# Studenten vriendelijk colloquium $\mathbb{Z}$ is moeilijk, polynomen zijn makkelijk.

Stefan Maubach

Maart 2008

$\mathbb{Z}$ heeft priemgetallen: $2, 3, 5, 7, \ldots$ en een unieke priemfactor ontbinding. Als ik in een kamertje ga zitten en 2537 ontbind in producten van priemfactoren, en jij in een ander kamertje, dan komen daar dezelfde priemgetallen uit.

$\mathbb{Z}$ heeft priemgetallen: $2, 3, 5, 7, \ldots$ en een unieke priemfactor ontbinding. Als ik in een kamertje ga zitten en 2537 ontbind in producten van priemfactoren, en jij in een ander kamertje, dan komen daar dezelfde priemgetallen uit.
Stiekem: 2 en $-2$ worden als "hetzelfde priemgetal" gezien.
Ze verschillen exact een eenheid:

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

Of equivalent: $2\mathbb{Z}$ en $-2\mathbb{Z}$ zijn dezelfde verzameling.

$\mathbb{Z}$ heeft priemgetallen: $2, 3, 5, 7, \ldots$ en een unieke priemfactor ontbinding. Als ik in een kamertje ga zitten en 2537 ontbind in producten van priemfactoren, en jij in een ander kamertje, dan komen daar dezelfde priemgetallen uit.
Stiekem: 2 en $-2$ worden als "hetzelfde priemgetal" gezien.
Ze verschillen exact een eenheid:

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

Of equivalent: $2\mathbb{Z}$ en $-2\mathbb{Z}$ zijn dezelfde verzameling.
Een priemgetal is dus een element dat niet inverteerbaar is, en niet deelbaar door iets anders.

$\mathbb{Z}$ heeft priemgetallen: $2, 3, 5, 7, \ldots$ en een unieke priemfactor ontbinding. Als ik in een kamertje ga zitten en 2537 ontbind in producten van priemfactoren, en jij in een ander kamertje, dan komen daar dezelfde priemgetallen uit.

Stiekem: 2 en $-2$ worden als "hetzelfde priemgetal" gezien.

Ze verschillen exact een eenheid:

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

Of equivalent: $2\mathbb{Z}$ en $-2\mathbb{Z}$ zijn dezelfde verzameling.

Een priemgetal is dus een element dat niet inverteerbaar is, en niet deelbaar door iets anders.

Zijn er ook andere "dingen" met priemgetallen?

In $\mathbb{Z}$ kun je optellen, aftrekken, en vermenigvuldigen. Niet delen! Als je door alles zou kunnen delen dan heb je geen priemgetallen!

In $\mathbb{Z}$ kun je optellen, aftrekken, en vermenigvuldigen. Niet delen! Als je door alles zou kunnen delen dan heb je geen priemgetallen!

$\mathbb{Z}$ is een *ring*. Als je ook kunt delen dan heb je een lichaam.

In $\mathbb{Z}$ kun je optellen, aftrekken, en vermenigvuldigen. Niet delen! Als je door alles zou kunnen delen dan heb je geen priemgetallen!

$\mathbb{Z}$ is een *ring*. Als je ook kunt delen dan heb je een lichaam.

Zijn er ook andere “dingen” met priemgetallen?

Zijn er ook andere Ringen met priemgetallen?

Zijn er ook andere Ringen met priemgetallen?

$\mathbb{R}[X]$ is de verzameling polynomen, i.e.

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

Zijn er ook andere Ringen met priemgetallen?

$\mathbb{R}[X]$ is de verzameling polynomen, i.e.

$$\mathbb{R}[X] := \{a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}.$$

Zelfde:

$$\mathbb{C}[X] := \{a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \mid n \in \mathbb{N}, a_i \in \mathbb{C}\}.$$

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

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | | |

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| | | |

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | | |

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X + 1, X - 37.2, X^2 + 1$ |

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X)\cdots p_n(X)$.

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X) \cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X) \cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X-37$ zijn "hetzelfde" priemgetal! Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37).

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X) \cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X - 37$ zijn "hetzelfde" priemgetal!
Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37).
Verder is $X^2+1$ ook irreducibel...

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X)\cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X-37$ zijn "hetzelfde" priemgetal!
Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37).
Verder is $X^2+1$ ook irreducibel… maar…

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \dots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X)\cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X-37$ zijn "hetzelfde" priemgetal! Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37). Verder is $X^2+1$ ook irreducibel... maar... over $\mathbb{C}$ zijn alle "priem"polynomen van graad 1 ! $X^2+1 = (X+i)(X-i)$.

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X) \cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X-37$ zijn "hetzelfde" priemgetal! Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37). Verder is $X^2+1$ ook irreducibel... maar... over $\mathbb{C}$ zijn alle "priem" polynomen van graad 1 ! $X^2+1 = (X+i)(X-i)$. Dwz: als $p(X)$ van graad 37, dan is $p$ een product van 37 "priem" polynomen.

| | $\mathbb{Z}$ | $\mathbb{R}[X]$ |
|---|---|---|
| Inv. element. | $1, -1$ | $\mathbb{R}\backslash\{0\}$ |
| Priemgetallen | $2, 3, 5, \ldots$ | polynomen $X+1, X-37.2, X^2+1$ |

Want kijk maar: elk polynoom $p(X)$ valt uit elkaar als product van polynomen $p(X) = p_1(X) \cdots p_n(X)$. Als dat niet verder meer kan, dan heb je een irreducibel polynoom. Dat noem je "priem".

Merk op: $X+1$ en $-37X-37$ zijn "hetzelfde" priemgetal! Net als 2 en $-2$ verschillen ze een eenheid (in dit geval 37). Verder is $X^2+1$ ook irreducibel… maar… over $\mathbb{C}$ zijn alle "priem" polynomen van graad 1 ! $X^2+1 = (X+i)(X-i)$. Dwz: als $p(X)$ van graad 37, dan is $p$ een product van 37 "priem" polynomen. Laten we ook afspreken dat $1 \cdot X + \alpha$ de "standaardpriemen" zijn in $\mathbb{C}[X]$.

$$\mathrm{ggd}(12, 8) = \mathrm{ggd}(2^2 \cdot 3, 2^3) = 2^2 = 4.$$

$$\text{ggd}(12,8) = \text{ggd}(2^2 \cdot 3, 2^3) = 2^2 = 4.$$

$$\text{ggd}(X^3 + X^2 - X - 1, X^3 + 3X^2 + 3X + 1) =$$

$$\text{ggd}((X+1)^2(X-1), (X+1)^3) = (X+1)^2.$$

$\text{ggd}(12, 8) = \text{ggd}(2^2 \cdot 3, 2^3) = 2^2 = 4.$

$\text{ggd}(X^3 + X^2 - X - 1, X^3 + 3X^2 + 3X + 1) =$

$\text{ggd}((X+1)^2(X-1), (X+1)^3) = (X+1)^2.$

Voor $\mathbb{C}[X]$ kun je "$\text{ggd}(f, g) = 1$" ook zeggen als "$f$ en $g$ hebben verschillende nulpunten".

# De Laatste Stelling van Fermat

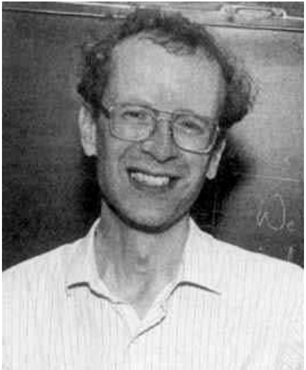
# De Laatste Stelling van Fermat

$a, b, c \in \mathbb{Z}$ zodat

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

Dan is $a^n + b^n = c^n$ niet mogelijk.

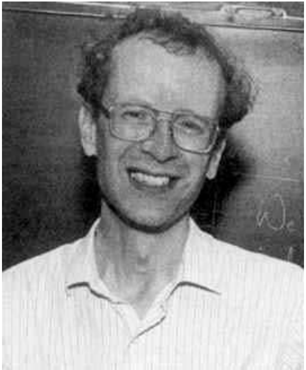
# De Laatste Stelling van Fermat

 $a, b, c \in \mathbb{Z}$ zodat

$\mathrm{ggd}(a, b, c) = 1$ en $n \geq 3$

Dan is $a^n + b^n = c^n$ niet mogelijk.

# De Laatste Stelling van Fermat



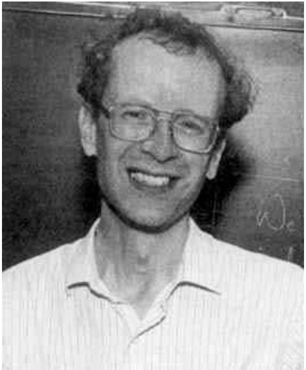
$a, b, c \in \mathbb{Z}$ zodat

ggd$(a, b, c) = 1$ en $n \geq 3$

Dan is $a^n + b^n = c^n$ niet mogelijk.

Bewijs van Wiles is vet moeilijk -

# De Laatste Stelling van Fermat



$a, b, c \in \mathbb{Z}$ zodat

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

Dan is $a^n + b^n = c^n$ niet mogelijk.

Bewijs van Wiles is vet moeilijk - handjes omhoog van wie het bewijs heeft gelezen en begrepen! NU!

# De Laatste Stelling van Fermat voor $\mathbb{C}[X]$

$a, b, c \in \mathbb{Z}$ zodat

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

Dan is $a^n + b^n = c^n$ niet mogelijk.

# De Laatste Stelling van Fermat voor $\mathbb{C}[X]$

$a, b, c \in \mathbb{Z}$ zodat

$\mathrm{ggd}(a, b, c) = 1$ en $n \geq 3$

Dan is $a^n + b^n = c^n$ niet mogelijk.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

Zij $f, g, h \in \mathbb{C}[X]$ zodat
$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

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

---

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

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

---

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

$$\begin{array}{llll} f^n & +g^n & = h^n & \text{maal } f' \\ f'f^{n-1} & +g'g^{n-1} & = h'h^{n-1} & \text{maal } f \\ \hline \end{array}$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

$$\begin{array}{llll} f^n\ f' & +g^n\ f' & = h^n\ f' & \text{maal } f' \\ f' f^{n-1}\ f & +g' g^{n-1}\ f & = h' h^{n-1}\ f & \text{maal } f \\ \hline \end{array}$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat
ggd$(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

$$
\begin{array}{lllll}
 & f^n\ f' & +g^n\ f' & = h^n\ f' & \text{maal } f' \\
- & f' f^{n-1}\ f & +g' g^{n-1}\ f & = h' h^{n-1}\ f & \text{maal } f \\
\hline
\end{array}
$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

$$
\begin{array}{rlllll}
 & f^n\ f' & +g^n\ f' & = h^n\ f' & & \text{maal } f' \\
- & f' f^{n-1}\ f & +g' g^{n-1}\ f & = h' h^{n-1}\ f & & \text{maal } f \\
\hline
 & & f' g^n - f g' g^{n-1} & = f' h^n - f h' h^{n-1} & &
\end{array}
$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:**

$$\begin{array}{clllr} & f^n\ f' & +g^n\ f' & = h^n\ f' & \text{maal } f' \\ - & f'f^{n-1}\ f & +g'g^{n-1}\ f & = h'h^{n-1}\ f & \text{maal } f \\ \hline & & f'g^n - fg'g^{n-1} & = f'h^n - fh'h^{n-1} & \end{array}$$

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat
$\operatorname{ggd}(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.
**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.
Stel $f'g - fg' = 0$.

dus we mogen aannemen dat $f'g - fg', f'h - f'h$, en $g'h - gh'$ ongelijk 0 zijn.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Stel $f'g - fg' = 0$. Dus $f'g = fg'$.

dus we

mogen aannemen dat $f'g - fg', f'h - f'h$, en $g'h - gh'$

ongelijk 0 zijn.

Zij $f, g, h \in \mathbb{C}[X]$ zodat
$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.
**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.
Stel $f'g - fg' = 0$. Dus $f'g = fg'$. Omdat $\mathrm{ggd}(g, f) = 1$ deelt $g$ dus $g'$, en $f$ deelt $f'$

dus we

mogen aannemen dat $f'g - fg', f'h - f'h$, en $g'h - gh'$ ongelijk 0 zijn.

Zij $f, g, h \in \mathbb{C}[X]$ zodat
$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.
**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.
Stel $f'g - fg' = 0$. Dus $f'g = fg'$. Omdat $\text{ggd}(g, f) = 1$ deelt $g$ dus $g'$, en $f$ deelt $f'$ - en dat kan alleen als $f, g$ constant zijn dus we mogen aannemen dat $f'g - fg', f'h - f'h$, en $g'h - gh'$ ongelijk 0 zijn.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$.

Stel $f'g - fg' = 0$. Dus $f'g = fg'$. Omdat $\text{ggd}(g, f) = 1$ deelt $g$ dus $g'$, en $f$ deelt $f'$ - en dat kan alleen als $f, g$ constant zijn en dan $h$ automatisch constant! Dit geval is af. dus we mogen aannemen dat $f'g - fg', f'h - f'h$, en $g'h - gh'$ ongelijk 0 zijn.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

en

alle $f'g - fg', f'h - f'h$, en $g'h - gh'$ zijn ongelijk 0.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

Dus $g^{n-1}$ deelt $f'h - fh'$,

en

alle $f'g - fg', f'h - f'h$, en $g'h - gh'$ zijn ongelijk 0.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

Dus $g^{n-1}$ deelt $f'h - fh'$,

en $h^{n-1}$ deelt $f'g - fg'$, en

en $f^{n-1}$ deelt $g'h - gh'$,

alle $f'g - fg', f'h - f'h$, en $g'h - gh'$ zijn ongelijk 0.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

Dus $g^{n-1}$ deelt $f'h - fh'$, $\quad deg(g^{n-1}) \leq deg(f'h - fh')$

en $h^{n-1}$ deelt $f'g - fg'$, $\quad deg(h^{n-1}) \leq deg(f'g - fg')$ en

en $f^{n-1}$ deelt $g'h - gh'$, $\quad deg(f^{n-1}) \leq deg(g'h - gh')$

alle $f'g - fg', f'h - f'h$, en $g'h - gh'$ zijn ongelijk 0.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

Dus $g^{n-1}$ deelt $f'h - fh'$, $\quad deg(g^{n-1}) \leq deg(f) + deg(h) - 1$

en $h^{n-1}$ deelt $f'g - fg'$, $\quad deg(h^{n-1}) \leq deg(f) + deg(g) - 1$

en $f^{n-1}$ deelt $g'h - gh'$, $\quad deg(f^{n-1}) \leq deg(g) + deg(h) - 1$

en alle $f'g - fg', f'h - f'h$, en $g'h - gh'$ zijn ongelijk 0.

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\operatorname{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

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

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

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

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

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

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

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

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

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat
$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.
Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.
**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

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

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$
\begin{aligned}
ndeg(g) &\leq deg(f) + deg(h) - 1 + deg(g) \\
ndeg(h) &\leq deg(f) + deg(g) - 1 + deg(h) \\
ndeg(f) &\leq deg(g) + deg(h) - 1 + deg(f) \\
\hline
\end{aligned}
$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\mathrm{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$\begin{array}{l} n deg(g) \leq deg(f) + deg(h) - 1 + deg(g) \\ n deg(h) \leq deg(f) + deg(g) - 1 + deg(h) \\ n deg(f) \leq deg(g) + deg(h) - 1 + deg(f) \\ \hline n(deg(f) + deg(g) + deg(h)) \\ \qquad\qquad \leq 3(deg(f) + deg(g) + deg(h)) - 3 \end{array}$$

Zij $f, g, h \in \mathbb{C}[X]$ zodat

$\text{ggd}(f, g, h) = 1$ en $n \geq 3$.

Dan is $f^n + g^n = h^n$ alleen mogelijk als $f, g, h \in \mathbb{C}$.

**Bewijs:** Dus $g^{n-1}(f'g - fg') = h^{n-1}(f'h - fh')$,

$$
\begin{array}{l}
n deg(g) \leq deg(f) + deg(h) - 1 + deg(g) \\
n deg(h) \leq deg(f) + deg(g) - 1 + deg(h) \\
n deg(f) \leq deg(g) + deg(h) - 1 + deg(f) \\
\hline
n(deg(f) + deg(g) + deg(h)) \\
\qquad \leq 3(deg(f) + deg(g) + deg(h)) - 3
\end{array}
$$

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

Hoe zit dat nu met $l, m, n \in \mathbb{N}$ groot genoeg en $x^l + y^m = z^n$ ? Als $x, y, z \in \mathbb{Z}$ dan bewees Wiles het alleen voor $l = m = n$ !

Nog even wat verder duwen. . .

Nog even wat verder duwen…

$\mathbb{C}[X]$: 3 is een nulpunt van $(X-3)(X+1)^2$

Nog even wat verder duwen...

$\mathbb{C}[X]$: 3 is een nulpunt van $(X-3)(X+1)^2$

$\mathbb{Z}$: 3 is een deler van $3^2 57^3$.

Nog even wat verder duwen...

| | |
|---|---|
| $\mathbb{C}[X]$: | 3 is een nulpunt van $(X-3)(X+1)^2$ |
| $\mathbb{Z}$: | 3 is een deler van $3^2 57^3$. |
| $\mathbb{C}[X]$: | De nulpunten van $(X-3)(X+1)^2$ zijn $3, 1$ |

Nog even wat verder duwen...

| | |
|---|---|
| $\mathbb{C}[X]$: | 3 is een nulpunt van $(X-3)(X+1)^2$ |
| $\mathbb{Z}$: | 3 is een deler van $3^2 5 7^3$. |
| $\mathbb{C}[X]$: | De nulpunten van $(X-3)(X+1)^2$ zijn $3, 1$ |
| $\mathbb{Z}$: | De delers van $3^2 5 7^3$ zijn 3,5,7. |

Nog even wat verder duwen...

| | |
|---|---|
| $\mathbb{C}[X]$: | 3 is een nulpunt van $(X-3)(X+1)^2$ |
| $\mathbb{Z}$: | 3 is een deler van $3^2 5 7^3$. |
| $\mathbb{C}[X]$: | De nulpunten van $(X-3)(X+1)^2$ zijn $3, 1$ |
| $\mathbb{Z}$: | De delers van $3^2 5 7^3$ zijn 3,5,7. |

Definieer: $\mathrm{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7$.

Nog even wat verder duwen...

| | |
|---|---|
| $\mathbb{C}[X]$: | 3 is een nulpunt van $(X-3)(X+1)^2$ |
| $\mathbb{Z}$: | 3 is een deler van $3^2 5 7^3$. |
| $\mathbb{C}[X]$: | De nulpunten van $(X-3)(X+1)^2$ zijn $3, 1$ |
| $\mathbb{Z}$: | De delers van $3^2 5 7^3$ zijn 3,5,7. |

Definieer: $\mathrm{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7$.

**ABC-vermoeden:**

Nog even wat verder duwen...

| | |
|---|---|
| $\mathbb{C}[X]$: | 3 is een nulpunt van $(X-3)(X+1)^2$ |
| $\mathbb{Z}$: | 3 is een deler van $3^2 5 7^3$. |
| $\mathbb{C}[X]$: | De nulpunten van $(X-3)(X+1)^2$ zijn $3, 1$ |
| $\mathbb{Z}$: | De delers van $3^2 5 7^3$ zijn 3,5,7. |

Definieer: $\mathrm{rad}(3^2 5 7^3) = 3 \cdot 5 \cdot 7$.

**ABC-vermoeden:** Als $a + b = c$, $a, b, c \in \mathbb{N}$, $\mathrm{ggd}(a, b, c) = 1$, dan kan $c$ niet al te groot zijn in verhouding tot $\mathrm{rad}(abc)$:

voor elke $\epsilon > 0$ bestaat er een $K_\epsilon$ zodat

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

# ABC-vermoeden:

Als $a + b = c$, $a, b, c \in \mathbb{N}$, $\mathrm{ggd}(a, b, c) = 1$, dan kan $c$ niet al te groot zijn in verhouding tot $\mathrm{rad}(abc)$:
voor elke $\epsilon > 0$ bestaat er een $K_\epsilon$ zodat

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

# ABC-vermoeden:

Als $a + b = c$, $a, b, c \in \mathbb{N}$, $\text{ggd}(a, b, c) = 1$, dan kan $c$ niet al te groot zijn in verhouding tot $\text{rad}(abc)$:
voor elke $\epsilon > 0$ bestaat er een $K_\epsilon$ zodat

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

Versie voor $\mathbb{C}[X]$:

# ABC-vermoeden:

Als $a + b = c$, $a, b, c \in \mathbb{N}$, $\text{ggd}(a, b, c) = 1$, dan kan $c$ niet al te groot zijn in verhouding tot $\text{rad}(abc)$:
voor elke $\epsilon > 0$ bestaat er een $K_\epsilon$ zodat

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

Versie voor $\mathbb{C}[X]$:
Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

waar $N(fgh)$ het aantal nulpunten van $fgh$ is.

Uit ABC vermoeden volgt Fermat en nog meer van dat soort dingen ($x^l + y^m = z^n$). We zullen dat niet bewijzen, maar: we gaan het $ABC$ vermoeden voor polynomen bewijzen!!

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

$$f \qquad +g \qquad\qquad = h$$

**Bewijs:**

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

**Bewijs:**
$$\begin{array}{lll} f & +g & = h \\ f' & +g' & = h' \\ \hline \end{array}$$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

$$\begin{array}{lllll} & f & +g & = h & \text{maal } f' \\ \textbf{Bewijs:} & f' & +g' & = h' & \text{maal } f \\ \cline{2-5} \end{array}$$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

**Bewijs:**

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

$$\begin{array}{llllll} & & f\ f' & +g\ f' & = h\ f' & \text{maal } f' \\ \textbf{Bewijs:} & - & f'\ f & +g'\ f & = h'\ f & \text{maal } f \\ \hline \end{array}$$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

**Bewijs:**

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\text{ggd}(f, f')|f'g - fg'$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\text{ggd}(f, f')|f'g - fg'$

$\text{ggd}(g, g')|f'g - fg'$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\text{ggd}(f, f')|f'g - fg'$

$\text{ggd}(g, g')|f'g - fg'$

$\text{ggd}(h, h')|f'h - fh'$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\text{ggd}(f, f')|f'g - fg'$

$\text{ggd}(g, g')|f'g - fg'$

$\text{ggd}(h, h')|f'h - fh' = f'g - fg'$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\text{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\text{ggd}(f, f')|f'g - fg'$

$\text{ggd}(g, g')|f'g - fg'$

$\text{ggd}(h, h')|f'h - fh' = f'g - fg'$.

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\mathrm{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus $f'g - fg' = f'h - fh'$. Nu geldt: $\mathrm{ggd}(f, f')|f'g$ en $|fg'$. Dus

$\mathrm{ggd}(f, f')|f'g - fg'$

$\mathrm{ggd}(g, g')|f'g - fg'$

$\mathrm{ggd}(h, h')|f'h - fh' = f'g - fg'$.

Dus $\mathrm{ggd}(f, f')\mathrm{ggd}(g, g')\mathrm{ggd}(h, h')|f'g - fg'$.

Dus

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus

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

Alles naar rechts, en dan $+deg(h)$:

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:** Dus

$$deg(\text{ggd}(f, f')) + deg(\text{ggd}(g, g')) + deg(\text{ggd}(h, h')) \\ \leq deg(f) + deg(g) - 1.$$

Alles naar rechts, en dan $+deg(h)$:

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, ggd$(f, g, h) = 1$, dan

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

**Bewijs:**

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

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\mathrm{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\mathrm{ggd}(f, f')) + N(f)$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\text{ggd}(f, f')) + N(f)$.

**Bewijs:** Stel $(X - c)^n$ deelt $f$

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\text{ggd}(f, f')) + N(f)$.

**Bewijs:** Stel $(X - c)^n$ deelt $f = (X - c)^n \tilde{f}$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\text{ggd}(f, f')) + N(f)$.

**Bewijs:** Stel $(X - c)^n$ deelt $f = (X - c)^n \tilde{f}$. Dan $(X - c)^{n-1}$ deelt $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1} \tilde{f}$.

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\text{ggd}(f, f')) + N(f)$.

**Bewijs:** Stel $(X - c)^n$ deelt $f = (X - c)^n \tilde{f}$. Dan $(X - c)^{n-1}$ deelt $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1}\tilde{f}$. …(krijtbord?)

# Mason's Theorem:

Zij $f, g, h \in \mathbb{C}[X]$ met $f + g = h$, $\text{ggd}(f, g, h) = 1$, dan

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

**Bewijs:**

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

**Lemma:** $deg(f) \leq deg(\text{ggd}(f, f')) + N(f)$.

**Bewijs:** Stel $(X - c)^n$ deelt $f = (X - c)^n \tilde{f}$. Dan $(X - c)^{n-1}$ deelt $f' = (X - c)^n \tilde{f}' + n(X - c)^{n-1} \tilde{f}$. ...(krijtbord?)

Gebruik makend van het lemma volgt Mason's!

# Stelling:

Zij $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$. Als $F, G, H \in \mathbb{C}[X]$ met $\mathrm{ggd}(F, G, H) = 1$ en $F^p + G^q = H^r$ dan $F, G, H \in \mathbb{C}$.

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. D

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.
Dan Mason's:

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.
Dan Mason's:

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

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.
Dan Mason's:

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

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.
Dan Mason's:

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

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$q deg(G) \leq p deg(F)$,
$r deg(H) \leq p deg(F)$.
Dan Mason's:

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

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$q deg(G) \leq p deg(F)$,
$r deg(H) \leq p deg(F)$.
Dan Mason's:

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

Deel door $p deg(F)$:

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$qdeg(G) \leq pdeg(F)$,
$rdeg(H) \leq pdeg(F)$.
Dan Mason's:

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

Deel door $pdeg(F)$:
$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}$.

# Bewijs:

We mogen aannemen dat $deg(F^p) \geq deg(G^q), deg(H^r)$. Dus
$q deg(G) \leq p deg(F)$,
$r deg(H) \leq p deg(F)$.
Dan Mason's:

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

Deel door $p deg(F)$:
$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}$. Tegenspraak!

Merk op: $p = q = r$ geeft $\frac{1}{n} + \frac{1}{n} + \frac{1}{n} \leq 1$ dus $n \geq 3$.

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)
Hoezo kunnen we nou alles bewijzen voor $\mathbb{C}[X]$ en is het zo moeilijk voor $\mathbb{Z}$?

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)
Hoezo kunnen we nou alles bewijzen voor $\mathbb{C}[X]$ en is het zo moeilijk voor $\mathbb{Z}$?
Herinner je het bewijs...

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)
Hoezo kunnen we nou alles bewijzen voor $\mathbb{C}[X]$ en is het zo moeilijk voor $\mathbb{Z}$?

Herinner je het bewijs...

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

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)

Hoezo kunnen we nou alles bewijzen voor $\mathbb{C}[X]$ en is het zo moeilijk voor $\mathbb{Z}$?

Herinner je het bewijs...

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

Wat gaat hier niet als $f, g, h \in \mathbb{Z}$?

Het is nog erger: er is een variant van de Riemann hypothese die je kunt bewijzen voor polynomen! (Over $\mathbb{F}_p$)

Hoezo kunnen we nou alles bewijzen voor $\mathbb{C}[X]$ en is het zo moeilijk voor $\mathbb{Z}$?

Herinner je het bewijs...

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

Wat gaat hier niet als $f, g, h \in \mathbb{Z}$? Inderdaad! Op $\mathbb{C}[X]$ kun je afgeleiden nemen!

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met $\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1.

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de “priemen” $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

Dorie.

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

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

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

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

Ook: $\delta$ is *locaal nilpotent*. Dwz: voor elke $f$ bestaat er een $n$

met $\delta^n(f) = 0$.

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest:

gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

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

Ook: $\delta$ is *locaal nilpotent*. Dwz: voor elke $f$ bestaat er een $n$

met $\delta^n(f) = 0$.

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

$\mathbb{C}[X]$ heeft een *derivatie:* een afbeelding $\delta$ met

$\delta(fg) = f\delta(g) + g\delta(f)$ alle $f, g$. (Leibniz regel.)

Nou, dan maken we er toch eentje op $\mathbb{Z}$?

Na-apen van $\mathbb{C}[X]$: de "priemen" $(X - c)$ gaan naar 1.

Dus: op $\mathbb{Z}$: stuur $2, 3, 5, 7, 11, \ldots$ naar 1. En voor de rest: gebruik de Leibniz regel:

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

Leuk!! Kunnen we nu Fermat oplossen hiermee??

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

Ook: $\delta$ is *locaal nilpotent*. Dwz: voor elke $f$ bestaat er een $n$ met $\delta^n(f) = 0$.

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

$D(2^2 a) = 2^2 D(a) + 2 \cdot 2a = 2^2(D(a) + a)$ dus die gaat maar groter worden als $a > 1$ !

Een tipje van de sluier van mijn onderzoek...

Een tipje van de sluier van mijn onderzoek... $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$.

Een tipje van de sluier van mijn onderzoek... $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$. Willen deze verzameling beter begrijpen - bestaan er groepsacties van $\mathbb{C}, +$ op deze verzameling?

Een tipje van de sluier van mijn onderzoek... $V := \{(x, y, z) \in \mathbb{C}^3 \mid x^2 + y^3 + z^7 = 0\}$. Willen deze verzameling beter begrijpen - bestaan er groepsacties van $\mathbb{C}, +$ op deze verzameling?

Komt neer op het vinden van locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2+y^3+z^7=0$, dus $f^2+g^3+h^7=0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f,g,h)=1$, Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2 + y^3 + z^7 = 0$, dus $f^2 + g^3 + h^7 = 0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f, g, h) = 1$, en dan volgt uit Mason's dat $f, g, h \in \mathbb{K}$.

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2 + y^3 + z^7 = 0$, dus $f^2 + g^3 + h^7 = 0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f, g, h) = 1$, en dan volgt uit Mason's dat $f, g, h \in \mathbb{K}$. Maar $D$ is nul op elementen uit $\mathbb{K}$

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2 + y^3 + z^7 = 0$, dus $f^2 + g^3 + h^7 = 0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f, g, h) = 1$, en dan volgt uit Mason's dat $f, g, h \in \mathbb{K}$. Maar $D$ is nul op elementen uit $\mathbb{K}$ - dus $D(x) = D(y) = D(z) = 0$

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2 + y^3 + z^7 = 0$, dus $f^2 + g^3 + h^7 = 0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f, g, h) = 1$, en dan volgt uit Mason's dat $f, g, h \in \mathbb{K}$. Maar $D$ is nul op elementen uit $\mathbb{K}$ - dus $D(x) = D(y) = D(z) = 0$ en $D$ is nul op de hele ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^7)$ !

Locaal nilpotente derivaties $D$ op de ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$. Stel $D \neq 0$. Dan kan ik die derivatie $D$ voortzetten op iets groters - $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7) \subset \mathbb{K}[S]$ waar $K$ een of ander lichaam is. En op $\mathbb{K}[S]$ gedraagt $D$ zich als $\frac{\partial}{\partial S}$. Dus kan ik $x, y, z$ elk als elementen uit $\mathbb{K}[S]$ zien: $x = f(S), y = g(S), z = h(S)$. Maar zowiezo: $x^2+y^3+z^7=0$, dus $f^2+g^3+h^7=0$. Ik kan ook om een reden aannemen dat $\text{ggd}(f,g,h)=1$, en dan volgt uit Mason's dat $f,g,h \in \mathbb{K}$. Maar $D$ is nul op elementen uit $\mathbb{K}$ - dus $D(x)=D(y)=D(z)=0$ en $D$ is nul op de hele ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$ ! Tegenspraak, dus er zijn geen locaal nilpotente derivaties op $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^7)$ (behalve $D=0$).

# Conclusie

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$?

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$? (Of waarom kunnen we niks met $\mathbb{Z}$ en wel met $\mathbb{C}[X]$?)

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$? (Of waarom kunnen we niks met $\mathbb{Z}$ en wel met $\mathbb{C}[X]$?)
Er bestaat geen "afgeleide" op $\mathbb{Z}$ (of tenminste, geen lekkere...)

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$? (Of waarom kunnen we niks met $\mathbb{Z}$ en wel met $\mathbb{C}[X]$?)

Er bestaat geen "afgeleide" op $\mathbb{Z}$ (of tenminste, geen lekkere...)

**MORAAL VAN DIT VERHAAL:**

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$? (Of waarom kunnen we niks met $\mathbb{Z}$ en wel met $\mathbb{C}[X]$?)

Er bestaat geen "afgeleide" op $\mathbb{Z}$ (of tenminste, geen lekkere...)

**MORAAL VAN DIT VERHAAL:** Wees blij als je een Locaal Nilpotente Derivatie vindt op je ring...

# Conclusie

Waarom is $\mathbb{Z}$ moeilijker dan $\mathbb{C}[X]$? (Of waarom kunnen we niks met $\mathbb{Z}$ en wel met $\mathbb{C}[X]$?)

Er bestaat geen “afgeleide” op $\mathbb{Z}$ (of tenminste, geen lekkere. . . )

**MORAAL VAN DIT VERHAAL:** Wees blij als je een Locaal Nilpotente Derivatie vindt op je ring. . .

****** BEDANKT ******