On Fermat's Last Theorem

by Hagop Taminian

Harvard University

> *"And perhaps, posterity will thank me for having shown it that the ancients did not know everything." - Pierre de Fermat (1601-1665)*

Introduction

$$x^n + y^n \neq z^n \text{ for an integer } n > 2 \text{ with } x, y, z \neq 0$$

In this paper, I present a proof of Fermat's Last Theorem for n=3, n=4 and a special case of the theorem when x=y for general n. I also provide proofs for the irrationality of e and π.

Section 1

In this section, I present Fermat's proof of the case n=4 using his infinite descent argument.

Lemma 1. *If $x^4 + y^4 = z^2$ has integer solutions where $x, y, z \in \mathbb{Z}^+$, then there exists $a, b, c \in \mathbb{Z}^+$ such that $a^4 + b^4 = c^2$ with $c < z$.*

Definition 2. *A fundamental Pythagorean triple is a triple (x,y,z) with x,y,z $\in \mathbb{Z}$ if $x^2 + y^2 = z^2$ and x,y, and z are coprime.*

We rewrite $x^4 + y^4 = z^2$ as

$(x^2)^2 + (y^2)^2 = z^2$ ...(1)

Assume that x,y,z are coprime. Since all numbers are either even or odd, $x \equiv 0 (\operatorname{mod} 2)$ or $x \equiv 1 (\operatorname{mod} 2)$. Therefore, $x^2 \equiv 0 (\operatorname{mod} 4)$ or $x^2 \equiv 1 (\operatorname{mod} 4)$. This means that no square can be equivalent to $2 (\operatorname{mod} 4)$ or $3 (\operatorname{mod} 4)$. Therefore, x and y cannot both be odd, since $(x^4 + y^4) \equiv 2 (\operatorname{mod} 4)$, which isn't a square. Obviously, x and y cannot both be even, since that would imply that z is even, which would mean that x,y,z have at least one common factor - a contradiction to the assumption that x,y,z are coprime. Therefore, one of x and y must be even and the other odd.

Without loss of generality, let x be even and y be odd. Then, for $m, n \in \mathbb{Z}^+$, such that m, n are coprime, we can write:

$x = 2\text{mn}$

$y = m^2 - n^2$

$z = m^2 + n^2$

(Note: this parameterization is well-known, and seeing why it is true is simple. Consider the equation

$\alpha^2 + \beta^2 = \gamma^2$, with α, β, γ coprime and such that α is even.

It follows from above that β and γ are odd. We can rewrite this as:

$\alpha^2 = \gamma^2 - \beta^2 = (\gamma - \beta)(\gamma + \beta)$

Consider an odd prime p such that p is a factor of $(\gamma - \beta)$ but not a repeated factor. Then, $p|\alpha^2$ and hence $p|\alpha$. Hence, p is a repeated factor of α^2, which means that it is a repeated factor of $(\gamma - \beta)(\gamma + \beta)$. Therefore, p must also divide $(\gamma + \beta)$. This means that p divides all of α, $(\gamma - \beta)$, $(\gamma + \beta)$, and hence, must divide $\alpha, 2\gamma, 2\beta$. But since p is an odd prime, then p also divides α, β and γ, and there is a contradiction since it was assumed that a, β, γ are coprime.

Hence, every factor of $(\gamma-\beta)$ and $(\gamma+\beta)$ other than 2 must be repeated. Note that each of α, $(\gamma-\beta)$ and $(\gamma+\beta)$ are even. Obviously, α^2 must have an even number of factors of 2. If $(\gamma-\beta)$ and $(\gamma+\beta)$ also had an even number of factors of 2, then it would follow that α, β and γ have a common factor - a contradiction. Hence, we can write

$\gamma-\beta=2\upsilon^2$ and

$\gamma+\beta=2\sigma^2$ for some $\upsilon,\sigma\in\mathbb{Z}$.

Adding these two equations gives $\gamma=\upsilon^2+\sigma^2$, and subtracting would give $\beta=\sigma^2-\upsilon^2$. It would follow by substituting for β and γ that $\alpha=2\upsilon\sigma$.)

Going back to equation (1), we see that (x^2, y^2, z) is a Pythagorean triple. There are two cases to consider now: one with x, y and z having a common prime factor, and one with x,y and z having no common factor.

Consider the first case. In other words, let p be a prime number such that x, y, and z have a common factor p. Then, we can write that the following is also a valid solution for our equation:

$(x/p)^4+(y/p)^4=(z/p^2)^2$

(Note: this is true since the multiple of any pythagorean triple is also a pythogorean triple itself)

Hence, we have found a new Pythogrean triple $(x/p, y/p, z/p^2)$ such that $z/p^2 <$ z.

Now, consider the case where x, y, z are coprime. This means, by definition 2, that if $x^4+y^4=z^2$ has solutions, then (x^2, y^2, z) is a fundamental Pythogrean triple. Recall that for m,n coprime such that m,n $\in\mathbb{Z}^+$, without loss of generality,

$x^2=2$mn ...(2)

$y^2=m^2-n^2$ ...(3)

$z=m^2+n^2$ ...(4)

Rewrite equation (3) as

$y^2+n^2=m^2$. Since m and n are coprime, then there must exist a fundamental Pythagorean triple (y,n,m) satisfying this equation. Since y^2 is odd, then y is odd, and n^2 must be even. If n^2 is even, then n is also even. Hence, once again, we can write for $r,s\in\mathbb{Z}^+$ and r,s coprime:

$n=2$rs ...(5)

$b=r^2-s^2$ ...(6)

$m=r^2+s^2$ ...(7)

Note that if the product of two coprime positive integers is a perfect square, then each is a perfect square individually.

Consider $m\cdot n/2$

$m\cdot n/2=2\text{mn}\cdot 1/4=x^2/4=(x/2)^2$

Hence, the product of m and n/2 is a square, which means that m and n/2 are each a perfect square too.

In a similar way, rs = 2rs/2 = n/2, which we just showed is a perfect square

Finally, let

$r=a^2$

$s=b^2$

$m=c^2$

Then, from equation (7),

$c^2 = a^4 + b^4$

Obviously, $c < z$ since $z = m^2 + n^2$ (from equation (4)), which means that $z = c^4 + n^2$, which means that $c^4 < z$, which implies that $c < z$.

Hence, the lemma is proved, which means that we can have an infinite sequence of decreasing integers, which is clearly impossible.

Section 2

Euler was the first to make a substantial attempt to prove the case of Fermat's Last Theorem for n=3. His proof, however, was incomplete, and his work lead to Kummer's theory of ideals. I will consider Euler's proof of the theorem for n=3 in this section in reference to L.J. Mordell's paper *"Three Lectures on Fermat's Last Theorem"*.

$x^3 + y^3 = z^3$, with $x, y, z \in \mathbb{Z}$ and x, y, z coprime ...(8)

Two of x, y, z must be odd, since if all three are even there is a common factor between them. Since x, y, z are all integers, they can take positive or negative values. Therefore, it is immaterial which two of x, y, z are odd. So assume without loss of generality that x, y are odd and z is even.

Since x, y are odd, then their difference and sums are even. This means we can write that

$x + y = 2p, p \in \mathbb{Z}$ and

$x - y = 2q, q \in \mathbb{Z}$.

Adding these two equations gives $x = p + q$ and $y = p - q$. Substituting these values in equation 8,

$(p + q)^3 + (p - q)^3 = z^3$

$\Rightarrow (p^3 + 3p^2q + 3q^2p + q^3) + (p^3 - 3p^2q + 3q^2p - q^3) = z^3$

$\Rightarrow 2p^3 + 6q^2p = z^3$

$\Rightarrow 2p(p^2 + 3q^2) = z^3$ ...(9)

Note that p and q are coprime. If p and q are both odd, then their difference is even and their sum is even, which means that x and y would be even - a contradiction since it is assumed that x and y are coprime. Also, p cannot be odd and q even. This can be seen by considering modulo arguments: first, note that any cube is equivalent to 0, 1, or 3 (mod 4). If p is odd, then $p \equiv 1 (\mathrm{mod}\, 4)$ or $p \equiv 3 (\mathrm{mod}\, 4)$. This implies that $2p \equiv 2 (\mathrm{mod}\, 4)$, and that $p^2 \equiv 1 (\mathrm{mod}\, 4)$. If q is even, then $q \equiv 0 (\mathrm{mod}\, 4)$ or $q \equiv 2 (\mathrm{mod}\, 4)$. This means that $q^2 \equiv 0 (\mathrm{mod}\, 4)$, and oviously, that $3q^2 \equiv 0 (\mathrm{mod}\, 4)$. So, from equation (9), this would imply that $z^3 \equiv 2 (\mathrm{mod}\, 4)$, which is impossible. So p cannot be odd and q even. Finally, this means that p is even and q is odd. This means that $(p^2 + 3q^2)$ is odd.

Now, since p and q are coprime, the terms $2p$ and $(p^2 + 3q^2)$ are either coprime or have a common factor of 3. I shall only consider the first case, since both cases involve the same approach:

If $2p$ and $p^2 + 3q^2$ are coprime, then each must be a perfect cube in order for z^3 to be a perfect cube. Hence, we write

$p^2 + 3q^2 = m^3$ ...(10)

These values for p, q and m can be found by taking

$m = r^2 + 3s^2$, with $r, s \in \mathbb{Z}$ ...(11)

and then

$p+q\sqrt{-3}=(r+s\sqrt{-3})^3$

Expanding,

$p+q\sqrt{-3}=r^3+3r^2s\sqrt{-3}-9s^2r-3s^3\sqrt{-3}$

Equating real and imaginary parts,

$p=r^3-9s^2r$, and ...(12)

$q=3r^2s-3s^3=3s(r^2-s^2)=3s(r-s)(r+s)$ ...(13)

(Note: finding solutions satisfying equations similar to equation (10) lead to the theory of ideals.)

In equation (13), q is odd, which implies that r is even and s is odd. If r and s are coprime, not both odd, and $3\nmid r$, then p and q are coprime and $3\nmid p$. Since $2p$ is a cube, then $2r(r+3s)(r-3s)$ is a perfect cube. Since $3\nmid r$, then $2r, r+3s, r-3s$ must be coprime. In order for both these conditions to hold, then $2r, r+3s, r-3s$ are each a cube. Hence, we write

$r+3s=a^3,\ r-3s=b^3,\ 2r=c^3$ ...(14)

Going back to equations (9), (12) and (13):

$z^3=2p(p^2+3q^2)$

$=2(r^3-9s^2r)((r^3-9s^2r)^2+3(3r^2s-3s^3)^2)$

$=2r(r^2-9s^2)(r^6-18s^2r^4+81s^4r^2+3(9r^4s^2-18r^2s^4+9s^4)$

$=2r(r-3s)(r+3s)(r^6+9r^4s^2+27r^2s^4+27s^4)$

$=2r(r-3s)(r+3s)((r^2+3s^2)(r^4+6s^2r^2+9s^4)$

$=2r(r-3s)(r+3s)((r^2+3s^2)(r^2+3s^2)(r^2+3s^2))$

$=a^3\cdot b^3\cdot c^3\cdot(r^2+3s^2)^3$

Taking the cubic root,

$z=a\cdot b\cdot c\cdot(r^2+3s^2)$ ...(15)

From equations (14), we can get

$2r=a^3+b^3\Rightarrow r=(a^3+b^3)/2\Rightarrow r^2=(a^6+2a^3b^3+b^6)/4$

$6s=a^3-b^3\Rightarrow s=(a^3-b^3)/6\Rightarrow s^2=(a^6-2a^3b^3+b^6)/36$

Substituting in (15),

$z=a\cdot b\cdot c\cdot((a^6+2a^3b^3+b^6)/4+(a^6-2a^3b^3+b^6)/12)$

$\Rightarrow z=(1/3)a\cdot b\cdot c\cdot(a^6+a^3b^3+b^6)$

Since $a,b\neq 1,\ \ z>c$. Now, using an infinite descent argument not unsimilar to that in the case for $n=4$, we can find an infinite sequence of continually decreasing integers, which is impossible.

Section 3

In this section, I provide a proof for a special case of Fermat's Last Theorem where $x=y$. First, let us consider proving the irrationality of $\sqrt{2}$, since the proof that follows makes use of similar ideas:

Definition 3. *An irrational number is a number that cannot be expressed as a fraction p/q, where $p,q\in\mathbb{Z}$ and $q\neq 0$.*

Assume that $\sqrt{2}$ *is rational. That is, assume that*

$\sqrt{2} = p/q$, *where* $p, q \in \mathbb{Z}$, $q \neq 0$, *and* p *and* q *are coprime.*

Squaring, we get

$2 = p^2/q^2 \Rightarrow 2q^2 = p^2$

Observe that the L.H.S is even, which means that p^2 *is even too. Since* p^2 *is even, it follows that* p *is even. Hence,* $p = 2a$, for some $a \in \mathbb{Z}$. *Substituting,*

$2q^2 = (2a)^2 \Rightarrow 2q^2 = 4a^2 \Rightarrow q^2 = 2a^2$

Observe that the R.H.S is even, which means that q^2 *is even. Since* q^2 *is even, it follows that* q *is even. Therefore,* p *and* q *must have at least one common factor, and there is a contradiction.* $\square$

Going back to

$x^n + y^n = z^n, x, y, z \in \mathbb{Z}$, and x, y, z coprime

We consider the case when $x = y$. We substitute in the above equation to get

$2x^n = z^n \qquad ...(16)$

This means that z^n is even, which means that z is even. Therefore, we can write

$z = 2m$ for some $m \in \mathbb{Z}$

Substituting in equation 16, we get

$2x^n = (2m)^n = 2^n m^n$

$\Rightarrow x^n = 2^{n-1} m^n$

This implies that x^n is even, which means that x, too, is even. Since both x and z are even, then they must have at least one common factor, which contradicts the assumption that they are coprime. $\square$

Section 4

In this section, I provide a simple proof for the irrationality of e.

Recall the Taylor series expansion for $e^x = 1 + x + x^2/2! + x^3/3! + ... + x^n/n! + x^{n+1} \cdot e^k/(n+1)!$ where $0 < k < x$.

Theorem. The number e is irrational.

Proof. Assume that e is rational. That is, assume

$e = p/q$, for $p, q \in \mathbb{Z}, q \neq 0$

Consider the taylor series expansion for $x = 1$:

$e = p/q = 1 + 1 + 1/2! + 1/3! + ... + 1/n! + e^k/(n+1)!$, where $0 < k < 1 \qquad ...(17)$

Take $n \in \mathbb{Z}$ such that $n \geqslant q$ and multiply (17) by $n!$,

$n!e = n!p/q = n! + n! + n!/2! + n!/3! + ... + 1 + e^k/(n+1) \qquad ...(18)$

Observe that in (18), $(n! + n! + n!/2! + n!/3! + ... + 1)$ is an integer.

Consider the term $e^k/(n+1)$. Since $n \geqslant q$ and $q \neq 1$, then $n \geqslant 2$. Hence,

$0 < e^k/(n+1) < e^k/e < 1$ for $0 < k < 1$

$\Rightarrow 0 < e^k/(n+1) < 1$

Since every term on the R.H.S in equation 18 is an integer except $e^k/(n+1)$, then the R.H.S is definitely not an integer.

Consider the L.H.S,

$n!p/q = n(n-1)(n-2)\ldots \cdot p/q$

Since $n \geqslant q$, q will cancel one of the $n(n-1)(n-2)\ldots$ terms, which means that the L.H.S is definitely an integer. Hence, there is a contradiction. $\square$

Section 5

In this section I outline Niven's proof of the irrationality of π.

Theorem. The number π is irrational.

Proof. Assume that π is rational. That is, assume

$\pi = p/q$, where $p, q \in \mathbb{Z}^+$

Define two functions $f(x)$ and $F(x)$ by

$f(x) = x^n (p - qx)^n / n!$

$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \ldots + (-1)^n f^{2n}(x)$

Notice that when $x = 0$ or $x = \pi$, $f(x)$ and its derivatives are integers. This implies that $F(0)$ and $F(\pi)$ are integers too. Consider now

$d/dx(F'(x)\sin x - F(x)\cos x) = (F''(x) + F(x))\sin x = f(x)\sin x$,

which implies

$\int_0^\pi f(x) \sin x \cdot dx = F(\pi) - F(0)$ ...(19)

is an integer. But, for $0 < x < \pi$ and sufficiently large n, we have

$0 < f(x)\sin x < \pi^n \cdot a^n / n! < 1/\pi$,

so that

$0 < \int_0^\pi f(x) \sin x \cdot dx < 1$

Which contradicts the equation (19) being an equation in integers. $\square$