# Fermat's Proof on the Margin

Rahul Saha

Splash

# Fermat's Last Theorem

**Theorem.** There exist no positive integers $x, y, z$ that satisfy the equation

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

for $n$ larger than $2$.

*"I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."* - **Pierre de Fermat**

What was Fermat's "proof"?

Find all positive integers $x, y, z$ that satisfy the following equation.

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

## Make some simplifying assumptions.

**Make some simplifying assumptions.**

If **any** two of these numbers are even, then the third one has to be even.

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

## Make some simplifying assumptions.

If **any** two of these numbers are even, then the third one has to be even.

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

This means that if $(x, y, z)$ is a solution, then so is $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ because

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

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

**Make some simplifying assumptions.**

If **any** two of these numbers are even, then the third one has to be even.

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

This means that if $(x, y, z)$ is a solution, then so is $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ because

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

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

To make our life easier, assume that at most one of $x, y, z$ can be even.

**Make some simplifying assumptions.**

If **any** two of these numbers are even, then the third one has to be even.

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

This means that if $(x, y, z)$ is a solution, then so is $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ because

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

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

To make our life easier, assume that at most one of $x, y, z$ can be even.

Similarly this means that no two of $x, y, z$ can have common factors.

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

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

Note that all three cannot be odd.

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

Note that all three cannot be odd.

So exactly one of $x, y, z$ is even.

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

Note that all three cannot be odd.

So exactly one of $x, y, z$ is even.

Similarly, prove that $z$ cannot be even!

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

Note that all three cannot be odd.

So exactly one of $x, y, z$ is even.

Similarly, prove that $z$ cannot be even!

So make another **simplifying** assumption.

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

Note that all three cannot be odd.

So exactly one of $x, y, z$ is even.

Similarly, prove that $z$ cannot be even!

So make another **simplifying** assumption. Assume $x$ is odd, and $y$ is even.

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

Note that all three cannot be odd.

So exactly one of $x, y, z$ is even.

Similarly, prove that $z$ cannot be even!

So make another **simplifying** assumption. Assume $x$ is odd, and $y$ is even.

# Now Factor!

## Now Factor!

$$x^2 = z^2 - y^2$$

Now Factor!

$$x^2 = z^2 - y^2$$

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

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z + y$ and $z - y$ are both multiples of some prime number $p$.

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z+y$ and $z-y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z+y$ and $z-y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

So we have $2y$ and $2z$ are multiples of this prime $p$.

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z+y$ and $z-y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

So we have $2y$ and $2z$ are multiples of this prime $p$.

But $y$ and $z$ have no common factors!

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z+y$ and $z-y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

So we have $2y$ and $2z$ are multiples of this prime $p$.

But $y$ and $z$ have no common factors!

This means that $2$ is the only possible common factor!

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z + y$ and $z - y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

So we have $2y$ and $2z$ are multiples of this prime $p$.

But $y$ and $z$ have no common factors!

This means that $2$ is the only possible common factor! But $z + y$ and $z - y$ are both odd!

Now Factor!

$$x^2 = z^2 - y^2$$

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

Suppose $z+y$ and $z-y$ are both multiples of some prime number $p$. Then it must divide their sum and difference!

So we have $2y$ and $2z$ are multiples of this prime $p$.

But $y$ and $z$ have no common factors!

This means that $2$ is the only possible common factor! But $z+y$ and $z-y$ are both odd!

So their greatest common divisor must be $1$.

$$z + y = a^2$$
$$z - y = b^2$$

$$z + y = a^2$$
$$z - y = b^2$$

Adding and subtracting, this gives us

$$z = \frac{a^2 + b^2}{2}$$

$$y = \frac{a^2 - b^2}{2}$$

$$z + y = a^2$$
$$z - y = b^2$$

Adding and subtracting, this gives us

$$z = \frac{a^2 + b^2}{2}$$

$$y = \frac{a^2 - b^2}{2}$$

This means

$$x^2 = z^2 - y^2 = a^2 b^2$$
$$x = ab$$

up to sign.

This means all solutions are of the form

$$(x, y, z) = \left(ab, \frac{a^2 - b^2}{2}, \frac{a^2 + b^2}{2}\right)$$

Next up - An absurdist proof!

The key idea in the previous proof was factoring $z^2 - y^2$

The key idea in the previous proof was factoring $z^2 - y^2$

This time, let us factor the equation differenly!

The key idea in the previous proof was factoring $z^2 - y^2$

This time, let us factor the equation differenly!

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

The key idea in the previous proof was factoring $z^2 - y^2$

This time, let us factor the equation differenly!

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

$$(y + ix)(y - ix) = z^2$$

Assume $y + ix$ and $y - ix$ are both multiples of some prime $p$.

Assume $y + ix$ and $y - ix$ are both multiples of some prime $p$.

$2y$ and $2ix$ have to be multiples of the prime $p$!

Assume $y + ix$ and $y - ix$ are both multiples of some prime $p$.

$2y$ and $2ix$ have to be multiples of the prime $p$!

But $x$ and $y$ have no common factors!

Assume $y + ix$ and $y - ix$ are both multiples of some prime $p$.

$2y$ and $2ix$ have to be multiples of the prime $p$!

But $x$ and $y$ have no common factors!

So their only common factor must be $2$!

Assume $y + ix$ and $y - ix$ are both multiples of some prime $p$.

$2y$ and $2ix$ have to be multiples of the prime $p$!

But $x$ and $y$ have no common factors!

So their only common factor must be $2$!

But $y + ix$ and $y - ix$ are not multiples of $2$!

This means

$$y + ix = A^2$$

$$y - ix = B^2$$

This means

$$y + ix = A^2$$
$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

This means

$$y + ix = A^2$$

$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

$$y + ix = (m + ni)^2 = (m^2 - n^2) + 2mni$$

This means

$$y + ix = A^2$$
$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

$$y + ix = (m + ni)^2 = (m^2 - n^2) + 2mni$$

Comparing the real and imaginary parts,

This means

$$y + ix = A^2$$

$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

$$y + ix = (m + ni)^2 = (m^2 - n^2) + 2mni$$

Comparing the real and imaginary parts, we get

$$x = 2mn$$

This means

$$y + ix = A^2$$

$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

$$y + ix = (m + ni)^2 = (m^2 - n^2) + 2mni$$

Comparing the real and imaginary parts, we get

$$x = 2mn$$

$$y = m^2 - n^2$$

This means

$$y + ix = A^2$$

$$y - ix = B^2$$

Let $A = m + ni$ for some integers $m$ and $n$

$$y + ix = (m + ni)^2 = (m^2 - n^2) + 2mni$$

Comparing the real and imaginary parts, we get

$$x = 2mn$$

$$y = m^2 - n^2$$

$$z = m^2 + n^2$$

**Problem.** (Fermat's last theorem for $n = 3$) Show that there exists no positive integers $x, y, z$ that satisfy the equation

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

**Make a simplifying assumption** that $x, y, z$ have no common factors.

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$.

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

$$x^3 - 1 = (x - \omega)(x - \omega^2)(x - 1)$$

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

$$x^3 - 1 = (x - \omega)(x - \omega^2)(x - 1)$$

$$x^3 + 1 = (x + \omega)(x + \omega^2)(x + 1)$$

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

$$x^3 - 1 = (x - \omega)(x - \omega^2)(x - 1)$$

$$x^3 + 1 = (x + \omega)(x + \omega^2)(x + 1)$$

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

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

$$x^3 - 1 = (x - \omega)(x - \omega^2)(x - 1)$$

$$x^3 + 1 = (x + \omega)(x + \omega^2)(x + 1)$$

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

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

**Make a simplifying assumption** that $x, y, z$ have no common factors.

Also assume that $y$ and $z$ are not multiples of $3$.

Let $\omega$ be a complex number so that $\omega^3 = 1$. Then the other solutions are given by $1, \omega, \omega^2$.

$$x^3 - 1 = (x - \omega)(x - \omega^2)(x - 1)$$

$$x^3 + 1 = (x + \omega)(x + \omega^2)(x + 1)$$

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

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$.

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

But because $x$ and $y$ are coprime, so the only common divisor must divide $\omega - 1$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

But because $x$ and $y$ are coprime, so the only common divisor must divide $\omega - 1$

$$(\omega - 1)^2 + 3(\omega - 1) = -3$$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

But because $x$ and $y$ are coprime, so the only common divisor must divide $\omega - 1$

$$(\omega - 1)^2 + 3(\omega - 1) = -3$$

$$(\omega - 1)(\omega + 2) = -3$$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

But because $x$ and $y$ are coprime, so the only common divisor must divide $\omega - 1$

$$(\omega - 1)^2 + 3(\omega - 1) = -3$$

$$(\omega - 1)(\omega + 2) = -3$$

But remember! $z$ is comprime with $3$. This is an impossibility!

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Suppose $x + y\omega$ and $x + y$ are multiples of some prime $p$. Then we have $p$ has to divide $(\omega - 1)x$ and $(\omega - 1)y$.

But because $x$ and $y$ are coprime, so the only common divisor must divide $\omega - 1$

$$(\omega - 1)^2 + 3(\omega - 1) = -3$$

$$(\omega - 1)(\omega + 2) = -3$$

But remember! $z$ is comprime with $3$. This is an impossibility!

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Similarly we can show that all the factors are coprime!

$$(x + y\omega)(x + y\omega^2)(x + y) = z^3$$

Similarly we can show that all the factors are coprime!

So

$$x + y\omega = a^3$$

$$x + y\omega^2 = b^3$$

$$x + y = c^3$$

$$x + y\omega = a^3$$
$$x + y\omega^2 = b^3$$

$$x + y\omega = a^3$$
$$x + y\omega^2 = b^3$$

So let $a = m + n\omega$, then $b = m + n\omega^2$

$$x + y\omega = a^3$$
$$x + y\omega^2 = b^3$$

So let $a = m + n\omega$, then $b = m + n\omega^2$

$$x + y\omega = (m + n\omega)^3 = m^3 + n^3 + 3mn\omega(m + n\omega)$$
$$\implies x + y\omega = (m^3 + n^3 - 3mn) + 3(m^2n - mn^2)\omega$$

$$x + y\omega = a^3$$
$$x + y\omega^2 = b^3$$

So let $a = m + n\omega$, then $b = m + n\omega^2$

$$x + y\omega = (m + n\omega)^3 = m^3 + n^3 + 3mn\omega(m + n\omega)$$
$$\implies x + y\omega = (m^3 + n^3 - 3mn) + 3(m^2n - mn^2)\omega$$

Similarly

$$x + y\omega^2 = (m^3 + n^3 - 3mn) + 3(m^2n - mn^2)\omega^2$$

Now subtracting the two equations we get

$$y(\omega - \omega^2) = (x + y\omega) - (x + y\omega^2) = 3(m^2 n - mn^2)(\omega - \omega^2)$$

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

But we assumed at the start that $3$ does not divide $y$, so we once again have an impossibility!! So Fermat's last theorem for $n = 3$ is proved!!!

**Homework:** Justify that the simplifying assumptions we made are indeed correct.

**Homework:** There is a small mistake in this proof that does not alter what the proof is. What is the mistake? Hint: factorizations are unique upto multiplication by units $(1, \omega, \omega^2)$

**Problem.** (Fermat's last theorem) Prove that for $p > 2$, there exists no positive integer solutions to $x^p + y^p = z^p$.

Make similar simplifying assumptions as before.

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$.

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$. Then $1, \omega, \ldots, \omega^{p-1}$ are the $p$-th roots of unities.

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$. Then $1, \omega, \ldots, \omega^{p-1}$ are the $p$-th roots of unities.

You can recognize that

$$x^p - 1 = (x - \omega)(x - \omega^2) \ldots (x - \omega^{p-1})$$

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$. Then $1, \omega, \ldots, \omega^{p-1}$ are the $p$-th roots of unities.

You can recognize that

$$x^p - 1 = (x - \omega)(x - \omega^2) \ldots (x - \omega^{p-1})$$

So as before, we have

$$x^p + y^p = (x + y)(x + \omega y) \ldots (x + \omega^{p-1} y) = z^p$$

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$. Then $1, \omega, \ldots, \omega^{p-1}$ are the $p$-th roots of unities.

You can recognize that

$$x^p - 1 = (x - \omega)(x - \omega^2) \ldots (x - \omega^{p-1})$$

So as before, we have

$$x^p + y^p = (x + y)(x + \omega y) \ldots (x + \omega^{p-1} y) = z^p$$

Show just like before that the factors have no common divisor.

Make similar simplifying assumptions as before. Assume that $p$ is prime.

Let $\omega$ be a solution of $x^p - 1$. Then $1, \omega, \ldots, \omega^{p-1}$ are the $p$-th roots of unities.

You can recognize that

$$x^p - 1 = (x - \omega)(x - \omega^2) \ldots (x - \omega^{p-1})$$

So as before, we have

$$x^p + y^p = (x + y)(x + \omega y) \ldots (x + \omega^{p-1} y) = z^p$$

Show just like before that the factors have no common divisor.

$$x^p + y^p = (x+y)(x+\omega y)\dots(x+\omega^{p-1}y) = z^p$$

Then if we let

$$x + y\omega = a^p$$

$$x + y\omega^{p-2} = \overline{a}^p$$

Subtracting

$$y(\omega - \omega^{p-2}) = a^p - \overline{a}^p$$

The right side is a multiple of $p$ (you can show this by expanding!) but $y$ is not a multiple of $p$ by our simplifying assumption. Impossible!!

So where did it go wrong!!

# Unique Factorization

$$ab = 2020^2$$

"If $a$ and $b$ share no common factors, then $a$ and $b$ are squares."

# Unique Factorization

$$ab = 2020^2$$

"If $a$ and $b$ share no common factors, then $a$ and $b$ are squares."

This only holds because of unique factorization!

# Unique Factorization

$$ab = 2020^2$$

"If $a$ and $b$ share no common factors, then $a$ and $b$ are squares."

This only holds because of unique factorization!

Does unique factorization hold, say, with complex numbers $a + bi$?

# Unique Factorization

$$ab = 2020^2$$

"If $a$ and $b$ share no common factors, then $a$ and $b$ are squares."

This only holds because of unique factorization!

Does unique factorization hold, say, with complex numbers $a + bi$?

What about $a + b\omega$, where $w^3 = 1$?

# Unique Factorization

$$ab = 2020^2$$

"If $a$ and $b$ share no common factors, then $a$ and $b$ are squares."

This only holds because of unique factorization!

Does unique factorization hold, say, with complex numbers $a + bi$?

What about $a + b\omega$, where $w^3 = 1$?

Yes!!

Sadly, it doesn't hold for $a + b\omega + \ldots$ where $\omega^p = 1$ in general :(

Sadly, it doesn't hold for $a + b\omega + \dots$ where $\omega^p = 1$ in general :(

In fact, it only holds for finitely many $p$.

Sadly, it doesn't hold for $a + b\omega + \dots$ where $\omega^p = 1$ in general :(

In fact, it only holds for finitely many $p$.

How can unique factorization fail?

How can unique factorization fail?

Consider numbers of the form $a + b\sqrt{-5}$.

How can unique factorization fail?

Consider numbers of the form $a + b\sqrt{-5}$.

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

How can unique factorization fail?

Consider numbers of the form $a + b\sqrt{-5}$.

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \times 3$$

How can unique factorization fail?

Consider numbers of the form $a + b\sqrt{-5}$.

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3$$

But the factors above are all irreducible!!

How can unique factorization fail?

Consider numbers of the form $a + b\sqrt{-5}$.

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3$$

But the factors above are all irreducible!!

So unique factorization fails!

# Things to Take Away

1. Make simplifying assumptions.

# Things to Take Away

1. Make simplifying assumptions.

2. Factor equations.

# Things to Take Away

1. Make simplifying assumptions.

2. Factor equations.

3. Make sure you understand the underlying reason behind your claims!

# Fermat's Last Theorem Proof

Sadly the slides are too narrow to contain Andrew Wile's proof of Fermat's Last Theorem :(

# Credits

Michael Gintz

Sabrina Reguyal

Trinh Le Quang

Ahsan Al Mahir Lazim