Fermats formodning

Pytagoreiske tripler: $x^2+y^2=z^2$, $x,y,z\in\mathbb{N}$

Generalisering: $x^n+y^n=z^n$, $x,y,z\in\mathbb{N}$

Fermats formodning: Ingen løsninger for $n\geq 3$. Wiles 94.

Fermat viste dette for $n=4$.

Teorem: Det finnes ikke naturlige tall x,y,z slik at $x^4+y^4=z^4$.

$\Downarrow$ $u=z^2$

Skal vise noe litt sterkere:

Teorem: Det finnes ikke naturlige tall x,y,u slik at $x^4+y^4=u^2$

Bevis: Anta for motsigelse at det finnes tripler x,y,u slik at $x^4+y^4=u^2$, og la oss se på en slik løsning der u er minst mulig.

Påstand 1: x,y og u har ingen felles faktorer

Bevis for påstand 1: Anta at t er en felles primfaktor i x,y og u. Da er $x=ta$, $y=tb$, $u=tc$. Dermed er

$$(ta)^4+(tb)^4=(tc)^2$$

Forenkler.

$$t^2(a^4+b^4)=c^2$$ viser at $t\mid c$, dvs $c=td$

som gir $t^2(a^4+b^4)=t^2d^2 \Rightarrow a^4+b^4=d^2$ (med $d<u$). Umulig siden u er minimal.

Ligningen $(x^2)^2+(y^2)^2=u^2$ viser at (x^2,y^2,u) er et pytagoreisk trippel som er primitivt etter det vi nettopp viste.

Det finnes innbyrdes primiske p,q slik: $x^2=p^2-q^2$, $y^2=2pq$, $u=p^2+q^2$

Påstand 2: p er odde og q er like.

Bevis for påstand 2: Vi har $x^2=p^2-q^2 \pmod 4$

$$1=1-0$$

Setter $q=2c$: $y^2=4pc \Rightarrow \left(\frac{y}{2}\right)^2=pc$ (p,c innbyrdes primisk)

Dette medfører at p,c er kvadrater.

$$pc=\left(\frac{y}{2}\right)^2=p_1^2p_2^2\cdots p_r^2=\underbrace{(p_1p_2\cdots p_k)^2}_{\text{går opp i } p}\underbrace{(p_{k+1}\cdots p_r)^2}_{\text{går opp i } c}$$

Vi har altså $p=d^2$, $c=f^2$, dvs $q=2f^2$. Bruker: $x^2+q^2=p^2$

$$x^2+(2f^2)^2=(d^2)^2 \quad \text{Primitivt pytagoreisk trippel } (x,2f^2,d^2)$$

Det finnes derfor innbyrdes primiske l,m slik

$$x=l^2-m^2,\quad 2f^2=2lm,\quad d^2=l^2+m^2$$

l og m er kvadrater siden de er innbyrdes primiske og:

$$lm=f^2=q_1^2q_2^2\cdots q_s^2=\underbrace{(q_1q_2\cdots q_t)^2}_{l}\underbrace{(q_{t+1}\cdots q_s)^2}_{m}$$

Altså $l=r^2$ og $m=s^2$

$r^4+s^4=d^2$ (ny løsning av ligning) gjelder at $d<u$: $u=p^2+q^2>p^2\geq p=d^2\geq d$

$u>d$

Selvmotsigelse siden u var en minimal løsning av ligningen.

Algebraiske operasjoner

Har i bakhodet: For tall: $+, \cdot$
Vektorer: $+, \times$ ikke så mye $-, :$
Matriser: $+, \cdot$ avhengt operasjoner.
Mengder: $\cap, \cup$
generelle operasjoner

Observasjon: $a+b$, $+(a,b) = a+b$ → a, b → $+$ → $a+b$

Definisjon: Anta at Σ er en ikke-tom mengde. En **algebraisk operasjon** på Σ er en funksjon $*: \Sigma^2 \to \Sigma$. Vi skriver gjerne $a*b$ istedenfor $*(a,b)$.

Operasjoner som ikke gjerne inngår: **Prikkprodukt**: $\vec{u} \cdot \vec{v} \in \mathbb{R}$ ($\mathbb{R}^n$)

Multiplikasjon med skalar: $\alpha \vec{v} \in \mathbb{R}^n$ ($\mathbb{R}$, $\mathbb{R}^n$)

Definisjon: Vi sier at $*$ er **kommutativ** dersom
$a*b = b*a$ for alle $a, b \in \Sigma$

Eksempel: $+, \cdot$ i $\mathbb{R}$ er kommutativ.
kryssprodukt, matrisemultiplikasjon er ikke-kommutative

Definisjon: Vi sier at $*$ er **assosiativ** dersom
$(a*b)*c = a*(b*c)$
for alle $a, b, c \in \Sigma$

Kryssprodukt er ikke-assosiativ: $\vec{a} \times (\vec{b} \times \vec{c}) \neq (\vec{a} \times \vec{b}) \times \vec{c}$
$\vec{a} \times \vec{b} \times \vec{c}$ gir ikke mening.

Eksempel: $7x = 3 \mid \cdot \frac{1}{7}$

assosiativ: $\frac{1}{7}(7x) = \frac{1}{7} \cdot 3$

$(\frac{1}{7} \cdot 7)x = \frac{3}{7}$

$1 \cdot x = \frac{3}{7}$

$x = \frac{3}{7}$

Definisjon: e er et **nøytralt element** dersom
$x*e = e*x = x$ for alle $x \in \Sigma$

Eksempel: i $\mathbb{R}$ $+$: 0 er nøytralt element $x+0 = 0+x = x$
$\cdot$: 1 —"— $x \cdot 1 = 1 \cdot x = x$

Setning: Det finnes ikke mer enn ett nøytralt element for en operasjon $*$.
Bevis: Anta at e og e' er to nøytrale elementer for $*$.
$e = e*e' = e'$.
↑ Fordi e' er nøytral ↑ Fordi e er nøytral.

Definisjon: Anta at e er et nøytralt element og $x \in \Sigma$. Vi sier at $y \in \Sigma$ er en **invers til** x dersom
$x*y = y*x = e$

Eksempel: $\mathbb{R}$: $+$ invers element til x er $-x$: $x+(-x) = (-x)+x = 0$
$\cdot$ invers element til x er $\frac{1}{x}$: $x \cdot \frac{1}{x} = \frac{1}{x} x = 1$
$x \neq 0$.

Setning: Anta at $*$ er assosiativ. Da har et element høyst en invers.
Bevis: Anta at y og z er inverser til x. Skal vise at $y = z$.

$y = y*e = y*(x*z) = (y*x)*z = e*z = z$
↑ Fordi e er nøytral ↑ assosiativitet ↑ Fordi y er invers

Definisjon: Hvis x har en invers y, skriver vi $y = x^{-1}$ (hvis operasjonen heter $+$, skriver vi gjerne $-x$ istedenfor)
For $*$ assosiativ
Setning: Hvis x og y er invertibare (dvs. har inverser), så er $x*y$ også invertibar og
$(x*y)^{-1} = y^{-1} * x^{-1}$

Bevis: Vi viser at $(x*y)*(y^{-1}*x^{-1}) = e$
$(y^{-1}*x^{-1})*(x*y) = e$

Skal du finne: $(x*y)*(y^{-1}*x^{-1}) = ((x*y)*y^{-1})*x^{-1}$
$a*(b*c)$ $= (x*(y*y^{-1}))*x^{-1}$
$= (x*e)*x^{-1}$
$= x*x^{-1} = e$

Anta at vi har to operasjoner på Σ: $*, +$.
Vi sier at $*$ er **distributiv** over $+$ dersom
$x*(y+z) = x*y + x*z$
$(y+z)*x = y*x + z*x$

I tilfellene $\cdot$ er distributiv over $+$, viser det seg at
$x(y+z) = xy + xz$.
(men ikke $x+(y+z) = (x+y)\cdot(x+z)$!)

Med $\cap$ og $\cup$ gjelder de distributive lover vi har sett.

Strukturer:
- **Grupper**: En operasjon $*$ (som regel ikke-kommutativ)
- **Ringer**: To operasjoner $+, \cdot$ (ringen multiplikativt invers, $\mathbb{Z}$, $\mathbb{Z}/(6)$)
- **Kropper**: Ringer med multiplikativt inverser. (Karakteristikk forskjellig fra 0)
$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(p)$