Talteori, Föreläsning 8

Pytagoriska taltripplar, Fermats förmodan

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

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

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Sammanfattning

Pytagoriska taltripplar

- Definition, primitiva taltripplar
- Klassifikation
- Rationell parametrisering

Fermats förmodan/sats

- Nedstigning

Sammanfattning

Pytagoriska taltripplar
- Definition, primitiva taltripplar
- Klassifikation
- Rationell parametrisering

Fermats förmodan/sats
- Nedstigning

Definition

- Heltalen x, y, z utgör en Pytagorisk trippel om det finns en rätvinklig triangel med dessa sidlängder, dvs om
$$x^2 + y^2 = z^2$$
- PTn (x, y, z) är primitiv om $\gcd(x, y, z) = 1$, i.e. det finns inget primtal p som samtidigt delar x, y och z

Exempel

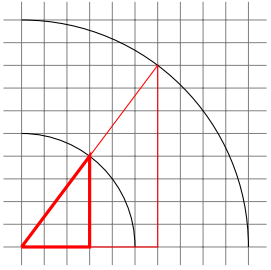
$(3, 4, 5)$ är en PPT, $(6, 8, 10)$ PT ej PPT.

Skalning

Lemma

- *Om* (x, y, z) *är en PT och* $d \in \mathbb{Z}$*, så är* (dx, dy, xz) *en PT*
- *Om* (x, y, z) *är en PT,* $\gcd(x, y, z) = d$*, så är* $(x/d, y/d, z/d)$ *en PPT*

Det räcker alltså att hitta alla PPT för att förstå alla PT. Vi kan också begränsa oss till PPT där x, y, z är positiva.



Lemma

Om (x, y, z) *är en PPT så*

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$$

Bevis.

Antag, får att få en motsägelse, att $\gcd(x, y) > 1$, så finns primtal p som delar x och y. Då $p^2|x^2$, $p^2|y^2$, så $p^2|x^2 + y^2$ varför $p^2|z^2$, och det följer att $p|z$. Så p delar x, y, z, vilket motsäger att $\gcd(x, y, z) = 1$. □

Lemma

Om (x, y, z) *är en PPT så*

$$x \not\equiv y \mod 2$$

Bevis.

Tidigare lemmat visar att x och y inte båda kan vara jämna.
Skulle både x och y vara udda, så modulo 4

x	x^2	y	y^2	z	z^2
1	1	1	1		2
-1	1	1	1		2
1	1	-1	1		2
-1	1	-1	1		2

Men ingenting i kvadrat är kongruent med 2 modulo 4. □

Teorem

Låt r, s, t vara positiva heltal. Om $\gcd(r, s) = 1$ och $rs = t^2$ så finns positiva heltal m, n så att

$$r = m^2, \qquad s = n^2$$

Bevis.

Eftersom $\gcd(r, s) = 1$, så gäller för varje primtal p att $v_p(r)v_p(s) = 0$. Vidare, $v_p(t^2) = 2d_p$ för något heltal d_p. Men $rs = t^2$ så $2d_p = v_p(r) + v_p(s)$, varför det antingen gäller att

- $v_p(r) = v_p(s) = d_p = 0$,
- $v_p(r) = 2d_p > 0$, $v_p(s) = 0$, eller att
- $v_p(s) = 2d_p > 0$, $v_p(r) = 0$.

Sätt

$$m = \prod_{\{p \mid v_p(r) > 0\}} p^{d_p}, \qquad n = \prod_{\{p \mid v_p(s) > 0\}} p^{d_p}$$

□

Exempel

$r = 2^4 * 3^8 * 11^4$, $s = 5^4 * 7^8 * 13^2$,
$rs = 2^4 * 3^8 * 5^4 * 7^8 * 11^4 * 13^2 = (2 * 3^4 * 11^2)^2 * (5^2 * 7^4 * 13)^2$

Teorem

(x, y, z) är en PPT med y jämn omm det finns heltal $0 < n < m$, $m \not\equiv n \mod 2$, så att

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

Bevis

- Antag (x, y, z) är en PPT. Kan anta y jämn, x, z udda.
- Så $z + x$, $z - x$ jämna. Sätt $r = (z + x)/2$, $s = (z - x)/2$. Då $r + s = z$, $r - s = x$.
- $y^2 = z^2 - x^2 = (z + x)(z - x)$, varför $(y/2)^2 = rs$.

Bevis (forts)

- Sätt $d = \gcd(r, s)$, då $d|r$, $d|s$, så $d|z$, $d|x$. Men $\gcd(x, z) = 1$, så $d = 1$.
- Tidagare sats: finns m, n med $r = m^2$, $s = n^2$.
-

$$x = r - s = m^2 - n^2$$
$$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn$$
$$z = r + s = m^2 + n^2$$

- Om $p|m$, $p|n$ så $p|m^2 - n^2$, $p|2mn$, $p|m^2 + n^2$. Men $\gcd(x, y, z) = 1$. Alltså $\gcd(m, n) = 1$.
- m, n kan inte ha samma paritet.

Bevis (forts)

- Antag $0 < n < m$, $\gcd(m, n) = 1$, m, n olika paritet.
- Sätt

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

- Vill visa att (x, y, z) PPT.
- Kollar att $x^2 + y^2 = z^2$
- $d = \gcd(x, y, z)$. Antag finns primtal p, $p|d$.
- x udda, så $p > 2$.
- $p|x$, $p|y$, $p|z$, så $p|z + x$, så $p|2m^2$. Alltså $p|m$.
- På samma sätt, $p|n$.
- Motsäger $\gcd(m, n) = 1$, så $d = 1$.

Teorem

Låt $p(x, y, z) \in \mathbb{Z}[x, y, z]$ vara ett homogent polynom. Då svarar heltalstripplar $(a, b, c) \in \mathbb{Z}^3$ med $p(a, b, c) = 0$, $c \neq 0$, mot rationella punkter $(a/c, b/c)$ på kurvan $C \subseteq \mathbb{A}^2$, där C är nollställemängden till polynomet $\tilde{p}(x, y) = p(x, y, 1)$

Bevis.

Om $p(a, b, c) = 0$, så $\tilde{p}(a/c, b/c) = 0$, eftersom polynomet är homogent.
Omvänt, om $\tilde{p}(r, s) = 0$ så $p(rd, sd, d) = 0$ för alla d. □

Speciellt, om $a^2 + b^2 = c^2$, så är $(a/c, b/c)$ en rationell punkt på enhetscirkeln $x^2 + y^2 = 1$. Omvänt så ger varje rationell punkt $(x/d, y/d)$ på enhetscirkeln en PT (xd, yd, d) med $(xd)^2 + (yd)^2 = d^2(x^2 + y^2) = d^2$.

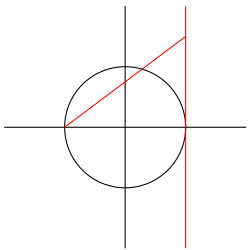
Så, att hitta PT är samma sak som att hitta rationella punkter på enhetscirkeln. Men detta är enkelt:

Teorem

Parametriseringen

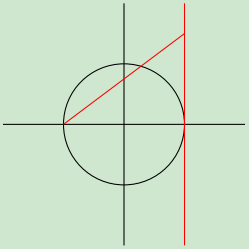
$$\mathbb{R} \ni t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \in S$$

avbildar tallinjen bijektivt på enhetscirkeln minus punkten $(-1, 0)$*, och denna avbildning ger en bijektion från rationella punker till rationella punkter*



Linjen $y = t(x+1)$ skär enhetscirkeln i $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ (och tangentlinjen i $(1, 2t)$).

Exempel



Tag $t = 7/11$. Den rationella punkten

$$\left(\frac{1-(\frac{7}{11})^2}{1+(\frac{7}{11})^2}, \frac{2(\frac{7}{11})^2}{1+(\frac{7}{11})^2}\right) = (\frac{36}{85}, \frac{77}{85})$$

ger PPT

$$(36, 77, 85)$$

Exempel

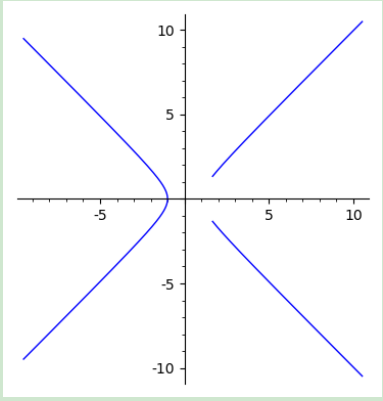
Den rationella parametrisering

$$\mathbb{R} \ni t \mapsto \left(\frac{t^2+1}{t^2-1}, \frac{2t}{t^2-1} \right)$$

av hyperbeln

$$x^2 - y^2 = 1$$

tillåter oss att hitta alla rationella punkter



Exempel

För att hitta alla heltalslösningar till

$$x^2 + 3y^2 = z^2,$$

så tar vi fram alla rationella punkter på

$$x^2 + 3y^2 = 1$$

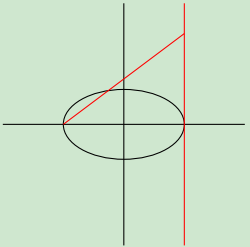
mha den rationella parametriseringen

$$\mathbb{R} \ni t \mapsto \left(\frac{1 - 3t^2}{1 + 3t^2}, \frac{2t}{1 + 3t^2} \right)$$

och sluter oss till att de primitiva lösningarna är

$$x = \frac{m^2 - 3n^2}{2}$$
$$y = mn$$
$$z = \frac{m^2 + 3n^2}{2}$$

med $m > \sqrt{3}n$.



Fermats förmodan

- n positiv heltal
- Studera

$$x^n + y^n + z^n = 0, \qquad x, y, z \in \mathbb{Z}, (x, y, z) \neq (0, 0, 0) \tag{1}$$

- Ekvivalent: $x, y, z \in \mathbb{N}$
- Ekvivalent: $x^n + y^n = z^n$
- Ekvivalent: $x^n + y^n = 1$, $x, y \in \mathbb{Q}$
- $n = 1$: trivialt, $n = 2$: PT
- Om $n = ab$ så

$$0 = x^n + y + z^n = (x^a)^b + (y^a)^b + (z^a)^b$$

så lösn för sammansatt n ger lösn för faktor

Teorem (Fermats förmodan)

För $n \geq 3$ så har ekvationen $x^n + y^n = z^n$ inga icke-triviala heltalslösningar.

- Fermat 1637: marginalanteckning *Arithmetica* av Diofantes:
  It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain
- Bevisade fallet $n = 4$ med "oändlig nedstigning"
- Euler: $n = 3$

Teorem (Fermat)

Ekvationen

$$x^4 - y^4 = z^2$$

har inga icke-triviala heltalslösningar.

Bevis

- Kan anta $\gcd(x, y) = 1$
- $(x^2 + y^2)(x^2 - y^2) = z^2$
- Om $d|x^2 + y^2$ och $d|x^2 - y^2$ så $d|2x^2$ och $d|2y^2$, varför $\gcd(x^2 + y^2, x^2 - y^2) \in \{1, 2\}$.

Bevis (forts)

- Antag $\gcd(x^2+y^2, x^2-y^2) = 1$. Eftersom $(x^2+y^2)(x^2-y^2) = z^2$ så

$$x^2 + y^2 = s^2$$
$$x^2 - y^2 = t^2$$

- s, t relativt prima, båda udda, ty $s^2 + t^2 = 2x^2$.
-

$$u = (s+t)/2$$
$$v = (s-t)/2$$

- u, v relativt prima. Eftersom $y^2 = 2uv$, så är precis en av dem jämn, säg u jämn.
- $u = 2m^2$, $v = k^2$
- $(s^2+t^2)/2 = u^2 + v^2 = x^2$, (u, v, x) PPT.

Bevis (forts)

- Så

$$u = 2de$$
$$v = d^2 - e^2$$
$$x = d^2 + e^2$$

- $u = 2m^2 = 2de$, $\gcd(d, e) = 1$, så $d = g^2$, $e = h^2$.
- Så $v = d^2 - e^2 = g^4 - h^4 = k^2$
- Men (g, h, k) annan lösning till $x^4 - y^4 = z^2$; denna lösning strikt mindre un ursprungslösningen (x, y, z) så tillvida att $g < x$.

Bevis (forts)

- Antag istället att $\gcd(x^2+y^2, x^2-y^2) = 2$. Då x, y udda, z jämn.
- (y^2, z, x) PPT, så

$$z = 2de$$
$$y^2 = d^2 - e^2$$
$$x^2 = d^2 + e^2$$

  med $d > e > 0$
- Så

$$x^2y^2 = d^4 - e^4$$

  och (d, e, xy) lösn, strikt mindre än ursprungslösn.
- Så varje icke-trivial lösning ger upphov till strikt mindre annan icke-triv lösning; omöjligt ty finns endast ändligt många strikt mindre lösn!

Teorem (Fermat)

Ingen rätvinklig triangle vars alla sidlängder är heltal kan ha en area som är kvadraten på ett helta.

Bevis

- Antag (u, v, w) PT, $u^2 + v^2 = w^2$, arean av triangeln $uv/2$
- Antag, för att få motsägelse, att $uv/2 = s^2$
- Då

$$2uv = 4s^2$$
$$-2uv = -4s^2$$

så

$$u^2 + 2uv - v^2 = w^2 + 4s^2$$
$$u^2 - 2uv - v^2 = w^2 - 4s^2$$

Bevis (forts)

- Så

$$(u+v)^2 = w^2 + 4s^2$$
$$(u-v)^2 = w^2 - 4s^2$$

- Alltså

$$(u^2 - v^2)^2 = (u+v)^2(u-v)^2 = (w^2 + 4s^2)(w^2 - 4s^2) = w^2 - 2^4 s^4$$

- Men vi visade just att $x^4 - y^4 = z^2$ saknar icke-triviala heltalslösningar!