Modulär aritmetik, talbaser

Ex Vad blir resten när

$35^{115} - 2 \cdot 112^{37}$

delas med 9.

Ex:

$(37)_{10} = (100101)_2$

Problem: Hur hittar man från decimal till binärt?

Räkning med rester (restklasser)

Ex 37 delat med 5 ger resten 2

ty $37 = 7 \cdot 5 + 2$

Allmänt Om $n = kd + r$

så är r resten vid division av n med d.

Ex $37 = 5 \cdot 5 + 12$ då även 12 rest när

37 delas med 5.

Absolutminsta rest
minsta positiva rest

Ex $38 = 8 \cdot 5 - 2$

$38 = 7 \cdot 5 + 3$

-2 är absolut minsta rest

3 är minsta positiva rest

vid division med 5

Obs: $38 = 9 \cdot 5 - 7$ men $|-7| > |-2|$

Beteckning:

Om $a = kd + r$

Så

$$a \equiv r \pmod{d}$$

alt: $a \equiv_d r$

| a är kongruent med r modulo d

Ex $37 \equiv 2 \pmod{5}$, $37 \equiv_5 2$

$37 \equiv_5 -3$,

Ex $48 \equiv_7 6 \equiv_7 41 \equiv_7 -1$.

Obs: Om $a \equiv r \pmod{d}$

$r \equiv s \pmod{d}$

så $a \equiv s \pmod{d}$

Bevis: Vet $a = k_1 d + r$

$r = k_2 d + s$

$\Rightarrow a = k_1 d + r = k_1 d + k_2 d + s =$

$= (k_1 + k_2) d + s = k d + s$

Sats Anta, $a \equiv r \pmod{d}$
$b \equiv s \pmod{d}$.

obs: fixt tal d.

Då gäller

$$a+b \equiv r+s \pmod{d}$$

$$a-b \equiv r-s \pmod{d}$$

$$a \cdot b \equiv r \cdot s \pmod{d}$$

$$a^n \equiv r^n \pmod{d}$$

Ex $10 \equiv 1 \pmod{9} \Rightarrow 10^{10000000} \equiv_9 1^{10000000} \equiv_9 1$

Ex $323 \cdot 512$ Dividera med 5

Vad blir resten?

Lösning: $323 \equiv_5 3$, $512 \equiv_5 2$.

$323 \cdot 512 \equiv_5 3 \cdot 2 \equiv_5 6 \equiv_5 1$

Svar 1, th

$6 = 1 \cdot 5 + 1$

Ex: $323^{512} \equiv ? \pmod 5$

Lösning: $323 \equiv 3 \pmod 5$

$$323^{512} \equiv_5 3^{512} \equiv_5 (3^4)^{128} \equiv_5 81^{128} \equiv_5 1^{128} \equiv_5 1.$$

Ex Vad blir resten när

$$35^{115} - 2 \cdot 112^{37}$$

delas med 9.

Lösning: $35 \equiv_9 (-1)$, $112 \equiv_9 4$.

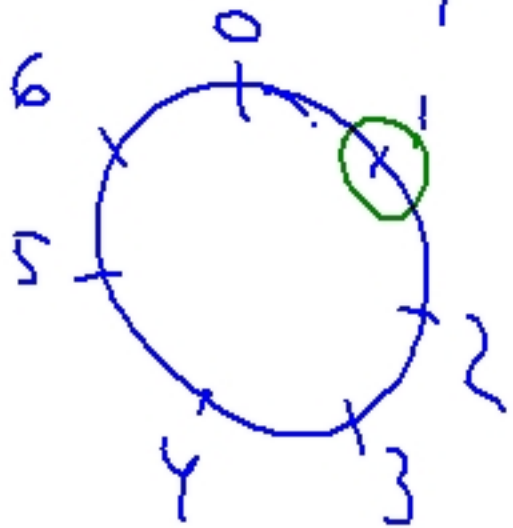
$$35^{115} - 2 \cdot 112^{37} \equiv_9 (-1)^{115} - 2 \cdot 4^{37} \equiv_9 -1 - 2(4^3)^{12} \cdot 4 \equiv_9$$

$$\equiv_9 -1 - 2 \cdot (64)^{12} \cdot 4 \equiv_9 -1 - 2 \cdot 1^{12} \cdot 4 \equiv_9 -9 \equiv_9 0$$

Ringen $\mathbb{Z}_n$

Ex $\mathbb{Z}_7$ består av elementen

$0, 1, 2, \ldots, 6$



man räknar modulo 7.

$5+4=2$

ty $5+4 \equiv_7 2$

$5 \cdot 4 = 6$ $\quad 3 \cdot 5 - 6 = 1 - 6 = 2$

$3 \cdot 5 - 6 \equiv -15 - 6$

$\equiv_7 9 \equiv 2$

Allmänt: $\mathbb{Z}_n$ består av elementen

$$0, 1, 2, \ldots, n-1.$$

Addition, subtraktion och multiplikation sker modulo n.

(Anm. Egentligen är elementen restklasser t.ex: $\mathbb{Z}_7$ är 1 resterna $1, 8, -6, 15, -13 \ldots$)

Ex Betrakta $\mathbb{Z}_{13}$

Beräkna $9 \cdot 2 - 11 \cdot 5 + 8 \cdot 3 \; : \mathbb{Z}_{13}$

Lösning:

$9 \cdot 2 - 11 \cdot 5 + 8 \cdot 3 = 5 - 3 + 11 = 0$

Övning $\mathbb{Z}_{11}$ $5 \cdot 4 - 2(3+4) = 6$

ty $5 \cdot 4 - 2(3+4) \equiv_{11} 20 - 14 \equiv_{11} 6$

Övning Lös i Z_5 resp Z_6

$2x = 1$

Lösning:

Vi prövar

$2 \cdot 0 = 0$

$2 \cdot 1 = 2$

$2 \cdot 2 = 4$, $2 \cdot 4 = 3$

$2 \cdot 3 = 1$

$k = 3$ i Z_5

$2 \cdot 0 = 0$ $2 \cdot 4 = 2$

$2 \cdot 1 = 2$ $2 \cdot 5 = 4$

$2 \cdot 3 = 0$

Svar i Z_6 ingen lösning

Ex Lös $8x = 1$ i $\mathbb{Z}_{13}$

Lösning: m.hj.a Euklides algoritm.

OBS: Att $8x = 1$ i $\mathbb{Z}_{13}$ är samma sak att

$8x = n \cdot 13 + 1$ eller $1 = k \cdot 8 - n \cdot 13$

Diofantisk ekv.

$13 = 2 \cdot 8 - 3$ || $1 = 3 \cdot 3 - 8$ || $1 = 5 \cdot 8 - 3 \cdot 13$

$8 = 3 \cdot 3 - 1$ || $= 3 \cdot (2 \cdot 8 - 13) - 8$ ||

Räkna nu modulo 13

$1 \equiv_{13} 5 \cdot 8 - 3 \cdot 13 \equiv_{13} 5 \cdot 8 - 3 \cdot 0 \equiv_{13} 5 \cdot 8$

Svar:
$x = 5$
+y
$5 \cdot 8 \equiv_{13} 1$

Ex Lös $23x = 5$ i $\mathbb{Z}_{37}$

Lösning: Skall lösa $23x = n \cdot 37 + 5$

$5 = -n \cdot 37 + x \cdot 23$

Löser först

Svar

$x = 34$.

Euklides alg.

$37 = 2 \cdot 23 - 9$

$23 = 3 \cdot 9 - 4$

$9 = 2 \cdot 4 + 1$

$1 = n_1 \cdot 37 - x_1 \cdot 23$

$1 = 9 - 2 \cdot 4 = 9 - 2 \cdot (3 \cdot 9 - 23) =$

$= 2 \cdot 23 - 5 \cdot 9 = 2 \cdot 23 - 5 \cdot (2 \cdot 23 - 37)$

$= -8 \cdot 23 + 5 \cdot 37$

Nu vet vi

$1 = 5 \cdot 37 - 8 \cdot 23 \Rightarrow 5 = 25 \cdot 37 - 40 \cdot 23$

$5 \equiv_{37} -40 \cdot 23$

$-40 \equiv_{37} -3 \equiv$

$\equiv 34$

$5 = 25 \cdot 37 - 40 \cdot 23$ | $23x = 5$: Z_{37}

Räknar nu modulo 37, ty vi vill tillbaka in i ringen Z_{37}

$\boxed{5} \equiv_{37} 25 \cdot 37 - 40 \cdot 23 \equiv_{37} 25 \cdot 0 - 40 \cdot 23$

$\boxed{\equiv_{37} -40 \cdot 23}$. Obs -40 inget av elementen i Z_{37}

Men

$-40 = (-1) \cdot 37 - 3$ så $-40 \equiv_{37} -3$

och $-3 = -37 + 34$ så $-3 \equiv_{37} 34$

$5 \equiv_{37} -40 \cdot 23 \equiv_{37} 34 \cdot 23$ Svar $x = 34$

Ex Z_{52} lös ekv $3x+7=11$

Lösning: $(3x+7)-7=11-7$

$3x=4$

Söker nu x s.a

$3x \equiv_{52} 4$

dvs $3x=4+52$

$4=x\cdot 3-4\cdot 52$

Löser först $1=43+m52$

Euklides alg.

$52=17\cdot 3+1$

$1=1\cdot 52-17\cdot 3$

Räkna nu modulo 52

$1\equiv_{52} 1\cdot 0-17\cdot 3\equiv_{52} 35\cdot 3$

$4\equiv_{52} 140\cdot 3\equiv 36\cdot 3$

Svar $x=36$.

Talbaser:

Transformera decimaltal till binärtal.

Ex $23 = 2 \cdot 10^1 + 3 \cdot 10^0 = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2 + 1$

Man kan skriva $(23)_{10} = (10111)_2$

ty $23 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

Algoritm för bestämning av binär framställning av tal.

Ex 67 skrivs binärt

$67 = 2 \cdot 33 + 1$

$33 = 2 \cdot 16 + 1$

$16 = 2 \cdot 8 + 0$

$8 = 2 \cdot 4 + 0$

$4 = 2 \cdot 2 + 0$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

Binära framställningen av 67 är

1000011

1000011 motsvarar

$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1$

VARFÖR FUNGERAR DET

Ex

$23 = 2 \cdot 11 + 1$

$11 = 2 \cdot 5 + 1$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

$(23)_{10} = (1\,0\,1\,1\,1)_2$

$23 = 2 \cdot 11 + 1 = 2 \cdot (2 \cdot 5 + 1) + 1 =$

$= 2 \cdot (2 \cdot (2 + 1) + 1) + 1 =$

$= 2 \cdot (2 \cdot (2 \cdot 1 + 0) + 1) + 1) + 1$

$= 2 \cdot (2 \cdot (2 \cdot (2 \cdot 0 + 1) + 0) + 1) + 1) + 1$

$= 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$