Модуларна аритметика

Нека је $m \in \mathbb{Z}$. Релацију $\equiv_m$ на $\mathbb{Z}$ дефинисану са:

$$x \equiv_m y \text{ акко } m \mid x-y$$

називамо конгруенција по модулу m. Ово је једна важна релација еквиваленције на скупу $\mathbb{Z}$, класе ове релације називамо класе конгруенције.

Нека $x, y \in \mathbb{Z}$, тада је

$$\begin{aligned} x \equiv_m y &\iff y \equiv_m x \quad \text{(симетричност)} \\ &\iff m \mid y-x \\ &\iff y-x = m \cdot k, \text{ за неко } k \in \mathbb{Z} \\ &\iff y = x + m \cdot k, \text{ за неко } k \in \mathbb{Z} \end{aligned}$$

Према томе, класа конгруенције елемента x (у ознаци $[x]_m$) је

$$[x]_m = \{ y \in \mathbb{Z} \mid x \equiv_m y \} = \{ x + m \cdot k \mid k \in \mathbb{Z} \}$$

Приметимо да важе следеће:

1° $[x]_0 = \{ x + 0 \cdot k \mid k \in \mathbb{Z} \} = \{x\}$

2° $[x]_1 = \{ x + 1 \cdot k \mid k \in \mathbb{Z} \} = \mathbb{Z}$

3° $[x]_{-m} = \{ x + (-m) \cdot k \mid k \in \mathbb{Z} \} = \{ x + mk \mid k \in \mathbb{Z} \} = [x]_m$

Дакле, на основу 1° релације $=$ и $\equiv_0$ су исте на $\mathbb{Z}$, такође, релација $\equiv_{-m}$ се своди на $\equiv_m$ па ћемо у наставку претпостављати да је $m \geq 2$.

Подсетимо се да за дато x и m постоје јединствени бројеви $q, r \in \mathbb{Z}$ такви да је $x = qm + r$ и $0 \leq r < m$.

Број q означавамо са x DIV m, док r означавамо са x MOD m.

Како је $r = x - qm$ следи да $m \mid x - r$, па је $x \equiv_m r$ и

$$[x]_m = [x \text{ MOD } m]_m.$$

Количнички скуп $\mathbb{Z}/\equiv_m = \{ [x]_m \mid x \in \mathbb{Z} \}$ означава се са $\mathbb{Z}/\langle m \rangle$ и назива се скуп остатака по модулу m. Приметимо да овај скуп има коначно елемената (елементи су класе). Прецизније,

$$\mathbb{Z}/\langle m \rangle = \{ [0]_m, [1]_m, \ldots, [m-1]_m \}.$$

Сабирање и множење у $\mathbb{Z}/\langle m \rangle$

Тврђење: Нека су $m, a, b, c, d \in \mathbb{Z}$ такви да је $a \equiv_m c$ и $b \equiv_m d$. Тада је

$$a + b \equiv_m c + d \quad \text{и} \quad ab \equiv_m cd.$$

доказ:

Како је $a \equiv_m c$ и $b \equiv_m d$ следи да постоје $k, \ell \in \mathbb{Z}$ такви да је

$$c = a + km \quad \text{и} \quad d = b + \ell m.$$

Према томе,

$$\begin{aligned} c + d &= a + km + b + \ell m \\ &= a + b + (k + \ell)m \equiv_m a + b \end{aligned}$$

$$cd = (a+km)(b+\ell m)$$
$$= ab + a\ell m + kmb + km\ell m$$
$$= ab + (a\ell + kb + km\ell)m \equiv_m ab$$

На основу претходног тврђења доказано је да дефинисује множења и сабирања у $\mathbb{Z}/\langle m\rangle$:

$$[a]_m + [b]_m = [a+b]_m,$$
$$[a]_m \cdot [b]_m = [ab]_m.$$

Ове операције су добро дефинисане у смислу да резултат не зависи од избора представника класа.

Инвертибилни елементи у $\mathbb{Z}/\langle m\rangle$

деф: Нека $a \in \mathbb{Z}/\langle m\rangle$. Елемент a је инвертибилан уколико постоји елемент $b \in \mathbb{Z}/\langle m\rangle$ такав да је $ab = [1]_m$.

Наредно тврђење показује да ако је $a \in \mathbb{Z}/\langle m\rangle$ инвертибилан елемент, тада постоји јединствено $b \in \mathbb{Z}/\langle m\rangle$ такво да је $ab = [1]_m$

Тврђење: Нека $a, b, c \in \mathbb{Z}/\langle m\rangle$, a је инвертибилан елемент и $ab = ac = [1]_m$. Тада је $b = c$.

доказ:

$$ab = ac \Rightarrow bab = bac$$
$$\Rightarrow \underbrace{ab}b = \underbrace{a}bc$$
$$\Rightarrow [1]_m b = [1]_m c$$
$$\Rightarrow b = c$$

Пример:

Елементи $\mathbb{Z}/_{\langle 4\rangle}$ и њихови мултипликативни инверзи:

a	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
a^{-1}	не постоји	$[1]_4$	не постоји	$[3]_4$

Зашто,

$$[1]_4 \cdot [1]_4 = [1 \cdot 1]_4 = [1]_4$$
$$[3]_4 \cdot [3]_4 = [3 \cdot 3]_4 = [3 \cdot 3 \text{ MOD } 4]_4 = [1]_4 .$$

Када не постоји мултипликативна инверзија, елемент $[x]_m$ скупа $\mathbb{Z}/_{\langle m\rangle}$ означавамо краће са x.

При алгоритамском одређивању мултипликативног модуларног инверза елемента $a \in \mathbb{Z}$ при модулу $m \geq 2$ присутан може бити "грубом силом":

тако што се испитују сви бројеви b од 0 до $m-1$ и проверава се да ли је $b \cdot a \equiv_m 1$.

Међутим, за велике бројеве m овакав приступ је веома неефикасан.

Уколико су a и m узајамно прости бројеви постоји знатно ефикаснији приступ - приступ који користи обрнути Еуклидов алгоритам.

Наиме, уколико су $a, m \in \mathbb{Z}$ узајамно прости, на основу обрнутог Еуклидовог алгоритма, могуће је пронаћи $s, t \in \mathbb{Z}$ такве да је:

$$s \cdot m + t \cdot a = 1$$

Како је тада

$$1 \equiv_m sm + ta \equiv_m ta$$

означавамо да је елемент t тражени мултипликативни инверз елемента a.

Може се десити да елемент t буде негативан, у том случају за инверз се може узети $t+m$. Тада је

$$(s-a)\cdot m + (t+m)\cdot a = 1,$$

а пошто је $|t| < n$, број $t+m$ је сигурно позитиван.

Примећујемо да вредности елемената s у овој примени обрнутог Еуклидовог алгоритма нису потребне, па се може изостављати рачунање ове вредности.

Ојлерова теорема

Још један начин да се израчуна мултипликативни инверз је коришћењем познате Ојлерове теореме. Пре него што наведемо формулацију ове теореме, дефинисаћемо следеће битне појмове.

Нека је $n \geq 1$. Скуп $\Phi(n) = \{a \mid 1 \leq a \leq n, \text{НЗД}(a,n) = 1\}$ називамо Ојлеров скуп.

примери:

$\Phi(1) = \{1\}$

$\Phi(2) = \{1\}$

$\Phi(3) = \{1,2\}$

$\Phi(4) = \{1,3\}$

$\Phi(5) = \{1,2,3,4\}$

$\Phi(10) = \{1,3,7,9\}$

$\Phi(12) = \{1,5,7,11\}$

$\varphi(n) := |\Phi(n)|$

функцију $\varphi: \mathbb{N} \to \mathbb{N}^+$ називамо Ојлеровом функцијом.

Ова функција броји колико има бројева мањих од n који су узајамно прости са n.

$\varphi(1)=1$ $\quad$ $\varphi(5)=4$

$\varphi(2)=1$ $\quad$ $\varphi(10)=4$

$\varphi(3)=2$ $\quad$ $\varphi(12)=4$

$\varphi(4)=2$

Како израчунати вредност Ојлерове функције?

* Ако је p прост број тада је

$$\Phi(p)=\{1,2,3,\dots,p-1\}$$

па је $\varphi(p)=p-1$.

* Ако је p прост број тада је за $k\in\mathbb{N}$

$$НЗД(p^k,a)\in\{1,p,p^2,\dots,p^k\}$$

па је

$$НЗД(p^k,a)=1 \text{ акко } НЗД(a,p^k)\notin\{p,p^2,\dots,p^n\}$$

Дакле, елементи скупа $\Phi(p^k)$ су сви они бројеви мањи од p^k који нису дељиви са p, па је

$$\varphi(p^k)=p^k-\underbrace{p^{k-1}}_{\text{толико има оних који су дељиви са } p}=p^k\left(1-\frac{1}{p}\right).$$

(сваки p-ти је дељив са p)

* Ојлерова функција је под одређеним условима мултипликативна.

Прецизније, $\varphi(mn)=\varphi(m)\cdot\varphi(n)$ када је $НЗД(m,n)=1$.

Претходне три особине можемо искористити да бисмо добили "формулу" за израчунавање Ојлерове функције произвољног природног броја n.

Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ тада је

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

Коначно, долазимо до Ојлерове теореме коју наводимо без доказа.

Теорема: Нека је $\text{НЗД}(a, m) = 1$, тада је $a^{\varphi(m)} \equiv_m 1$.

На основу Ојлерове теореме видимо да је

$$a^{\varphi(m)} = a^{\varphi(m)-1} \cdot a \equiv_m 1$$

па је $a^{\varphi(m)-1}$ инверз елемента a по модулу m.