ЈЕДНА МЕТОДА РЕШАВАЊА КВАДРАТНИХ КОНГРУЕНЦИЈА

***мр Еуген Ведрал,* Београд**

Ако је p прост број онда је скуп $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$ поље у односу на модулско сабирање $(+_p)$ и модулско множење $(\cdot_p)$. Ове операције ће бити даље означаване уобичајено: $+$ и $\cdot$. У пољу $(\mathbf{Z}_p, +, \cdot)$ може се рачунати, слично као у пољу реалних бројева. Претпостављамо да је читалац упознат са решавањем линеарних конгруенција и њиховим особинама. Скуп $\mathbf{Z}_p$ обично зовемо *потпун систем остатака по модулу* p. У овом раду биће изложен оригиналан метод решавања квадратних конгруенција

$$x^2 \equiv a \pmod{p} \quad (p \text{ је прост број и } a \in \mathbf{Z}_p) \tag{1}$$

свођењем проблема на решавање линеарних конгруенција.

Дефиниција 1. Ако једначина (1) има решења онда се a зове *квадратни остатак по модулу* p.

Пример 1. Уочимо таблицу:

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

,

при чему $x \in \mathbf{Z}_{13}$ и $x^2 = x \cdot x$, где је $\cdot$ одговарајуће модулско множење. Уочавамо да су бројеви $1, 3, 4, 9, 10, 12$ квадратни остаци по модулу 13. То значи да, на пример, конгруенција $x^2 \equiv 10 \pmod{13}$ има два решења, 6 или 7, у $\mathbf{Z}_{13}$, што се види из таблице, док, на пример, једначина $x^2 \equiv 2 \pmod{13}$ нема решења.

Теорема 1. Ако је a квадратни остатак по модулу p, $a \neq 0$, $\mathrm{NZD}(a, p) = 1$, $p > 2$, тада конгруенција (1) има два решења у $\mathbf{Z}_p$, чији је збир p.

Доказ следи из импликације: Ако $x_0^2 \equiv a \pmod{p}$, $x_0 \in \mathbf{Z}_p$, онда $(p - x_0)^2 \equiv a \pmod{p}$ па су x_0 или $p - x_0$ решења конгруенције (1) у $\mathbf{Z}_p$. Зато је довољно наћи једно решење једначине (1), ако оно постоји. □

Познат је *Ојлеров критеријум* помоћу којег се може утврдити да ли је $a \in \mathbf{Z}_p$ квадратни остатак. Наводимо га без доказа.

Теорема 2. За прост број $p > 2$, број $a \in \mathbf{Z}_p$ $(a \neq 0)$ је квадратни остатак по модулу p ако и само ако $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, док број $a \in \mathbf{Z}_p$ није квадратни остатак ако и само ако $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Дефиниција 2. Број a из $\mathbf{Z}_p$ се зове *очигледно квадратни остатак по модулу* p ако за неко $\ell \in \mathbf{Z}_p$ важи $\ell^2 \equiv a \pmod{p}$ и $\ell^2 \leqslant p - 1$, где је $\leqslant$ уобичајена релација поретка из прстена целих бројева.

Приметимо да се услов $\ell^2 \leqslant p - 1$ може заменити условом $\ell \leqslant [\sqrt{p}]$, где је $[\cdot]$ ознака за цео део реалног броја. У примеру 1 *очигледно квадратни остаци* су 1, 4 и 9, док 3, 10 и 12 нису *очигледно квадратни остаци*. Ако је број у конгруенцији (1) *очигледно квадратни остатак* онда се решења ове једначине могу непосредно „прочитати".

Пример 2. Решења једначине $x^2 \equiv 16 \pmod{29}$ су 4 или -4, односно 4 или 25, јер је $-4 \equiv 25 \pmod{29}$. Слично се непосредно решавају, на пример и конгруенције $x^2 \equiv 100 \pmod{101}$, односно $x^2 \equiv 49 \pmod{97}$. Њихово решавање препуштамо читаоцу.

Решење конгруенције $x^2 \equiv 57 \pmod{101}$ не може се непосредно прочитати јер 57 није *очигледно квадратни остатак* по модулу 101. Наиме, *очигледно квадратни остаци* по модулу 101 су $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$, а ниједан од њих није 57.

Сада је јасно да ћемо формулу (1) лако решити ако нађемо алгоритам којим се ова своди на еквивалентну у којој је десна страна конгруентна неком елементу из $\mathbf{Z}_p$ који је *очигледно квадратни остатак*. С обзиром на резултат теореме 1 довољно је наћи решење x_0 једначине (1), ако оно постоји, у скупу $\mathbf{Z}_p^* = \{0, 1, 2, \ldots, \frac{p-1}{2}\}$, јер се онда друго решење налази у скупу $\mathbf{Z}_p \setminus \mathbf{Z}_p^*$. Алгоритам за решавање конгруенције (1) даје следећа теорема.

Теорема 3. Ако једначина (1) има решења, онда постоји $\ell \in \mathbf{Z}_p$, $\ell \leqslant [\sqrt{p}]$, такав да је $\ell^2 \cdot a$ конгруентан *очигледно квадратном остатку* по модулу p.

Доказ. Ако је a *очигледно квадратни остатак*, онда је доказ завршен (видети пример 2). Претпоставимо да a није *очигледно квадратни остатак*, што значи да постоји $b \in \mathbf{Z}_p$ тако да је $b > [\sqrt{p}]$ и $b^2 \equiv a \pmod{p}$. Зато формулу (1) можемо написати у облику:

$$x^2 \equiv b^2 \pmod{p} \tag{2}$$

Ако на p и b применимо Еуклидов алгоритам дељења: $p = b \cdot n + r, 0 < r < b$ и $n \leqslant [\sqrt{p}]$, јер је $b > [\sqrt{p}]$, добијамо да је $b = \dfrac{p-r}{n}$. Ако заменимо у (2), добићемо $n^2x^2 \equiv (p-r)^2 \pmod{p}$, односно

$$n^2x^2 \equiv r^2 \pmod{p}. \tag{3}$$

Ако је $r \leqslant [\sqrt{p}]$, онда је r^2 *очигледно квадратни остатак* па је доказ завршен. **Уочимо да постоји $n \in \mathbf{Z}_p$, $n \leqslant [\sqrt{p}]$, тако да $n^2x^2 \equiv n^2a \pmod{p}$ и $n^2a \equiv r^2 \pmod{p}$.** Сада се формула (3) може написати у еквивлентном облику:

$$nx \equiv r \pmod{p} \quad \text{или} \quad nx \equiv -r \pmod{p}. \tag{4}$$

Тако се решавање квадратне конгруенције своди на решавање линеарних конгруенција. Ако је у (3), $r > [\sqrt{p}]$, онда настављамо Еуклидов алгоритам: $p = r \cdot n_1 + r_1, 0 < r_1 < r$, одакле је $r = \dfrac{p-r_1}{n_1}$, због претпоставке $r > [\sqrt{p}]$ је $n_1 \leqslant [\sqrt{p}]$. Вредност за r заменимо у (3) и добијемо:

$$n_1^2n^2x^2 \equiv r_1^2 \pmod{p}. \tag{5}$$

Ово поново потврђује горе (масним словима) истакнути закључак. Ако је $r_1 \leqslant [\sqrt{p}]$, онда је r_1^2 *очигледно квадратни остатак* па се једначина (5) може факторисати на линеарне конгруенције: $n_1nx \equiv r_1 \pmod{p}$ или $n_1nx \equiv -r_1 \pmod{p}$. Ако $r_1 > [\sqrt{p}]$ наставља се Еуклидов алгоритам. Претпоставимо да у $k+1$ кораку овог алгоритма добијамо: $p = r_{k-1}n_k + r_k$, са $0 < r_k < r_{k-1} < r_{k-2} < \ldots < r_2 < r_1 < r < b$ $(*)$ и $r_k \leqslant [\sqrt{p}]$. Овај последњи услов мора се десити после коначно много корака јер је низ природних бројева $(*)$ строго опадајући. Тако добијемо:

$$A^2x^2 \equiv r_k^2 \pmod{p}, \quad r_k \leqslant [\sqrt{p}] \tag{6}$$

и $A = n_k n_{k-1} \cdots n_1 n$. Из формуле (6) лако добијамо:

$$Ax \equiv r_k \pmod{p} \quad \text{или} \quad Ax \equiv -r_k \pmod{p},$$

па је, тако, теорема у целини доказана. □

Пример 3. Решити по $x \in \mathbf{Z}_{97}$ формулу $x^2 \equiv 43 \pmod{97}$. *Очигледно квадратни остаци* по модулу 97 су $1, 4, 9, 16, 25, 36, 49, 64$ и 81. Производе $1 \cdot 43, 4 \cdot 43, 9 \cdot 43, \ldots, 81 \cdot 43$ једначимо по модулу 97. Лако се уверавамо да је $16 \cdot 43 \equiv 9 \pmod{97}$. Зато дату формулу множимо са 16. Решење даје следећи ланац еквиваленција:

$$\begin{aligned} x^2 \equiv 43 \pmod{97} &\Leftrightarrow 16x^2 \equiv 9 \pmod{97} \\ &\Leftrightarrow 4x \equiv 3 \pmod{97} \quad \text{или} \quad 4x \equiv -3 \pmod{97} \\ &\Leftrightarrow x \equiv 25 \pmod{97} \quad \text{или} \quad x \equiv 72 \pmod{97}. \end{aligned}$$

Тако су решења дате једначине у $\mathbf{Z}_p$ бројеви 25 или 72. Приметимо да је и $64 \cdot 43 \equiv 36 \pmod{97}$ и да се решења могу добити множењем дате једначине са 64.

Пример 4. Решити по $x \in \mathbf{Z}_{1999}$ конгруенцију $x^2 \equiv 1632 \pmod{1999}$.

У овом примеру би требало извршити највише $44 (= \sqrt{1999}])$ проверавања. Рачунањем производа $1 \cdot 1632, 4 \cdot 1632, \ldots 44 \cdot 1632$ и једначењем по модулу 1999 налазимо да је $256 \cdot 1632 \equiv 1 \pmod{1999}$. Решење дате формуле следи из ланца еквиваленције, пошто формулу, претходно помножимо са 256:

$$\begin{aligned} x^2 \equiv 1632 \pmod{1999} &\Leftrightarrow 256x^2 \equiv 1 \pmod{1999} \\ &\Leftrightarrow 16x \equiv 1 \pmod{1999} \quad \text{или} \quad 16x \equiv -1 \pmod{1999} \\ &\Leftrightarrow x \equiv 125 \pmod{1999} \ , \text{или} \quad x \equiv 1874 \pmod{1999}, \quad (**) \end{aligned}$$

па су, у $\mathbf{Z}_{1999}$, решења 125 или 1874.

НАПОМЕНА. Формулама $(**)$ одређено је опште решење дате конгруенције.

Контрапозиција теореме 3 може да послужи и као критеријум егзистенције решења конгруенције (1). О томе говори следећа теорема.

Теорема 4. Ако не постоји $\ell \in \mathbf{Z}_p$, $\ell \leqslant [\sqrt{p}]$, такав да је $\ell^2 a$ конгруентан очигледно квадратном остатку по модулу p, онда конгруенција (1) нема решења.

Пример 5. Доказати да конгруенција $x^2 \equiv 2 \pmod{37}$ нема решења.

Претпоставимо супротно да дата формула има решења. Тада, један од производа $2 \cdot 1, 4 \cdot 2, 9 \cdot 2, 16 \cdot 2, 25 \cdot 2, 36 \cdot 2$ мора бити конгруентан *очигледно квадратном остатку* по модулу 37. Међутим, ови производи су редом конгруентни са $2, 8, 18, 32, 13, 35$ по модулу 37 од којих ниједан није *очигледно квадратни остатак*. Зато дата конгруенција нема решења.

Рецимо на крају да је решавање квадратне конгруенције облика (1) фундаментално за решавање квадратних конгруенција облика

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad \mathrm{NZD}(a, p) = 1, \ p > 2. \tag{7}$$

Наиме, конгруенција (7) еквивалентна је са

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{8}$$

Конгруенција (8) има облик (1). Тако је, уопште, дат алгоритам за решавање квадратних конгруенција облика (7).

Пример 6. Решити по $x \in \mathbf{Z}_{37}$ конгруенцију $3x^2 + 7x + 31 \equiv 0 \pmod{37}$.
Користећи еквиваленцију (7) $\Leftrightarrow$ (8) лако добијамо:

$$3x^2 + 7x + 31 \equiv 0 \pmod{37} \Leftrightarrow (6x + 7)^2 \equiv 10 \pmod{37}.$$

На десну страну ове еквиваленције применимо теорему 4. Међу очигледно квадратним остацима по модулу 37 налазимо да конгруенцију треба множити са 9 јер је $9 \cdot 10 \equiv 16 \pmod{37}$. Тако добијамо следећи ланац еквиваленција:

$$\begin{aligned}(6x + 7)^2 \equiv 10 \pmod{37} &\Leftrightarrow 9(6x + 7) \equiv 16 \pmod{37} \\ &\Leftrightarrow 3(6x + 7) \equiv 4 \pmod{37} \quad \text{или} \quad 3(6x + 7) \equiv -4 \pmod{37} \\ &\Leftrightarrow 9x \equiv 10 \pmod{37} \quad \text{или} \quad 3x \equiv 2 \pmod{37} \\ &\Leftrightarrow x \equiv 34 \pmod{37} \quad \text{или} \quad x \equiv 13 \pmod{37},\end{aligned}$$

па су 13 или 34 решења дате конгруенције у $\mathbf{Z}_{37}$.

Изложена теорија и урађени примери поткрепљују корист ове методе у решавању квадратних конгруенција и применом рачунара (када је p велики прост број). Заправо, конгруенција (1) или (7) може се решавати претраживањем у скупу $\mathbf{Z}_p$. Овом методом се број проверавања многоструко смањује и, у ствари, своди на број $[\sqrt{p}]$.

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] В. Мићић, З. Каделбург, Д. Ђукић, Увод у теорију бројева, Београд, 2004.

Статијата прв пат е објавена во списанието ТАНГЕНТА на ДМ на Србија во 2005/06 година