Forelesning 12

MER TALLTEORI

- Euklids (utviklende) algoritme for
  - ↳ å lage gcd(a,b)
  - ↳ å løse diofantiske ligninger
- Minste felles multiplum, LCM
- Litt mer om primtall og primtallsfaktorisering
  - ↳ Eratosthenes' sil
  - ↳ Fermat's faktoriseringsmetode

Forrige gang så vi på lineære diofantiske ligninger

$ax + by = c$ der $a,b,c \in \mathbb{Z}$ og vi er ute etter heltallsløsninger av slike

Vi så at $20x+24y=14$ ikke kan løses fordi $\gcd(20,24)=4$ ikke deler 14.

Det viser seg at $ax+by=c$ kan løses hvis og bare hvis $\gcd(a,b) \mid c$

M.a.o. hvis det finnes en d slik at $ax+by=c=d\cdot\gcd(a,b)$

Eksempel

$36x+60y=24$ kan løses fordi $\gcd(36,60)=12$ og $12 \mid 24$

Men: Kan vi raskt beregne $\gcd(a,b)$?
Og: Hvordan finner vi løsninger hvis de finnes?

Begge deler gjøres med Euklids (utvidede) algoritme ♡

Euklids algoritme baserer seg på følgende (anta at $a \geq b > 0$)

1. Hvis $d|a$ og $d|b$ så vil $d|(a-b)$
2. Hvis $d|(a-b)$ og $d|b$ så vil $d|a$

Bevis i ØF

Dermed vil $\gcd(a,b) = \gcd(a-b,b)$

Eksempel

$$\gcd(74,22) = \gcd(74-22,22) = \gcd(52,22)$$
$$= \gcd(52-22,22) = \gcd(30,22)$$
$$= \gcd(30-22,22) = \gcd(8,22) = \underline{\underline{2}}$$

Hva skjedde nettopp?

$74 = 3 \cdot 22 + 8$ (74 delt på 22 gir rest på 8)

Så hvis $a = q \cdot b + r$ så er $\gcd(a,b) = \gcd(r,b)$
$= \gcd(b,r)$

Eller med andre ord

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

Eksempel (på nytt)

$$\gcd(74,22) = \gcd(22, 74 \bmod 22) = \gcd(22,8)$$
$$= \gcd(8, 22 \bmod 8) = \gcd(8,6)$$
$$= \gcd(6, 8 \bmod 6) = \gcd(6,2)$$
$$= 2$$

Oppsummert:

1. Hvis $b|a$ så er $\gcd(a,b) = b$
2. $\gcd(a,b) = \gcd(b, a \bmod b)$

Euklids algoritme:

Repeter punkt 2 til du kan bruke punkt 1

Eksempel

Finn gcd(234,42)

Ofte bruker vi Euklids algoritme ved å gjennomføre heltallsdivisjoner og ta med relevante tall videre

$$a = q \cdot b + r \ (a \bmod b)$$

$$234 = 5 \cdot 42 + 24$$
$$42 = 1 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6$$
$$18 = 3 \cdot 6 + 0$$

Løsning: Siste rest som ikke er lik null

Så $\underline{\underline{\gcd(234,42) = 6}}$

Så slik kan vi beregne gcd(a,b) og avgjøre om $ax + by = c$ kan løses

Men hvordan finner vi løsningen?

Euklids utvidede algoritme

Definisjon

Et uttrykk på formen $ax + by$ kalles en lineærkombinasjon av a og b

Hvis vi finner gcd(a,b) med Euklids algoritme så kan vi jobbe oss bakover og skrive gcd(a,b) som en lineær kombinasjon av a og b.

Eksempel

Løs ligningen $234x + 42y = 6$

Vi hadde

$$234 = 5 \cdot 42 + 24 \iff 24 = 234 - 5 \cdot 42$$
$$42 = 1 \cdot 24 + 18 \iff 18 = 42 - 1 \cdot 24$$
$$24 = 1 \cdot 18 + 6 \iff 6 = 24 - 1 \cdot 18$$
$$18 = 3 \cdot 6 + 0$$

Hvis vi starter med 6 og går baklengs får vi

$$6 = 24 - 1 \cdot 18 = 24 - 1 \cdot (42 - 1 \cdot 24) = -1 \cdot 42 + 2 \cdot 24$$
$$= -1 \cdot 42 + 2 \cdot (234 - 5 \cdot 42) = 2 \cdot 234 - 11 \cdot 42$$

Dvs: $234 \cdot 2 + 42(-11) = 6$ og løsningen er $\underline{x = 2}$ og $\underline{y = -11}$

Men hva om høyresiden c ikke er lik $\gcd(a,b)$?
Vi vet at det finnes løsning $\Leftrightarrow \gcd(a,b) \mid c$.
Så da må høyresiden være et multiplum av $\gcd(a,b)$.

Eksempel

Løs ligningen $234x + 42y = 24$

Vi har at $\gcd(234,42) = 6$ og $6 \mid 24$ så dette kan løses.
Fra i stad har vi

$$234 \cdot 2 = 42 \cdot (-11) = 6 \quad | \cdot 4$$
$$234 \cdot 8 = 42 \cdot (-44) = 24$$

Så $\underline{x = 8}$ og $\underline{y = -44}$

Fremgangsmåte (for å løse $ax + by = c$)

① Beregn $\gcd(a,b)$ med Euklids algoritme

② Hvis $\gcd(a,b) \nmid c \Rightarrow$ ingen løsning

③ Hvis $\gcd(a,b) \mid c$, skriv $\gcd(a,b)$ som en lineærkombinasjon av a og b, og gang ligningen med $\dfrac{c}{\gcd(a,b)}$ for å finne x og y.

Minste felles multiplum (LCM)

"least common multiplum

Definisjon

La a og b være heltall. Da er $\mathrm{lcm}(a,b)$ (minste felles multiplum) det minste tallet som er et multiplum av både a og b.

Eksempel

Hva er $\mathrm{lcm}(4,10)$?

$$\left.\begin{array}{ll} \text{Vi har} & 4 \;\; 8 \;\; 12 \;\; 16 \;\; 20 \;\; 24 \\ & 10 \;\; 20 \;\; 30 \;\; 40 \end{array}\right\} \; \mathrm{lcm}(4,10) = 20$$

Merk at $\mathrm{lcm}(a,b) \leq a \cdot b$
Og en liten funfact:

$$a \cdot b = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$$

Litt mer om primtall og primtallsfaktorisering

Eratosthenes' sil: Enkel algoritme for å finne alle primtall mindre enn n.

Eksempel $n = 20$

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

(Gir ikke en faktorisering, men en liste med primtall)

Fermat's faktoriseringsmetode:

Godt egnet for tall som er produktet av to ca. like store primtall, $n = p \cdot q$ der $p \approx q$

Ideen: Kan vi finne tall a og b slik at $n = a^2 - b^2$?

I så fall er vi i mål siden $n = (a-b)(a+b)$
Hvis faktorene er ca. like store ($\approx \sqrt{n}$), så vi kan gå ut fra at b er liten og at a er nærme $\sqrt{n}$.

Metoden går slik: (hvis $n = a^2 - b^2$ så er $a^2 - n = b^2$)

1. Sett $a_1 = \lceil \sqrt{n} \rceil$ ($\sqrt{n}$ rundet opp til nærmeste heltall)
2. Undersøk om $a_1^2 - n$ er et kvadrattall. Hvis ja: ferdig
3. Hvis nei, la $a_2 = a_1 + 1$ og sjekk om $a_2^2 - n$ er et kvadrattall

fortsett til vi har a_k slik at $a_k^2 - n$ er et kvadrattall

Eksempel

Finn primtallsfaktoriseringen av $n = 778207$

$\sqrt{n} \approx 882{,}16$ så la $a_1 = 883$
$a_1^2 - n = 1482$ ← ikke et kvadrattall
Prøv med $a_2 = a_1 + 1 = 884$
$a_2^2 - n = 3249 = 57^2$ ← kvadrattall

Så la $a = 884$ og $b = 57$ og vi har
$n = p \cdot q$ med $p = a \cdot b = 827$ og
$q = a \cdot b = 941$