

Heltalsaritmetik del 1: Euklides algoritm och modulär aritmetik

Johan Jonasson

November 2022

"Onyttig talteori som kom till nytta efter 400 år".

Vi talar bara om heltal idag.

Definition

Man säger att a delar b och skriver

$$a|b$$

om det finns ett heltal n sådant att

$$b = na.$$

Obs att $a|0$ för alla a (ta $n = 0$).

Theorem

Sats 1: $a|b$ och $a|c$ om och endast om $a|mb + nc$ för alla m och n .

Bevis:

$\Leftarrow$: Tag $m = 0, n = 1$ respektive $m = 1, n = 0$.

$\Rightarrow$: Att $a|b$ och $a|c$ betyder att det finns heltal p och q sådana att $b = pa$ och $c = qa$. Detta ger $mb + nc = (mp + nq)a$.

Theorem

Sats 2: Om $a|b$ och $a, b > 0$, gäller att $a \leq b$.

Theorem

Sats 3: Om $a|b$ och $b|a$ gäller antingen $a = b$ eller $a = -b$.

Definition

Den största gemensamma delaren till a och b ges av

$$\operatorname{sgd}(a, b) = \max\{d : d|a \text{ och } d|b\}.$$

Exempel: $\operatorname{sgd}(39, 63) = 3$.

Det är uppenbart att $\operatorname{sgd}(a, 0) = a$ för alla a .

Definition

Om $\operatorname{sgd}(a, b) = 1$ kallas a och b *relativt prima*.

Theorem

Sats 4: $\text{sgd}(a, b) = \text{sgd}(a + nb, b)$ för alla n .

Bevis: Låt $d = \text{sgd}(a, b)$ och $d' = \text{sgd}(a + nb, b)$. Eftersom $d|a$ och $d|b$ gäller $d|a + nb$ enligt Sats 1. Alltså delar d både b och $a + nb$, så $d \leq d'$.

Å andra sidan medför $d'|a + nb$ och $d'|b$ att $d'|(a + nb) - nb$, dvs $d'|a$. Alltså $d' \leq d$.

Divisionsalgoritmen: för varje par a, b av positiva heltal finns heltal q och r sådana att $0 \leq r \leq b - 1$ och

$$a = qb + r.$$

Detta är heltalsdivision. Man kallar q för *kvoten* och r för *resten* vid heltalsdivision av a med b .

Euklides algoritm:

$$a = q_1 b + r_1, \quad 0 < r_1 \leq b - 1$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 \leq r_1 - 1$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 \leq r_2 - 1$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n \leq r_{n-1} - 1$$

$$r_{n-1} = q_{n+1} r_n.$$

Då är $r_n = \text{sgd}(a, b)$, ty

$$\text{sgd}(a, b) = \text{sgd}(a - q_1 b, b) = \text{sgd}(r_1, b) = \text{sgd}(r_1, r_2)$$

$$\dots = \text{sgd}(r_{n-1}, r_n) = \text{sgd}(r_n, 0) = r_n.$$

Euklides algoritm är mycket effektiv, kräver högst $\log_2 b$ steg. Man kan också "köra den baklänges" och få *Euklides utökade algoritm*, där man finner två heltal u och v så att $au + bv = \text{sgd}(a, b)$.

Illustreras bäst med ett exempel:

Exempel: $a = 876$, $b = 204$

$$876 = 4 \cdot 204 + 60$$

$$204 = 3 \cdot 60 + 24$$

$$60 = 2 \cdot 24 + 12$$

$$24 = 2 \cdot 12.$$

Alltså är $\text{sgd}(876, 204) = 12$. Baklänges

$$\begin{aligned} 12 &= 60 - 2 \cdot 24 = 60 - 2(204 - 3 \cdot 60) = 7 \cdot 60 - 2 \cdot 204 \\ &= 7(876 - 4 \cdot 204) - 2 \cdot 204 = 7 \cdot 876 - 30 \cdot 204. \end{aligned}$$

Vi kan alltså skriva $12 = 876u + 204v$ med $u = 7$ och $v = -30$.

Primtal

Om $p \geq 2$ och de enda delarna till p är 1 och p , så kallas p för ett primtal.

Theorem

Aritmetikens fundamentalsats: *För alla heltal $a \geq 2$ gäller att a kan skrivas som en produkt av primtal. Detta kan göras på endast ett sätt, bortsett från ordningen på faktorerna.*

Bevis av existens: Påståendet är sant för $a = 2$. Tag ett $a > 2$ och antag att alla $b = 2, 3, \dots, a - 1$ kan skrivas som produkter av primtal. Nu är a antingen ett primtal, i vilket fall a är sin egen produkt av primtal, eller så kan man skriva $a = a_1 a_2$ för två tal $2 \leq a_1, a_2 \leq a/2$. Enligt antagande kan båda dessa skrivas som produkter av primtal, vilket då gäller även a . Nu följer påståendet av induktionsprincipen.

Theorem

Sats 5: Om a och b är relativt prima och $a|bc$ gäller att $a|c$.

Bevis: Enligt EUA kan man finna u och v så att $au + bv = 1$, vilket medför $acu + bcv = c$.

Att $a|acu$ är självklart och att $a|bcv$ följer av att $a|bc$. Därför gäller att $a|acu + bcv$, dvs $a|c$.

Theorem

Sats 6: Om p är ett primtal och $p|ab$ så måste $p|a$ eller $p|b$.

Bevis: Om p inte delar a gäller $\text{sgd}(a, p) = 1$, så $p|b$ enligt Sats 5.

Theorem

Sats 7: Om p är ett primtal och $p|a_1 a_2 \cdots a_k$ gäller att $p|a_i$ för minst ett i .

Theorem

Sats 8: Om p är ett primtal, $q_1, q_2, \dots, q_k$ är primtal och $p | q_1 q_2 \cdots q_k$, gäller att $p = q_i$ för minst ett i .

Bevis av entydighet i AFS: Skriv a som två olika primtalsprodukter:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

med $m \leq n$.

Då gäller att $p_1 | q_1 q_2 \cdots q_n$, så $p_1 = q_j$ för något j . Eftersom vi inte bryr oss om ordningen på primtalsfaktorerna kan vi anta att $j = 1$. Förkorta och få

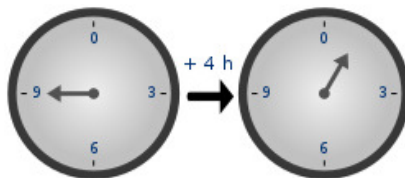
$$p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

Enligt exakt samma resonemang kan vi förkorta bort p_2, q_2 och sedan p_3, q_3 etc, tills vi får

$$1 = q_{m+1} q_{m+2} \cdots q_n.$$

Eftersom alla primtal är ≥ 2 , måste produkten till höger vara tom.

Modulär aritmetik



Definition

Man säger att a är kongruent med b modulo n , skrivet

$$a \equiv b \pmod{n}$$

om $n \mid a - b$.

Notera att $a \equiv b \pmod{n}$ är en ekvivalensrelation, ty $a \equiv a$,
 $a \equiv b \Rightarrow b \equiv a$, och $a \equiv b, b \equiv c \Rightarrow a \equiv c$. Skriv

$$[k] = [k]_n = \{j : j \equiv k \pmod{n}\}$$

för ekvivalensklassen som innehåller k .

Definition

Heltalen modulo n ges av $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$.

$\mathbb{Z}_n$ kallas också för den cykliska gruppen av ordning n .

Exempel: Med $n = 7$ får vi $\mathbb{Z}_7 = \{[0], [1], \dots, [6]\}$ och $[5] = \{\dots, -9, -2, 5, 12, 19, \dots\}$, "mängden av alla klockslag som är samma som 5 på en sjutimmarsklocka".

Räkning i $\mathbb{Z}_n$ gör man som vanligt, men slänger bort multipler av n :

- $[a] + [b] = [a + b]$,
- $[a][b] = [ab]$.

Theorem

Sats 9: Om $a \equiv c$ och $b \equiv d$ modulo n gäller att

- $a + b \equiv c + d \pmod{n}$
- $ab \equiv cd \pmod{n}$.

Bevis: Vi gör bara andra delen. Per definition finns heltal s och t så att $c - a = sn$ och $d - b = tn$. Detta ger

$$cd - ab = cd - ad + ad - ab = d(c - a) + a(d - b) = dsn + atn = (ds + at)n.$$

I uträkningar kan man när som helst slänga bort överfödiga multipler av n . Det kan underlätta mycket eller t.o.m. vara nödvändigt.

Exempel. Vad är $[2]^{4120}$ i $\mathbb{Z}_{13}$? Alternativ 1:

$$[2]^{4120} = [2^{4120}] = [\text{ett tal med ca 1300 siffror}] = [?].$$

Alternativ 2: Notera först att $[2]^{12} = [16]^3 = [3]^3 = [1]$. Alltså

$$[2]^{4120} = [2]^{2 \cdot 12^3 + 4 \cdot 12^2 + 7 \cdot 12 + 4} = [2]^4 = [3].$$

För vilka element $[b] \in \mathbb{Z}_n$ finns det invers, dvs ett element $[c]$ sådant att $[b][c] = [1]$? För detta krävs att $bc \equiv 1 \pmod{n}$, dvs $bc + nk = 1$ för något heltal k . För $\text{sgd}(b, n) = 1$ finns en lösning enligt EUA. För $\text{sgd}(b, n) = d > 1$ är $bc + nk$ delbart med d för alla k , så ingen lösning finns. Alltså:

$[b]^{-1}$ existerar i $\mathbb{Z}_n$ om och endast om $\text{sgd}(b, n) = 1$.

Man finner $[b]^{-1}$ med EUA.

Exempel. Finns $[8]^{-1}$ i $\mathbb{Z}_{19}$? Ja, ty $\text{sgd}(8, 19) = 1$. EA ger

$$19 = 2 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Baklänges ger

$$1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 = 3(19 - 2 \cdot 8) - 8 = 3 \cdot 19 - 7 \cdot 8.$$

Detta ger $[8]^{-1} = [-7] = [12]$.

Kontroll $[8][12] = [96] = [5 \cdot 19 + 1] = [1]$.