5 Fermat's Method of Descent

The *method of infinite descent* is a standard approach to Diophantine equations. Feeling somewhat like induction in reverse, arguments of this type have been known for millenia, though credit for the method's popularisation is often given to Pierre de Fermat who used it regularly. The method is essentially a combination of two ideas:

Well-ordering/least positive integer principle Any non-empty set of positive integers has a minimum.

Descent Given a solution to an equation in positive integers, construct a *smaller* solution.

There are two standard applications, though the approach is similar in both.

1. To show that an equation has *no solutions*. If a solution exists in positive integers, there must be a minimal such: constructing a smaller solution contradicts minimality.

2. To show the *existence* of, or *construct solutions* to, an equation. By starting with a solution to a related equation, we produce a smaller solution to the equation we desire.

5.1 Contradiction by Descent: Fermat's Last Theorem

We start with a very simple example of the method.

Example 5.1. The equation[a] $x^2 + y^2 = 3z^2$ has no solutions (x, y, z) in integers where $z \neq 0$.

Suppose we have a solution (x, y, z). Without loss of generality, we may assume that $z > 0$. By the least integer principle, we may also assume that our solution has z *minimal.* Taking remainders modulo three, we see that

$$x^2 + y^2 \equiv 0 \pmod 3$$

Recalling that squares may only be congruent to 0 or 1 modulo 3, we conclude that

$$x^2 \equiv y^2 \equiv 0 \implies x \equiv y \equiv 0 \mod 3$$

Writing $x = 3a$ and $y = 3b$ we obtain

$$9a^2 + 9b^2 = 3z^2 \implies 3(a^2 + b^2) = z^2 \implies 3 \mid z^2 \implies 3 \mid z$$

Now let $z = 3c$ and cancel 3's to obtain

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

We've therefore constructed another solution $(a, b, c) = (\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ to the *original equation.* However $0 < c < z$ contradicts the minimality of z.

[a] Equivalently, the circle $x^2 + y^2 = 3$ contains no rational points.

The structure of the argument should seem familiar. Indeed if you recall the standard proof that $\sqrt{2}$ is irrational, you should be able to rephrase this as a proof by descent of the fact that the equation $x^2 = 2y^2$ has no non-zero solutions in integers.

In 1637 Fermat stated his famous Last Theorem in the margin of his copy of Diophantus' *Arithmetica*.

Theorem 5.2. *If $n \in \mathbb{N}_{\geq 3}$, then the equation $x^n + y^n = z^n$ has no non-zero integer solutions.*

In perhaps the most famous claim in mathematical history, Fermat stated that the margin was too small to contain his argument. After his death in 1665, an edited version of the *Arithmetica* was published including Fermat's unproved notes and comments. As proofs to essentially everything else slowly appeared, the *last* theorem steadily grew in notoriety. In 1994 (after 350 years!) Andrew Wiles finally proved the last theorem via a related result regarding elliptic curves. Only the most romantic modern mathematicians now believe that Fermat had a valid argument.

We'll discuss elliptic curves later. For the present, we prove a modified version of the $n = 4$ case.

Theorem 5.3. *$x^4 + y^4 = w^2$ has no non-zero solutions in pairwise coprime integers.*

Proof. Suppose such a solution (x, y, w) exists and WLOG assume that this has w minimal.

Clearly (x^2, y^2, w) is a primitive Pythagorean triple. WLOG assume that x^2 is odd and y^2 even. It follows that $\exists u, v$ coprime with exactly one odd and $u > v$ such that[a]

$$x^2 = u^2 - v^2, \qquad y^2 = 2uv, \qquad w = u^2 + v^2$$

Consider the first equation modulo 4: observing that

$$\lambda^2 \equiv \begin{cases} 0 \mod 4 \iff \lambda \text{ is even} \\ 1 \mod 4 \iff \lambda \text{ is odd} \end{cases}$$

we see that u must be odd and v even. Since u and v are coprime, $y^2 = 2uv \implies u, 2v$ are perfect squares. Let $u = a^2$ and $v = 2b^2$ where a, b must be coprime. But then

$$x^2 = a^4 - 4b^4 \implies x^2 + (2b^2)^2 = (a^2)^2$$

whence $(x, 2b^2, a^2)$ is another primitive Pythagorean triple. We may therefore write

$$x = c^2 - d^2, \qquad 2b^2 = 2cd, \qquad a^2 = c^2 + d^2$$

for some coprime c, d. Finally $b^2 = cd \implies c, d$ are perfect squares: write $c = r^2, d = s^2$, from which

$$r^4 + s^4 = a^2$$

To recap; starting with a solution (x, y, w), we have constructed a new solution (r, s, a) satisfying

$$a \leq a^2 = u \leq u^2 < w$$

This contradicts the minimality of w: by the method of descent, there are no solutions. ∎

[a] A Pythagorean triple (α, β, γ) is *primitive* if α, β, γ are pairwise coprime. This parameterization was covered in 180A.

This recovers the $n = 4$ case of Fermat's theorem since $x^4 + y^4 = z^4 = (z^2)^2$.

In the only relevant proof attributable to Fermat, he uses the descent method to prove that the equation $w^2 + y^4 = z^4$ has no solutions in positive integers (Exercise 5). This is a little more irritating than our version since multiple cases are required. The purpose of his result was in fact geometric (see Exercise 4): a right triangle with integer sides cannot have area equal to a perfect square.

Over the next couple of centuries, mathematicians obtained proofs for several other cases. The first proofs for specific exponents are generally credited as follows:

- $n = 3$: Euler (1770)
- $n = 5$: Legendre/Dirichlet (1825)
- $n = 7$: Lamé (1839)

Numerous other proofs for these cases appeared, as well as for a few redundant exponents such as $n = 6$. All early proofs used some variation on the method of descent.

Exercises 1. To show that $x^4 + y^4 = w^2$ has no solutions $x, y, w \in \mathbb{N}$, explain why we need only check that the equation has no *pairwise coprime* solutions.

2. Prove that it is enough to demonstrate Theorem 5.2 when $n = 4$ or is any odd prime.

3. Here is a descent argument due to Dedekind, showing the irrationality of $\sqrt{2}$.
   - Assume that $\sqrt{2}$ is rational and write $\sqrt{2} = 1 + \frac{p}{q}$ where $p < q$.
   - Then $2q^2 = q^2 + 2pq + p^2 \implies p^2 = q(q - 2p) \implies \frac{p}{q} = \frac{q-2p}{p}$
   - But now $\sqrt{2} = 1 + \frac{q-2p}{p}$ has fractional part with denominator p *smaller* than q. Repeating the argument, we obtain a contradiction by descent.

   Generalize the argument to prove that $\sqrt{n}$ is irrational whenever $n \in \mathbb{N}$ is not a perfect square. (*Hint: Write* $\sqrt{n} = m + \frac{p}{q}$ *where m is the integer part of* $\sqrt{n}$*...*)

4. Suppose that (a, b, c) is a Pythagorean triple and that these form the sides of a right-triangle whose area is a perfect square: thus $\exists d \in \mathbb{N}$ such that $\frac{1}{2}ab = d^2$. Prove that

$$(a^2 - b^2)^2 + (2d)^4 = c^4$$

   (*The next exercise shows that this arrangment is impossible*)

5. We show that $w^2 + y^4 = z^4$ has no non-zero integer solutions. As before, it is enough to show that the equation has no solutions which are pairwise coprime. Assume, for contradiction, that (w, y^2, z^2) is a primitive Pythagorean triple.

   (a) Suppose w is even. Find an expression for $(yz)^2$ and thus a solution to $A^2 + B^4 = C^4$ where A is odd and (A, B, C) are pairwise coprime. It is enough therefore to show that w cannot be odd.

   (b) Now suppose w is odd. Write $z^2 = u^2 + v^2$ so that (u, v, z) is a primitive Pythagorean triple. Treat the cases u odd/v odd separately, but show in either case that $\exists a, b \in \mathbb{N}$ coprime $a > b$ not both odd such that

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

   (c) All three factors of the right hand side above must be perfect squares: why?

   (d) Show that we obtain a new solution to $W^2 + Y^4 = Z^4$ with W odd and $Z < z$.

5.2 Sums of Squares

Fermat also considered the question of which integers can be written as a sum of squares. For instance

$$9 = 3^2 + 0^2 \quad \text{and} \quad 10 = 3^2 + 1^2$$

are both the sum of two squares, although 7 is not. Indeed 7 is not the sum of three squares either, though it is the sum of four squares

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

We'll consider some generalizations later, but in the hope of finding a pattern, we first ask which *primes* may be expressed as the sum of two squares. Here are the first few examples:

$$2 = 1^2 + 1^2, \quad 5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2, \quad 29 = 5^2 + 2^2, \quad 37 = 6^2 + 1^2$$

The following result is immediately suggested.

Theorem 5.4. *An odd prime p may be written as a sum of two squares if and only $p \equiv 1 \pmod 4$.*

We again use the method of descent, though this time *constructively.*

Proof. ($\Rightarrow$) If $p = x^2 + y^2$, then both x and y are non-zero modulo p. Taking Legendre symbols, we see that

$$1 = \left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) \implies p \equiv 1 \pmod 4$$

($\Leftarrow$) Suppose that p is a prime congruent to 1 modulo 4. We must show that there exist integers x, y such that $x^2 + y^2 = p$. We do this by descent:

1. Modulo p, the congruence $x^2 + 1 \equiv 0$ has a solution x since -1 is a quadratic residue. By taking $y = 1$, we may therefore assume the existence of a solution to an equation $x^2 + y^2 = mp$ for some integer $1 \le m < p$. If $m = 1$ we are done. Otherwise...

2. Define

   $$\begin{cases} u \equiv x \pmod m \\ v \equiv y \pmod m \end{cases} \qquad \text{such that} \quad |u|, |v| \le \frac{m}{2}$$

   Since $xu + yv$, $xv - yu$ and $u^2 + v^2$ are all divisible by m, we may divide the identity

   $$(u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2 \tag{$*$}$$

   by m^2 to obtain an equation in *integers*:

   $$kp = \left(\frac{xu + yv}{m}\right)^2 + \left(\frac{xv - yu}{m}\right)^2 \quad \text{where} \quad k = \frac{u^2 + v^2}{m} \le \frac{m}{2}$$

3. We have therefore constructed an integer solution to $X^2 + Y^2 = kp$ with $k < m$. If $k \ge 2$, simply repeat the process from step 2: by descent, we must eventually reach $k = 1$.

■

Example 5.5. As a concrete example of the descent at work, suppose we start with $12^2 + 1^2 = 5 \cdot 29$ where $m = 5$ and $p = 29$. Now let

$$\begin{cases} u \equiv 12 \equiv 2 \pmod 5 \\ v \equiv 1 \pmod 5 \end{cases}$$

whence

$$\begin{aligned} &(12^2+1^2)(2^2+1^2) = (12\cdot 2 + 1\cdot 1)^2 + (12\cdot 1 - 1\cdot 2)^2 = 25^2 + 10^2 \\ &\Longrightarrow\ 29 = \frac{12^2+1^2}{5}\cdot\frac{2^2+1^2}{5} = 5^2 + 2^2 \end{aligned}$$

For small primes p it is easy to find a solution to $x^2 + y^2 = p$ by a simple search. For larger p the proof provides a fairly efficient algorithm. For any $a \in \mathbb{Z}_p^\times$, consider $x \equiv a^{\frac{p-1}{4}}$ and observe that

$$x^2 \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv \pm 1 \pmod p \qquad \text{(Euler's criterion)}$$

Each a provides an even chance of producing a suitable candidate to start the algorithm. The above example could have got started with $a = 2$ since $2^{\frac{29-1}{4}} \equiv 12$ and $12^2 \equiv -1 \pmod{29}$.

Example 5.6. Let $p = 953$. A quick check with a calculator or computer shows that $3^{\frac{953-1}{4}} \equiv 511 \pmod{953}$ and that $511^2 \equiv -1 \pmod{953}$. We take $x = 953 - 511 = 442$ and observe that

$$442^2 + 1^2 = 205 \cdot 953$$

With $m = 205$, let

$$\begin{cases} u \equiv 442 \equiv 32 \pmod{205} \\ v \equiv 1 \pmod{205} \end{cases}$$

whence

$$\begin{aligned} &(442^2+1^2)(32^2+1^2) = (442\cdot 32 + 1\cdot 1)^2 + (442\cdot 1 - 1\cdot 32)^2 = 14145^2 + 410^2 \\ &\Longrightarrow\ \frac{442^2+1^2}{205}\cdot\frac{32^2+1^2}{205} = \left(\frac{14145}{205}\right)^2 + \left(\frac{410}{205}\right)^2 \\ &\Longrightarrow\ 953\cdot 5 = 69^2 + 2^2 \end{aligned}$$

Now repeat with $m = 5$: let

$$\begin{cases} u \equiv 69 \equiv -1 \pmod 5 \\ v \equiv 2 \pmod 5 \end{cases}$$

whence

$$\begin{aligned} &(69^2+2^2)\big((-1)^2+2^2\big) = \big(69\cdot(-1) + 2\cdot 2\big)^2 + \big(69\cdot 2 - 2\cdot(-1)\big)^2 = 65^2 + 140^2 \\ &\Longrightarrow\ \frac{69^2+2^2}{5}\cdot\frac{(-1)^2+2^2}{5} = \left(\frac{65}{5}\right)^2 + \left(\frac{140}{5}\right)^2 \\ &\Longrightarrow\ 953 = 13^2 + 28^2 \end{aligned}$$

Even this second example required a lot of work and would have been easier using a simple search program. As the numbers get larger, however, the descent process becomes more efficient. For example, the following steps took less than 10 minutes with the assistance of a pocket calculator.[1]

$$3721 \cdot 15328637 = 238826^2 + 1^2$$
$$125 \cdot 15328637 = 43773^2 + 64^2$$
$$34 \cdot 15328637 = 8023^2 + 21373^2$$
$$5 \cdot 15328637 = 8408^2 + 2439^2$$
$$15328637 = 3851^2 + 706^2$$

A simple computer program could do this in microseconds.

Generalizations

The identity $(*)$ shows that products of sums of squares are also sums of squares. With a little effort, this affords a proof of the more general result:

Theorem 5.7. *The integers which can be written as the sum of two squares are precisely those of the form $p_1 \cdots p_k m^2$ where $p_1, \ldots, p_k$ are distinct primes; either 2 or congruent to 1 modulo 4.*

Explicit expressions can be found using $(*)$: for example

$$\begin{aligned} 248733 &= 9 \cdot 29 \cdot 953 = 3^2(5^2+2^2)(13^2+28^2) = 3^2(65+56)^2 + 3^2(140-26)^2 \\ &= 363^2 + 342^2 \end{aligned}$$

- Lagrange proved the four-square theorem in 1770: all positive integers may be expressed as the sum of four squares (Exercise 5.2.4).
- In 1797 Legendre proved the harder theorem that an integer may be written as the sum of three squares if and only if it is not of the form $4^m(8n+7)$.
- In 1813 Cauchy proved that any integer can be written as a sum of at most n n-polygonal numbers (generalizations of triangular and square numbers). This was another of Fermat's many statements made without proof.
- In 1909 Hilbert proved that there exists a function $g(k)$ such that every positive integer may be written as a sum of $g(k)$ k^{th} powers: this is known as Waring's problem. Hilbert's proof is not constructive but has since been improved and a complete formula for $g(k)$ is conjectured.
- A variant of Waring's problem considers how many squares, cubes, fourth-powers, etc., are necessary to express any *sufficiently large* integer. For small integers, one often requires more k^{th} powers since there are few small powers available. For instance 23 requires *nine* cubes

  $$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3$$

  and indeed $g(3) = 9$. However, it can be shown that every sufficiently large integer can be written as the sum of at most *seven* cubes. At the present, it is unknown whether seven is optimal: it is conjectured that four cubes are sufficient for all large integers.

[1] The first step comes from computing $2^{\frac{15328637-1}{4}}$ (mod 15328637).

Exercises 1. As in Example 5.5, start with $8^2+1^2=5\cdot 13$ with $m=5$ and $p=13$ and apply the descent argument to obtain $13=3^2+2^2$.

2. Starting from the given data, perform the steps of the two-squares algorithm to find an expression for p as the sum of two squares.

   (a) $p=997, \quad m=26, \quad 997m=161^2+1^2$

   (b) $p=2089, \quad m=298, \quad 2089m=789^2+1^2$

3. (a) In the proof of Theorem 5.4, explain why we can assume that $x^2+1=mp$ with $m<p$.

   (b) Explain why the proof fails if we ever obtain $u=x$ and $v=y$. However, show that this can only happen if $m\geq p$.

   (c) The identity $(u^2+v^2)(x^2+y^2)=(xu+yv)^2+(xv-yu)^2$ is related to the norms of complex numbers: $|w|^2\,|z|^2=|wz|^2$. Check the identity. What are w and z in this case?

   (d) Use identity in (c) to find an expression for 1508 as a sum of two squares.

4. In this question we prove Lagrange's result that every positive integer may be expressed as the sum of four squares. Fair warning: this is very long…

   (a) Verify the following identity:

$$\begin{aligned}(x^2+y^2+z^2+t^2)(X^2+Y^2+Z^2+T^2) &= (xX+yY+zZ+tT)^2\\ &\quad+(xY-yX+zT-tZ)^2\\ &\quad\quad+(xZ-zX+tY-yT)^2\\ &\quad\quad\quad+(xT-tX+yZ-zY)^2\end{aligned}$$

   For those who have met quaternions, this is just the fact that $|\gamma|^2\,|\delta|^2=|\gamma\delta|^2$ *where*

$$\gamma=x+iy+jz+kt, \qquad \delta=X-iY-jZ-kT$$

The identity in (a) says that the product of two sums of four squares is also a sum of four squares. Since 1 and 2 are trivial

$$1=1^2+0^2+0^2+0^2, \qquad 2=1^2+1^2+0^2+0^2$$

it is enough to prove that every odd prime may be written expressed. Throughout the rest of the question, we assume that p *is an odd prime.*

   (b) Use the box principle to prove that there exist integers x,y which satisfy

$$0\leq x,y\leq\frac{p-1}{2} \quad\text{and}\quad 1+x^2+y^2\equiv 0 \pmod{p}$$

   (*Hint: There are* $\frac{p+1}{2}$ *values in the range* $0\leq x\leq\frac{p-1}{2}$*, no two of which are congruent modulo* p*. The same is true for values* $-1-y^2$*. Why must some* x^2 *be congruent to some* $-1-y^2$*?*)

   (c) By part (b), $\exists m\in\mathbb{N}$ such that $x^2+y^2+z^2=mp$ and $0\leq x,y,z\leq\frac{p-1}{2}$ (take $z=1$). Explain why $m<\frac{3p}{4}$

Let $n \in \mathbb{N}$ be minimal such that np is the sum of four squares. We know that $n < \frac{3p}{4}$ by part (c) and want to prove that $n = 1$. Write $np = x^2 + y^2 + z^2 + t^2$ (x, y, z are likely different from in part (c)).

(d) Suppose n is even.

i. Prove that none, two or all four of x, y, z, t are even.

ii. Let x, y have the same parity, then so also do z, t. Check that

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

Why is this a contradiction?

(e) Suppose $n \geq 3$ is odd. Let X, Y, Z, T be congruent modulo n to x, y, z, t respectively and such that $|X|, |Y|, |Z|, |T| < \frac{n}{2}$.

i. Prove that $X^2 + Y^2 + Z^2 + T^2 = kn$ for some $0 < k < n$.

ii. Show that there exist integers A, B, C, D such that

$$(np)(kn) = A^2 + B^2 + C^2 + D^2$$

where each of A, B, C, D is divisible by n. Hence conclude that kp may be written as a sum of four squares.

(f) Complete the proof of the main result.