мр Еуген Ведрал

РЕШАВАЊЕ ЈЕДНАЧИНЕ $a^x \equiv b \pmod{p^k}$

У овом раду ће бити изведена рекурентна формула за добијање решења једначине

$$a^x \equiv b \pmod{p^k}, \tag{1}$$

где су a и b цели бројеви, p и k природни бројеви, а p прост број. Биће, дакле, доказано да се помоћу решења једначине (1) може доста лако добити решење једначине $a^x \equiv b \pmod{p^{k+1}}$, што значи да се помоћу решења једначине $a^x \equiv b \pmod{p}$ може добити решење једначине $a^x \equiv b \pmod{p^2}$, а помоћу решења ове дођи до решења једначине $a^x \equiv b \pmod{p^3}$ и тако даље, редом. О појму конгруенције по модулу и њеним основним својствима читалац може видети у [1] од стране 46 до стране 56, као и у [3].

Пођимо од важне дефиниције. Нека је m природан број већи од 1 и a цео број, такав да су a и m релативно прости, тј. да је њихов највећи заједнички делилац једнак 1, што ћемо писати овако: $(a, b) = 1$. Нека је d најмањи природан број такав да $a^d \equiv 1 \pmod{m}$ (такав број под датом претпоставком увек постоји). Тада кажемо да је d *ред елемента* a или да a *припада изложиоцу* d *по модулу* m. То записујемо овако: $r_m(a) = d$.

У вези са појмом реда елемента значајна је

Теорема 1. (i) *Ако* $r_m(a) = d$, *онда су бројеви* a, a^2, $\ldots$, a^{d-1} *по паровима неконгруентни по модулу* m.

(ii) *Ако је* $r_m(a) = d$ *и* n *било који природан број, онда је формула* $a^n \equiv 1 \pmod{m}$ *тачна ако и само ако* $d \mid n$.

Доказ. (i) изводимо свођењем на противречност. Нека је супротно претпоставци, $a^s \equiv a^k \pmod{m}$ и $0 < k < s \leqslant d$. Тада, због $(a, m) = 1$ важи $a^{s-k} \equiv 1 \pmod{m}$, а то би значило да је $s - k$ ред елемента a, што је, због $0 < k < s \leqslant d$ немогуће.

(ii) Претпоставимо прво да $d \mid n$. Тада имамо $r_m(a) = d$ и $n = dk$, $k \in \mathbf{Z}$. Зато је $a^n = a^{kd} = (a^d)^k \equiv 1^k \equiv 1 \pmod{m}$. Дакле, $a^n \equiv 1 \pmod{m}$. Обратно, нека је $a^n \equiv 1 \pmod{m}$. Поделимо n са d са остатком: $n = dq + r$, $0 \leqslant r < d$. Тада $1 \equiv a^n = a^{dq+r} = (a^d)^q \cdot a^r \equiv a^r \pmod{m}$. Пошто је $1 \equiv a^r \pmod{m}$, $0 \leqslant r < d$ и $d = r_m(a)$, то r не може бити ред елемента $a \pmod{m}$, па $r = 0$. То значи да $n = dq$, односно $d \mid n$. ■

Према Ојлеровој теореми ([1], страна 51) важи $a^{\varphi(m)} \equiv 1 \pmod{m}$, $(a,m) = 1$, где је $\varphi(m)$ Ојлерова карактеристика природног броја m, односно број свих природних бројева мањих од m који су релативно прости са m. Позната је релација

$$\varphi(p^k) = p^{k-1}(p-1), \qquad p \text{ прост број}. \tag{2}$$

На основу теореме 1 (ii) као и Ојлерове теореме лако се закључује да ред неког елемента треба тражити међу делиоцима броја $\varphi(m)$. Поменимо још и ову дефиницију. Ако је ред елемента g по модулу m једнак $\varphi(m)$, тада се g зове *примитивни корен по модулу* m.

Теорема 2. *Нека је* $(a,m) = 1$ *и* $d = r_m(a)$. *Формула* $a^s \equiv a^k \pmod{m}$ *је тачна ако и само ако* $k \equiv s \pmod{d}$.

Доказ. Из $a^s \equiv a^k \pmod{m}$ и, на пример, $k \geqslant s$, због $(a,m) = 1$ следи $a^{k-s} \equiv 1 \pmod{m}$. Тада, према теореми 1 (ii), $d \mid (k-s)$ па стога $k \equiv s \pmod{d}$.

Обратно, нека је $k \equiv s \pmod{d}$. Тада $d \mid (k-s)$, односно $k - s = dl$, $l \in \mathbf{Z}$. Зато је $a^{k-s} = a^{dl} = (a^d)^l \equiv 1 \pmod{m}$ па отуда $a^k \equiv a^s \pmod{m}$. ■

Последица. *Ако је* p *прост број и* a *примитивни корен по модулу* p, *тада* $a^k \equiv a^s \pmod{p}$ *ако и само ако* $k \equiv s \pmod{p-1}$.

Доиста, ако је a примитивни корен по модулу p, онда је ред елемента a једнак $\varphi(p) = p - 1$. ■

Сада ћемо доказати теорему помоћу које се решења једначине (1) могу наћи рекурентном формулом: ако знамо решење x_k једначине $a^x \equiv b \pmod{p^k}$, онда помоћу њега можемо наћи решење x_{k+1} једначине $a^x \equiv b \pmod{p^{k+1}}$, ако оно постоји.

Теорема 3. *Ако* $a^{x_k} \equiv b \pmod{p^k}$ *и* $r_{p^k}(a) = d$, *онда из* $a^{x_{k+1}} \equiv b \pmod{p^{k+1}}$ *следи да је* $x_{k+1} = x_k + d\nu$, $\nu \in \mathbf{Z}$.

Доказ. Користећи дефиницију конгруенције по модулу, исказ теореме можемо овако записати:

$$(a^{x_k} = b + p^k n \wedge r_{p^k}(a) = d) \implies (a^{x_{k+1}} = b + p^{k+1} l \implies x_{k+1} = x_k + d\nu),$$

n, l, ν су цели бројеви. Смењујући b из $a^{x_k} = b + p^k l$ у формулу $a^{x_{k+1}} = b + p^{k+1} l$ добијамо $a^{x_{k+1}} = a^{x_k} - p^k n + p^{k+1} l$, односно, еквивалентно $a^{x_{k+1}} = a^{x_k} - p^k(n - pl)$, тј. $a^{x_{k+1}} \equiv a^{x_k} \pmod{p^k}$. Ово је, према теореми 2, еквивалентно са

$$x_{k+1} \equiv x_k \pmod{d}, \tag{3}$$

где је $d = r_{p^k}(a)$. То значи да је d један од делилаца броја $\varphi(p^k) = p^{k-1}(p-1)$. Формула (3) се може писати у облику

$$x_{k+1} = x_k + d\nu, \qquad \nu \in \mathbf{Z}, \tag{4}$$

што је и требало доказати. ■

Доказана теорема има импликацијски облик, што значи да су формулом (4) одређени „кандидати“ за решења једначине (1). Доиста, ако су $\mathcal{F}_1$ и $\mathcal{F}_2$ две формуле (једначине) а $\mathcal{R}(\mathcal{F}_1)$, $\mathcal{R}(\mathcal{F}_2)$ скупови њихових решења, онда важи

$$(\mathcal{F}_1 \implies \mathcal{F}_2) \implies (\mathcal{R}(\mathcal{F}_1) \subset \mathcal{R}(\mathcal{F}_2)).$$

Број ν у формули (4) може се наћи „пробањем“ или из услова

$$a^{x_k+d\nu} \equiv b \pmod{p^{k+1}}. \tag{5}$$

Ако је ред елемента a по модулу p^{k+1} једнак r, онда важи и ограничење

$$x_k + d\nu < r, \tag{6}$$

чиме се број „кандидата“ које је потребно проверити може смањити. Теорему 3 можемо користити и за налажење реда неког елемента по модулу p^k.

Пример 1. Наћи ред елемента 2 по: а) mod 7, б) mod 49 и в) mod 343.

а) Како $\varphi(7) = 6$, а природни делиоци броја 6 су 1, 2, 3 и 6, то су онда и кандидати за ред елемента 2. „Пробањем“ се налази да је $r_7(2) = 3$. То значи да је 3 решење једначине $2^x \equiv 1 \pmod 7$ у потпуном систему остатака mod 7.

б) Сада, у ствари, знамо партикуларно решење $x_1 = 3$ једначине $2^x \equiv 1 \pmod 7$. Пошто је $r_7(2) = 3$, користећи теорему 3, формула (4), можемо потражити решење x_2 једначине $2^x \equiv 1 \pmod{49}$ у облику $x_2 = 3 + 3t$, $t \in \mathbf{Z}$. Како x_2 треба да буде ред елемента 2 по mod 49, а ред елемента је према формули (2) делилац броја $\varphi(49) = 7 \cdot 6 = 42$, то мора важити $x_2 \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. Но, због $x_2 = 3 + 3t$ списак „кандидата“ се своди на 3, 6, 21, 42. „Пробањем“ налазимо да је 21 најмањи број који задовољава једначину $2^x \equiv 1 \pmod{49}$ па је зато $r_{49}(2) = 21$.

в) Како једначина $2^x \equiv 1 \pmod{49}$ има партикуларно решење $x_2 = 21$, онда, према формули (4) теореме 3, решење једначине $2^x \equiv 1 \pmod{343}$ (ако постоји) мора бити облика

$$x_3 = 21 + 21u, \quad u \in \mathbf{Z}. \tag{$*$}$$

Пошто је $\varphi(343) = \varphi(7^3) = 7^2 \cdot 6 = 294$, то је ред елемента 2 mod 343 делилац броја 294 што значи да је

$$x_3 \in \{2, 3, 6, 14, 21, 42, 49, 98, 147, 294\}. \tag{$**$}$$

Систем формула $(*)$, $(**)$ је задовољен ако и само ако $x_3 \in \{21, 42, 147, 294\}$. Провером налазимо да је $r_{343}(2) = 147$. $\triangle$

Пример 2. Решити по x у потпуном систему остатака mod 343 једначину $2^x \equiv 338 \pmod{343}$.

Први корак. Нађемо партикуларно решење једначине $2^x \equiv 338 \pmod 7$. То решење означимо са x_1. Зато $x_1 = 1$ и, према претходном примеру, $r_7(2) = 3$.

Други корак. Према формули (4), теорема 3, следи да решење x_2 једначине $2^x \equiv 338 \pmod{49}$ мора имати облик $x_2 = 1 + 3t$, $t \in \mathbf{Z}$. Пошто је према примеру 1б $r_{49}(2) = 21$, то због формуле (6) мора бити $1 + 3t < 21$ па су зато „кандидати“ за решење 1, 4, 7, 10, 13, 16 и 19. Лаком провером налазимо $2^{10} \equiv 338 \pmod{49}$ па је 10 решење једначине $2^x \equiv 338 \pmod{49}$. Опште параметарско решење ове једначине у $\mathbf{Z}$ је $10 + 21t$ јер је $r_{49}(2) = 21$.

Трећи корак. Како је $x_2 = 10$, а према примеру 1в је $r_{343}(2) = 147$, то је према теореми 3, формула (4)

$$x_3 = 10 + 21u, \quad u \in \mathbf{Z}$$

а према формули (6) је

$$10 + 21u < 147$$

одакле добијамо „кандидате“ за решење једначине $2^x \equiv 338 \pmod{343}$: 10, 31, 52, 73, 94, 115 и 136. Непосредно налазимо да је тачна формула $2^{10} \equiv 338 \pmod{343}$, што значи да је 10 партикуларно, а $10 + 147t$, $t \in \mathbf{Z}$ опште решење једначине $2^x \equiv 338 \pmod{343}$. △

Пример 3. Решити по $x \in \mathbf{Z}$ једначину $9^x \equiv 4 \pmod{121}$.

Први корак. Партикуларно решење једначине $9^x \equiv 4 \pmod{11}$ је 2. Ред елемента 9 mod 11 је 5. Наиме, „кандидати“ за ред елемента су делиоци броја $\varphi(11) = 10$.

Други корак. Према теореми 3, формула (4) могућа решења једначине $9^x \equiv 4 \pmod{121}$ су тада описана формулом

$$(*) \qquad x_2 = 2 + 5t, \quad t \in \mathbf{Z}.$$

Потражимо ограничење у смислу формуле (6). Према формули (2) ред елемента 9 mod 121 налазимо међу делиоцима броја $\varphi(121) = 11 \cdot 10 = 110$. То су бројеви 1, 2, 5, 10, 22, 55 и 110. Лаком провером налазимо $r_{121}(9) = 5$. То значи да вредност за x_2 мора бити између 0 и 5, односно $0 \leqslant x_2 < 5$ или, због $(*)$ $0 \leqslant 2 + 5t < 5$, $t \in \mathbf{Z}$. Овај систем неједначина има једино решење $t = 0$, међутим $9^2 \not\equiv 4 \pmod{121}$, па једначина $9^x \equiv 4 \pmod{121}$ нема решења. До тог закључка долазимо и израчунавањем вредности $9^0 \equiv 1$, $9^1 \equiv 9$, $9^2 \equiv 81$, $9^3 \equiv 3$, $9^4 \equiv 27 \pmod{121}$. Дакле, ниједна вредност степена броја 9 mod 121 није 4. △

ЛИТЕРАТУРА

[1] I. Niven, S. Zuckerman, H. Montgomery, *An Introduction to the Theory of Numbers*, New York 1991.

[2] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford 1979.

[3] V. Mićić, Z. Kadelburg, *Uvod u teoriju brojeva*, Beograd 1983.