Pythagorean Triples

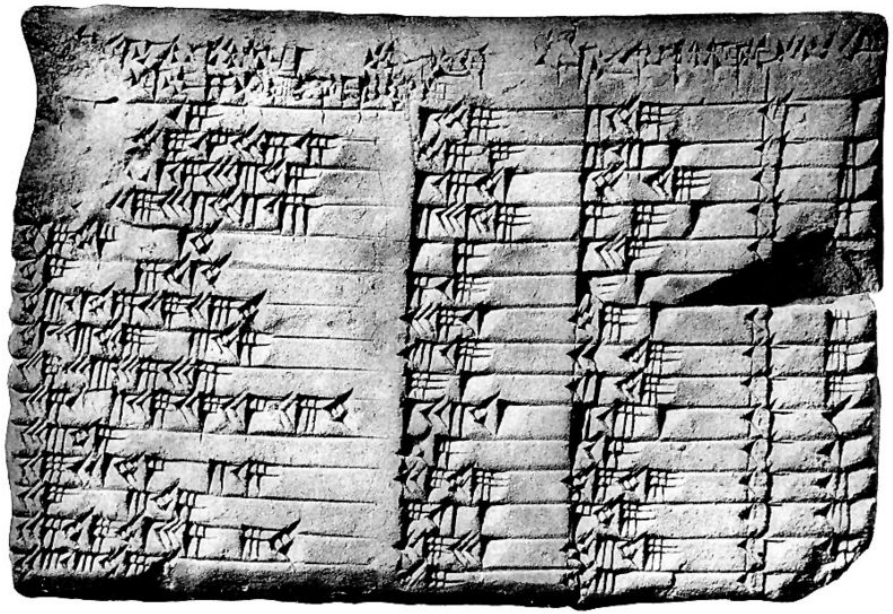
Keith Conrad
University of Connecticut

August 4, 2008

Introduction

We seek positive integers a, b, and c such that

$$a^2 + b^2 = c^2.$$



Plimpton 322

Babylonian table of Pythagorean triples (1800 BC). Eleventh row is $(3, 4, 5)$.

Reduction Step

$$a^2 + b^2 = c^2$$

a	3	5	7	8	9	115
b	4	12	24	15	40	252
c	5	13	25	17	41	277

Examples of Pythagorean Triples

If $d|a$ and $d|b$ then $d^2|c^2$, so $d|c$. Similarly, if $d|a$ and $d|c$ then $d|b$, and if $d|b$ and $d|c$ then $d|a$. Therefore $(a, b) = (a, b, c)$. Writing $a = da'$, $b = db'$, and $c = dc'$,

$$a^2 + b^2 = c^2 \Longrightarrow a'^2 + b'^2 = c'^2.$$

From now on we focus on *primitive* triples: $(a, b) = 1$.

Classification

$$a^2 + b^2 = c^2, \quad (a, b) = 1.$$

Certainly a and b are not both even. Also they are not both odd: otherwise, $c^2 = a^2 + b^2 \equiv 1 + 1 \equiv 2 \bmod 4$, which is impossible. So one of a or b is even and the other is odd. Then $c^2 = a^2 + b^2$ is odd, so c is odd. Our *convention*: take b even.

Theorem

The primitive Pythagorean triples (a, b, c) where b is even are given by

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

where $u > v > 0$, $(u, v) = 1$, and $u \not\equiv v \bmod 2$.

For u and v in $\mathbf{Z}^+$, need $u > v$ so that $a > 0$. The conditions $(u, v) = 1$ and $u \not\equiv v \bmod 2$ are forced by primitivity.

Classification

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

$$u > v > 0, \quad (u, v) = 1, \quad u \not\equiv v \bmod 2$$

u	2	3	3	4	4	5	14
v	1	1	2	3	1	4	9
a	3	8	5	7	15	9	115
b	4	6	12	24	8	40	252
c	5	10	13	25	17	41	277

Which u and v give the triple $(a, b, c) = (190281, 78320, 205769)$?

Classification

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

$$u > v > 0, \quad (u, v) = 1, \quad u \not\equiv v \bmod 2$$

Can solve for u^2 and v^2:

$$u^2 = \frac{a+c}{2}, \quad v^2 = \frac{c-a}{2}.$$

For $(a, b, c) = (190281, 78320, 205769)$,

$$\frac{a+c}{2} = 198025 = 445^2, \quad \frac{c-a}{2} = 7744 = 88^2.$$

So $u = 445$ and $v = 88$.

Primitive Triples of Nonzero Integers

Theorem

Triples (a, b, c) of nonzero integers where $a^2 + b^2 = c^2$, $(a, b) = 1$, b is even, and $c > 0$, are given by

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

where $u, v \in \mathbf{Z} - \{0\}$, $(u, v) = 1$, and $u \not\equiv v \bmod 2$.

Why? Suppose $a > 0$, $b > 0$, and $c > 0$, so the classification says

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

$$u > v > 0, \quad (u, v) = 1, \quad u \not\equiv v \bmod 2.$$

In terms of this u and v, how do the parametric formulas apply to $(a, -b, c)$? To $(-a, b, c)$? To $(-a, -b, c)$? To $(a, b, -c)$?

Outline

- Classify primitive Pythagorean triples by unique factorization in $\mathbf{Z}$.
- Classify primitive Pythagorean triples by unique factorization in $\mathbf{Z}[i]$.
- Classify primitive Pythagorean triples by analytic geometry.
- See additional use of each method of proof.

First proof: unique factorization in Z, I

$$a^2 + b^2 = c^2 \Longrightarrow b^2 = c^2 - a^2 = (c+a)(c-a).$$

Both $c+a$ and $c-a$ are positive and even. What's their gcd? If $d|(c+a)$ and $d|(c-a)$ then $d|2c$ and $d|2a$, so $d|2$ because $(a,c)=1$. Since $c+a$ and $c-a$ are even, $(c+a, c-a) = 2$. So

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2},$$

with factors relatively prime.

Theorem

If $xy = \square$ in $\mathbf{Z}^+$ and $(x,y)=1$ then $x = \square$ and $y = \square$.

So $(c+a)/2 = u^2$ and $(c-a)/2 = v^2$ with $u, v \in \mathbf{Z}^+$. Solving, $c = u^2 + v^2$ and $a = u^2 - v^2$; $b^2 = (c+a)(c-a) = (2uv)^2$.

First proof: unique factorization in Z, II

Let's try a different subtraction:

$$a^2 + b^2 = c^2 \Longrightarrow a^2 = c^2 - b^2 = (c+b)(c-b).$$

Both $c+b$ and $c-b$ are positive and odd. What's their gcd? If $d|(c+b)$ and $d|(c-b)$ then $d|2c$ and $d|2b$, so $d|2$. Since $c+b$ and $c-b$ are odd, $(c+b, c-b) = 1$.
Then $c+b = k^2$ and $c-b = \ell^2$ where k and ℓ are in $\mathbf{Z}^+$ and odd. Must have $(k,\ell) = 1$. Adding and subtracting,

$$c = \frac{k^2+\ell^2}{2}, \quad b = \frac{k^2-\ell^2}{2}.$$

Then $a^2 = (c+b)(c-b) = k^2\ell^2$, so $a = k\ell$. We expect that $a = u^2 - v^2$, and so on. Since $u^2 - v^2 = (u+v)(u-v)$, try to get $k = u+v$ and $\ell = u-v$. Define

$$u = \frac{k+\ell}{2}, \quad v = \frac{k-\ell}{2}.$$

Another parametrization

Theorem

The primitive Pythagorean triples (a, b, c) where b is even are given by

$$a = k\ell, \quad b = \frac{k^2 - \ell^2}{2}, \quad c = \frac{k^2 + \ell^2}{2},$$

where $k > \ell > 0$, $(k, \ell) = 1$, and k and ℓ are both odd.

k	3	5	7	5	9	23
ℓ	1	1	1	3	1	5
a	3	5	7	15	9	115
b	4	12	24	8	40	252
c	5	13	25	17	41	277

Second proof: unique factorization in $\mathbf{Z}[i]$

Write

$$c^2 = a^2 + b^2 = (a + bi)(a - bi).$$

Suppose $\delta|(a + bi)$ and $\delta|(a - bi)$ in $\mathbf{Z}[i]$. Taking the norm, $\mathrm{N}(\delta)$ divides $a^2 + b^2 = c^2$, which is odd, so $\mathrm{N}(\delta)$ is odd. Also δ divides $2a$ and $2bi$ in $\mathbf{Z}[i]$, so $\mathrm{N}(\delta)|4a^2$ and $\mathrm{N}(\delta)|4b^2$ in $\mathbf{Z}$. Since $(a, b) = 1$, $\mathrm{N}(\delta)|4$, so $\mathrm{N}(\delta) = 1$. Thus $\delta = \pm 1$ or $\pm i$.

Theorem

If $\alpha\beta = \square$ in $\mathbf{Z}[i]$ and $(\alpha, \beta) = 1$ then α and β are squares up to unit multiple.

Either $a + bi = (u + vi)^2$ or $a + bi = i(u + vi)^2$.
First case: $a + bi = u^2 - v^2 + 2uvi \Rightarrow a = u^2 - v^2$ and $b = 2uv$.
Second case: $a + bi = -2uv + (u^2 - v^2)i \Rightarrow a = -2uv$, but a odd!
Choose sign on u so $u > 0$. Then $v > 0$ and

$$c^2 = a^2 + b^2 = \mathrm{N}((u + vi)^2) = \mathrm{N}(u + vi)^2 = (u^2 + v^2)^2.$$

Pythagorean triples from Gaussian integers

Pythagorean triples arise from squaring Gaussian integers:

$$(u+vi)^2 = a+bi \overset{\text{Norm}}{\Longrightarrow} (u^2+v^2)^2 = a^2+b^2.$$

α	α^2	Triple
$1+2i$	$-3+4i$	$(3,4,5)$
$2+3i$	$-5+12i$	$(5,12,13)$
$7+4i$	$33+56i$	$(33,56,65)$
$7+5i$	$24+70i$	$(24,70,74)$
$10+3i$	$91+60i$	$(91,60,109)$

From $7+5i$ get nonprimitive $(24,70,74) = 2(12,35,37)$. In $\mathbf{Z}[i]$,

$$\frac{7+5i}{1+i} = \frac{(7+5i)(1-i)}{(1+i)(1-i)} = \frac{12-2i}{2} = 6-i$$

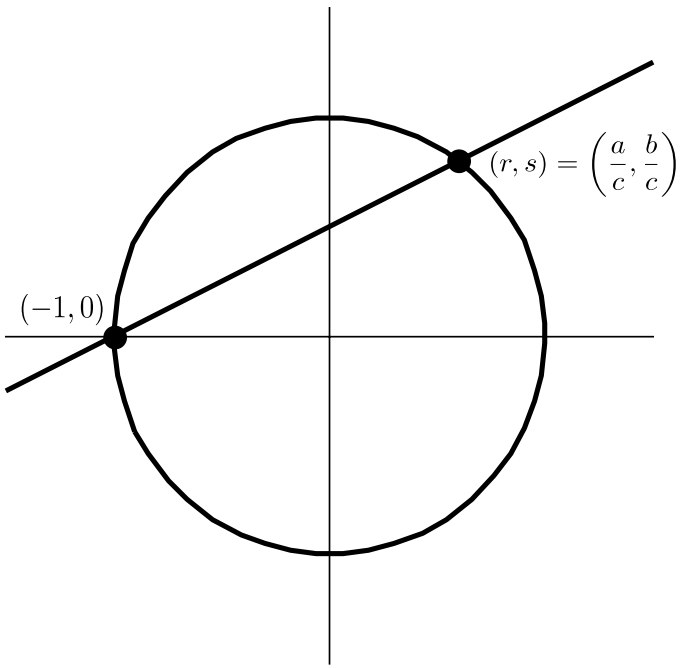
and

$$(6-i)^2 = 35-12i,$$

which gives the primitive triple $(35,12,37)$.

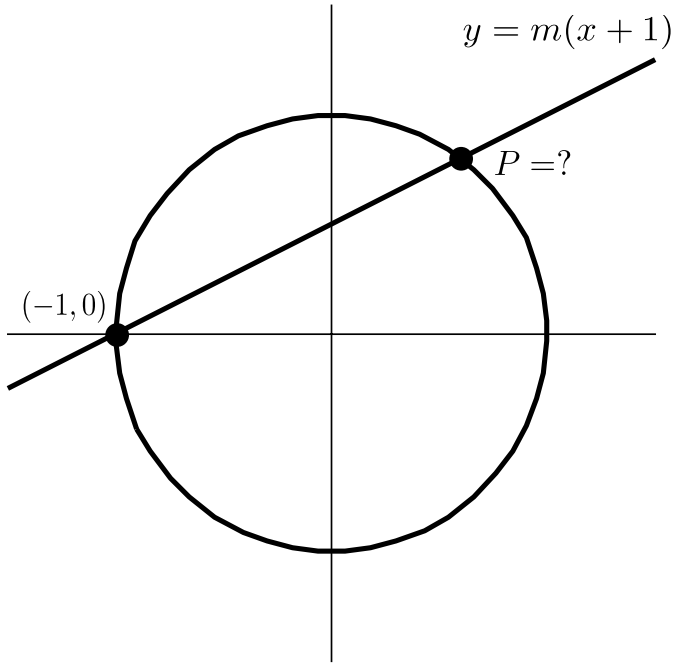
Third proof: analytic geometry

$$a^2 + b^2 = c^2 \Longrightarrow r^2 + s^2 = 1, \quad r = \frac{a}{c}, s = \frac{b}{c}.$$



The line through $(-1, 0)$ and (r, s) is $y = m(x + 1)$, where $m = \dfrac{s}{r+1}$. If $r, s \in \mathbf{Q}$ then $m \in \mathbf{Q}$.

Third proof: analytic geometry



Conversely, for $m \in \mathbf{Q}$ where does $y = m(x+1)$ meet the circle?

$$1 = x^2 + y^2 = x^2 + (m(x+1))^2 = (m^2+1)x^2 + 2m^2x + m^2,$$

so

$$0 = x^2 + \frac{2m^2}{m^2+1}x + \frac{m^2-1}{m^2+1} = (x+1)\left(x + \frac{m^2-1}{m^2+1}\right).$$

Third proof: analytic geometry

$$0 = (x+1)\left(x + \frac{m^2-1}{m^2+1}\right)$$

The second point of intersection is at (r, s), where

$$r = -\frac{m^2-1}{m^2+1} = \frac{1-m^2}{1+m^2}$$

and

$$s = m(r+1) = \frac{2m}{1+m^2}.$$

We have a correspondence

$$\{\text{rational points } (r,s) \neq (-1,0) \text{ on } x^2+y^2=1\} \longleftrightarrow m \in \mathbf{Q}$$

given by

$$(r,s) \mapsto m = \frac{s}{r+1}; \quad m \mapsto r = \frac{1-m^2}{1+m^2}, \quad s = \frac{2m}{1+m^2}.$$

Slope m gives point in first quadrant when $0 < m < 1$.

From triples to slopes

$$(a,b,c) \rightsquigarrow \left(\frac{a}{c}, \frac{b}{c}\right) \rightsquigarrow m = \frac{b/c}{a/c+1} = \frac{b}{a+c},$$

$$m \rightsquigarrow \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right).$$

a	3	5	7	15	9	115
b	4	12	24	8	40	252
c	5	13	25	17	41	277
m	1/2	2/3	3/4	1/4	4/5	9/14

It looks like $m = v/u$ in our earlier notation:

(u,v)	(2,1)	(3,2)	(4,3)	(4,1)	(5,4)	(14,9)
a	3	5	7	15	9	115
b	4	12	24	8	40	252
c	5	13	25	17	41	277

From triples to slopes

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

Earlier, we said we can solve for u^2 and v^2:

$$u^2 = \frac{a+c}{2}, \quad v^2 = \frac{c-a}{2}.$$

For $(a, b, c) = (190281, 78320, 205769)$, earlier we found

$$\frac{a+c}{2} = 198025 = 445^2, \quad \frac{c-a}{2} = 7744 = 88^2,$$

so $u = 445$ and $v = 88$. Now geometry makes us notice that

$$\frac{b}{a+c} = \frac{2uv}{2u^2} = \frac{v}{u},$$

so

$$\frac{b}{a+c} = \frac{78320}{396050} = \frac{88}{445} = \frac{v}{u}.$$

From slopes to triples

m	$1/2$	$1/3$	$2/3$	$1/4$	$3/4$
$(1-m^2)/(1+m^2)$	$3/5$	$4/5$	$5/13$	$15/17$	$7/25$
$2m/(1+m^2)$	$4/5$	$3/5$	$12/13$	$8/17$	$24/25$

m	$1/5$	$2/5$	$12/17$	$19/101$
$(1-m^2)/(1+m^2)$	$12/13$	$21/29$	$145/433$	$4920/5281$
$2m/(1+m^2)$	$5/13$	$20/29$	$408/433$	$1919/5281$

If $m \leftrightarrow (x, y)$ then $\dfrac{1-m}{1+m} \leftrightarrow (y, x)$.

Application 1: Polynomial Pythagorean triples

Consider polynomials $f(x), g(x), h(x)$ satisfying

$$f(x)^2 + g(x)^2 = h(x)^2$$

and all nonzero. Call the triple primitive if $(f(x), g(x)) = 1$.

Theorem

The primitive Pythagorean triples in $\mathbf{R}[x]$ *are given by*

$$f(x) = c(u(x)^2 - v(x)^2), \quad g(x) = 2cu(x)v(x),$$

$$h(x) = c(u(x)^2 + v(x)^2),$$

where $c \in \mathbf{R} - \{0\}$ *and* $(u(x), v(x)) = 1$.

There is a proof by unique factorization in $\mathbf{R}[x]$, as in $\mathbf{Z}$. Even/odd considerations drop out since 2 is a unit as a polynomial.

Application 2: $a^2 + 2b^2 = c^2$

Suppose $a^2 + 2b^2 = c^2$ in $\mathbf{Z}^+$ and $(a, b) = 1$. Then a is odd: if a is even then b is odd so $2 \equiv c^2 \bmod 4$: NO. From a odd, also c odd, so $2b^2 = c^2 - a^2 \equiv 1 - 1 \equiv 0 \bmod 8$, so b is even.

Theorem

The solutions (a, b, c) to $a^2 + 2b^2 = c^2$ in $\mathbf{Z}^+$ with $(a, b) = 1$ are given by

$$a = |u^2 - 2v^2|, \quad b = 2uv, \quad c = u^2 + 2v^2,$$

where $u, v > 0$, $(u, v) = 1$, and u is odd.

u	1	1	1	3	1	3	1	5
v	1	2	3	1	4	2	5	1
a	1	7	17	7	31	1	49	23
b	2	4	6	6	8	12	10	10
c	3	9	19	11	33	17	51	27

Application 3: $a^2 + b^2 = c^3$

In $\mathbf{Z}[i]$,

$$\begin{aligned}(u+vi)^3 &= u^3 + 3u^2(vi) + 3u(vi)^2 + (vi)^3 \\ &= (u^3 - 3uv^2) + (3u^2v - v^3)i.\end{aligned}$$

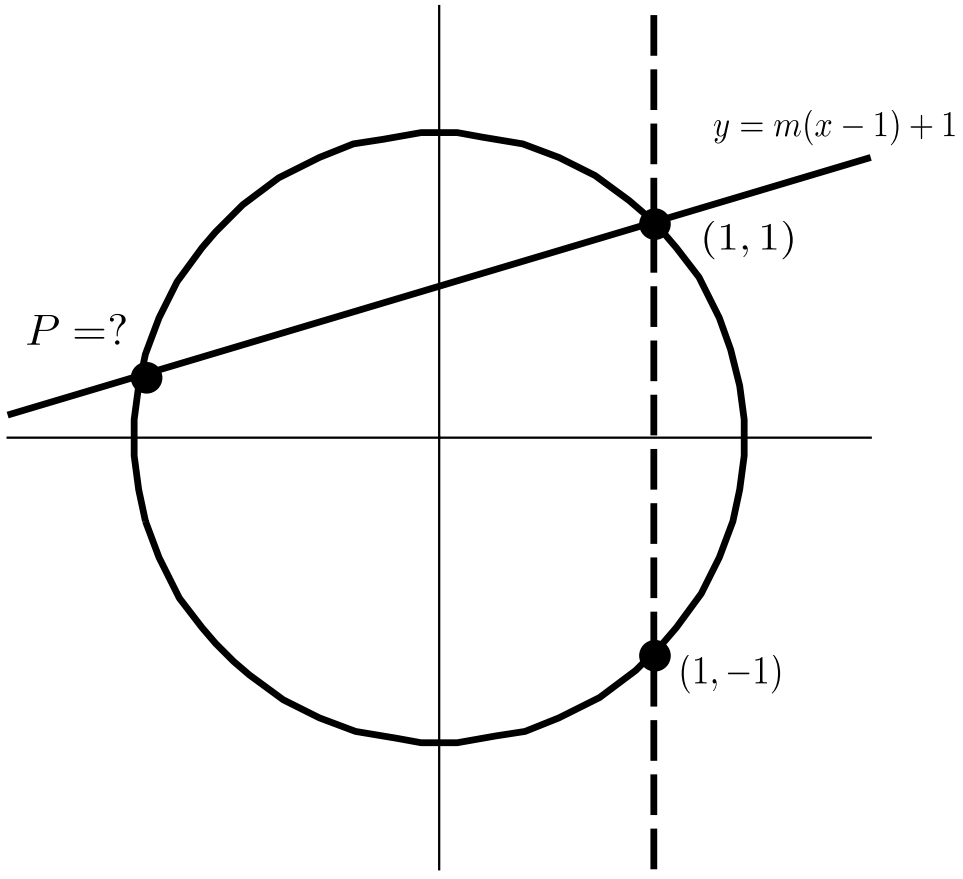
Take norms of both sides:

$$(u^2+v^2)^3 = (u^3 - 3uv^2)^2 + (3u^2v - v^3)^2.$$

u	1	2	4	7	9
v	1	1	3	2	5
$a = u^3 - 3uv^2$	-2	2	-44	259	54
$b = 3u^2v - v^3$	2	11	117	286	1090
$c = u^2 + v^2$	2	5	25	53	106

Exercise: All integral solutions to $a^2 + b^2 = c^3$ with $(a, b) = 1$ arise in this way with $(u, v) = 1$ and $u \not\equiv v \bmod 2$.

Application 4: Rational parametrizations of other conics



$$x^2 + y^2 = 2$$

Rational parametrizations of other conics

Theorem

The rational solutions to $x^2 + y^2 = 2$ *have the form*

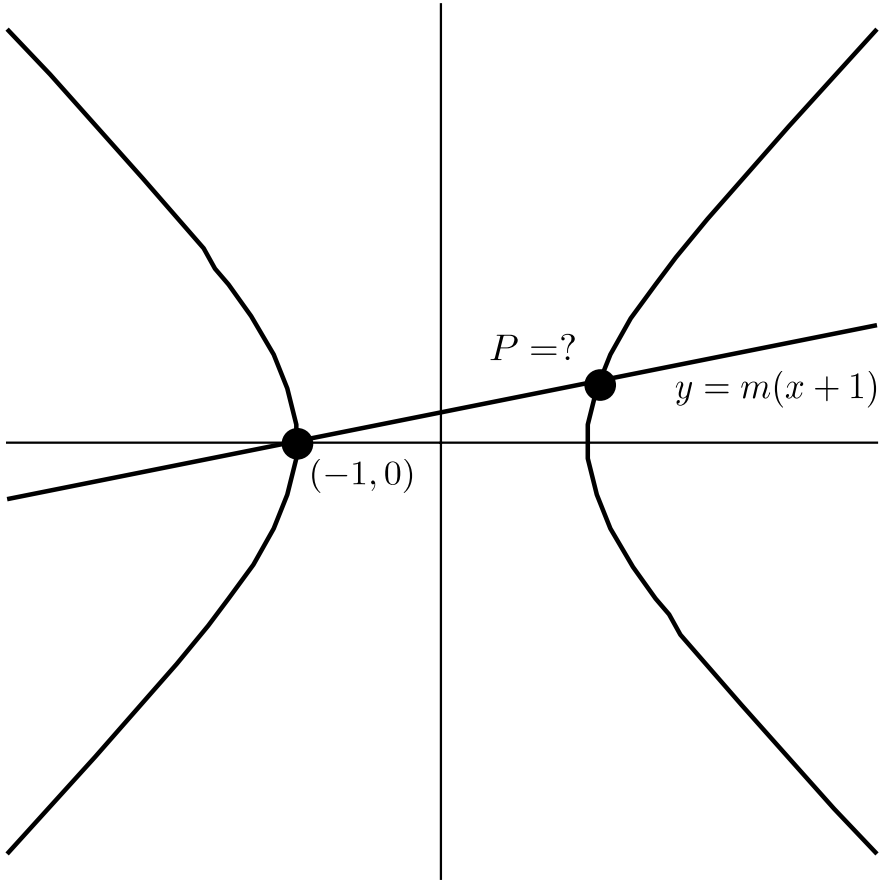
$$x = \frac{m^2 - 2m - 1}{1 + m^2}, \quad y = \frac{1 - 2m - m^2}{1 + m^2}$$

for $m \in \mathbf{Q}$, *and* $(1, -1)$.

m	1	$3/2$	$-5/7$	$8/5$	12
x	-1	$-7/13$	$23/37$	$-41/89$	$119/145$
y	-1	$-17/13$	$47/37$	$-119/89$	$-167/145$

$$\frac{7^2 + 17^2}{2} = 13^2, \quad \frac{23^2 + 47^2}{2} = 37^2, \quad \frac{41^2 + 119^2}{2} = 89^2.$$

Rational parametrizations of other conics



$$x^2 - dy^2 = 1$$

Rational parametrizations of other conics

Theorem

The rational solutions to $x^2 - dy^2 = 1$ *have the form*

$$x = \frac{1 + dm^2}{1 - dm^2}, \quad y = \frac{2m}{1 - dm^2}$$

with $m \in \mathbf{Q}$, *and* $(-1, 0)$.

m	$1/2$	$1/3$	$2/3$	$8/9$	-20
x	3	$11/7$	17	$-209/47$	$-801/799$
y	2	$6/7$	12	$-144/47$	$40/799$

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

There's no simple formula for *integral* solutions to $x^2 - dy^2 = 1$!

Application 5: Factoring quadratics

In $\mathbf{Z}[x]$,

$$x^2 + 4x + 3 = (x+1)(x+3), \quad x^2 + 4x - 3 \text{ irreducible.}$$

but

$$x^2 + 5x + 6 = (x+2)(x+3), \quad x^2 + 5x - 6 = (x-1)(x+6).$$

Question: When do $x^2 + mx + n$ and $x^2 + mx - n$ factor in $\mathbf{Z}[x]$?

Here m and n are nonzero. If $x^2 + mx + n = (x - r_1)(x - r_2)$ then $x^2 - mx + n = (x + r_1)(x + r_2)$. So we may assume $m > 0$. May take $n > 0$ too.

Factoring quadratics

Roots of $x^2 + mx \pm n$ are $\dfrac{-m \pm \sqrt{m^2 \pm 4n}}{2}$, which are integers exactly when $m^2 \pm 4n = \square$, since

$$m^2 \pm 4n \equiv m \bmod 2.$$

So we can factor $x^2 + mx + n$ and $x^2 + mx - n$ if and only if

$$m^2 - 4n = d^2, \quad m^2 + 4n = e^2, \quad d \text{ and } e \in \mathbf{Z}.$$

Then $d^2 + e^2 = 2m^2$, so $d \equiv e \bmod 2$. Solving,

$$m^2 = \frac{d^2 + e^2}{2} = \left(\frac{e+d}{2}\right)^2 + \left(\frac{e-d}{2}\right)^2.$$

Thus we have a Pythagorean triple (without specified even term)

$$\left(\frac{e-d}{2}, \frac{e+d}{2}, m\right), \quad \frac{e-d}{2} < \frac{e+d}{2} < m.$$

Exercise: This triple is primitive if and only if $(m, n) = 1$.

Factoring quadratics

Theorem (J. L. Poet, D. L. Vestal, 2005)

There is a one-to-one correspondence between Pythag. triples (a, b, c) *with* $a < b < c$ *and reducible pairs* $x^2 + mx \pm n$ *with* $m, n > 0$, *given by*

$$(a, b, c) \mapsto x^2 + cx \pm \frac{ab}{2}, \quad x^2 + mx \pm n \mapsto \left(\frac{e-d}{2}, \frac{e+d}{2}, m \right),$$

with $m^2 - 4n = d^2$ *and* $m^2 + 4n = e^2$.

a	b	c	m	n	$x^2 + mx + n$	$x^2 + mx - n$
3	4	5	5	6	$(x+2)(x+3)$	$(x-1)(x+6)$
5	12	13	13	30	$(x+3)(x+10)$	$(x-2)(x+15)$
8	15	17	17	60	$(x+5)(x+12)$	$(x-3)(x+20)$

Exercise. Factor $x^2 + (u^2 + v^2)x \pm uv(u^2 - v^2)$ in $\mathbf{Z}[x]$.