Number Theory, Lecture 8

Pythagorean triples, Fermat's conjecture

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

Summary

Definition

- The integers x, y, z constitue a Pythagorean triple if there is a right-angled triangle with these side lengths; i.e. if
$$x^2 + y^2 = z^2$$
- The Pythagorean triple (x, y, z) is primitive if $\gcd(x, y, z) = 1$, i.e. if there does not exist exist a prime p dividing all of x, y, and z

Example

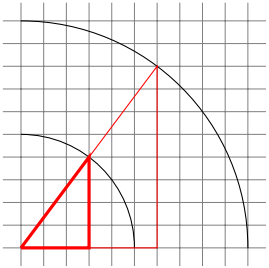
$(3, 4, 5)$ is a primitive Pythagorean triple, $(6, 8, 10)$ is not primitive.

Scaling

Lemma

- *If* (x, y, z) *is a PT and* $d \in \mathbb{Z}$*, then* (dx, dy, xz) *is a PT*
- *If* (x, y, z) *is a PT,* $\gcd(x, y, z) = d$*, then* $(x/d, y/d, z/d)$ *is a PPT*

So it is enough to enumerate all PPT.



Lemma

If (x, y, z) is a PPT then

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

Proof.

Suppose, towards a contradiction, that $\gcd(x, y) > 1$, so that there is some prime p dividing x and y. Then $p^2|x^2$, $p^2|y^2$, so $p^2|x^2 + y^2$ hence $p^2|z^2$, whence $p|z$. So p divides x, y, z, contradicting that $\gcd(x, y, z) = 1$. □

Lemma

If (x, y, z) is a PPT, then

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

Proof.

By the previous lemma it is impossible for both x and y to be even. Should both x and y both be odd, then 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

But nothing squares to 2. □

Theorem

Let r, s, t be positive integers. If $\gcd(r,s) = 1$ and $rs = t^2$ then there exists positive integers m, n such that

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

Proof.

Since $\gcd(r,s) = 1$, for each prime p it holds that $v_p(r)v_p(s) = 0$. Furthermore, $v_p(t^2) = 2d_p$ for some integer d_p. But $rs = t^2$ so $2d_p = v_p(r) + v_p(s)$, whence either

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

Put

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

□

Example

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

Theorem

(x, y, z) is a PPT with y even if and only if there exists integers $0 < n < m$, $m \not\equiv n \mod 2$, such that

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

Proof

- Assume (x, y, z) is a PPT. May assume y even, x odd, z odd.
- So $z + x$, $z - x$ both even. Put $r = (z + x)/2$, $s = (z - x)/2$. Then $r + s = z$, $r - s = x$.
- $y^2 = z^2 - x^2 = (z + x)(z - x)$, hence $(y/2)^2 = rs$.

Proof (contd)

- $d = \gcd(r, s)$, then $d|r$, $d|s$, so $d|z$, $d|x$. But $\gcd(x, z) = 1$, so $d = 1$.
- Previous thm: exists m, n with $r = m^2$, $s = n^2$.
- $$x = r - s = m^2 - n^2$$
  $$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn$$
  $$z = r + s = m^2 + n^2$$
- If $p|m$, $p|n$ then $p|m^2 - n^2$, $p|2mn$, $p|m^2 + n^2$. But $\gcd(x, y, z) = 1$. Hence $\gcd(m, n) = 1$.
- m, n can not both be odd, nor can both be even

Proof (contd)

- Now suppose $0 < n < m$, $\gcd(m, n) = 1$, m, n have different parity.
- Put

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

- Want to show (x, y, z) PPT.
- Check $x^2 + y^2 = z^2$
- $d = \gcd(x, y, z)$. Suppose exists prime p, $p|d$.
- x odd, so $p > 2$.
- $p|x$, $p|y$, $p|z$, so $p|z + x$, so $p|2m^2$. Hence $p|m$.
- Similarly, $p|n$.
- This contradicts $\gcd(m, n) = 1$, so $d = 1$.

Theorem

Let $p(x,y,z) \in \mathbb{Z}[x,y,z]$ be a homogeneous polynomial. Then integer triples $(a,b,c) \in \mathbb{Z}^3$ with $p(a,b,c) = 0$, $c \neq 0$, correspond to rational points on the affine curve $C \subseteq \mathbb{A}^2$, where C is the zeroset of the polynomial $\tilde{p}(x,y) = p(x,y,1)$

Proof.

If $p(a,b,c) = 0$, then $\tilde{p}(a/c, b/c) = 0$, by homogeneity. Conversely, if $\tilde{p}(r,s) = 0$ then $p(rd, sd, d) = 0$ for all d. □

In particular, if $a^2 + b^2 = c^2$, then $(a/c, b/c)$ lie on the unit circle $x^2 + y^2 = 1$. Conversely, any (x,y) on the unit circle scale to (xd, yd, d) with $(xd)^2 + (yd)^2 = d^2(x^2 + y^2) = d^2$.

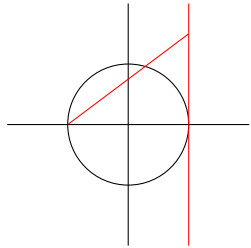
So, finding PT is the same thing as finding rational points on the unit circle. However:

Theorem

The parametrization

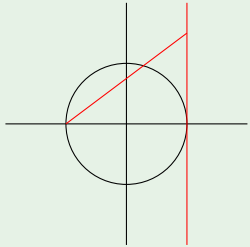
$$\mathbb{R} \ni t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \in S$$

maps the real line bijectively to the unit circle minus the point $(-1, 0)$*, and this map, and its inverse, preserves rationality.*



Line: $y = t(x+1)$ intersect unit circle at $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ and tangent line at $(1, 2t)$.

Example



Take $t = 7/11$. Then the rational point

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

yields the PPT

$$(36, 77, 85)$$

Example

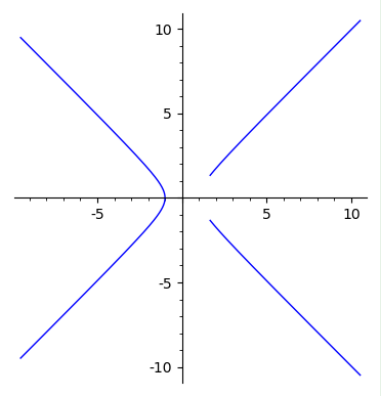
The rational parametrization

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

of the hyperbola

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

allows us to find all rational points.



Example

To find all integer solutions to

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

we find all rational points on

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

using the rational parametrization

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

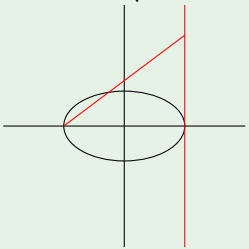
and conclude that the primitive solutions are

$$x = \frac{m^2 - 3n^2}{2}$$

$$y = mn$$

$$z = \frac{m^2 + 3n^2}{2}$$

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



Fermat's conjecture

- n positive integer
- Study

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

- Equivalent: $x, y, z \in \mathbb{N}$
- Equivalent: $x^n + y^n = z^n$
- Equivalent: $x^n + y^n = 1$, $x, y \in \mathbb{Q}$
- $n = 1$: trivial, $n = 2$: Pythagorean triples
- If $n = ab$ then

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

so any soln for composite n gives soln for the factors

Theorem (Fermat's conjecture)

For $n \geq 3$, the equation $x^n + y^n = z^n$ has no non-trivial integer solutions.

- Fermat 1637: marginal note in *Arithmetica* by Diophantus:

  > *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*

- Proved the case $n = 4$ by infinite descent
- Euler: $n = 3$

Theorem (Fermat)

The equation

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

have no non-trivial integer solutions.

Proof

- May assume $\gcd(x, y) = 1$
- $x^2 + y^2)(x^2 - y^2) = z^2$
- If $d|x^2 + y^2$ and $d|x^2 - y^2$ then $d|2x^2$ and $d|2y^2$, so $\gcd(x^2 + y^2, x^2 - y^2)$ is either 1 or 2.

Proof (contd)

- Suppose $\gcd(x^2+y^2, x^2-y^2) = 1$. Then since their product is z^2,

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

- s, t relatively prime, and both odd, since $s^2 + t^2 = 2x^2$.
-

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

- u, v relatively prime. Since $y^2 = 2uv$, precisely one of them even (suppose u).
- $u = 2m^2$, $v = k^2$
- $(s^2+t^2)/2 = u^2 + v^2 = x^2$, (u, v, x) PPT.

Proof (contd)

- So

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

- $u = 2m^2 = 2de$, $\gcd(d, e) = 1$, so $d = g^2$, $e = h^2$.
- So $v = d^2 - e^2 = g^4 - h^4 = k^2$
- But (g, h, k) another solution to $x^4 - y^4 = z^2$; this solution is strictly smaller than original (x, y, z) in that $g < x$.

Proof (contd)

- Suppose instead that $\gcd(x^2+y^2, x^2-y^2) = 2$. Then x, y odd, z even.
- (y^2, z, x) PPT, so

$$\begin{aligned} z &= 2de \\ y^2 &= d^2 - e^2 \\ x^2 &= d^2 + e^2 \end{aligned}$$

  with $d > e > 0$
- So

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

  and (d, e, xy) another, strictly smaller soln to original eqn.
- So, any non-trivial soln yields another, strictly smaller non-trivial soln; impossible since there can be only finitely many strictly smaller.

Theorem (Fermat's right triangle thm)

No right triangle with integer sides can have an area which is a square (of an integer).

Proof

- Suppose (u, v, w) PT, $u^2 + v^2 = w^2$, area of triangle $uv/2$
- Suppose, towards a contradiction, that $uv/2 = s^2$
- Then

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

hence

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

Proof (contd)

- So

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

- Thus

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

- But we have proved that $x^4 - y^4 = z^2$ have no non-trivial integer soln!