

Algebra och talteori

MMGL31

Läroprogrammet,
Göteborgsuniversitet
VT 2010

Samuel Bengmark

Lite om mig

- Doktorerat i Algebraisk geometri
- Lektor vid Matematiska vetenskaper, Chalmers och Göteborgs universitet.
- Drivit Resurscentrum MV
- Programansvarig Informationsteknikprogrammet på Chalmers

Lite om er

På övningen vill jag höra lite om er:

- Namn
- Inriktning och åldersgrupp
- Pendlar
- Personligt

Kursintroduktion

- Kurshemsidan

Okej, då börjar vi

Pytagoreiska trippler

Minns pytagoras sats: $a^2 + b^2 = c^2$

Definition

En trippel (a,b,c) av nollskilda heltal som uppfyller sambandet $a^2 + b^2 = c^2$ kallas en pytagoreisk trippel.

Exempel

$(a,b,c)=(3,4,5)$
 $(a,b,c)=(6,8,10)$

...

Hur hittar man dem?

Man kan leta på måfå men det ger mycket sällan en pytagoreiska trippel

$$1^2 + 2^2 = c^2 \Rightarrow c = \sqrt{5}$$

Ej heltal

Har man väl hittat en, (a,b,c) , finns oändligt många eftersom om d är ett heltal så är även (da,db,dc) en pytagoreisk trippel då

$$(da)^2 + (db)^2 = (dc)^2 \Leftrightarrow d^2(a^2 + b^2) = d^2c^2 \Leftrightarrow a^2 + b^2 = c^2$$

Primitiva pytagoreiska trippler

Definition

En primitiv pytagoreisk trippel (PPT) är en pytagoreisk trippel som uppfyller $\text{SGD}(a,b,c)=1$.

Exempel

Fler exempel från Plimpton322



I bas 60

	width	diagonal
1.	1:59	2:49
2.	56:7	1:20:25
3.	1:16:41	1:50:49
4.	3:31:49	5:09:01
5.	1:05	1:37
6.	5:19	8:01
7.	38:11	59:01
8.	13:19	20:49
9.	8:01	12:49
10.	1:22:41	2:16:01
11.	45	1:15
12.	27:59	48:49
13.	2:41	4:49
14.	29:31	53:49
15.	56	1:46

I decimalform

	width	diagonal
1.	119	169
2.	3367	4825
3.	4601	6649
4.	12709	18541
5.	65	97
6.	319	481
7.	2291	3541
8.	799	1249
9.	481	769
10.	4961	8161
11.	45	75
12.	1679	2929
13.	161	289
14.	1771	3229
15.	56	106

Att finna PPTer

Hur fann babylonierna dessa? Jag vet inte men vi skall ni se två sätt på vilket vi kan finna alla PPTer.

Vi skall börja med ett talteoretiskt sätt och sedan skall vi se ett geometriskt sätt. Båda metoderna använder mycket algebra.

Först lite repetition: delbarhet

Definition

Heltalet m sägs dela heltalet n om det finns ett heltal k så att $n=mk$.
Man skriver $m|n$.

Exempel

$3|12$ eftersom $12=3 \cdot 4$

Mer repetition: kongruens

Definition

- Två heltal x och y sägs vara kongruenta modulo n om $n | x-y$.
- Man skriver $x \equiv y \pmod{n}$ eller $x \equiv_n y$
- Mängden av alla kongruensklasser utgör en mängd som vi betecknar $\mathbb{Z}_n$.

Obs: Varje tal är kongruent med något av talen $0, 1, \dots, n-1$ modulo n , dvs

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}.$$

Exempel

$$1 \equiv_7 8$$

$$0^2 \equiv_2 0, 1^2 \equiv_2 1 \text{ (paritet bevaras vid kvadrering)}$$

$$0^2 \equiv_4 0, 1^2 \equiv_4 1, 2^2 \equiv_4 0, 3^2 \equiv_4 1 \text{ (inga kvadrater } \equiv_4 2 \text{ eller } 3)$$

Talteoretisk metod

Vi söker bara primitiva pytagoreiska tripler

$$\text{Betrakta } a^2 + b^2 = c^2$$

Om

- **a och b jämna:** är c jämn, dvs ej primitiv
- **a och b udda:** betrakta ekvationen mod 4. I VL är varje term 1 eftersom kvadrat av udda är 1 mod 4. Detta ger att VL $1+1 \equiv_4 2$. Men HL är kvadrat och sådana kan inte bli 2 mod 4.
- **a udda, b jämn:** ger c udda.

Slutsats: a och c udda, b jämn.

Talteoretisk metod

Antag att (a,b,c) är en PPT.

Flyttar över b i $a^2 + b^2 = c^2$ och får

$$\begin{cases} a^2 = c^2 - b^2 = (c+b)(c-b) = xy \\ c+b = x \\ c-b = y \end{cases}$$

Påstående

1. $\text{SGD}(x,y)=1$.
2. x och y är kvadrater

Bevis för påstående 1: $\text{SGD}(x,y)=1$

Antag att d delar x och y . Då måste d även dela deras summa, differens och produkt dvs

$$\begin{cases} d | x+y \Leftrightarrow d | (c+b) + (c-b) \Leftrightarrow d | 2c \\ d | x-y \Leftrightarrow d | (c+b) - (c-b) \Leftrightarrow d | 2b \\ d | (x+y)(x-y) \Leftrightarrow d | a^2 \end{cases}$$

Eftersom b och c inte har någon gemensam delare (de är relativt prima) så ger de två översta att $d|2$.

Den nedre ger att d är udda eftersom a är udda.

Slutsats: $d=1$, dvs enda delaren till x och y är 1.

Bevis för påstående 2: x och y är kvadrater

Minns att om p primtal gäller att

$$p|nm \Rightarrow p|n \text{ eller } p|m$$

- Tag en godtycklig primtalsfaktor p i xy . Då kommer p dela den ena faktorn, säg x . Den kan då inte dela y (eftersom x och y är relativt prima).
- Eftersom $p|a^2$ måste $p|a$, dvs $p^2|a^2=xy$.

Slutsats varje primtalsfaktor förekommer ett jämnt antal gånger i x , dvs x är en kvadrat. Pss med y .

Sätter nu $\begin{cases} x = s^2 \\ y = t^2 \end{cases}$ där $s > t \geq 1$, dvs

$$\begin{cases} a^2 = c^2 - b^2 = (c+b)(c-b) = xy = s^2 t^2 \\ c+b = x = s^2 \\ c-b = y = t^2 \end{cases}$$

Löser nu ut a,b och c

$$\begin{cases} a = \sqrt{xy} = st \\ b = \frac{x-y}{2} = \frac{s^2-t^2}{2} \\ c = \frac{x+y}{2} = \frac{s^2+t^2}{2} \end{cases}$$

Slutsats

$$(a, b, c) = (st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$$

Där s och t är udda heltal som uppfyller $s > t \geq 1$ ger alla primitiva pytagoreiska tripler.

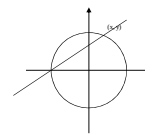
Geometrisk metod

Ser att $a^2 + b^2 = c^2 \Leftrightarrow \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$

Söker nu rationella punkter på cirkel $x^2 + y^2 = 1$

Exempel

...



Linjens ekvation

- $y = kx + m$.
- Vår linje passerar $(-1, 0)$ ger att $0 = k(-1) + m \Leftrightarrow m = k$
dvs $y = k(x+1)$

Skärningspunkt mellan linje och cirkel

Ekvationsystem

$$\begin{cases} y = k(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

Ger

$$1 = x^2 + (k(x+1))^2 = x^2 + k^2(x^2 + 2x + 1) = (k^2 + 1)x^2 + 2k^2x + k^2$$

dvs en andragradsekvation i x.

Löses med polynomdivision

dvs

$$(k^2 + 1)x^2 + 2k^2x + k^2 - 1 = (x+1) \cdot ((k^2 + 1)x + k^2 - 1)$$

För den andra skärningspunkten gäller att

$$\begin{cases} x = -\frac{k^2 - 1}{k^2 + 1} \\ y = k(x+1) = k\left(-\frac{k^2 - 1}{k^2 + 1} + 1\right) = \frac{2k}{k^2 + 1} \end{cases}$$

Får nu PPTer

Givet rationell lutning $k = \frac{u}{v}$

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{1-k^2}{1+k^2}, \frac{2k}{1+k^2}\right) = \left(\frac{1-\left(\frac{u}{v}\right)^2}{1+\left(\frac{u}{v}\right)^2}, \frac{2\frac{u}{v}}{1+\left(\frac{u}{v}\right)^2}\right) = \left(-\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right)$$

$$\begin{cases} a = v^2 - u^2 \\ b = 2uv \\ c = v^2 + u^2 \end{cases}$$

Övning

Uppgifterna inte alltid fullständigt lösbara,
tex i 1.4 är frågan:

”Tror du att ...”