

# Talteori, Föreläsning 9

## Summor av kvadrater

Jan Snellman<sup>1</sup>

<sup>1</sup>Matematiska Institutionen  
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan <http://courses.mai.liu.se/GU/TATA54/>



Jan Snellman

Summa av två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater

- ① **Summa av två kvadrater**  
n ej summa två kvadrater  
Produkter  
p summa två kvadrater
- ② **Summa av fyra kvadrater**

Tre kvadrater ej tillräckligt  
Produkter  
Bevis för fyrkvadratsatsen

- ③ **Antal sätt att skriva som  
summa kvadrater**

Summa av två  
kvadratern ej summa två  
kvadrater

Produkter

p summa två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater

## Teorem

Låt  $n$  vara ett positivt heltal. Om  $n \equiv 3 \pmod{4}$  så kan inte  $n$  skrivas som summan av två kvadrater (på heltal).

## Bevis.

		$x$	0	1	2	3
		$x^2$	0	1	0	1
$y$	$y^2$					
0	0		0	1	0	1
1	1		1	2	1	2
2	0		0	1	0	1
3	1		1	2	1	2



Jan Snellman

Summa av två  
kvadratern ej summa två  
kvadrater

Produkter

p summa två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater

## Lemma

*Om  $m, n$  båda summor av två kvadrater, så ock  $mn$ .*

## Bevis.

Antag  $m = a^2 + b^2$ ,  $n = c^2 + d^2$ . då

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

□

Notera att om vi sätter  $z = a + ib$ ,  $w = c + id$ , så  $|z|^2 = z\bar{z} = a^2 + b^2$ ,  
 $|w|^2 = w\bar{w} = c^2 + d^2$ ,  $|z|^2|w|^2 = (a^2 + b^2)(c^2 + d^2)$ ,  
 $|zw|^2 = (ac + bd)^2 + (ad - bc)^2$ .

Summa av två  
kvadrater

n ej summa två  
kvadrater

Produkter

p summa två  
kvadrater

Summa av fyra  
kvadrater

Antal sätt att  
skriva som  
summa  
kvadrater

## Teorem

*Varje primtal  $p$  med  $p \equiv 1 \pmod{4}$  kan skrivas som en summa av två kvadrater.*

## Bevis.

Kommer senare. □

Notera att  $2 = 1^2 + 1^2$ , och att primtal  $\equiv 3 \pmod{4}$  ej kan skrivas som en summa av två kvadrater.

Summa av två kvadrater

n ej summa två kvadrater

Produkter

p summa två kvadrater

Summa av fyra kvadrater

Antal sätt att skriva som summa kvadrater

## Lemma

Om  $p = 4m + 1$  primtal så finns positiva heltal  $x, y, k$  så att  $x^2 + y^2 = kp$ ,  $k < p$ .

## Bevis.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{2m} = 1 \pmod{p}$$

så  $-1$  är en k.r. mod  $p$ . Alltså finns  $0 < a < p$ ,  $a^2 \equiv -1 \pmod{p}$ . Så  $p \mid (a^2 + 1)$ , så  $a^2 + 1 = a^2 + 1^2 = kp$  för något  $k$ . Eftersom

$$kp = a^2 + 1^2 \leq (p-1)^2 + 1 < p^2$$

följer det att  $k < p$ .



Summa av två  
kvadrater

n ej summa två  
kvadrater

Produkter

p summa två  
kvadrater

Summa av fyra  
kvadrater

Antal sätt att  
skriva som  
summa  
kvadrater

## Bevis (för att $p = 4k + 1$ summma två kvadrater)

- Låt  $m$  vara minsta heltal så att  $mp = x^2 + y^2$ . Vi kommer visa att  $m = 1$ .
- Antag  $m > 1$ , och sätt  $a \equiv x \pmod{m}$ ,  $b \equiv y \pmod{m}$ ,  
 $-m/2 < a \leq m/2$ ,  $-m/2 < b \leq m/2$ . Då  $a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{m}$ .
- Så existerar  $k$  s.a.  $a^2 + b^2 = km$ .
- Vi har att  $(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p^2$ .
- Vi har också att  $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$
- Vidare så  $ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$ ,  $ay - bx \equiv xy - yx \equiv 0 \pmod{m}$ .
- $\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = km^2p/m^2 = kp$  (tryckfel i Rosen)
- Vi kommer att visa att  $0 < k < m$ , en motsägelse (alltså var  $m > 1$  falskt)

Summa av två  
kvadrater

n ej summa två  
kvadrater

Produkter

p summa två  
kvadrater

Summa av fyra  
kvadrater

Antal sätt att  
skriva som  
summa  
kvadrater

## Bevis (fortsättning)

- $a^2 + b^2 = km$ ,  $-m/2 < a \leq m/2$ ,  $-m/2 < b \leq m/2$ .
- Så  $a^2 \leq m^2/4$ ,  $b^2 \leq m^2/4$ .
- Alltså  $0 \leq km = a^2 + b^2 \leq m^2/4 + m^2/4 = m^2/2$ .
- Alltså  $0 \leq k \leq m/2$ . Så  $k < m$ . Återstår visa att  $k > 0$ .
- Men om  $k = 0$  så  $a^2 + b^2 = 0$ , så  $a = b = 0$ , så  $x \equiv y \equiv 0 \pmod{m}$ , så  $m|x$  och  $m|y$ . Vidare  $x^2 + y^2 = mp$ , alltså  $m^2|mp$ , alltså  $m|p$ . Men  $m < p$ , så måste ha  $m = 1$ .



Summa av två kvadrater

$n$  ej summa två kvadrater

Produkter

$p$  summa två kvadrater

Summa av fyra kvadrater

Antal sätt att skriva som summa kvadrater

## Teorem

Heltalet  $n = \prod_p p^{a_p}$  kan skrivas som summa av två kvadrater omm  $a_p$  jämn för alla  $p \equiv 3 \pmod{4}$ .

## Bevis

- 2 summa av två kvadrater
- Varje  $p = 4k + 1$  summa av två kvadrater
- "Tvåkvadratsummighet" bevaras av produkt
- Varje kvadrat är summa av två kvadrater (tex sig själv plus noll i kvadrat)
- Så om  $a_p$  jämn för varje  $p = 4k + 1$ , så  $n$  produkt av heltal som är summa av två kvadrater, alltså summa av två kvadrater

## Proof (contd)

- Antag nu att  $p \equiv 3 \pmod{4}$ ,  $a_p = 2j + 1$ . Kommer att visa att  $n$  ej summa av två kvadrater.
- Antag, för motsägelse, att  $n = x^2 + y^2$
- $d = \gcd(x, y)$ ,  $a = x/d$ ,  $b = y/d$ ,  $m = n/d^2$ ,  $\gcd(a, b) = 1$ ,  $a^2 + b^2 = m$ .
- $a_p = 2j + 1 = v_p(n)$ ,  $k = v_p(d)$ ,  $v_p(m) = 2j + 1 - 2k \geq 0$ , alltså  $\geq 1$ . Så  $p|m$ .
- $\gcd(a, b) = 1$ ,  $m = a^2 + b^2$ ,  $p|m$ , så  $p \nmid a$ .
- Så  $aX \equiv b \pmod{p}$  lösbar, med lösning  $X = z$ , säg.
- $a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1 + z^2) \pmod{p}$
- Men  $a^2 + b^2 = m$ ,  $p|m$ , så  $a^2(1 + z^2) \equiv 0 \pmod{p}$
- $\gcd(a, p) = 1$  så via cancellering  $1 + z^2 \equiv 0 \pmod{p}$ . Så  $z^2 \equiv -1 \pmod{p}$ . Men  $\left(\frac{-1}{p}\right) = -1$  eftersom  $p \equiv 3 \pmod{4}$ . Motsägelse.

Summa av två kvadrater

n ej summa två kvadrater

Produkter

p summa två kvadrater

Summa av fyra kvadrater

Antal sätt att skriva som summa kvadrater

Summa av två  
kvadrater

n ej summa två  
kvadrater

Produkter

p summa två  
kvadrater

Summa av fyra  
kvadrater

Antal sätt att  
skriva som  
summa  
kvadrater

## Exempel

- $2^3 * 3^5 = 1944$  kan ej skrivas som summa av två kvadrater
- $2^3 * 13^3 = 17576$  kan skrivas som summa av två kvadrater, och vi kan tex få en framställning genom

$$2 = 1^2 + 1^2$$

$$2^2 = 2^2 + 0^2$$

$$2^3 = (1 * 2 + 0)^2 + (1 * 0 - 1 * 2)^2 = 2^2 + 2^2$$

$$13 = 2^2 + 3^2$$

$$13^2 = 13^2 + 0^2$$

$$13^3 = (2 * 13 + 3 * 0)^2 + (2 * 0 - 3 * 13)^2 = 26^2 + 39^2$$

$$2^3 * 13^3 = (2 * 26 + 2 * 39)^2 + (2 * 39 - 2 * 26)^2 = 130^2 + 26^2$$

Jan Snellman

## Exempel

7 kan inte skrivas som en summa av tre kvadrater: modulo 8 så antar en kvadrat värdena 0, 1, 4, alltså (antag  $x^2 \geq y^2 \geq z^2$ )

$x^2$	$y^2$	$z^2$	$x^2 + y^2 + z^2$
0	0	0	0
1	0	0	1
4	0	0	4
1	1	0	2
4	1	0	5
4	4	0	0
1	1	1	3
4	1	1	6
4	4	1	1
4	4	4	4

Summa av två kvadrater

Summa av fyra kvadrater

Tre kvadrater ej tillräckligt

Produkter

Bevis för fyrkvadratsatsen

Antal sätt att skriva som summa kvadrater

Jan Snellman

Summa av två  
kvadraterSumma av fyra  
kvadraterTre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrekvadratsatsenAntal sätt att  
skriva som  
summa  
kvadrater**Teorem**

Om  $m, n$  båda summor av fyra kvadrater, så ock  $mn$ .

**Bevis.**

Antag  $m = a^2 + b^2 + c^2 + d^2$ ,  $n = e^2 + f^2 + g^2 + h^2$ . Då

$$mn = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = R^2 + S^2 + T^2 + U^2$$

med

$$R = ae + bf + cg + dh$$

$$S = af - be + ch - dg$$

$$T = ag - bh - ce + df$$

$$U = ah + bg - cf - de$$



Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

**Produkter**

Bevis för  
fyrekvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

Vi kan använda oss av de "Hamiltonska heltalen"

$$\alpha = a + bi + cj + dk$$

$$\beta = e + fi + gj + hk$$

och deras normer (precis som vi använde komplexa tal för två kvadrater).

Kom ihåg:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, \quad jk = i, \quad ki = j,$$

och  $i, j, k$  anti-kommuterar sinsemellan.

Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Lemma

Om  $p > 2$  primtal så finns heltal  $0 < k < p$  så att

$$x^2 + y^2 + z^2 + w^2 = kp$$

har en heltalslösning  $(x, y, z, w)$ .

## Bevis

- Först hittar vi en heltalslösning till  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ , med  $0 \leq x < p/2$ ,  $0 \leq y < p/2$ .
- Sätt  $S = \{j^2 \mid 0 \leq j \leq (p-1)/2\}$ ,  $T = \{-1 - j^2 \mid 0 \leq j \leq (p-1)/2\}$ . Alla elems i  $S$  icke-kongruenta mod  $p$ , ty  $j_1^2 \equiv j_2^2 \pmod{p}$  medför  $0 \equiv j_1^2 - j_2^2 = (j_1 + j_2)(j_1 - j_2) \pmod{p}$ , så  $j_1 \equiv j_2 \pmod{p}$  eller  $j_1 \equiv -j_2 \pmod{p}$ , motsäger  $0 \leq j \leq (p-1)/2$ .
- På samma sätt, alla elems i  $T$  icke-kongruenta mod  $p$ .

Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Bevis (forts)

- $S, T$  disjunkta, båda innehåller  $(p+1)/2$  elems, så  $S \cup T$  har  $p+1$  elems
- Bara  $p$  kongruensklasser mod  $p$
- Duvslagsprincipen ger: finns  $0 \leq x, y \leq (p-1)/2$ ,  $x^2 \in S$ ,  $-1 - y^2 \in T$ ,  
och  $x^2 \equiv -1 - y^2 \pmod{p}$
- Så  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$
- Så  $x^2 + y^2 + 1 = kp$  för något heltal  $k > 0$
- Men  $kp = x^2 + y^2 + 1 \leq 2((p-1)/2)^2 + 1 < p^2$ , så  $k < p$ .



Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrekvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Teorem

Varje primtal  $p$  kan skrivas som  $p = x^2 + y^2 + z^2 + w^2$  med  $x, y, z, w \in \mathbb{Z}$ .

## Bevis (skiss)

- Liknar beviset att  $p = 4k + 1$  summa två kvadrater: använd lemma för att visa att  $mp = x^2 + y^2 + z^2 + w^2$  något  $m$ , låt  $m$  vara minimalt, visa  $m = 1$ .
- Vi gör första halvan, hänvisar till Rosen för slutklämman
- $p = 2$  OK ty  $2 = 1^2 + 1^2 + 0^2 + 0^2$
- $m$  minsta pos så att  $mp = x^2 + y^2 + z^2 + w^2$
- Antag, för motsägelse, att  $m > 1$ .

Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrekvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Proof (contd)

- Kanske är  $m$  jämn?
- Då är ett jämnt antal av  $x, y, z, w$  jämna
- Byt namn och kan anta  $x \equiv y \pmod{2}, z \equiv w \pmod{2}$
- $a = (x - y)/2, b = (x + y)/2, c = (z - w)/2, d = (z + w)/2$  heltal
- $a^2 + b^2 + c^2 + d^2 = \frac{1}{4}((x - y)^2 + (x + y)^2 + (z - w)^2 + (z + w)^2) = \frac{1}{2}(x^2 + y^2 + z^2 + w^2) = \frac{1}{2}mp$
- Motsäger minimaliteten för  $m$
- Kanske att  $m$  är udda?
- Rosen: Nix!

Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrekvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Teorem

*Varje positivt heltal  $n$  kan skrivas som summan av fyra kvadrater.*

## Bevis.

- $n = \prod_p p^{a_p}$
- Varje  $p$  summa av fyra kvadrater
- Enligt produktlemmat, varje  $p^{a_p}$  summa av fyra kvadrater
- Samma lemma ger att  $n$  summa av fyra kvadrater



Summa av två  
kvadrater

Summa av fyra  
kvadrater

Tre kvadrater ej  
tillräckligt

Produkter

Bevis för  
fyrvadratsatsen

Antal sätt att  
skriva som  
summa  
kvadrater

## Exempel

$$3 = 1^2 + 1^2 + 1^2 + 0^2$$

$$5 = 2^2 + 1^2 + 0^2 + 0^2$$

$$4 = 2^2 + 0^2 + 0^2 + 0^2 = 1^2 + 1^2 + 1^2 + 1^2$$

$$15 = 3^2 + 2^2 + 1^2 + 1^2$$

$$20 = 4^2 + 2^2 + 0^2 + 0^2 = 3^2 + 3^2 + 1^2 + 1^2$$

Jan Snellman

Summa av två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater**Teorem**

$$\prod_j \frac{1}{1 - st^{j^2}} = \sum_n t^n \sum_v (c_{n,v} s^v)$$

där  $c_{n,v}$  räknar antalet sätt att skriva  $n$  som en summa av  $v$  kvadrater (svagt växande).

Dessa olika sätt är nedkodade i motsvarande monom  $i$

$$\prod_j \frac{1}{1 - st^{j^2} u_j}$$

Summa av två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater

## Exempel

Koefficienten till  $t^{20}$  i

$$\prod_j (1 - st^{j^2} u_j)^{-1}$$

är

$$s^{20} u_1^{20} + s^{17} u_1^{16} u_2 + s^{14} u_1^{12} u_2^2 + s^{12} u_1^{11} u_3 + s^{11} u_1^8 u_2^3 + \\ s^9 u_1^7 u_2 u_3 + s^8 u_1^4 u_2^4 + s^6 u_1^3 u_2^2 u_3 + s^5 (u_2^5 + u_1^4 u_4) + s^4 u_1^2 u_3^2 + s^2 u_2 u_4$$

så vi ser att

- 20 kan skrivas som en summa av två kvadrater på det unika sättet  $2^2 + 4^2$
- 20 kan skrivas som en summa av fyra kvadrater på det unika sättet  $1^2 + 1^2 + 3^2 + 3^2$
- 20 kan skrivas som en summa av fem kvadrater på precis två sätt:  $2^2 + 2^2 + 2^2 + 2^2 + 2^2$  och  $1^2 + 1^2 + 1^2 + 1^2 + 4^2$

Summa av två  
kvadraterSumma av fyra  
kvadraterAntal sätt att  
skriva som  
summa  
kvadrater

## Exempel

Taylorutvecklingen, i  $t$ , av

$$\prod_j (1 - st^{j^2})^{-1}$$

börjar som

$$\begin{aligned} s^2 t^{20} + s^3 t^{19} + (s^3 + s^2) t^{18} + (s^3 + s^2) t^{17} + \\ st^{16} + s^3 t^{14} + s^2 t^{13} + s^3 t^{12} + s^3 t^{11} + s^2 t^{10} + \\ (s^3 + s) t^9 + s^2 t^8 + s^3 t^6 + s^2 t^5 + st^4 + s^3 t^3 + s^2 t^2 + st + 1 \end{aligned}$$

Vi ser att  $t^3, t^7, t^{15}$  saknas: 3, 7 är primtal kongruenta med 3 mod 4, och 15 innehåller 3 till udda exponent.