McGill University

MATH 377

Honors Number Theory

On Fermat's Method of Infinite Descent

Author:
Akash Jaggia, 260418452
25th April 2013

1 Introduction

The 17th century was a golden age for mathematics. Northern Europe produced the likes of Descartes, Desargues, Pascal, Wallis, Bernoulli, and Leibniz. Amongst them was a French royal councillor from the Parliament of Toulouse, Pierre De Fermat (1601-1665). Fermat, nicknamed the "Prince of Amateurs," was the last great mathematician to pursue the subject as a sideline to a nonscientific career. Before taking up the position of a royal councillor, Fermat was a lawyer in Bordeaux. Interestingly, Fermat did not seem to have formal mathematical training; he received a Bachelor's degree in civil law from the University of Orleans. Furthermore, Fermat didn't develop an interest in the subject until he was past 30; it was just a hobby to be cultivated during leisure time. Yet no practitioner of the time had as much of an impact. Independently inventing analytic geometry, laying the foundations of differential and integral calculus, and establish the conceptual guidelines of probability theory with Pascal were a few of Fermat's contributions. Even though he published significant results in various fields, Fermat's true legacy is as the father of modern number theory, a subject whose revival began with his work in it. [2] [4]

Given his huge contributions to the field of number theory, Fermat was notoriously infamous for not providing proofs for his conjectures. (We return to this when we discuss Fermat's Last Theorem.) Fermat would be in correspondance with the number theorists of the day, including Pascal, Carcavi, and Frenicle. His go-between in exchanges with the other mathematicians was Mersenne. It was in fact Mersenne who inspired Fermat to jump into the field of number theory. In his letters, Fermat would formulate number-theoretical questions, but there are also several definitive statements and discussions of special numerical examples. His most important number-theoretical heritage is a letter to Carcavi in August 1650. Before stating any results in his letter, Fermat describes a certain method of proof that he discovered himself and utilized with great success. He writes the following about his method of proof, quoted from E.T. Bell, Men of Mathematics: [2] [4]

> For a long time I was unable to apply my method to affirmative propositions, because the twist and the trick for getting at them is much more troublesome than that which I use for negative propositions. Thus, when I had to prove that every prime number which exceeds a multiple of 4 by 1 is composed of two squares, I found myself in a fine torment. But at last a medita-

> tion many times repeated gave me the light I lacked, and now affirmative propositions submit to my method, with the aid of certain new principles which necessarily must be adjoined to it. The course of my reasoning in affirmative propositions is such: if an arbitrarily chosen prime of the form $4n + 1$ is not a sum of two squares, [I prove that] there will be another of the same nature, less than the one chose, and [therefore] next a third still less, and so on. Making an infinite descent in this way, we finall arive at the number 5, the least of all the numbers of this kind $[4n + 1]$. [By the proof mentioned and the preceding argument from it], it follows that 5 is not a sum of two squares. But it is. Therefore we must infer by a reduction ad absurdum that all numbers of the form $4n + 1$ are sums of two squares.

This method is now known as the method of infinite descent. It is based on the Well-Ordering Principle of the natural numbers, which states that every non-empty subset of $\mathbb{N}$ has a minimal element. The general idea of infinite descent may be described as follows. Let A be the subset of $\mathbb{N}$ *s.t.* for $a \in A$, the truth of the statement $P(a)$ implies that $\exists$ a subset B of A with an element b with $b < a$ s.t $P(b)$ is true. This is the descent step. Now, since $P(b)$ is true, $\exists$ a subset C of B s.t. $P(c)$ holds for $c \in C$ where $c < b$. Continuing in this fashion, the set $\{a, b, c, ...\}$ is not bounded below, so by the well-ordering principle, $P(a)$ is false, implying the statement is false $\forall\ n \in \mathbb{N}$. The rest of the project will illustrate how this method can be used to establish some of Fermat's results. As Fermat begins his letter by describing the method of infinite descent for the decomposition of a prime of the form $4n + 1$ as the sum of two squares, this project begins by providing the details to this result, and then the method is used to establish Fermat's Last Theorem for the exponents $n = 3$ and $n = 4$.

2 Sums of Two Squares

Theorem 2.1 *Every prime number p of the form $4n + 1$ can be written uniquely as the sum of two squares.*

The proof of this theorem is credited to Euler, who established it in a series of propositions, with the help of the method of infinite descent.

Proposition 2.2 *The product of any two numbers that are the sum of two squares is itself the sum of two squares.*

Proof This follows immediately from the identity $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 = (ac+bd)^2 + (ad-bc)^2$. $\square$

Proposition 2.3 *If a number which is the sum of two squares is divisible by a prime that is the sum of two squares, then the quotient is a sum of two squares.*

Proof Suppose that a^2+b^2 is divisible by a prime $p = c^2+d^2$. Then c^2+d^2 divides $(cb-ad)(cb+ad) = c^2b^2 - a^2d^2 = c^2(a^2+b^2) - a^2(c^2+d^2)$, clearly, since $p|(c^2+d^2)$ by definition and $p|(a^2+b^2)$ by assumption. Since p is prime, either $p|(cb-ad)$ or $p|(cb+ad)$. Suppose that $p|(cb-ad)$. From Proposition 2.1, we have that $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$ so c^2+d^2 must divide $(ac+bd)^2$. Thus, we can divide the entire equation by p^2 to get $\frac{a^2+b^2}{c^2+d^2} = \frac{ac+bd}{c^2+d^2}^2 + \frac{ad-bc}{c^2+d^2}^2$. Thus, the quotient can be expressed as the sum of two squares. Now suppose $p|(cb+ad)$. Using $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$, a similar argument shows that the quotient is representable by a sum of two squares. $\square$

Proposition 2.4 *If a number which can be written as the sum of two squares has a divisor that is not a sum of two squares, then the quotient is not a sum of two squares.*

Proof Suppose $x|(a^2+b^2)$ and that $p_1p_2...p_n$ is the prime factorization of the quotient. Then $a^2+b^2 = xp_1...p_n$. If all the prime factors $p_1, ..., p_n$ are of the form of the sums of two squares, then we can divide a^2+b^2 successively by $p_1, ..., p_n$ by Proposition 2.2, then each of the quotients is a sum of two squares, hence x is the sum of two squares. Therefore, if x is not the sum of the two squares, then one of the $p_1, ..., p_n$ is not a sum of two squares. $\square$

The next proposition is where we use the method of infinite descent.

Proposition 2.5 *If a, b are relatively prime, then every factor of a^2+b^2 is the sum of two squares.*

Proof Let x be a factor of a^2+b^2. By division, $a = mx \pm c$, $b = nx \pm d$, $c, d \leqq \frac{1}{2}|x|$. Then, $a^2+b^2 = m^2x^2 \pm 2mxc + c^2 + n^2x^2 \pm 2nxd + d^2 = Ax + (c^2+d^2)$. Since $x|(a^2+b^2)$, so is c^2+d^2, and let $c^2+d^2 = yx$. If $gcd(c,d) = D > 1$, then $D|x$ which implies that $D|a$ and $D|b$, which is not possible. So we can divide $c^2+d^2 = yx$ by D to give an equation of the form $e^2+f^2 = zx$. We have $zx = e^2+f^2 \leqq c^2+d^2 \leqq \frac{x}{2}^2 + \frac{x}{2}^2 = \frac{x^2}{2}$. Thus $z \leqq \frac{x}{2}$. If x were not the sum of two squares, then by Proposition 2.3, $\exists$ a divisor w

of z s.t. w is not the sum of two squares. By construction, $w < x$, and both w and x divide sums of two squares but neither are sums of two squares. We have constructed an infinite descent, and arrive at a contradiction because no such minimal x exists. Therefore x must be the sum of two squares. $\square$

Proof *(Of the Two-Square Theorem)* Assume that a prime p is of the form $4n+1$. By Fermat's Little Theorem, $1, 2^{4n}, 3^{4n}, ..., (4n)^{4n}$ is congruent to 1 *mod* p. In particular, $2^{4n} - 1, 3^{4n} - 2^{4n}, ...$, are all divisible by p. We can factor these differences into $a^{4n} - b^{4n} = (a^{2n} + b^{2n})(a^{2n} - b^{2n})$. Since p is prime, it must divide one of the two factors. If $p|(a^{2n}+b^{2n})$ in any of the first $4n-1$ cases then, by Proposition 2.4 and the fact that a and b are relatively prime (since they differ by 1), it follows that p is the sum of two squares. So it is sufficient to show that p does not divide all $4n-1$ differences.

If p divides $2^{4n}-1, 3^{4n}-2^{4n}, ...$, then it would divide all $4n-2$ differences of successive numbers, all $4n-3$ differences of the differences, and so on. Now, the kth differences of the sequence $1^k, 2^k, 3^k, ...$, is $k!$ So the $(2n)!$th differences would all be constant and would equal $(2n)!$. Since $p = 4n+1$, p cannot divide $(2n)!$, thus p cannot divide all the second factors, so p is the sum of two squares. $\square$

3 Fermat's Last Theorem for exponents 3 and 4

The 15th century saw the fall of Constantinope to the Turks. Many scholarly texts were lost during the Turk invasion, but Byzantine scholars had managed to salvage some of the greatest texts of ancient Greek mathematics. One of the books that survived was Diophantus' *Arithmetica*. It wasn't until the second half of the 17th century that the book started to circulate again. The credit for this goes to Claude Bachet, who published the original Greek text alongside a Latin translation with comments and notes, making the book accessible to European mathematicians. It was Bachet's edition that steered Fermat to number theory. He would write down notes in the margin of his copy of *Arithmetica* and as mentioned earlier, Fermat would not prove these results. Undoubtedly the most famous marginal comment was the one written around 1637, which states (as in Burton's *Elementary Number Theory*):[2]

> It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I

> have discovered a truly wonderful proof, but the margin is too small to contain it.

The statement came be to known as Fermat's Last Theorem (FLT), not because it was his last, but since it was his only comment in *Arithmetica* that eluded mathematicians for 300 years, including the likes of Euler, Gauss, Legendre, Dirichlet, Riemann, etc. The theorem is stated more generally today as:

Theorem 3.1 *There is no solution in the positive integers to* $x^n + y^n = z^n$ *for* $n > 2$.

Until 1993, only proofs for specific exponents were known. Andrew Wiles, a British mathematician, presented a series of lectures in Cambridge in June of 1993, claiming to have proved Fermat's Last Theorem (there was a gap in the proof that took Wiles 3 years to fill in), using techniques that were only discovered in the 20th century, casting a shadow of doubt over whether Fermat actually had a proof. Fermat did provide a proof, using his method of infinite descent, for the case n=4, which is an easier result to establish than the one for n=3, so it is provided here first.

3.1 The case n=4

We establish a stronger version of the theorem, and show that the case n=4 follows as a corollary almost immediately.

Theorem 3.2 *The quadratic Diophantine equation* $x^4 + y^4 = z^2$ *has no solutions in positive integers.*

We start with a discussion on the quadratic equation $x^2 + y^2 = z^2$ and all its solutions, i.e. the Pythagorean triples.

Definition A Pythagorean triple is a set of three integers satisfying $x^2 + y^2 = z^2$. It is said to be primitive if x, y, z are relatively prime.

In the rest of this discussion, it is enough to only work with primitive Pythagorean triples. Suppose $\gcd(x, y, z) = d > 1$. Then $x = dX$, $y = dY$, $z = dZ$ for some integers X, Y, Z and we have $X^2 + Y^2 = \frac{x^2+y^2}{d^2} + \frac{z^2}{d^2} = Z^2$, where X, Y, Z are relatively prime. Also, we can restrict $x, y, z > 0$ since all other triples arise from a change in sign from any of the three integers.

Lemma 3.3 *If* x, y, z *is a primitive Pythagorean triple, then one of the integers* x *and* y *is even, while the other is odd.*

Proof Suppose that both x and y are even. Then $2|x$ and $2|y$, and in particular, $2|(x^2+y^2)=z^2$. Thus, $2|z$. Then the greatest common divisor of x, y, z is greater than or equal to 2, which is a contradiction to the initial assumption.

Now suppose that both x and y are odd. Then $x^2 \equiv 1(\text{mod}4)$ and $y^2 \equiv 1(\text{mod}4)$ (the square of an odd number of the form $4k+3$ is $\equiv 1(mod4)$), so $z^2 \equiv x^2+y^2 \equiv 2(\text{mod}4)$. But this is impossible since $\forall n \in \mathbb{N}$, $n^2 \equiv 0, 1(mod4)$. $\square$

For the rest of this section we assume that x is even and y is odd, so z is necessarily odd. Observe that x, y, z are pairwise relatively prime. Suppose that $\gcd(x,y)=d>1$. Then $\exists$ a prime p dividing d, and thus $p|x$ and $p|y$, which implies that $p|z$. This contradicts the assumption that x, y, z are all relative prime. Thus, $d=1$. Similarly, one can verify that $\gcd(y,z)=\gcd(x,z)=1$.

Lemma 3.4 *If $ab=c^n$, where a, b are relatively prime, then a and b can both be factorized into nth powers.*

Proof We assume without loss of generality that $a>1$, $b>1$, else the result follows triviallly. By unique factorization, $a = {p_1}^{k_1}{p_2}^{k_2}...{p_r}^{k_r}$ and $b = {q_1}^{q_1}{q_2}^{q_2}...{q_s}^{j_s}$. Since a, b are relatively prime, the prime factors of a and b are distinct. Therefore, $ab = {p_1}^{k_1}{p_2}^{k_2}...{p_r}^{k_r}{q_1}^{q_1}{q_2}^{q_2}...{q_s}^{j_s}$. Now, c also admits a prime factorization, say ${u_1}^{l_1}{u_2}^{l_2}...{u_t}^{l_t}$. Then, $ab=c^n$ implies ${p_1}^{k_1}{p_2}^{k_2}...{p_r}^{k_r}{q_1}^{q_1}{q_2}^{q_2}...{q_s}^{j_s} = {u_1}^{nl_1}{u_2}^{nl_2}...{u_t}^{nl_t}$.

Since prime factorizations are unique up to multiplication by the identity and reordering, we have that $u_1, ..., u_t$ are $p_1, ..., p_r, q_1, ...q_s$ and $nl_1, ..., nl_t$ are the corresponding exponents $k_1, ..., k_r, j_1, ...j_s$. We conclude that $n|k_i$, $n|j_i$ $\forall i$. Let $A = {p_1}^{\frac{k_1}{n}}{p_2}^{\frac{k_2}{n}}...{p_r}^{\frac{k_r}{n}}$ and $B = {q_1}^{\frac{j_1}{n}}{q_2}^{\frac{j_2}{n}}...{q_s}^{\frac{j_s}{n}}$ and we have the desired result.

Theorem 3.5 *Suppose that x, y, z are positive integers where x is even and y, z are odd. Let x, y, z be relatively prime. Then all the solutions to the Pythagorean equation $x^2+y^2=z^2$ are given by $x=2st$, $y=s^2-t^2$, $z=s^2+t^2$, where $s>t>0$, s, t are relatively prime, and s, t are of different parity.*

Proof Suppose that x, y, z is a primitive Pythagorean triple. We have that $z-y$ and $z+y$ are both even, so let $z-y=2u$, $z+y=2v$ for some integers, u, v. Rearraging the Pythagorean equation gives $x^2=z^2-y^2=(z+y)(z-y)$,

so $\frac{x}{2}^2 = \frac{z-y}{2}\frac{z+y}{2} = uv$. Note that u, v are relatively prime. If not then, $\gcd(u, v) = d > 1$ means that $d|(u - v) = y$ and $d|(u + v) = z$, which contradicts the assumptions that y, z are relatively prime. From the previous lemma, it follows that we can factor u, v as perfect squares, say, $u = s^2$, $v = t^2$, where $s, t > 0$. Then $z = u + v = s^2 + t^2$, $y = u - v = s^2 - t^2$, $x^2 = 4uv = 4s^2t^2$, so $x = 2st$. If s, t are not relatively prime, then it would contradict the assumption that x, y, z are relatively prime, so s, t must be relatively prime.

It remains to establish that s, t have different parity. Suppose that both s and t are even, or both odd. Then y, z would both be even, which is a contradiction to the assumption that y, z are odd. Thus, one of s, t is even and the other is odd.

Conversely, let s, t satisfy the assumptions in the theorem. Then letting $x = 2st$, $y = s^2 - t^2$, $z = s^2 + t^2$ gives us another Pythagorean triple. Indeed, $x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = 4s^2t^2 + s^4 - 2s^2t^2 + t^4 = (s^2 + t^2)^2 = z^2$. It remains to show that this set of solutions is primitive. Suppose to the contrary that $\gcd(x, y, z) = d > 1$ and let p be a prime divisor of d. Since $z = s^2 + t^2$, the sum of an even and odd number, then z is odd. So we cannot have $p = 2$, else we would have a contradiction. Since p divides y and p divides z, $p|(z + y) = 2s^2$ and $p|(z - y) = 2t^2$. Since p $\not\equiv$ 2, $p|s$ and $p|t$, which is impossible. Thus $d = 1$, and the theorem is established. □

Proof *(Of Theorem 3.2)* Suppose to the contrary that $\exists$ positive integers x, y, z s.t. $x^4 + y^4 = z^2$. We can assume that x, y, z are all relatively prime, else a common divisor of two necessarily divides the third, so the entire equation can be divided through to get relatively prime integers satisfying the equation. Expressing the equation as $(x^2)^2 + (y^2)^2 = z^2$, we see that x^2, y^2, z form a primitive Pythagorean triple. Thus, by the previous theorem, $\exists$ integers s, t s.t. $x^2 = 2st, y^2 = s^2 - t^2, z = s^2 + t^2$ with s, t relatively prime and of opposite parity. Since $t^2 + y^2 = s^2$ and s, t, y are relatively prime, then again by the previous theorem, $\exists$ positive integers a, b relatively prime with $a > b$ and of different parity with $t = 2ab, y = a^2 - b^2, s = a^2 + b^2$. Thus $x^2 = 2st = 4ab(a^2 + b^2)$. It is clear that $a, b, a^2 + b^2$ are relatively prime, so by Lemma 3.3, we have that $a, b, a^2 + b^2$ are squares of positive integers. Let $a = c^2, b = d^2, a^2 + b^2 = e^2$. Then $c^4 + d^4 = e^2$. Observe that $z = s^2 + t^2 = (a^2 + b^2)^2 + 4a^2b^2 > e^4 > e > 0$, thus, (c, d, e) is a smaller solution to the quadratic Diophantine equation than (x, y, z). Thus, by infinite descent, there are no solutions to the quadratic Diophantine equation $x^4 + y^4 = z^2$. □

Corollary 3.6 *The equation $x^4 + y^4 = z^4$ has no solutions in the positive*

integers.

Proof Suppose that X, Y, Z are s.t. $X^4+Y^4 = Z^4$. Then, X, Y, Z^2 would be a solution to $x^4 + y^4 = z^2$, contradicting the result of the previous theorem. □

3.2 The case n=3

Theorem 3.7 *The equation $x^3 + y^3 = z^3$ has no solutions in the positive integers.*

Once again, most of the credit for the proof of this theorem goes to Euler, who first published a proof in 1770. Euler studied the properties of numbers that can be expressed as $a^2 + 3b^2$. Then assuming that a solution for Fermat's Last Theorem for the exponent n=3 existed, he uses these properties to show that a smaller solution exists, hence by infinite descent, no solution exists. Although, it turned out to be incomplete, as Euler did not prove an existence lemma which is crucial, as will be seen. Gauss later filled in this "gap" using the arithmetic properties of $\mathbb{Z}[\sqrt{-3}]$. We begin where Euler did, and establish the results of numbers of the form $a^2 + 3b^2$ that are needed in the proof of the theorem.

3.2.1 Preliminary results

Proposition 3.8 *The product of two numbers of the form $a^2 + 3b^2$ is again of the same form.*

Proof This follows immediately from the identity $(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$.

Proposition 3.9 *If a number of the form $a^2 + 3b^2$ is divisible by 2, then it must be divisible by 4, and its quotient on dividing by 4 is of the form $a^2 + 3b^2$.*

Proof If a and b have opposite parities, then $a^2 + 3b^2$ is not divisible by 2.

If a and b are both even, then $a^2 + 3b^2$ divisible by 4, and the quotient of is of the form $c^2 + 3d^2$, where $c = \frac{a}{2}, = \frac{b}{2}$.

Now suppose that a and b are both odd, so $a = 4m \pm 1$ and $b = 4n \pm 1$ where m, n, and the signs are properly chosen. Then $4|(a+b)$ or $4|(a-b)$. If $4|(a+b)$, then $4(a^2+3b^2) = (1^2+(3)1^2)(a^2+3b^2) = (a-3b)^2+3(a=b)^2 = ((a+b)-4b)^2+3(a+b)^2$. So $4^2|(a-3b)^2+3(a+b)^2$ and thus the quotient also has the desire form. If $4|(a-b)$, then $4(a^2+3b^2) = ((-1)^2+(3)1^2)(a^2+3b^2) = (a+3b)^2+3(a-b)^2$, and the argument proceeds exactly as before. □

Proposition 3.10 *If a number of the form $a^2 + 3b^2$ is divisble by a prime of the form $p^2 + 3q^2$ then the quotient can be written in the form $c^2 + 3d^2$.*

Proof Observe that $(pb - aq)(pb + aq) = p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2 = b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$. Therefore $p^2 + 3q^2 | (pb - aq)$ or $p^2 + 3q^2 | (pb + aq)$. Thus, $(p^2 + 3q^2)(a^2 + 3b^2) = [p^2 + 3(\pm q)^2][a^2 + 3b^2] = (pa \mp 3qb)^2 + 3(pb \pm aq)^2$ is divisible by $(p^2 + 3q^2)^2$ where the sign is chosen correctly and we have the desired form for the quotient. □

Proposition 3.11 *If a number which can be written in the form $a^2 + 3b^2$ has an odd factor that is not of the same form, then the quotient has an odd factor which is not of this form.*

Proof Let $xy = a^2 + 3b^2$ where x is odd. If y is even then by Proposition 3.9, $4|y$ so $\frac{xy}{4} = c^2 + 3d^2$. This process can be repeated until $\frac{y}{4^k}$ is odd. Therefore, $y = 4^k p_1 p_2 ... p_n$ where the p_is are odd primes. If all the primes can be written as $c^2 + 3d^2$, then $xy = a^2 + 3b^2$ can be divided by 4^k and $p_1, ..., p_n$, whence it follows from the last two propositions that x is of the form $c^2 + 3d^2$. Therefore if x does not have this form, then y has an odd factor which is not of this form. □

Proposition 3.12 *If a, b are relatively prime, then every odd factor of $a^2 + 3b^2$ is of the form $c^2 + 3d^2$.*

Proof Let x be an odd factor of $a^2 + 3b^2$. Then on division we obtain $a = mx \pm c, b = nx \pm d$, and $|c|, |d| < \frac{x}{2}$. Then $c^2 + 3d^2$ is divisible by x, say $c^2 + 3d^2 = xy$ and $y < x$. No common factor of c, d (other than 1) can divide x, else it would contradict the assumption of a, b being relatively prime. So we can divide xy by $\gcd(c, d)$ to get $e^2 + 3f^2 = xz$ where e, f are relatively prime.

If x is not of the form, then by Proposition 3.11, z has an odd factor, say, w, that is not of this form. Thus, we conclude by infinite descent that every odd factor that is not of the form $a^2 + 3b^2$ has an odd factor which is not of the same form by showing that for such an x, $\exists$ a $w < x$ which is not of the same form. □

Proposition 3.13 *A number is of the form $a^2 + 3b^2$ if its quotient by the largest square it contains contain no prime factors of the form $3n + 2$.*

Proof Note that every odd prime other than 3 is of the form $3n+1$ or $3n+2$. If $a^2 + 3b^2$ is not divisble by 3, then 3 does not divide a, so $a = 3m \pm 1$ and

$a^2+3b^2 = 9n^2 \pm 6m+3b^2+1$, so a^2+3b^2 is of the form $3n+1$. By the previous proposition, an odd prime which divides a number of the form a^2+3b^2 where a, b are relatively prime is not of the form $3n+2$. If $\gcd(a,b) = d > 1$, then $a^2+3b^2 = d^2(A^2+3B^2)$ where A^2+3B^2 have no odd factors of the form $3n+2$ by the previous argument since A, B are relatively prime. Now, the even prime factors of a^2+3b^2 contain a power of 4 by Proposition 3.11 so it contains a square. We conclude that the quotient of a number of the form a^2+3b^2 contains no prime factors of the form $3n+2$. □

Proposition 3.14 *Every prime of the form* $3n+1$ *can be written as* a^2+3b^2.

Proof By Fermat's Little Theorem, $\exists$ a prime p of the form $3n+1$ dividing the $p-2$ differences of the numbers $1, 2^{3n}, 3^{3n}, ..., (p-1)^{3n}$. We can factor the difference $(a^{3n}-b^{3n}) = (a^n-b^n)(a^{2n}+a^nb^n+b^{2n})$. Either a or b is even, so $(a^{2n}+a^nb^n+b^{2n})$ can be written as $A^2+A(2B)+(2B)^2 = (A+B)^2+3B^2$, where A, B are relatively prime. Thus, by Proposition 3.11, p must be of the form c^2+3d^2 unless p divides the $p-2$ differences of $1, 2^n, 3^n, ..., (p-1)^n$. But this would mean that $p|n!$ since the nth differences are constants. Note that p is of the form $3n+1$ but p cannot divide $n!$. Therefore, we have our desired result. □

3.2.2 Proof of the theorem

Assume to the contrary that $\exists\ x, y, z$ s.t. $x^3+y^3 = z^3$. We can assume x, y, z to be pairwise relatively prime, else a common divisor of two would automatically divide the third, so we can divide through the equation we have by the gcd to get a solution set where integers are pairwise relatively prime. Also, at most one of the three is even and at least one of the three is even (since the sum of two odd numbers is even). Thus, only one is even.

First suppose that x, y are odd and z is even. Then $x+y$ and $x-y$ are both even, say $x+y = 2p, x-y = 2q$. From these, we get that $x = p+q, y = p-q$, so $x^3+y^3 = (x+y)(x^2-xy+y^2) = 2p[(p+q)^2-(p+q)(p-q)+(p-q)^2] = 2p(p^2+3q^2)$.

Since $p+q, p-q$ are both odd, any common divisor of p, q would divide x, y contradicting the assumption that x, y are relatively prime. Thus, p, q are relatively prime, and moreover, they have different parity. We can also assume that p, q are positive. If $x < y$, we can interchange the roles to get $q > 0$. Note that if $x = y$ then $x^n+y^n = 1+1+2 \neq z^3 \forall z$. Thus, the assumption that $x^3+y^3 = z^3$ with x, y odd and z even implies that $\exists$ relatively prime positive integers p, q s.t. $2p(p^2+3q^2)$ is a cube.

The same conclusion can be reached if z is odd and either of x or y is even (assume y is even). So we have $x^3 = z^3 - y^3 = (z-y)(z^2+2y+y^2)$. Then $z - y = 2p, z + y = 2q$ implying $z = q + p, y = q - p$ and $x^3 = 2p[(q+p)^2 + (q+p)(q-p) + (q-p)^2] = 2p(p^2+3q^2)$, where p, q are of oppositve parity and are relatively prime.

We claim that $2p, p^2+3q^2$ are relatively prime. Since p, q are of opposite parity, $p^2 + 3q^2$ is odd, so if $\gcd(2p, p^2+3q^2) = d > 1$, then $d > 2$ since p, q are of opposite parity, so d is a common factor of $p, p^2 + 3q^2$, thus a common factor of $p, 3q^2$. Since p, q are relatively prime, the only possible common factor of $2p, p^2 + 3q^2$ is 3. The remainder of the proof will be split into two cases: the first will deal with where 3 does not divide p implying that $2p, p^2+3q^2$ are relatively prime, and the second will deal with where 3 does divide p. In both cases, it will be shown that a smaller solution exists.

Before we establish the last part of the proof, we return momentarily to the pair $2p, p^2 + 3q^2$. Since the product is a cube, they must both equal to cubes themselves. This is where Euler's proof is incomplete. [1] He mistakenly confuses necessity and sufficiency, and does not show (under the conditions of p, q above) that p^2+3q^2 can be expressed as a cube of the same form, yet implicity assumes it. This fact is non-trivial and will be established in the next subsection. For now, we assume it is true and complete the proof.

Assume first that 3 does not divide p. Since $2p, p^2 + 3q^2$ are relatively prime and they each equal a cube. Recall the identity from Proposition 3.7: $(a^2+3b^2)(c^2+3d^2) = (ac-3bd)^2 + 3(ad+bc)^2$. We can use this formula to find cubes of the form p^2+3q^2 by writing $(a^2+3b^2)^3 = (a^2+3b^2)[(a^2 - 3b^2)^2 + 3(2ab)^2] = [a(a^2-3b^2) - 3b(2ab)]^2 + 3[a(2ab) + b(a^2-3b^2)]^2 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2$. Set $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ when a and b are chosen at random. Factorizing gives $p = a(a-3b)(a+3b), q = 3b(a-b)(a+b)$. Another restatement of what Euler failed to show is that if p^2+3q^2 is a cube then $\exists\ a, b$ s.t. p, q admit the factorization given above. Moving on, we deduce that a, b are relatively prime, else any common factor would also divide p, q, contradicting that p, q are relatively prime. Moreover, $2p = 2a(a-3b)(a+3b)$ is a cube. Now, if a, b are both odd or both even, then p, q are even, contradicting p, q having different parity, hence a, b have different parity. Thus, $a - 3b, a + 3b$ are odd and the only possible common factor of $2a, a \pm 3b$ is the only common factor of $a, a \pm 3b$, whose only common factor is the same as that of $a, \pm 3b$, whose only possible common factor is 3, the same as before. 3 cannot be the factor, otherwise $3|p$, contradicting our initial assumption. Therefore, $2a, a - 3b, a + 3b$ are relatively prime, so by Proposition 3.7, they must be cubes, say $2a = A^3, a - 3b = B^3, a + 3b = C^3$. Then, $B^3 + C^3 = a - 3b + a + 3b = 2a = A^3$, implying that (A, B, C) is

another solution to $x^3+y^3=z^3$. We have $A^3B^3C^3 = 2a(a-3b)(a+3b) = 2p$, which is positive and divides z^3 if z is even and x^3 if x is even. Thus, $A^3B^3C^3 < z^3$. A, B, C can take negative values and since we have the identity $(-A)^3 = -A^3$, the negative exponents can be moved to the other side of the equation to become positive cubes, and we have an equation of the form $X^3 + Y^3 = Z^3$, where $X, Y, Z > 0$ and $Z^3 < z^3$. The result then follows from infinite descent.

Now assume that 3 does divide p. Then $p = 3s$ for some s and 3 does not divide q. Then $2p(p^2 + 3q^2) = 3^2 2s(3s^2 + q^2)$, where $3^2 2s, 3s^2 + q^2$ are relative prime (else any common factor would have to be a common factor of s, q^2 which is not possible since p, q have different parity. Therefore, by $3^2 2s$ and $3s^2 + q^2$ are both cubes, so q, s admit the factorizations $a(a - 3b)(a + 3b), 3b(a - b)(a + b)$ respectively for some integers a, b. Since $3^2 2s$ is a cube, $3^3 2b(a - b)(a + b)$ is a cube, thus $2b(a - b)(a + b)$ is a cube. Now, it is clear that $2b, a - b, a + b$ are relatively prime, hence each of them is a cube since their product is, say $2b = A^3, a - b = B^3, a + b = C^3$ and we have $C^3 - B^3 = A^3$. An equation of the form $X^3 + Y^3 = Z^3$ can then be found in the same way as in the previous case where $Z^3 < z^3$. Again, by infident descent, this means that $x^3 + y^3 = z^3$ cannot be solved in positive integers. □

3.2.3 Filling the gap

The proof of the existence of a, b s.t. the factorization of p, q above that is provided in this section is due to Gauss and his work in $\mathbb{Z}[\sqrt{-3}]$. Before the lemma can be stated and proved, it first has to be shown that the above factorization of p, q has an equivalent factorization in $\mathbb{Z}[\sqrt{-3}]$. Recall that $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. It is a ring under the operations of addition and multiplication defined respectively by $(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3}$ and $(a + b\sqrt{-3})(c + d\sqrt{-3}) = ac + ad\sqrt{-3} + bc\sqrt{-3} + ad(-3) = (ac - 3ad) + (ad + bc)\sqrt{-3}$. The associative, distributive, and commutative laws apply, even to multiplication. Thus, $\mathbb{Z}[\sqrt{-3}]$ forms a commutative ring with unit.

The idea behind working in $\mathbb{Z}\sqrt{-3}$ is the factorization of $p^2 + 3q^2$ in it. Instead of the identity that we had in Proposition 3.7, we have the factorization $p^2 + 3q^2 = (p + q\sqrt{-3})(p - \sqrt{-3})$. If one of the these factors is a cube, suppose $(p + q\sqrt{-3}) = (a + b\sqrt{-3})^3$, then the complex conjugate's cube will be equal to $p - q\sqrt{-3}$, i.e. $p - q\sqrt{-3} = (a - b\sqrt{-3})^3$ (this can be seen by applying the binomial theorem to $(a + b\sqrt{-3})^3$ and then taking its conjugate, which factors into $(a - b\sqrt{-3})^3$), so from the commutavity of

multiplication, $(p+q\sqrt{-3})(p-q\sqrt{-3}) = [(a+b\sqrt{-3})(a-b\sqrt{-3})]^3$. From the Binomial theorem, $p+q\sqrt{-3} = (a+b\sqrt{-3})^3 = a^3+3a^2b\sqrt{-3}+3ab^2i^2+b^3(-3)\sqrt{-3} = (a^3-3ab^2)+3(a^2b-b^3)\sqrt{-3}$. So it suffices to find integers a, b s.t. $p = a^3-3ab^2, q = 3(a^2b-b^3)$, which is just the desired conclusion from the previous section.

Lemma 3.15 *Let a, b be relatively prime numbers s.t. a^2+3b^2 is a cube. Then $\exists$ integers p, q s.t. $a+b\sqrt{-3} = (p+q\sqrt{-3})^3$*

Before we can prove this lemma, we need some technical results about the factorization of elements in $\mathbb{Z}[\sqrt{-3}]$.

Proposition 3.16 *If a, b are relatively prime integers and if a^2+3b^2 is even then $a+b\sqrt{-3}$ can be written in the form $(1\pm\sqrt{-3})(u+v\sqrt{-3})$.*

Proof Since a^2+3b^2 is even, a and b must be of the same parity, and since they are relatively prime, a, b must both be odd. Therefore, they are of the form $4n\pm 1$. Now, either $4|(a+b)$ or $4|(a-b)$. Assume the first. Then $4(a^2+3b^2) = (1^2+(3)1^2)(a^2+3b^2) = (a-3b)^2+3(a+b)^2$. 4^2 divides this equation, so we have $\frac{a^2+3b^2}{4} = \frac{(a-3b)}{4}^2 + \frac{3(a+b)}{4}^2 = u^2+v^2$ for some u, v integers. Then, factorizing the equation in $\mathbb{Z}[\sqrt{-3}]$ gives $\frac{(a+b\sqrt{-3})(a-\sqrt{-3})}{4} = (u+v\sqrt{-3})(u-v\sqrt{-3})$. Therefore, $u+v\sqrt{-3} = \frac{(1+\sqrt{-3})(a+b\sqrt{-3})}{4}, u-v\sqrt{-3} = \frac{(1-\sqrt{-3})(a-b\sqrt{-3})}{4}$. We conclude that $a+b\sqrt{-3} = (u+v\sqrt{-3})(1-\sqrt{-3})$, which is what was desired.

Now suppose $4|(a-b)$.. Then a similar argument to the above shows that $a-b\sqrt{-3} = (u-v\sqrt{-3})(1+\sqrt{-3})$ for suitvable u, v. Not that u, v are relatively prime, else a, b would not be. Also, $a^2+3b^24(u^2+3v^2)$. □

Proposition 3.17 *If a, b are relatively prime and if a^2+3b^2 is divisible by the odd prime P then P can be written in the form p^2+3q^2 with p, q positive integers and $a+b\sqrt{-3} = (p\pm q\sqrt{-3})(u+v\sqrt{-3})$ where the sign is appropriately chosen and where u, v are integers.*

Proof Note that the first statement is just Proposition 3.12. Now, we have that either $P|(pb+aq)$ $P|(pb-aq)$. Suppose the first. Then the equation $P(a^2+3b^2) = (p^2+3q^2)(a^2+3b^2) = (pa-3qb)^2+3(pb+aq)^2$ is divisble by P^2 and we have $\frac{a^2+3b^2}{P}$ in the form u^2+3v^2, where $u = \frac{pa-3qb}{P}, v = \frac{pb+aq}{P}$, and in $\mathbb{Z}[\sqrt{-3}]$, $u+v\sqrt{-3} = (p+q\sqrt{-3})\frac{a+b\sqrt{-3}}{P}$, which implies that $a+b\sqrt{-3} = (u+v\sqrt{-3})(p-q\sqrt{-3})$.

Now suppose the latter. A similar argument reveals that $a-b\sqrt{-3} = (p+q\sqrt{-3})(u+\sqrt{-3})$, where u, v are relatively prime and $a^2+3b^2 = P(u^2+4v^2)$. $\square$

Proposition 3.18 *Let a, b be relatively prime. Then $a+b\sqrt{-3}$ can be written in the form $\pm(p_1 \pm q_1\sqrt{-3})(p_2 \pm q_2\sqrt{-3})...(p_n \pm q_n\sqrt{-3})$, where the p's and q's are positive integers and ${p_i}^2 + 3{q_i}^2$ is either 4 or an odd prime.*

Proof If a^2+3b^2 is even, then it is divisible by 4. If a^2+3b^2 is not 1 then it has a factor P equal to 4 or an odd prime, and from the previous two propositions, we have either $a+b\sqrt{-3} = (p \pm q\sqrt{-3})(u+v\sqrt{-3})$ where $p^2+3q^2 = P$. Now, u, v are relatively prime, and from the above decomposition of $a+b\sqrt{-3}$, taking a $p \pm q\sqrt{-3}$ out of $u+v\sqrt{-3}$ is the same as taking one out of $a+b\sqrt{-3}$. We have that $u^2+3v^2 = \frac{a^2+3b^2}{P} < a^2+3b^2$, so by repeating this process, we know that it must stop, i.e. we will reach a stage where $a+b\sqrt{-3} = (p_1 \pm q_1\sqrt{-3})(p_2 \pm q_2\sqrt{-3})...(p_n \pm q_n\sqrt{-3})(u+v\sqrt{-3})$ where $u^2+3v^2 = 1$. Thus, $u = \pm 1, v = 0$, and we have the desired result. $\square$

Proposition 3.19 *Let a, b be relatively prime. Then the factors in the above factorization of $a+b\sqrt{-3}$ are completely determined, except for the choice of sign as indicated, by the fact that $({p_1}^2+3{q_1}^2)({p_2}^2+3{q_2}^2)...({p_n}^2+3{q_n}^2) = (a^2+3b^2)$ is a factorization of a^2+3b^2 into odd primes and 4's. Moreover, if the factor $p+q\sqrt{-3}$ occurs then the factor $p-q\sqrt{-3}$ does not, and this holds conversely.*

Proof In the first statement, we want to show that $p^2+3q^2 = P$ determines p, q up to a sign if P is 4 or an odd prime. If P=4, then the choice of p, q is obvious. Suppose that P is an odd prime and that a^2+3b^2 were another representation of it, then by Proposition 3.17, $a+b\sqrt{-3} = (p \pm q\sqrt{-3})(u+v\sqrt{-3})$, which implies that $P = P(u^2+3v^2)$, hence $u^2+3v^2 = 1$.

So, we have $u = \pm 1, v = 0$, so we have the desire form $a+b\sqrt{-3} = \pm(p+q\sqrt{-3})$. Now since a, b are relatively prime, then $p+q\sqrt{-3}$ and $p-q\sqrt{-3})$ would give p^2+3q^2 as a factor, which is not possible, so the second statement holds. $\square$

Proof *(Of the lemma)* Let $a^2+3b^2 = P_1P_2...P_n$ be a factorization into 4s and odd primes as in the previous proposition. Then, if this factorization contains k factors of 4, 2^{2^k} is the largest power of 2 dividing a^2+3b^2.. Since a^2+3b^2 is a cube, $2k$ (hence, a fortiori, k) must be multiples of 3. Any odd prime p in the factorization must occur with a multiplicity which is a multiple of 3, thus n is divisible by 3 and the factors $P_1P_2...P_n$ can

be arranged s.t. $P_{3k+1} = P_{3k+2} = P_{3k+3}$, whence, in the factorization of $a+b\sqrt{-3}$ given by Proposition 3.16 the factors corresponding to each group of three P's are identical because the only choice is the one of sign and we cannot have both signs. Taking one factor from each group of three and multplying them together then gives a number $c+d\sqrt{-3}$ s.t. $a+b\sqrt{-3} = \pm(c+d\sqrt{-3})^3$. Since $(-c+d\sqrt{-3})^3 = (-c-d\sqrt{-3})^3$, the desired conclusion follows. □

This completes our dicussion on Fermat's method of infinite descent. This exposition was meant to provide an introduction to method of infinite descent and how it can be used to solve various number theoretic problems. The reason that both Euler's and Gauss's proofs for the exponent n=3 for FLT was to motivate two different problems. Similar properties to those that were derived for numbers of the form a^2+3b^2 can be derived for numbers of the form a^2+2b^2, and the properties of these numbers is then used to show (via infinite descent) that the only solution to the Diophantine equation $x^2+2 = y^3$ is $(x,y) = (5,3)$. Similarly, Legendre studied the properties of elements of $\mathbb{Z}[\sqrt{-5}]$ to establish Fermat's Last Theorem for the exponent n=5, and he also used the method of infinite descent. This is outlined in [1] For the motivated reader, a detailed proof can be found in Larry Freeman's blog [5]. A caveat: There might be typing mistakes present in the blog and it is a bit hard to navigate, but it is amazingly detailed. Also, Gauss's complete proof of FLT for n=3 can be seen in [3].

References

[1] H. Edwards *Fermat's Last Theorem - A Genetic Introduction to Algebraic Number Theory* 1977: Springer, NY.

[2] D. M. Burton *Elementary Number Theory* 1980: Allyn and Bacon, Inc., Boston.

[3] P. Ribenboim *13 Lectures on Fermat's Last Theorem* 1979: Springer, NY.

[4] W. Scharlau, H. Opolka *From Fermat to Minkowski: Lectures on the Theory of Numbers and its Historical Development* 1985: Springer, NY.

[5] L. Freeman*fermatslasttheorem.blogspot.com* 2009.