Fulfillment.

Annie Raymond

May 12, 2006

Intro. "Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet." [1] How many mathematicians have been infuriated by Fermat's last theorem? How many tried to solve it? How many failed? Only one is known to have succeeded, and it is Andrew Wiles in the mid-nineties. However, his proof is extremely long and hard. It is certainly not the proof that Fermat was talking about, especially since it contains modern mathematics. Still, how could a theorem so simple require such work to prove?

Another question also arises: had Fermat really found an elegant and simple proof or was he just making it up? And, if he did, was it error-free? After all, Pierre de Fermat wasn't really a "mathematician". He was only a French lawyer who occupied his spare time with mathematics. Maybe, in order to find **his** proof (if it exists), you cannot think like a true mathematician does. Maybe you ought to be slightly illogical and childish in your approach to the proof... two things that I am. Therefore, here is, as an exercise, a very incomplete and erroneous attempt to prove Fermat's last theorem. Why would one try to do such a thing? Simply because it is incredibly fun to work on that theorem. One could even say it is addictive.

But, first, let's try to achieve an accessible goal and prove Fermat's last theorem for two particular cases: the one when $n = 4$ and the one when $n = 3$. The first one was actually proven by Fermat himself and the second one was proved by Euler. Actually, for the first case, we'll show a stronger result: we shall demonstrate that there is no solution with x, y, z integers for $x^4 + y^4 = z^2$. Here are the tools we'll need to prove it.

Lemma 1. Let's state the obvious:

1. If $(a, b) = 1$ and $x^2 = ab$, then a and b are both squares.
2. If $(a, n) = 1$ and $ax \equiv ay \pmod{n}$, then $x \equiv y \pmod{n}$.

Now, let's look at the Pythagoean equation $x^2 + y^2 = z^2$ where $(x, y, z) = 1$. Indeed, we only need to consider that case because if $(x, y, z) \neq 1$, then we have $x = \lambda\bar{x}$, $y = \lambda\bar{y}$, and $z = \lambda\bar{z}$ which gives us $\bar{x}^2 + \bar{y}^2 = \bar{z}^2$. If I multiply this equation by λ^2, I trivially get $x^2 + y^2 = z^2$.

Thus, considering what we have said before and the fact that $(x, y, z) = 1$, then $(x, y) = 1$, $(x, z) = 1$, and $(y, z) = 1$. Now, let's do a parity table for $x^2 + y^2 = z^2$:

x	y	z
even	even	even
even	odd	odd
odd	even	odd
odd	odd	even

The first case is impossible because 2 is a common factor. The last case is also impossible because $\text{odd}^2 + \text{odd}^2 \equiv 2 \pmod{4}$, which means that z^2 can be divided by 2, but not by 4. However, we also know that $2 \mid z^2$, which implies that $2 \mid z$. Thus, $4 \mid z^2$ which brings a contradiction. Therefore, the only interesting cases are the ones where x **or** y is even, and z is odd.

Without loss of generality, let x be even (the following statements would also hold if it was y that was even). Then, we know that $(\frac{x}{2})^2 = \frac{1}{4}(z^2 - y^2)$. We can rewrite the right-hand side as $(\frac{z-y}{2})(\frac{z+y}{2})$. Also, $\frac{z-y}{2}$ and $\frac{z+y}{2}$ are relatively prime. Thus, $\frac{z-y}{2} = a^2$ and $\frac{z+y}{2} = b^2$ which implies that $(\frac{x}{2})^2 = a^2b^2$. Thus, $x^2 = 4a^2b^2$, and $x = 2ab$. From that, we get that $y = \frac{z+y}{2} - \frac{z-y}{2} = b^2 - a^2$, and $z = \frac{z+y}{2} + \frac{z-y}{2} = b^2 + a^2$.

Briefly, we have shown that if we have $(x, y, z) = 1$ and $x^2 + y^2 = z^2$, then there exists a, b such that, for $a < b$,

$$x = 2ab,$$
$$y = b^2 - a^2,$$
$$z = b^2 + a^2.$$

Theorem. *There exists no solutions made only of integers for the equation*

$$x^4 + y^4 = z^2.$$

Proof. First, let's suppose that x, y, z are relatively prime, and even that x and y, x and z, and y and z have no common factors (this shall be proved later in this paper). Now, let $p \mid (x, y, z)$. Thus, we can say that $p \mid x$ which implies that $p^4 \mid x^4$. It is possible to state this for y as well. Also, since we know that $p^4 \mid x^4 + y^4$, then p^4 must divide z^2 because $x^4 + y^4 = z^2$. Therefore, $p^2 \mid z$.

So, we have that the following equation must be a solution:

$$(\frac{x}{p})^4 + (\frac{y}{p})^4 = (\frac{z}{p^2})^2.$$

Now, let's go back to our original equation that we can rewrite as

$$(x^2)^2 + (y^2)^2 = z^2,$$

which brings us back to Pythagorean triplets. Suppose x^2 is even. Then, $x = 2\bar{x}$. So,

$$(4\bar{x}^2)^2 + (y^2)^2 = z^2.$$

Thus, there must exist a, b such that $(a, b) = 1$, and that $4\bar{x}^2 = 2ab$. It is possible to say that $2\bar{x} = ab$ which implies that ab is even. Also, since a, b are relatively prime, only one of them can be even. Anyhow, since $(x^2) + (y^2)^2 = z^2$, a square, y^2 must equal $b^2 - a^2$ or, in other words, $a^2 + y^2 = b^2$ and $z = b^2 + a^2$. This shows that it is impossible to get b even and a odd. So, $a = 2\bar{a}$, b is odd, and we have that

$$2\bar{x}^2 = 2\bar{a}b,$$
$$\bar{x}^2 = \bar{a}b.$$

Thus, we have that $\bar{a} = s^2$ and $b = t^2$ with $(s, t) = 1$. If we plug these into the previous equation $a^2 + y^2 = b^2$, we get that

$$(2\bar{a})^2 + y^2 = b^2,$$
$$(2s^2)^2 + y^2 = (t^2)^2.$$

If we apply the same old trick again, we see that, for $(u, v) = 1$, $2s^2 = 2uv$, and that $y = u^2 - v^2$, implying that $t^2 = u^2 + v^2$. Therefore, $s^2 = uv$, where

$u = \alpha^2$, and $v = \beta^2$. So, $t^2 = (\alpha^2)^2 + (\beta^2)^2$ or, in other words, $t^2 = \alpha^4 + \beta^4$.

Thus, $x^4 + y^4 = z^2$ implies that $\alpha^4 + \beta^4 = t^2$ for $t < z$, and $(\alpha, \beta, t) = 1$. From there on, we could restart from the beginning and do it all over again which means that we would have $x_1^4 + y_1^4 = z_1^2$, $x_2^4 + y_2^4 = z_2^2$, $x_3^4 + y_3^4 = z_3^2$, ..., $x_n^4 + y_n^4 = z_n^2$, ... with $|z_1| > |z_2| > |z_3| > ... > |z_n| > ... > 0$ which is impossible. [2]

□

Now, let's look at the case when $n = 3$. [3]

Lemma 2. We know from previous results that $(x, y, z) = 1$. This implies that exactly one of them is an even number. Let's analyze two cases: the one where x or y is even and the one when z is even.

Case 1: x is even

We know then that $z - y$ and $z + y$ is even. Thus, we can write that

$$z - y = 2p,$$
$$z + y = 2q.$$

Also, the following statements should always be true:

$$z = \frac{1}{2}[(z - y) + (z + y)], \text{ and}$$
$$y = \frac{1}{2}[(z + y) - (z - y)].$$

Therefore, we have that $z = p + q$ and $y = q - p$. Since z and y are both odd, then p is even and q is odd or vice-versa. Also, $(p, q) = 1$. Finally, since $x^3 = z^3 - y^3$, we can observe that:

$$\begin{aligned} x^3 &= (z - y)(z^2 + yz + y^2), \\ &= [(p + q) - (q - p)][(p + q)^2 + (p + q)(q - p) + (q - p)^2], \\ &= 2p(p^2 + 2pq + q^2 + q^2 - p^2 + q^2 - 2pq + p^2), \\ &= 2p(p^2 + 3q^2). \end{aligned}$$

Therefore, $2p(p^2 + 3q^2)$ is a cube when x (or y) is even.

Case 2: z is even

We know that x and y must be odd. This means that $x+y$ and $x-y$ are even, so we can write that

$$x+y=2p,$$
$$x-y=2q.$$

Once again, the following statements should always be true as well:

$$x=\frac{1}{2}[(x+y)+(x-y)], \text{ and}$$
$$y=\frac{1}{2}[(x+y)-(x-y)].$$

So, we see that $x=p+q$ and $y=p-q$. Also, we can show that $(p,q)=1$. Moreover, since x and y are both odd, then p is even and q is odd or vice-versa. Finally, here again, we could show that $2p(p^2+3q^2)$ equals z^3, thus is a cube.

Now, we know that whatever the x,y,z are, we'll have that $2p(p^2+3q^2)$ is a cube. We'll now show how $(2p,p^2+3q^2)=1$ or 3. Indeed, let's suppose there is a prime that divides both $2p$ and p^2+3q^2. We know it cannot be 2 because p and q have opposite parity and so do $2p$ and p^2+3q^2.

Now, let's assume that there exists a prime greater than 3 that divide those two expressions. Then,

$$2p=\lambda P \text{ and } p^2+3q^2=\lambda Q.$$

We see that 2 must divide P. So we know that there must exist $R=\frac{P}{2}$ where R is an integer. This allows us to rewrite $2p=\lambda P$ as $p=\lambda R$. So,

$$\begin{aligned}3q^2&=\lambda Q-p^2,\\&=\lambda Q-\lambda^2R^2,\\&=\lambda(Q-\lambda R^2).\end{aligned}$$

By our initial conditions on λ, we know that λ doesn't divide 3. Therefore, λ must divide q^2 since $\frac{3q^2}{\lambda}$ is an integer. This means that λ divides q and we'll already know that it divides p. Thus, this means that if λ is greater than 3, $(x,y)\neq 1$ and we have a contradiction. So, $(2p,p^2+3q^s)=1$ or 3.

Theorem. *There exists no whole solutions to the equation*

$$x^3 + y^3 = z^3.$$

Proof. We know from previous results that $(x, y, z) = 1$. This implies that exactly one of them is an even number. We also know from the lemma that $2p(p^2 + 3q^2)$ is a cube and that $(2p, p^2 + 3q^2) = 1$ or 3.

If $(2p, p^2+3q^2) = 1$, then $2p$ and p^2+3q^2 are both cubes. Let $u^3 = p^2+3q^2$, then u is odd since p and q have opposite parities. Therefore, u is of the form $a^2 + 3b^2$ with $(a, b) = 1$. It is also possible to rewrite that expression as:

$$\begin{aligned}(a^2 + 3b^2)^3 &= (a^2 + 3b^2)[(a^2 - 3b^2)^2 + 12a^2b^2], \\ &= (a^3 - 6ab^2)^2 + 3(2a^2b + a^2b - 3b^3)^2, \\ &= (a^3 - 9ab^2)^2 + 27(a^2b - b^3)^2.\end{aligned}$$

Therefore, $p^2 + 3q^2 = (a^3 - 9ab^2)^2 + 3(a^2b - b^3)^2$ which implies that we can set $p = a^3 - 9ab^2$ and $q = a^2b - b^3$ with $(a, b) = 1$. So, we have that $2p = 2a^3 - 18ab^2 = 2a(a-3b)(a+3b)$. It is rather easy to see that $2a$, $a-3b$ and $a + 3b$ are all relatively prime. So, since $2p$ is a cube, they must all be cubes as well:

$$\begin{aligned}2a &= A^3, \\ a - 3b &= B^3, \\ a + 3b &= C^3.\end{aligned}$$

However, this gives us a new solution for Fermat's last theorem for the case when $n = 3$: $A^3 = B^3 + C^3$ since $2a = (a - 3b) + (a + 3b)$. This solution must be smaller than x, y, z. Indeed, we have that $A^3B^3C^3 = 2p$ and x^3or $z^3 = 2p(p^2 + 3pq)$ which implies that this solution is smaller.

We could build a similar argument to show that the same thing happens when $(2p, p^2 + 3q^2) = 3$.

Therefore, like in the case for $n = 4$, we can always find smaller solutions, but those solutions must necessarily always be bigger than zero, which is impossible. So, there are no integer solutions to $x^3 + y^3 = z^3$.

□

Remark. A far-stretched corollary of those two proves, but a possible one nonetheless, is that Fermat's last theorem is proved for all n composite numbers. Therefore, only prime numbers remain. Around 1850, the mathematician Ernst Eduard Kummer actually proved the theorem for all regular primes. He was hoping that this would be sufficient to prove the theorem since, at that time, it wasn't known that there was an infinite number of irregular primes (that was only proven in 1915 by Jensen). Let's briefly look at his theorem which nicely conjugates number theory and analysis. [4]

Lemma 3. First, we must define what a Bernoulli number is. It is usually generated by the following function:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n x^n}{n!}.$$

It is interesting to notice that $B_n = 0$ for all odd $n > 1$.

Also, a Dirichlet series is defined as

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where a_n is an integer function. Let's point out that the series can converge absolutely under certain conditions. A particular and well-known Dirichlet series is the case when $a_n = 1$. It gives us the Riemann Zeta Function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Euler was able to relate Dirichlet series and Bernoulli numbers in the following way:

$$\zeta(2n) = \frac{2n\pi^2 |B_{2n}|}{(2n)!},$$

for any integer n.

A prime p is called a regular prime if p does not divide the numerator of B_2, B_3, ..., B_{p-3}. Also, a prime that is not regular is said to be irregular.

Let's look at $p = 17$ for example. We must consider the following bernoulli numbers B_2 to B_14: $\frac{1}{6}, \frac{-1}{30}, \frac{1}{42}, \frac{-1}{30}, \frac{5}{66}, \frac{-691}{2730}, \frac{7}{6}$. Obviously, 17 doesn't divide

any of the numerators. Thus, p is regular.

On the other hand, for $q = 37$, if we consider $B-2$ to B_34, we can see that q is an irregular prime since it divides the numberator of $B_32 = \frac{-7709321041217}{510}$.

There are only three irregular primes below 100: $37, 59$, and 67. That is why Kummer thought is proof was interesting: he thought that there would be a limited finite number of cases left to prove.

Theorem. *There exists no solutions for $u^\lambda + v^\lambda + w^\lambda = 0$ if λ is a regular prime and u, v, w are complex numbers of the form*

$$a + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-2}\alpha^{\lambda-2},$$

where a_n are integers and such that u, v, w are relatively prime pairwise.

Remark. We shall not offer a complete proof of Kummer's theorem, however we invite the reader to read it on its own in Kummer's collected papers. Still, here are a few words on his proof.

First of all, this theorem allows complex numbers which is alright since it leads to an even stronger result. However, to achieve such a thing, Kummer spends over a 100 pages introducing complex numbers before stating his theorem. He shows that the number H of classes of ideal complex numbers cannot be divided by a regular prime, and thus, by λ. Moreover, if $f(\alpha)$ is ideal, then $f(\alpha)^\lambda$ doesn't exist unless λ and H have common factors, which is impossible. Therefore, $f(\alpha)$ cannot be ideal.

Relating all of those facts, he proves his theorem by considering two cases:

1. None of u, v, w can be divided by $1 - \alpha$, and
2. One of u, v, w can be divided by $1 - \alpha$.

He show that the two cases are impossible (in a fashion similar to what we've done for n=3,4, but more difficult of certain restrictions), thus proving his theorem.

Now, let's jump into the burning part of the subject: let's try to "prove" Fermat's last theorem!

Let n be the number of cold months. I am cold. The cold months form the winter.

Just kidding (even though it probably makes more sense than what is about to follow). However, once again, let's create a useful lemma first.

Lemma 4. It is rather obvious that, in order to get nontrivial solutions to the equation $x^n + y^n = z^n$, x, y, z can have no common factors or, in other words, $(x, y, z) = 1$. However, nothing tells us that $(x, y) = 1$ for example. Let's try to prove that x, y, z are relatively prime pairwise. So, first, let's assume that they are not and that only $(x, y, z) = 1$ holds. Thus, it could be possible to have:

$$x^n = ab\bar{x}^n,$$
$$y^n = bc\bar{y}^n,$$
$$z^n = ac\bar{z}^n,$$

with a, b, c different and relatively prime two by two. Then, we would have that

$$ab\bar{x}^n + bc\bar{y}^n = ac\bar{z}^n.$$

This is clearly impossible because, if you divide the equation by b for example, strange things happen:

$$a\bar{x}^n + c\bar{y}^n = \frac{ac}{b}\bar{z}^n.$$

We have that an integer plus an integer gives a fraction... except if $b = 1$. We can do the same trick for a and c. So, $a, b, c = 1$ and, thus, x, y, z are relatively prime pairwise.

Theorem. *For $x, y, z \in \mathbb{N}^*$ and $n > 2$, there exists no solution to the equation $x^n + y^n = z^n$.*

Proof. Basically, if we can show that $x^n + y^n$ cannot equal $(x + \alpha)^n$ where α is an integer between 1 and $y - 1$, we win. Of course, $x + \alpha$ is supposed to equal z.

We can rewrite $x^n + y^n = (x + a)^n = z^n$ as

$$y^n = \sum_{k=0}^{n-1} \binom{n}{k} x^k \alpha^{n-k}.$$

It would be rather interesting to transform the right side to get $(x+\alpha)^{n-1}$. Let's try it:

$$\begin{aligned}\frac{y^n R}{\alpha} &= \frac{\sum_{k=0}^{n-1}\binom{n}{k}x^k\alpha^{n-k}(\frac{(n-k)}{n})}{\alpha}\\ &= (x+\alpha)^{n-1}.\end{aligned}$$

It is not possible to know what is R. All we can say about it for now is that it is at least a rational number and might even be an integer. Now, let's see what happens if we transform the right side to be $(x+\alpha)^{n-2}$ for $n>2$. We get:

$$\begin{aligned}\frac{y^n S}{\alpha^2} &= \frac{\sum_{k=0}^{n-1}\binom{n}{k}x^k\alpha^{n-k}(\frac{(n-k)(n-1-k)}{n(n-1)})}{\alpha^2}\\ &= (x+\alpha)^{n-2}.\end{aligned}$$

Once again, it is impossible to say much about S. Still, we can equate our two y^n to get that

$$\frac{\alpha(x+\alpha)^{n-1}}{R} = \frac{\alpha^2(x+\alpha)^{n-2}}{S}.$$

From this statement and from others of the same nature (and also from knowing that x, y, α, n are integers), we can easily get a rather impressive list of possible divisions which might or might not be useful:

$R-S \mid xS$	$R-S \mid xR$	$(R-S)^2 \mid RSx^2$	$S \mid \alpha R$
$R \mid (x+\alpha)S$	$S \mid \alpha(R-S)$	$R \mid (x+\alpha)(R-S)$	$S(R-S) \mid \alpha R^2$
$\alpha^2 \mid y^n S$	$(x+\alpha)^{n-2} \mid y^n S$	$\alpha \mid y^n R$	$R-S \nmid S$
$R-S \nmid R$	$R-S \nmid x$	$S \nmid \alpha$	$R \nmid x+\alpha$
$x \nmid x+\alpha$	$R \nmid x+\alpha$	$R \nmid S$	$x \nmid \alpha$
$xs \nmid R-S$	$\alpha^2(x+\alpha)^{n-2} \nmid y^n$	$\alpha R \nmid x+\alpha$	

Let's keep those in mind, but for now, let's continue.

The question, of course, is how to continue from that point on. I've spent more than thirty sheets of paper on that topic. Loads of fun were had, and many interesting facts were found, but none that lead to something resembling a proof. Actually, many proofs were found, all of which were very wrong after inspection and introspection. Here is the latest one which has not been inspected yet, and thus must wrong. Still, here it is.

It is easy to show that $z = \frac{Rx}{R-S}$. We also know that $(x,z) = 1$; indeed,

x and z have no common factors by lemma 2. Thus, x has nothing to do with z. Nothing. If they saw each other on the street, they would ignore each other. So, when we say that $z = \frac{R}{R-S}x$, then it means that $\frac{R}{R-S}$ must somehow make x disappear because z won't tolerate its presence. However, R doesn't have any effect either on x. Why? Well, $R = \frac{\alpha z^{n-1}}{y^n}$, and $(y, x) = 1$, so R leaves x untouched, whole, intact, pure.

So, it must be $R-S$ that annihilates x, there's no other possibilities. Therefore, we must have that $x \mid (R-S)$. We also know that $\frac{R-S}{x} = \frac{R}{z}$, so z must also divide R. However, $\frac{R}{z} = \frac{\alpha z^{n-2}}{y^n}$ = integer, and $(y, z) = 1$, so y^n must divide α. This is impossible because α is smaller than y. So, $x \nmid R - S$, and $(x, z) \neq 1$.

So, this shows that there is something rotten in Denmark. It also "proves" Fermat's last theorem. (Of course, this is completely wrong; x doesn't need to divide $R - S$.)

□

Remark. You may have noticed that I only "proved" Fermat's last theorem for x, y, z positive integers. It would probably be fairly easy to change the initial conditions used here to get it for x, y, z any integer but 0. However, laziness requires us to only look at what happens when we have a situation with negative integers.

If n is even, then nothing changes at all because everything becomes positive anyway. If n is odd, then many situations can arise. If x, y, z are all negatives, then we come back to the original equation since

$$-|x|^n - |y|^n = -|z|^n,$$
$$|x|^n + |y|^n = |z|^n.$$

If x or y is negative and z is positive, then

$$x^n - |y|^n = z^n,$$
$$x^n = z^n + |y|^n,$$

and once again, we're back to a situation equivalent to the initial one.

If x or y is negative and z is negative, then

$$x^n - |y|^n = -|z|^n,$$

$$x^n + |z|^n = |y|^n,$$

which comes back to the same idea.

Finally, we can also have that either x and y are negative **or** z or negative. Then, it is simply impossible because one side of the equation will be negative and the other, positive.

Therefore, x, y, z can be positive or negative integers.

Conclusion. As I worked through this proof, I hit many knots. Every time I "thought" I was done, there was always a little crack left which contained the initial problem again. That is certainly one of the most interesting aspects of this theorem: whatever you do to it, it will always jump right back at you, whole, where you least expect it. It is like a fractal. It's truly beautiful. No wonder it has resisted to the wisdom of so many great mathematicians.

References

[1] Eric W. Weisstein. "Fermat's Last Theorem" From MathWorld - A Wolfram Web Resource. http://mathworld.wolfram.com/FermatsLastTheorem.html

[2] Mathieu Dufour: *Dans le coin des carres*, conference given in June 2004.

[3] H.M. Edwards. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1996.

[4] Ernst Eduard Kummer: *Collected Papers - Memoire sur la theorie des nombres complexes composes de racines de l'unite et de nombre entiers*, Springer-Verlag, 1975.