Диофантове једначине - Рачун конгруенција

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Диофантове једначине

Рјешавамо једначину облика

$$ax + by = c,$$

гдје су a, b и c цијели бројеви.
Испоставља се да ова једначина има цјелобројна рјешења ако и само ако $d|c$, гдје је $d = \textbf{нзд}(a, b)$.

Диофантове једначине

Ако је пар x^*, y^* рјешење једначине, онда су сва рјешења дата формулом

$$x = x^* + \frac{b}{d}t \text{ и } y = y^* - \frac{a}{d}t, \ t \in \mathbb{Z}$$

Примјетимо да се пар (x^*, y^*) може добити као

$$(x^*, y^*) = \left(\frac{c}{d}x_1, \frac{c}{d}y_1\right),$$

гдје је (x_1, y_1) рјешење једначине

$$ax + by = d$$

Поступак рјешевања Диофантове једначине

Рјешавамо једначину облика

$$ax + by = c.$$

Како $d = \textbf{нзд}(a, b)$, знамо да по Безуовом идентитету постоје x_1, y_1 такви да

$$ax_1 + by_1 = d.$$

Множењем претходне једнакости са c/d добијамо

$$a\left(\frac{c}{d}x_1\right) + \left(\frac{c}{d}y_1\right) = c,$$

чиме добијамо пар

$$x^* = \frac{c}{d}x_1, y^* = \frac{c}{d}y_1$$

као рјешење почетне једначине.

Идеја аритметике затвореног круга

Модуларна аритметика је веома заступљен и користан апарат у теорији бројева. Основна идеја се може сликовито представити као **аритметика затвореног круга**, у којој напримјер имамо бројеве од 1 до 12, а следећи број 13 опет третирамо као 1 итд.

Дефиниција

Нека је $m \geq 1$ цио број. Кажемо да су цијели бројеви a и b ***конгруентни по модулу*** *m ако је њихова разлика $a - b$ дјељива са m, односно ако $m \mid a - b$. Тада пишемо*

$$a \equiv b \pmod{m}.$$

Лема

Релација конгруенције по модулу m је релација еквиваленције на скупу цијелих бројева.

Основне особине модуларне аритметике

Разлог због којег користимо ознаку $\equiv$ у модуларној аритметици је тај што она има многе особине које подсјећају на једнакост, као што показује следећа лема

Лема

Ако је $a_1 \equiv a_2 \pmod{m}$ *и* $b_1 \equiv b_2 \pmod{m}$ *онда је*

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m},$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

Примјер

Рачунамо $3^{188} \pmod{13}$. *Наивни, али практично немогућ приступ би се састојао од тражења вриједности* 3^{188} *коју би потом дијелили са 13 да би се нашао тражени остатак. Међутим, бирамо другачији пут. Наиме*

$$3^2 = 9 \equiv -4 \pmod{13},\ 3^4 = (3^2)^2 \equiv (-4)^2 = 16 \equiv 3 \pmod{13},$$

па је

$$3^8 = (3^4)^2 \equiv 3^2 = 9 \pmod{13},\ 3^{12} = 3^8 3^4 \equiv 9 \cdot 3 \equiv 1 \pmod{13}.$$

Чињеница да је $3^{12} \equiv 1 \pmod{13}$ *је од кључне вриједности, јер онда из* $188 = 12 \cdot 15 + 8$, *схватамо да је*

$$3^{188} = \left(3^{12}\right)^{15} \cdot 3^8 \equiv 1 \cdot 9 \pmod{13}.$$

Примјер

Наћи последњу цифру броја

$$1997^{1998^{1999}}.$$

Нека је $N = 1997^{1998^{1999}}$. Задатак се заправо своди на одређивање $N \pmod{10}$. Како је $1997 \equiv 7 \pmod{10}$, онда је

$$N \pmod{10} \equiv 7^{1998^{1999}}.$$

Посматрајмо низ $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$, $7^5 \equiv 7 \pmod{10}, \ldots,$

Из претходног низа, видимо да је

$$7^a \equiv \begin{cases} 1 \pmod{10} & \text{ако је } a \equiv 0 \pmod 4 \\ 7 \pmod{10} & \text{ако је } a \equiv 1 \pmod 4 \\ 9 \pmod{10} & \text{ако је } a \equiv 2 \pmod 4 \\ 3 \pmod{10} & \text{ако је } a \equiv 3 \pmod 4 \end{cases}$$

Из $1998 \equiv 2 \pmod 4$, слиједи $1998^{1999} \equiv 2^{1999} \equiv 4 \cdot 2^{1997} \equiv 0 \pmod 4$, одакле закључујемо да је

$$N = 1997^{1998^{1999}} \equiv 1 \pmod{10}.$$

Лема

Нека су a, x, y цијели бројеви, при чему $a \neq 0$. Вриједи

$$ax \equiv ay \pmod{m} \quad \textit{ако и само ако} \quad x \equiv y \pmod{\frac{m}{\textbf{нзд}(a, m)}}.$$

Лема

Нека су a, b, x, y цијели бројеви, $a \neq 0$, $b \neq 0$. Онда је

$$x \equiv y \pmod{a} \ \textit{и}\ x \equiv y \pmod{b} \iff x \equiv y \pmod{\textbf{нзс}(a, b)}.$$

Рјешавање конгруенција

Теорема

Нека су $a, m \in \mathbb{N}$, *а* $b \in \mathbb{Z}$. *Конгруенција*

$$ax \equiv b \pmod{m} \text{ [еквивалентно са } ax + my = b]$$

има рјешења ако и само ако $d = (a, m)$ *дијели* b. *Ако је* x_0 *било које рјешење задате конгруенције, онда су сва друга рјешења дата са*

$$x = x_0 + \frac{mt}{d},\ t \in \mathbb{Z}.$$

Посебно, ова рјешења формирају тачно d *класа конгруенције по модулу* m, *а чији су представници*

$$x = x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

Ријешимо конгруенцију $555x \equiv 15 \pmod{5005}$.
Ако скратимо са 5 цијелу конгруенцију, добијамо $111x \equiv 3 \pmod{1001}$.
Најприје, рјешавамо конгруенцију

$$111x \equiv 1 \pmod{1001}.$$

Користимо Бланкишип методу

$$\begin{bmatrix} 111 & 1 & 0 \\ 1001 & 0 & 1 \end{bmatrix}$$

Ако помножимо прву врсту са 9 и то одузмемо од друге врсте, добијамо

$$\begin{bmatrix} 111 & 1 & 0 \\ 2 & -9 & 1 \end{bmatrix}$$

Рјешавање конгруенција

Одузимање од прве врсте друге, претходно помножене са 55

$$\begin{bmatrix} 1 & 496 & -55 \\ 2 & -5 & 1 \end{bmatrix}$$

На крају, одузимањем прве врсте од друге, претходно помножене са 2, имамо

$$\begin{bmatrix} 1 & 496 & -55 \\ 0 & x & y \end{bmatrix}$$

Дакле, имамо да је $111 \cdot 496 \equiv 1 \pmod{1001}$.
Дакле, једно рјешење почетне конгруенције је $3 \cdot 49 \equiv 487 \pmod{1001}$. На основу Теореме 1 имамо 5 неконгруентних рјешења почетне једначине

$$x \equiv 487,\ 1488,\ 2489,\ 3490,\ 4491 \pmod{5005}.$$

Мултипликативни инверз по модулу

Један од најважнијих појмова у модуларној аритметици уопште, а који ће бити веома често коришћен и у опису теоријске, математичке основе за криптографске системе је појам **мултипликативног инверза** по модулу.

Лема

Нека је a цио број. Тада је

$$a \cdot b \equiv 1 \pmod{m} \text{ за неко } b \in \mathbb{Z} \text{ акко } \textbf{нзд}(a, m) = 1.$$

Број b називамо мултипликативним инверзом броја a по модулу m.

Например, бројеви $1, 3, 5, 9, 11, 13$ имају мултипликативне инверзе по модулу 14.

Кинеска теорема о остацима

Теорема

(Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_r$ у паровима релативно прости природни бројеви, те нека су $a_1, a_2, \ldots, a_r$ цијели бројеви. Тада систем конгруенција

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots \quad , x \equiv a_r \pmod{m_r}$$

има рјешења. Ако је x_0 једно рјешење, онда су сва рјешења система дата са

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}.$$

Посебно, постоји јединствено рјешење датог система по модулу M, гдје је $M = m_1 \cdots m_r$.

Кинеска теорема о остацима

Нека је $n_j = \frac{M}{m_j}$, за $j = 1, 2, \ldots, r$. Јасно је да је **нзд**$(m_j, n_j) = 1$, па на основу Леме 1 постоји цијели број x_j такав да

$$n_j x_j \equiv a_j \pmod{m_j}.$$

Посматрајмо број

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Кинеска теорема о остацима

Очигледно, за овај број вриједи да је

$$x_0 \equiv 0 + \cdots + n_j x_j + \cdots + 0 \equiv a_j \pmod{m_j}.$$

Дакле, x_0 јесте рјешење датог система конгруенција.
Ако су x, y два рјешења датог система, онда је

$$x \equiv y \pmod{m_j} \text{ за } j = 1, \ldots, r.$$

Због чињенице да су m_j у паровима релативно прости, слиједи да је $x \equiv y \pmod{M}$, што значи да је рјешење јединствено по модулу M.

Кинеска теорема о остацима

Примјер

Ријешити систем конгруенција

$$x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7, \quad x \equiv 4 \pmod{11}.$$

Најприје, имамо да је

$$x_0 = 77x_1 + 55x_2 + 35x_3,$$

гдје x_1, x_2, x_3 задовољавају

$$77x_1 \equiv 2 \pmod 5, \quad 55x_2 \equiv 3 \pmod 7, \quad 35x_3 \equiv 4 \pmod{11},$$

односно

$$2x_1 \equiv 2 \pmod 5, \quad 6x_2 \equiv 3 \pmod 7, \quad 2x_3 \equiv 4 \pmod{11}.$$

Кинеска теорема о остацима

Рјешавањем појединачних конгруенција, добијамо

$$x_1 = 1,\ x_2 = 4,\ x_3 = 2,$$

што даје $x_0 = 367$. Према томе, сва рјешења система су дата са

$$x \equiv 367 \pmod{385}.$$

Хвала на пажњи :)