. Notând cu a un generator al grupului ciclic $U(\mathbb{Z}_q)$ şi cu $\tilde{1}$ elementul neutru al grupului $U(\mathbb{Z}_m)$, o verificare simplă arată că $(a, \tilde{1})$ este un element de ordin $q-1$ în grupul $U(\mathbb{Z}_q) \times U(\mathbb{Z}_m)$, de unde cerinţa.

□

Propoziţia 3. *Fie $n \geq 2$ un număr natural şi m un număr prim de forma $m = 2p^s + 1$, unde p este prim, $p \geq 3$ şi $s \in \mathbb{N}^*$. Considerăm mulţimea $D = \{i \in \{1, 2, \ldots, s\} \mid 2p^i + 1$ este prim$\}$. Atunci, următoarele afirmaţii sunt echivalente*:

a) $x^{2p^s} = \widehat{1}, \forall x \in U(\mathbb{Z}_n)$.

b) *n divide* $24 \cdot \prod_{i \in D}(2p^i + 1)$.

Demonstraţie. a) $\Rightarrow$ b). Din $s \in D$ rezultă $D \neq \emptyset$. Conform ipotezei, ordinul oricărui element din $U(\mathbb{Z}_n)$ divide $2p^s$. Astfel, în virtutea teoremei lui *Cauchy*, putem scrie $\varphi(n) = 2^a p^b$, unde $a, b \in \mathbb{N}$.

Dacă 7 divide n, atunci 3 divide $\varphi(n)$, deci $3 \in \{2, p\}$, fals. Prin urmare $(7, n) = 1$, de unde $7 \in U(\mathbb{Z}_n)$. Din $\widehat{7}^{2p^s} = \widehat{1}$ rezultă că n divide $7^{2p^s} - 1$.

Să presupunem că 5 divide n. Dacă 25 divide n, atunci 5 divide $\varphi(n)$, de unde $p = 5$. Astfel n divide $7^{2 \cdot 5^s} - 1$ şi, întrucât 5 divide n, rezultă că 5 divide $7^{2 \cdot 5^s} - 1$, număr cu cifra unităţilor 8, fals. Dacă 25 nu divide n, conform proprietăţii 2), există în $U(\mathbb{Z}_n)$ un element de ordin 4, deci 4 divide $2p^s$, contradicţie.

Prin urmare $(5, n) = 1$, adică $\widehat{5} \in U(\mathbb{Z}_n)$. Atunci $\widehat{5}^{2p^s} = \widehat{1}$, de unde n divide $5^{2p^s} - 1 = 25^{p^s} - 1 = 24r$, unde $r = 25^{p^s - 1} + 25^{p^s - 2} + \ldots + 25 + 1$. Cei doi factori din ultimul produs sunt primi între ei, căci suma din scrierea lui r conţine un număr impar de termeni impari, deci r este nedivizibil cu 2, iar din $r \equiv p^s \pmod 3$ şi p^s nedivizibil cu 3 rezultă că r este nedivizibil cu 3.

Fie $t \in D$. Întrucât $5 < 2p^t + 1$, obţinem $(5, 2p^t + 1) = 1$. Astfel, în virtutea teoremei lui *Fermat*, $2p^t + 1$ divide $5^{2p^t} - 1$ şi atunci, cu atât mai mult, $2p^t + 1$ divide $5^{2p^s} - 1$. Dar $(24, 2p^t + 1) = 1$, deci $2p^t + 1$ divide r, $\forall t \in D$. Cum numerele de forma $2p^t + 1$, $t \in D$, sunt două câte două prime

între ele, rezultă că $\prod_{i\in D}(2p^i+1)$ divide r, de unde $5^{2p^s}-1=24\cdot\prod_{i\in D}(2p^i+1)h$, cu $h\in\mathbb{N}^*$ şi $(24,h)=1$.

Dacă $(2p^t+1)^2$ divide n pentru un număr $t\in D$, atunci există în $U(\mathbb{Z}_n)$ un element de ordin $2p^t+1$. Astfel $2p^t+1$ divide $2p^s$, adică $2p^t+1\in\{2,p\}$, fals. Prin urmare $(2p^i+1)^2$ nu divide n, $\forall\, i\in D$. Mai mult, dacă q este un divizor prim al lui n, atunci $q\in\{2,3\}\cup\{2p^i+1\mid i\in D\}$.

Într-adevăr, în ipoteza q^2 divide n, există în $U(\mathbb{Z}_n)$ un element de ordin q, deci q divide $2p^s$. Cum $q=p$ implică p divide $5^{2p^s}-1$, putem scrie $\tilde{5}^{2p^s}=\tilde{1}$, egalitate gândită în $\mathbb{Z}_p$. Din p divide n şi 5 nu divide n rezultă $(5,p)=1$, deci $\tilde{5}^{p-1}=\tilde{1}$, sau încă $\tilde{5}^p=\tilde{5}$. Atunci $\tilde{5}^{p^s}=\tilde{5}$, aşa că $\tilde{1}=\tilde{5}^{2p^s}=(\tilde{5}^{p^s})^2=\tilde{25}$, adică p divide 24, fals. Aşadar $q\neq p$ şi q divide $2p^s$, deci $q=2$.

Dacă q^2 nu divide n, atunci există un element $u\in U(\mathbb{Z}_n)$ cu $\mathrm{ord}(u)=q-1$. Pe de altă parte, din $\widehat{u}^{2p^s}=\widehat{1}$ rezultă

$$\mathrm{ord}(u)\in\{2\}\cup\{p^i\mid i\in\{1,2,\ldots,s\}\}\cup\{2p^i\mid i\in\{1,2,\ldots,s\}\},$$

deci $q\in\{3\}\cup\{p^i+1\mid i\in\{1,2,\ldots,s\}\}\cup\{2p^i+1\mid i\in\{1,2,\ldots,s\}\}$.

Deoarece $q=p^i+1$, cu $1\leq i\leq s$ implică $q>3$ şi q impar, contradicţie, găsim $q\in\{3\}\cup\{2p^i+1\mid i\in\{1,2,\ldots,s\}\}$. Dar q este prim, deci $q\in\{3\}\cup\{2p^i+1\mid i\in D\}$.

În definitiv, n este de forma $n=2^a3^b\prod_{i\in D}(2p^i+1)^{c_i}$, unde $a\in\{0,1,2,3\}$, $b\in\{0,1\}$ şi $c_i\in\{0,1\}$, $\forall i\in D$, de unde n divide $24\prod_{i\in D}(2p^i+1)$.

b) $\Rightarrow$ a). Fie $D=\{i_1,i_2,\ldots,i_t\}$, cu $1\leq t\leq s$. În virtutea ipotezei, avem $n=2^a3^b\prod_{i\in D}(2p^i+1)^{c_i}$, unde $a\in\{0,1,2,3\}$, $b\in\{0,1\}$ şi $c_i\in\{0,1\}$, $\forall\, i\in D$.

Notând cu $\widehat{1}_a$ elementul unitate din inelul $\mathbb{Z}_{2^a}$, cu $\widehat{1}_b$ elementul unitate din inelul $\mathbb{Z}_{3^b}$ şi cu $\widehat{1}_{c_{i_k}}$ elementul unitate din inelul $\mathbb{Z}_{(2p^{i_k}+1)^{c_{i_k}}}$, unde $1\leq k\leq t$, cerinţa de demonstrat este o consecinţă imediată a izomorfismului de grupuri $U(\mathbb{Z}_n)$ şi $U(\mathbb{Z}_{2^a})\times U(\mathbb{Z}_{3^b})\times U(\mathbb{Z}_{(2p^{i_1}+1)^{c_{i_1}}})\times U(\mathbb{Z}_{(2p^{i_2}+1)^{c_{i_2}}})\times\ldots\times$ $\times U(\mathbb{Z}_{(2p^{i_t}+1)^{c_{i_t}}})$ cât şi a faptului că $x^2=\widehat{1}_a$, $a=0,1,2,3$, $\forall x\in U(\mathbb{Z}_{2^a})$, apoi $x^2=\widehat{1}_b$, $b=0,1$, $\forall x\in U(\mathbb{Z}_{3^b})$ şi $x^{2p^{i_k}}=\widehat{1}_{c_{i_k}}$, $k=1,2,\ldots,t$, $x\in\mathbb{Z}_{(2p^{i_k}+1)^{c_{i_k}}}$.

Bibliografie

[1] I. Băetu, C. Băetu, *Capitole speciale de algebră*, Ed.Taida, Iaşi, 2015.
[2] M. Piticari, V. Cerbu, *Problema 27388*, Gazeta Matematică - B nr. 5/2017.
[3] M. Ţena, *Algebră*, Ed. Corint, 1996.