28/10 - 2013

MAT1140

Litt mer om kvadratiske rester

Husk:

Eulers kriterium: Anta at $p > 2$ er et primtall og at $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$. Da er $\bar{a}$ en kvadratisk rest hvis og bare hvis $\bar{a}^{\frac{p-1}{2}} = \bar{1}$.

Korollar: Hvis p er et primtall, er -1 en kvadratisk rest i $\mathbb{Z}/(p)$ hvis og bare hvis $p = 2$ og $p \equiv 1 \pmod 4$

Bevis: For $p = 2$ er $-\bar{1} = \bar{1} = \bar{1} \cdot \bar{1}$.

For $p > 2$ vet vi at $(-\bar{1})$ er en kvadratisk rest hvis og bare hvis $(-1)^{\frac{p-1}{2}} = 1$. Skriver vi $p = 4m + k$, får vi

$$\frac{p-1}{2} = \frac{4m+k-1}{2} = 2m + \frac{k-1}{2}$$

som er et partall når $k = 1$ og et oddetall når $k = 3$. Altså er $(-1)^{\frac{p-1}{2}} = 1$ hvis og bare hvis $k = 1$, dvs når $p \equiv 1 \pmod 4$.

Vi har tidligere vist at det finnes uendelig mange primtall som er kongruente med 3 mod 4. Nå skal vi vise at det også er uendelig mange som er kongruente med 1.

Teorem: Det finnes uendelig mange primtall som er kongruente med 1 mod 4.

Bevis: Anta at $p_1, p_2, \ldots, p_n$ er primtall som er kongruente med 1 mod 4. Da finnes det et primtall p til som er kongruent med 1 mod 4.
La

$$N = (2p_1p_2 \cdots p_n)^2 + 1$$

Vi ser at ingen p_i deler N. La p være en av primfaktorene i N. Da er

$$(2p_1p_2 \cdots p_n)^2 + 1 \equiv 0 \pmod{p}$$

Dette betyr at $-\bar{1}$ er en kvadratisk rest i $\mathbb{Z}/(p)$ og følgelig er $p = 2$ eller $p \equiv 1 \pmod 4$.
Siden N ikke er delelig med 2, er $p \equiv 1 \pmod 4$

Kvadratsummer

Vi skriver opp primtallene som er kongruente med henholdsvis 1 og 3 mod 4

$\equiv 1$: 5, 13, 17, 29, 37, 41, 53
$\equiv 3$: 3, 7, 11, 19, 23, 31, 43, 47

De første kan alltid skrives som en sum av to kvadrattall:

$5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, ...

mens de andre aldri kan skrives slik.
La oss begynne med den enkle delen

Lemma: Et naturlig tall som er kongruent med 3 mod 4, kan ikke skrives som en sum av to kvadrattall

Bevis: I $\mathbb{Z}/(4)$ er: $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{0}$, $\bar{3}^2 = \bar{1}$, så en sum av to kvadrater kan aldri bli lik $\bar{3}$.

Teorem: Et primtall er en sum av to kvadrattall hvis og bare hvis det er lik 2 eller kongruent med 1 mod 4.

Bevis: Siden $2 = 1^2 + 1^2$, gjenstår det å vise at hvis p er kongruent med 1 mod 4, så er p en sum av to kvadrattall. La K være det største hele tallet mindre enn $\sqrt{p}$ og $\bar{i}^2 = -\bar{1}$ i $\mathbb{Z}/(p)$.

For alle hele tall u, v, $0 \leq u, v \leq K$, setter vi

$$f(u,v) = u + iv$$

Siden det finnes $(K+1)^2 > (\sqrt{p})^2 = p$ slike par og bare p restklasser, må det finnes to par (u,v), (u',v') ~~slik at~~ slik at $f(u,v)$ og $f(u',v')$ tilhører samme restklasse, dvs

$$u+iv \equiv u'+iv' \pmod{p}$$

Setter vi $x = u-u'$ og $y = v'-v$, får vi

$$x \equiv iy \pmod{p}$$

Siden $i^2 = -1$, får vi

$$\bar{x}^2 + \bar{y}^2 = (i\bar{y})^2 + \bar{y}^2 = -\bar{y}^2 + \bar{y}^2 = \bar{0},$$

dvs $x^2 + y^2 = np$ for $n \in \mathbb{N}$. Hvis vi kan vise at $n=1$, er setningen vist.

Siden ikke både x og y er lik null, er $n > 0$. Siden $x = u-u'$, $y = v'-v$ der $0 \le u, v \le \sqrt{p}$, er

$$-\sqrt{p} < x, y < \sqrt{p},$$

så $x^2 + y^2 < p + p = 2p$. Dermed er $n = 1$, og beviset er fullført.

Vi skal nå prøve å beskrive alle tall (ikke nødvendigvis primtall) som kan skrives som en sum av to kvadrattall.

Lemma: Et produkt av kvadratsummer (dvs tall som er summen av to kvadrattall) er selv en kvadratsummer:

Bevis: La $a = (b^2+c^2)(d^2+e^2)$, da er

$$a = (bd+ce)^2 + (be-cd)^2.$$

Ved induksjon gjelder resultatet også for produkter med flere faktorer

---

Lemma: Anta at $a = x^2 + y^2$ der x og y er innbyrdes primisk. Da er a ikke delelig med noe primtall som $p \equiv 3 \pmod 4$

Bevis: Anta at p er et primtall som deler a. Da kan p ikke dele x eller y, for da ville p også dele det andre av disse tallene, og det er ikke mulig siden x og y er innbyrdes primiske

Siden $p \mid a$, er

$$\bar{a} = \bar{x}^2 + \bar{y}^2 = \bar{0} \quad i \quad \mathbb{Z}/(p)$$

Siden $p \nmid y$, er $\bar{y} \neq 0$, og det finnes en $\bar{k}$ slik at $\bar{k}\bar{y} = \bar{x}$. Dermed er

$$\bar{0} = \bar{k}^2\bar{y}^2 + \bar{y}^2 = (\bar{k}^2 + \bar{1})\bar{y}^2$$

Dermed er $\bar{k}^2 = -\bar{1}$, som betyr at $p \not\equiv 3 \pmod 4$.

Lemma: Anta at a er en kvadratsum og at p er et primtall som er kongruent med $3 \pmod 4$. Da deler p a et like antall ganger.

Bevis: La $a = x^2 + y^2$, og la d være største felles divisor for x og y. La $x_0 = \frac{x}{d}$, $y_0 = \frac{y}{d}$. Da har x_0 og y_0 ingen felles faktorer, så $x_0^2 + y_0^2$ er ikke delelig med noe primtall $p \equiv 3 \pmod 4$. Da er

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

p går derfor opp i a like mange ganger som den går opp i d^2, dvs et like antall ganger.

Teorem: Et naturlig tall a er en kvadratsum hvis og bare hvis hvert primtall p som er kongruent med 3 mod 4, går opp et like antall ganger i a.

Bevis: Det gjenstår å vise at hvis alle primtall $p \equiv 3 \pmod 4$ går opp et like antall ganger i a, så er a en kvadratsum. Vi kan skrive

$$a = (p_1 p_2 \cdots p_m)^2 q_1 q_2 \cdots q_k$$

der $p_i \equiv 3 \pmod 4$, $q_j \not\equiv 3 \pmod 4$. Dermed er hver q_j en kvadratsum, og følgelig er $q_1 q_2 \cdots q_k$ en kvadratsum og det samme er $(p_1 p_2 \cdots p_m)^2$ siden kvadrattall regnes som kvadratsummer. Følgelig er a en kvadratsum.