Eukleidův algoritmus

Eukleidův algoritmus slouží k nalezení největšího společného dělitele dvou čísel. Jeho rozšířená verze umožňuje nalézt multiplikativní inverzi čísla X modulo M. Čehož lze třeba využít pro počítání kombinačních čísel v modulární aritmetice. Pojďme si nyní pojmy vedoucí k Eukleidovu algoritmu postupně vysvětlit.

1 Multiplikativní inverze

Multiplikativní inverze čísla X v modulu M je takové číslo Y pro které platí, že

$$X \cdot Y \equiv 1 \mod (M).$$

Symbol $\equiv$ se nazývá kongruence. Říká, že zbytek po dělení (číslem M) výrazu na levé straně je stejný jako zbytek po dělení výrazu na pravé straně.

Pokud je číslo M prvočíslo, pak číslo Y vždy existuje. Pokud M není prvočíslo, pak Y může, ale nemusí existovat. Například pro $M = 4$ a $X = 2$ neexistuje žádné Y, pro které by byla výše uvedená rovnice splněna. Naopak pro $M = 4$ a $X = 3$ je Y rovno 3, protože $X \cdot Y \bmod M = 3 \cdot 3 \bmod 4 = 9 \bmod 4 = 1$.

V úlohách se často zadává veliké prvočíslo, např. $M = 1\,000\,000\,007$, aby multiplikativní inverze vždy existovala.

2 Eukleidův algoritmus

Eukleidův algoritmus slouží k nalezení největšího společného dělitele (gcd) dvou celých čísel A a B. Nechť $A \geq B$. Potom lze A vyjádřit ve tvaru

$$A = k \cdot B + q$$

kde k a q jsou celá čísla.

Uvědomme si nyní dvě věci – levá i pravá strana rovnice musí být dělitelná gcd. gcd je určitě faktorem čísla B, proto můžeme násobek B klidně vynechat. Dále víme, že pokud gcd dělí číslo B a zároveň je celá pravá strana dělitelná gcd, pak i zbytek q musí být nutně dělitelný gcd.

Proto můžeme celý postup opakovat pro čísla B a q, protože jejich gcd je stejný, jako gcd čísel A a B.

Celý postup opakujeme až do chvíle, kdy q je rovno 0. Hledaný gcd je hodnota čísla B z posledního kroku (tedy q z předchozího kroku), protože to je největší číslo, které dělí jak levou, tak pravou stranu rovnice.

Příklad 1

Nalezněme gcd čísel 46 a 51, tedy $A = 51$ a $B = 46$.

$$51 = k \cdot 46 + q$$

Pro koeficienty rovnice platí $k = \lfloor A/B \rfloor$ a $q = A \bmod B$

$$51 = 1 \cdot 46 + 5$$

Pokračujeme s čísly $A = B = 46$ a $B = q = 5$

$$46 = 9 \cdot 5 + 1$$

Pokračujeme s čísly $A = B = 5$ a $B = q = 1$

$$5 = 5 \cdot 1 + 0$$

Koeficient q je nyní 0, tudíž algoritmus končí, a gcd $= B = 1$.

Příklad 2

Nalezněme gcd čísel 406 a 1120, tedy $A = 1120$ a $B = 406$.

$$1120 = k \cdot 406 + q$$

$$1120 = 2 \cdot 406 + 308$$

Pokračujeme s čísly $A = B = 406$ a $B = q = 308$

$$406 = 1 \cdot 308 + 98$$

Pokračujeme s čísly $A = B = 308$ a $B = q = 98$

$$308 = 3 \cdot 98 + 14$$

Pokračujeme s čísly $A = B = 98$ a $B = q = 14$

$$98 = 7 \cdot 14 + 0$$

Koeficient q je nyní 0, tudíž algoritmus končí, a gcd $= B = 14$.

3 Rozšířený Eukleidův algoritmus

Jestliže hledáme multiplikativní inverzi čísla X modulo M, řešíme rovnici

$$X \cdot Y \equiv 1 \mod (M).$$

Tuto rovnici je možné vyjádřit ve tvaru

$$X \cdot Y + M \cdot L = 1.$$

Známe X a M hledáme Y a L. Umíme nalézt takové koeficienty, aby hodnota výrazu $X \cdot Y + M \cdot k$ byla rovna X nebo M:

$$X \cdot 1 + M \cdot 0 = X$$

$$X \cdot 0 + M \cdot 1 = M.$$

Postupným upravováním dle Eukleidova algoritmu nalezneme takové koeficienty, aby hodnota výrazu byla rovna jedné. Poté je koeficient Y multiplikativní inverzí čísla X.

Algoritmus výpočtu je podobný, jako výpočet dle Eukleidova algoritmu, pouze si poznamenáváme některé koeficienty navíc.

Vytvoříme tabulku o 4 sloupcích (viz příklad 3). V tabulce je vyjádřeno, jak můžeme číslo v prvním sloupečku vyjádřit jako lineární kombinaci čísel X a M (tedy ve tvaru $X \cdot A + M \cdot B$), přičemž koeficient A je v daném řádku ve druhém sloupečku a koeficient B je v daném řádku ve třetím sloupečku. Začneme tím, že si vyjádříme čísla X a M jako lineární kombinace čísel X a M (viz výše). Obecně řečeno

$$X \cdot A + M \cdot B = X,$$

$$X \cdot C + M \cdot D = M.$$

Pokračujeme tím, že nalezneme hodnotu $q = X \bmod M$ (za předpokladu $X \geq M$, jinak prohodíme X a M). Toto číslo q chceme opět vyjádřit jako lineární kombinaci čísel X a M. Analogicky jako ve výpočtu Eukleidova algoritmu položíme $k = \lfloor X/M \rfloor$, toto číslo je v tabulce znázorněno ve 4. sloupečku.

$$X \cdot E + M \cdot F = q.$$

Pro koeficienty E a F platí

$$E = A - k \cdot C,$$

$$F = B - k \cdot D.$$

Algoritmus opět opakujeme s novými hodnotami $X = M$ a $M = q$ a hodnotami koeficientů z řádků tabulky příslušících těmto číslům, až do té doby, kdy $q = 0$, stejně jako v základním Eukleidově algoritmu.

Příklad 3

Chceme nalézt multiplikativní inverzi čísla 51 modulo 46. Řešíme rovnici

$$51 \cdot Y \equiv 1 \mod (46).$$

Tuto rovnici je možné vyjádřit ve tvaru

$$51 \cdot Y + 46 \cdot k = 1.$$

Obecně:

q	X	M	k
X	A = 1	B = 0	-
M	C = 0	D = 1	$k = \lfloor X/M \rfloor$
$q = X \ mod \ (M)$	E = A – k·C	F = B – k·D	

Pro tento příklad:

q	51	46	k
51	1	0	-
46	0	1	$\lfloor X/M \rfloor = 1$
$X \ mod \ (M) = 5$	A – k·C = 1	B – k·D = -1	

Nyní pokračujeme dále s tím, že výpočet je prováděn na základě hodnot ve druhém a třetím řádku tabulky stejným způsobem jako v prvnímu kroku:

q	51	46	k
51	1	0	-
46	0	1	1
5	1	-1	9

q	51	46	k
51	1	0	-
46	0	1	1
5	1	-1	9
1	-9	10	5

q	51	46	k
51	1	0	-
46	0	1	1
5	1	-1	9
1	-9	10	5
0			

Nyní algoritmus končí, protože $q = 0$. Multiplikativní inverze Y čísla X je hodnota ve druhém sloupečku v posledním řádku, kde q není 0, tedy $Y = -9$.

A skutečně:

$$X \cdot Y = 51 \cdot (-9) = -459,$$

přičemž

$$-459 \equiv 1 \mod (46).$$

Tak jsme ověřili, že -9 je skutečně multiplikativní inverzí čísla 51 v modulu 46.

Pomocí rozšířeného Eukleidova algoritmu je tedy možné nalézt multiplikativní inverzi. Díky ní můžeme realizovat dělení v modulární aritmetice, a tak počítat například veliká kombinační čísla.