Fermat's Method of Descent

Andrew D Smith
University College Dublin

29 November 2025

IMO 1988 Problem 6

Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that

$$\frac{a^2+b^2}{1+ab}$$

is a perfect square.

Examples (not included within the original question):

$$4=\frac{0^2+2^2}{1+0\cdot 2}=\frac{2^2+8^2}{1+2\cdot 8}=\frac{8^2+30^2}{1+8\cdot 30}=\frac{30^2+112^2}{1+30\cdot 112}$$

1 Fermat's Method of Descent

1.1 Definition

Sometimes we have an equation whose solution is not obvious, but where we can find a way, given one solution, to find another solution.

Fermat's *method of descent* involves creating a relation between different solutions to a Diophantine (in integers) equation. Applying the relation can either provide a way to construct all solutions from a base case, or (by deriving a contradiction involving the smallest solution), to show that no solution exists.

1.2 Geometric Example

Is it possible to draw a regular pentagon on a square lattice such that every vertex of the pentagon lies on a lattice point?

2 Approximating $\sqrt{3}$

2.1 Irrationality of $\sqrt{3}$

Suppose (for a contradiction) that there are positive integers (a, b) such that

$$\sqrt{3} = \frac{a}{b}$$

Let us take the smallest solution in positive integers.

Then $a^2 = 3b^2$ so a^2 is a multiple of 3, implying that a is a multiple of 3, and so $a/3$ is an integer.

We can then write:

$$\sqrt{3} = \frac{3}{\sqrt{3}} = \frac{3b}{a} = \frac{b}{a/3}$$

This produces a smaller solution, hence a contradiction.

2.2 Alternative Proof of $\sqrt{3}$ Irrational

Suppose that $a = b\sqrt{3}$ witha, b positive integers and b minimal. Then

$$\frac{2a-3b}{2b-a} = \frac{2b\sqrt{3}-3b}{2b-b\sqrt{3}} = \frac{2\sqrt{3}-3}{2-\sqrt{3}} = \sqrt{3}$$

This will lead to a contradiction if we can show that the numerator and denominator of the left-hand side are positive integers and $2b - a < b$.

This follows because

- $4a^2 > 3a^2 = 9b^2$ which, on taking square roots, implies $2a > 3b > 2b$ and so $2b - a < b$.

- $4b^2 > 3b^2 = a^2$ which, on taking square roots, implies $2b > a$

2.3 Brahmagupta's Identity

$$\begin{aligned}(2a-3b)^2 - 3(2b-a)^2 &= 4a^2 - 12ab + 9b^2 - 12b^2 + 12ab - 3a^2\\ &= a^2 - 3b^2\\ &= 4a^2 + 12ab + 9b^2 - 12b^2 - 12ab - 3a^2\\ &= (2a+3b)^2 - 3(2b+a)^2\end{aligned}$$

These are special cases of Brahmagupta's identity (628 AD).

How does this help?

It relates solutions of

$$a^2 - 3b^2 = r$$

For different integers r.

If $r = 0$ solutions imply expressions of $\sqrt{3}$ as a rational number. We know that has no solutions.

If $r = 1$ this is the *Pell* equation.

If $r = -1$ this is the *Negative Pell* equation.

If (a, b) is an integer solution for some r, then so are $(2a - 3b, 2b - a)$ and $(2a + 3b, 2b + a)$.

A more general form of Brahmagupta's identity is:

$$\begin{aligned}\left(a^2 + nb^2\right)\left(c^2 + nd^2\right) &= (ac - nbd)^2 + n\,(ad + bc)^2\\ &= (ac + nbd)^2 + n\,(ad - bc)^2\end{aligned}$$

2.4 Irrationality of $\sqrt{3}$ Using Brahmagupta's Identity

Suppose $a^2 = 3b^2$ with a, b positive integers. Take the smallest such b.

Then $2a > 3b$ and $2b > a$ (why?)

And so $(2a - 3b, 2b - a)$ is a smaller solution, hence a contradiction.

2.5 Solutions of Pell's Equation using Brahmagupta's Identity

If (a, b) is an integer solution of $a^2 - 3b^2 = r$ for some r, then so are $(2a - 3b, 2b - a)$ and $(2a + 3b, 2b + a)$.

With $r = 1$, that allows us to build a set of solutions starting with $1^2 - 3 \cdot 0^2 = 1$.

With $r = -2$, that allows us to build a set of solutions starting with $1^2 - 3 \cdot 1^2 = -2$.

Question: Do all solutions arise in this way?

Can you use this method to show there are no solutions to the negative Pell equation $a^2 - 3b^2 = -1$? Can you think of a simpler way to reach that conclusion?

3 Close Approximation by Rational Numbers

3.1 Rationals are Dense

It is easy to see that rational numbers can get arbitrarily close to any real number $\xi > 0$. Indeed, for any integer denominator $b > 0$ we can find a integer a such that

$$\left|\xi - \frac{a}{b}\right| \le \frac{1}{2b}.$$

The proof is easy. Just take a to be the closest integer to $b\xi$. That minimised distance is at most $\frac{1}{2}$. Dividing by b implies the result claimed.

That is the best possible if the value of the denominator b is forced upon us. Suppose instead choose b subject only to a maximum value.

3.2 Dirichlet's Approximation Theorem

Let $N \ge 1$ be a positive integer and let $\xi > 0$ be a real number. Then there exist positive integers a, b with $1 \le b \le N$ such that

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{Nb} \le \frac{1}{b^2}$$

Proof: consider the $N+1$ numbers (for $0 \le j \le N$)

$$x_j = \xi j - \lfloor \xi j \rfloor$$

for $0 \leq j \leq N$, where $\lfloor z \rfloor$ is the greatest integer not exceeding z. These all satisfy $0 \leq x_j < 1$.

Now partition the unit interval into N disjoint buckets:

$$[0,1) = \left[0, \frac{1}{N}\right) \cup \left[\frac{1}{N}, \frac{2}{N}\right) \cup \cdots \cup \left[\frac{N-1}{N}, 1\right)$$

By Dirichlet's pigeon-hole principle, one of these N buckets must contain two (or more) of the $N+1$ numbers$\{x_j\}$. Those two numbers must differ by less than $1/N$.

Thus, we have $0 \leq j < k \leq N$ with

$$\frac{1}{N} < |x_k - x_j| = |\xi k - \lfloor \xi k \rfloor - \xi j + \lfloor \xi j \rfloor|$$

Dividing by $k-j$ gives

$$\left| \xi - \frac{\lfloor \xi k \rfloor - \lfloor \xi j \rfloor}{k-j} \right| \leq \frac{1}{N(k-j)}$$

This proves Dirichlet's theorem.

3.3 Integer-free Zones about $b\sqrt{3}$

Lemma:

- There are infinitely many integers $b \geq 1$ for which the interval
$$\left(b\sqrt{3} - \frac{1}{\sqrt{3}(b-\frac{1}{4})}, b\sqrt{3} - \frac{1}{\sqrt{3}b} \right)$$
contains an integer.

- There are no integers $b \geq 1$ for which the interval
$$\left(b\sqrt{3} - \frac{1}{\sqrt{3}b}, b\sqrt{3} + \frac{1}{2\sqrt{3}(b+\frac{1}{4})}\right)$$
contains in integer.

- There are infinitely many integers $b \geq 1$ for which the interval
$$\left(b\sqrt{3} + \frac{1}{2\sqrt{3}(b+\frac{1}{4})}, b\sqrt{3} + \frac{1}{2\sqrt{3}b}\right)$$
contains an integer.

Proof: Let a represent an integer. The first condition is

$$3b^2 - 2 - \frac{1}{2(b-\frac{1}{4})} + \frac{1}{3(b-\frac{1}{4})^2} < a^2 < 3b^2 - 2 + \frac{1}{3b^2}$$

This is satisfied by any $a^2 = 3b^2 - 2$, for example $a = b = 1$, then extend upwards by Brahmagupta.

Squaring the second condition gives:

$$3b^2 - 2 + \frac{1}{3b^2} < a^2 < 3b^2 + 1 - \frac{1}{4(b+\frac{1}{4})} + \frac{1}{12(b+\frac{1}{4})^2}$$

As a and b are integers, these can be satisfied only if $a^2 - 3b^2 = -1$ or if $a^2 - 3b^2 = 0$, both of which, as we have already seen, have no integer solutions.

The third case is similar to the first case, but involving solutions to Pell's equation $a^2 - 3b^2 = 1$.

3.4 Hurwitz Theorem

Given any irrational number $\xi > 0$, there are infinitely pairs (a, b) of relatively-prime positive integers such that:

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{\sqrt{5}b^2}$$

Remark: Hurwitz' theorem might not hold if ξ is rational. For example, put $\xi = 1$ and suppose $b \geq 2$. Then relative primality of a and b imply $a \neq b$ and so either $a \leq b - 1$ or $a \geq b + 1$ and $|1 - \frac{a}{b}| \geq \frac{1}{b}$.

4 Fermat's Last Theorem

Some maths history.

Fermat's last theorem states that the equation:

$$x^n + y^n = z^n$$

has no solution in positive integers x, y, z for integer $n \geq 3$.

Of course there are infinitely many solutions with $n = 1$ and (Pythagorean triples) for $n = 2$.

Fermat's last theorem was (probably) not proved by Fermat, but by Andrew Wiles in 1994.

But there were proofs known for small values of n. Proofs of Fermat's last theorem for $n = 3$ and for $n = 4$ both use Fermat's method of descent (a lot of detail - search online).

5 Markov's Equation

5.1 Roots of Quadratic Polynomials

A quadratic polynomial in x can be written as

$$p(x) = ax^2 + bx + c$$

If$a \neq 0$ and $b^2 \geq 4ac$ then the roots (that is, solutions to $p(x) = 0$ are given by the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

If we know one root, then we can compute the other as the roots add to $-\frac{b}{a}$.

In particular, if $a = 1$, b, c are integers and there is one integer root x, then $-b - x$ is the other root.

This technique is called *Vieta jumping*.

5.2 Markov Numbers

Markov's equation is

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

Obvious solutions are $x = y = z = 0$, $x = y = z = 1$. The Markov numbers are those that arise as integer solutions of Markov's equation.

Holding x and y constant, treat this as a quadratic equation in z, that is

$$z^2 - 3xyz + x^2 + y^2 = 0$$

This has two roots, say z and z'. The sum of those roots is $z + z' = 3xy$.

So given one solution (x, y, z) with $z < 3xy$ we can produce another solution (x, y, z'). Similarly, we could replace x with $x' = 3yz - x$ or y with $y' = 3xz - y$.

Do all integer solutions arise in this way?

6 Solution to IMO 1988 Problem 6

6.1 The Problem

Let a and b be positive integers such that:

$$\frac{a^2 + b^2}{1 + ab} = k$$

where k is also a positive integer. Show that k must be a perfect square.

We can apply Vieta jumping. Treat the equation as a quadratic in a. Two roots add to kb, so if (a, b) works, then so does $(kb - a, b)$.

6.2 Explicit Checking for Small k

Given a positive integer k, do there exist positive integers a, b such that

$$\frac{a^2 + b^2}{1 + ab} = k\ ?$$

Case $k = 1$: Only solution is $a = b = 1$. Locus in the real plane is an ellipse passing through $(1, 0)$ $(1, 1)$, $(0, 1)$, $(-1, 0)$, $(-1, -1)$, $(0, -1)$.

Case $k = 2$: Equation reduces to $(a - b)^2 = 2$. The locus in the plane is two straight lines. It is clear there are no integer solutions to $b = a \pm \sqrt{2}$.

Case $k = 3$: Can you see how to combine Fermat's method of descent with Vieta jumps to prove there are no solutions?

Case $k = 4$: Infinitely many solutions using Vieta jumping.

6.3 Reaching a Contradiction for non-square k

General case: Why do Vieta jumps and Fermat's descent principle exclude solutions unless k is a square?

Interesting Fact: One of the eleven young mathematicians who solved this problem in 1988 was Nicuşor Dan, who at the time of writing (November 2025) is the President of Romania.