FERMAT'S PROOF

WAYNE AITKEN

1. Introduction

Mathematics most famous marginal note is Fermat's assertion of what is now called Fermat's Last Theorem. This was made in his edition of *Arithmetica* by Diophantus, which had recently been translated from Greek to Latin, the common language of science and all forms of learning. Fermat's note was also in Latin, and translates roughly as follows: "It is impossible for a cube and a cube to give a cube, or a fourth power and a fourth power to give a fourth power, or, more generally, for any power of degree greater than two to be the sum of two powers of the given degree. I have a truly marvelous proof for this, but this margin is too small to contain it." In other words, $x^n + y^n = z^n$ has no solution if $n > 2$ and if x, y, z are required to be positive integers.

What is less known is that Fermat *was* able to fit a proof of a related result in the margin in a later section of this same book. The result in this other marginal note can be used to give a quick proof of the $n = 4$ case of Fermat's Last Theorem. It is not known whether he proved the $n = 4$ case in this way, or saw the connection between the two marginal notes. However, it is believed that Fermat did have some sort of proof of the $n = 4$ case of "Fermat's Last Theorem" since it can be proved with techniques well-known to Fermat, and since he claimed to be able to prove the $n = 3$ and $n = 4$ cases in several letters. In contrast, Fermat never publically claimed a proof of the general case ($n > 4$). The claim was confined to the above mentioned marginal note written apparently only for himself.

The result that Fermat stated in this later marginal note is related to Pythagorean triples, right triangles with all three sides of integral length:[1]

Main Theorem 1. *It is impossible for a right triangle with sides all of integral length to have square area.*

As part of his proof of the above theorem, Fermat also proved the following interesting theorem:

Main Theorem 2. *It is impossible for two positive square integers to have a sum and a difference that are both positive square integers.*

The proof he gives is sketchy. Fermat himself realized this and ended this long marginal note with the statement "The margin is too small to allow me to give a complete proof with all the details."

His proof is based on a technique he developed which he called the *method of descent*. Basically one shows that a solution to a problem, if it exists, can be

Date: September 26, 2010.

[1]Diophantus, hence Fermat, also considered right triangles with rational sides, but for all the problems considered here, the rational case reduces to the integral case

used to produce a strictly smaller solution (where size is measured by some natural number). The existence of any solution then leads to a contradiction since there are no strictly decreasing infinite sequences of postive integers. In what follows we will measure the size of a Pythagorean triple by taking the maximum of the triple, in other words, the lenghth of the corresponding hypotenuse.

The purpose of this note is to give proofs to the above two theorems. I roughly follow Fermat's sketch but I take a few liberties. In any case the argument uses only tools and ideas available to Fermat, although dressed up in modern notation. A similar reconstructed proof can be found in Harold M. Edwards very useful book *Fermat's Last Theorem* published by Springer-Verlag. In fact, I was inspired to develop my version after seeing Edwards's version. Edwards himself follows Dickson's reconstruction of the gaps in Fermat's proof. I differ from Edwards, and Fermat himself, in certain aspects of the organization, and in how I prove the $n = 4$ case of Fermat's Last Theorem from these results.

2. Pythagorean Triples

Let a, b, c be positive integers such that $a^2+b^2 = c^2$. Of course, these correspond to right triangle with integer sides a, b, c. Such triples are called *Pythagorean triples*. This terminology is traditional and common, although it is well-known since the 1930's that such triples appeared much earlier than the time of Pythagoras on cuneiform tablets in Mesopotamia.

Observation. *If the integer $d > 1$ divides each of a, b, c, then $(a/d), (b/d), (c/d)$ is also a Pythagorean triple.*

If no such $d > 1$ exists, we call (a, b, c) a *primitive Pythagorean triple*.

Observation. *The Pythagorean triple (a, b, c) is primitive if and only if (a, b, c) are pairwise relatively prime. If any two of the three are relatively prime, then the triple is primitive.*

For the remainder of this section, we assume that (a, b, c) is a primitive Pythagorean triple. Also we assume a is odd: a and b cannot both be even by the proceeding observation, so we switch a, b if necessary so that a is odd.

By looking at solutions to $x^2 + y^2 \equiv z^2$ modulo 4 we get the following:

Observation. *Both a and c are odd, and b is even.*

We rewrite the equation $a^2 + b^2 = c^2$ as follows:

$$\frac{c+a}{2}\,\frac{c-a}{2} = \left(\frac{b}{2}\right)^2.$$

Note that any common divisor of $(c+a)/2$ and $(c-a)/2$ would divide their sum c and difference a, but a and c are relatively prime. Thus

Observation. *The integers $(c + a)/2$ and $(c - a)/2$ are relatively prime, so both are squares since their product is a square.*

Let p and q be such that $p^2 = (c + a)/2$ and $q^2 = (c - a)/2$. This immediately gives the following.

Observation. *There are relatively prime integers $p > q > 0$ such that*

$$a = p^2 - q^2, \qquad b = 2pq, \qquad c = p^2 + q^2.$$

Since a and c are odd, p and q cannot both be odd:

Observation. *The integers p and q defined above have different parities. In other words, they differ modulo 2.*

Conversely, given $p > q > 0$ of different parities and relatively prime, the above formulas are easily seen to give primitive Pythagorean triples. This method of generating all Pythagorean triples was well-known even by the time of Diophantus, and by Fermat and his contemporaries.

3. Reduction Lemmas

The best strategy for proving the two main theorems is to, in some sense, prove them at the same time. More specifically, we will set up a descent that snakes between the two problems. Recall that we will use c as the measure of the size of a pythagorean triple (a, b, c).

Lemma 1. *Suppose x, y, z, w are postive integers such that $x^2 + y^2 = z^2$ and $x^2 - y^2 = w^2$. Also suppose x and y are relatively prime (we can always reduce to this case). Then (1) x, z and w are odd, and y is even, (2) $u = (z + w)/2$ and $v = (z - w)/2$ satisfy the equations*

$$u^2 + v^2 = x^2 \qquad \frac{1}{2}uv = \left(\frac{y}{2}\right)^2,$$

and (3) u and v are relatively prime. In particular, (u, v, x) is a smaller primitive Pythagorean triple than (x, y, z), and yields a right triangle with square area.

Proof. Part 1, concerning the parity of x, y, z, w, is obtained by looking at the given equations modulo 4. Part 2 is a simple calculation. Part 3 is established by noting that any common divisor of u, v is a common divisor of $z = u + v$ and $w = u - v$, and any common divisor of z and w is a divisor of $2x^2 = z^2 + w^2$ and $2y^2 = z^2 - w^2$. Since z and w are odd, and x^2 and y^2 are relatively prime (since x and y are), the result follows. □

Lemma 2. *Suppose (a, b, c) is a primitive Pythagorean triple such that the area of the corresponding right triangle is a square:*

$$\frac{1}{2}ab = d^2$$

for some integer d. Then there is a primitive pythagorean triple (m, n, s) of smaller size such that $m^2 - n^2$ is also a square. In particular, the sum and difference of m^2 and n^2 are squares.

Proof. As discussed about, the triple (a, b, c) can be expressed in terms of relatively prime integers p, q such that $p > q > 0$ and such that p and q have opposite parities. So

$$(a, b, c) = (p^2 - q^2,\ 2pq,\ p^2 + q^2).$$

Thus

$$d^2 = \frac{1}{2}ab = pq(p^2 - q^2) = pq(p + q)(p - q).$$

Note that the four integers p, q, $p + q$, $p - q$ are pairwise relatively prime (for example, any common divisor of $p + q$ and $p - q$ divides the sum $2p$ and the difference $2q$, but $p + q$ is odd so any such divisor divides p and q). Since their

product is a square, each of p, q, $p+q$, $p-q$ is a square. Write $p = m^2, q = n^2$, and $p+q = s^2$. The result follows easily from this and the observation that

$$s < s^2 = p + q < p^2 + q^2 = c.$$

□

4. Main Results

We are now in a position to prove either of the main theorems. Which one to prove first is a mater of taste. Fermat's marginal note describes the descent that proves Main Theorem 2, and we will follow his lead.

Suppose x_0, y_0 are two positive integers such that $x_0^2+y_0^2$ and $x_0^2-y_0^2$ are squares. After dividing by the greatest common divisor, we can assume that x_0, y_0 are relatively prime. Thus x_0 and y_0 are a part of a primitive Pythagorean triple (x_0, y_0, z_0). Lemma 1 produces a smaller Pythagorean triple, and if we apply Lemma 2 to that triple we get a yet smaller primitive Pythagorean triple (x_1, y_1, z_1) such that $x_1^2+y_1^2$ and $x_1^2 - y_1^2$ are squares. Continuing in this way we produce an infinite sequence of primitive Pythagorean triples (x_i, y_i, z_i). So $z_0 > z_1 > z_2 > \cdots$, which is clearly impossible.

This contradiction establishes Main Theorem 2. There is no need to prove Main Theorem 1 by descent. We merely note that Lemma 2 combined with Main Theorem 2 yields Main Theorem 1.

Finally, we show how Main Theorem 2 also yields a short proof of the $n = 4$ case of Fermat's Last Theorem.

Corollary 3. *There are no positive integers x, y, z such that $x^4 + y^4 = z^4$.*

Proof. Suppose that such a triple (x, y, z) exists. By dividing all three integers by the greatest common divisor of x and y, we reduce to the case where x and y are relatively prime. This implies that (x^2, y^2, z^2) is a primitive Pythagorean triple, and so there are relatively prime positive integers p and q such that

$$(x^2,\, y^2,\, z^2) = (p^2 - q^2,\, 2pq,\, p^2 + q^2).$$

Thus the sum and difference of p^2 and q^2 are both squares, contradicting Main Theorem 2. □

5. Related Results

Edwards points out that if a, b, c are positive solutions to $a^4 + b^4 = c^4$ then $(x, y, z) = (c, b, a^2)$ is a solution to $x^4 - y^4 = z^2$. He also points out that the equation $x^4 - y^4 = z^2$ can be shown to have no positive integer solution using the main theorems discussed above. This gives another path to establishing Fermat's Last Theorem for $n = 4$.[2]

Theorem 4. *There are no positive integers x, y, z such that $x^4 - y^4 = z^2$.*

[2] I do not think it is an easier path, nor that it is more likely the path Fermat actually followed. But since the theorem concerning $x^4 - y^4 = z^2$ is stronger than the $n = 4$ case of Fermat's Last Theorem, since it is of independent interest, and since it follows easily from the main theorems, it is worth supplying the proof.

Proof. Suppose otherwise that (x, y, z) is a solution. Suppose first that x and y are divisible by a prime p. Then z is divisible by p^2. In this case we replace (x, y, z) with $(x/p, y/p, z/p^2)$ to get a smaller solution. In this way we eventually arrive at a solution with x and y relatively prime.

We first consider the case where x and y have opposite polarities. Consider the equation

$$(x^2 + y^2)(x^2 - y^2) = z^2.$$

The two terms x^2+y^2 and x^2-y^2 are relatively prime: any common divisor divides the sum $2x^2$ and the difference $2y^2$. Since x^2+y^2 is odd, any common divisor is odd, so actually divides x^2 and y^2 which are relatively prime. Since they are relatively prime, we conclude that $x^2 + y^2$ and $x^2 - y^2$ are both squares, contracting Main Theorem 2.

The remaining case is where x and y are odd, so z is even. Then we have

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

We observe that $u = (x^2 + y^2)/2$ and $v = (x^2 - y^2)/2$ are relatively prime since their sum is x^2 and their difference is y^2. Thus u and v are squares. However, $u + v = x^2$ and $u - v = y^2$ again contradicting Main Theorem 2. □

Most arguments given nowadays for the proof of Fermat's Last Theorem for the case $n = 4$ follows the following strategy. Observe that if $a^4+b^4 = c^4$ then (a, b, c^2) is a solution to $x^4+y^4 = z^2$. So the proof reduces to proving the following theorem. This gives a third path to the result. The proof given here of the following theorem is the usual proof, and is independent of the Main Theorems above. It is given so that the reader can compare the complexity of the various approaches. Edwards suggests that proving Fermat's Last Theorem for the case $n = 4$ using the following theorem is the most direct method, I personal favor the approach of proving Main Theorem 2 by descent, and then proving Fermat's Last Theorem as a corollary.

Theorem 5. *There are no positive integers x, y, z such that $x^4 + y^4 = z^2$.*

Proof. Suppose (x, y, z) is a solution. Suppose first that x and y are divisible by a prime r. Then z is divisible by r^2. In this case we replace (x, y, z) with $(x/r, y/r, z/r^2)$ to get a smaller solution. In this way we eventually arrive at a solution (x_0, y_0, z_0) with x_0 and y_0 relatively prime. By symmetry we can assume x_0 is odd.

Since (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple, we can find positive $p > q$ that are relatively prime such that $x_0^2 = p^2 - q^2$, $y_0^2 = 2pq$ and $z_0 = p^2 + q^2$, and such that p and q have opposite parities.

In particular, (x_0, q, p) is a Pythagorean triple. Since p and q are relatively prime, it is primitive Pythagorean triple. This implies that p is odd. Since p and q have opposite parities, we conclude that q is even. So we can find positive $P > Q$ that are relatively prime such that $x_0 = P^2 - Q^2$, $p = 2PQ$ and $q = P^2 + Q^2$. Hence

$$\left(\frac{y_0}{2}\right)^2 = \frac{1}{4}y_0^2 = \frac{1}{4}(2pq) = PQ(P^2 + Q^2).$$

Since P and Q are relatively prime, P, Q, P^2+Q^2 must be pairwise relatively prime. Since their product is a square, it follows that P, Q, P^2+Q^2 are individually squares. So we can find x_1, y_1, z_1 so that $P = x_1^2$, $Q = y_1^2$ and $P^2 + Q^2 = z_1^2$. In particular, (x_1, y_1, z_1) is another solution to $x_1^4 + y_1^4 = z_1^2$. Since P and Q are relatively

prime, x_1, y_1 are relatively prime. So from the solution (x_0, y_0, z_0) with relatively prime x_0, y_0 we can generate a solution (x_1, y_1, z_1) with relatively prime x_1, y_1. The resulting solution is in smaller in the sense that

$$z_1^2 = P^2 + Q^2 = p + q < p^2 + q^2 = z_0 < z_0^2.$$

Repeating gives a descending sequence of positive integers $z_0 > z_1 > z_2 > \cdots$, an impossibility. $\square$