

\mathbb{Z} is difficult, polynomials are easy.

Stefan Maubach

Saginaw, October 2008

\mathbb{Z} has prime numbers: 2, 3, 5, 7, ... and unique prime factorisation. If I sit in a room and factor the number 1776, and you sit in a different room and factor this same number, we end up with the same prime factorisation: $37 \cdot 17 \cdot 3$.

\mathbb{Z} has prime numbers: 2, 3, 5, 7, ... and unique prime factorisation. If I sit in a room and factor the number 1776, and you sit in a different room and factor this same number, we end up with the same prime factorisation: $37 \cdot 17 \cdot 3$.

Actually: 2 and -2 are seen as “the same prime number”.

They differ exactly a unit:

$$-2 = (-1) \cdot 2.$$

Or, equivalently: $2\mathbb{Z}$ and $-2\mathbb{Z}$ are the same set.

\mathbb{Z} has prime numbers: 2, 3, 5, 7, ... and unique prime factorisation. If I sit in a room and factor the number 1776, and you sit in a different room and factor this same number, we end up with the same prime factorisation: $37 \cdot 17 \cdot 3$.

Actually: 2 and -2 are seen as “the same prime number”.

They differ exactly a unit:

$$-2 = (-1) \cdot 2.$$

Or, equivalently: $2\mathbb{Z}$ and $-2\mathbb{Z}$ are the same set.

So, we could say that a prime number N is an element which is not invertible, and if it is divisible by some element x , then either x is a unit, or $N = ux$ where u is a unit.

\mathbb{Z} has prime numbers: 2, 3, 5, 7, ... and unique prime factorisation. If I sit in a room and factor the number 1776, and you sit in a different room and factor this same number, we end up with the same prime factorisation: $37 \cdot 17 \cdot 3$.

Actually: 2 and -2 are seen as “the same prime number”.

They differ exactly a unit:

$$-2 = (-1) \cdot 2.$$

Or, equivalently: $2\mathbb{Z}$ and $-2\mathbb{Z}$ are the same set.

So, we could say that a prime number N is an element which is not invertible, and if it is divisible by some element x , then either x is a unit, or $N = ux$ where u is a unit.

Are there any other sets with something like “prime numbers”?

In \mathbb{Z} one can add, subtract, and multiply. You *cannot* divide by everything - that's the point, if you could divide by everything, then you don't have prime numbers!

In \mathbb{Z} one can add, subtract, and multiply. You *cannot* divide by everything - that's the point, if you could divide by everything, then you don't have prime numbers!

\mathbb{Z} is a *ring*. If you can also divide by everything (except zero) then you have a *field*.

In \mathbb{Z} one can add, subtract, and multiply. You *cannot* divide by everything - that's the point, if you could divide by everything, then you don't have prime numbers!

\mathbb{Z} is a *ring*. If you can also divide by everything (except zero) then you have a *field*.



Are there any other “things” having prime numbers?

Are there any other Rings having prime numbers?

Are there any other Rings having prime numbers?

$\mathbb{R}[X]$ is the collection of polynomials, i.e.

$$\mathbb{R}[X] := \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}.$$

Are there any other Rings having prime numbers?

$\mathbb{R}[X]$ is the collection of polynomials, i.e.

$$\mathbb{R}[X] := \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}.$$

Same way:

$$\mathbb{C}[X] := \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n \mid n \in \mathbb{N}, a_i \in \mathbb{C}\}.$$

\mathbb{Z} $\mathbb{R}[X]$

\mathbb{Z} $\mathbb{R}[X]$

Invertible elements:

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers		

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$.

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”! Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”!

Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

Furthermore: $X^2 + 1$ is also irreducible. . .

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”!

Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

Furthermore: $X^2 + 1$ is also irreducible... but...

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”!

Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

Furthermore: $X^2 + 1$ is also irreducible... but... over \mathbb{C} all prime polynomials are of degree 1 ! $X^2 + 1 = (X + i)(X - i)$.

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”! Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

Furthermore: $X^2 + 1$ is also irreducible... but... over \mathbb{C} all prime polynomials are of degree 1! $X^2 + 1 = (X + i)(X - i)$. Which means: if $p(X)$ of degree 37, then p is a product of exactly 37 “prime” polynomials.

	\mathbb{Z}	$\mathbb{R}[X]$
Invertible elements:	$1, -1$	$\mathbb{R} \setminus \{0\}$
Prime numbers	$2, 3, 5, \dots$	polynomials $X + 37, X^2 + 1$

Just check it out: any polynomial $p(X)$ decomposes into a product of polynomials: $p(X) = p_1(X) \cdots p_n(X)$. If you cannot decompose further, then you have irreducible polynomials. Those you can call “prime”.

Notice: $X + 1$ and $-37X - 37$ are “the same prime number”! Just as 2 and -2 they only differ a unit: the latter -1 which is a unit in \mathbb{Z} , the former -37 , which is a unit in $\mathbb{R}[X]$.

Furthermore: $X^2 + 1$ is also irreducible... but... over \mathbb{C} all prime polynomials are of degree 1! $X^2 + 1 = (X + i)(X - i)$.

Which means: if $p(X)$ of degree 37, then p is a product of exactly 37 “prime” polynomials. Let’s agree on $1 \cdot X + \alpha$ being the ‘standard primes’ in $\mathbb{C}[X]$.

$$\gcd(12, 8) = \gcd(2^2 \cdot 3, 2^3) = 2^2 = 4.$$

$$\gcd(12, 8) = \gcd(2^2 \cdot 3, 2^3) = 2^2 = 4.$$

$$\gcd(X^3 + X^2 - X - 1, X^3 + 3X^2 + 3X + 1) =$$

$$\gcd((X + 1)^2(X - 1), (X + 1)^3) = (X + 1)^2.$$

$$\gcd(12, 8) = \gcd(2^2 \cdot 3, 2^3) = 2^2 = 4.$$

$$\gcd(X^3 + X^2 - X - 1, X^3 + 3X^2 + 3X + 1) =$$

$$\gcd((X + 1)^2(X - 1), (X + 1)^3) = (X + 1)^2.$$

In $\mathbb{C}[X]$ one may describe “ $\gcd(f, g) = 1$ ” by saying: “ f and g have different zeroes”.

Fermat's Last Theorem:

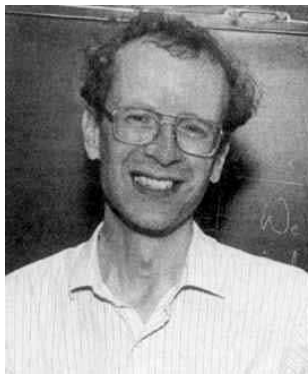
Fermat's Last Theorem:

$a, b, c \in \mathbb{Z}$ such that

$\gcd(a, b, c) = 1$ and $n \geq 3$

Then $a^n + b^n = c^n$ is not possible.

Fermat's Last Theorem:

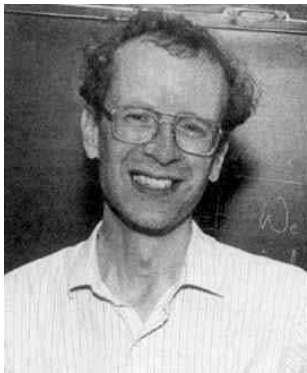


$a, b, c \in \mathbb{Z}$ such that

$$\gcd(a, b, c) = 1 \text{ and } n \geq 3$$

Then $a^n + b^n = c^n$ is not possible.

Fermat's Last Theorem:



$a, b, c \in \mathbb{Z}$ such that

$\gcd(a, b, c) = 1$ and $n \geq 3$

Then $a^n + b^n = c^n$ is not possible.

Proof of Wiles is very difficult! My guess is: no one present in this room has read and understood the proof...!

Fermat's Last Theorem for $\mathbb{C}[X]$

$a, b, c \in \mathbb{Z}$ such that

$\gcd(a, b, c) = 1$ and $n \geq 3$

Then $a^n + b^n = c^n$ is not possible.

Fermat's Last Theorem for $\mathbb{C}[X]$

$a, b, c \in \mathbb{Z}$ such that

$\gcd(a, b, c) = 1$ and $n \geq 3$

Then $a^n + b^n = c^n$ is not possible.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$f^n + g^n = h^n$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$\begin{array}{rcl} f^n & + g^n & = h^n \\ f'f^{n-1} & + g'g^{n-1} & = h'h^{n-1} \end{array}$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$\begin{array}{rcll} f^n & + g^n & = h^n & \text{times } f' \\ f'f^{n-1} & + g'g^{n-1} & = h'h^{n-1} & \text{times } f \end{array}$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$\begin{array}{rcll} f^n f' & + g^n f' & = h^n f' & \text{times } f' \\ f' f^{n-1} f & + g' g^{n-1} f & = h' h^{n-1} f & \text{times } f \end{array}$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$\begin{array}{rcll} f^n f' & + g^n f' & = h^n f' & \text{times } f' \\ - f' f^{n-1} f & + g' g^{n-1} f & = h' h^{n-1} f & \text{times } f \end{array}$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$f^n f' + g^n f' = h^n f' \quad \text{times } f'$$

$$- f' f^{n-1} f + g' g^{n-1} f = h' h^{n-1} f \quad \text{times } f$$

$$f' g^n - f g' g^{n-1} = f' h^n - f h' h^{n-1}$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof:

$$f^n f' + g^n f' = h^n f' \quad \text{times } f'$$

$$- f' f^{n-1} f + g' g^{n-1} f = h' h^{n-1} f \quad \text{times } f$$

$$f' g^n - f g' g^{n-1} = f' h^n - f h' h^{n-1}$$

so $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$.

So we can assume that $f'g - fg', f'h - fh'$, and $g'h - gh'$ are unequal to 0.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$. Hence $f'g = fg'$.

So we can assume that $f'g - fg', f'h - fh'$, and $g'h - gh'$ are unequal to 0.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$. Hence $f'g = fg'$. Since $\gcd(g, f) = 1$
 g divides g' , and f divides f'

So we can assume that $f'g - fg', f'h - f'h$, and
 $g'h - gh'$ are unequal to 0.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$. Hence $f'g = fg'$. Since $\gcd(g, f) = 1$ g divides g' , and f divides f' - That is only possible if f, g are constant

So we can assume that $f'g - fg', f'h - fh'$, and $g'h - gh'$ are unequal to 0.

Let $f, g, h \in \mathbb{C}[X]$ be such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Suppose $f'g - fg' = 0$. Hence $f'g = fg'$. Since $\gcd(g, f) = 1$ g divides g' , and f divides f' - That is only possible if f, g are constant and then h is automatically constant! So this case is done. So we can assume that $f'g - fg', f'h - fh'$, and $g'h - gh'$ are unequal to 0.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

and all of $f'g - fg'$, $f'h - fh'$, and $g'h - gh'$ are nonequal to zero.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

So g^{n-1} divides $f'h - fh'$,

and all of $f'g - fg'$, $f'h - fh'$, and $g'h - gh'$ are nonequal to zero.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

So g^{n-1} divides $f'h - fh'$,

and h^{n-1} divides $f'g - fg'$,

and f^{n-1} divides $g'h - gh'$,

and all of $f'g - fg'$, $f'h - fh'$, and $g'h - gh'$ are nonequal to zero.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

So g^{n-1} divides $f'h - fh'$, $\deg(g^{n-1}) \leq \deg(f'h - fh')$

and h^{n-1} divides $f'g - fg'$, $\deg(h^{n-1}) \leq \deg(f'g - fg')$

and f^{n-1} divides $g'h - gh'$, $\deg(f^{n-1}) \leq \deg(g'h - gh')$

and all of $f'g - fg'$, $f'h - fh'$, and $g'h - gh'$ are nonequal to zero.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

So g^{n-1} divides $f'h - fh'$, $\deg(g^{n-1}) \leq \deg(f) + \deg(h) - 1$

and h^{n-1} divides $f'g - fg'$, $\deg(h^{n-1}) \leq \deg(f) + \deg(g) - 1$

and f^{n-1} divides $g'h - gh'$, $\deg(f^{n-1}) \leq \deg(g) + \deg(h) - 1$

and all of $f'g - fg'$, $f'h - fh'$, and $g'h - gh'$ are nonequal to zero.

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$\deg(g^{n-1}) \leq \deg(f) + \deg(h) - 1$$

$$\deg(h^{n-1}) \leq \deg(f) + \deg(g) - 1$$

$$\deg(f^{n-1}) \leq \deg(g) + \deg(h) - 1$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$\deg(h^{n-1}) \leq \deg(f) + \deg(g) - 1$$

$$\deg(f^{n-1}) \leq \deg(g) + \deg(h) - 1$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$n \deg(h) \leq \deg(f) + \deg(g) - 1 + \deg(h)$$

$$\deg(f^{n-1}) \leq \deg(g) + \deg(h) - 1$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$n \deg(h) \leq \deg(f) + \deg(g) - 1 + \deg(h)$$

$$n \deg(f) \leq \deg(g) + \deg(h) - 1 + \deg(f)$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$n \deg(h) \leq \deg(f) + \deg(g) - 1 + \deg(h)$$

$$n \deg(f) \leq \deg(g) + \deg(h) - 1 + \deg(f)$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$n \deg(h) \leq \deg(f) + \deg(g) - 1 + \deg(h)$$

$$n \deg(f) \leq \deg(g) + \deg(h) - 1 + \deg(f)$$

$$n(\deg(f) + \deg(g) + \deg(h))$$

$$\leq 3(\deg(f) + \deg(g) + \deg(h)) - 3$$

Let $f, g, h \in \mathbb{C}[X]$ such that

$\gcd(f, g, h) = 1$ and $n \geq 3$.

Then $f^n + g^n = h^n$ is only possible if $f, g, h \in \mathbb{C}$.

Proof: So $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$n \deg(g) \leq \deg(f) + \deg(h) - 1 + \deg(g)$$

$$n \deg(h) \leq \deg(f) + \deg(g) - 1 + \deg(h)$$

$$n \deg(f) \leq \deg(g) + \deg(h) - 1 + \deg(f)$$

$$n(\deg(f) + \deg(g) + \deg(h))$$

$$\leq 3(\deg(f) + \deg(g) + \deg(h)) - 3$$

$(n - 3)(\deg(f) + \deg(g) + \deg(h)) \leq -3$, contradiction!!

What's the story about $l, m, n \in \mathbb{N}$ large enough and $x^l + y^m = z^n$? If $x, y, z \in \mathbb{Z}$ then Wiles only gave a proof for $l = m = n !$

Let's take it a little further. . .



Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 57^3$.

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 57^3$.

$\mathbb{C}[X]$: The zeroes of $(X - 3)(X + 1)^2$ are 3, 1

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 5 7^3$.

$\mathbb{C}[X]$: The zeroes of $(X - 3)(X + 1)^2$ are 3, 1

\mathbb{Z} : The divisors of $3^2 5 7^3$ are 3, 5, 7.

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 5 7^3$.

Define:

$\mathbb{C}[X]$: The zeroes of $(X - 3)(X + 1)^2$ are 3, 1

\mathbb{Z} : The divisors of $3^2 5 7^3$ are 3, 5, 7.

$$\text{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7.$$

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 5 7^3$.

Define:

$\mathbb{C}[X]$: The zeroes of $(X - 3)(X + 1)^2$ are 3, 1

\mathbb{Z} : The divisors of $3^2 5 7^3$ are 3, 5, 7.

$\text{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7$.

ABC-conjecture:

Let's take it a little further...

$\mathbb{C}[X]$: 3 is zero of $(X - 3)(X + 1)^2$

\mathbb{Z} : 3 is a divisor of $3^2 5 7^3$.

Define:

$\mathbb{C}[X]$: The zeroes of $(X - 3)(X + 1)^2$ are 3, 1

\mathbb{Z} : The divisors of $3^2 5 7^3$ are 3, 5, 7.

$$\text{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7.$$

ABC-conjecture: If $a + b = c$, $a, b, c \in \mathbb{N}$, $\gcd(a, b, c) = 1$,

then c cannot be too big, compared to $\text{rad}(abc)$:

for every $\epsilon > 0$ there exists some K_ϵ such that

$$c < K_\epsilon \text{rad}(abc)^{1+\epsilon}.$$

ABC-conjecture:

If $a + b = c$, $a, b, c \in \mathbb{N}$, $\gcd(a, b, c) = 1$, then c cannot be too big, compared to $\text{rad}(abc)$:

for every $\epsilon > 0$ there exists some K_ϵ such that

$$c < K_\epsilon \text{rad}(abc)^{1+\epsilon}.$$

ABC-conjecture:

If $a + b = c$, $a, b, c \in \mathbb{N}$, $\gcd(a, b, c) = 1$, then c cannot be too big, compared to $\text{rad}(abc)$:

for every $\epsilon > 0$ there exists some K_ϵ such that

$$c < K_\epsilon \text{rad}(abc)^{1+\epsilon}.$$

Version for $\mathbb{C}[X]$:

ABC-conjecture:

If $a + b = c$, $a, b, c \in \mathbb{N}$, $\gcd(a, b, c) = 1$, then c cannot be too big, compared to $\text{rad}(abc)$:

for every $\epsilon > 0$ there exists some K_ϵ such that

$$c < K_\epsilon \text{rad}(abc)^{1+\epsilon}.$$

Version for $\mathbb{C}[X]$:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh)$$

where $N(fgh)$ is the number of zeroes of fgh .

If ABC conjecture true, then Fermat is an immediate consequence. And more stuff ($x^l + y^m = z^n$). I'll not prove this today, but - I'll prove the *ABC* conjecture for polynomials!!

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: _____

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

$$f + g = h$$

Proof: _____

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

f	$+g$	$= h$
f'	$+g'$	$= h'$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

f	$+g$	$= h$	times f'
f'	$+g'$	$= h'$	times f

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$f f'$	$+g f'$	$= h f'$	times f'
$f' f$	$+g' f$	$= h' f$	times f

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

	$f f'$	$+g f'$	$= h f'$	times f'
	$- f' f$	$+g' f$	$= h' f$	times f
<hr/>				

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

	$f f'$	$+g f'$	$= h f'$	times f'
	$- f' f$	$+g' f$	$= h' f$	times f
<hr/>				
	$f'g - fg'$		$= f'h - fh'$	

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$ and $\mid fg'$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$
and $\mid fg'$. So

$$\gcd(f, f') \mid f'g - fg'$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$
and $\mid fg'$. So

$$\gcd(f, f') \mid f'g - fg'$$

$$\gcd(g, g') \mid f'g - fg'$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$
and $\mid fg'$. So

$$\gcd(f, f') \mid f'g - fg'$$

$$\gcd(g, g') \mid f'g - fg'$$

$$\gcd(h, h') \mid f'h - fh'$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$ and $\mid fg'$. So

$$\gcd(f, f') \mid f'g - fg'$$

$$\gcd(g, g') \mid f'g - fg'$$

$$\gcd(h, h') \mid f'h - fh' = f'g - fg'.$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') \mid f'g$ and $\mid fg'$. So

$$\gcd(f, f') \mid f'g - fg'$$

$$\gcd(g, g') \mid f'g - fg'$$

$$\gcd(h, h') \mid f'h - fh' = f'g - fg'.$$

So $\gcd(f, f')\gcd(g, g')\gcd(h, h') \mid f'g - fg'$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So $f'g - fg' = f'h - fh'$. Now we have: $\gcd(f, f') | f'g$ and $|fg'$. So

$$\gcd(f, f') | f'g - fg'$$

$$\gcd(g, g') | f'g - fg'$$

$$\gcd(h, h') | f'h - fh' = f'g - fg'.$$

$$\text{So } \gcd(f, f')\gcd(g, g')\gcd(h, h') | f'g - fg'.$$

So

$$\begin{aligned} \deg(\gcd(f, f')) + \deg(\gcd(g, g')) + \deg(\gcd(h, h')) \\ \leq \deg(f) + \deg(g) - 1. \end{aligned}$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So

$$\begin{aligned} \deg(\gcd(f, f')) + \deg(\gcd(g, g')) + \deg(\gcd(h, h')) \\ \leq \deg(f) + \deg(g) - 1. \end{aligned}$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So

$$\begin{aligned} \deg(\gcd(f, f')) + \deg(\gcd(g, g')) + \deg(\gcd(h, h')) \\ \leq \deg(f) + \deg(g) - 1. \end{aligned}$$

Everything to the right, and then $+\deg(h)$:

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof: So

$$\begin{aligned} \deg(\gcd(f, f')) + \deg(\gcd(g, g')) + \deg(\gcd(h, h')) \\ \leq \deg(f) + \deg(g) - 1. \end{aligned}$$

Everything to the right, and then $+\deg(h)$:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Proof: Suppose $(X - c)^n$ divides f

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Proof: Suppose $(X - c)^n$ divides $f = (X - c)^n \tilde{f}$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ &\deg(f) - \deg(\gcd(f, f')) + \\ &\deg(g) - \deg(\gcd(g, g')) + \\ &\deg(h) - \deg(\gcd(h, h')) \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Proof: Suppose $(X - c)^n$ divides $f = (X - c)^n \tilde{f}$. Then $(X - c)^{n-1}$ divides $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1} \tilde{f}$.

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Proof: Suppose $(X - c)^n$ divides $f = (X - c)^n \tilde{f}$. Then $(X - c)^{n-1}$ divides $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1} \tilde{f}$.
... (krijtbord?)

Mason's Theorem:

Let $f, g, h \in \mathbb{C}[X]$ satisfy $f + g = h$, $\gcd(f, g, h) = 1$, then

$$\deg(f) < N(fgh).$$

Proof:

$$\begin{aligned} \deg(h) &\leq \\ \deg(f) - \deg(\gcd(f, f')) &+ \\ \deg(g) - \deg(\gcd(g, g')) &+ \\ \deg(h) - \deg(\gcd(h, h')) & \end{aligned}$$

Lemma: $\deg(f) \leq \deg(\gcd(f, f')) + N(f)$.

Proof: Suppose $(X - c)^n$ divides $f = (X - c)^n \tilde{f}$. Then $(X - c)^{n-1}$ divides $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1} \tilde{f}$.
... (krijtbord?) Using the lemma we get Mason's!

Theorem:

Let $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$. If $F, G, H \in \mathbb{C}[X]$ satisfying $\gcd(F, G, H) = 1$ and $F^p + G^q = H^r$ then $F, G, H \in \mathbb{C}$.

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$.

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$p\deg(F) < N(F^p G^q H^r)$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$\begin{aligned} p\deg(F) &< N(F^p G^q H^r) \\ &= N(FGH) \end{aligned}$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$p\deg(F) < N(F^p G^q H^r)$$

$$= N(FGH)$$

$$\leq \deg(F) + \deg(G) + \deg(H)$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$\begin{aligned} p\deg(F) &< N(F^p G^q H^r) \\ &= N(FGH) \\ &\leq \deg(F) + \deg(G) + \deg(H) \\ &\leq \deg(F) + \frac{p}{q}\deg(F) + \frac{p}{r}\deg(F) \end{aligned}$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$\begin{aligned} p\deg(F) &< N(F^p G^q H^r) \\ &= N(FGH) \\ &\leq \deg(F) + \deg(G) + \deg(H) \\ &\leq \deg(F) + \frac{p}{q}\deg(F) + \frac{p}{r}\deg(F) \end{aligned}$$

Divide by $p\deg(F)$:

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$\begin{aligned} p\deg(F) &< N(F^p G^q H^r) \\ &= N(FGH) \\ &\leq \deg(F) + \deg(G) + \deg(H) \\ &\leq \deg(F) + \frac{p}{q}\deg(F) + \frac{p}{r}\deg(F) \end{aligned}$$

Divide by $p\deg(F)$:

$$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}.$$

Proof:

We may assume that $\deg(F^p) \geq \deg(G^q), \deg(H^r)$. Thus

$$q\deg(G) \leq p\deg(F),$$

$$r\deg(H) \leq p\deg(F).$$

Using Mason's:

$$\begin{aligned} p\deg(F) &< N(F^p G^q H^r) \\ &= N(FGH) \\ &\leq \deg(F) + \deg(G) + \deg(H) \\ &\leq \deg(F) + \frac{p}{q}\deg(F) + \frac{p}{r}\deg(F) \end{aligned}$$

Divide by $p\deg(F)$:

$$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}. \text{ Contradiction!}$$

Notice: $p = q = r$ gives $\frac{1}{n} + \frac{1}{n} + \frac{1}{n} \leq 1$ so $n \geq 3$.

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

Why can we prove all these things for $\mathbb{C}[X]$ and is it so hard for \mathbb{Z} ?

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

Why can we prove all these things for $\mathbb{C}[X]$ and is it so hard for \mathbb{Z} ?

Remember the proof. . .

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

Why can we prove all these things for $\mathbb{C}[X]$ and is it so hard for \mathbb{Z} ?

Remember the proof...

$$f f' + g f' = h f' \quad \text{maal } f'$$

$$- f' f + g' f = h' f \quad \text{maal } f$$

$$f'g - fg' = f'h - fh'$$

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

Why can we prove all these things for $\mathbb{C}[X]$ and is it so hard for \mathbb{Z} ?

Remember the proof. . .

$$\begin{array}{rcll} f f' + g f' & = & h f' & \text{maal } f' \\ - f' f + g' f & = & h' f & \text{maal } f \\ \hline f' g - f g' & = & f' h - f h' & \end{array}$$

What is wrong in these lines if $f, g, h \in \mathbb{Z}$?

It's even worse- There's a variant of the Riemann hypothesis for polynomials (over \mathbb{F}_p) that one can prove !

Why can we prove all these things for $\mathbb{C}[X]$ and is it so hard for \mathbb{Z} ?

Remember the proof. . .

$$\begin{array}{rcll} f f' + g f' & = & h f' & \text{maal } f' \\ - f' f + g' f & = & h' f & \text{maal } f \\ \hline f' g - f g' & = & f' h - f h' & \end{array}$$

What is wrong in these lines if $f, g, h \in \mathbb{Z}$? Exactly! In $\mathbb{C}[X]$ one can take derivatives!

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ all } f, g. \text{ (Leibniz rule.)}$$

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ all } f, g. \text{ (Leibniz rule.)}$$

Well, let's make one on \mathbb{Z} , so we can prove stuff!

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ all } f, g. \text{ (Leibniz rule.)}$$

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ all } f, g. \text{ (Leibniz rule.)}$$

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ all } f, g. \text{ (Leibniz rule.)}$$

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

Bummer.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

Bummer. $D(a + b) \neq D(a) + D(b)$.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

Bummer. $D(a + b) \neq D(a) + D(b)$.

Als: δ is *locally nilpotent*. Which means: for every $f \in \mathbb{C}[X]$ there exists some n such that $\delta^n(f) = 0$.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use

Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^3 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

Bummer. $D(a + b) \neq D(a) + D(b)$.

Als: δ is *locally nilpotent*. Which means: for every $f \in \mathbb{C}[X]$ there exists some n such that $\delta^n(f) = 0$.

On \mathbb{Z} : $D(2^2) = 2 \cdot 2$.

$\mathbb{C}[X]$ has a *derivation*: a map δ satisfying

$\delta(fg) = f\delta(g) + g\delta(f)$ all f, g . (Leibniz rule.)

Well, let's make one on \mathbb{Z} , so we can prove stuff!

Copying $\mathbb{C}[X]$: "primes" $(X - c)$ go to 1.

So: on \mathbb{Z} : send 2, 3, 5, 7, 11, ... to 1. For anything else: use Leibniz rule:

$$D(5^7) = 7 \cdot 5^6, \quad D(2^3 5^2) = 3 \cdot 2^2 5^2 + 2 \cdot 2^3 5.$$

Fun!! Can we now solve Fermat with this??

Bummer. $D(a + b) \neq D(a) + D(b)$.

Als: δ is *locally nilpotent*. Which means: for every $f \in \mathbb{C}[X]$ there exists some n such that $\delta^n(f) = 0$.

On \mathbb{Z} : $D(2^2) = 2 \cdot 2$. And

$D(2^2 a) = 2^2 D(a) + 2 \cdot 2a = 2^2(D(a) + a)$ so that one increases and increases if $a > 1$!

Lifting a tip of the veil of my
research. . .

Lifting a tip of the veil of my

research. . . $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$.

Lifting a tip of the veil of my research. . . $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$. We want to understand this set - do there exist “nice” group actions of $\mathbb{C}, +$ on this set?

Lifting a tip of the veil of my research. . . $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$. We want to understand this set - do there exist “nice” group actions of $\mathbb{C}, +$ on this set?

Comes down to finding a locally nilpotent derivation D on the ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something bigger

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some field.

Locally nilpotent derivations D on the ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more? Suppose $D \neq 0$. Then it is possible to extend D on something bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something

bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some

field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements

x, y, z can be seen as elements in $\mathbb{K}[S]$:

$x = f(S), y = g(S), z = h(S)$.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something

bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some

field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements

x, y, z can be seen as elements in $\mathbb{K}[S]$:

$x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so

$f^2 + g^3 + h^7 = 0$. I can assume for some reason that

$\gcd(f, g, h) = 1$,

Locally nilpotent derivations D on the ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more? Suppose $D \neq 0$. Then it is possible to extend D on something bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements x, y, z can be seen as elements in $\mathbb{K}[S]$:
 $x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so $f^2 + g^3 + h^7 = 0$. I can assume for some reason that $\gcd(f, g, h) = 1$, and now Mason's yields that $f, g, h \in \mathbb{K}$.

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something

bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some

field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements

x, y, z can be seen as elements in $\mathbb{K}[S]$:

$x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so

$f^2 + g^3 + h^7 = 0$. I can assume for some reason that

$\gcd(f, g, h) = 1$, and now Mason's yields that $f, g, h \in \mathbb{K}$.

But D is zero on elements of \mathbb{K}

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something

bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some

field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements

x, y, z can be seen as elements in $\mathbb{K}[S]$:

$x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so

$f^2 + g^3 + h^7 = 0$. I can assume for some reason that

$\gcd(f, g, h) = 1$, and now Mason's yields that $f, g, h \in \mathbb{K}$.

But D is zero on elements of \mathbb{K} - so

$$D(x) = D(y) = D(z) = 0$$

Locally nilpotent derivations D on the ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more? Suppose $D \neq 0$. Then it is possible to extend D on something bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where \mathbb{K} is some field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements x, y, z can be seen as elements in $\mathbb{K}[S]$: $x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so $f^2 + g^3 + h^7 = 0$. I can assume for some reason that $\gcd(f, g, h) = 1$, and now Mason's yields that $f, g, h \in \mathbb{K}$. But D is zero on elements of \mathbb{K} - so $D(x) = D(y) = D(z) = 0$ and that implies that D is zero on the whole ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$!

Locally nilpotent derivations D on the ring

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. $D = 0$ is one, are there more?.

Suppose $D \neq 0$. Then it is possible to extend D on something

bigger - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ where K is some

field. And on $\mathbb{K}[S]$ the map D behaves like $\frac{\partial}{\partial S}$. So elements

x, y, z can be seen as elements in $\mathbb{K}[S]$:

$x = f(S), y = g(S), z = h(S)$. For sure: $x^2 + y^3 + z^7 = 0$, so

$f^2 + g^3 + h^7 = 0$. I can assume for some reason that

$\gcd(f, g, h) = 1$, and now Mason's yields that $f, g, h \in \mathbb{K}$.

But D is zero on elements of \mathbb{K} - so

$D(x) = D(y) = D(z) = 0$ and that implies that D is zero on

the whole ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$! Contradiction, so

the only locally nilpotent derivation on

$\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$ is $D = 0$.

Conclusions

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$?

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$? (Or why can't we do things with \mathbb{Z} and why can we with $\mathbb{C}[X]$?)

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$? (Or why can't we do things with \mathbb{Z} and why can we with $\mathbb{C}[X]$?)

There's no "derivative" on elements of \mathbb{Z} ! (At least, no tasty one. . .)

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$? (Or why can't we do things with \mathbb{Z} and why can we with $\mathbb{C}[X]$?)

There's no "derivative" on elements of \mathbb{Z} ! (At least, no tasty one. . .)

MORAL OF THIS STORY:

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$? (Or why can't we do things with \mathbb{Z} and why can we with $\mathbb{C}[X]$?)

There's no "derivative" on elements of \mathbb{Z} ! (At least, no tasty one. . .)

MORAL OF THIS STORY: Be Happy If You Find A
Locally Nilpotent Derivation on your ring. . .

Conclusions

Why is \mathbb{Z} so much more difficult as $\mathbb{C}[X]$? (Or why can't we do things with \mathbb{Z} and why can we with $\mathbb{C}[X]$?)

There's no "derivative" on elements of \mathbb{Z} ! (At least, no tasty one. . .)

MORAL OF THIS STORY: Be Happy If You Find A Locally Nilpotent Derivation on your ring. . .

****** THANK YOU ******