5 Fermat's Method of Descent

5.1 Two Reasons to Descend

The *method of infinite descent* is a standard approach to Diophantine equations. The method is often attributed to Pierre de Fermat, who made multiple uses of it. There are two standard types of application:

1. To show that an equation has *no solutions*. Consider the set of all positive integer solutions to an equation: if this is non-empty then (least integer principle) there must be a *minimal* such solution. We proceed to construct a *smaller* solution thus contradicting minimality. Fermat used this method to show that certain Pythagorean triples cannot exist: as a corollary this gives a proof of the $n = 4$ case of his last theorem.

2. To show that an equation has a solution. By starting with a solution to a related equation, we produce a smaller solution to the equation we desire. Later we shall see this applied to another claim of Fermat's, this one eventually proved by Euler, regarding which integers are the sums of two squares.

We start with a very simple example of the method.

Example The equation[1] $x^2 + y^2 = 3z^2$ has no solutions (x, y, z) in integers where $z \neq 0$.

Suppose we have a solution to the given equation. We may assume, without loss of generality, that $z > 0$. By the least integer principle, we may assume that we have a solution (x, y, z) for which $z > 0$ is *minimal.* Taking remainders modulo three, we see that

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

Recalling the fact that squares can only be congruent to 0 or 1 modulo 3, we see that we must have

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

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

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

Therefore $(a, b, c) = (\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ is a solution to *exactly the equation we started with.* Since $0 < c < z$, this contradicts the assumed minimality of z.

The structure of the proof should seem familiar: recall the standard proof that $\sqrt{2}$ is irrational. If you think carefully, you should see that this can be rephrased as a proof by descent of the fact that the equation $x^2 = 2y^2$ has no non-zero solutions in integers.

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

5.2 Fermat's Last Theorem

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

Theorem 5.1. *If $n \in \mathbb{N}_{\geq 3}$, then there exist no integers $x, y, z \in \mathbb{N}$ for which $x^n + y^n = z^n$.*

As was common with Fermat, he gave no proof. Intriguingly however, he claimed that the margin was too small to contain his argument. After Fermat's death in 1665 his 'theorem' gained notority: his son published an edited version of *Arithmetica* including all of his notes and comments. Fermat's vast trove of unproved results provided a challenge to future generations of mathematicians, with Euler being particularly effective in proving many of these. The result became known as his *last* theorem as it was the last of his claims to go unproven. The Theorem was finally proved in 1994 when Andrew Wiles proved a related result regarding elliptic curves: if you've never read the story, do so! Given the complexity of the modern proof, and the fact that countless mathematicians tried and failed over the centuries, modern mathematicians do not believe that Fermat had a valid proof.

Theorem 5.2. *Proving Theorem 5.1 is equivalent to proving the cases when $n = 4$ and when n is any odd prime.*

Proof. Suppose that $x^n + y^n = z^n$ and that $n = pq$ where p is an odd prime. Then (x^q, y^q, z^q) is a solution to the equation $x^p + y^p = z^p$. If $x^p + y^p = z^p$ cannot be solved, neither can $x^n + y^n = z^n$. The argument is identical if $4 \mid n$. ■

Historically, mathematicians tried to prove Fermat's Last Theorem one case at a time. The simplest case turns out to be when $n = 4$ and we give a modified version of a result proved by Fermat.

Theorem 5.3. *$x^4 + y^4 = z^4$ has no non-zero solutions in integers.*

Proof. It is enough to show that $x^4 + y^4 = w^2$ has no solutions where x, y, w are pairwise coprime positive integers.

Suppose such a solution exists. By the least integer principle we may assume that the solution (x, y, w) has w minimal.

Clearly (x^2, y^2, w) is a primitive Pythagorean triple. Without loss of generality we may 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[2]

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

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,

$$y^2 = 2uv \implies u, 2v \quad \text{are perfect squares.}$$

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

Let $u = a^2$ and $v = 2b^2$ where a, b must be coprime. Then

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

whence $(x, 2b^2, a^2)$ is a 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 $b^2 = cd \implies c, d$ perfect squares: write $c = r^2, d = s^2$, hence

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

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

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

By the method of infinite descent, there are no solutions.

■

The above argument is not the one given by Fermat. The only relevant proof attributable to Fermat uses the descent method to prove that $x^2 + y^4 = z^4$ has no solutions in positive integers. This is a little more irritating than our result: assuming (x, y^2, z^2) is a primitive Pythagorean triple, we have to deal with the cases where x is even or y is even separately. Fermat didn't state the obvious corollary that now bears his name, but he clearly believed it due to his famous margin note. The purpose of his result was actually geometric: as a special case he demonstrates that a right triangle with integer sides cannot have area equal to a perfect square.

For the next hundred years or so, mathematicians obtained proofs for a few other cases of the Last Theorem. 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.

5.3 Sums of Squares

Our second application of the method of descent is *constructive*: we use it to build solutions to equations. The method lends itself to the consideration of which positive integers may be written as sums of (two, three, four) squares. Thus

$$10 = 1^2 + 3^2$$

is the sum of two squares, although 7 is not.[3] Indeed 7 is not the sum of three squares either, though it is the sum of four squares

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

[3] Trivial examples, such as writing $9 = 0^2 + 3^2$ as the sum of two squares, are explicitly allowed.

The question of which integers can be written as the sum of two squares was also studied by Fermat.[4] We restrict to primes in the hope of finding a pattern and as the easier question: which *primes* are the sums of two squares? Here are the first few examples where it is possible:

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

You should immediately be able to hypothesize the following:

Theorem 5.4. *A prime p may be written as a sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proof. The statement is trivial if $p = 2$. For an odd prime p, the forward direction is also easy. If $p = x^2 + y^2$, then both x and y are non-zero modulo p. Taking Legendre symbols, we see that

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

whence $p \equiv 1 \mod 4$.
The question now turns to the converse. 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. The congruence $x^2 + 1 \equiv 0 \mod p$ has a solution x since -1 is a quadratic residue modulo p.

2. Taking $y = 1$, we may assume that we have a solution to an equation $x^2 + y^2 = mp$ for some integer $1 \leq m < p$. If $m = 1$ we are done. Otherwise define

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

3. By the definitions of u, v we see that the three expressions $xu + yv$, $xv - yu$ 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*:

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

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

■

For small values of p it is easier to find a solution to $x^2 + y^2 = p$ by trial and error or a brute force search algorithm. For larger p the process is more efficient. Recalling Euler's criterion $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$, it follows that we have an even chance that $b = a^{\frac{p-1}{4}}$ satisfies $b^2 \equiv -1 \mod p$ for some random a. This, or using some other guesswork, will quickly be enough to get us started.

[4] Both Fermat, and an earlier mathematician named Girard stated the result, but neither gave a proof. Fermat extended the statement to discuss *how many* ways an integer may be expressed as the sum of two squares. The first proof was announced by Euler in the 1740's.

Examples

1. First we recover $p = 29 = 5^2 + 2^2$ in a way that mirrors the descent argument. Suppose that we start with the expression[5] $12^2 + 1^2 = 5 \cdot 29$. We thus have $m = 5$. Now let

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

whence

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

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

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

Now let

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

whence

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

Now repeat with $m = 5$: let

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

whence

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

[5] For example, obtained from $2^{\frac{29-1}{4}} \equiv 12$ and $12^2 \equiv -1 \mod 29$.

The second example required a lot of work, and it likely would have been easier using a simple search program. As the numbers get larger, the descent process becomes more efficient. For example, the following five applications of the descent method took less than 10 minutes with the assistance of a pocket calculator: how long would it take by trial and error? (Note that the starting value comes from computing $2^{\frac{15328637-1}{4}} \mod 15328637$.)

$$\begin{aligned}
&3721 \cdot 15328637 = 238826^2 + 1^2\\
&125 \cdot 15328637 = 43773^2 + 64^2\\
&34 \cdot 15328637 = 8023^2 + 21373^2\\
&5 \cdot 15328637 = 8408^2 + 2439^2\\
&15328637 = 3851^2 + 706^2
\end{aligned}$$

A simple computer program could do this in microseconds.

Generalizations

- The identity $(*)$ shows that products of sums of squares are also sums of squares. Using this, it can be shown (try it yourself!) that the integers which may be written as the sums of two squares are precisely those of the form $p_1 \cdots p_k m^2$ where m is any integer and the $p_1, \ldots, p_k$ are *distinct* primes which are 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.

- 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 $4^m(8n + 7)$ for some integers m and n.

- In 1813 Cauchy proved that any integer can be written as a sum of at most n n-polygonal numbers. This was another of Fermat's many statements made without proof.

- In 1909 Hilbert proved that there is a function $g(k)$ such that every positive integer may be written as a sum of $g(k)$ kth powers of positive integers: 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 discusses the more difficult issue of deciding how many squares, cubes, fourth-powers, etc., are necessary to sum to any *sufficiently large* integer. The challenge is that the estimates $g(k)$ defined above are not very useful for large integers. For small integers, one is often required to sum more kth powers than for larger integers as 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 this number is the best that can be done. It is conjectured that four cubes are sufficient for all large integers.