Дјељивост - Еуклидов алгоритам

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Бројеви у криптографији

Највећи дио модерне криптографије је изграђен на темељу алгебре и теорије бројева. Зато је неопходно да развијемо одговарајући математички апарат прије него што се почнемо бавити типично криптографским темама.

Скупови бројева

Основни скупови бројева са којима ћемо се сусретати у криптографији су природни и цијели борјеви. Скуп природних бројева је

$$\mathbb{N} = \{1, 2, \ldots\},$$

а скуп цијелих бројева

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

Дефиниција и основне особине дјељивости

Подсјетимо се дефиниције и основних особина дјељивости.

Дефиниција

Нека су a и b цијели бројеви и $b \neq 0$. Кажемо да b дијели a, у ознаци $b \mid a$, односно да је a дјељиво са b, ако постоји цио број c тако да $a = bc$.

Лема

Нека су a, b, c цијели бројеви.

(а) Ако је $a \mid b$ и $b \mid c$, онда $a \mid c$.

(б) Ако је $a \mid b$ и $b \mid a$, онда је $a = \pm b$.

(в) Ако је $a \mid b$ и $a \mid c$, онда $a \mid b \pm c$.

Теорема о дјељењу са остатком

Можда најелементарнија теорема, на којој почива модуларна аритметика је Теорема о дјељењу са остатком.

Теорема

За произвољан природан број a и цијели број b постоје јединствени цијели бројеви q и r такви да је

$$b = qa + r, \ 0 \leq r < a.$$

Једна од важних посљедица ове теореме је у томе да су могући остаци при дијељењу са k из скупа $\{0, \ldots, k\}$.

Примјер

Доказати да је број $m^5 - m$, $m \in \mathbb{N}$, дјељив са 30.

Највећи заједнички дјелилац

Појам највећег заједничког дјелиоца, иако елементаран, има бројне апликације у аритметици.

Дефиниција

Заједнички дјелилац два броја a и b је позитиван цио број d који дијели оба броја. Ако је бар један од датих бројева различит од нуле, онда постоји коначан број заједничких дјелилаца a и b. Највећи цио број d такав да $d \mid a$ и $d \mid b$ је највећи заједнички дјелилац a и b и означава се са ***нзд***(a, b)*, односно са* (a, b).

Слично се дефинише и највећи заједнички дјелилац бројева $b_1, b_2, \ldots, b_n$ од којих је бар један различит од нуле и означава са ***нзд***$(b_1, b_2, \ldots, b_n)$.

Примјер простог налажења **нзд** два броја

Прво, елементарно, питање је како ефикасно наћи **нзд**(a, b) за два природна броја a, b. На примјер, један метод тражења **нзд** се састоји у издвајању заједничких дјелитеља оба броја, а након тога налажењем највећег међу њима.

Примјер

Дјелитељи од 748, 2024 *су*

$$\{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\},$$

$$\{1, 2, 4, 8, 11, 22, 23, 44, 46, 88, 92, 184, 253, 506, 1012, 2024\}.$$

Видимо да је 44 *највећи међу заједничким дјелитељима два посматрана броја, те је стога* **нзд**$(748, 2024) = 44$.

Уочимо да за два цијела броја a, b од којих је бар један различит од нуле, вриједи **нзд**$(a, b) \geq 1$. Дефиницију **нзд** можемо уопштити на коначан број цијелих бројева од којих је бар један различит од нуле.

Теорема

*Нека је $d =$ **нзд**$(a_1, a_2, \ldots, a_n)$. Онда је d најмањи позитивни елемент скупа*

$$S = \{a_1 t_1 + a_2 t_2 + \cdots + a_n t_n \mid t_1, t_2, \ldots, t_n \in \mathbb{Z}\},$$

па постоје цијели бројеви $t_1', t_2', \ldots, t_n'$ тако да је

$$d = a_1 t_1' + a_2 t_2' + \ldots + a_n t_n'.$$

Дакле, претходна теорема установљава могућност приказа за највећег заједничког дјелиоца **нзд**$(a_1, a_2, \ldots, a_n)$ цијелих бројева $a_1, a_2, \ldots, a_n$ у облику цјелобројне линеарне комбинације

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = a_1 u_1 + a_2 u_2 + \ldots a_n u_n,$$

за одговарајуће $u_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$. Ово представљање највећег заједничког дјелиоца скупа бројева се у литератури назива Безуов идентитет.

Примјетимо да **нзд**$(a_1, a_2, \ldots, a_n) \geq 1$. Такође, елементарном анализом закључујемо да је

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = \textbf{нзд}(\pm a_1, \pm a_2, \ldots, \pm a_n),$$

што значи да су само апсолутне вриједности бројева битне за највећи заједнички дјелилац датог скупа бројева.

Лема

Сваки заједнички дјелилац цијелих бројева $a_1, \ldots, a_n$ дијели ***нзд***$(a_1, \ldots, a_n)$.

Лема

За цијеле бројеве $a_1, a_2, \ldots, a_n$ вриједи

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = \textbf{нзд}(a_1, a_2, \ldots, a_{n-2}, \textbf{нзд}(a_{n-1}, a_n))$$

Дефиниција

Бројеви a и b су релативно прости ако је $\textbf{нзд}(a, b) = 1$. За цијеле бројеве $a_1, a_2, \ldots, {}_n$ рећи ћемо да су релативно прости ако $\textbf{нзд}(a_1, a_2, \ldots, a_n) = 1$, а да су у паровима релативно прости ако је $\textbf{нзд}(a_i, a_j) = 1$ за све $1 \leq i, j \leq n$, $i \neq j$.

Примјер

Доказати да се разломци

$$\frac{12n+1}{30n+2} \text{ и } \frac{21n+4}{14n+3}$$

не могу скратити ни за један природан број.

Следеће двије леме, иако елементарне по суштини, врло су корисне пприликом доказивања комплекснијих тврђења.

Лема

Нека су a, b, m цијели бројеви. Ако је $\textbf{нзд}(a, m) = \textbf{нзд}(b, m) = 1$ онда је $\textbf{нзд}(ab, m) = 1$.

Лема

Нека су a, b, x цијели бројеви. Онда вриједи

$$\textbf{нзд}(a, b) = \textbf{нзд}(a, b + ax).$$

Хеуристика Еуклидовог алгоритма

Наш циљ је да установимо ефикасан алгоритам за налажење **нзд**(a, b) за два цијела броја a, b. У том смислу користимо Еуклидов алгоритам.
Ако је

$$a = bq + r, \quad 0 \leq r < b,$$

онда елементарном анализом закључујемо

$$\textbf{нзд}(a, b) = \textbf{нзд}(b, r).$$

Ово елементарно запажање је суштина Еуклидовог алгоритма. Јасно, поступак можемо наставити, а следећа итерација, умјесто бројева a, b ће почети са бројевима b, r. Очигледно, сваки следећи корак садржи мање бројеве од претходног.

Основни облик Еуклидовог алгоритма

Нека су дати природни бројеви a и b, такви да $a \geq b$. Следећи алгоритам рачуна **нзд**(a, b) у коначном броју корака на ефикасан начин.

(1) Нека је $r_0 = a$, $r_1 = b$, а $i = 1$.

(2) Дијељем r_{i-1} са r_i добијамо количник q_i и остатак r_{i+1}, тако да

$$r_{i-1} = r_i q_i + r_{i+1} \quad 0 \leq r_{i+1} < r_i.$$

(3) Ако је $r_{i+1} = 0$ онда $r_i =$ **нзд**(a, b) и алгоритам је окончан.

(4) Ако је $r_{i+1} > 0$, онда поставимо $i = i + 1$ и враћамо се на корак (2).

Корак подјеле (2) обављамо у највише $2 \lg_2(b) + 1$ пута.

Проширени Еуклидов алгоритам

Као што смо већ видјели, за природне бројеве a и b једначина

$$ax + by = \textbf{нзд}(a, b)$$

увијек има рјешење за (u, v) у скупу цијелих бројева. Општије, ако је (u_0, v_0) једно рјешење претходне једначине, онда свако њено рјешење има облик

$$u = u_0 + \frac{b \cdot k}{\textbf{нзд}(a, b)} \text{ и } v = v_0 - \frac{a \cdot k}{\textbf{нзд}(a, b)},$$

за $k \in \mathbb{Z}$.

Најмањи заједнички садржалац

За два природна броја a, b, дефинишемо најмањи заједнички садржалац **нзс**(a, b) као најмањи природан број који је дјељив са оба броја a, b. Најмањи заједнички садржалац често означавамо као $[a, b]$.
Следећа, врло корисна лема даје везу између **нзд**(a, b) и **нзс**(a, b) за природне бројеве a, b.

Лема

Нека су дати природни бројеви a, b. Тада је

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

Бланкиншип метода

Бланкиншип (W. A. Blankinship) је дао веома једноставан метод за налажење најјвећег заједничког дјелиоца два броја, као и коефицијената одговарајуће линеарне комбинације. За дате цијеле бројеве $a > b > 0$ почињемо са матрицом

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Изводимо *елементарне матричне операције над врстама*, а са циљем да добијемо једну од двије форме

$$\begin{bmatrix} 0 & x_1 & x_2 \\ d & y_1 & y_2 \end{bmatrix} \text{ или } \begin{bmatrix} d & y_1 & y_2 \\ 0 & x_1 & x_2 \end{bmatrix}$$

Дакле, крајњи циљ је да се добије нула у првој колони. Овај метод гарантује да је $d = \textbf{нзд}(a, b) = y_1 a + y_2 b$.

Бланкиншип метода

Примјер

Нека је $a = 35$, $b = 15$.

$$\begin{bmatrix} 35 & 1 & 0 \\ 15 & 0 & 1 \end{bmatrix}$$

Примјетимо да је $35 = 15 \cdot 2 + 5$, *па је* $35 + 15(-2) = 5$. *Ако помножимо другу врсту са* -2 *и додамо је првој врсти, а онда множимо прву врсту са* -3 *и додамо другој врсти, добијамо*

$$\begin{bmatrix} 5 & 1 & -2 \\ 0 & -3 & 7 \end{bmatrix}.$$

Сада, можемо рећи да је **нзд**$(35, 15) = 5$ *и* $5 = 1 \cdot 35 + (-2) \cdot 15$.

Хвала на пажњи :)