En sætning om primtal som en sum af to kvadrater

Frederik Møllerstrøm Lauridsen

Der kan være mange forskellige måder at bevise en sætning på og visse heldige sætninger er da også netop blevet bevist på et utal af forskellige måder. En af disse sætninger er sætningen om muligheden for at skrive et primtal som summen af to kvadrater. Denne sætning har være kendt siden Fermat, som muligvis også har haft et bevis for den. Senere har eksempelvis Euler fundet et bevis og Hardy & Wright giver hele fem forskellige beviser for sætningen. Måske mest berømt er Zagiers bevis [3] der kun fylder en *linie*. Nedenfor følger et elegant og bemærkelsværdigt bevis for en tilstrækkelig betingelse for at et primtal p kan skrives som summen af to kvadrater[2]. Beviset tager udgangspunkt i Heath-Browns bevis fra 1984 som fremstillet i [1] og [2].

Sætning 1 *Lad p være et primtal som opfylder at $p \equiv 1 \pmod 4$. Da findes $x, y \in \mathbb{N}$ sådan at $p = x^2 + y^2$.*

Bevis. Lad p være et primtal som opfylder at $p \equiv 1 \pmod 4$ d.v.s $p = 4k + 1$ for et $k \in \mathbb{N}$, og betragt følgende tre endelige ikke-tomme mængder:

$$S = \{(x, y, z) \in \mathbb{Z}^3 \colon 4xy + z^2 = p, x > 0, y > 0\},$$

$$T = \{(x, y, z) \in S \colon z > 0\}, \quad U = \{(x, y, z) \in S \colon x - y + z > 0\}$$

samt de tre lineære afbildninger, $f_A \colon S \to S, f_B \colon T \to T$ og $f_C \colon U \to U$ givet ved matricerne

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}.$$

[2]Det er let at vise at betingelsen ligeledes er nødvendig når $p \neq 2$.

Det overlades som en let øvelse til læseren at tjekke at disse afbildninger er veldefinerede.

Det bemærkes først at $A^2 = B^2 = C^2 = E$, hvor E som sædvanlig betegner enhedsmatricen, og at afbildningerne dermed alle er involutioner[3]. Videre ses det let at

$$f_A(T) = \{(x, y, z) \in S \colon z < 0\} \quad \text{og}$$
$$f_A(U) = \{(x, y, z) \in S \colon x - y + z < 0\}$$

samt at disse opfylder at $S = T \cup f_A(T)$ da punkter af formen $(x, y, 0)$ ikke kan være elementer i S, eftersom fire ikke går op i p, og at $S = U \cup f_A(U)$ eftersom $x - y + z = 0$ giver at

$$p = 4xy + z^2 = 4xy + (y - x)^2 = (x + y)^2$$

hvilket ikke er muligt da p er et primtal.

Da videre $f_A \colon S \to S$ er en involution, og således specielt en bijektion, må vi have at $|T| = |f_A(T)|$ og $|U| = |f_A(U)|$. Vi kan således slutte at $2|T| = |S| = 2|U|$, da $T \cap f_A(T) = U \cap f_A(U) = \emptyset$, og dermed er $|T| = |U|$.

Vi bemærker nu at punktet $(k, 1, 1)$ er et fikspunkt for funktionen $f_C \colon U \to U$ samt at dette er det eneste sådanne fikspunkt eftersom

$$(x, y, z) = f_C((x, y, z)) = (x - y + z, y, 2y - z) \Rightarrow y = z$$

men da er $p = 4xy + y^2 = (4x + y)y$ og eftersom p er et primtal kan vi slutte at $y = z = 1$ og dermed at $x = k$.

Eftersom $f_C \colon U \to U$ er en involution på U med netop et fikspunkt, følger det nu at kardinaliteten af U er ulige, og dermed

[3]En involution er en funktion som er sin egen invers.

at kardinaliteten af T ligeledes er ulige. Heraf følger at enhver involution på T må have mindst et fikspunkt (og altid et ulige antal), specielt må $f_B\colon T \to T$ have et fikspunkt. Altså et punkt $(t_0, t_1, t_2) \in T$ som opfylder at

$$(t_0, t_1, t_2) = f_B((t_0, t_1, t_2)) = (t_1, t_0, t_2)$$

d.v.s at $t_0 = t_1$, og da nu $(t_0, t_1, t_2) \in T$ kan vi slutte at

$$p = 4t_0t_1 + {t_2}^2 = (2t_1)^2 + {t_2}^2,$$

hvilket var hvad vi ønskede at vise. □

Litteratur

[1] M. Aigner og C.M. Ziegler: *Proofs from the book.* 2. udg Springer 2001

[2] C. Elsholtz: *Kombinatorische Beweise des Zweiquadratesatzes und Verallgemeinerungen* i Mathematische Semesterberichte 50, Heft 1, p.77-93, 2003.

[3] D. Zagier: *A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares* i The American Mathematical Monthly Vol. 97, No. 2 (Feb., 1990), p. 144.