Den almindelige, den gode og den smarte

Tre beviser for at ethvert primtal $p \equiv 1 \pmod 4$ er en sum af to kvadrater

Pia Mikkelsen

De fleste af os har i løbet af vores karriere som matematikstuderende stiftet bekendtskab med ovenstående kendte sætning. F.eks. i forbindelse med nærmere granskning af Anders Thorups 2 AL noter [1].
Sætningen går tilbage til Fermat. -Fermat opskriver sætningen, men giver ikke noget bevis for sin påstand.
Der er dog senere blevet givet en lang række beviser for denne sætning (bl.a. af Euler, Lagrange og Dedekind), og vi skal her se nærmere på tre forskellige indgangsvinkler.

Den almindelige

De fleste af os har nok før set et bevis baseret på teorien om kvadratiske talringe (se f.eks. RNG.6 [1]). -Mere præcist betragtes *Gauss' talring*

$$\mathbb{Z}[i] = \{x + yi \mid x,\ y \in \mathbb{Z}\}.$$

Elementerne i $\mathbb{Z}[i]$ kaldes *gaussiske heltal.*
Ved $\overline{\cdot}$ menes kompleks konjugering og vi minder kort om, at *normen* $N : \mathbb{Z}[i] \to \mathbb{Z}$,

$$x + yi \longmapsto (x + yi)\,\overline{(x + yi)} = x^2 + y^2,$$

er multiplikativ. Det er desuden nemt at overbevise sig om, at der for et element $\alpha \in \mathbb{Z}[i]$ gælder:

$$N(\alpha) = 1 \quad \Leftrightarrow \quad \alpha \text{ er en enhed i } \mathbb{Z}[i].$$

(Se evt. s.211 [1]).
Hvis p er reducibel i $\mathbb{Z}[i]$ -d.v.s. hvis der findes en opløsning

$$p = \alpha\beta, \quad \alpha,\ \beta \in \mathbb{Z}[i],$$

hvor α, β ikke er enheder i $\mathbb{Z}[i]$, må

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Da α og β ikke er enheder, er $N(\alpha)$, $N(\beta)$ positive heltal forskellig fra 1, så $N(\alpha) = p$. I.e. hvis $\alpha = x + yi$, er

$$p = N(\alpha) = x^2 + y^2.$$

Hvis vi kan vise, at p er et reducibelt element i $\mathbb{Z}[i]$, har vi altså vores ønskede sætning. Da $\mathbb{Z}[i]$ er et PID (se s.217 [1]), er de irreducible elementer netop primelementerne, så det er nok at vise, at p ikke er et primelement i $\mathbb{Z}[i]$, i.e. vi søger α, $\beta \in \mathbb{Z}[i]$ for hvilket der gælder, at p går op i $\alpha\beta$, men p går hverken op i α eller β. Til dette benyttes følgende sætning også kendt som "Første supplement til den kvadratiske reciprocitetssætning":

Sætning 1. *Lad p være et primtal og antag $p \equiv 1 \pmod 4$. Da findes et heltal n, så*

$$p \mid n^2 + 1.$$

Bevis. Iflg. Fermat's lille Sætning (se GRP. 4, s. 82 [1]) gælder der for ethvert heltal z primisk med p, at

$$z^{p-1} - 1 \equiv 0 \pmod p.$$

Da $p \equiv 1 \pmod 4$, skrives $p-1 = 4k$. For ethvert heltal z primisk med p , gælder således, at

$$p | z^{4k} - 1 = \left(z^{2k} + 1\right)\left(z^{2k} - 1\right).$$

Da p er et primtal, må p gå op i $z^{2k} + 1$ eller $z^{2k} - 1$. I.e.

$$z^{2k} + 1 \equiv 0 \pmod p \quad \text{eller} \quad z^{2k} - 1 \equiv 0 \pmod p.$$

Tallene $z = 1, \ldots, p - 1 = 4k$ er alle primiske med p og altså løsninger til en af ovenstående kongruenser. Da $\mathbb{Z}_p$ er et legeme og altså specielt et integritetsområde, har polynomiet

$$z^{2k} - 1 \in \mathbb{Z}_p[z]$$

højst $2k$ rødder (se POL 3, s.236 [1]). Derfor findes et heltal z blandt tallene $1, \ldots, 4k$, så $z^{2k} + 1 \equiv 0 \pmod p$. Sættes $n = z^k$ fås det ønskede. □

Der findes altså et n, så

$$p \mid n^2 + 1 = (n + i)(n - i).$$

Da $\frac{n}{p} \pm \frac{1}{p} i \notin \mathbb{Z}[i]$, går p hverken op i $n + i$ eller $n - i$ og p er således ikke et primelement i $\mathbb{Z}[i]$.

Den gode[2]

Denne udgave af vores bevis bygger på følgende sætning:

Thues sætning. Lad $n > 1$ være et naturligt tal og lad k være det mindste heltal, således $k > \sqrt{n}$. -D.v.s. $k - 1 \leq \sqrt{n} < k$. For ethvert heltal a primisk med n findes $x,\ y \in \mathbb{N}$, så $x,\ y \leq k - 1$ og

$$ay \equiv \pm x \pmod{n}.$$

Bevis. Betragt tal på formen

$$ay + x, \quad x,\ y \in \{0, 1, \ldots, k-1\}.$$

Da der findes $k^2 > n$ sådanne tal og kun n restklasser modulo n, må mindst to af tallene ligge i samme restklasse (Skuffeprincippet). Der findes altså $x_1, y_1, x_2, y_2 \in \{0, 1, \ldots, k-1\}$, hvor

$$x_1 - x_2 \neq 0 \quad \text{eller} \quad y_1 - y_2 \neq 0$$

og

$$a\,(y_1 - y_2) \equiv x_2 - x_1 \pmod{n}\,.$$

Desuden må der gælde, at

$$0 < |x_2 - x_1|,\ |y_1 - y_2| \leq k - 1.$$

Antag nemlig $x_2 - x_1 = 0$. Så går n op i $a(y_1 - y_2)$. Da a og n er primiske vil n gå op i $y_1 - y_2$, hvorfor $y_1 - y_2 = 0$. Ligeledes giver $y_1 - y_2 = 0$, at $x_2 - x_1 = 0$. Vi kan antage, at $y_1 > y_2$. Sættes

$$y = y_1 - y_2 \quad \text{og} \quad x = \begin{cases} x_2 - x_1 & \text{hvis } x_2 > x_1 \\ x_1 - x_2 & \text{hvis } x_1 > x_2 \end{cases}$$

fås den ønskede kongruens. □

Vi så i foregående bevis, at hvis $p \equiv 1 \pmod 4$, har kongruensen

$$z^2 + 1 \equiv 0 \pmod{p} \tag{1}$$

en løsning. Da en sådan løsning z er primisk med p findes, iflg. Thues Sætning, $x,\ y \in \mathbb{N}$, så

$$yz \equiv \pm x \pmod{p}$$

og $x,\ y < \sqrt{p}$. Af kongruensen (1) haves så, at

$$y^2z^2 + y^2 \equiv 0 \pmod{p},$$

hvorfor

$$x^2 + y^2 \equiv 0 \pmod{p}.$$

Men da $x^2 + y^2 < 2p$, må $x^2 + y^2 = p$.

Den smarte[3]

En afbildning $\sigma : S \to S$ kaldes en involution (eller involutorisk), hvis den er selvinvers, i.e. hvis $\sigma^2 = \mathrm{Id}_S$. For en involution σ givet på en endelig mængde S haves, at

Lemma 2.

$$|S| \text{ er ulige } \Leftrightarrow \sigma \text{ har et ulige antal fixpunkter .}$$

Specielt må en involution, givet på en mængde med et ulige antal elementer, have mindst ét fixpunkt.

Bevis. Ved

$$(x,y,z) \sim (x',y',z') \overset{\text{def}}{\Leftrightarrow} (x,y,z) = (x',y',z') \vee \sigma(x,y,z) = (x',y',z')$$

defineres en ækvivalensrelation på S. Ækvivalensklasserne indeholder præcist et element, hvis dette er et fixpunkt, og ellers 2. Da ækvivalensklasserne udgør en klassedeling på S, kan elementantallet $|S|$ findes som summen af elementantallet i hver ækvivalensklasse. Involutionen σ har altså et ulige antal fixpunkter netop hvis $|S|$ er ulige. □

Betragt nu den endelige mængde

$$S := \{(x,y,z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

Det er klart, at $S \neq \emptyset$, da $(1,1,k) \in S$, $p = 4k+1$. Betragt desuden afbildningen $\sigma : S \to S$:

$$\sigma : (x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{hvis } x < y-z \\ (2y-x, y, x-y+z) & \text{hvis } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{hvis } x > 2y \end{cases} .$$

Et punkt $(x,y,z) \in \mathbb{N}^3$, hvor $x = y-z$ eller $x = 2y$, ligger ikke i S, da p er et primtal. Derfor er σ defineret på hele S. Ved udregning ses desuden let, at σ faktisk afbildeder ind i S. Vores afbildning σ er således veldefineret.
Faktisk er σ involutorisk og har netop ét fixpunkt. Betragt nemlig de tre tilfælde

- Hvis $x < y - z$:

  Da $x + 2z > 2z$, er

$$\begin{aligned} \sigma^2(x,y,z) &= \sigma(x+2z, z, y-x-z) \\ &= ((x+2z)-2z, (x+2z)-z+(y-x-z), z) \\ &= (x,y,z). \end{aligned}$$

- Hvis $y - z < x < 2y$:

  Da $y - (x - y + z) < 2y - x < 2y$ er

$$\begin{aligned}\sigma^2(x,y,z) &= \sigma(2y - x, y, x - y + z)\\ &= (2y - (2y - x), y, (2y - x) - y + (x - y + z))\\ &= (x, y, z).\end{aligned}$$

- Hvis $x > 2y$:

  Da $x - 2y < (x - y + z) - y$ er

$$\begin{aligned}\sigma^2(x,y,z) &= \sigma(x - 2y, x - y + z, y)\\ &= ((x - 2y) + 2y, y, (x - y + z) - (x - 2y) - y)\\ &= (x, y, z).\end{aligned}$$

I.e. $\sigma^2 = \mathrm{Id}_S$.
Det er umiddelbart, at der for et eventuelt fixpunkt $(x, y, z) \in S$, må gælde, at $y - z < x < 2y$ og i så fald er $x = y$. De mulige fixpunkter i S har altså formen (x, x, z) og opfylder

$$x^2 + 4xz = x(x + 4z) = p.$$

Da p er et primtal, må $x = 1$ og $z = k$, hvor $p = 4k + 1$. Afbildningen σ har altså netop ét fixpunkt - nemlig $(1, 1, k)$.
Iflg. vores Lemma er $|S|$ ulige og involutionen

$$(x, y, z) \mapsto (x, z, y)$$

har ligeledes et fixpunkt i S. For dette må gælde, at $y = z$ og altså er $x^2 + (2y)^2 = p$.

Det følger umiddelbart af vores sætning, at ethvert heltal, der er et produkt af primtal $\equiv 1 \pmod 4$, kan skrives som en sum af to kvadrater, idet

$$(x^2 + y^2)(a^2 + b^2) = (xa + yb)^2 + (xb - ya)^2.$$

Ingen af vores beviser ovenfor er konstruktive, men der findes faktisk konstruktive beviser. Et sådant bevis findes bl.a. i [4], som bygger på teorien om kvadratiske rester.

Man kan desuden spørge sig selv om opskrivning af primtal $\equiv 1 \pmod 4$ som en sum af to kvadrater er entydig? Svaret er ja til og med ombytning og fortegn. Dette kan vises på flere måder. F.eks. følger det af entydig primfaktorisering i $\mathbb{Z}[i]$. Ellers antag, at $p = x^2 + y^2 = a^2 + b^2$. Da der som før nævnt findes heltal z, så $z^2 \equiv -1 \pmod p$, sluttes

$$\begin{aligned}x^2 &\equiv -y^2 \equiv z^2 y^2 \pmod p\\ a^2 &\equiv -b^2 \equiv z^2 b^2 \pmod p.\end{aligned}$$

Da er

$$\begin{aligned} x &\equiv \pm zy \pmod{p} \\ a &\equiv \pm z \pmod{p} \end{aligned}$$

og ved eventuelt at erstatte y med $-y$ eller b med $-b$, kan vi antage, at

$$\begin{aligned} x &\equiv zy \pmod{p} \\ a &\equiv zb \pmod{p}. \end{aligned}$$

Altså må

$$xa \equiv z^2 yb \equiv -yb \pmod{p}.$$

Da

$$p^2 = (x^2 + y^2)(a^2 + b^2) = (xa + yb)^2 + (xb - ya)^2$$

og p går op i $xa + yb$, er p^2 her skrevet som en sum af to hele ikke-negative tal begge delelig med p^2. Derfor må et af disse tal være nul.
Hvis $xa = -yb$, går x op i b, da x og y er primiske. Tilsvarende sluttes, at b går op i x. I.e. $x = \pm b$, hvorfor $x^2 = b^2$ og $y^2 = a^2$. Hvis $xb - ya = 0$ fås tilsvarende, at $x^2 = a^2$ og $y^2 = b^2$ [4].

[1] A. Thorup, Matematik 2AL, Algebra, 2.udg., 2.oplag, Matematisk Afdeling, Københavns Universitet, 1998.

[2] T. Nagell, Introduction To Number Theory, Kapitel VI, s. 122-123, 188-189, John Wiley & Sons, Inc., New York, 1951.

[3] D. Zagier, A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares, American Mathematical Monthly, s.144, Bind 97, 1990. [4] C.U.Jensen, Matematik 3AL, Klassisk Algebra, HCØ Tryk, 2000.