Kræsjkurs MNF130

Steinar Simonnes og Carina Seidel

Institutt for Informatikk
Universitetet i Bergen

22. Mai 2024

Agenda

Slides 'n' Slido

Dere kan stille spørsmål digitalt og anonymt her:
`sli.do`, med koden "MNF130"

Dere finner presentasjonen og kildekoden på mittuib, eller her:
`tinyurl.com/MNF130-Slides`

Divisjon og Modulær aritmetikk

Delelighet $a|b$ (a deler b)

a kan dele b uten rest
$a|b$ er det samme som $\frac{b}{a} = c$ eller $b = a \cdot c$ med $c \in \mathbb{Z}$
Eksempel: $3|12$ eller $\frac{12}{3} = 4$ eller $12 = 3 \cdot 4$

Modulo (Klokkearitmetikk)

$a\, mod\, b$ gir ut resten av heltall divisjon av $\frac{a}{b}$ ($a\%b$ i programmeringsspråk) $a\, mod\, b = r$ kalles *remainder* Eksempel: $17\, mod\, 5 = 2$ fordi $17 = 3 \cdot 5 + 2$

Algoritme for divisjon /modulo

- $d = q \cdot a + r$ med
- $q = \left\lfloor \frac{d}{a} \right\rfloor$ og $r = d\, mod\, a$
- Eksempel: $q = \left\lfloor \frac{17}{5} \right\rfloor = \lfloor 3.4 \rfloor = 3$
- $17 = 3 \cdot 5 + r \iff 17 = 15 + r \iff r = 2$

Modulo regneregler

Kongruens $\equiv$

- $a \equiv b \pmod{m}$: a og b kongruent i forhold til mod m
- $a \equiv b \pmod{m}$ betyr $a \mod m = b \mod m$
- vi skriver $[a]_m := a (\mathrm{mod}\ m)$
- Eksempel: $8 \equiv 3 \pmod{5} \equiv [3]_5$ betyr $[8]_5 = 3 = [3]_5$

- Addisjon: $[a+b]_m = [[a]_m + [b]_m]_m$
- $[8+21]_6 = [[8]_6 + [21]_6]_6 = [2+3]_6 = [5]_6 = 5$
- Multiplikasjon: $[a \cdot b]_m = [[a]_m \cdot [b]_m]_m$
- $[8 \cdot 21]_6 = [[8]_6 \cdot [21]_6]_6 = [2 \cdot 3]_6 = [6]_6 = 0$

Eksempel

- $x \equiv 3 \,(mod\, 5)$ eller $[x]_5 = 3$
- $y \equiv 4 \,(mod\, 5)$ eller $[y]_5 = 4$
- Finn løsningen: $(3 \cdot x + 2 \cdot y^2)\, mod\, 5$

$$[3 \cdot x + 2 \cdot y^2]_5 = [[3 \cdot x]_5 + [2 \cdot y^2]_5]_5$$

$$[3 \cdot x]_5 = [[3]_5 \cdot [x]_5]_5 = [3 \cdot 3]_5 = [9]_5 = 4$$
$$[2 \cdot y^2]_5 = [[2]_5 \cdot [y \cdot y]_5]_5 = [[2]_5 \cdot [y]_5 \cdot [y]_5]_5 = [2 \cdot 4 \cdot 4]_5 = [32]_5 = 2$$

$$[[3 \cdot x]_5 + [2 \cdot y^2]_5]_5 = [4 + 2]_5 = [6]_5 = 1$$

Modulo ved subtraksjon

Vi vet at vi har addisjon, men hva er med subtrasjon?

Substraksjon:
$[6-3]_8 = [3]_8$
$[3-6]_8$?
$[3-6]_8 = [-3]_8 = [0-3]_8 = [8-3]_8 = [5]_8 = 5$

Subtraksjon fungerer også for modulo.

Modulo ved divisjon

Vi vet at vi har multiplikasjon, men hva med divisjon?

Divisjon:
$[6/3]_8 = [2]_8$? ja, fordi $[2 \cdot 3]_8 = [6]_8$
$[3/6]_8$?
Nei, noen ganger fungerer det, noen ganger fungerer det ikke.

Vi kan ikke alltid dele!

Tallsystem

En representasjon av tall med forskjellige tegn med en base

Navn	Sifre	5	11	34
Desimal (b=10)	0-9	5	11	34
Binær (b=2)	0-1	101	1011	100010
Octal (b=8)	0-7	5	13	42
Hexadesimal (b=16)	0-9,a-f	5	B	22
base=13	0-9,a-c	5	B	28

Tabell: Eksempler på forskjellige tallsystemer

Desimal til base b

pseudokode

tall n til base b:

next digit $= n\%b$

$n = \frac{n}{b}$

forsette med det til $n = 0$

n	nextDigit	output
22		0
11	0	0
5	1	10
2	1	110
1	0	0110
0	1	10110

Tabell: Eksempel for dec til base 2

Base b til desimal

pseudokode

tall n og base b
$sum = 0; index = 0$
starter med først siffer s:
$sum + = base^{index} \cdot s$
$index + = 1$
forsette med hver siffer s

tall	1	0	1	1	0
base	16	8	4	2	1
produkt	16	0	4	2	0

Tabell: Eksempel for 2 til dec

$$16 + 0 + 4 + 2 + 0 = 22$$

GCD

La oss si at vi har en brøk: $\frac{12}{18}$. Hvordan forenkle den?
Vi deler telleren og nevneren på 6, og får $\frac{2}{3}$. Men hvorfor 6?
Fordi 6 er det største tallet som deler både 12 og 18. Den største felles faktoren er 6.

Største felles faktor (/Greatest Common Divisor)

$gcd(a,b) :=$ det største tallet som deler både a og b
Eksempel: $gcd(12,18) = 6$.

Relativt primisk (/co-prime)

To heltall a og b kalles *relativt prime*, eller *co-prime*, dersom $gcd(a,b) = 1$.
Eksempel: 8 og 21 er relativt prime, siden $gcd(8,21) = 1$.

LCM

Vi har en sum av to brøker: $\frac{5}{18} + \frac{7}{12}$. Hvordan forenkle det?
Vi ganger den venstre med 2, og den høyre med 3, så begge får 36 i nevneren:
$\frac{10}{36} + \frac{21}{36} = \frac{31}{36}$. Men hvorfor 36?
Fordi 36 er det laveste tallet som begge nevnerene kan ganges opp til, deres laveste felles multiplum er 36.

Laveste felles multiplum (/Least common multiple)

$lcm(a, b) :=$ det minste tallet som kan deles av både a og b
Eksempel: $lcm(18, 12) = 36$
Det er alltid sant at $a \cdot b = lcm(a, b) \cdot gcd(a, b)$, så vi kan regne ut LCM med $lcm(a, b) = \frac{a \cdot b}{gcd(a,b)}$.

Euklids algoritme

```python
def gcd(a, b):
    while b != 0:
        r = a % b
        a = b
        b = r
    return a
```

$gcd(\underline{1180},\underline{482})$:

$$\underline{1180} = 2 \cdot \underline{482} + \underline{216}$$
$$\underline{482} = 2 \cdot \underline{216} + \underline{50}$$
$$\underline{216} = 4 \cdot \underline{50} + \underline{16}$$
$$\underline{50} = 3 \cdot \underline{16} + \underline{2}$$
$$\underline{16} = 8 \cdot \underline{2} + 0$$

$gcd(1180, 482) = 2.$

Utvidet Euklids algoritme

Regner ut to parameter s og t slik at $gcd(a, b)$ kan skrives som linærkombinasjon
$gcd(a, b) = s \cdot a + t \cdot b$
$gcd(12, 28) = 4 = -2 \cdot 12 + 1 \cdot 28$

Kan brukes for å finne multiplikativt invers
Multiplikativ inverse finnes dersom $gcd(a, b) = 1$

Finne multiplikativt invers for a med $mod\, m$

- Funker bare dersom $gcd(a, m) = 1$
- Regn ut linærkombinasjon $gcd(a, b) = s \cdot a + t \cdot b$ med gcd
- $a \cdot x \equiv 1(mod\, m)$ er multiplicative inverse

Extended Euklids algoritme

gcd(26,7)

$(26) = 3 \cdot (7) + (5)$

$(7) = 1 \cdot (5) + (2)$

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

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

gcd(26,7)=1

Nå går vi tilbake:

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

$\implies 1 = (5) - 2 \cdot (2)$

$= (5) - 2 \cdot ((7) - (5))$

$= 3 \cdot (5) - 2 \cdot (7)$

$= 3 \cdot ((26) - 3 \cdot (7)) - 2 \cdot (7)$

$= 3 \cdot (26) - 11 \cdot (7)$

Eksempel Multiplikativt Invers

- Hva er multiplikativt invers av $7\, mod\, 26$? $(a \cdot 7 = 1\, mod\, 26)$
- $gcd(a, m) = gcd(7, 26) = 1 \rightarrow$ har multiplikativt invers
- Linærkombinasjon fra gcd: $3 \cdot (26) - 11 \cdot (7) = 1$
- $[1]_{26} = [3 \cdot (26) - 11 \cdot (7)]_{26} = [-11 \cdot 7]_{26}$
- $a = -11$
- $[-11]_{26} = [26 - 11]_{26} = [15]_{26} = 15$
- 15 er inverse av 7 modulo 26

Spørsmål?

Figur: Guillaume på Sandviksfjellet

Spørretid

Lykke til på eksamen!

Takk for oss :)