Div og Mod

Div og mod eru aðgerðir þar sem deilt er með afgangi, t.d. að deila 7 upp í 30 sem er 4 með 2 í afgang.

Skilgreining Ef $a \in \mathbb{Z}, d \in \mathbb{Z}$ og $d > 0$, þá eru til ótvírætt ákvarðaðar tölur $q \in \mathbb{N}, r \in \mathbb{N}$, svo $a = q \cdot d + r$.

q er kllaður kvóti (*quotient*), og r er kallaður afgangur (*remainder*).

Ritháttur $q = a \bmod d$, (Java: a/d). $r = a$ rem d (Java: $a\%d$).

Leyfareikningur (*modular arithmetic*)

Deiling með m upp í tölur a, b sem gefur sama afgang er táknuð

$$a \equiv b \text{ (mod m)}$$

Lesið a er samleyfa b mátað við m. (a is congruent to b modulo m)

Dæmi:

4 og 76 eru samleyfa mátað við 24, svo: $4 \equiv 76 \text{ (mod 24)}$.

Reglur

Ef:

$a \equiv b$ (mod m)

$c \equiv d$ (mod m)

Þá:

$a + c \equiv b + d$ (mod m)

$a - b \equiv b - d$ (mod m)

$ac \equiv bd$ (mod m)

$a^n \equiv b^n$ (mod m) fyrir öll n

Hagnýtingar

1. Að reikna hakkaföll, t.d. $h(k) = k$ mod m, þar sem m er fjöldi plássa.
2. Að reikna slmebitölur. t.d $x_n = (a \cdot x_{n-1} + b)$ mod m, þar sem a er stór tala og $m = 2^{64}$. Gæfi 64 bita PSEUDO-random tölu
3. Að reikna vartölur (*checksum digit*), t.d. mod 10 í luhn-algorithmanum, md5-checksum

Dæmi Kennitöluvartala

Tökum kennitöluna $170858 - 4259$

og margföldum með 32765432

	1	7	0	8	5	8	4	2	5	9
x	3	2	7	6	5	4	3	2	vartala	öld
=	3	14	0	48	25	34	12	4	=	138

Reiknum $11 - (138 \bmod 11) = 11 - 6 = 5$, sem er vartalan okkar.

Gcd (*greatest common divisor*)

Stærsti samþáttur a og b er stærsta talan sem gengur upp í bæði a og b, táknað: $\gcd(ab)$.

Lcm (*least common multiple*)

Minnsti samnefnari a og b er minnsta tala sem a og b ganga upp í, táknað $\text{lcm}(a, b)$.

Reiknirit Evklíðs (*Euclid's algorithm*)

Notað til að finna stærsta samþátt tveggja jávæðra heiltalna $a < b$. Deilum a upp í b og finnum afganginn. Ef afgangurinn: $r_0 = 0$ þá er a stærsti samþátturinn, annars er næst deilt r_0 upp í a og svo með r_1 í r, og svo framvegis þar til $r_n = 0$.

Regla: $a \cdot b = \mathbf{lcm}(a, b) \cdot \mathbf{gcd}(a, b)$

Dæmi

Finnum $\gcd(18, 30)$. $18 < 30$ svo við byrjum:

$\frac{30}{18} = 1, r_0 = 12$

$\frac{18}{12} = 1, r_1 = 6$

$\frac{12}{\mathbf{6}} = 2, r_2 = 0$, svo: $\gcd(18, 30) = 6$.

Samleifa andhverfur

Setning Bezout:

Fyrir öll a og b eru til tölur s og t þannig að $sa + tb = \gcd(a, b)$

Ef $\gcd(a, b) = 1$ (a og b eru ósamþátta (*coprime*)), þá er hægt ap finna samleifa andhverfu a mod b. Í öðrum orðum, það er til tala s svo:

$s \cdot a \equiv 1 \pmod{b}$.

Til er reiknirit til að finna s og t, en það er tímafrekt og í staðin ef a og b eru lágar tölur er hægt að prófa sig áfram:

Dæmi:

$a = 3$, $b = 4$

Skrifum margföldunartöflur:

$3 \cdot s : 3, 6, \mathbf{9}, 12, 15, \ldots$

$-4 \cdot t : -4, -\mathbf{8}, -12, -16, -20, \ldots$

$9 - 8 = 1$ svo andhverfa 3(mod 4) er 9

Prímtölur (*prime numbers*)

Skilgreining

Tala sem er bara deilanleg með sjálfri sér og 1. Í öðrum orðum: p er prímtala þá og því aðeins að ef $n|p$, þá er $n = 1$, $n = p$.

Ritháttur:

a gengur upp í b, er táknað $a|b$.

Meginsetning algebrunnar

Ef $n \in \mathbb{N}$, þá má rita $n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \cdots \cdot p_n^{k_n}$, þar sem p_i eru prímtölur og $k_j \in \mathbb{N}^+$, á nákvæmlega einn veg. Kallað **prím þáttun**.

Dæmi um prím þáttun:

$14 = 2 \cdot 7$

$18 = 2 \cdot 3^2$

$780 = 10 \cdot 78 = 2^2 \cdot 3 \cdot 5 \cdot 13$