Ordinul unui număr modulo n

Ioan Laurenţiu Ploscaru

Voi începe aceast articol cu nişte rezultate cunoscute.

DEFINIŢIE: *Indicatorul lui Euler, notat cu $\varphi(n)$ unde $n \in \mathbb{N}^*$, reprezintă numărul de numere mai mici sau egale cu n şi prime cu acesta.*

Acesta se calculează după formula $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right)$ unde $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$, $p_1, p_2, ..., p_k$ fiind numere prime distincte, iar $a_1, a_2, ..., a_k \in \mathbb{N}^*$.

TEOREMA lui EULER: *Dacă $a, n \in \mathbb{N}^*$ cu $(a, n) = 1$, atunci are loc relaţia $a^{\varphi(n)} \equiv 1 \ (mod\ n)$.*

Consecinţă: Să observăm că pentru un număr prim p avem $\varphi(p) = p - 1$, prin urmare avem relaţia $a^{p-1} \equiv 1 \ (mod\ p)$ pentru $a, p \in \mathbb{N}^*$ cu p prim şi $(a, n) = 1$. (***Teorema lui Fermat***)

Nu am demonstrat rezultatele de mai sus, deoarece nu sunt decât o introducere pentru ceea ce urmează. Ne punem problema ce numere m verifică relaţia $a^m \equiv 1 \ (mod\ n)$ unde $(a, n) = 1$. Ei bine, sunt o infinitate de astfel de numere, de exemplu toţi multipli lui $\varphi(n)$. Dar mai există şi altele? Răspunsul este da, unele chiar mai mici decât $\varphi(n)$.

Mai departe, voi vorbi despre cel mai mic dintre acestea.

DEFINIŢIE: *Fie $a, n \in \mathbb{N}^*, \ n > 1$ cu $(a, n) = 1$. **Ordinul lui** a **modulo** n sau **gaussian**, notat cu $\gamma_n(a)$, reprezintă cel mai mic număr natural nenul k pentru care $a^k \equiv 1 \ (mod\ n)$.*

Putem considera de exemplu puterile consectutive ale lui 2 modulo 7. Obţinem congruenţele $2^1 \equiv 2, \ 2^2 \equiv 4, \ 2^3 \equiv 1, \ 2^4, \equiv 2, ...$, prin urmare ordinul lui 2 modulo 7 este 3, adică $\gamma_7(2) = 3$.

Să observăm că doi întregi care au acelaşi rest modulo n, au şi acelaşi ordin modulo n, deoarece pentru $a \equiv b \ (mod\ n)$ avem $a^k \equiv b^k \ (mod\ n)$.

De asemenea, condiţia $(a, n) = 1$ este absolut necesară. Dacă $(a, n) > 1$, atunci $(a^k, n) > 1$, ceea ce reprezintă o contradicţie fiindcă relaţia $a^k \equiv 1 \ (mod\ n)$ implică $(a^k, n) = 1$. Deci în cazul în care $(a, n) > 1$, $\gamma_n(a)$ nu există. Prin urmare, oricând se va face referire la ordinul lui a modulo n, se va înţelege automat că $(a, n) = 1$.

TEOREMA 1: *Fie $k = \gamma_n(a)$ şi $t \in \mathbb{N}^*$. Atunci $a^t \equiv 1 \ (mod\ n) \Leftrightarrow k \mid t$.*

Demonstraţie: Să presupunem mai întai că $t \vdots k$, prin urmare $t = ks, \ s \in \mathbb{N}^*$. Avem deci relaţia $a^t = (a^k)^s \equiv 1^s \equiv 1 \ (mod\ n)$. Acum, trecem la partea în care avem $a^t \equiv 1 \ (mod\ n)$. Fie $q, r \in \mathbb{N}$ cu $0 \leq r < k$ a.î. $t = qk + r$. Avem astfel $a^t = (a^k)^q \cdot a^r$. Deoarece $a^t \equiv a^k \equiv 1 \ (mod\ n)$, obţinem că $a^r \equiv 1 \ (mod\ n)$, însă $0 \leq r < k$, iar datorită minimalităţii ordinului trebuie ca $r = 0$. Mai departe $t = qk$, deci $k \mid t$, iar teorema este demonstrată.

Teorema 1 ajută la găsirea lui $\gamma_n(a)$, deoarece în loc să încercăm toate puterile lui a, putem lua doar divizorii lui $\varphi(n)$ sau ai altui $b \in \mathbb{N}^*$ pentru care $a^b \equiv 1 \ (mod\ n)$.

De exemplu, să-l găsim pe $\gamma_{13}(2)$. Deoarece $\varphi(13) = 12$, $\gamma_{13}(2) \in \{1, 2, 3, 4, 6, 12\}$. Din congruenţele $2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12,\ 2^{12} \equiv 1$, se observă uşor că $\gamma_{13}(2) = 12$, de asemenea am încercat doar 6 numere în loc de 12, deci ne-am uşurat munca.

Să nu facem însă greşeala de a afirma că pentru orice divizor d al lui $\varphi(n)$, există a a.î. $\gamma_n(a) = d$. Un exemplu este $n = 12$ cu $\varphi(12) = 4$. Să observăm că nu există a pentru care $\gamma_n(a) = 4$, fiindcă $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1\ (mod\ 12)$.

TEOREMA 2: *Dacă* $a^{2^k} \equiv -1\ (mod\ n)$*, atunci* $\gamma_n(a) = 2^{k+1}$.

Demonstraţie: Deoarece $a^{2^k} \equiv -1\ (mod\ n) \Rightarrow a^{2^{k+1}} \equiv 1\ (mod\ n)$, prin urmare $\gamma_n(a) \mid 2^{k+1}$. Să presupunem acum că $\gamma_n(a) < 2^{k+1}$, atunci $\gamma_n(a) = 2^b,\ b \in \mathbb{N}$ cu $b < k$. Fie $k = b + c,\ c \in \mathbb{N}^*$. Avem atunci $a^{2^k} = (a^{2^b})^{2^c} \equiv 1^{2^c} \equiv 1\ (mod\ n)$, contradicţie! Deci $\gamma_n(a) = 2^{k+1}$.

TEOREMA 3: *Dacă* $\gamma_n(a) = k$*, atunci* $a^i \equiv a^j\ (mod\ n) \Leftrightarrow i \equiv j\ (mod\ k)$ *pentru orice* $i, j \in \mathbb{N}^*$.

Demonstraţie: Să presupunem mai întâi că $a^i \equiv a^i\ (mod\ n)$ cu $i \geq j$. Deoarece $(a, n) \equiv 1$, relaţia dată se rescrie $a^{i-j} \equiv 1\ (mod\ n)$. Conform Teoremei 1 avem $k \mid i - j$, adică $i \equiv j\ (mod\ k)$.

Acum, să presupunem că $i \equiv j\ (mod\ k)$ cu $i \geq j$. Atunci vom avea $i = j + qk$ unde $q \in \mathbb{N}$. Mai departe $a^i = (a^k)^q \cdot a^j \equiv 1^k \cdot a^j \equiv a^j\ (mod\ n)$, deci am obţinut ceea ce ne-am dorit.

Consecinţă: *Numerele* $a, a^2, ..., a^{\gamma_n(a)}$ *dau resturi diferite două câte două mdoulo* n.

Să demonstrăm aceasta. Fie $k = \gamma_n(a)$. Alegem $i, j \in \{1, 2, ..., k\}$ a.î. $a^i \equiv a^j\ (mod\ n)$. Atunci, conform Teoremei 3, $i \equiv j\ (mod\ k)$, dar $1 \leq i, j \leq k$, prin urmare $i = j$.

Probabil cititorul şi-a pus deja următoarea întrebare: Este posibil oare să exprimăm ordinul unei puteri a lui a în funcţie de ordinul lui a? Răspunsul se află în următoarea:

TEOREMA 4: *Dacă* $\gamma_n(a) = k$*, iar* $h \in \mathbb{N}^*$*, atunci* $\gamma_n(a^h) = \frac{k}{(h,k)}$.

Demonstraţie: Fie $d = (h, k)$. Putem scrie $h = h_1 d,\ k = k_1 d$ cu $h_1, k_1 \in \mathbb{N}^*,\ (h_1, k_1) = 1$. Evident $(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1\ (mod\ n)$. Dacă luăm $r = \gamma_n(a^h)$, atunci conform Teoremei 1 obţinem $r \mid k_1$. Pe de altă parte, deoarece $k = \gamma_n(a)$, relaţia $a^{hr} \equiv (a^h)^r \equiv 1\ (mod\ n)$ implică $hr \vdots k$, cu alte cuvinte $k_1 d \mid h_1 dr$ sau $k_1 \mid h_1 r$. Însă $(k_1, h_1) = 1$, prin urmare $k_1 \mid r$. Mai sus am arătat că $r \mid k_1$, deci $r = k_1 = k/d$, iar demonstraţia e completă.

Consecinţă: *Fie* $k = \gamma_n(a)$*, iar* $h \in \mathbb{N}^*$*. Atunci* $k = \gamma_n(a^h) \Leftrightarrow (h, k) = 1$.

Să vedem acum un exemplu pentru această teoremă. Din exemplul precedent ştim că $12\gamma_{13}(2)$, în timp ce $\gamma_{13}(2^2) = 6$, iar $\gamma_{13}(2^3) = 4$. Este uşor de verificat că $6 = 12/(2, 12)$ şi $4 = 12/(3, 12)$. De asemenea $12 = \gamma_{13}(2^k)$ unde $k \in \{5, 7, 11\}$.

DEFINIŢIE: *Numărul natural* $a < n$ *se numeşte* ***rădăcină primitivă a lui*** n *dacă* $\gamma_n(a) = \varphi(n)$.

De exemplu 3 este o rădăcină primitivă a lui 7, fapt arătat de următoarele congruenţe modulo 7: $3^1 \equiv 1,\ 3^2 \equiv 2,\ 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^{\varphi(7)} = 3^6 \equiv 1$.

TEOREMA 5: *Fie* $a, n \in \mathbb{N}^*$ *cu* $(a, n) = 1$*, iar* $a_1, a_2, ..., a_{\varphi(n)}$ *numerele naturale mai mici decât* n *şi realtiv prime cu acesta. Dacă* a *este o rădăcină primitivă a lui* n*, atunci numerele* $a, a^2, ..., a^{\varphi(n)}$ *dau aceleaşi resturi modulo* n *ca numerele* $a_1, a_2, ..., a_{\varphi(n)}$*, nu neapărat în aceeaşi ordine.*

Demonstraţie: Deoarece $(a,n)=1$, avem $(a^k,n)=1$ pentru orice $k\in\mathbb{N}^*$. Prin urmare fiecare dintre numerele $a,a^2,...,a^{\varphi(n)}$ este congruent cu un $a_i,\ i\in\{1,2,3,...,\varphi(n)\}$. Dar cele $\varphi(n)$ numere din mulţimea $\{a,a^2,...,a^{\varphi(n)}\}$ dau resturi diferite două câte două mdoulo n conform consecinţei Teoremei 3. Aşadar, resturile acestora modulo n sunt numerele $a_1,a_2,...,a_{\varphi(n)}$.

Conform celor arătate mai sus, dacă un număr are rădăcini primitive, putem stabili exact numărul acestora. Are loc următoarea:

Consecinţă: *Dacă n are măcar o rădăcină primitivă, atunci are exact $\varphi(\varphi(n))$ rădăcini primitive.*

Demonstraţie: Să presupunme că a este o rădăcină primitivă a lui n. Din Teorema 5 deducem că orice altă rădăcină primitivă a lui n este restul unuia dintre numerele $a,a^2,...,a^{\varphi(n)}$. Este deci suficient să vedem pentru câte dintre acestea avem $\gamma_n(a^k)=\varphi(n)$. Însă conform Teoremei 4, numărul acestora este egal cu numărul de valori ale lui $k\in\{1,2,...,\varphi(n)\}$ pentru care $(k,\varphi(n))=1$. Acestea sunt în număr de $\varphi(\varphi(n))$, deci n are $\varphi(\varphi(n))$ rădăcini primitive.

Să vedem acum un exemplu pentru cele demonstrate mai sus. Să luăm $a=2$ şi $n=9$, iar $\varphi(9)=6$. Să observăm că $2^1\equiv 2,\ 2^2\equiv 4,\ 2^3\equiv 8,\ 2^4\equiv 7,\ 2^5\equiv 5, 2^6\equiv 1$. Deci 2 este o rădăcină primitivă a lui 9, iar într-adevăr primele 6 puteri ale lui 2 dau resturile $1,2,4,5,7,8$ modulo 9, care sunt numerele prime cu 9 mai mici decât acesta.

De asemenea, trebuie să avem $\varphi(\varphi(9))=\varphi(6)=2$ rădăcini primitive ale lui 9. Una este 2, mai trebuie să o găsim pe cealaltă. Evident aceasta nu este 1 sau 8, nici 7 fiindcă $7^3\equiv -2^3\equiv 1$. O verificare directă a valorilor rămase ne arată ca aceasta este 5.

Mai departe voi prezenta câteva probleme rezolvate, pentru a arăta utilitatea acestor noţiuni.

Problema 1. Să se găsească toate numerele prime p,q pentru care $pq\mid 2^p+2^q$.

Soluţie: Să presupunem că $p\geq q$. Dacă $q=2$, atunci relaţia din ipoteză se rescrie $p\mid 2+2^{p-1}$. Observăm că $p=2$ verifică, iar pentru $p\geq 3$ avem $2^{p-1}\equiv 1\ (mod\ p)$, deci $p\mid 3\Rightarrow p=3$.

În continuare presupunem că $p,q\neq 2$. Există atunci $k,l,m,n\in\mathbb{N}^*$ cu m,n impare a.î. $p-1=2^l\cdot n$, iar $q-1=2^k\cdot m$. Deoarece $pq\mid 2^p+2^q$, deducem că $0\equiv 2^p+2^q\equiv 2+2^p\ (mod\ q)$, deci $2^{p-1}\equiv -1\ (mod\ q)$ sau $(2^{2^l})^n\equiv -1\ (mod\ q)\Rightarrow 2^{2^l}\equiv -1\ (mod\ q)\Rightarrow \gamma_q(2)=2^{l+1}$. Însă $\gamma_q(2)\mid\varphi(q)\Rightarrow 2^{l+1}\mid q-1$, adică $2^{l+1}\mid 2^k\cdot m$, de unde $l+1\leq k$.

În mod analog obţinem $k+1\leq l$, de unde contradicţia $k+l+2\leq k+l$.

Conchidem că soluţiile problemei sunt $(p,q)\in\{(2,2);(2,3);(3,2)\}$.

Problema 2. Să se arate că $n\nmid 2^{n-1}+1$ oricare ar fi $n\in\mathbb{N},\ n\geq 2$.

Soluţie: Să presupunem că există un astfel de n şi fie $n=p_1^{a_1}\cdot p_2^{a_2}\cdot ...\cdot p_r^{a_r}$ descompunerea sa în factori primi. Este evident că un astfel de n ar trebui să fie impar. Atunci există $m\in\mathbb{N}^*$ a.î. $p_i\equiv 1\ (mod\ 2^m)$ pentru orice $i=\overline{1,r}$ şi există un indice j pentru care $p_j\not\equiv 1\ (mod\ 2^{m+1})$.

Deoarece $p_i\equiv 1\ (mod\ 2^m)$ pentru orice $i=\overline{1,r}$, obţinem că $n\equiv 1\ (mod\ 2^m)$, deci $n-1=2^m\cdot t$ cu $t\in\mathbb{N}^*$. Avem $p_j\mid n\mid 2^{n-1}+1=2^{2^m\cdot t}+1$. Notând cu $s=2^t$ avem că $s^{2^m}\equiv -1\ (mod\ p_j)\Rightarrow \gamma_{p_j}(s)=2^{m+1}$. Însă $\gamma_{p_j}(s)\mid\varphi(p_j)$, adică $2^{m+1}\mid p_j-1$, contradicţie!

În concluzie, nu există $n\in\mathbb{N},\ n\geq 2$ a.î. $n\mid 2^{n-1}+1$.

Probleme propuse

1. Fie $a \in \mathbb{N},\ a > 1$. Arătaţi că $n \mid \varphi(a^n - 1)$ pentru orice $n \in \mathbb{N}^*$.

2. Determinaţi $n \in \mathbb{N}$ pentru care: *a)* $11 \mid 5^n + 7^n$; *b)* $37 \mid 5^n + 7^n$.

3. Determinaţi $x \in \mathbb{N}$ pentru care $2x^8 \equiv 3\ (mod\ 13)$.

4. Fie $a, n \in \mathbb{N}^*$ şi $p > 2$ prim cu $(a, p) = 1$ a.î. $p \mid a^n + 1$. Notăm cu $i = \gamma_p(a)$ şi fie $j \in \mathbb{N}^*$ minim pentru care $p \mid a^j + 1$. Să se arate că i este par şi $i = 2j$.

5. Să se arate că $n \nmid 2^n - 1$ pentru orice $n \in \mathbb{N},\ n \geq 2$.

6. Să se arate că $n \nmid 3^n - 2^n$ pentru orice $n \in \mathbb{N},\ n \geq 2$.

7. Fie p prim, iar a o rădăcină primitivă a lui p. Arătaţi că măcar unul dintre numerele a şi $a + p$ este rădăcină primitivă a lui p^2.

8. Determinaţi $n \in \mathbb{N}^*$ pentru care $n^2 \mid 2^n + 1$.

9. Demonstraţi că există o infinitate de numere $n \in \mathbb{N}$ pentru care $n^2 \mid 3^n + 2^n$.

10. Să se găsească toate perechile de $(n, p) \in \mathbb{N} \times \mathbb{N}$ a.î. p este număr prim cu $n \leq 2p$, iar numerele n, p verifică relaţia $n^{p-1} \mid (p-1)^n + 1$.

Acest articol reprezintă doar o introducere în domeniu. Sper ca exemplele prezentate să fi convins elevii doritori de a face performanţă la olimpiadele şcolare sau pe cei pasionaţi de matematică de utilitatea acestor noţiuni şi că aticolul de faţă le va deschide interesul pentru a aprofunda această frumoasă temă ce are multe alte lucruri interesante de aflat.

Bibliografie

[1] David M. Burton - *Elementary Number Theory*, editura *Allyn and Bacon*;
[2] L. Panaitopol & A. Gica - *Probleme de aritmetică şi teoria numerelor*, editura *GIL*.