EUKLIDS ALGORITME

Den Diofantiske ligningen

$$aX + bY = C$$

kan løses hvis og bare hvis

$$\overbrace{(a,b)}^{d} \mid C$$

I så fall holder det å løse

$$C = Kd$$

$$ax + by = d$$

$$r_0 = a \,,\; r_1 = b$$

$$r_0 = q_1 r_1 + r_2$$

$$r_1 = q_2 r_2 + r_3$$

$$r_j = q_{j+1} r_{j+1} + r_{j+2}$$

$$r_n = q_{n+1} r_{n+1} + r_{n+2} = d$$

$$r_{n+1} = q_{n+2} r_{n+2}$$

EKSEMPEL: Finn $(105, 27)$

$$105 = 3 \cdot 27 + 24$$

$$27 = 1 \cdot 24 + 3$$

$$24 = 8 \cdot 3$$

Så $(105, 27) = 3$

Finn lineær kombinasjon.

$$3 = 27 - 1\,24 = 27 - (105 - 3 \cdot 27)$$

$$= 4 \cdot 27 - 105$$

Prop: Vi kan alltid skrive (a,b) som en lineær kombinasjon av a og b.

Prop: Anta at x og y løser ligningen

$$ax + by = (a,b) = d$$

27)

b.

Da er også

$x_k = x + k\frac{b}{d}$, $y_k = y - k\frac{a}{d}$, $k \in \mathbb{Z}$

løsninger av ligningen.

Lemma 18 Anta at $(a', b') = 1$ og

anta at $a' | b' \cdot c$.

Da har vi $a' | c$

Bevis: • $sa' + tb' = 1$ $\Rightarrow$ $csa' + ctb' = c$

• $b'c = da'$

$$csa' + ctb' = csa' + tda' = a'(cs + td) \quad \blacksquare$$

Korollar: Anta at $(a', b') = 1$ Dersom $\frac{a'}{b'} \cdot x_0 = c \in \mathbb{Z}$

Da må $b' | x_0$

$ax + by = d$

x, y.

Vi finne alle løsninger av ligningen

$$\boxed{ax + by = 0}$$

Vi kan skrive $a = a'd$, $b = b'd$, $d \nmid (a, b)$

Da er $(a', b') = 1$.

Må ha $y_0 = -\frac{a x_0}{b} = -\frac{a' x_0}{b'}$

Må ha $x_0 = k b' = k \cdot \frac{b}{d}$

Får da at $y_0 = -\frac{a'}{b'} k \frac{b}{d} = -k \frac{a}{d}$.

Da har vi at

$$\tilde{x}_k = k \frac{b}{d}, \quad \tilde{y}_k = -k \frac{a}{d}$$

løser ligningen $a\tilde{x}_k + b\tilde{y}_k = 0$ for alle $k \in \mathbb{Z}$, og disse er de eneste løsningene.

Da løser

$$x_k = x + k \frac{b}{d}, \quad y_k = y - k \frac{a}{d}$$

ligningen $ax_k + by_k = d$ for alle $k \in \mathbb{Z}$, og disse er de eneste løsningene

Primtall og primtallsfaktorisering

DEF: Et naturlig tall $p \geq 2$ kalles et **primtall** dersom det ikke har andre divisorer enn 1 og p.

Lemma 23 La p være et primtall og anta $p \mid a \cdot b$. Da har vi $p \mid a$ eller $p \mid b$.

Bevis: Hvis $p \mid a$ V.
Ellers har vi $(a, p) = 1$

Men da har vi selv $p \mid b$. ∎

Generalisert: $p \mid a_1 a_2 \dots a_n \Rightarrow p \mid a_j$ for minst en j.

Teorem 23. Ethvert naturlig tall $a > 0$ kan skrives som et produkt

$$a = p_1 \cdot \dots \cdot p_n$$

av primtall, og dette er unikt opp til rekkefølge

Bevis: EKSISTENS

Hvis ikke finns et minste tall $a \geq 2$ som ikke er produkt av primtall.

Da er a ikke et primtall, så $a = b \cdot c$, der $b, c \neq 1$. Det vil si at $b < a$, $c < a$.

Men da er både b og c produkt av primtall.

UNIKHET:

Vil vise unikhet

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

ved induksjon på n.

For $n = 1$ OK.

Anta at det holdes for n, og se på

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

$p_{n+1} \mid a$

Da kan vi anta at $p_{n+1} \mid q_{m+1}$,

men da har vi $p_{n+1} = q_{m+1}$

Da faktoriserer vi ut p_{n+1},

og resultatet følges ved induksjon.

Teorem 2.4 Vi har at $\sqrt{2}$ er irrasjonal.

Bevis: Hvis ikke

$$2 = \frac{n^2}{n^2} = \frac{p_1^2 \cdots p_n^2}{q_1^2 \cdots q_m^2}$$

$$2\, q_1^2 q_2^2 \cdots q_m^2 = p_1^2 \cdots p_n^2$$

oddetall antall 2-ere = like antall 2-ere.

motsigelse ∎

Teorem 2.5 Det finns uendelig mange primtall.

Bevis: Anta at alle primtallene er $p_1, p_2, \ldots, p_n$.

Se på $q = p_1 p_2 \cdots p_n + 1$.

Da må en av p_j'ene dele q; for eksempel p_1.

Men $\frac{q}{p_1} = p_2 p_3 \cdots p_n + \frac{1}{p_1}$ er ikke et naturlig tall. Motsigelse. ∎

Ethvert primtall $p > 2$ kan skrives

$p = K \cdot 4 + r$,

$0 < r < 4$. Da må $r = 1$ eller $r = 3$.

Prop 26. Det fins uendelig mange primtall som er kongruente med 3 (mod 4).

Lemma Dersom $a \equiv_4 1$ og $b \equiv_4 1$, så er $a \cdot b \equiv_4 1$

Bevis: $a = K_1 4 + 1$

$b = K_2 4 + 1$

Regn ut $a \cdot b$.

Bevis for Prop. 26

Anta at det kun fins endelig mange primtall $P_1, P_2, \ldots, P_m$ som er kongruente med 3 (mod 4);

og anta at $p_1 = 3$.

Vi ser på

$a = 4 p_2 p_3 \cdots P_{11} + 3$

Ingen av p_j'ene kan dele a.

Men a må ha en primtallsfaktorisering

$a = q_1 q_2 \cdots q_n$

Pga gjenn av lemmaet er

minst en $q_j \equiv_4 1$ — MOTSIGELSE!