

# Infinite Descent

Keith Conrad  
University of Connecticut

August 6, 2008

## Fermat's original idea

*As ordinary methods, such as are found in the books, are inadequate to proving such difficult propositions, I discovered at last a most singular method . . . which I called the infinite descent.*

Fermat, 1659

The idea: to prove an equation has no integral solutions, show one solution forces the existence of a smaller solution, leading to

$$a_1 > a_2 > a_3 > \cdots > 0,$$

which is impossible in  $\mathbf{Z}^+$ .

Ordinary mathematical induction could be considered infinite ascent, from  $n$  to  $n + 1$ .

## Outline

- Irrationality
- Nonsolvability of several equations in  $\mathbf{Z}$  and  $\mathbf{Q}$
- Sums of Two Squares

## Irrationality of $\sqrt{2}$

Here is the usual proof.

Suppose

$$\sqrt{2} = \frac{m}{n},$$

with  $m$  and  $n$  in  $\mathbf{Z}^+$ . Without loss of generality,  $(m, n) = 1$ . Then

$$m^2 = 2n^2,$$

so  $m^2$  is even, so  $m$  is even:  $m = 2m'$ . Substitute and cancel:

$$2m'^2 = n^2.$$

Thus  $n^2$  is even, so  $n$  is even. This contradicts  $(m, n) = 1$ .

## Irrationality of $\sqrt{2}$

Here is a proof by descent. We don't have to insist  $(m, n) = 1$ .

Suppose

$$\sqrt{2} = \frac{m}{n},$$

with  $m$  and  $n$  in  $\mathbf{Z}^+$ . Then

$$m^2 = 2n^2,$$

so  $m^2$  is even, so  $m$  is even:  $m = 2m'$ . Substitute and cancel:

$$2m'^2 = n^2.$$

Thus  $n^2$  is even, so  $n$  is even:  $n = 2n'$ , so

$$m'^2 = 2n'^2.$$

A solution  $(m, n)$  to  $x^2 = 2y^2$  in  $\mathbf{Z}^+$  leads to another  $(m', n')$  where  $0 < m' < m$  (or  $0 < n' < n$ ): a contradiction.

## Irrationality of $\sqrt{2}$

Here is a wholly different proof by descent.

Suppose  $\sqrt{2} \in \mathbf{Q}$ . Since  $1 < \sqrt{2} < 2$ ,

$$\sqrt{2} = 1 + \frac{a}{b}, \quad \text{with } 0 < \frac{a}{b} < 1.$$

Square both sides and clear the denominator:

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

Thus  $a^2 = b^2 - 2ab = (b - 2a)b$ , so

$$\frac{a}{b} = \frac{b - 2a}{a}.$$

Now

$$\sqrt{2} = 1 + \frac{a}{b} = 1 + \frac{b - 2a}{a},$$

with a smaller denominator:  $0 < a < b$ . By descent we have a contradiction. (Or the denominator is eventually 1:  $\sqrt{2} \in \mathbf{Z}$ .)

## Irrationality of $\sqrt{d}$

Let  $d \in \mathbf{Z}^+$  with  $d \neq \square$ .

Suppose  $\sqrt{d} \in \mathbf{Q}$ . Let  $l < \sqrt{d} < l + 1$ ,  $l \in \mathbf{Z}$ . Write

$$\sqrt{d} = l + \frac{a}{b}, \quad \text{with } 0 < \frac{a}{b} < 1.$$

Square both sides and clear the denominator:

$$db^2 = l^2b^2 + 2lab + a^2.$$

Thus  $a^2 = db^2 - l^2b^2 - 2lab = (db - l^2b - 2la)b$  so

$$\frac{a}{b} = \frac{db - l^2b - 2la}{a}.$$

Now

$$\sqrt{d} = l + \frac{a}{b} = l + \frac{db - l^2b - 2la}{a},$$

with a smaller denominator:  $0 < a < b$ . By descent we have a contradiction. (Or the denominator is eventually 1:  $\sqrt{d} \in \mathbf{Z}$ .)

## Impossibility of $x^2 + y^2 = 3$ in $\mathbf{Q}$

### Theorem

*There is no solution to  $x^2 + y^2 = 3$  in rational numbers.*

If there is,  $x$  and  $y$  are not 0. We can take them both positive. Write  $x = a/c$  and  $y = b/c$  with  $a, b, c$  in  $\mathbf{Z}^+$ , so

$$a^2 + b^2 = 3c^2.$$

Then  $a^2 + b^2 \equiv 0 \pmod{3}$ , so (!)  $a$  and  $b$  are multiples of 3:  $a = 3a'$  and  $b = 3b'$ . Then

$$9a'^2 + 9b'^2 = 3c^2 \implies 3(a'^2 + b'^2) = c^2,$$

so  $3|c$ :  $c = 3c'$ . Then

$$3(a'^2 + b'^2) = 9c'^2 \implies a'^2 + b'^2 = 3c'^2.$$

We have a new solution with  $0 < c' < c$ : contradiction.



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

### Theorem (Fermat)

*There is no solution in  $\mathbf{Z}^+$  to  $x^4 + y^4 = z^2$ .*

This is the *only* result for which we have details of his proof!

### Corollary

*The equation  $a^4 + b^4 = c^4$  has no solution in  $\mathbf{Z}^+$ .*

To prove the theorem, let's make the Pythagorean triple  $(x^2, y^2, z)$  primitive. If a prime  $p$  divides  $x$  and  $y$  then  $z^2 = x^4 + y^4$  is divisible by  $p^4$ :  $p^4 | z^2$ , so  $p^2 | z$ .

$$x = px', y = py', z = p^2 z' \Rightarrow p^4(x'^4 + y'^4) = p^4 z'^2.$$

Thus  $x'^4 + y'^4 = z'^2$ . So without loss of generality,  $(x, y) = 1$ .

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

When  $x^4 + y^4 = z^2$  in  $\mathbf{Z}^+$  with  $(x, y) = 1$ ,  $(x^2, y^2, z)$  is a primitive triple: one of  $x$  or  $y$  is odd and the other even. By symmetry, take  $x$  odd and  $y$  even, so

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad z = u^2 + v^2$$

where  $u > v > 0$  and  $(u, v) = 1$  (and  $u \not\equiv v \pmod{2}$ ). Then  $(x, v, u)$  is a primitive triple with  $x$  odd, so  $v$  is even:

$$x = s^2 - t^2, \quad v = 2st, \quad u = s^2 + t^2,$$

where  $s > t > 0$  and  $(s, t) = 1$ . Note  $z > u^2 \geq u = s^2 + t^2$ , and

$$y^2 = 2uv = 2(s^2 + t^2)(2st) = 4st(s^2 + t^2).$$

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

$$y^2 = 4st(s^2 + t^2), \quad (s, t) = 1, \quad z > s^2 + t^2.$$

Since  $y$  is even,

$$\left(\frac{y}{2}\right)^2 = st(s^2 + t^2).$$

The factors on the right are pairwise relatively prime (why?) and each is positive, so they are all squares:

$$s = x'^2, \quad t = y'^2, \quad s^2 + t^2 = z'^2.$$

where  $x', y', z'$  are positive and pairwise relatively prime. Then

$$x'^4 + y'^4 = z'^2,$$

so we have a second primitive solution to our equation. Since

$$z > s^2 + t^2 = z'^2 \geq z',$$

we are done by descent on  $z$ :  $z' < z$ . Put differently, if  $x^4 + y^4 = z^2$  has soln in  $\mathbf{Z}^+$ , so does  $x^4 + y^4 = 1$ , but it doesn't.

## Summary of the descent

$$\begin{aligned}
 x^4 + y^4 &= z^2, \quad (x, y) = 1, \quad y \text{ even,} \\
 x^2 &= u^2 - v^2, \quad y^2 = 2uv, \quad z = u^2 + v^2, \quad (u, v) = 1, \\
 x &= s^2 - t^2, \quad v = 2st, \quad u = s^2 + t^2, \quad (s, t) = 1, \\
 s &= x'^2, \quad t = y'^2, \quad s^2 + t^2 = z'^2 \Rightarrow x'^4 + y'^4 = z'^2.
 \end{aligned}$$

Suppose we started with  $x^4 + y^4 = z^4$ . Then what happens?

$$\begin{aligned}
 x^4 + y^4 &= z^4, \quad (x, y) = 1, \quad y \text{ even,} \\
 x^2 &= u^2 - v^2, \quad y^2 = 2uv, \quad z^2 = u^2 + v^2, \quad (u, v) = 1, \\
 x &= s^2 - t^2, \quad v = 2st, \quad u = s^2 + t^2, \quad (s, t) = 1, \\
 s &= x'^2, \quad t = y'^2, \quad s^2 + t^2 = z'^2 \Rightarrow x'^4 + y'^4 = z'^2.
 \end{aligned}$$

## Alternate Descent Parameter

The first solution  $(x, y, z)$  to  $x^4 + y^4 = z^2$  can be written in terms of the second (smaller) solution  $(x', y', z')$ :

$$x = x'^4 - y'^4, \quad y = 2x'y'z', \quad z = 4x'^4y'^4 + z'^4.$$

So in fact  $z > z'^4$ , not just  $z > z'^2$  as before. These explicit formulas tell us

$$0 < y' < y \text{ and } 0 < \max(x', y') < y \leq \max(x, y),$$

so we could do descent on  $\max(x, y)$  (on  $y$ ?) rather than on  $z$ .

## Consequences of nonsolvability of $x^4 + y^4 = z^2$ in $\mathbf{Z}^+$

### Corollary

*Any integral solution to  $x^4 + y^4 = z^2$  has  $x$  or  $y$  equal to 0.*

Otherwise change signs to make  $x$  and  $y$  (and  $z$ ) all positive.

### Corollary

*The only rational solutions to  $y^2 = x^4 + 1$  are  $(0, \pm 1)$ .*

Set  $x = a/c$  and  $y = b/c$  to get  $(bc)^2 = a^4 + c^4$ . Thus  $a = 0$ , so  $x = 0$ .

### Corollary

*The only rational solutions to  $2y^2 = x^4 - 1$  are  $(\pm 1, 0)$ .*

Square and fiddle to get  $(y/x)^4 + 1 = ((x^4 + 1)/2x^2)^2$ , so  $y = 0$ .

Consequences of nonsolvability of  $x^4 + y^4 = z^2$  in  $\mathbf{Z}^+$ **Corollary**

*The only rational solutions to  $y^2 = x^3 - 4x$  are  $(0, 0), (\pm 2, 0)$ .*

There is a one-to-one correspondence

$$v^2 = u^4 + 1 \iff y^2 = x^3 - 4x, \quad x \neq 0.$$

given by

$$\begin{aligned} x &= \frac{2}{u^2 - v} & y &= \frac{4u}{u^2 - v} \\ u &= \frac{y}{2x} & v &= \frac{y^2 - 8x}{4x^2}, \end{aligned}$$

so from the corollary that  $v^2 = u^4 + 1$  only has rational solutions with  $u = 0$ , rational solutions to  $y^2 = x^3 - 4x$  have  $x = 0$  or  $y = 0$ .

Consequences of nonsolvability of  $x^4 + y^4 = z^2$  in  $\mathbf{Z}^+$ 

## Corollary

*The only rational solution to  $y^2 = x^3 + x$  is  $(0, 0)$ .*

Assume  $x \neq 0$ . Since  $y^2 = x(x^2 + 1)$ ,  $y \neq 0$ . May take  $x, y > 0$ .  
Then (!)  $x = a/c^2$  and  $y = b/c^3$  in reduced form, so

$$\left(\frac{b}{c^3}\right)^2 = \left(\frac{a}{c^2}\right)^3 + \frac{a}{c^2} \implies b^2 = a^3 + ac^4 = a(a^2 + c^4).$$

Since  $(a, c) = 1$ ,

$$a = u^2, \quad a^2 + c^4 = v^2 \implies u^4 + c^4 = v^2.$$



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

## Theorem (Fermat)

*There is no solution in  $\mathbf{Z}^+$  to  $x^4 - y^4 = z^2$ .*

To prove the theorem, since  $z^2 + y^4 = x^4$  instead of  $x^4 + y^4 = z^2$ , reverse the roles of  $x$  and  $z$ ; do descent on  $x$  instead of on  $z$ . Some extra details arise. On the right side below are explicit formulas for a solution  $(x, y, z)$  in terms of a “smaller” solution  $(x', y', z')$ .

$x^4 + y^4 = z^2$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $x = x'^4 - y'^4$ $y = 2x'y'z'$ $z = 4x'^4y'^4 + z'^4$ $z' \leq z'^4 < z$	$x^4 - y^4 = z^2$ <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> $x = x'^4 + y'^4$ $y = 2x'y'z'$ $z =  4x'^4y'^4 - z'^4 $ $x' \leq x'^4 < x$
--	--

Consequences of nonsolvability of  $x^4 - y^4 = z^2$  in  $\mathbf{Z}^+$ 

Old corollaries

$$x^4 + y^4 = z^2 \text{ in } \mathbf{Z} \Rightarrow xy = 0$$

$$y^2 = x^4 + 1 \text{ in } \mathbf{Q} \Rightarrow x = 0$$

$$2y^2 = x^4 - 1 \text{ in } \mathbf{Q} \Rightarrow x = \pm 1$$

$$y^2 = x^3 - 4x \text{ in } \mathbf{Q} \Rightarrow y = 0$$

$$y^2 = x^3 + x \text{ in } \mathbf{Q} \Rightarrow y = 0$$

New corollaries

$$x^4 - y^4 = z^2 \text{ in } \mathbf{Z} \Rightarrow yz = 0$$

$$y^2 = x^4 - 1 \text{ in } \mathbf{Q} \Rightarrow y = 0$$

$$2y^2 = x^4 + 1 \text{ in } \mathbf{Q} \Rightarrow x = \pm 1$$

$$y^2 = x^3 + 4x \text{ in } \mathbf{Q} \Rightarrow y = 0$$

$$y^2 = x^3 - x \text{ in } \mathbf{Q} \Rightarrow y = 0$$

Consequences of nonsolvability of  $x^4 \pm y^4 = z^2$  in  $\mathbf{Z}^+$ 

## Theorem

*No Pythagorean triple has two terms that are squares.*

Otherwise we could solve  $x^4 + y^4 = z^2$  or  $x^4 + y^2 = z^4$  in  $\mathbf{Z}^+$ .  
Many Pythagorean triples have one term that is a square:

$a$	3	7	9	16	17	225
$b$	4	24	40	63	144	272
$c$	5	25	41	65	145	353

## Theorem

*The only triangular number that is a fourth power is 1.*

If  $m(m+1)/2 = n^4$  with  $m > 1$  then  $\{m, m+1\} = \{x^4, 2y^4\}$  with  $x > 1$  and  $y > 1$ , so  $x^4 - 2y^4 = \pm 1 \implies y^8 \pm x^4 = ((x^4 \pm 1)/2)^2$ .  
This is impossible in positive integers.

Consequences of nonsolvability of  $x^4 \pm y^4 = z^2$  in  $\mathbb{Z}^+$ 

Why did Fermat look at  $x^4 \pm y^4 = z^2$  rather than  $x^4 \pm y^4 = z^4$ ?

**Theorem (Fermat)**

*No Pythagorean triangle has area equal to a square or twice a square.*

This first part was stated by Fibonacci (1225), without proof.

$a^2 + b^2 = c^2,$ $\frac{1}{2}ab = d^2$	$x^4 - y^4 = z^2$	$a^2 + b^2 = c^2,$ $\frac{1}{2}ab = 2d^2$	$x^4 + y^4 = z^2$
$x = c$	$a = z^2$	$x = b$	$a = x^2$
$y = 2d$	$b = 2x^2y^2$	$y = 2d$	$b = y^2$
$z =  a^2 - b^2 $	$c = x^4 + y^4$	$z = bc$	$c = z$
	$d = xyz$		$d = xy/2$

These are not inverse correspondences, but that's okay.

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

### Theorem (Euler, 1768)

*There is no solution in  $\mathbf{Z}^+$  to  $x^3 + y^3 = z^3$ .*

Euler used descent and needed a lemma.

### Lemma

*If  $a^2 + 3b^2 = \text{cube}$  and  $(a, b) = 1$  then  $a = u^3 - 9uv^2$  and  $b = 3u^2v - 3v^3$  for some  $u, v \in \mathbf{Z}$ .*

This is analogous to a description of  $a^2 + b^2 = \text{cube}$  with  $(a, b) = 1$ :  $a = u^3 - 3uv^2$  and  $b = 3u^2v - v^3$ . Euler proved the lemma with unique factorization in  $\mathbf{Z}[\sqrt{-3}]$ , but that is *false*:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Nevertheless, the lemma is true!

## Selmer's example

**Theorem (Selmer, 1951)**

*The only integral solution to  $3x^3 + 4y^3 = 5z^3$  is  $(0, 0, 0)$ .*

It can be shown  $3x^3 + 4y^3 \equiv 5z^3 \pmod{n}$  has a solution  $\neq (0, 0, 0) \pmod{n}$  for all  $n \geq 2$ , so nonsolvability in  $\mathbf{Z}$  can't be seen by congruence considerations.

We sketch a proof of the theorem using descent. From an integral solution  $(x, y, z) \neq (0, 0, 0)$ , none of the terms is 0 and we get

$$3x^3 + 4y^3 = 5z^3 \implies (2y)^3 + 6x^3 = 10z^3,$$

so

$$a^3 + 6b^3 = 10c^3$$

for  $a = 2y, b = x, c = z$ . May take  $a, b, c$  pairwise relatively prime.

## Selmer's example

$$a^3 + 6b^3 = 10c^3, \quad (a, b, c) = 1$$

Using  $\mathbf{Z}[\sqrt[3]{6}] = \{k + \ell\sqrt[3]{6} + m\sqrt[3]{36} : k, \ell, m \in \mathbf{Z}\}$ , basically get

$$a + b\sqrt[3]{6} = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\alpha^3$$

for some  $\alpha \in \mathbf{Z}[\sqrt[3]{6}]$ . Write  $\alpha = k + \ell\sqrt[3]{6} + m\sqrt[3]{36}$  and equate coefficients of  $\sqrt[3]{36}$  on both sides above:

$$0 = k^3 + 6\ell^3 + 36m^3 + 36klm + 2(3k\ell^2 + 3k^2m + 18\ell m^2) - 3(3k^2\ell + 18km^2 + 18\ell^2m).$$

Reduce mod 3:  $0 \equiv k^3$ , so  $3|k$ . Reduce mod 9:  $0 \equiv 6\ell^3$ , so  $3|\ell$ .

Reduce mod 27:  $0 \equiv 36m^3$ , so  $3|m$ . Divide by  $3^3$  and repeat again.

Thus  $\alpha = 0$ , so  $a = b = 0$ , so  $x = b = 0$ ,  $y = a/2 = 0$ ,  $z = 0$ .

## Fermat speaks

*If there is a right triangle with integral sides and with an area equal to the square of an integer, then there is a second triangle, smaller than the first, which has the same property [...] and so on ad infinitum. [...] From which one concludes that it is impossible that there should be [such] a right triangle.*

*It was a long time before I was able to apply my method to affirmative questions, because the way and manner of getting at them is much more difficult than that which I employ with negative theorems. So much so that, when I had to prove that every prime number of the form  $4k + 1$  is made up of two squares, I found myself in much torment. But at last a certain meditation many times repeated gave me the necessary light, and affirmative questions yielded to my method [...]* Fermat, 1659



## Affirmative Questions

Some positive theorems Fermat (1659) suggested he could prove by descent:

- Two Square Theorem: Any prime  $p \equiv 1 \pmod{4}$  is a sum of two squares (Euler, 1747)
- Four Square Theorem: Every positive integer is a sum of four squares (Lagrange, 1770).
- For  $d \neq \square$ ,  $x^2 - dy^2 = 1$  has infinitely many integral solutions (Lagrange, 1768). The difficult step is existence of even one nontrivial solution ( $y \neq 0$ ).

## Sums of Two Squares

### Theorem

For prime  $p$ , if  $-1 \equiv \square \pmod{p}$  then  $p = x^2 + y^2$  in  $\mathbf{Z}$ .

By hypothesis,  $-1 \equiv a^2 \pmod{p}$ . May take  $|a| \leq p/2$ . Write

$$a^2 + 1 = pd,$$

so

$$pd = a^2 + 1 \leq \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{4} + 1 < \frac{p^2}{2}$$

and thus  $d < p/2$ . From any equation with side condition

$$pk = x^2 + y^2, \quad 0 < k < \frac{p}{2}$$

where  $k > 1$ , we will find such an equation with  $0 < k' < k$ . So eventually  $k = 1$  and  $p$  is sum of two squares! How do we get  $k'$ ?

## Sums of Two Squares

We have

$$pk = x^2 + y^2, \quad 1 < k < \frac{p}{2}.$$

Set  $x \equiv r \pmod{k}$ ,  $y \equiv s \pmod{k}$ , with  $|r|, |s| \leq k/2$ . At least one of  $r$  and  $s$  is not 0: otherwise,  $k|x$  and  $k|y$ , so  $k^2|pk$ , and thus  $k|p$ . But  $1 < k < p$ . Since

$$r^2 + s^2 \equiv x^2 + y^2 \equiv 0 \pmod{k},$$

we can set  $r^2 + s^2 = kk'$  with  $k' > 0$ . Then

$$0 < kk' = r^2 + s^2 \leq \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 = \frac{k^2}{2},$$

which makes  $0 < k' \leq k/2 < k$ . We will show  $pk'$  is a sum of two squares.

## Sums of Two Squares

$$pk = x^2 + y^2, \quad kk' = r^2 + s^2, \quad x \equiv r \pmod{k}, \quad y \equiv s \pmod{k}.$$

Multiplying,

$$(pk)(kk') = (x^2 + y^2)(r^2 + s^2) = (xs - yr)^2 + (xr + ys)^2,$$

and modulo  $k$ ,  $xs - yr \equiv xy - yx \equiv 0$ ,  $xr + ys \equiv x^2 + y^2 \equiv 0$ .

Write  $xs - yr = kx'$  and  $xr + ys = ky'$ . Then

$$pk^2k' = (kx')^2 + (ky')^2 = k^2(x'^2 + y'^2).$$

Divide by  $k^2$ :  $pk' = x'^2 + y'^2$ , and  $0 < k' < k$  (so  $0 < k' < p/2$ ).

Repeat until  $k = 1$ .

**Remark.** Fermat's own proof by descent that  $p$  is a sum of two squares used counterexamples: from one, get a smaller one.

Eventually reach 5, which is not a counterexample!

## Sums of Two Squares

### Theorem

If  $n \in \mathbf{Z}^+$  is a sum of two squares in  $\mathbf{Q}$  then it is a sum of two squares in  $\mathbf{Z}$ .

### Example

No solution to  $21 = x^2 + y^2$  in  $\mathbf{Q}$  since none in  $\mathbf{Z}$ .

Suppose  $n = r^2 + s^2$  with rational  $r$  and  $s$ . Write  $r = a/c$  and  $s = b/c$  with common denominator  $c \geq 1$ . If  $c > 1$ , find a second representation  $n = r'^2 + s'^2$  in  $\mathbf{Q}$  with common denominator  $0 < c' < c$ . So eventually  $c = 1$  and  $n = a^2 + b^2$  in  $\mathbf{Z}$ .

The idea for this descent is geometric: get new pairs  $(r, s)$ ,  $(r', s')$ ,  $(r'', s'')$ ,  $\dots$  using repeated intersections of lines with the circle  $x^2 + y^2 = n$  in  $\mathbf{R}^2$ .

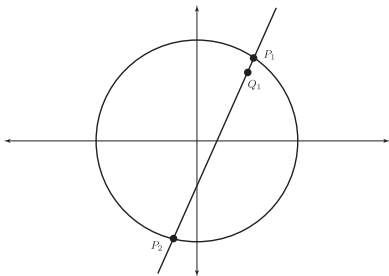
## An Example

Start with  $193 = (933/101)^2 + (1048/101)^2$ . Let

$$P_1 = \left( \frac{933}{101}, \frac{1048}{101} \right) \approx (9.2, 10.3).$$

Its nearest integral point is  $Q_1 = (9, 10)$ , and the line  $\overline{P_1 Q_1}$  meets the circle  $x^2 + y^2 = 193$  in  $P_1$  and

$$P_2 = \left( -\frac{27}{5}, -\frac{64}{5} \right).$$



## An Example, contd.

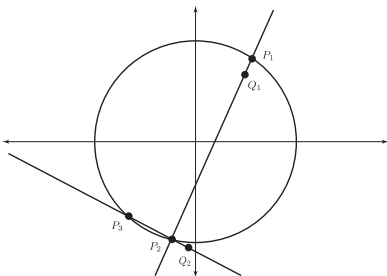
The nearest integral point to

$$P_2 = \left( -\frac{27}{5}, -\frac{64}{5} \right) = (-5.4, -12.8)$$

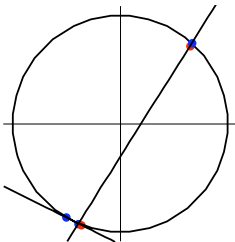
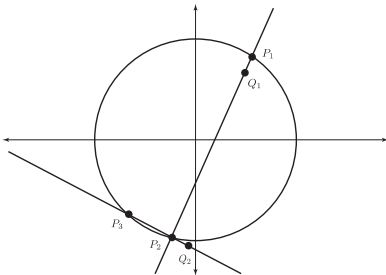
is  $Q_2 = (-5, -13)$ , and the line  $\overline{P_2Q_2}$  meets the circle in  $P_2$  and the point

$$P_3 = (-7, -12).$$

$$193 = (-7)^2 + (-12)^2 = 7^2 + 12^2$$



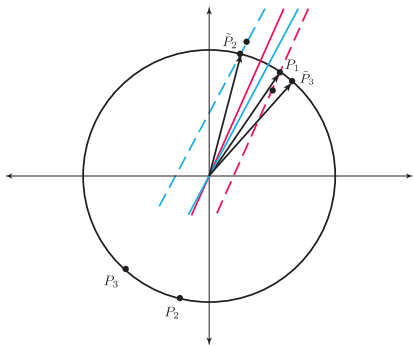
# The Real Picture





## Using Reflections

The second intersection point of a line with a circle could be replaced with reflection across a parallel line through the origin.



$$\tilde{P}_2 = \left( \frac{27}{5}, \frac{64}{5} \right), \quad \tilde{P}_3 = (7, 12)$$

## Sums of Two Squares

Intersections of lines with a sphere in  $\mathbf{R}^3$  works for three squares:

### Theorem

*If  $n \in \mathbf{Z}^+$  is a sum of three squares in  $\mathbf{Q}$  then it is a sum of three squares in  $\mathbf{Z}$ .*

Start with  $13 = (18/11)^2 + (15/11)^2 + (32/11)^2$ .

$$P_1 = \left( \frac{18}{11}, \frac{15}{11}, \frac{32}{11} \right) \rightsquigarrow Q_1 = (2, 1, 3),$$

$\overline{P_1 Q_1}$  meets  $x^2 + y^2 + z^2 = 13$  in  $P_1$  and  $P_2 = (2/3, 7/3, 8/3)$ .

$$P_2 = \left( \frac{2}{3}, \frac{7}{3}, \frac{8}{3} \right) \rightsquigarrow Q_2 = (1, 2, 3),$$

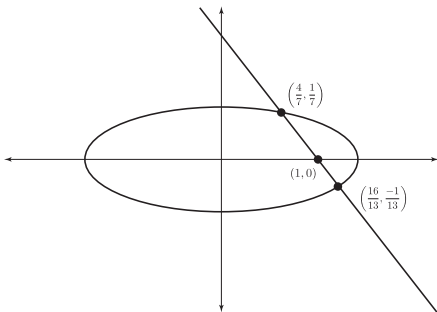
$\overline{P_2 Q_2}$  meets the sphere in  $P_2$  and  $P_3 = (0, 3, 2)$ :  $13 = 0^2 + 3^2 + 2^2$ .

## Cautionary examples

The equation

$$x^2 + 82y^2 = 2$$

has no integral solution, but it has the rational solution  $(4/7, 1/7)$ . What happens if we try the method of proof? The nearest integral point is  $(1, 0)$  and the line through them meets the ellipse in  $(16/13, -1/13)$ : the denominator has gone up, not down.



## Cautionary examples

The equation

$$x^3 + y^3 = 13$$

has no integral solution, but it has the rational solution  $(7/3, 2/3)$ . Its nearest integral point is  $(2, 1)$ , and the line through them meets the curve in  $(2/3, 7/3)$ , whose nearest integral point is  $(1, 2), \dots$

