

# 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 two examples.

**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 certain equations have no solution in nonconstant rational functions. In a positive direction, descent will be used in Section 5 to show any prime  $p$  such that  $-1 \equiv \square \pmod{p}$  is a sum of two squares. In Section 6 we will argue by descent that 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

$$(2.1) \quad \sqrt{2} = 1 + \frac{m}{n},$$

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  $\ell$  be the integer such that  $\ell < \sqrt{d} < \ell + 1$ . (Note  $\ell$  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.  $\square$

Here is another proof of Theorem 2.2, using descent in  $\mathbf{Z}^2$  rather than in  $\mathbf{Z}$ . The argument is taken from [3].

*Proof.* Set  $A = \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$ . Its characteristic polynomial is  $\det(\lambda I_2 - A) = \lambda^2 - d$ , with an eigenvalue  $\sqrt{d}$  and associated eigenvector  $\begin{pmatrix} \sqrt{d} \\ 1 \end{pmatrix}$ . 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  $\begin{pmatrix} \sqrt{d} \\ 1 \end{pmatrix} = \begin{pmatrix} a/b \\ 1 \end{pmatrix}$  can be scaled to  $\begin{pmatrix} a \\ b \end{pmatrix}$ . This is also an eigenvector of  $A$ :  $A\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} db \\ a \end{pmatrix} = \sqrt{d}\begin{pmatrix} a \\ b \end{pmatrix}$ . Let  $\ell$  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  $\begin{pmatrix} a \\ b \end{pmatrix}$  is an eigenvector of the integral matrix  $A - \ell I_2$  with eigenvalue between 0 and 1.

Since  $\begin{pmatrix} a \\ b \end{pmatrix}$  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  $\ell$  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.  $\square$

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

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

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  $r \rightarrow \infty$ , 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.  $\square$

**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  $k$ th 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  $k \not\equiv \ell \pmod{2}$ .

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  $z^2 \equiv 2 \pmod{4}$ , 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

$$(3.1) \quad x^2 = k^2 - \ell^2, \quad y^2 = 2k\ell, \quad z = k^2 + \ell^2,$$

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

$$(3.2) \quad x = a^2 - b^2, \quad \ell = 2ab, \quad k = a^2 + b^2,$$

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:

$$(3.3) \quad a = x'^2, \quad b = y'^2, \quad a^2 + b^2 = z'^2,$$

where  $x'$ ,  $y'$ , and  $z'$  can all be taken as positive. From  $(a, b) = 1$ ,  $(x', y') = 1$ . The last equation in (3.3) can be rewritten as  $x'^4 + y'^4 = z'^2$ , so we have another solution to our original equation with  $(x', y') = 1$ . Now we compare  $z'$  to  $z$ . Since

$$0 < z' \leq z'^2 = a^2 + b^2 = k \leq k^2 < z,$$

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

**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  $x'$ ,  $y'$ , and  $z'$  are all less than  $y$ , so  $0 < \max(x', y', z') < y \leq \max(x, y, z)$ . Using  $\max(x, y, z)$  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 use this parametrization, see [1, pp. 55–56].

If we apply the descent technique for  $x^4 + y^4 = z^2$  to  $a^4 + b^4 = c^4$ , with a fourth power on the right side, 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 extra generality of dealing with  $x^4 + y^4 = z^2$  is essential for the descent to work as above.

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  $a^4 + b^4 = c^4$ . Of course it isn't. 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.

Now we present a number of corollaries to Theorem 3.1, concerning solvability of certain equations in integers or rationals. None of the proofs (which are mostly short) will involve descent. They are presented here simply to show Theorem 3.1 has uses other than Fermat's Last Theorem for exponent 4.

**Corollary 3.3.** *Any rational solution to  $x^4 + y^4 = z^2$  has  $x$  or  $y$  equal to 0.*

*Proof.* Assume  $x$  and  $y$  are both nonzero. Then  $z^2 > 0$ , so  $z \neq 0$  too. Write  $x = a/d$ ,  $y = b/d$ , and  $z = c/d$  with  $a, b, c, d \in \mathbf{Z}$  and  $d > 0$ . Then  $a, b$ , and  $c$  are nonzero. Clearing the denominator in  $x^4 + y^4 = z^2$ , we have  $a^4 + b^4 = (cd)^2$ . Changing signs if necessary,  $a, b$ , and  $cd$  are positive. Then we have a contradiction with Theorem 3.1.  $\square$

**Corollary 3.4.** *The only rational solutions to  $y^2 = x^4 + 1$  are  $(0, \pm 1)$ .*

*Proof.* Use Corollary 3.3 to see  $x = 0$ .  $\square$

**Corollary 3.5.** *The only rational solutions to  $2y^2 = x^4 - 1$  are  $(\pm 1, 0)$ .*

*Proof.* Squaring both sides,  $4y^4 = x^8 - 2x^4 + 1$ . Add  $4x^4$  to both sides and divide by 4 to get  $y^4 + x^4 = ((x^4 + 1)/2)^2$ . Since  $x \neq 0$  in the original equation, we can divide by  $x^4$  to get  $(y/x)^4 + 1 = ((x^4 + 1)/2x^2)^2$ . By Corollary 3.4,  $y/x = 0$ , so  $y = 0$  and therefore  $x = \pm 1$ .  $\square$

**Corollary 3.6.** *The integral solutions of  $x^4 - y^4 = 2z^2$  are  $(x, \pm x, 0)$ .*

*Proof.* If  $y = 0$  then  $x = z = 0$  since  $\sqrt{2}$  is irrational. If  $y \neq 0$ , then divide by  $y^4$  to get  $(x/y)^4 - 1 = 2(z/y^2)^2$ . By Corollary 3.5,  $z/y^2 = 0$ , so  $z = 0$  and therefore  $y = \pm x$ .  $\square$

**Corollary 3.7.** *The only rational solutions to  $y^2 = x^3 - 4x$  are  $(0, 0)$ ,  $(\pm 2, 0)$ .*

*Proof.* There is a bijection between solutions of  $y^2 = x^3 - 4x$  with  $x \neq 0$  and solutions to  $v^2 = u^4 + 1$  by

$$(x, y) \mapsto \left( \frac{y}{2x}, \frac{y^2 + 8x}{4x^2} \right), \quad (u, v) \mapsto \left( \frac{2}{v - u^2}, \frac{4u}{v - u^2} \right).$$

Since any rational solution to  $v^2 = u^4 + 1$  has  $u = 0$ , any rational solution to  $y^2 = x^3 - 4x$  has  $y = 0$ , so  $x = 0$  or  $x = \pm 2$ .  $\square$

**Corollary 3.8.** *The only rational solution to  $y^2 = x^3 + x$  is  $(0, 0)$ .*

*Proof.* Writing the equation as  $y^2 = x(x^2 + 1)$ , we see  $x = 0$  if and only if  $y = 0$ . Assume there is a rational solution other than  $(0, 0)$  so  $x \neq 0$  and  $y \neq 0$ . From the equation,  $x$  must be positive.

Write  $x$  and  $y$  in reduced form as  $x = a/b$  and  $y = c/d$  where  $b$  and  $d$  are positive. Clearing denominators in  $(c/d)^2 = (a/b)^3 + a/b$ , we get

$$b^3 c^2 = d^2 (a^3 + ab^2).$$

Therefore  $d^2 | b^3 c^2$ . Since  $(c, d) = 1$ ,  $d^2 | b^3$ . Also  $b^3 | d^2 (a^3 + ab^2)$ . Since  $(a, b) = 1$ ,  $b^3$  is relatively prime to  $a^3 + ab^2$ , so  $b^3 | d^2$ . Thus  $b^3 = d^2$ , so by unique factorization  $b = t^2$  and  $d = t^3$  for some positive integer  $t$ . Then  $(a, t) = 1$  and  $(c, t) = 1$ .

In the equation  $y^2 = x^3 + x$  with  $x = a/t^2$  and  $y = c/t^3$ , we get  $c^2 = a^3 + t^4 a = a(a^2 + t^4)$  after clearing the denominator. Since  $(a, t) = 1$ ,  $a$  and  $a^2 + t^4$  are relatively prime and positive. Their product is a square, so each factor is a square:

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

Thus  $u^4 + t^4 = v^2$ . By Theorem 3.1,  $u$  or  $t$  is 0. Since  $t \neq 0$ ,  $u = 0$  so  $x = 0$  and then  $y = 0$ .  $\square$

**Remark 3.9.** Conversely, Corollary 3.8 implies Theorem 3.1. If  $x^4 + y^4 = z^2$  in positive integers then multiplying through by  $x^2/y^6$  gives us  $(x/y)^6 + (x/y)^2 = (xz/y^3)^2$ , so  $Y^2 = X^3 + X$  for  $X = (x/y)^2$  and  $Y = xz/y^3$ . Since  $X$  is a nonzero rational number, we have a contradiction with Corollary 3.8.

Here is another theorem about fourth powers and squares proved by Fermat using descent.

**Theorem 3.10** (Fermat). *There is no solution to  $x^4 - y^4 = z^2$  in positive integers.*

*Proof.* We will argue by descent in a 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. For example, we will use descent on  $x^2$  (or equivalently, on  $x$ ) rather than on  $z$  as we did in Theorem 3.1.

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  $z^2 + y^4 \equiv 1 + 1 \equiv 2 \pmod{4}$ , 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

$$(3.4) \quad z = k^2 - \ell^2, \quad y^2 = 2k\ell, \quad x^2 = k^2 + \ell^2,$$

where  $k > \ell > 0$ ,  $(k, \ell) = 1$ , and  $k \not\equiv \ell \pmod{2}$ . The third equation in (3.4) says  $(k, \ell, x)$  is a Pythagorean triple. Since  $(k, \ell) = 1$ , this triple is primitive. One of  $k$  or  $\ell$  is odd and the other is even. If  $k$  is odd, the formula for primitive Pythagorean triples says

$$(3.5) \quad k = a^2 - b^2, \quad \ell = 2ab, \quad x = a^2 + b^2,$$

where  $a > b > 0$ ,  $(a, b) = 1$ , and  $a \not\equiv b \pmod{2}$ . If  $\ell$  is odd the formula says

$$(3.6) \quad \ell = a^2 - b^2, \quad k = 2ab, \quad x = a^2 + b^2,$$

where  $a > b > 0$ ,  $(a, b) = 1$ , and  $a \not\equiv b \pmod{2}$ . Using whichever of (3.5) or (3.6) is correct (depending on the parity of  $k$  and  $\ell$ ), the second equation in (3.4) becomes

$$(3.7) \quad y^2 = 4(a^2 - b^2)ab.$$

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:

$$(3.8) \quad a = x'^2, \quad b = y'^2, \quad a^2 - b^2 = z'^2,$$

where  $x', y'$ , and  $z'$  can all be taken as positive. From  $(a, b) = 1$ ,  $(x', y') = 1$ . The last equation in (3.8) can be rewritten as  $x'^4 - y'^4 = z'^2$ , so we have another solution to our original equation. Moreover,  $z'^2 = a^2 - b^2$  is odd, so our new solution again has an odd square on the right and we are still in Case 1. Now we compare  $x'$  to  $x$ :

$$0 < x' \leq x'^2 = a < a^2 + b^2 = x.$$

Since  $x' < x$ , 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.  $\square$

**Remark 3.11.** In Case 1 we can solve for  $x$ ,  $y$ , and  $z$  in terms of  $x'$ ,  $y'$ , and  $z'$ . From (3.5) or (3.6),  $x = a^2 + b^2$ . This becomes, by (3.8),

$$x = x'^4 + y'^4.$$

From (3.7) and (3.8),  $y^2 = 4(a^2 - b^2)ab = 4z'^2(x'^2y'^2) = (2x'y'z')^2$ , so

$$y = 2x'y'z'.$$

Lastly, by (3.4), (3.5) or (3.6), and (3.8),

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

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

Theorems 3.1 and 3.10 together lead to the following two results.

**Corollary 3.12.** *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 by Theorems 3.1 and 3.10.  $\square$

There are many primitive Pythagorean triples where just one of the terms is a square. See Table 1.

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

TABLE 1. Pythagorean triples with a square term

**Corollary 3.13.** *The only  $m \in \mathbf{Z}^+$  such that  $1 + 2 + 3 + \cdots + m$  is a fourth power is 1.*

*Proof.* Since  $1 + 2 + 3 + \cdots + m = m(m+1)/2$ , we are trying to solve  $m(m+1)/2 = n^4$ . Clearing the denominator,  $m(m+1) = 2n^4$ . Since  $m$  and  $m+1$  are relatively prime,

$$\{m, m+1\} = \{x^4, 2y^4\}$$



for some positive integers  $x$  and  $y$ , which must be relatively prime. Therefore  $x^4 - 2y^4 = \pm 1$ . Rewrite as  $y^4 = (x^4 \mp 1)/2$  and square both sides followed by a little algebra to get

$$(3.9) \quad y^8 \pm x^4 = \left( \frac{x^4 \pm 1}{2} \right)^2.$$

The right side is an integer since  $x$  is odd from  $x^4 = 2y^4 \pm 1$ . Equation (3.9) expresses a sum or difference of positive fourth powers as a perfect square. Using Theorems 3.1 and 3.10, we see this is impossible for a sum, and for a difference the square must be 0, so  $x = 1$  (since  $x > 0$ ). Therefore  $m = 1$ .  $\square$

Now we present consequences of Theorem 3.10 alone, paralleling the consequences of Theorem 3.1.

**Corollary 3.14.** *Any rational solution to  $x^4 - y^4 = z^2$  has  $y$  or  $z$  equal to 0.*

*Proof.* Similar to Corollary 3.3.  $\square$

**Corollary 3.15.** *The only rational solutions to  $y^2 = x^4 - 1$  are  $(\pm 1, 0)$ .*

*Proof.* Similar to Corollary 3.4.  $\square$

**Corollary 3.16.** *The only rational solutions to  $2y^2 = x^4 + 1$  are  $(\pm 1, \pm 1)$ .*

*Proof.* Squaring both sides,  $4y^4 = x^8 + 2x^4 + 1$ . Subtract  $4x^4$  from both sides and divide by 4 to get  $y^4 - x^4 = ((x^4 - 1)/2)^2$ . Since  $x \neq 0$  in the original equation, we can divide by  $x^4$  to get  $(y/x)^4 - 1 = ((x^4 - 1)/2x^2)^2$ . By Corollary 3.15,  $(x^4 - 1)/2x^2 = 0$ , so  $x = \pm 1$  and therefore  $y = \pm 1$ .  $\square$

**Corollary 3.17.** *The integral solutions of  $x^4 + y^4 = 2z^2$  are  $(x, \pm x, \pm x^2)$ .*

*Proof.* If  $y = 0$  then  $x = z = 0$  since  $\sqrt{2}$  is irrational. If  $y \neq 0$ , then divide by  $y^4$  to get  $(x/y)^4 + 1 = 2(z/y^2)^2$ . By Corollary 3.16,  $x/y = \pm 1$  and  $z/y^2 = \pm 1$ , so  $y = \pm x$  and  $z = \pm y^2 = \pm x^2$ .  $\square$

**Corollary 3.18.** *The only rational solutions to  $y^2 = x^3 + 4x$  are  $(0, 0)$  and  $(2, \pm 4)$ .*

*Proof.* A bijection between solutions of  $y^2 = x^3 + 4x$  with  $x \neq 0$  and solutions of  $v^2 = u^4 - 1$  is given by

$$(x, y) \mapsto \left( \frac{y}{2x}, \frac{y^2 - 8x}{4x^2} \right), \quad (u, v) \mapsto \left( \frac{2}{u^2 - v}, \frac{4u}{u^2 - v} \right).$$

Any rational solution to  $v^2 = u^4 - 1$  has  $v = 0$ , so any rational solution to  $y^2 = x^3 + 4x$  has  $x = 0$  or  $y^2 = 8x$ . The second case implies  $x^3 = 4x$ , so  $x = \pm 2$ . Only  $x = 2$  leads to a solution,  $(x, y) = (2, \pm 4)$ .  $\square$

**Corollary 3.19.** *The only rational solutions to  $y^2 = x^3 - x$  are  $(0, 0)$  and  $(\pm 1, 0)$ .*

*Proof.* This stands in relation to  $x^4 - y^4 = z^2$  in the same way that  $y^2 = x^3 + x$  does to  $x^4 + y^4 = z^2$  in Corollary 3.8. Details are left to the reader as an exercise.  $\square$

**Remark 3.20.** In the other direction, Corollary 3.19 implies Theorem 3.10. The argument is like that in Remark 3.9.

## 4. EQUATION WITH NO RATIONAL FUNCTION SOLUTION

There are many rational solutions to  $x^2 + y^2 = 1$ , like  $(x, y) = (3/5, 4/5)$  or  $(5/13, 12/13)$ . These solutions are nearly all described by a single parametric formula:  $x = 2t/(1+t^2)$  and  $y = (1-t^2)/(1+t^2)$  for some  $t \in \mathbf{Q}$ . Try  $t = 1/3, 1/4$ , and  $1/5$ . Algebraically, we have an identity of rational functions

$$\left(\frac{2t}{1+t^2}\right)^2 + \left(\frac{1-t^2}{1+t^2}\right)^2 = 1$$

and specializing  $t$  to rational numbers gives rational solutions to  $x^2 + y^2 = 1$ .<sup>1</sup>

However, it is not true that rational solutions to other equations can always be fit into a parametric formula using rational functions. For example, the equation  $y^2 = x^3 - 2$  has infinitely many rational solutions (two of them are  $(x, y) = (3, 5)$  and  $(129/100, 383/1000)$ ), but there are no rational functions  $f(t)$  and  $g(t)$  in  $\mathbf{Q}(t)$  such that  $g(t)^2 = f(t)^3 - 2$  other than constant functions, which “parametrize” only one solution (so really do not provide a parametric formula at all). To prove negative results like this we will use descent on the degree in a hypothetical nonconstant solution.

Several times we will need the following lemma.

**Lemma 4.1.** *If  $f(t)$  and  $g(t)$  in  $\mathbf{C}[t]$  are relatively prime and  $fg = \square$  in  $\mathbf{C}[t]$  then  $f = \square$  and  $g = \square$  in  $\mathbf{C}[t]$ .*

*Proof.* By unique factorization, the multiplicity of any irreducible factor of  $fg$  is even. Since  $f$  and  $g$  are relatively prime, it follows that the multiplicity of any irreducible factor of  $f$  is even and likewise for  $g$ . Therefore  $f$  and  $g$  are squares up to a nonzero scaling factor. Every nonzero complex number is the square of a complex number, so  $f$  and  $g$  are squares.  $\square$

This lemma easily extends by induction on the number of terms to a product of any finite number of polynomials in  $\mathbf{C}[t]$  which are pairwise relatively prime.

**Theorem 4.2.** *For distinct complex numbers  $r, r', r''$ , any solution to the equation  $y^2 = (x-r)(x-r')(x-r'')$  in rational functions  $x = f(t)$  and  $y = g(t)$  in  $\mathbf{C}(t)$  is a constant solution:  $f(t)$  and  $g(t)$  are in  $\mathbf{C}$ .*

The example  $y^2 = x^3 - 2$  which we discussed above is the special case where  $r, r'$ , and  $r''$  are the three cube roots of 2.

*Proof.* Our argument is adapted from [2, pp. 75–76].

Assume there is a solution in rational functions:  $x = p_1(t)/p_2(t)$  and  $y = q_1(t)/q_2(t)$  where  $p_1(t)$ ,  $p_2(t)$ ,  $q_1(t)$ , and  $q_2(t)$  are polynomials in  $\mathbf{C}[t]$ . Without loss of generality we can assume  $(p_1, p_2) = 1$  and  $(q_1, q_2) = 1$  in  $\mathbf{C}[t]$ .

Substituting the formulas for  $x$  and  $y$  into the equation  $y^2 = (x-r)(x-r')(x-r'')$ , we have

$$\frac{q_1^2}{q_2^2} = \left(\frac{p_1}{p_2} - r\right) \left(\frac{p_1}{p_2} - r'\right) \left(\frac{p_1}{p_2} - r''\right) = \frac{(p_1 - rp_2)(p_1 - r'p_2)(p_1 - r''p_2)}{p_2^3},$$

so after clearing denominators

$$(4.1) \quad p_2^3 q_1^2 = (p_1 - rp_2)(p_1 - r'p_2)(p_1 - r''p_2) q_2^2.$$

<sup>1</sup>This method produces all the rational solutions to  $x^2 + y^2 = 1$  except for  $(0, -1)$ , but we will not show that here.

Since  $(p_1, p_2) = 1$ , the factors  $p_1 - rp_2$ ,  $p_1 - r'p_2$ , and  $p_1 - r''p_2$  are relatively prime to  $p_2$  (why?). Thus by (4.1),  $p_2^3 | q_2^2$ . Since  $(q_1, q_2) = 1$ ,  $q_2^2 | p_2^3$ , so  $p_2^3 = cq_2^2$  for some nonzero  $c \in \mathbf{C}$ . Since  $c$  is a square in  $\mathbf{C}$ ,  $p_2^3$  is a square in  $\mathbf{C}[t]$ . That implies  $p_2$  is a square by unique factorization in  $\mathbf{C}[t]$ . Write  $p_2 = f_2^2$ .

Substituting  $cq_2^2$  for  $p_2^3$  in (4.1) and cancelling  $q_2^2$  from both sides,

$$cq_1^2 = (p_1 - rp_2)(p_1 - r'p_2)(p_1 - r''p_2).$$

The factors on the right side are pairwise relatively prime since  $(p_1, p_2) = 1$  (why?) and the numbers  $r$ ,  $r'$ , and  $r''$  are distinct, so by an extension of Lemma 4.1 to a product of three terms,  $p_1 - rp_2$ ,  $p_1 - r'p_2$ , and  $p_1 - r''p_2$  are all squares in  $\mathbf{C}[t]$ . Since  $p_2 = f_2^2$ ,

$$p_1 - rf_2^2 = \square, \quad p_1 - r'f_2^2 = \square, \quad p_1 - r''f_2^2 = \square.$$

Writing the first equation as  $p_1 - rf_2^2 = f_1^2$ , the second and third equations become

$$(4.2) \quad f_1^2 - (r' - r)f_2^2 = \square, \quad f_1^2 - (r'' - r)f_2^2 = \square.$$

The coefficients  $r' - r$  and  $r'' - r$  are nonzero and distinct. We want to show  $f_1$  and  $f_2$  are constants.

Now we set up our descent statement, based on (4.2): we will show for all distinct  $a$  and  $b$  in  $\mathbf{C}$  that relatively prime polynomials  $g_1$  and  $g_2$  in  $\mathbf{C}[t]$  which satisfy

$$(4.3) \quad g_1^2 - ag_2^2 = \square, \quad g_1^2 - bg_2^2 = \square$$

must both be constant. Note (4.2) is a special case of this.

Assume for some  $a$  and  $b$  that there is a solution  $(g_1, g_2)$  to (4.3) where  $g_1$  or  $g_2$  is not constant. In (4.3), write  $a = c^2$  and  $b = d^2$  with  $c$  and  $d$  in  $\mathbf{C}$ . Since  $a \neq b$ ,  $c \neq \pm d$ . We can rewrite (4.3) as

$$(4.4) \quad (g_1 + cg_2)(g_1 - cg_2) = \square, \quad (g_1 + dg_2)(g_1 - dg_2) = \square.$$

A common factor of  $g_1 + cg_2$  and  $g_1 - cg_2$  is a factor of both  $g_1$  and  $g_2$  (why?), so it is constant since  $(g_1, g_2) = 1$ . Therefore the factors on the left side of the first equation in (4.4) are relatively prime, and the product of the factors is a square, so by Lemma 4.1

$$(4.5) \quad g_1 + cg_2 = h_1^2, \quad g_1 - cg_2 = h_2^2,$$

where  $h_1$  and  $h_2$  are relatively prime. Adding and subtracting the equations in (4.5),  $g_1 = (h_1^2 + h_2^2)/2$  and  $g_2 = (h_1^2 - h_2^2)/(2c)$ . Since  $g_1$  or  $g_2$  is not constant,  $h_1$  or  $h_2$  is not constant.

Arguing in a similar way with the second equation in (4.4),

$$(4.6) \quad g_1 + dg_2 = \square, \quad g_1 - dg_2 = \square.$$

Substituting the formulas for  $g_1$  and  $g_2$  in terms of  $h_1$  and  $h_2$  into (4.6),

$$\frac{1}{2} \left(1 + \frac{d}{c}\right) h_1^2 + \frac{1}{2} \left(1 - \frac{d}{c}\right) h_2^2 = \square, \quad \frac{1}{2} \left(1 - \frac{d}{c}\right) h_1^2 + \frac{1}{2} \left(1 + \frac{d}{c}\right) h_2^2 = \square.$$

The numbers  $1 \pm d/c$  are nonzero since  $c \neq \pm d$ , so we can divide by the coefficient of  $h_1^2$ :

$$h_1^2 + \frac{1 - d/c}{1 + d/c} h_2^2 = \square, \quad h_1^2 + \frac{1 + d/c}{1 - d/c} h_2^2 = \square.$$

Set  $a' = -(1 - d/c)/(1 + d/c)$  and  $b' = -(1 + d/c)/(1 - d/c) = 1/a'$ . Both  $a'$  and  $b'$  are nonzero,  $a' \neq b'$ , and

$$(4.7) \quad h_1^2 - a'h_2^2 = \square, \quad h_1^2 - b'h_2^2 = \square.$$

From (4.5),  $2 \deg h_1 \leq \max(\deg g_1, \deg g_2)$  and  $2 \deg h_2 \leq \max(\deg g_1, \deg g_2)$ . Therefore

$$(4.8) \quad 0 < \max(\deg h_1, \deg h_2) \leq \frac{1}{2} \max(\deg g_1, \deg g_2).$$

We can now repeat the argument leading from (4.3) to (4.7) with  $h_1, h_2, a', b'$  in place of  $g_1, g_2, a, b$ . Each repetition leads to a new version of (4.8) where the maximum degree in the new solution is positive and smaller than the maximum degree in the previous solution. By descent this leads to a contradiction (positive degrees can't strictly drop forever), so any solution to (4.3) in relatively prime polynomials  $g_1$  and  $g_2$  must be a constant solution. What this tells us in (4.2) is that  $f_1$  and  $f_2$  are both constant, so  $p_1 = f_1^2 + r f_2^2$  and  $p_2 = f_2^2$  are constant. That makes  $x = p_1/p_2$  constant, so the equation  $y^2 = (x-r)(x-r')(x-r'')$  implies that  $y^2 = (q_1/q_2)^2$  is constant. Therefore the rational function  $y = q_1/q_2$  is constant.  $\square$

**Corollary 4.3.** *Let  $F(x)$  be a polynomial with coefficients in  $\mathbf{C}$  of degree 3 or 4 which has distinct roots. Any solution to the equation  $y^2 = F(x)$  where  $x$  and  $y$  are in  $\mathbf{C}(t)$  has  $x \in \mathbf{C}$  and  $y \in \mathbf{C}$ .*

*Proof.* First suppose  $F(x)$  has degree 3. In factored form  $F(x) = c(x-r)(x-r')(x-r'')$  where the roots  $r, r',$  and  $r''$  are distinct and  $c \neq 0$ .<sup>2</sup> In  $\mathbf{C}$ ,  $c$  is a square, so the equation

$$(4.9) \quad y^2 = c(x-r)(x-r')(x-r'')$$

can be scaled to  $Y^2 = (x-r)(x-r')(x-r'')$  where  $Y = y/\sqrt{c}$ . If there is a solution to (4.9) where  $x, y \in \mathbf{C}(t)$  then  $Y \in \mathbf{C}(t)$ . By Theorem 4.2,  $x \in \mathbf{C}$  and  $Y \in \mathbf{C}$ , so  $y \in \mathbf{C}$ .

Next suppose  $F(x)$  has degree 4 with distinct roots  $r, r', r'',$  and  $r'''$ . In factored form

$$F(x) = c(x-r)(x-r')(x-r'')(x-r'''),$$

where  $c \neq 0$ . Suppose we can solve

$$(4.10) \quad y^2 = c(x-r)(x-r')(x-r'')(x-r''')$$

where  $x, y \in \mathbf{C}(t)$ . The roots of  $F$  are distinct, so without loss of generality  $x \neq r'''$ . Dividing through (4.10) by  $(x-r''')^4$ ,

$$\begin{aligned} \frac{y^2}{(x-r''')^4} &= c \left( \frac{x-r}{x-r'''} \right) \left( \frac{x-r'}{x-r'''} \right) \left( \frac{x-r''}{x-r'''} \right) \\ &= c \left( 1 + \frac{r'''-r}{x-r'''} \right) \left( 1 + \frac{r'''-r'}{x-r'''} \right) \left( 1 + \frac{r'''-r''}{x-r'''} \right). \end{aligned}$$

Set  $X = 1/(x-r''')$  and  $Y = y/(x-r''')^2$ , so  $X$  and  $Y$  are in  $\mathbf{C}(t)$ . Then

$$Y^2 = c(1 + (r'''-r)X)(1 + (r'''-r')X)(1 + (r'''-r'')X),$$

where the right side is cubic in  $X$  with distinct roots. By the cubic case we already discussed,  $X \in \mathbf{C}$  and  $Y \in \mathbf{C}$ , so  $x \in \mathbf{C}$  and  $y \in \mathbf{C}$ .  $\square$

---

<sup>2</sup>The only difference between this case and Theorem 4.2 is that we now allow a leading coefficient other than 1.

## 5. SUMS OF TWO SQUARES

We have used descent so far to prove “negative” theorems, which say certain equations have no (or very few) solutions of a certain type. At first, Fermat’s applications of descent all had this flavor.<sup>3</sup> He eventually discovered descent could be used to prove “positive” theorems, such as the following.

**Theorem 5.1.** *For a prime  $p$ , if  $-1 \equiv \square \pmod{p}$  then we can write  $p$  as a sum of two squares:  $p = x^2 + y^2$  for some  $x$  and  $y$  in  $\mathbf{Z}$ .*

*Proof.* Write  $-1 \equiv s^2 \pmod{p}$ . Without loss of generality,  $1 \leq s \leq p/2$ , so  $s^2 + 1 = pd$  with  $d \in \mathbf{Z}$ . Since  $s^2 + 1 \leq p^2/4 + 1 < p^2$ ,  $0 < d < p$ . So our hypothesis tells us a certain multiple of  $p$  is a sum of two squares and the multiplying factor is less than  $p$ . If  $d = 1$  then we are done.

If  $d > 1$ , we will show that  $pd'$  is a sum of two squares for some integer  $d'$  such that  $0 < d' < d$ . Then repeating the argument, by descent eventually we must reach  $d = 1$ , so  $p \cdot 1 = p$  is a sum of two squares.

To make our descent step recursive, we don’t work with the specific equation  $pd = s^2 + 1$  but more generally

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

where  $0 < k < p$ . (For  $k = d$  this holds with  $x = s$  and  $y = 1$ , so such an equation does exist for some choice of  $k$ .) If  $k > 1$ , we want to produce another equation of this form where  $k$  is smaller. Reduce  $x$  and  $y$  modulo  $k$ :  $x \equiv r \pmod{k}$  and  $y \equiv r' \pmod{k}$ , where  $|r|, |r'| \leq k/2$ . Squaring and adding,

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

so

$$r^2 + r'^2 = k\ell$$

for integer  $\ell \geq 0$ . Let’s show  $r$  or  $r'$  is not 0, so  $\ell > 0$ . If  $r = 0$  and  $r' = 0$  then  $k|x$  and  $k|y$ , so  $k^2$  divides  $x^2 + y^2 = kp$ , so  $k|p$ , but this is not true since  $0 < k < p$  and  $p$  is prime. Now let’s bound  $\ell$  from above. From the bounds on  $|r|$  and  $|r'|$ ,

$$k\ell = r^2 + r'^2 \leq \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2} < k^2,$$

so  $0 < \ell < k$ . We will show  $p\ell$  is a sum of two squares.

Since

$$(pk)(k\ell) = (x^2 + y^2)(r^2 + r'^2) = (x^2 + y^2)(r'^2 + r^2) = (xr' - yr)^2 + (xr + yr')^2.$$

Modulo  $k$ ,  $xr' - yr \equiv xy - yx \equiv 0$  and  $xr + yr' \equiv r^2 + r'^2 \equiv 0$ . Therefore  $xr' - yr$  and  $xr + yr'$  are multiples of  $k$ , so we can write

$$pk^2\ell = (ka)^2 + (kb)^2$$

for some positive integers  $a$  and  $b$ . Dividing by  $k^2$ ,  $p\ell = a^2 + b^2$ . This completes our descent step, since  $0 < \ell < k$ .  $\square$

**Remark 5.2.** Fermat’s own proof by descent of Theorem 5.1 was based on counterexamples: assuming some odd  $p$  with  $-1 \equiv \square \pmod{p}$  is not a sum of two squares, Fermat said he could show there has to be a smaller prime with the same property, and thus by descent we eventually will obtain that 5 is not a sum of two squares, but it is, so we have a contradiction.

<sup>3</sup>Almost none of Fermat’s proofs are known in detail, but he did include in letters that statements of some propositions that he established with descent.

## 6. 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 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  $r = 3yz - x$ . 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, which uses descent, can be found in [4].

We want to use descent for a different purpose, also taken from [4]. 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 6.1.** *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 this, 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

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

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

$$0 < \max(kbc - a, b, c) = b < a = \max(a, b, c),$$

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  $2 \equiv 0 \pmod{4}$ , a contradiction. If exactly 2 are even then reducing modulo 2 gives  $1 \equiv 0 \pmod{2}$ , 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  $(a, b, c) = (2a', 2b', 2c') = (0, 0, 0)$ .  $\square$

Why is  $k = 1$  not considered in Theorem 6.1? Looking at the equation  $x^2 + y^2 + z^2 = xyz$  modulo 3 shows  $x$ ,  $y$ , and  $z$  are all multiples of 3 (check!). Writing  $x = 3x'$ ,  $y = 3y'$ , and  $z = 3z'$  yields  $x'^2 + y'^2 + z'^2 = 3x'y'z'$ , so any integral solution to  $x^2 + y^2 + z^2 = xyz$  is simply 3 times an integral solution 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 2. 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  $z^2 \equiv 2 \pmod{4}$ , which is impossible)

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

TABLE 2

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 Theorems 3.1 and 3.10 that  $x^4 \pm y^4 = z^2$  has no solution in positive integers, so there are no integral right triangles whose area is a perfect square or twice a perfect square.

## APPENDIX B. ANOTHER DESCENT WITH SUMS OF TWO SQUARES

We will prove a theorem by descent where rational solvability of an equation implies integral solvability.

**Theorem B.1.** *Let  $n \in \mathbf{Z}^+$ . If  $n$  is a sum of two rational squares then it is a sum of two integral squares.*

This is saying: if  $n = x^2 + y^2$  has a solution in fractions then it also has a solution in integers.

**Example B.2.** We have  $193 = (933/101)^2 + (1048/101)^2 = (83/109)^2 + (1512/109)^2$  and  $193 = 7^2 + 12^2$ .

*Proof.* Our descent argument is taken from [5, App. II, Chap. III], and the main idea goes back to L. Aubry (1912).

Suppose  $n = r_1^2 + r_2^2$  with fractions  $r_1$  and  $r_2$ . If  $r_1$  and  $r_2$  are in  $\mathbf{Z}$ , we're done, so we assume at least one of them is not in  $\mathbf{Z}$ . Write the  $r_i$ 's with a common denominator:  $r_1 = a_1/b$  and  $r_2 = a_2/b$ , where the  $a_1$ ,  $a_2$ , and  $b$  are in  $\mathbf{Z}$  and  $b > 1$ . We want to write  $n = r_1'^2 + r_2'^2$  where  $r_1'$  and  $r_2'$  are fractions with a common denominator less than  $b$ . Repeating this enough times, we will eventually get a common denominator of 1, meaning we have written  $n$  as a sum of integral squares.

The point  $(r_1, r_2)$  lies on the circle  $x^2 + y^2 = n$ . Pick a nearby  $\mathbf{Z}$ -point in the plane: choose  $k_1$  and  $k_2$  in  $\mathbf{Z}$  such that  $|r_i - k_i| \leq 1/2$ . Since  $r_1$  and  $r_2$  are not both in  $\mathbf{Z}$ ,  $(r_1, r_2) \neq (k_1, k_2)$ , so there is a line through these two points. This line meets the circle  $x^2 + y^2 = n$  in the point  $(r_1, r_2)$ . We will show this line meets the circle in a second point with rational coordinates having a smaller common denominator than  $b$  (a common denominator of the coordinates of the point  $(r_1, r_2)$ ).

First let's check the line through  $(r_1, r_2)$  and  $(k_1, k_2)$  meets  $x^2 + y^2 = n$  in a second point. We argue by contradiction. If the line only meets the circle at  $(r_1, r_2)$  then the line is tangent to the circle at  $(r_1, r_2)$ , so the three points  $(r_1, r_2)$ ,  $(k_1, k_2)$ , and  $(0, 0)$  are the vertices of a right triangle (a tangent line to a point on a circle is always perpendicular to the line connecting the origin to the point of tangency). Then the Pythagorean theorem tells us

$$k_1^2 + k_2^2 = (r_1^2 + r_2^2) + ((k_1 - r_1)^2 + (k_2 - r_2)^2) = n + ((k_1 - r_1)^2 + (k_2 - r_2)^2).$$

Both  $k_1^2 + k_2^2$  and  $n$  are integers, so  $(k_1 - r_1)^2 + (k_2 - r_2)^2$  is an integer. However,  $|k_1 - r_1|$  and  $|k_2 - r_2|$  are both less than  $1/2$ , so  $0 \leq (k_1 - r_1)^2 + (k_2 - r_2)^2 \leq (1/2)^2 + (1/2)^2 = 1/2$ . Then the only way  $(k_1 - r_1)^2 + (k_2 - r_2)^2$  could be an integer is if it is 0, which forces  $r_1 = k_1$  and  $r_2 = k_2$ . However, we are supposing  $r_1$  and  $r_2$  are not both integers, so we have a contradiction.



Now let's look more closely at the algebraic formula for the squared distance between  $(r_1, r_2)$  and  $(k_1, k_2)$ . This number, which is positive, equals

$$\begin{aligned}
 (r_1 - k_1)^2 + (r_2 - k_2)^2 &= \left(\frac{a_1}{b} - k_1\right)^2 + \left(\frac{a_2}{b} - k_2\right)^2 \\
 &= \left(\frac{a_1}{b}\right)^2 + \left(\frac{a_2}{b}\right)^2 - \frac{2(a_1 k_1 + a_2 k_2)}{b} + k_1^2 + k_2^2 \\
 &= n - \frac{2(a_1 k_1 + a_2 k_2)}{b} + k_1^2 + k_2^2 \\
 &= n + k_1^2 + k_2^2 - \frac{2(a_1 k_1 + a_2 k_2)}{b}.
 \end{aligned}$$

We can write this fraction in the form  $b'/b$ , where

$$b' := b(n + k_1^2 + k_2^2) - 2(a_1 k_1 + a_2 k_2) \in \mathbf{Z}$$

and

$$(r_1 - k_1)^2 + (r_2 - k_2)^2 = \frac{b'}{b} \implies (a_1 - b k_1)^2 + (a_2 - b k_2)^2 = b b'.$$

We will show the line through  $(r_1, r_2)$  and  $(k_1, k_2)$  meets  $x^2 + y^2 = n$  in a rational point whose coordinates have  $b'$  as a common denominator. Since  $(r_1 - k_1)^2 + (r_2 - k_2)^2 \leq (1/2)^2 + (1/2)^2 = 1/2$ , we have  $0 < b'/b \leq 1/2$ , so

$$0 < b' \leq \frac{b}{2} < b.$$

The line through  $(r_1, r_2)$  and  $(k_1, k_2)$  can be described parametrically by

$$(B.1) \quad L(t) = (k_1 + (r_1 - k_1)t, k_2 + (r_2 - k_2)t).$$

This meets  $x^2 + y^2 = n$  at  $t = 1$  ( $L(1) = (r_1, r_2)$ ). Where else does it meet the circle? To find out, we solve for  $t$  in

$$\begin{aligned}
 n &= (k_1 + (r_1 - k_1)t)^2 + (k_2 + (r_2 - k_2)t)^2 \\
 &= k_1^2 + 2k_1(r_1 - k_1)t + (r_1 - k_1)^2 t^2 + k_2^2 + 2k_2(r_2 - k_2)t + (r_2 - k_2)^2 t^2 \\
 &= k_1^2 + k_2^2 + 2(k_1 r_1 - k_1^2 + k_2 r_2 - k_2^2)t + ((r_1 - k_1)^2 + (r_2 - k_2)^2)t^2 \\
 &= k_1^2 + k_2^2 + 2(k_1 r_1 + k_2 r_2 - (k_1^2 + k_2^2))t + ((r_1 - k_1)^2 + (r_2 - k_2)^2)t^2 \\
 &= k_1^2 + k_2^2 + \frac{2(a_1 k_1 + a_2 k_2) - 2b(k_1^2 + k_2^2)}{b}t + \frac{(a_1 - b k_1)^2 + (a_2 - b k_2)^2}{b^2}t^2.
 \end{aligned}$$

Using the definition of  $b'$  to rewrite the coefficients of  $t$  and  $t^2$ , we have

$$\begin{aligned}
 n &= k_1^2 + k_2^2 + \frac{b(n + k_1^2 + k_2^2) - b' - 2b(k_1^2 + k_2^2)}{b}t + \frac{b'}{b}t^2 \\
 &= k_1^2 + k_2^2 + \left(n - (k_1^2 + k_2^2) - \frac{b'}{b}\right)t + \frac{b'}{b}t^2.
 \end{aligned}$$

Bringing all terms to the right side,

$$0 = \frac{b'}{b}t^2 + \left(n - (k_1^2 + k_2^2) - \frac{b'}{b}\right)t + k_1^2 + k_2^2 - n.$$

This has a root at  $t = 1$  (because  $L(1)$  is on the circle, but it can also be seen algebraically), so we know  $t - 1$  is a factor on the right, leading to

$$0 = (t - 1) \left( \frac{b'}{b}t + n - (k_1^2 + k_2^2) \right).$$

Thus the second point of intersection of the line  $L(t)$  with the circle  $x^2 + y^2 = n$  is at

$$t = \frac{b(k_1^2 + k_2^2 - n)}{b'}.$$

Feeding this value of  $t$  into (B.1), and writing  $r_i$  as  $a_i/b$ , we get the point

$$L\left(\frac{b(k_1^2 + k_2^2 - n)}{b'}\right) = \left(k_1 + \frac{(a_1 - bk_1)(k_1^2 + k_2^2 - n)}{b'}, k_2 + \frac{(a_2 - bk_2)(k_1^2 + k_2^2 - n)}{b'}\right),$$

which shows this second point of intersection of the line and circle is a rational point and  $b'$  is a common denominator for its coordinates. We noted earlier that  $0 < b' \leq b/2 < b$ , so the common denominator for this new rational point on  $x^2 + y^2 = n$  is smaller than that for  $(r_1, r_2)$ , so we are done.  $\square$

The proof of Theorem B.1 works for a sum of three squares, using lines and spheres in three dimensions. That is, an integer which is a sum of three rational squares is also a sum of three integral squares. The only change to be made in the proof is the following: now we have  $|a_i/b - k_i| \leq 1/2$  for  $i = 1, 2, 3$ , and  $(a_1/b - k_1)^2 + (a_2/b - k_2)^2 + (a_3/b - k_3)^2 \leq 3/4$  instead of  $1/2$ . So the new rational point on the sphere  $x^2 + y^2 + z^2 = n$  will have a common denominator  $b' \leq (3/4)b$ , which is still less than  $b$ , which means everything still works in the proof when it is done for sums of three squares.

It is a theorem of Lagrange (1770) that every positive integer is a sum of four squares. This is called the four-square theorem and it suggests an analogue of Theorem B.1 for four squares is pointless. But historically it went the other way: Euler (1751) was able to prove every positive integer is a sum of four rational squares and could not figure out how to use this to prove every positive integer is a sum of four integral squares. After Lagrange's proof of the four-square theorem, Euler realized how he could make a descent argument work and thereby deduce Lagrange's integral four-square theorem from his own rational four-square theorem.

Theorem B.1 is no longer true if we replace sums of two squares by slightly different algebraic expressions. For example, the equation  $x^2 + 82y^2 = 2$  has no integral solutions, but it has the rational solution  $(x, y) = (4/7, 1/7)$ . The equation  $x^3 + y^3 = 13$  has no integral solutions but it has the rational solution  $(x, y) = (7/3, 2/3)$ .

## REFERENCES

- [1] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge Univ. Press, Cambridge, 1991.
- [2] H. Clemens, *A Scrapbook of Complex Curve Theory*, 2nd ed., Amer. Math. Soc., 2003.
- [3] D. Kalman, R. Mena, and S. Shahriari, "Variations on an Irrational Theme – Geometry, Dynamics, Algebra," *Math. Mag.* **70** (1997), 93–104.
- [4] 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.
- [5] A. Weil, *Number Theory: An Approach Through History from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.