Kvadratsummer

Et naturlig a kalles en kvadratsum dersom det finnes tall $x, y \in \mathbb{Z}$ slik at

$$a = x^2 + y^2$$

OBS: Tillater $x=0$ eller $y=0$. Hvis a er et primtall, så er $x \neq 0, y \neq 0$.

a primtall:
$2 = 1^2 + 1^2$
$3 = ?$
$5 = 2^2 + 1^2$
$7 = ?$
$11 = ?$
$13 = 3^2 + 2^2$

Lemma: En kvadratsum kan ikke være kongruent med 3 (mod 4)

Bevis: Anta at $a = x^2 + y^2$, da $\bar{a} = \bar{x}^2 + \bar{y}^2$ i $\mathbb{Z}/(4)$

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{x}^2$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$

$\bar{0} + \bar{0} = \bar{0}$
$\bar{1} + \bar{0} = \bar{1}$
$\bar{0} + \bar{1} = \bar{1}$
$\bar{1} + \bar{1} = \bar{2}$

Teorem: Hvis p er et primtall som ikke er kongruent med 3 (mod 4) (dvs $p = 2$ eller $p \equiv 1 \pmod 4$), så er p en kvadratsum.

Bevis: $p = 2$: $2 = 1^2 + 1^2$, så 2 er en kvadratsum.

$p \equiv 1 \pmod 4$: I dette tilfellet er $\bar{-1}$ en kvadratisk rest, så det finnes en i slik at $\bar{i}^2 = \bar{-1}$.

La nå k være det største hele tallet mindre enn $\sqrt{p}$:

$$0, 1, 2, \dots, k, \quad k+1, \dots, p-1$$

($\sqrt{p}$ ligger mellom k og $k+1$)

La $f(\bar{u}, \bar{v}) = \bar{u} + \bar{i}\bar{v}$ og se på alle par (u, v) $0 \leq u, v \leq k$. Ser på $(k+1)^2$ par, dvs flere enn p par.

Siden det bare finnes p restklasser, må det finnes par (u, v) og (u', v') slik at

$$\bar{u} + \bar{i}\bar{v} = \bar{u}' + \bar{i}\bar{v}'$$

Det betyr at $\underbrace{\bar{u} - \bar{u}'}_{\bar{x}} = \bar{i}\underbrace{(\bar{v}' - \bar{v})}_{\bar{y}}$ dvs $\bar{x} = \bar{i}\bar{y}$.

Dermed er

$$\bar{x}^2 + \bar{y}^2 = \bar{i}^2\bar{y}^2 + \bar{y}^2 = (\underbrace{\bar{i}^2}_{-1} + 1)\bar{y}^2 = \bar{0} \cdot \bar{y}^2 = \bar{0}$$

Dette betyr at $x^2 + y^2 = np$ for et helt tall n.

Hvis vi kan vise at $n = 1$, så er vi ferdige.

Siden $0 \leq u, v < \sqrt{p}$, så er $|x| = |u - u'| < \sqrt{p}$
$|y| = |v' - v| < \sqrt{p}$

Dermed er $x^2 + y^2 < p + p = 2p$, så $x^2 + y^2 = p$.

Dette viser at p er en kvadratsum.

Hva skjer når a ikke er et primtall?

Lemma: Hvis x og y er kvadratsummer, så xy også en kvadratsum.
Tilsvarende $x_1, \dots, x_n$ er kvadratsummer, så $x_1 x_2 \cdots x_n$ en kvadratsum.

Bevis: Hvis $x = b^2 + c^2$, $y = d^2 + e^2$, så

$$xy = (b^2+c^2)(d^2+e^2) = (bd+ce)^2 + (be-cd)^2$$

gang ut og sammenlign.

Lemma: Hvis $a = x^2 + y^2$ der x og y er innbyrdes primiske, så
a ikke delelig med noe primtall som er kongruent med 3 (mod 4).

Bevis: Anta at p er en primfaktor i a. Observer at p ikke
deler x eller y siden x og y er innbyrdes primiske. Vi vet
at ligningen $\bar{k}\bar{x} = \bar{y}$ har en løsning $\bar{k}$ i $\mathbb{Z}/(p)$. Dermed er

$\mathbb{Z}/(p)$: $\bar{0} = \bar{a} = \bar{x}^2 + \bar{y}^2 = \bar{x}^2 + \bar{k}^2\bar{x}^2 = (\bar{1}+\bar{k}^2)\bar{x}^2$, altså $\bar{1}+\bar{k}^2 = \bar{0}$ eller $\bar{k}^2 = -\bar{1}$.
Dette betyr at -1 er en kvadratisk rest i $\mathbb{Z}/(p)$, så $p \neq 3$ i $\mathbb{Z}/(4)$

Lemma: Hvis a er en kvadratsum, så vil enhver primfaktor i a
som er kongruent med 3 (mod 4), gå opp i a et like antall ganger.

Bevis: Hvis $a = x^2 + y^2$ og d er største felles faktor i x og y, så kan
vi $x_0 = \frac{x}{d}$ og $y_0 = \frac{y}{d}$. Da er x_0 og y_0 innbyrdes primiske og

$$a = x^2 + y^2 = d^2 x_0^2 + d^2 y_0^2 = d^2(x_0^2 + y_0^2)$$

kvadratsum av innbyrdes primiske elementer
$\Rightarrow$ ikke delelig med noe primtall $p \equiv 3 \pmod 4$

primfaktorisering: $p_1^2 p_2^2 \cdots p_r^2 \cdot q_1 q_2 \cdots q_s^2$ (q^2, $x_0^2 + y_0^2$).

Siden alle primfaktorene som $\equiv 3 \pmod 4$ kommer fra den første delen, er det alltid et like antall av dem.

Teorem: Et naturlig tall a er en kvadratsum hvis og bare hvis
enhver primfaktor i a som er kongruent med 3 (mod 4) går opp
i a et like antall ganger.

Bevis: Ved fra lemmaet at hvis betingelsen ikke er oppfylt, så er ikke
a en kvadratsum. Vi må derfor vise at hvis betingelsen er
oppfylt, så er a en kvadratsum. Primfaktorisering.

kvadratsummer.

$a = p_1^2 p_2^2 \cdots p_r^2 \cdot q_1 q_2 \cdots q_s$ (kvadratsum)

$p_1^2 + 0^2$

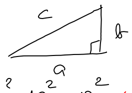
primfaktorene som er kong med 3 (mod 4)

andre primfaktorer.

Siden a er et produkt av kvadratsummer, er a også en
kvadratsum.

Pythagoreiske tripler

Et pythagoreisk trippel (a, b, c) er et trippel av naturlige tall slik at
$a^2 + b^2 = c^2$



Kjenner: $3^2 + 4^2 = 5^2$ $\quad 5^2 + 12^2 = 13^2$ ← primitive pythagoreiske tripler: ingen felles faktorer i a, b, c

$6^2 + 8^2 = 10^2$ $\quad 10^2 + 24^2 = 26^2$

$9^2 + 12^2 = 15^2$ $\quad \vdots$

Maskin for å lage pythagoreiske tripler: Velg naturlige tall p, q, $p > q$. Sett $a = p^2 - q^2$, $b = 2pq$, $c = p^2 + q^2$. Da er (a, b, c) et pythagoreiske trippel.

Sjekk: $a^2 + b^2 = (p^2 - q^2)^2 + (2pq)^2 = p^4 - 2p^2q^2 + q^4 + 4p^2q^2 = p^4 + 2p^2q^2 + q^4$
$= (p^2 + q^2)^2 = c^2$

Lemma: Hvis a, b, c er et primitivt pythagoreisk trippel $a^2 + b^2 = c^2$, så er c et oddetall og én av a og b er også et oddetall, mens det andre er et partall.

Bevis: $a^2 + b^2 = c^2$ siden primitivt, kan ikke alle være partall.

$\mathbb{Z}/(4)$: $\bar{a}^2 + \bar{b}^2 = \bar{c}^2$ ⇒ må få en to 1'ere og én $\bar{0}$.
$\quad$ 0 1, 0 1, 0 1

Teorem: Anta at (a, b, c) er et primitivt pythagoreisk trippel der a er den odde kateten og b er den like kateten. Da finnes det innbyrdes primiske naturlige tall p, q slik at

$$a = p^2 - q^2,\ \boxed{b = 2pq},\ c = p^2 + q^2.$$

$a^2 + b^2 = c^2$

Bevis: Hva må p, q være for at dette skal gjelde?

$a + c = (p^2 - q^2) + (p^2 + q^2) = 2p^2 \Rightarrow p = \sqrt{\frac{c+a}{2}}$
$c - a = (p^2 + q^2) - (p^2 - q^2) = 2q^2 \Rightarrow q = \sqrt{\frac{c-a}{2}}$) heltall

Sjekker den midterste ligningen:
$$2pq = 2\sqrt{\frac{c+a}{2}}\sqrt{\frac{c-a}{2}} = \sqrt{(c+a)(c-a)} = \sqrt{c^2 - a^2} = \sqrt{b^2} = b$$

Vi har
$$\frac{c+a}{2} \cdot \frac{c-a}{2} = \frac{c^2 - a^2}{4} = \frac{b^2}{4} = \frac{(2k)^2}{4} = k^2 \quad (\text{der } b = 2k)$$

Observer nå at $\frac{c+a}{2}$ og $\frac{c-a}{2}$ er innbyrdes primiske fordi en felles faktor ville også ha gått opp $\frac{c+a}{2} + \frac{c-a}{2} = c$ og $\frac{c+a}{2} - \frac{c-a}{2} = a$, noe som er umulig siden c og a er innbyrdes primiske.

Dermed
$$\underbrace{\frac{c+a}{2} \cdot \frac{c-a}{2}}_{} = k^2 = p_1^2 p_2^2 \cdots p_n^2 = (p_1 p_2 \cdots p_r)^2 \underbrace{(p_{r+1} \cdots p_n)^2}_{}$$

$\frac{c+a}{2}$: går opp i $\frac{c+a}{2}$ $\qquad$ $\frac{c-a}{2}$: går opp i $\frac{c-a}{2}$

Dette gir:
$$\frac{c+a}{2} = (p_1 p_2 \cdots p_r)^2 \qquad \frac{c-a}{2} = (p_{r+1} \cdots p_n)^2 \quad \text{kvadrattall.}$$

Siden $p = \sqrt{\frac{c+a}{2}}$, $q = \sqrt{\frac{c-a}{2}}$ er p, q hele tall.

Ser at
$$p = \sqrt{\frac{c+a}{2}} = p_1 p_2 \cdots p_r \qquad q = \sqrt{\frac{c-a}{2}} = p_{r+1} \cdots p_n$$
ingen felles.

Så p, q er innbyrdes primiske.

$x^4 + y^4 = z^4$

$x^n + y^n = z^n \quad n \geq 3$