PROOFS BY DESCENT

KEITH CONRAD

> *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.

1. Introduction

The method of descent is a technique developed by Fermat for proving certain equations have no (or few) integral solutions. The idea is to show that if there is an integral solution to an equation then there is another integral solution which is smaller in some way. Repeating this process and comparing the sizes of the successive solutions leads to an infinitely decreasing sequence

$$a_1 > a_2 > a_3 > \cdots$$

of positive integers, and that is impossible. Let's take a look at an example.

Example 1.1 (Euler)**.** We will show the equation $x^3 + 2y^3 + 4z^3 = 0$ has no solution in integers other than the obvious solution $(0, 0, 0)$. Assume there is a solution $(x, y, z) \neq (0, 0, 0)$, so at least one of x, y, and z is not 0. The equation tells us x^3 is even, so x is even. Write $x = 2x'$. Then $8x'^3 + 2y^3 + 4z^3 = 0$. Dividing by 2 and rearranging terms, we get $y^3 + 2z^3 + 4x'^3 = 0$. This is just like our original equation, with (x, y, z) replaced by (y, z, x'). Since y is now playing the role previously played by x, the argument used before on x shows y is even. Writing $y = 2y'$, substituting this in, and removing a common factor of 2, we get $z^3 + 2x'^3 + 4y'^3 = 0$. Therefore z is even, so $z = 2z'$. Substituting this in and simplifying, $x'^3 + 2y'^3 + 4z'^3 = 0$. Thus (x', y', z') fits the original equation and at least one of x', y' or z' is nonzero (corresponding to whichever of x, y, and z is nonzero). Since $0 < \max(|x'|, |y'|, |z'|) = (1/2)\max(|x|, |y|, |z|)$, we have produced a smaller integral solution measured by the maximum absolute value, which is a positive integer. This process can be repeated infinitely often, leading to a contradiction.

The same proof shows for any prime p that the equation $x^3 + py^3 + p^2z^3 = 0$ has no integral solution other than $(0, 0, 0)$. Indeed, if (x, y, z) fits the equation then $p|x^3$, so $p|x$ and we can proceed exactly as in the special case $p = 2$.

In Section 2 we will give proofs by descent that certain numbers are irrational. In Section 3 we will show the equation $a^4 + b^4 = c^4$ (a special

case of Fermat's Last Theorem) has no solution in positive integers using descent. In Section 4 we will use descent to show for any integer $k > 0$ other than 1 or 3, the equation $x^2+y^2+z^2 = kxyz$ has no integral solutions (x, y, z) besides $(0, 0, 0)$.

While descent may appear to be something like "reverse induction," it is not as widely applicable in the whole of mathematics as induction. Descent is nevertheless quite central to some important developments in number theory.

2. Irrationality by descent

Here is the usual proof that $\sqrt{2}$ is irrational, expressed using the idea of descent.

Example 2.1. We assume $\sqrt{2}$ is rational, so $\sqrt{2} = a/b$ with positive integers a and b. Squaring both sides and clearing the denominator, $2b^2 = a^2$. (This is an equation we want to show is not solvable in positive integers.) Since $2|a^2$, $2|a$. Write $a = 2a'$ for some positive integer a', so $2b^2 = 4a'^2$, which is the same as $b^2 = 2a'^2$. Thus $2|b^2$, so $2|b$. Write $b = 2b'$, so $4b'^2 = 2a'^2$, which is the same as $2b'^2 = a'^2$. Since a' and b' are positive, we have $\sqrt{2} = a'/b'$, so

$$\sqrt{2} = \frac{a}{b} = \frac{a'}{b'}.$$

Since $b = 2b'$ and both b and b' are positive, $0 < b' < b$, so we started with one rational expression for $\sqrt{2}$ and found another rational expression with a smaller (positive) denominator. Now we can repeat this process and obtain a sequence of rational expressions for $\sqrt{2}$ with decreasing positive denominators. This can't go on forever, so we have a contradiction.

The way this proof usually is written starts with $\sqrt{2} = a/b$ where the fraction is in lowest terms. Then the fact that $a = 2a'$ and $b = 2b'$, as shown in the theorem, is a contradiction since it means the fraction wasn't in lowest terms. The method of descent bypassed having to put the fraction in lowest terms, obtaining a contradiction in a different way.

Let's take a look at another proof by descent that $\sqrt{2}$ is irrational. We assume $\sqrt{2}$ is rational. Since $1 < \sqrt{2} < 2$, we can write

$$\sqrt{2} = 1 + \frac{m}{n}, \tag{2.1}$$

where m and n are positive integers with $0 < m/n < 1$, so $0 < m < n$. Squaring both sides of (2.1) and clearing the denominator,

$$2n^2 = n^2 + 2mn + m^2,$$

so $m^2 = n^2 - 2mn = n(n - 2m)$. Since m^2 and n are positive, so is $n - 2m$, and

$$\frac{m}{n} = \frac{n - 2m}{m}.$$

This lies between 0 and 1, by the definition of m/n, so $0 < n - 2m < m$. We have reached the descent step: the fractional part m/n of $\sqrt{2}$ has been written as a fraction $(n-2m)/m$ with a smaller denominator than before: $0 < m < n$. We can repeat this process again and again, eventually reaching a contradiction.

This proof by descent that $\sqrt{2}$ is irrational is not the same as the proof by descent in Example 2.1, since it does not use anything about even and odd numbers. It also generalizes nicely to other square roots.

Theorem 2.2. *If $d \in \mathbf{Z}^+$ and d is not a perfect square then $\sqrt{d}$ is irrational.*

Proof. (Dedekind, 1858) Suppose $\sqrt{d}$ is rational. Since d is not a perfect square, its square root lies between two consecutive integers. Let ℓ be the integer such that $\ell < \sqrt{d} < \ell + 1$. (Note ℓ is uniquely determined by $\sqrt{d}$.) Write

$$\sqrt{d} = \ell + \frac{m}{n},$$

where m and n are positive integers with $0 < m/n < 1$, so $0 < m < n$. Squaring both sides and clearing the denominator,

$$dn^2 = n^2\ell^2 + 2mn\ell + m^2,$$

so $m^2 = nq$, where $q = n(d - \ell^2) - 2m\ell$. Since m^2 and n are positive, q is positive. Then $m/n = q/m$, so

$$\sqrt{d} = \ell + \frac{m}{n} = \ell + \frac{q}{m}.$$

Since $q/m = m/n$, $0 < q/m < 1$, so $0 < q < m$. The fraction q/m has a smaller (positive) denominator than m/n, so from one representation $\sqrt{d} - \ell = m/n$ we get another representation $\sqrt{d} - \ell = q/m$ with a smaller (positive) denominator. This leads to a contradiction by repeating this process enough times. □

Here is another proof of Theorem 2.2, using descent in $\mathbf{Z}^2$ rather than in $\mathbf{Z}$. The argument is taken from [2].

Proof. Set $A = \left(\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right)$. Its characteristic polynomial is $\det(\lambda I_2 - A) = \lambda^2 - d$, with an eigenvalue $\sqrt{d}$ and associated eigenvector $\binom{\sqrt{d}}{1}$. Assuming $\sqrt{d}$ is rational, write $\sqrt{d} = a/b$ with nonzero integers a and b. Any scalar multiple of an eigenvector is an eigenvector, and $\binom{\sqrt{d}}{1} = \binom{a/b}{1}$ can be scaled to $\binom{a}{b}$. This is also an eigenvector of A: $A\binom{a}{b} = \binom{db}{a} = \sqrt{d}\binom{a}{b}$. Let ℓ be the integer such that $\ell < \sqrt{d} < \ell + 1$. Then

$$(A - \ell I_2)\begin{pmatrix} a \\ b \end{pmatrix} = \sqrt{d}\begin{pmatrix} a \\ b \end{pmatrix} - \ell\begin{pmatrix} a \\ b \end{pmatrix} = (\sqrt{d} - \ell)\begin{pmatrix} a \\ b \end{pmatrix},$$

where $\sqrt{d} - \ell$ lies between 0 and 1. The integral vector $\binom{a}{b}$ is an eigenvector of the integral matrix $A - \ell I_2$ with eigenvalue between 0 and 1.

Since $\binom{a}{b}$ is an eigenvector of $A-\ell I_2$, it is also an eigenvector of $(A-\ell I_2)^r$ for any $r \geq 1$, with eigenvalue $(\sqrt{d}-\ell)^r$:

$$(A-\ell I_2)^r \begin{pmatrix} a \\ b \end{pmatrix} = (\sqrt{d}-\ell)^r \begin{pmatrix} a \\ b \end{pmatrix}.$$

On the left side, for any $r \geq 1$ we have a vector in $\mathbf{Z}^2$ since A has integer entries and a, b, and ℓ are integers. On the right side we have a *nonzero* vector (since a, b, and $\sqrt{d}-\ell$ are nonzero) and it is getting arbitrarily small as r grows since $|\sqrt{d}-\ell| < 1$. So we have a sequence of nonzero vectors in $\mathbf{Z}^2$ with length shrinking to 0 (the descent idea). This is impossible, so we have a contradiction. □

We can extend the same proof to cube roots, using descent in $\mathbf{Z}^3$.

Theorem 2.3. *If $d \in \mathbf{Z}$ and d is not a perfect cube then $\sqrt[3]{d}$ is irrational.*

Proof. Suppose $\sqrt[3]{d} = a/b$ with nonzero integers a and b. Let

$$A = \begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} a^2 \\ ab \\ b^2 \end{pmatrix},$$

so $\det(\lambda I_3 - A) = \lambda^3 - d$ and $Av = (a/b)v = \sqrt[3]{d}v$.

Let $\ell \in \mathbf{Z}$ satisfy $\ell < \sqrt[3]{d} < \ell + 1$, so $(A - \ell I_3)v = (\sqrt[3]{d} - \ell)v$. Then

$$(A-\ell I_3)^r v = (\sqrt[3]{d}-\ell)^r v \tag{2.2}$$

for all $r \geq 1$. Since $v \in \mathbf{Z}^3$ and A has integer entries, the left side of (2.2) is a vector in $\mathbf{Z}^3$. Since $v \neq \mathbf{0}$ and $0 < \sqrt[3]{d} - \ell < 1$, the right side of (2.2) is nonzero and its length is tending to 0 as r grows. Thus, as $r \to \infty$, the nonzero vectors $(A - \ell I_3)^r v$ are a sequence in $\mathbf{Z}^3$ with length shrinking to 0. This is impossible, so $\sqrt[3]{d}$ must be irrational. □

Remark 2.4. In a similar way one can deal with higher roots: if $d \in \mathbf{Z}$ and $k \geq 2$ (with $d > 0$ if k is even) and d is not a kth power in $\mathbf{Z}$ then $\sqrt[k]{d}$ is irrational. Just assume $\sqrt[k]{d} = a/b$ is rational and use the $k \times k$ matrix and vector

$$A = \begin{pmatrix} 0 & d \\ I_{k-1} & 0 \end{pmatrix}, \quad v = \begin{pmatrix} a^{k-1} \\ a^{k-2}b \\ \vdots \\ b^{k-1} \end{pmatrix}.$$

3. Fermat's Last Theorem for $n = 4$

We will use descent to prove the exponent 4 case of Fermat's Last Theorem: the equation $a^4 + b^4 = c^4$ has no solution in positive integers. Fermat proved something more general, allowing a square and not just a fourth power on the right side.

Theorem 3.1 (Fermat)**.** *There is no solution to the equation $x^4 + y^4 = z^2$ in positive integers. In particular, the equation $a^4 + b^4 = c^4$ has no solution in positive integers.*

Proof. We will use the parametrization of primitive Pythagorean triples, so let's recall that: a primitive solution to $a^2 + b^2 = c^2$ where a, b, and c are positive integers with b even is

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

where $k > \ell$, $(k, \ell) = 1$, and $k \not\equiv \ell \bmod 2$.

Assume there is a solution to $x^4 + y^4 = z^2$ where x, y, and z are positive integers. If p is a common prime factor of x and y then $p^4|z^2$, so $p^2|z$. Then we can cancel the common factor of p^4 throughout and get a similar equation with smaller positive values of x, y, and z. Doing this enough times, we may suppose that $(x, y) = 1$. Then $(x, z) = 1$ and $(y, z) = 1$ too.

We will find a second positive integer solution (x', y', z') with $(x', y') = 1$ which is smaller in a suitable sense.

Since $x^4 + y^4 = z^2$ and $(x, y) = 1$, at least one of x and y is odd. They can't both be odd, since otherwise $z^2 \equiv 2 \bmod 4$, which has no solution. Without loss of generality, say x is odd and y is even. Then z is odd. Since $(x^2)^2 + (y^2)^2 = z^2$, (x^2, y^2, z) is a primitive Pythagorean triple with y^2 the even term, so by the formula for primitive triples we can write

$$x^2 = k^2 - \ell^2, \quad y^2 = 2k\ell, \quad z = k^2 + \ell^2, \tag{3.1}$$

where $k > \ell > 0$ and $(k, \ell) = 1$ (also $k \not\equiv \ell \bmod 2$, but we don't need this). The first equation in (3.1) says $x^2 + \ell^2 = k^2$. Since $(k, \ell) = 1$, (x, ℓ, k) is another primitive Pythagorean triple. Since x is odd, using the formula for primitive Pythagorean triples once again tells us

$$x = a^2 - b^2, \quad \ell = 2ab, \quad k = a^2 + b^2, \tag{3.2}$$

where $a > b > 0$ and $(a, b) = 1$. The second equation in (3.1) now says

$$y^2 = 4(a^2 + b^2)ab.$$

Since y is even,

$$\left(\frac{y}{2}\right)^2 = (a^2 + b^2)ab.$$

Since $(a, b) = 1$, the three factors on the right are pairwise relatively prime. They are all positive, so their product being a square means each one is a square:

$$a = x'^2, \quad b = y'^2, \quad a^2 + b^2 = z'^2, \tag{3.3}$$

where x', y', and z' can all be taken as positive. From $(a, b) = 1$, $(x', y') = 1$. The equation for z'^2 can be rewrittten as $x'^4 + y'^4 = z'^2$, so we have another solution to our original equation. Now we compare z' to z. Since

$$z' \leq z'^2 = a^2 + b^2 = k \leq k^2 < z,$$

measuring the size of positive integer solutions (x, y, z) by the size of z leads to a contradiction by descent. □

Remark 3.2. At the end of the proof a simple estimate showed $z > z'^2$. We can also get a formula for z in terms of x', y', and z' which explains this inequality. By (3.1), (3.2), and (3.3),

$$z = k^2 + \ell^2 = (a^2 + b^2)^2 + (2ab)^2 = z'^4 + 4x'^4y'^4,$$

so in fact $z > z'^4$, not just $z > z'^2$ as we found before.

Let's write x and y in terms of x', y', and z' too. From (3.2) and (3.3), $x = a^2 - b^2 = x'^4 - y'^4$, and $y^2 = 2k\ell = 2(a^2 + b^2)(2ab) = 4z'^2(x'y')^2$, so $y = 2x'y'z'$. This formula for y shows x' and y' are both less than y, so $0 < \max(x', y') < y \leq \max(x, y)$. Using $\max(x, y)$ rather than z to measure the size of a solution (x, y, z) is another way to get a contradiction for Theorem 3.1 by descent.

Our proof of Theorem 3.1 used the parametric formula for primitive Pythagorean triples twice. For a proof which does not explicitly appeal to this parametrization, see [1, pp. 55–56].

If we apply the descent technique for $x^4+y^4 = z^2$ to $a^4+b^4 = c^4$ directly, then the proof breaks down. The reason is that the descent step will not return another solution of $a^4 + b^4 = c^4$; the smaller c which comes out will only show up as a square, not a 4th power. So the added generality of dealing with $x^4 + y^4 = z^2$ is essential for the descent used above to work.

Elementary number theory books that discuss Fermat's Last Theorem for exponent 4 introduce the equation $x^4 + y^4 = z^2$ out of the blue, like we did, as if it were the most natural thing in the world to look at this equation instead of $a^4 + b^4 = c^4$. Fermat was actually thinking about $x^4 + y^4 = z^2$ not in order to solve $a^4 + b^4 = c^4$ but for an entirely different reason, and it was natural to consider the equation for that other problem. See Appendix A for more details.

Corollary 3.3. *The only rational solutions to* $y^2 = x^4 + 1$ *are* $(0, \pm 1)$.

Proof. Write x and y with a common denominator: $x = a/c$ and $y = b/c$ where c is nonzero. Then $b^2/c^2 = a^4/c^4 + 1$, so clearing the denominators gives $a^4 + c^4 = (bc)^2$. By Theorem 3.1, a or c or bc is 0. By its definition c is not zero. If $a = 0$ then $x = 0$, so $y^2 = 1$ and we get the solution $(0, \pm 1)$. If $b = 0$ then $a^4 + c^4 = 0$, so $c = 0$, which isn't true. Thus $(0, \pm 1)$ is the only rational solution. □

4. Markoff's equation

The Markoff equation, introduced by Markoff in 1880, is

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

One solution is $(1, 1, 1)$. Markoff's insight about this equation is that for such a triple (x, y, z), we can bring $3xyz$ to the left side to let us interpret

x as a root of the quadratic polynomial

$$T^2 - (3yz)T + (y^2 + z^2) = 0.$$

To find the second root of this equation besides x, we bypass the quadratic formula and think about relations between roots and coefficients. Letting the other root be r, our polynomial is $(T-x)(T-r) = T^2 - (x+r)T + xr$. Therefore $x + r = 3yz$, so the second root is $r = 3yz - x$. We have obtained from one solution (x, y, z) of Markoff's equation a second solution: $(3yz - x, y, z)$. Interchanging the roles of x, y, and z, we similarly get the additional solutions $(x, 3xz - y, z)$ and $(x, y, 3xy - z)$. From $(1, 1, 1)$ we can successively generate, for instance, $(2, 1, 1)$, $(2, 1, 5)$, and $(2, 29, 5)$. Markoff proved that all the solutions in positive integers to his equation can be produced in this way from $(1, 1, 1)$. His proof[1] can be found in [3].

We want to use descent for a different purpose, also taken from [3]. We will prove a theorem of Frobenius and Hurwitz which shows the special role of 3 as a coefficient on the right side of Markoff's equation.

Theorem 4.1. *For any positive integer k other than 1 or 3, the equation $x^2 + y^2 + z^2 = kxyz$ has no integral solution except $(0, 0, 0)$.*

Proof. First we will treat the case $k > 3$, returning later to $k = 2$.

Suppose a, b, and c satisfy $a^2 + b^2 + c^2 = kabc$. If any of a, b, or c is 0 then the equation says the sum of the squares of the other two is 0, so a, b, and c are all 0. Thus, assuming $(a, b, c) \neq (0, 0, 0)$ means a, b, and c are all nonzero. At least one of them is positive (otherwise the right side of the equation is negative). The other two are both positive or both negative, and in the negative case we can change their signs to get a solution where all are positive. So without loss of generality a, b, and c are all positive.

The numbers a, b, and c are distinct. To show, we argue by contradiction. Suppose (without loss of generality) that $a = b$. Then $2a^2 + c^2 = ka^2c$, so $a^2(kc - 2) = c^2$. Therefore $kc - 2$ is a rational square, hence an integral square. Write $kc - 2 = d^2$ with $d \geq 1$, so $kc = 2 + d^2$. Therefore $2a^2 + c^2 = (2 + d^2)a^2$, so $c^2 = d^2a^2$, so $c = da$. Now $d^2 = kc - 2 = k(da) - 2$, so $2 = d(ka - d)$, which means $d|2$, so d is 1 or 2. In either case we get $ka = 3$, which contradicts $k > 3$.

Without loss of generality, say $a > b > c \geq 1$. The triple $(kbc - a, b, c)$ is also a solution to $x^2 + y^2 + z^2 = kxyz$, and $kbc - a$ is positive since $a(kbc - a) = b^2 + c^2$ and $a > 0$. Which coordinate in $(kbc - a, b, c)$ is maximal? We know $b > c$ by design. Is $kbc - a > b$ or is $b > kbc - a$? We answer this by looking at the polynomial $f(x) = x^2 - (kbc)x + b^2 + c^2$. The roots of $f(x)$ are a and $kbc - a$, and

$$f(b) = 2b^2 + c^2 - kb^2c \leq 2b^2 + c^2 - kb^2 < 3b^2 - kb^2 = (3 - k)b^2 < 0.$$

[1]Markoff's proof uses descent, so this is an example of descent which proves a positive theorem. For other affirmative theorems by descent, see [4, Chap. 26, 30].

The region where f is negative is between its two roots. Thus b lies between a and $kbc - a$. Since $b < a$ we must have $kbc - a < b$, so

$$\max(kbc - a, b, c) = b < a = \max(a, b, c),$$

Repeating this construction, by descent we get a contradiction, so the equation $a^2 + b^2 + c^2 = kabc$ has only $(0, 0, 0)$ as an integer solution when $k > 3$.

Now we look at $k = 2$. Suppose $a^2 + b^2 + c^2 = 2abc$ with integers a, b, and c. Since $a^2 + b^2 + c^2$ is even, a, b, and c are not all odd. If exactly 1 of them is even then reducing both sides of the equation modulo 4 gives $2 \equiv 0 \bmod 4$, a contradiction. If exactly 2 are even then reducing modulo 2 gives $1 \equiv 0 \bmod 2$, another contradiction. Therefore a, b, and c are all even. Write $a = 2a'$, $b = 2b'$, and $c = 2c'$, so $a'^2 + b'^2 + c'^2 = 4a'b'c'$. This is the case $k = 4$, which we have already shown has no integral solution except $(0, 0, 0)$, so $(a, b, c) = (2a', 2b', 2c') = (0, 0, 0)$. □

What about $k = 1$? Looking at the equation $x^2 + y^2 + z^2 = xyz$ modulo 3 shows x, y, and z are all multiples of 3. Writing $x = 3x'$, $y = 3y'$, and $z = 3z'$ yields $x'^2 + y'^2 + z'^2 = 3x'y'z'$, so solutions to $x^2 + y^2 + z^2 = xyz$ are simply multiples of 3 times solutions of Markoff's equation.

Appendix A. Areas of Right Triangles

We saw in Section 3 that Fermat's Last Theorem for exponent 4 is a consequence of $x^4 + y^4 = z^2$ having no solution in positive integers. Here we will explain the background that led Fermat to this equation, which has nothing to do with Fermat's Last Theorem. Fermat was thinking about the following problems concerning areas of right triangles:

(1) Can a right triangle with integer side lengths have the same area as a square with integer side lengths?
(2) Can a right triangle with integer side lengths have twice the area of a square with integer side lengths?

Algebraically, if (a, b, c) is a Pythagorean triple we are asking if $(1/2)ab$ can be a perfect square or twice a perfect square.

The first question is connected with $x^4 - y^4 = z^2$ and the second question is connected with $x^4 + y^4 = z^2$. This is explained in Table 1. The first column shows how to turn a Pythagorean triple (a, b, c) such that $(1/2)ab$ is a perfect square into a positive integer solution of $x^4 - y^4 = z^2$. In the second column we turn such a solution (x, y, z) into a Pythagorean triple (a, b, c) such that $(1/2)ab$ is a perfect square. In the next two columns we turn Pythagorean triples (a, b, c) with $(1/2)ab$ being twice a perfect square into positive integer solutions of $x^4 + y^4 = z^2$ and *vice versa*. Note d in the fourth column is an integer since x or y must be even (otherwise $z^2 \equiv 2 \bmod 4$, which is impossible)

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

TABLE 1

The transformations we wrote down in the table from (a,b,c) to (x,y,z) and back again are not inverses to each other, but they at least show the existence of an integral right triangle having a certain kind of area is equivalent to the existence of a positive integer solution to a certain equation.

We showed by descent in Theorem 3.1 that $x^4+y^4=z^2$ has no solution in positive integers, so there is no integral right triangle whose area is twice a perfect square. The following theorem shows, in light of Table 1, that there is no integral right triangle with area equal to a perfect square.

Theorem A.1 (Fermat)**.** *There is no solution to $x^4-y^4=z^2$ in positive integers.*

Proof. We will argue by descent in a very similar style to the proof of Theorem 3.1. In particular, we will use the formula for primitive Pythagorean triples twice. Since now we have $z^2+y^4=x^4$ while in Theorem 3.1 we had $x^4+y^4=z^2$, the roles of x^2 and z basically get interchanged.

Assume $x^4-y^4=z^2$ with x, y, and z in $\mathbf{Z}^+$. There must be a solution with x, y, and z pairwise relatively prime (see the start of the proof of Theorem 3.1; the same argument there applies here), so we suppose this is the case. Since $x^4-y^4>0$, $x>y$.

There are two cases to consider: z odd and z even.

Case 1: z is odd. Since $z^2+y^4=x^4$ and z is odd, y must be *even*. (Otherwise $z^2+y^4\equiv 1+1\equiv 2 \bmod 4$, but 2 is not a 4th power modulo 4.) Since $(x,y)=1$, (z,y^2,x^2) is a primitive Pythagorean triple with y^2 the even term, so the formula for primitive Pythagorean triples says

$$z=k^2-\ell^2, \quad y^2=2k\ell, \quad x^2=k^2+\ell^2, \tag{A.1}$$

where $k>\ell>0$, $(k,\ell)=1$, and $k\not\equiv\ell \bmod 2$. The third equation in (A.1) says (k,ℓ,x) is a Pythagorean triple. Since $(k,\ell)=1$, this triple is primitive. One of k or ℓ is odd and the other is even. If k is odd, the formula for primitive Pythagorean triples says

$$k=a^2-b^2, \quad \ell=2ab, \quad x=a^2+b^2, \tag{A.2}$$

where $a>b>0$ and $(a,b)=1$. If ℓ is odd the formula says

$$\ell=a^2-b^2, \quad k=2ab, \quad x=a^2+b^2, \tag{A.3}$$

where $a > b > 0$ and $(a, b) = 1$ Using whichever of (A.2) or (A.3) is correct (depending on the parity of k and ℓ), the second equation in (A.1) becomes

$$y^2 = 4(a^2 - b^2)ab. \tag{A.4}$$

Since y is even, we can divide by 4 (in $\mathbf{Z}$):

$$\left(\frac{y}{2}\right)^2 = (a^2 - b^2)ab.$$

Since $(a, b) = 1$, the three factors on the right are pairwise relatively prime. They are all positive, so their product being a square means each one is a square:

$$a = x'^2, \quad b = y'^2, \quad a^2 - b^2 = z'^2, \tag{A.5}$$

where x', y', and z' can all be taken as positive. From $(a, b) = 1$, $(x', y') = 1$. The equation for z'^2 can be rewrittten as $x'^4 - y'^4 = z'^2$, so we have found another solution to our original equation. Now we compare z' to z. If (A.2) holds then

$$z' \leq z'^2 = a^2 - b^2 = k \leq k^2 < z.$$

If (A.3) holds then

$$z' \leq z'^2 = a^2 - b^2 = \ell \leq 4a^2b^2 = k^2 < z.$$

Since $z' < z$, by descent we have a contradiction.

Case 2: z is even. (This has no analogue in the proof of Theorem 3.1.)

Since $y^4 + z^2 = x^4$, we have a primitive Pythagorean triple (y^2, z, x^2) with even z. Thus

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

where m and n are positive and $(m, n) = 1$. Multiplying the first and third equations,

$$(xy)^2 = m^4 - n^4,$$

with xy odd. This expresses a square as the difference of two fourth powers, with the square being odd, so by Case 1 we have a contradiction. □

Remark A.2. In Case 1 we can solve for x, y, and z in terms of x', y', and z'. From (A.2) or (A.3), $x = a^2 + b^2$. This becomes, by (A.5), $x = x'^4 + y'^4$. From (A.4) and (A.5), $y^2 = 4(a^2 - b^2)ab = 4z'^2(x'^2y'^2) = (2x'y'z')^2$, so $y = 2x'y'z'$. Lastly, by (A.1), (A.2) or (A.3), and (A.5),

$$z = k^2 - \ell^2 = \pm((a^2 - b^2)^2 - (2ab)^2) = \pm(z'^4 - 4x'^4y'^4),$$

so $z = |z'^4 - 4x'^4y'^4|$. From the formula $y = 2x'y'z'$ we get $0 < \max(x', y') < y \leq \max(x, y)$, so using $\max(x, y)$ as a measure of the size of a positive integer solution is another way of reaching a contradiction by descent for Theorem A.1. This parallels Remark 3.2.

Corollary A.3. *There is no Pythagorean triple in which two of the terms are squares.*

Proof. Such a triple would give a solution in positive integers to either $x^4 + y^4 = z^2$ (the two legs are squares) or $x^4 = y^4 + z^2$ (a leg and hypotenuse are squares), but such solutions do not exist. □

There are many primitive Pythagorean triples where just one of the terms is a square. See Table 2.

a	b	c
3	**4**	5
7	24	**25**
9	40	41
16	63	65
17	**144**	145
225	272	353
161	240	**289**

TABLE 2. Pythagorean triples with a square term

Corollary A.4. *The only rational solutions to the equations* $y^2 = x^4 - 1$ *and* $u^2 + v^2 + u^2v^2 = 1$ *are* $(x, y) = (\pm 1, 0)$ *and* $(u, v) = (\pm 1, 0), (0, \pm 1)$.

Don't confuse $y^2 = x^4 - 1$ with $y^2 = x^4 + 1$ from Corollary 3.3.

Proof. Suppose $y^2 = x^4 - 1$ with rational x and y. Write $x = a/c$ and $y = b/c$ with common denominator $c \neq 0$. Clearing the denominator in the equation shows $(bc)^2 = a^4 - c^4$, so a square is a difference of fourth powers in $\mathbf{Z}$. This means one of the powers must be 0 by Theorem A.1. Since $c \neq 0$, either $b = 0$ or $a = 0$. If $b = 0$ then $y = 0$ and $x = \pm 1$, while if $a = 0$ there is a contradiction.

Now suppose $u^2 + v^2 + u^2v^2 = 1$ with rational u and v. Rewrite this as $u^2(1 + v^2) = 1 - v^2$. Multiplying both sides by $1 + v^2$ makes the equation $(u(1 + v^2))^2 = 1 - v^4$, which expresses a rational square as a difference of 4th powers. Clearing a common denominator leads to an integral square being equal to a difference of integral fourth powers. As before, one of the powers must vanish, so either $u = 0$ or $v = 0$. This leads to the indicated solutions. □

REFERENCES

[1] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge Univ. Press, Cambridge, 1991.

[2] D. Kalman, R. Mena, and S. Shahriari, "Variations on an Irrational Theme – Geometry, Dynamics, Algebra," Math. Mag. **70** (1997), 93–104.

[3] M. G. Krein, "Markov's Diophantine Equation," pp. 121–126 in *Kvant Selecta: Algebra and Analysis, I* (S. Tabachnikov, ed.), Amer. Math. Soc., Providence, 1991.

[4] J. H. Silverman, *A Friendly Introduction to Number Theory*, 3rd ed., Prentice-Hall, Englewood Cliffs, NJ, 2005.

[5] A. Weil, *Number Theory: An Approach Through History from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.