DIVIZIBILITATE ŞI NUMERE PRIME

de MIRCEA BECHEANU

Vom nota cu **N** mulţimea numerelor naturale,

$$\mathbf{N} = \{0,1,2,\ldots,n,\ldots\}$$

şi cu **Z** mulţimea numerelor întregi,

$$\mathbf{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}.$$

Mulţimea numerelor întregi are o structură de inel în raport cu adunarea şi înmulţirea numerelor. Datorită acestui fapt, în unele probleme de teoria numerelor este mai convenabil să lucrăm cu numere întregi, această lărgire a cadrului permiţând folosirea metodelor algebrice.

Vom folosi în mod curent două proprietăţi fundamentale ale mulţimii numerelor întregi.

1. Axioma lui *Peano*. *Dacă M este o mulţime de numere naturale care îndeplineşte condiţiile* :

($P1$) $O \in M$;

($P2$) *dacă* $n \in M$ *atunci* $n+1 \in M$

atunci $M = \mathbf{N}$.

Această axiomă stă la baza principiului inducţiei matematice, o metodă prin care se demonstrează că o propoziţie matematică depinzând de o variabilă n, $n \in \mathbf{N}$, este adevărată pentru orice valoare naturală a variabilei.

2. Principiul elementului minimal. *Orice submulţime nevidă* $A \subset \mathbf{N}$ *conţine un cel mai mic element* (*i.e. există* $a \in A$ *astfel încât* $a \leq x$, $\forall x \in A$).

3. Teoremă. *Axioma lui Peano şi principiul elementului minimal sunt echivalente.*

Demonstraţie. Presupunem că în **N** este îndeplinit principiul elementului minimal şi fie $M \subset \mathbf{N}$ o submulţime care satisface ($P1$) şi ($P2$). Presupunem prin absurd că există $m \in \mathbf{N}$, $m \notin M$. Rezultă că mulţimea

$\overline{M} = \{m \in \mathbf{N} \mid m \notin M\}$ este nevidă. Fie n_0 cel mai mic element al lui $\overline{M}$. Deoarece M satisface $(P1)$ rezultă că $n \neq 0$. Deci $n_0 > 0$; atunci $n_1 = n_0 - 1 \in \mathbf{N}$ şi $n_1 \notin M$. Conform $(P2)$ rezultă că $n_0 = n_1 + 1 \in M$; s-a obţinut o contradicţie.

Reciproc, fie $A \subset \mathbf{N}$ o submulţime. Dacă $0 \in A$ atunci 0 este cel mai mic element al lui A. Dacă $0 \notin A$, notăm cu M mulţimea numerelor naturale n care îndeplinesc condiţia : $n \leq x$, $\forall\, x \in A$. Este evident că $0 \in M$. Deoarece $A \neq \varnothing$, există $a \in A$ şi atunci $a + 1 \notin M$; deci $M \neq \mathbf{N}$. Conform axiomei $(P2)$ rezultă că există $m \in M$ astfel încât $m + 1 \notin M$. Afirmăm că m este cel mai mic element al lui A. Într-adevăr din definiţia lui M rezultă că $m \leq x$, $\forall\, x \in A$. În plus, $m \in A$ deoarece $m \notin A$ implică $m < x$, $\forall\, x \in A$ şi aceasta implică $m + 1 \in M$.

Reamintim unele definiţii. Dacă a, b sunt numere întregi, spunem că a divide pe b, sau că a este un divizor al lui b dacă există un număr întreg c astfel încât $b = ac$. Vom nota relaţia "*a divide pe b*" prin $a \mid b$. Se mai spune uneori că b este un multiplu al lui a. Se vede că oricare ar fi $a \in \mathbf{Z}$ avem $a \mid 0$ şi $1 \mid a$, $-1 \mid a$. Relaţia de divizibilitate este reflexivă şi tranzitivă ; aceasta înseamnă că ea este o relaţie de preordine pe $\mathbf{Z}$. Divizibilitatea nu este o relaţie simetrică, nici antisimetrică. În schimb avem următorul rezultat :

4. Lemă. *Fie $a, b \in \mathbf{Z}$. Următoarele afirmaţii sunt echivalente* :

(i) $a \mid b$ şi $b \mid a$

(ii) $a = \pm b$.

Demonstraţie. (i) $\Rightarrow$ (ii). Din $b = ac$ şi $a = bc'$ rezultă $a = acc'$ şi deci $a(cc' - 1) = 0$. Dacă $a = 0$, din $a \mid b$ rezultă $b = 0$ şi prin urmare $a = b$. Dacă $a \neq 0$, din $cc' = 1$ rezultă $c' = \pm 1$. Reciproca, (ii) $\Rightarrow$ (i) este evidentă.

Pentru orice număr întreg a, notăm cu D_a mulţimea divizorilor (întregi) ai lui a. În condiţiile lemei precedente, dacă $a \mid b$ şi $b \mid a$ rezultă că a şi b au aceleaşi mulţimi de divizori, adică $D_a = D_b$. Spunem, în acest caz, că a şi b sunt *asociate în divizibilitate*. Pe mulţimea numerelor naturale, relaţia de divizibilitate este antisimetrică : $a \mid b$ şi $b \mid a \Rightarrow a = b$. Deci două numere naturale sunt asociate în divizibilitate dacă şi numai dacă sunt egale.

Pentru orice număr întreg a notăm cu $a\mathbf{Z}$ mulţimea multiplilor lui a :

$$a\mathbf{Z} = \{n \in \mathbf{Z} \mid a \mid n\}.$$

Din definiţie rezultă că $a\mathbf{Z} = \{n \in \mathbf{Z} \mid \exists c \in \mathbf{Z}, n = ac\} = \{ac \mid c \in \mathbf{Z}\}$. Mulţimea multiplilor lui a are următoarea proprietate importantă :

dacă $b, c \in a\mathbf{Z}$ atunci $bm + cn \in a\mathbf{Z}$, oricare ar fi $m, n \in \mathbf{Z}$.

În particular, rezultă că $0 \in a\mathbf{Z}$ şi $b, c \in a\mathbf{Z} \Rightarrow b - c \in a\mathbf{Z}$. În Algebră se spune că $a\mathbf{Z}$ este un ideal al mulţimii $\mathbf{Z}$ şi aceasta ne conduce să dăm definiţia noţiunii de ideal.

5. Definiţie. *O submulţime nevidă $I \subset \mathbf{Z}$ se numeşte ideal dacă îndeplineşte condiţia :*

(I) oricare ar fi $a, b \in I$ şi oricare ar fi $x, y \in \mathbf{Z}$,

$$ax + by \in I.$$

Este clar că dacă $a \neq 0$, mulţimea $a\mathbf{Z}$ este infinită. Este de asemenea clar că dacă $a = 0$ atunci $D_0 = \mathbf{Z}$, că $D_1 = \{\pm 1\}$ şi că D_a conţine cel puţin elementele a, $-a$, 1, -1, oricare ar fi a. Ce se poate spune în general despre D_a când $a \neq 0$ şi $a \neq \pm 1$?

6. Definiţie. *Numărul întreg p se numeşte indecompozabil dacă $p \neq 0$, $p \neq \pm 1$ şi p nu are alţi divizori, exceptându-i pe ± 1, $\pm p$.*

Să observăm că p este indecompozabil dacă şi numai dacă $-p$ este indecompozabil ; numerele 2 şi -2 sunt indecompozabile deci există asemenea numere. Un număr întreg nenul şi diferit de ± 1 care nu este indecompozabil se numeşte decompozabil. Pentru a studia decompozabilitatea este suficient să ne limităm la numerele naturale. Rezultă că $n \in \mathbf{N}$ este decompozabil dacă şi numai dacă admite un divizor d, $1 < d < n$.

7. Propoziţie. *Orice număr natural n, $n > 1$, admite un divizor q indecompozabil.*

Demonstraţie. Dacă n este indecompozabil, afirmaţia este apriori demonstrată. Presupunem că n este decompozabil. Fie M mulţimea divizorilor d ai lui n, $1 < d < n$. Deoarece M este nevidă, ea are un cel mai mic element q. Atunci q este indecompozabil deoarece orice divizor d al lui q cu $1 < d < q$ este un divizor al lui n, şi $n < q$.

8. Teorema fundamentală a Aritmeticii (*Euclid*). *Orice număr întreg a diferit de zero şi de ± 1 este un produs finit de numere indecompozabile.*

Demonstraţie. Este suficient să demonstrăm afirmaţia pentru numere naturale n, $n > 1$. Din aceasta va rezulta afirmaţia : orice număr întreg a, $a \neq 0$ şi $a \neq \pm 1$ se scrie ca un produs finit

$$a = \pm q_1 q_2 \dots q_t$$

unde q_i sunt numere naturale indecompozabile. Dacă n este indecompozabil afirmaţia este adevărată. Presupunem că există numere naturale $n > 1$, care nu se descompun într-un produs finit de numere indecompozabile. Considerăm mulţimea M a acestor numere. Aceasta conţine un cel mai mic element n ; n este număr decompozabil, deci $n = n_1 n_2$ unde $1 < n_1 < n$; $1 < n_2 < n$. Rezultă că $n_1 \notin M$, $n_2 \notin M$. Deci n_1 şi n_2 se descompun în produse finite de numere indecompozabile :

$$n_1 = q_{11} q_{12} \dots q_{1r},\ n_2 = q_{21} q_{22} \dots q_{2s}.$$

Deci $n = q_{11} \dots q_{1r} q_{21} \dots q_{2s}$ se descompune ca un produs finit de numere indecompozabile.

9. Teorema fundamentală a Aritmeticii (*Gauss*). *Descompunerea unui număr întreg n, diferit de zero şi* ± 1, *ca produs finit de numere indecompozabile înmulţit cu semnul* ± 1 *este unică, mai puţin ordinea factorilor.*

Vom da două demonstraţii ale acestei teoreme, care a fost pentru prima dată formulată şi demonstrată de *Gauss* în celebrul său tratat "Disquisitiones Arithmeticae" (1801) (cf. [1], Addenda, cap. I).

10. Prima demonstraţie a teoremei 9. Este suficient să ne rezumăm la numere naturale mai mari ca 1. Presupunem că există numere naturale n, $n > 1$, care admit descompuneri distincte ca produs de numere indecompozabile. Fie M mulţimea acestor numere şi fie a cel mai mic element al lui M. Rezultă că

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s ,$$

unde p_i, q_j sunt indecompozabile. Remarcăm că $\forall\ i = 1,\dots, r$ şi $\forall\ j = 1,\dots, s$, $p_i \neq q_j$; în caz de egalitate se împarte cu $p_i = q_j$ şi se contrazice alegerea lui a. Putem presupune că $p_1 \leq p_2 \leq \dots \leq p_r$ şi $q_1 \leq q_2 \leq \dots \leq q_s$. Deoarece $p_1 \neq q_1$ putem presupune că $p_1 < q_1$. Considerăm numărul $b = p_1 q_2 \dots q_s$. Este evident că $b < a$ şi deci $a - b \geq 1$. Dar din $p_1 \mid a - b$ rezultă că $a - b > 1$. Deoarece $a - b > 1$ şi $p_1 \mid a - b$, aplicând teorema 8 rezultă că $a - b$ are descompunerea

$$a - b = p_1 l_1 \dots l_t . \tag{10.1}$$

Pe de altă parte avem egalitatea $a - b = (q_1 - p_1) q_2 \dots q_s$. Dacă $q_1 - p_1 > 1$, aplicând teorema 8, obţinem descompunerea

$$q_1 - p_1 = k_1 \dots k_v ,$$

unde nici unul din k_1, k_2, ..., k_v nu este p_1, căci $p_1 \nmid q_1 - p_1$. Pentru $a - b$ se obţine descompunerea

$$a - b = k_1 \dots k_v q_2 \dots q_s . \tag{10.2}$$

Descompunerile (10.1) şi (10.2) ale lui $a - b$ sunt diferite căci în (10.1) apare p_1, iar în (10.2) nu apare p_1. Deoarece $a - b < a$ şi are două descompuneri distincte, se contrazice alegerea lui a.

11. Definiţie. *Un număr întreg p diferit de* ± 1 *se numeşte număr prim dacă îndeplineşte condiţia :*

(P) oricare ar fi $a, b \in \mathbf{Z}$ *astfel încât* $p \mid ab$, *rezultă* $p \mid a$ *sau* $p \mid b$.

Se vede că 0 verifică această definiţie, dar el este un număr prim special.

12. Lemă. *Orice număr prim nenul este indecompozabil.*

Demonstraţie. Presupunem că $p > 0$ şi că $p = ab$ unde $a < p$, $b < p$. Din proprietatea evidentă $p \mid ab$ rezultă : $p \mid a$ sau $p \mid b$. Presupunem că $p \mid a$. Deoarece avem şi $a \mid p$, rezultă $p = a$. Am obţinut o contradicţie. Remarcăm că în demonstraţia lemei nu am folosit 9.

13. Teoremă. *Orice număr întreg indecompozabil este prim.*

Demonstraţie. Fie $p > 1$ un număr indecompozabil şi fie $a, b \in \mathbf{Z}$ astfel încât $p \mid ab$. Putem presupune $a > 1$ şi $b > 1$ şi fie $ab = pc$. Considerăm descompunerile în produse finite de numere indecompozabile : $a = p_1 \dots p_r$; $b = q_1 \dots q_s$; $c = k_1 \dots k_l$. Din egalitatea

$$pk_1 \dots k_l = p_1 \dots p_r q_1 \dots q_s ,$$

aplicând teorema 9, rezultă că $p = p_i$ sau $p = q_j$. Deci $p \mid a$ sau $p \mid b$.

Comentariu. Din demonstraţia de mai sus rezultă că unicitatea descompunerii unui număr întreg în produs de numere indecompozabile implică faptul că orice număr indecompozabil este prim. Vom demonstra acum teorema 13 în mod independent de teorema 9 şi apoi vom arăta că teorema 9 devine o consecinţă a teoremei 13.

14. Teoremă (teorema împărţirii cu rest). *Oricare ar fi numerele întregi a şi b, $b \neq 0$, există numerele unice q şi r astfel încât* :

(i) $a = bq + r$;

(ii) $0 \leq r < |b|$.

Demonstraţie. Vom distinge mai multe cazuri. Semnificativ este cazul $a \geq 0$ şi $b > 0$. Fixând pe b, vom demonstra prin inducţie că oricare ar fi $a \in \mathbf{N}$, există numerele naturale q şi r care verifică (i) şi (ii). Fie

$$M = \left\{ a \in \mathbf{N} \,\middle|\, \exists\, q, r \text{ a.î. } a = bq + r \text{ şi } 0 \leq r < b \right\} .$$

Este clar că $0 \in M$, căci $0 = 0 \cdot b + 0$. Presupunem că $a \in M$, adică $a = bq + r$, $0 \leq r < b$. Avem :

$$a + 1 = bq + r + 1 .$$

Dacă $r + 1 < b$, rezultă că $a + 1 \in M$. Dacă $r + 1 = b$ scriem $a + 1 = b(q + 1) + 0$ şi din nou rezultă $a + 1 \in M$.

Cazul al doilea : $a > 0$, $b < 0$. Aplicând cazul precedent lui a şi $-b$ obţinem $a = (-b)q + r$ cu $0 \leq r < |b|$. Scriind egalitatea precedentă sub forma $a = b(-q) + r$, demonstraţia rezultă.

Cazul al treilea : $a < 0$, $b > 0$. Din primul caz avem $-a = bq + r$ cu $0 \leq r < b$. Dacă $r = 0$, înmulţim egalitatea precedentă cu -1 şi obţinem $a = b(-q) + 0$. Dacă $0 < r < b$, înmulţim egalitatea precedentă cu -1 şi o scriem sub forma :

$$a = b(-q - 1) + (b - r) ,$$

unde $0 < b - r < b$.

Cazul al patrulea : $a < 0$, $b < 0$. Se procedează ca la cazul precedent. Să demonstrăm unicitatea lui q şi r ; fie scrierile $a = bq + r$ şi $a = bq' + r'$ cu

$0 \le r < |b|$, $0 \le r' < |b|$. Presupunem că $r < r'$; prin scăderea celor două egalităţi rezultă $b(q-q') = r'-r$, unde $0 < r'-r < |b| - r \le |b|$. Dar din egalitatea precedentă şi $q-q' \neq 0$ rezultă $|b(q-q')| = |b||q-q'| \ge |b|$. Am obţinut o contradicţie. Deci $r = r'$ şi atunci avem imediat $q = q'$.

(14.1) *Completare la definiţia* 5. Orice ideal I, $I \subset \mathbf{Z}$, este de forma $I = a\mathbf{Z}$. Dacă $I = 0$, afirmaţia este clară. Dacă $I \neq 0$, atunci I conţine numere naturale nenule. Fie $M = I \cap \mathbf{N}^*$ şi fie a cel mai mic element al lui M. Avem evident $a\mathbf{Z} \subset I$. Pe de altă parte, pentru orice element $n \in I$, există q şi $r \in \mathbf{Z}$ astfel încât $n = aq + r$ şi $0 \le r < a$. Rezultă că $r = n - aq \in I$; deoarece $r < a$ şi $r \in I$ rezultă $r = 0$ şi prin urmare $n \in a\mathbf{Z}$.

15. O nouă demonstraţie a teoremei 13. Presupunem că există numere indecompozabile care nu sunt prime şi fie $p > 1$ un indecompozabil neprim minimal. Aceasta înseamnă că există numere naturale nenule a, b astfel încât $p \nmid a, p \nmid b$ şi $p \mid ab$. Alegem o asemenea pereche cu ab minim. Din teorema împărţirii cu rest avem egalităţile :

$$a = pq + r \text{ şi } 0 < r < p,$$

$$b = pq' + r' \text{ şi } 0 < r' < p.$$

Înmulţind cele două relaţii obţinem :

$$ab = p(pqq' + q'r + qr') + rr'.$$

Deci $p \mid rr'$. Din condiţia de minimalitate a produsului ab rezultă că $ab = rr'$, deci $q = q' = 0$ şi $a = r$, $b = r'$. Aşadar avem $p \mid ab$ cu $a < p$ şi $b < p$.

Fie $ab = pc$, cu $c > 1$ (deoarece $c = 1$ contrazice faptul că p este indecompozabil). Fie q divizor indecompozabil al lui c. Avem $pqc' = ab < p \cdot p$, deci $qc' < p$, deci $q < p$. Deoarece q este indecompozabil mai mic decât p, q este prim. Din $q \mid ab$ rezultă $q \mid ab$ rezultă $q \mid a$ sau $q \mid b$. Fie $a = qa'$; atunci $pc' = a'b$ implică $p \mid a'b$, $a'b < ab$ şi aceasta contrazice minimalitatea lui ab.

16. A doua demonstraţie a teoremei 9. *Fie $a > 1$ un număr întreg şi fie descompunerile sale*

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

unde p_i, q_j sunt numere indecompozabile. Din $p_1 \mid q_1 q_2 \dots q_s$ şi faptul că p_1 este prim rezultă că există $j_1 \in \{1, 2, \dots, s\}$ astfel încât $p_1 \mid q_{j_1}$. Deoarece q_{j_1} este ireductibil rezultă $p_1 = q_{j_1}$. Simplificând cu $p_1 = q_{j_1}$ rezultă $p_2 \dots p_r = q_1 \dots q_{j_1-1} q_{j_1+1} \dots q_s$.

În mod asemănător, există $j_2 \neq j_1$ astfel încât $p_2 = q_{j_2}$ ş.a.m.d. Nu putem avea $r < s$ sau $r > s$ deoarece simplificând la fiecare pas câte un număr

indecompozabil obţinem că 1 este un produs de numere indecompozabile. În acest fel rezultă că cele două descompuneri au acelaşi număr de factori indecompozabili şi că aceştia coincid, abstracţie făcând de ordinea lor în produs.

Deoarece noţiunile de număr prim nenul şi număr indecompozabil coincid, se foloseşte prin tradiţie termenul de număr prim.

17. Teoremă (*Euclid*). *Mulţimea numerelor naturale prime este infinită.*

(17.1) *Prima demonstraţie* (*Euclid*). Presupunem prin absurd că numărul numerelor prime este finit : fie acestea p_1, p_2, ..., p_n. Considerăm numărul $N = p_1p_2 \ldots p_n + 1$. Conform propoziţiei 7, N admite un divizor prim q. Deoarece q coincide cu unul din numerele p_i, din $p_i \mid N$ rezultă $p_i \mid 1$. Am obţinut o contradicţie.

(17.2) *A doua demonstraţie.* Este suficient să arătăm că pentru orice număr natural n există un număr prim p, $p > n$. Pentru aceasta alegem un divizor prim al numărului $N = n! + 1$.

(17.3) *A treia demonstraţie.* Pentru orice număr natural n există un număr prim p satisfăcând condiţiile : $n < p < n!$. Pentru aceasta se ia un divizor prim al lui $N = n! - 1$.

(17.4) *A patra demonstraţie* (*Euler*). Presupunem prin absurd că există numai un număr finit de numere prime p_1, p_2, ..., p_k. Pentru orice i, $1 \le i \le k$ avem seria geometrică infinită

$$\sum_{n=0}^{\infty} \frac{1}{p_i^n} = \frac{p_i}{p_i - 1}.$$

Dar făcând produsul acestor serii se obţine :

$$\prod_{i=1}^{k}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\ldots+\frac{1}{p_i^n}+\ldots\right) = \sum_{n_1,n_2,\ldots,n_k} \frac{1}{p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}} = \sum_{n=1}^{\infty} \frac{1}{n},$$

ultima egalitate fiind o consecinţă a teoremei 8. Rezultă că

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \frac{p_i}{p_i - 1},$$

adică seria armonică este convergentă. S-a obţinut o contradicţie.

(17.5) *A cincea demonstraţie* (*G. Pólya*). Pentru orice număr natural n se formează numărul lui *Fermat* $f_n = 2^{2^n} + 1$. Numerele lui *Fermat* $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65.537$ sunt numere prime.

Vom demonstra acum afirmaţia : *dacă* $m \neq n$ *atunci* f_m *şi* f_n *nu au nici un divizor prim în comun.* Într-adevăr, dacă presupunem că $m = n + k$ are loc identitatea :

$$\frac{f_{n+k}-2}{f_n}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{\left(2^{2^n}\right)^{2^k}-1}{2^{2^n}+1}=\left(2^{2^n}\right)^{2^k-1}-\left(2^{2^n}\right)^{2^k-2}+\ldots-1.$$

În consecinţă dacă $p \mid f_n$ şi $p \mid f_{n+k}$ rezultă $p \mid 2$. Aceasta nu se poate deoarece numerele f_n sunt impare. Pentru a încheia demonstraţia este suficient să observăm că mulţimea numerelor prime conţine mulţimea divizorilor primi ai numerelor *Fermat* şi că aceasta este infinită ca o reuniune infinită de mulţimi (finite) disjuncte.

(17.6) *A şasea demonstraţie (Marcel Ţena).* Presupunem prin absurd că mulţimea numerelor prime este finită ; fie acestea $p_1, p_2, \ldots, p_k$. Pentru orice n, $n > 1$, considerăm mulţimile

$$A_n = \{1,2,3,\ldots,2^n\}$$

$$B_n = \left\{p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} \mid 0 \le r_i \le n\right\}.$$

Conform teoremei 9, are loc incluziunea de mulţimi $A_n \subset B_n$, deoarece orice număr întreg este un produs de numere prime şi elementele lui A_n nu depăşesc $p_1^n p_2^n \ldots p_k^n$. Trecând la cardinalele celor două mulţimi se obţine egalitatea : $2^n \le (n+1)^k$. Rezultă că

$$\frac{2^n}{(n+1)^k} \le 1.$$

Trecând la limită pentru $n \to \infty$, se obţine o contradicţie.

(17.7) Există metode variate de a fabrica şiruri de numere naturale având termenii primi doi câte doi şi de a folosi apoi aceste şiruri pentru a proba infinitatea numerelor prime. Exemplificăm aceasta cu următoarea problemă folosită la testarea elevilor pentru a 38-a O.I.M. în anul 1997 : *oricare ar fi numărul natural $a > 1$, şirul $(x_n)_{n\ge 1}$ definit prin $x_n = a^{n+1} + a^n - 1$ conţine o infinitate de termeni, relativi primi doi câte doi.*

(M. Becheanu)

Prima soluţie a problemei foloseşte principiul cutiei. Observăm mai întâi că doi termeni consecutivi ai şirului sunt numere relativ prime ; deci şirul conţine numere relativ prime două câte două. Fie

$$x_{n_1}, x_{n_2}, \ldots, x_{n_k}$$

o mulţime finită de termeni relativ primi doi câte doi şi fie

$$N = \prod_{i=1}^{k} x_{n_k}.$$

Numerele $a^0 = 1, a, a^2, \ldots, a^N$ sunt $N+1$ numere distincte ; conform principiului cutiei există $i > j$ a.î. $a^i \equiv a^j \pmod N$. Deoarece $(N, a) = 1$ rezultă că

$a^{i-j}-1 \equiv 0 \pmod N$. În consecinţă $\left(N, a^{i-j+1}+a^{i-j}-1\right)=1$. Deci la mulţimea $\left\{x_{n_1}, x_{n_2}, \ldots, x_{n_k}\right\}$ poate fi adăugat x_{i-j}.

A doua soluţie se bazează pe utilizarea teoremei lui *Fermat*. Notăm cu P mulţimea divizorilor primi ai lui N (de mai sus!) şi fie $n=\prod_{p\in P}(p-1)$.

Deoarece $(p, a)=1$, $\forall\, p\in P$ rezultă că $a^{p-1}\equiv 1 \pmod p$, $\forall p\in P$ şi prin urmare $a^{n+1}+a^n-1\equiv a \pmod p$. Aceasta arată că $\left(a^{n+1}+a^n-1, p\right)=1$, $\forall p\in P$, şi deci avem $\left(a^{n+1}+a^n-1, N\right)=1$.

18. Cum putem obţine numere prime ?

Deoarece mulţimea P a numerelor naturale prime este infinită rezultă că ele formează un şir infinit ; scriindu-le în ordine crescătoare obţinem şirul

$$2, 3, 5, 7, \ldots, p_n, \ldots$$

unde p_n este al n-lea număr prim. În legătură cu proprietăţile acestui şir matematicienii au pus, de-a lungul timpului, numeroase probleme extrem de interesante. Unele dintre acestea, cu totul neelementare, sunt nerezolvate, până în prezent. Vom trece în revistă câteva probleme cu caracter elementar privind şirul $\left(p_n\right)_{n\geq 1}$.

Dacă numărul natural n este destul de mare, este dificil să decidem dacă el este prim sau nu. Matematicienii au încercat încă din cele mai vechi timpuri să construiască numere prime mari. Pentru aceasta s-a încercat să se găsească funcţii numerice ale căror valori să fie numere prime.

(18.1) *P. Fermat a presupus că pentru orice* $n \geq 0$, *numerele* $f_n=2^{2^n}+1$ *sunt prime.* Am văzut deja (vezi (17.5)) că f_0, f_1, f_2, f_3, f_4 sunt numere prime. *L. Euler* a demonstrat că f_5 nu este prim şi anume că f_5 este divizibil cu 641. Reproducem o demonstraţie simplă a acestei afirmaţii care aparţine lui *G. T. Benneton* (cf. [1], cap. I). Scriem pe f_5 sub forma :

$$f_5=2^{2^5}+1=2^{32}+1=\left(2\cdot 2^7\right)^4+1.$$

Să punem $a=2^7$ şi $b=5$. Atunci $f_5=2^4\cdot a^4+1$. Dar

$$2^4=3b+1=(128-125)b+1=\left(a-b^3\right)b+1.$$

Deci :
$$f_5=\left(ab-b^4+1\right)a^4+1=\left(1+ab\right)a^4+\left(1-a^4b^4\right)=$$

$$=\left(1+ab\right)a^4+\left(1+ab\right)\left(1-ab\right)\left(1+a^2b^2\right)=\left(1+ab\right)\left[a^4+\left(1-ab\right)\left(1+a^2b^2\right)\right].$$

Prin calcul : $1+ab=641$ şi deci $641 \mid f_5$. Pentru o informaţie completă putem adăuga că avem descompunerea $f_5=641\cdot 6700417$.

Ipoteza lui *Fermat* a plecat de la următoarea observaţie : pentru ca numărul $2^n + 1$ să fie prim este necesar ca n să nu aibă factori primi impari, cu alte cuvinte n să fie de forma $n = 2^k$. Într-adevăr, dacă $n = pq$ cu p impar atunci :

$$2^n + 1 = \left(2^q\right)^p + 1 = \left(2^q + 1\right)\left(2^{q(p-1)} - 2^{q(p-2)} + \ldots - 2^q + 1\right),$$

ceea ce arată că $2^n + 1$ nu este prim.

(18.2) *L. Euler* a demonstrat că *nu există nici un polinom cu coeficienţi întregi* $P(t) \in \mathbf{Z}[t]$, *astfel încât toate numerele*

$$P(0), P(1), P(2), \ldots, P(n), \ldots$$

să fie numere prime.

El a dat exemple de polinoame care iau valori numere prime pentru un număr mare de valori ale lui n, dar nu pentru toate valorile lui n. De exemplu,

$$P(t) = t^2 - 79t + 1601,$$

furnizează 80 numere prime : $P(0) = 1601$, $P(1) = 1523$, $P(2) = 1447$, ... , $P(79) = 1601$. Dar $P(80) = 1681 = 41^2$.

Reproducem demonstraţia lui *Euler* privind afirmaţia de mai sus.

Fie polinomul $P(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$. Presupunem că există un număr întreg a astfel încât $P(a) = p$, p număr prim. Pentru orice întreg k vom calcula :

$$P(a + kp) - P(a) = \sum_{i=1}^{n} a_i \left[(a + kp)^i - a^i \right] =$$

$$= \sum_{i=1}^{n} a_i kp \left[(a + kp)^{i-1} + (a + kp)^{i-2} a + \ldots + a^{i-1} \right] = pN.$$

Rezultă că pentru orice $k \in \mathbf{Z}$, $P(a + kp)$ este divizibil cu p. Dacă presupunem prin absurd că $P(m)$ este prim, pentru orice $m \in \mathbf{Z}$, rezultă că $P(m) = \pm p$. Rezultă că cel puţin una din valorile $\pm p$ este luată pentru o infinitate de valori ale lui m. Aceasta este o contradicţie.

Din (18.1) şi (18.2) s-a văzut că este dificil de construit o funcţie elementară $h : \mathbf{N} \to \mathbf{N}$ cu proprietatea : $h(n)$ este număr prim pentru orice n. Cu atât mai mult, este dificil să caracterizăm funcţia $f : \mathbf{N}^* \to \mathbf{N}$, $f(n) = p_n$. În schimb se pot da majorări pentru funcţia $f(n) = p_n$.

(18.3) Teoremă. *Pentru orice* $n \geq 1$ *are loc inegalitatea*

$$p_n \leq 2^{2^{n-1}},$$

şi egalitatea are loc numai pentru $n = 1$.

Demonstraţie. Într-adevăr, $p_1 = 2 = 2^{2^{n-1}}$ şi $p_2 = 3 < 2^{2^{2-1}} = 4$.

Presupunem că $p_k < 2^{2^{k-1}}$, $\forall k$, $2 \leq k \leq n$. Din demonstraţia (17.1) rezultă că $p_{n+1} \mid p_1 p_2 \ldots p_n + 1$.

Deci $p_{n+1} \le p_1 p_2 \dots p_n + 1 < 2 \cdot 2^2 \cdot 2^{2^2} \dots 2^{2^{n-1}} + 1 = 2^{2^n - 1} + 1 < 2^{2^n}$.

Putem să dăm o caracterizare a funcţiei $f(n) = p_n$, dar nu prin funcţii elementare. Teorema de mai jos aparţine lui *W. Sierpinski*.

(18.4) Teoremă. *Fie numărul real*

$$a = \frac{p_1}{10^2} + \frac{p_2}{10^2} + \dots + \frac{p_n}{10^n} + \dots .$$

Atunci $p_n = \left[10^{2^n} \cdot a\right] - 10^{2^n - 1}\left[10^{2^n} \cdot a\right]$.

Demonstrraţie. Din (18.3) rezultă că seria $\sum_{k=1}^{\infty} \frac{p_k}{10^{2^k}}$ este convergentă, folosind criteriul comparaţiei :

$$\frac{p_k}{10^{2^k}} < \frac{2^{2^{k-1}}}{2^{2^k} \cdot 5^{2^k}} < \frac{1}{2} \cdot \frac{1}{5^{2^k}}.$$

Avem :

$$\left[10^{2^n} \cdot a\right] = 10^{2^n - 2} \cdot p_1 + 10^{2^n - 2^2} \cdot p_2 + \dots + p_n + \left[\frac{p_{n+1}}{10^{2^n}} + \frac{p_{n+2}}{10^{2^n(2^2-1)}} + \dots\right] \text{ şi}$$

$$10^{2^{n-1}}\left[10^{2^{n-1}} \cdot a\right] = 10^{2^{n-1}}\left(10^{2^{n-1}-2} \cdot p_1 + 10^{2^{n-1}-2^2} \cdot p_2 + \dots + p_{n-1}\right) +$$

$$+ \left[\frac{p_n}{10^{2^{n-1}}} + \frac{p_{n+1}}{10^{2^n - 2^{n-1}}} + \dots\right].$$

Din teorema (18.3) şi argumentul adus la începutul demonstraţiei rezultă că

$$\frac{p_{n+1}}{10^{2^n}} + \frac{p_{n+2}}{10^{2^{n+2}-2^n}} + \dots + \frac{p_{n+k}}{10^{2^{n+k}-2^n}} + \dots < 1 .$$

Atunci cele două părţi întregi din egalităţile de mai sus sunt zero. Scăzând cele două egalităţi rezultă formula din enunţ.

19. Consecinţe ale teoremei fundamentale a Aritmeticii.

Am văzut că oricare ar fi numărul întreg a, $a \neq 0$, $a \neq \pm 1$, descompunerea sa în produs de numere prime conţine numai un număr finit de numere prime ; fie acestea $p_1, p_2, \dots, p_k$. Dacă notăm cu $\alpha_1, \alpha_2, \dots, \alpha_k$, $\alpha_i > 0$, respectiv numărul de factori egali cu $p_1, p_2, \dots, p_k$ avem egalitatea

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} .$$

Să notăm $\alpha_i = v_{p_i}(a)$ şi, în general, cu $v_p(a)$ exponentul lui p în descompunerea lui a, unde $v_p(a) = 0$ dacă p nu apare în această descompunere. Se obţine în acest fel, pentru orice $p \in P$, o funcţie $v_p : \mathbf{N}^* \to \mathbf{N}$, $a \to v_p(a)$, numită valuarea p-adică.

Funcţiile $(v_p)_{p\in P}$ au următoarele proprietăţi :

(v1) $v_p(ab)=v_p(a)+v_p(b)$;

(v2) $v_p(a+b)\geq \min\{v_p(a),v_p(b)\}$;

(v3) oricare ar fi $a\in\mathbf{N}^*$, mulţimea $\{v_p(a)\}_{p\in P}$ este de suport finit, adică $v_p\neq 0$ pentru cel mult un număr finit de indici $p\in P$.

(v4) pentru orice $a\in\mathbf{Z}$, $a\neq 0$ are loc egalitatea

$$a=\pm\prod_{p\in P}p^{v_p(a)}.$$

Notaţia de la punctul (v4) simplifică prezentarea unor construcţii clasice din Teoria numerelor. De exemplu, două numere nenule a, b sunt prime între ele dacă şi numai dacă suporţii famiilor $\{v_p(a)\}_p$ şi $\{v_p(b)\}_p$ sunt mulţimi disjuncte. Mai general, cel mai mare divizor comun al numerelor a, b se poate exprima prin formula :

$$(a,b)=\prod_{p\in P}p^{\min\{v_p(a),v_p(b)\}},$$

iar cel mai mic multiplu comun se poate exprima prin formula

$$[a,b]=\prod_{p\in P}p^{\max\{v_p(a),v_p(b)\}}.$$

Din formula $v_p(a)+v_p(b)=\min\{v_p(a),v_p(b)\}+\max\{v_p(a),v_p(b)\}$ şi din (v1) rezultă egalitatea

$$ab=(ab)\cdot[a,b].$$

Dacă a, $b\in\mathbf{Z}\setminus\{0\}$ atunci $a\mid b$ dacă şi numai dacă $v_p(a)\leq v_p(b)$, $\forall\ p\in P$. Din această caracterizare a divizorilor rezultă că numărul divizorilor unui număr întreg nenul este finit şi el se poate calcula. Este suficient să ne rezumăm la numere naturale. Dacă $a>0$ este număr natural şi $a=p_1^{v_1}p_2^{v_2}\dots p_k^{v_k}$, $v_i>0$, orice divizor d al lui a este de forma $d=p_1^{w_1}p_2^{w_2}\dots p_k^{w_k}$ unde $0\leq w_1\leq v_1$, $0\leq w_2\leq v_2,\dots,0\leq w_k\leq v_k$. Rezultă că numărul divizorilor lui a este

$$\tau(a)=(1+v_1)(1+v_2)\dots(1+v_k)=\prod_{p\in P}(1+v_p(a)).$$

Se poate calcula şi suma divizorilor lui a care este :

$$\sigma(a)=\sum_{0\leq w_i\leq v_i}p_1^{w_1}p_2^{w_2}\dots p_k^{w_k}=\prod_{i=1}^{k}\left(1+p_i+p_i^2+\dots+p_i^{v_i}\right)=\prod_{i=1}^{k}\frac{p_i^{v_i+1}-1}{p_i-1}.$$

Reamintim că o funcţie aritmetică este o funcţie $f:\mathbf{N}^*\to\mathbf{C}$. Cele mai des utilizate funcţii aritmetice iau valori reale sau chiar întregi.

O funcţie aritmetică f se numeşte funcţie multiplicativă dacă este nenulă şi $f(mn)=f(m)\cdot f(n)$ pentru $(m,n)=1$. Condiţia de a fi nenulă se asigură de obicei punând $f(1)=1$. Am văzut în "Mulţimi finite şi elemente de combinatorică" (*Mircea Becheanu*) că indicatorul lui *Euler*, $\varphi(n)$ este o funcţie multiplicativă.

(19.1) Propoziţie. *Funcţiile τ şi σ sunt funcţii multiplicative.*

Demonstraţie. Dacă $(a,b)=1$ atunci suporţii mulţimilor $\{v_p(a)\}_{p\in P}$ şi $\{v_p(b)\}_{p\in P}$ sunt mulţimi disjuncte, deci

$$\tau(ab)=\prod_{p\in P}(1+v_p(ab))=\prod_{v_p(ab)\neq 0}(1+v_p(ab))=$$

$$=\prod_{v_p(a)\neq 0}(1+v_p(a))\prod_{v_p(b)\neq 0}(1+v_p(b))=\tau(a)\tau(b).$$

Pentru funcţia σ avem analog :

$$\sigma(a)=\prod_{v_p(a)\neq 0}\frac{p^{v_p(a)+1}-1}{p-1}\cdot\prod_{v_p(b)\neq 0}\frac{p^{v_p(b)+1}-1}{p-1}=\sigma(a)\sigma(b).$$

Funcţiile σ şi φ sunt legate prin următorul rezultat :

(19.2) Propoziţie. *Pentru orice număr natural n este adevărată inegalitatea*

$$\frac{n^2}{2}<\varphi(n)\sigma(n)<n^2.$$

Demonstraţie. Considerăm descompunerea lui n în factori primi : $n=p_1^{k_1}\dots p_r^{k_r}$. Ţinând seama de formulele care dau pe $\varphi(n)$ şi $\sigma(n)$ avem :

$$\varphi(n)\sigma(n)=n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)\cdot n\prod_{i=1}^{r}\left(1+\frac{1}{p_i}+\dots+\frac{1}{p_i^{k_i}}\right)=$$

$$=n^2\prod_{i=1}^{r}\left(1-\frac{1}{p_i^{k_i+1}}\right)<n^2.$$

Pentru a obţine minorarea, avem mai întâi :

$$\varphi(n)\sigma(n)\geq n^2\prod_{i=1}^{r}\left(1-\frac{1}{p_i^2}\right).$$

Dar $$\prod_{i=1}^{r}\left(1-\frac{1}{p_i^2}\right)>\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\sum_{i=3}^{\infty}\frac{1}{(i+1)^2}\right)>$$

$$> \frac{3}{4}\cdot\frac{8}{9}\left(1-\int_4^{\infty}\frac{dx}{x^2}\right)=\frac{3}{4}\cdot\frac{8}{9}\cdot\frac{3}{4}=\frac{1}{2}.$$

(19.3) Definiţie. *Numerele naturale a şi b se numesc numere amiabile dacă* $\sigma(a)-a=b$ *şi* $\sigma(b)-b=a$.

Rezultă că pentru două numrere amiabile a şi b avem $\sigma(a)=\sigma(b)=a+b$. Şcoala Pitagoricienilor cunoştea numerele amiabile a = 220, $b=284$. Într-adevăr, $a=2^2\cdot 5\cdot 11$, $b=2^2\cdot 71$ şi

$$\sigma(a)=\frac{2^3-1}{2-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{71^2-1}{71-1}=7\cdot 6\cdot 12=504=220+284$$

$$\sigma(b)=\frac{2^3-1}{2-1}\cdot\frac{71^2-1}{71-1}=7\cdot 72=504.$$

Euler a găsit 65 de perechi de numere amiabile.

(19.4) Definiţie. *Numărul natural a se numeşte număr perfect dacă* $\sigma(a)-a=a$.

Deci numerele perfecte sunt amiabile cu ele însele. Pitagoricienii cunoşteau trei numere perfecte şi anume : 6, 28, 496.

(19.5) Teoremă (Euclid). *Dacă numărul* $2^{n+1}-1$ *este prim atunci numărul* $a=2^n\left(2^{n+1}-1\right)$ *este perfect.*

Demonstraţie. Fie $p = 2^{n+1}-1$. Din $a = 2^n p$ şi formula lui $\sigma(a)$ obţinem :

$$\sigma(a)=\frac{2^{n+1}-1}{2-1}\cdot\frac{p^2-1}{p-1}=p(p+1)=\left(2^{n+1}-1\right)2^{n+1}=2a.$$

Euler a demonstrat că şi reciproca acestei teoreme este adevărată şi avem următoarea :

(19.6) Teoremă (Euler). *Dacă a este un număr par perfect atunci el este de forma* $a=2^n\left(2^{n+1}-1\right)$ *şi* $p=2^{n+1}-1$ *este număr par.*

Demonstraţie. Fie a un număr perfect par şi presupunem că $a = 2^n b$, cu b impar. În virtutea multiplicativităţii lui σ avem

$$\sigma(a)=\sigma\left(2^n\right)\sigma(b)=\left(2^{n+1}-1\right)\sigma(b).$$

Pe de altă parte, din ipoteză avem $\sigma(a)=2a=2^{n+1}b$. Deci avem egalitatea :

$$\left(2^{n+1}-1\right)\sigma(b)=2^{n+1}\cdot b.$$

Rezultă că $2^{n+1}-1 \mid b$; fie $b=\left(2^{n+1}-1\right)b'$. Egalitatea de mai sus devine prin simplificare : $\sigma(b)=2^{n+1}b'$.

Pe de altă parte avem egalitatea $b+b'=\left(2^{n+1}-1\right)b'+b'=2^{n+1}\cdot b'$.

Din $\sigma(b)=b+b'$, conform definiţiei lui σ rezultă că b are numai divizorii $1=b'$ şi b. Deci $b=2^{n+1}-1$ şi b este un număr prim.

Teoremele (19.5) şi (19.6) arată că există o corespondenţă bijectivă între mulţimea numerelor perfecte pare şi mulţimea numerelor prime de forma $p=2^n-1$.

(19.7) Definiţie. *Numerele prime de forma* $p=2^n-1$, $n>1$, *se numesc numere Mersenne.*

Introducerea lor este legată şi de următoarea observaţie : dacă a^n-1 este număr prim atunci $a=2$ şi n este număr prim. Într-adevăr, dacă $a>2$ avem descompunerea :

$$a^n-1=(a-1)\left(a^{n-1}+a^{n-2}+\ldots+a+1\right).$$

Dacă n nu este prim şi admite o descompunere $n=cq$ atunci

$$2^{cq}-1=\left(2^c\right)^q-1=\left(2^c-1\right)\left(2^{c(q-1)}+2^{c(q-2)}+\ldots+2^c+1\right).$$

Deci pentru a obţine numere *Mersenne* trebuie să cercetăm numerele de forma 2^p-1 cu p prim. Şirul $\left(\pi_n\right)_{n\geq 1}$, definit prin $\pi_n=2^{p_n}-1$, se numeşte şirul lui *Mersenne*. Nu se ştie dacă în şirul lui *Mersenne* există o infinitate de numere prime, deci dacă există o infinitate de numere pare perfecte. Nu se ştie nici dacă în şirul lui *Mersenne* există o infinitate de numere compuse.

Următorul exerciţiu ne arată că şirul numerelor prime ca subşir al lui **N** are goluri de lungime oricât de mare în care se află numere compuse cu cel puţin doi factori primi distincţi.

(19.8) Exerciţiu : *pentru orice număr întreg n,* $n>1$, *există n numerre naturale consecutive, nici unul dintre ele nefiind o putere a unui număr prim.*

Prima soluţie este inspirată din (17.2). Fie $N=\left((n+1)!\right)^2+1$. Vom arăta că $N+1$, $N+2$, ..., $N+n$ satisfac condiţia. Presupunem prin absurd că există un număr k astfel încât $N+k=p^m$. Deoarece $1\leq k\leq n$ rezultă $k+1 \mid ((n+1)!)^2+k+1$, deci $k+1 \mid N+k$. Prin urmare $k+1=p^s$. Deoarece $k+1\leq n+1$ rezultă că $p^{s+1} \mid ((n+1)!)^2$, deci $p^{s+1} \mid N-1$. Deoarece avem şi $p^{s+1} \mid p^m$, deci $p^{s+1} \mid N+k$ rezultă că $p^{s+1} \mid k+1$. Aceasta este o contradicţie.

A doua soluţie se bazează pe infinitatea şirului numerelor prime. Fie $p_1<p_2<\ldots<p_{2n}$ numere prime. Sistemul de congruenţe :

$$x \equiv -1 \pmod{p_1 p_{n+1}}$$
$$x \equiv -2 \pmod{p_2 p_{n+2}}$$
$$\dots$$
$$x \equiv -n \pmod{p_n p_{2n}}$$

are o soluţie naturală N, conform teoremei chineze a resturilor. Atunci $N+1$, $N+2$, ..., $N+n$ au fiecare cel puţin doi divizori primi distincţi. Din această soluţie se vede că putem obţine o infinitate de asemenea şiruri de numere consecutive.

20. Aplicaţii. Încheiem această lecţie cu câteva exerciţii în care teorema fundamentală a artimeticii şi noţiunea de număr prim apar în prim plan. Încercăm să le grupăm în jurul ideilor fundamentale care apar în acestea.

(20.1) *Să se arate că dacă n este un număr natural impar atunci*

$$2^{\frac{\varphi(n)}{2}} \equiv \pm 1 \pmod{n}.$$

Dacă, în plus, n are doi factori primi distincţi atunci

$$2^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}.$$

Soluţie. Din $(2,n)=1$ rezultă că $2^{\varphi(n)} \equiv 1 \pmod{n}$. Deoarece $\varphi(n)$ este par avem

$$n \mid \left(2^{\frac{\varphi(n)}{2}}+1\right)\left(2^{\frac{\varphi(n)}{2}}-1\right).$$

Presupunem că $n = p^k$, p prim. Atunci $p \mid 2^{\frac{\varphi(n)}{2}}+1$ sau $p \mid 2^{\frac{\varphi(n)}{2}}-1$ şi numai una din cele două divizibilităţi este adevărată, căci altfel ar rezulta $p = 2$. Deci avem una din divizibilităţile $p^k \mid 2^{\frac{\varphi(n)}{2}}+1$ sau $p^k \mid 2^{\frac{\varphi(n)}{2}}-1$.

Să presupunem că $n = p_1^{k_1} \dots p_r^{k_r} = p_1^{k_1} \cdot Q$. Atunci $\varphi(n) = \varphi\left(p_1^{k_1}\right) \cdot \varphi(Q)$. Ca mai sus rezultă că

$$2^{\frac{\varphi\left(p_1^{k_1}\right)}{2}} \equiv \pm 1 \pmod{p_1^{k_1}}.$$

Ridicând la puterea $\varphi(Q)$ obţinem :

$$2^{\frac{\varphi(n)}{2}} \equiv (\pm 1)^{\varphi(Q)} \pmod{p_1^{k_1}},$$

$$2^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{p_1^{k_1}}.$$

Făcând acelaşi lucru pentru $p_2^{k_2},\ldots,p_r^{k_r}$ obţinem $2^{\frac{\varphi(n)}{2}} \equiv 1(\mathrm{mod}\, n)$.

Exerciţiul (20.1) poate fi rafinat astfel :

(20.2) *Dacă p este un număr prim,* $p \equiv 1(\mathrm{mod}8)$ atunci

$$2^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$$

Soluţie. Fie K un corp care conţine corpul $\mathbf{Z}/(p)$ şi în care ecuaţia $X^4 + 1 = 0$ are o rădăcină. Fie a această rădăcină ; deci $a^4 = -1$. Calculăm

$$\left(a+a^{-1}\right)^p = a^p + \binom{p}{1}a^{p-1}\cdot a^{-1} + \ldots + \binom{p}{i}a^{p-i}\cdot a^{-i} + \ldots + a^{-p} = a^p + a^{-p}.$$

Dar $a^p + a^{-p} = a^{8k+1} + a^{-(8k+1)} = a^{8k}\cdot a + a^{-8k}\cdot a^{-1} = a + a^{-1}$. Deci $\left(a+a^{-1}\right)^p = a + a^{-1}$; înmulţind cu $a + a^{-1}$ găsim

$$\left(a+a^{-1}\right)^{p+1} = \left(a+a^{-1}\right)^2 = a^2 + 2 + a^{-2} = \frac{a^4+1}{a^2} + 2 = 2.$$

Dar $\left(a+a^{-1}\right)^{p+1} = \left[\left(a+a^{-1}\right)^2\right]^{\frac{p+1}{2}}$. Deci, în corpul K avem $2^{\frac{p+1}{2}} = 2$.

Simplificând cu 2 obţinem $2^{\frac{p-1}{2}} = 1$; egalitatea are loc şi în $\mathbf{Z}\,/\,(p)$, deci ea se poate scrie :

$$2^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$$

(20.3) *Nu există nici un număr natural n,* $n > 1$ *astfel încât :*

$$n \mid 2^n - 1.$$

Soluţie. Presupunem prin absurd că există $n > 1$ a.î. $n \mid 2^n - 1$. Fie p cel mai mic divizor prim al lui n. Conform teoremei lui *Fermat*, $p \mid 2^{p-1} - 1$, deoarece n este impar, deci p este impar. Fie r ordinul lui 2 mod$p$; i.e. $p \mid 2^r - 1$ şi r este cel mai mic întreg pozitiv cu această proprietate. Atunci $r \mid p - 1$ şi $r \mid n$. Deoarece p a fost ales ca cel mai mic divizor prim al lui n şi $r < p$, rezultă că $r = 1$ sau $r = p - 1$. Cazul $r = 1$ contrazice $p \mid 2^1 - 1$ şi cazul $r = p - 1$ implică $p - 1 \mid n$, ceea ce contrazice alegerea lui p.

(20.4) Observaţie. *Există o infinitate de numere naturale n astfel încât*

$$n \mid 2^n + 1.$$

De exemplu, dacă luăm n de forma $n = 3^k$, $k > 0$, atunci

$$3^k \mid 2^{3^k} + 1.$$

Vom demonstra aceasta prin inducţie după k. Pentru $k = 1$ obţinem $3 \mid 2^3 +$ adevărat. Presupunem că $3^k \mid 2^{3^k} + 1$. Avem descompunerea :

$$2^{3^{k+1}}+1=\left(2^{3^k}\right)^3+1=\left(2^{3^k}+1\right)\left(2^{2\cdot 3^k}-2^{3^k}+1\right).$$

Este suficient să demonstrăm că $3 \mid 4^{3^k}-2^{3^k}+1$. Aceasta rezultă din $4^{3^k} \equiv 1 \pmod 3$ şi $2^{3^k} \equiv 2 \pmod 3$.

(20.5) *Singurul număr natural $n>1$ pentru care $n^2 \mid 2^n+1$ este $n=3$.*

(*L. Panaitopol*, O.I.M. 1990)

Soluţie. Fie n un număr $n > 1$, cu proprietatea $n^2 \mid 2^n+1$. Considerăm descompunerea $n = 3^k d$, unde $k \geq 0$, d este impar şi $(3, d) = 1$. Conform ipotezei avem :

$$\text{(i)} \qquad 3^{2k} \cdot d^2 \mid 2^{3^k d}+1.$$

Are loc descompunerea în factori :

$$\left(2^d\right)^{3^k}+1=\left(2^{d\cdot 3^{k-1}}\right)^3+1=\left(2^{d\cdot 3^{k-1}}+1\right)\left(2^{2d\cdot 3^{k-1}}-2^{d\cdot 3^{k-1}}+1\right).$$

Procedând prin inducţie descrescătoare după k obţinem :

$$2^{d\cdot 3^k}+1=\left(2^d+1\right)\prod_{i=0}^{k-1}\left(2^{2d\cdot 3^i}-2^{d\cdot 3^i}+1\right).$$

Pentru orice m impar avem $2^{2m}-2^m+1 \equiv 3 \pmod 9$. Aceasta se vede din faptul că $2^6 \equiv 1 \pmod 9$ şi considerând apoi cazurile $m \equiv 1,3,5 \pmod 6$. Din congruenţa de mai sus rezultă :

$$2^{2d\cdot 3^i}-2^{d\cdot 3^i}+1 \equiv 3 \pmod 9.$$

Aceasta înseamnă că produsul

$$\prod_{i=0}^{k-1}\left(2^{2d\cdot 3^i}-2^{d\cdot 3^i}+1\right)$$

este divizibil cu 3^k şi nu este divizibil cu 3^{k+1}. Revenind la ipoteza (i) rezultă

$$\text{(ii)} \qquad 3^k \mid 2^d+1.$$

Dacă $d=1$, rezultă $k=1$ şi deci $n=3$.

Presupunem $d > 1$; evident cazul $d = 2$ nu convine, deci $d \geq 5$. Deoarece d este impar şi prim cu 3, considerăm pe rând cazurile $d \equiv 1,5 \pmod 6$ şi va rezulta :

$$d \equiv 1 \pmod 6 \Rightarrow 2^d+1 \equiv 2^{6q+1}+1 \equiv 3 \pmod 9$$

$$d \equiv 5 \pmod 6 \Rightarrow 2^d+1 \equiv 2^{6q+5}+1 \equiv 2^5+1 \equiv 6 \pmod 9.$$

Deoarece $9 \nmid 2^d+1$ rezultă $k=0$ sau $k=1$.

Fie p cel mai mic factor prim al lui d, $d \geq 5$. Din $p \mid 2^n+1$ rezultă $2^n \equiv -1 \pmod p$, deci $2^{2n} \equiv 1 \pmod p$. Din teorema lui *Fermat*, avem şi

$2^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Fie δ ordinul lui 2, modulo p. Atunci $2^{\delta} \equiv 1 (\mathrm{mod}\, p)$ şi deoarece δ e minim cu această proprietatea avem $\delta \mid p-1$, $\delta \mid 2n$. Din modul în care a fost luat p rezultă $(p-1, d) = 1$, şi aceasta implică $(\delta, d) = 1$. Deoarece $\delta \mid 2 \cdot 3^k \cdot d$, cu $k = 0$ sau $k = 1$ rezultă că $\delta \in \{1, 2, 3, 6\}$.

Revenim la $2^{\delta} \equiv 1 (\mathrm{mod}\, p)$; rezultă că p divide unul din numerele 1, 3, 7, 63. Deoarece $p \geq 5$, rămâne cazul $p = 7$. Dar 7 nu divide $2^n + 1$ pentru nici un întreg $m > 0$, deoarece

$$m = 3q + r \Rightarrow 2^m + 1 = 2^{3q} \cdot 2^r + 1 = (7+1)^q \cdot 2^r + 1 \equiv$$

$$\equiv 2^r + 1 (\mathrm{mod}\, 7) \equiv 2,3 \text{ sau } 5 (\mathrm{mod}\, 7).$$

Aceasta contrazice faptul că $p \mid 2^n + 1$. Rămâne singura posibilitate, $d = 1$ şi $n = 3$ (din (ii)).

(20.6) *Dacă $n > 1$ atunci n nu divide $2^{n-1} + 1$.*

(*W. Sierpinski*, [2], pg. 235)

Presupunem prin absurd că există $n > 1$ a.î. $n \mid 2^{n-1} + 1$. Atunci n este impar. Mai întâi observăm că n nu poate fi număr prim. Într-adevăr, dacă p este număr prim avem $2^{p-1} \equiv 1 (\mathrm{mod}\, p)$, conform teoremei lui *Fermat*. Din $p \mid 2^{p-1} + 1$ şi $p \mid 2^{p-1} - 1$ rezultă $p \mid 2$, deci $p = 2$; contradicţie. Observăm apoi că n nu este o putere a unui număr prim. Dacă $n = p^k$, aplicăm teorema lui *Euler* şi avem $2^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, p^k)$, deci $p^k \mid 2^{p^k - p^{k-1}} - 1$, Conform ipotezei avem şi $p^k \mid 2^{p^k} + 1$. Prin adunare rezultă $p^k \mid 2^{p^k - p^{k-1}} \left(2^{p^{k-1}} + 1\right)$. Deoarece p este prim cu 2, rezultă $p^k \mid 2^{p^{k-1}} + 1$. Este suficient să facem o inducţie descrescătoare după k şi obţinem o contradicţie.

Presupunem acum că $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, $k_i > 0$. Observăm mai întâi că n este prim cu $2^{n-1} - 1$; într-adevăr, dacă q este un factor prim comun al lui n şi $2^{n-1} - 1$, folosind faptul că $q \mid 2^{n-1} + 1$ rezultă $q = 2$. Dar n are divizori impari. Din această observaţie rezultă că $2^{n-1} - 1$ este prim cu p_i $\forall i = 1, \ldots, r$.

Pentru orice i, $i = 1, \ldots, r$, notăm cu d_i ordinul lui 2, modulo p_i ; i.e. $2^{d_i} \equiv 1 (\mathrm{mod}\, p_i)$ şi d_i este cel mai mic număr natural cu această proprietate. Din teorema lui *Fermat* : $2^{p_i - 1} \equiv 1 (\mathrm{mod}\, p_i)$, rezultă $d_i \mid p_i - 1$. Din $n \mid 2^{n-1} + 1$, rezultă $n \mid \left(2^{n-1} + 1\right)\left(2^{n-1} - 1\right)$ şi deci $2^{2(n-1)} \equiv 1 (\mathrm{mod}\, n)$. Rezultă că $2^{2(n-1)} \equiv 1 (\mathrm{mod}\, p_i)$ şi în consecinţă $d_i \mid 2(n-1)$. Deoarece $\left(p_i, 2^{n-1} - 1\right) = 1$ rezultă că $d_i \nmid n - 1$.

Din $d_i \mid 2(n-1)$ şi $d_i \nmid n-1$ rezultă că d_i este par şi că $v_2(d_i) > v_2(n-1)$; mai precis $v_2(d_i) = v_2(n-1)+1$.

Fie acum $r_i = v_2(p_i - 1)$. Deoarece $v_2(d_i) \geq 1$ şi $d_i \mid p_i - 1$ rezultă că $r_i \geq 1$ şi p_i este de forma $p_i = 2^{r_i} c_i + 1$, cu c_i impar. Un calcul atent ne arată că :

$$n-1 = \prod_{i=1}^{r} p_i^{k_i} - 1 = \prod_{i=1}^{r} \left(2^{r_i} c_i + 1\right)^{k_i} - 1 =$$

$$= \prod_{i=1}^{r} \left(2^{k_i r_i} c_i^{k_i} + k_i 2^{r_i (k_i - 1)} c_i^{k_i - 1} + \ldots + k_i 2^{r_i} c_i + 1\right) - 1 =$$

$$= \sum_{i=1}^{r} k_i 2^{r_i} c_i + \sum_{i<j} \binom{k_i}{2} \binom{k_j}{2} 2^{r_i + r_j} c_i c_j + \ldots + 1 - 1.$$

De aici, căutând exponentul lui 2 în $n-1$ găsim $v_2(n-1) \geq \min r_i$; aceasta contrazice faptul că $v_2(n-1) = v_2(d_i) - 1$.

Bibliografie

[1] *K. Chandrasekharan* - "Introduction to analytic number theory", Springer Verlag, 1968 ;

[2] *W. Sierpinski* - "Elementary theory of numbers", Warszawa and Amsterdam 1987 ;

[3] *I. M. Vinogradov* - "Osnovî teorii cisel", Izdatelystvo Nauka, Moskwa, 1972.