SPECIAL CASES OF FERMAT'S LAST THEOREM

EZRA FURTADO-TIWARI

Abstract.
We summarize various important results from Euler's paper
"E098: Theorematum quorundam arithmeticorum demonstrationes"
(Proofs of certain arithmetic theorems). [Eul47]

1. Sums of Squares

We start by introducing some interesting results about sums of squares. First, Euler converted Pythagorean triples into a simpler form.

Lemma 1.1. *If $a^2 + b^2 = c^2$ for positive integers a, b, c (such that $\gcd(a, b) = 1$) then $a = p^2 - q^2$ and $b = 2pq$ or $b = p^2 - q^2$ and $a = 2pq$, where p and q are relatively prime and $p \not\equiv q \pmod 2$.*

Proof. Let $\sqrt{a^2 + b^2}$ be represented by $a + b\frac{q}{p}$, where q and p are relatively prime. Then

$$a^2 + b^2 = a^2 + \frac{2abq}{p} + \frac{(bq)^2}{p^2}.$$

Simplifying, we find

$$b^2 = \frac{2abq}{p} + \frac{(bq)^2}{p^2}$$

and thus

$$\frac{a}{b} = \frac{p^2 - q^2}{2pq}.$$

It follows from this equation that

$$a = p^2 - q^2$$

and

$$b = 2pq,$$

as a and b are assumed to be relatively prime. Additionally, p and q must be of different parities in order to ensure that the numerator and denominator are relatively prime. ∎

Corollary 1.2. *If a and b are coprime odd integers, then $a^2 + b^2$ is not a square.*

To prove the above corollary, we note that $a^2 = (p^2 - q^2)^2$, which is odd, and $b^2 = (2pq)^2$, which is even.

Corollary 1.3. *If a and b are coprime integers and $a^2 + b^2$ is a square, then either $a \equiv 0 \pmod 3$ or $b \equiv 0 \pmod 3$.*

Date: August 19, 2023.

Proof. Assume that at least one of p and q is congruent to $0 \mod 3$. Then clearly $b = 2pq \equiv 0 \pmod 3$. This leaves us to check the case in which $p, q \not\equiv 0 \pmod 3$. Then $p^2 \equiv 1 \pmod 3$ and $q^2 \equiv 1 \pmod 3$, so $a = p^2 - q^2 \equiv 0 \pmod 3$. ■

Lemma 1.4. *If $a^2 - b^2$ is a square, then $a = p^2 + q^2$ and either $b = p^2 - q^2$ or $b = 2pq$ where p and q are coprime and $p \not\equiv q \pmod 2$.*

Proof. Let $a^2 - b^2 = c^2$. Then $a^2 = b^2 + c^2$ for coprime b and c, so $b = p^2 - q^2$ and $c = 2pq$ or $c = p^2 - q^2$ and $b = 2pq$ (by Lemma 1.1). In both cases, we have $a = p^2 + q^2$. ■

Corollary 1.5. *If $a^2 - b^2 = c^2$, then either a, b, or c is divisible by 5.*

Proof. We can let $a = p^2 + q^2$ and $b = p^2 - q^2$ or $2pq$ (so that c is the other expression). Clearly if p or q is divisible by 5 then $2pq$ will be divisible by 5. Otherwise, $p^2 \equiv \pm 1 \pmod 5$ and $q^2 \equiv \pm 1 \pmod 5$, so either $p^2 + q^2$ or $p^2 - q^2$ must be divisible by 5. ■

2. Sums of Fourth Powers

Euler chose to investigate similar forms with fourth powers, concluding that certain expressions cannot be squares. He started by proving Fermat's Last Theorem in the $n = 4$ case.

Theorem 2.1. *If a and b are positive integers, then $a^4 + b^4$ is not a square.*

Proof. We will show that if a and b are positive integers satisfying the condition given, we can construct smaller a and b that also satisfy this, showing that there is no smallest pair (a, b) among positive integers such that $a^4 + b^4$ is a square. As a result, we can assume a and b are relatively prime, so that a is odd and b is even. Thus we may write $a^2 = p^2 - q^2$ and $b^2 = 2pq$, where p and q are coprime positive integers of different parities. But notice that because $p^2 - q^2 = a^2$, p is in the form $m^2 + n^2$ for some coprime m and n of different parities, so p is odd.

Additionally, $2pq$ is a square, and since p and q are relatively prime, $2q$ and p must both be squares. We may also write $q = 2mn$ for the same m, n defined previously.

We note that $2q = 4mn$ must be a square, so m and n must individually be squares as well. Thus we may let $m = x^2$ and $n = y^2$, so that

$$p = m^2 + n^2 = x^4 + y^4.$$

Thus we have constructed a smaller pair of positive integers such that $x^4 + y^4$ is a square. We may repeat this process infinitely to show that there are no positive integers satisfying our condition.

■

Euler proved a stronger result than Fermat's Last Theorem for $n = 4$, but we may reduce this case of Fermat's Last Theorem to a case of Theorem 2.1.

Corollary 2.2. *There are no positive integer solutions to the equation $a^4 + b^4 = c^4$.*

Euler also considered some other expressions of similar degree, including multiple different combinations of two variables.

Corollary 2.3. *If a and b, and $a^2 + b^2$ are positive integers, then $ab(a^2 + b^2)$ cannot be a square.*

Proof. Note that if $ab(a^2+b^2)$ is a square, then a, b, a^2+b^2 would need to individually be squares, as they are pairwise coprime. Then $a^2+b^2 = m^4+n^4$ would need to be a square, which is impossible. ■

Theorem 2.4. *If a and b are distinct positive integers, then a^4-b^4 cannot be a square.*

We can split this proof into multiple cases, based on the parity of b.

Lemma 2.5. *If a and b are distinct positive integers and b is even, then a^4-b^4 cannot be a square.*

Proof. We can write $a^2 = p^2+q^2$ and $b^2 = 2pq$, where p and q are coprime positive integers, p is even, and q is odd. Because $p^2+q^2 = a^2$, we can write p and q as $q = m^2-n^2$ and $p = 2mn$. But $2p = 4mn$ is a square as $2pq$ is a square for relatively prime p, q, so $m = x^2$ and $n = y^2$ for some smaller relatively prime positive integers x, y. However, this would imply that $q = m^2-n^2 = x^4-y^4$, so we would have found smaller solutions to our equation, proving that there are none. ■

Lemma 2.6. *If a and b are distinct positive integers and b is odd, then a^4-b^4 cannot be a square.*

Proof. Because b is odd, we can write $a^2 = p^2+q^2$ and $b^2 = p^2-q^2$. As p^2+q^2 is a square, we know that q is even and p is odd. But then $a^2b^2 = p^4-q^4$, which is a square, but q is even, so this is impossible. Thus there are no distinct positive a, b such that b is odd and a^4-b^4 is a square. ■

Combining our lemmas above gives a proof of Theorem 2.4.

Theorem 2.7. *If a and b are distinct positive integers, then $2a^4+2b^4$ cannot be a square.*

Proof. Assume that a and b are relatively prime (if not, we can simply divide a and b by $\gcd(a,b)$). If one of a or b were even then we would have $2a^4+2b^4 \equiv 2 \pmod 4$, which is impossible. Thus both a and b must be odd.

Then a^2+b^2 and a^2-b^2 must both be even. Thus we can rewrite our expression as

$$\left(\frac{a^2+b^2}{2}\right)+\left(\frac{a^2-b^2}{2}\right)$$

where $\frac{a^2+b^2}{2}$ and $\frac{a^2-b^2}{2}$ are relatively prime positive integers, such that the first is odd and the second form is even. Then we can write $\frac{a^2+b^2}{2} = p^2-q^2$ and $\frac{a^2-b^2}{2} = 2pq$ for p and q. Thus

$$a^2 = p^2+2pq-q^2$$

and

$$b^2 = p^2-2pq-q^2,$$

so

$$a^2-b^2 = (a+b)(a-b) = 4pq.$$

Then $a+b = \frac{2mp}{n}$ and $a-b = \frac{2nq}{m}$, so that $a = \frac{mp}{n}+\frac{nq}{m}$ and $b = \frac{mp}{n}-\frac{nq}{m}$. From here we find

$$\frac{m^2}{n^2}p^2+\frac{n^2}{m^2}q^2 = p^2-q^2$$

so that

$$\frac{p^2}{q^2} = \frac{n^2(m^2+n^2)}{m^2(n^2-m^2)} = \frac{n^2(n^4-m^4)}{m^2(n^2-m^2)^2}.$$

However, this means that $n^4 - m^4$ is a square, which is impossible. Thus p and q cannot exist and neither can a and b. ■

Theorem 2.8. *If a and b are distinct positive integers, then $2a^4 - 2b^4$ cannot be a square.*

Proof. Assume a and b are relatively prime; clearly a and b must both be odd. Then $2(a+b)(a-b)(a^2+b^2) = 2a^4 - 2b^4$ must be a square, and so must be $\left(\frac{a+b}{2}\right)\left(\frac{a-b}{2}\right)\left(\frac{a^2+b^2}{2}\right)$. The terms in this product are pairwise coprime, so each term must be a square. Thus we can let $\frac{a-b}{2} = p^2$ and $\frac{a+b}{2} = q^2$, so that $a = p^2 + q^2$ and $b = q^2 - p^2$. Then $\frac{a^2+b^2}{2} = p^4 + q^4$, but $p^4 + q^4$ cannot be a square, so $2a^4 - 2b^4$ cannot be a square either. ■

3. Additional Arithmetic Theorems

After showing that various expressions cannot be squares, Euler turned his attention to the $n = 6$ case of Fermat's Last Theorem, as well as another theorem by Fermat about triangular numbers.

Theorem 3.1 (Fermat)**.** *If n is a triangular number, meaning that $n = \frac{k(k+1)}{2}$ for some k, then n cannot be a fourth power unless $n = 1$.*

Proof. This is equivalent to showing that unless $k = 1$, $\frac{k(k+1)}{2}$ cannot be a fourth power. We can consider cases where k is even and odd independently. If k is even, then we have $\frac{k(k+1)}{2} = (k+1)\left(\frac{k}{2}\right)$, and if k is odd, we have $\frac{k(k+1)}{2} = k\left(\frac{k+1}{2}\right)$. Both terms are relatively prime in both cases; in the first, we can let $k = 2m^4$ so that $k+1 = 2m^4+1$ must be a fourth power. In the second case, we can let $k+1 = 2m^4$, so that $2m^4 - 1$ must be a fourth power. Let $n^4 = 2m^4 \pm 1$; multiplying this equation by 2 and rearranging gives us $4m^4 = 2n^4 \pm 2$. However, $4m^4$ is a square, and we have shown that $2a^4 \pm 2b^4$ cannot be a square, so there are no solutions to this equation. Thus there are no triangular numbers that are fourth powers (unless $n = 1$). ■

Theorem 3.2. *If $\frac{a}{b}$ is a positive rational number, then $\frac{a^3}{b^3} + 1$ is not a square unless $\frac{a}{b} = 2$.*

Proof. We can reduce this to showing that $a^3b + b^4$ cannot be a square unless $a = 2b$. We can factorize this as $b(a+b)(a^2 - ab + b^2)$, which we can substitute c for $a + b$ in to find $b(a+b)(a^2 - ab + b^2) = bc(c^2 - 3bc + 3b^2)$. We need to show that this cannot be a square unless $c = 3b$. Additionally, we know that b and c are relatively prime.

We consider two cases; one where c is a multiple of 3, and one where c is not.

If c is not divisible by 3, then each of the factors b, c, and $c^2 - 3bc + 3b^2$ are squares. Let $c^2 - 3bc + 3b^2 = \left(\frac{m}{n}b - c\right)^2$, so that

$$\frac{b}{c} = \frac{3n^2 - 2mn}{3n^2 - m^2}$$

or

$$\frac{b}{c} = \frac{2mn - 3n^2}{m^2 - 3n^2}.$$

The numerator and denominator of these fractions are coprime unless m is a multiple of 3. We first assume that m is not divisible by 3. Thus either $c = 3n^2 - m^2$ or $c = m^2 - 3n^2$, but only the latter is possible as $m^2 \equiv 1 \pmod 3$. Then let $\sqrt{c} = m - \frac{p}{q}n$, so that $\frac{m}{n} = \frac{3q^2+p^2}{2pq}$ and

$$\frac{b}{n^2} = \frac{2m}{n} - 3 = \frac{3q^2 - 3pq + p^2}{pq}.$$

Then $pq(3q^2 - 3pq + p^2)$ is also a square, so we have found a smaller solution.

Now, assume that m is divisible by 3, so that $m = 3k$. Then

$$\frac{b}{c} = \frac{n^2 - 2kn}{n^2 - 3k^2},$$

so $c = n^2 - 3k^2$. Again, we let $\sqrt{c} = n - \frac{p}{q}k$, so that $\frac{k}{n} = \frac{2pq}{3q^2+p^2}$ and thus

$$\frac{b}{n^2} = 1 - \frac{2k}{n} = \frac{p^2 + 3q^2 - 4pq}{3q^2 + p^2}.$$

Then $(p^2 + 3q^2)(p - q)(p - 3q)$ should be a square; setting $p - q = t$ and $p - 3q = u$ gives $(p^2 + 3q^2)(p - q)(p - 3q) = tu(3t^2 - 3tu + u^2)$, which is another smaller solution.

Last, we need to check the case in which c is a multiple of 3. Letting $c = 3d$, we find that $bd(b^2 - 3bd + 3d^2)$ will also be a square, so we are done.

■

We can use a very similar proof to show that $\frac{a^3}{b^3} - 1$ is also not a square.

Corollary 3.3. *If a and b are positive integers, then neither $a^6 + b^6$ nor $a^6 - b^6$ can be a square.*

Clearly we cannot have $\frac{a^6}{b^6} = 2$, so this follows from Theorem 3.2.

Corollary 3.4. *There are no positive integer solutions to the equation $a^6 + b^6 = c^6$.*

Again, we restate this result in terms of Fermat's Last Theorem, as this is a stronger version of the case in which $n = 6$.

4. Conclusion

Euler considered various different expressions to determine which could be squares and which could not, which he used to prove special cases of Fermat's Last Theorem. We looked at some of the results, which generally used a proof style involving constructing the smallest solution and proving that a smaller solution could be constructed from it.

References

[Eul47] Leonhard Euler. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae*, 10:125–146, 1747.