Summer av to kvadrat

Marius Overholt

Institutt for Matematikk
Universitetet i Tromsø
9037 Tromsø
marius.overholt@uit.no

En sum av to kvadrat er et positivt heltall b som kan skrives på form $b = k^2 + m^2$ hvor k og m er (ikke nødvendigvis positive) heltall. De første få av disse tallene er $1 = 0^2 + 1^2, 2 = 1^2 + 1^2, 4 = 0^2 + 2^2, 5 = 1^2 + 2^2, 8 = 2^2 + 2^2, 9 = 0^2 + 3^2, 10 = 1^2 + 3^2, 13 = 2^2 + 3^2$. Umiddelbart fremtrer ikke noe klart mønster, men i 1625 publiserte den franske ingeniøren og matematikeren Albert Girard en beskrivelse som er ekvivalent med følgende: Et tall er sum av to kvadrat hvis og bare hvis det er produkt av potenser av tallene 2, primtall $p \equiv 1 \pmod 4$ og kvadrater p^2 av primtall $p \equiv 3 \pmod 4$.

Girard har neppe hatt noe fullstendig bevis for sin karakterisering, men har sikkert brukt polynomidentiteten

$$(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2$$

som ble oppdaget av den indiske matematikeren Brahmagupta i det syvende århundre. Fibonacci gjorde den kjent i Europa et halvt millennium senere. Ved hjelp av komplekse tall $z = x + iy$ og $w = u + iv$ skrives den mer kompakt som $|z|^2|w|^2 = |zw|^2$. Identiteten gjør det klart at et produkt av summer av to kvadrat selv er sum av to kvadrat, og på grunnlag av dette og noe regning fremtrer Girards beskrivelse som sannsynlig.

Etter dagens målestokk er bare ett genuint vanskelig resultat nødvendig for å bevise den multiplikative karakteriseringen av summer av to kvadrat. Det er den sats at ethvert primtall $p \equiv 1 \pmod 4$ er sum av to kvadrat. Dette resultatet forekommer uten bevis i et brev fra Pierre de Fermat til Marin Mersenne datert første juledag 1640, og derfor kalles satsen av og til på engelsk for *Fermat's Christmas Theorem.* Dette regnes ofte som det første dype resultatet i tallteorien.

Pierre de Fermat var juridisk embedsmann i Toulouse og den største av alle amatørmatematikere. Han gjorde viktige oppdagelser i kalkulus, optikk og sannsynlighetsteori, og fremfor alt var han en av de betydeligste tallteoretikere som har levet. Marin Mersenne var en munk i Paris med vitenskapelige interesser. Han brevvekslet med mange av de viktigste vitenskapsmennene i sin samtid, og holdt sin krets av korrespondenter orientert om nye framskritt i en tid da det ikke fantes vitenskapelige journaler.

Hvorfor er det rimelig å anta at Fermat hadde et bevis for sin sats, selv om han aldri publiserte det? Fermat publiserte stort sett ikke beviser, og mye av hva vi vet

om hans forskning i tallteori har vi fra marginalia i hans eksemplar av Diofantus' *Arithmetica*, publisert av hans sønn etter hans død. Men ett viktig bevis skrev han ut i detalj, for at likningen

$$x^4 + y^4 = z^2$$

ikke har løsninger i heltall med $xyz \neq 0$. Metoden han brukte var hans egen oppdagelse, og meget krevende. Den kalles *uendelig nedstigning* og er fremdeles svært viktig i tallteorien.

Vi illustrerer uendelig nedstigning på et enkelt problem: Å bevise at hvis a er et ikke-negativt og b et positivt heltall så finnes ikke-negative heltall q og r med $a = qb + r$ og $0 \leq r < b$. Dette er et grunnleggende resultat i elementær tallteori og kalles *divisjon med rest.* La A_b betegne de positive heltall a slik at divisjon av a på b med rest svikter. Vårt mål er å vise at A_b er den tomme mengde. Anta at $a \in A_b$; da må $a \geq b$ for ellers er $a = 0 \cdot b + a$ med $0 \leq a < b$. Hvis $a - b = qb + r$ med $0 \leq r < b$ så er $a = (q+1)b + r$. Derfor vil $a \in A_b$ implisere at $a - b \in A_b$, som strider mot at A_b består av ikke-negative heltall, hvis A_b er ikketom. Altså er A_b tom og divisjon med rest er gyldig. Åpenbart er uendelig nedstigning en variant av matematisk induksjon. Vår illustrasjon av metoden var et lett tilfelle, men Fermat anvendte den på problemer hvor konstruksjonen av en mindre løsning fra en antatt løsning var meget vanskeligere. I slike tilfelle gjennomføres konstruksjonen ved en blanding av algebra og tallteori, og kan kreve stor skarpsindighet.

I et brev har Fermat meddelt at han beviste resultatet om primtall som summer av to kvadrat ved uendelig nedstigning. Leonard Euler lyktes etter hardt arbeid å finne et bevis for satsen nesten ett århundre etter Fermats død. Beviset bygger på uendelig nedstigning! Det er grunn til å tro at mange av de vanskelige resultatene om likninger i heltall som Fermat annonserte, hadde han bevist ved uendelig nedstigning. Blant annet framsatte han som oppgave å bevise at likningen

$$x^3 + y^3 = z^3$$

ikke har løsninger i heltall med $xyz \neq 0$. Dette er vanskeligere enn de to andre av hans resultater nevnt over; det første beviset ble offentliggjort av Euler og var også basert på uendelig nedstigning.

Alle kjente bevis for Fermats sats om summer av to kvadrat bygger enten på et meget skarpsindig resonnement, eller så gjør de bruk av resultat fra en mer omfattende teori. Flere dusin bevis er publisert siden Euler fant det første i 1749; her skal vi gjengi et slående bevis som ble oppdaget av den britiske tallteoretikeren David Rodney Heath-Brown i nyere tid.

Sats 1. *Ethvert primtall p kongruent til 1 modulo 4 er sum av to kvadrat.*

Bevis. En *involusjon* på en ikketom mengde A er en bijektiv funksjon $\sigma : A \to A$ med den egenskap at for hver $a \in A$ så medfører $\sigma(a) = b$ at $\sigma(b) = a$. Hvis $b = a$ så kalles a for et *fikspunkt* til σ.

Involusjonen $(x, y, z) \overset{f}{\mapsto} (-x, z, y)$ på den endelige mengden

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

har intet fikspunkt siden $x = 0$ er umulig. Spesielt gjelder $f(T) = S \setminus T$ hvor

$$T = \{\, (x, y, z) \in S \,|\, x > 0 \,\}.$$

Videre er $f(U) = S \setminus U$ hvor

$$U = \{\, (x, y, z) \in S \mid x - y + z > 0 \,\}.$$

For det finnes ingen elementer i S med $x - y + z = 0$ siden dette ville medføre at $p = x^2 + 4yz = (y - z)^2 + 4yz = (y + z)^2$. Men f er en bijeksjon så

$$f(T \setminus U) = f(T) \setminus f(U) = (S \setminus T) \setminus (S \setminus U) = U \setminus T$$

viser at $T \setminus U$ og $U \setminus T$ har det samme antall elementer. Siden $T = (T \setminus U) \cup (T \cap U)$ og $U = (U \setminus T) \cup (T \cap U)$ følger at T og U har det samme antall elementer.

Avbildningen $(x, y, z) \mapsto (2y - x, y, x - y + z)$ er en involusjon på U, siden $(2y - x)^2 + 4y(x - y + z) = 4y^2 - 4xy + x^2 + 4xy - 4y^2 + 4yz = x^2 + 4yz = p$. Betingelsen for at (x, y, z) skal være et fikspunkt til denne involusjonen er at $x = y$. Det medfører at $x^2 + 4xz = p$, og siden p er primtall, er $x = \pm 1, \pm p$ de eneste mulighetene. Men $x = \pm p$ er umulig fordi $x^2 + 4yz = p$ med $y > 0$ og $z > 0$. Hvis $x = -1$ så er $y = -1$ og $z = (1 - p)/4$, som strider mot betingelsen $x - y + z > 0$. Vi står igjen med $(x, y, z) = (1, 1, (p-1)/4)$, som er et fikspunkt fordi $(p - 1)/4$ er heltall. Så involusjonen har nøyaktig ett fikspunkt, og da må antall elementer i U være oddetall, dermed er antall elementer i T også oddetall.

Avbildningen $(x, y, z) \mapsto (x, z, y)$ er en involusjon på T. Siden antall elementer i T er oddetall har denne involusjonen et odde antall fikspunkt, dermed minst ett, så det finnes et element $(x, y, z) \in T$ med $y = z$. Men da er $p = x^2 + 4yz = x^2 + (2z)^2$ så p er sum av to kvadrat. □

Ovenstående kombinatoriske bevis er ganske kort sett i lys av at det ikke bygger på noen mer omfattende teori. Enda kortere beviser krever mer teoretisk bakgrunn.

Noen heltall har ingen representasjon som sum av to kvadrat; det gjelder alle som er kongruente til 3 modulo 4 og i tillegg mange andre. Noen har bare få representasjoner, som for eksempel 5, som har den ene representasjonen $5 = 1^2 + 2^2$, eller åtte representasjoner hvis vi teller alle varianter med forskjellige valg av fortegn og rekkefølge til k og m i $5 = k^2 + m^2$. Men det viser seg også at noen heltall, som for eksempel produkter av mange små primtall kongruente til 1 modulo 4, har mange representasjoner. Definerer vi $r(n)$ som antall representasjoner til n som sum av to kvadrat, med fortegn og rekkefølge tatt hensyn til, så er for eksempel $r(3) = 0$ og $r(5) = 8$. Overraskende nok finnes en formel

$$r(n) = 4 \left(\sum_{\substack{d \mid n \\ d \equiv 1 \bmod 4}} 1 \right) - 4 \left(\sum_{\substack{d \mid n \\ d \equiv 3 \bmod 4}} 1 \right)$$

for antall representasjoner. Den ble oppdaget av Carl Gustav Jakob Jakobi i 1829 ved hjelp av teorien for elliptiske funksjoner. Det er en tidlig anvendelse av analyse i tallteorien. Jakobis formel kan utformes som en regel: For å finne antall representasjoner til et heltall som sum av to kvadrat, tell opp antall divisorer til heltallet som er kongruente til 1 modulo 4, trekk fra antall divisorer som er kongruente til 3 modulo 4, og multipliser med 4. Jakobis regel var foregrepet av en annen regel for

$r(n)$ som Carl Friedrich Gauss utledet fra teorien for binære kvadratiske former og nevnte i en fotnote i artikkel 182 i *Disquisitiones Arithmeticae.*

Jakobis bevis for hans formel bygger ikke på noen tallteoretiske forutsetninger i det hele tatt; siden den viser at $r(p) = 8$ hvis $p \equiv 1 \pmod 4$ er primtall så leverer formelen et nytt bevis for Fermats resultat. Men den viser mer, for eksempel at opp til fortegn og rekkefølge til k og m i $p = k^2 + m^2$ så har primtall $p \equiv 1 \pmod 4$ nøyaktig én representasjon som sum av to kvadrat. En lagniappe til formelen er at ingen heltall kan ha flere divisorer kongruente til 3 modulo 4 enn til 1 modulo 4. For antall representasjoner kan jo aldri bli negativt!

De uløste problemene som knytter seg til summer av to kvadrat vedrører deres fordeling blant de positive heltallene. Slike spørsmål kan formuleres med eller uten hensyntagen til antall representasjoner. For eksempel teller summen

$$R(x) = \sum_{n \le x} r(n)$$

det totale antall representasjoner som summer av to kvadrat til de positive heltallene $n \le x$. I denne summen veier heltallene med mange representasjoner tyngre enn de andre. Summen

$$B(x) = \sum_{b \le x} 1$$

teller antall positive heltall $n \le x$ som er sum av to kvadrat, uten å ta hensyn til hvor mange representasjoner de har. (Bokstaven b betegner en sum av to kvadrat ved konvensjon.)

Siden vi har Jakobis formel for $r(n)$ til rådighet, skulle vi kunne oppskatte $R(x)$ ved innsetting. Men et geometrisk resonnement fra Gauss' etterlatte papirer fører lettere til målet. Vi observerer at $n = k^2 + m^2$ utsier at avstanden fra origo til punktet (k, m) er $\sqrt{n}$. Et punkt i planet med heltallskoordinater kalles et *gitterpunkt.*

Sats 2. *Ulikheten*

$$|R(x) - \pi x| \le 6\sqrt{x}$$

gjelder for alle $x \ge 1$.

Bevis. Summen er lik det totale antall representasjoner $1 \le k^2 + m^2 = n \le x$ med $(k, m) \in \mathbb{Z}^2$. Så den er lik antall gitterpunkter som ligger på eller innenfor sirkelen $u^2 + v^2 = x$, minus ett fordi origo ikke telles med. Unionen av de akseparallelle lukkede kvadratene med sentre i disse gitterpunktene og sidelengde lik 1 er inneholdt i den lukkede sirkeldisken om origo med radius $\sqrt{x} + \sqrt{2}/2$ og inneholder den lukkede sirkeldisken om origo med radius $\sqrt{x} - \sqrt{2}/2$, siden disse kvadratene har diameter $\sqrt{2}$. Da er

$$\pi\left(\sqrt{x} - \frac{\sqrt{2}}{2}\right)^2 \le 1 + \sum_{n \le x} r(n) \le \pi\left(\sqrt{x} + \frac{\sqrt{2}}{2}\right)^2$$

ved arealsammenlikning, siden kvadratene har areal lik 1. Ulikheten følger fordi $\pi\sqrt{2} + \pi/2 - 1 \le 6$. □

Siden

$$\left| \frac{1}{x} \sum_{n \le x} r(n) - \pi \right| \le \frac{6}{\sqrt{x}}$$

impliserer Gauss' resultat at det gjennomsnittlige antall representasjoner som sum av to kvadrat til de positive heltallene $n \le x$ går mot π når $x \to +\infty$. Spørsmålet om hvor liten vi kan velge θ slik at en ulikhet

$$|R(x) - \pi x| \le C_\epsilon \, x^{\theta+\epsilon}$$

holder for hver $\epsilon > 0$ kalles *Gauss' sirkelproblem.* Etter Gauss vet vi at $\theta = 1/2$ er mulig her, men i 1914 beviste Godfrey Harold Hardy at $\theta \ge 1/4$. Den beste verdien er enda ikke kjent; Wacław Sierpiński viste i 1904 at $\theta = 1/3$ er mulig, og i 2000 oppnådde Martin Neil Huxley $\theta = 131/416$ som den siste av en lang rekke forbedringer. Elementære bevis for eksponenten $\theta = 1/3$ finnes, men de bedre eksponentene krever mer avanserte teknikker i analytisk tallteori. Det er gode grunner til å anta at den beste eksponenten er $\theta = 1/4$, men dit er det langt igjen.

Tellefunksjonen $B(x)$ er vanskeligere å hanskes med enn $R(x)$. Det grunnleggende asymptotiske estimatet

$$B(x) \sim \frac{\beta_0 x}{\sqrt{\log(x)}} \quad , \quad \beta_0 = \frac{1}{\sqrt{2}} \prod_{p \equiv 3(4)} (1 - p^{-2})^{-1/2}$$

ble bevist av Edmund Landau i 1908. Dette resultatet er et hakk vanskeligere å bevise enn den berømte Primtallssatsen

$$\pi(x) = \sum_{p \le x} 1 \sim \frac{x}{\log(x)}$$

for tellefunksjonen til primtallene. (Bokstaven p betegner et primtall ved konvensjon.) Ennå i dag er ikke noe elementært bevis for estimatet for $B(x)$ kjent. Merk at det gjennomsnittlige antallet representasjoner som sum av to kvadrat til de positive heltallene $n \le x$ som *er* sum av to kvadrat er

$$\frac{R(x)}{B(x)} \sim \frac{\pi}{\beta_0} \sqrt{\log(x)}.$$

For store x er dette forholdet adskillig større enn det gjennomsnittlige antall representasjoner

$$\frac{R(x)}{x} \sim \pi$$

fordi alle heltallene som ingen representasjoner har, ikke trekker ned. Det er ikke så få heltall som har mange forskjellige representasjoner som sum av to kvadrat.

Landaus sats kan forbedres til

$$B(x) \sim \frac{x}{\sqrt{\log(x)}} \left(\beta_0 + \beta_1 \log(x)^{-1} + \beta_2 \log(x)^{-2} + \cdots \right)$$

hvor rekkeuttrykket på høyre side ikke er en konvergent uendelig rekke, men en såkalt *asymptotisk ekspansjon.* Det vil si at om vi danner en approksimasjon, som for eksempel

$$B(x) \approx \frac{x}{\sqrt{\log(x)}} \left(\beta_0 + \beta_1 \log(x)^{-1} + \beta_2 \log(x)^{-2}\right),$$

ved å bryte av utviklingen etter et visst antall ledd, så er avbruddsfeilen dominert av et konstant multippel av det første utelatte leddet når $x \to +\infty$. Altså i dette eksemplet

$$\left| B(x) - \frac{\beta_0 x}{\log(x)^{1/2}} - \frac{\beta_1 x}{\log(x)^{3/2}} - \frac{\beta_2 x}{\log(x)^{5/2}} \right| \leq \frac{Cx}{\log(x)^{7/2}}$$

når $x \to +\infty$, med en passende positiv konstant C.

Vi har en tilsvarende asymptotisk utvikling

$$\pi(x) \sim \frac{x}{\log(x)} \left(1 + \log(x)^{-1} + \cdots + n! \log(x)^{-n} + \cdots\right)$$

for tellefunksjonen til primtallene. Det *logaritmiske integralet*

$$\mathrm{li}(x) = \int_2^x \frac{du}{\log(u)} \sim \frac{x}{\log(x)} \left(1 + \log(x)^{-1} + \cdots + n! \log(x)^{-n} + \cdots\right)$$

har den samme asymptotiske utviklingen, og tar vi differensen, ser vi at

$$\pi(x) = \mathrm{li}(x) + E(x)$$

med et restledd $E(x)$ som er dominert av et konstant multippel av $x/\log(x)^{n+1}$ for vilkårlig store n. Dette restleddet kan faktisk estimeres mye bedre enn som så. Nikolai Mikhailovich Korobov og Ivan Matveevich Vinogradov beviste i 1958 at

$$|E(x)| \leq C\, x\, e^{-c \log(x)^{3/5} \log\log(x)^{-1/5}}$$

for visse positive konstanter c og C.

Noe tilsvarende resultat er ikke kjent for $B(x)$. Koeffisientene β_n er gitt ved kompliserte tallteoretiske uttrykk, og det er langt fra klart at det skulle finnes noen rimelig beskrivbar funksjon som spiller samme rolle for $B(x)$ som $\mathrm{li}(x)$ gjør for $\pi(x)$. Intet bedre estimat for $B(x)$ enn den asymptotiske ekspansjonen ovenfor er kjent.

Så langt ser det ut som åpne spørsmål vedrørende summer av to kvadrat bare kan angripes med vanskelige teknikker fra analytisk tallteori. Men på det neste problemet har alle disse teknikkene kommet til kort, og det beste resultatet som er kjent vises med verktøy fra videregående skoles matematikk, og har stått urørt i seksti år! Spørsmålet er hvor stor vi må ta h som funksjon av x for å garantere at intervallet $(x-h, x]$ inneholder en sum av to kvadrat. Det dreier seg altså om eksistens av summer av to kvadrat i korte intervaller, i analogi med tilsvarende problem for primtall som har vært undersøkt siden det nittende århundre.

Gitt x velger vi k heltall slik at $x-k^2>0$ men ellers så stor som mulig. Det gir en rest $r_1=x-k^2$ av størrelsesorden $x^{1/2}$. Så velger vi m heltall slik at $r_1-m^2>0$ men ellers så stor som mulig. Det gir en rest r_2 av størrelsesorden $\sqrt{r_1}$ eller $x^{1/4}$. Nå er $x=k^2+m^2+r_2$ så $x-r_2<k^2+m^2<x$ og vi ser dermed at vi kan ta h av størrelsesorden $x^{1/4}$. Går vi dette resonnementet etter i sømmene og regner presist med ulikheter finner vi at intervallet $(x-2\sqrt{2}\,x^{1/4},x]$ inneholder en sum av to kvadrat for alle $x\geq 1$.

Ovenstående resonnement forekommer i et arbeide av Ram Prakash Bambah og Sarvadaman Chowla fra 1947. Den første som undersøkte problemet var antakelig Tirukkannapuram Vijayaraghavan, men han publiserte ikke sitt resultat. Det er ønskelig å redusere eksponenten $1/4$, men siden det ikke har vært noen fremskritt siden 1947, er svakere resultater også av interesse. Den store britiske matematikeren John Edensor Littlewood var interessert i summer av to kvadrat, og fremsatte som et forskningsproblem å bevise at det finnes en positiv funksjon $f(x)$ med $f(x)\to 0$ når $x\to+\infty$ slik at alle intervallene $(x-f(x)x^{1/4},x]$ inneholder en sum av to kvadrat.

Å redusere konstanten $2\sqrt{2}$, for eksempel med en faktor $1/2$, kan synes overkommelig uten noen grunnleggende ny idé, men er av liten interesse. Om vi slakker på kravet om at *alle* intervallene $(x-h,x]$ skal inneholde en sum av to kvadrat, kan vi ta h meget mindre. Problemet om eksistens av summer av to kvadrat i nesten alle korte intervaller er løst fullstendig: En dobbeltsidig ulikhet

$$\frac{a\,h(x)}{\sqrt{\log(x)}}\leq \sum_{x-h(x)<b\leq x} 1\leq \frac{A\,h(x)}{\sqrt{\log(x)}}\quad,\quad 0<a<A,$$

holder for nesten alle x hvis $h(x)/\sqrt{\log(x)}\to+\infty$ når $x\to+\infty$. Dette presise og nesten best mulige resultatet ble vist av John Benjamin Friedlander (øvre skranke i 1982) og Christopher Hooley (nedre skranke i 1994). At ulikheten holder for nesten alle intervaller betyr at om vi betegner lengden til mengden av de x med $1\leq x\leq X$ hvor ulikheten ikke holder med $\ell(X)$ så vil $\ell(X)/X\to 0$ når $X\to+\infty$. Ved den nedre skranken ser vi at hvis

$$\frac{h(x)}{\sqrt{\log(x)}}\to+\infty$$

når $x\to+\infty$ så inneholder nesten alle intervallene $(x-h(x),x]$ en sum av to kvadrat.

Men å forbedre resultatet til Bambah og Chowla for *alle* korte intervaller er fremdeles et åpent problem, og her er forbedringspotensialet formidabelt. En grovkornet sannsynlighetsteoretisk heuristikk indikerer at det skal finnes en positiv konstant C slik at intervallet $(x-C\log(x),x]$ inneholder en sum av to kvadrat for alle $x\geq 2$.

Det siste åpne spørsmålet som vi skal se på kan spores tilbake til et problem sendt inn til det britiske tidsskriftet *The Educational Times* i 1903: Å finne alle konsekutive tripler av to kvadrat. Problemet har dessverre ikke en elegant løsning, men vi kan ekstrahere en lettere oppgave med en elegant løsning: Vis at det finnes uendelig mange konsekutive tripler av summer av to kvadrat. For å gi leseren noe å bryne seg på, er løsningen skjøvet til slutten av artikkelen. Littlewood formulerte

en vanskeligere variant som forskningsproblem: Finnes det for vilkårlige positive heltall $h_1 < h_2$ uendelig mange tripler $n, n+h_1, n+h_2$ som er simultane summer av to kvadrat? Problemet sto åpent noen år, men ble løst av Hooley i 1973. Svaret viste seg å være ja, med et bevis som ikke er spesielt langt, men som bygger på teorien for ternære kvadratiske former.

Det er klart at hvis vi ser på vilkårlige kvadrupler $n, n+h_1, n+h_2, n+h_3$ så er svaret på spørsmålet i analogi med Littlewoods spørsmål *nei*. For ethvert konsekutivt kvadruppel $n, n+1, n+2, n+3$ inneholder et element som er kongruent med 3 modulo 4, og dermed ikke en sum av to kvadrat. Men en kan spørre hvilke betingelser de positive heltallene $h_1 < h_2 < \cdots < h_g$ må oppfylle for at uendelig mange av tuplene $n, n+h_1, \cdots, n+h_g$ skal være simultane summer av to kvadrat?

En pekepinn om dette problemets vanskelighetsgrad kan vi få ved å sammenlikne med de tilsvarende problemene for primtallene eller de kvadratfrie tallene. Spør vi for hvilke positive heltall $h_1 < h_2 < \cdots < h_g$ tuplet $n, n+h_1, \ldots, n+h_g$ uendelig ofte bare inneholder primtall, så er svaret ukjent. Det formodes at en kongruensbetingelse er tilstrekkelig; at polynomet $n(n+h_1)\cdots(n+h_g)$ ikke har noen fast primfaktor. For eksempel kan ikke $n, n+2, n+4$ alle være primtall uendelig ofte siden 3 er en fast primfaktor. Ikke et eneste tilfelle av denne formodningen er bevist; den kalles formodningen om primtallstupler (the prime tuplets conjecture). Det best kjente tilfellet er den ubeviste formodningen om at det finnes uendelig mange primtallstvillinger, altså at både n og $n+2$ uendelig ofte er primtall samtidig. Vi slutter at spørsmålet om tupler av summer av to kvadrat bør være adskillig lettere enn det tilsvarende for tupler av primtall, siden tilfellet $n, n+h_1, n+h_2$ er løst, og tilfellet hvor triplet er konsekutivt er en oppgave.

Et tall s kalles *kvadratfritt* hvis det ikke finnes noe kvadrat $k^2 \geq 4$ som går opp i s. Det er det samme som å si at intet primtall forekommer med eksponent større enn 1 i faktoriseringen av s som produkt av primtallspotenser. Problemer vedrørende kvadratfrie tall bruker å falle lettere enn de tilsvarende for primtall eller summer av to kvadrat. For eksempel har estimatet

$$Q(x) = \sum_{s \leq x} 1 \sim \frac{6}{\pi^2}\, x$$

for tellefunksjonen til de kvadratfrie tallene et lett bevis, mens de tilsvarende bevisene for $\pi(x)$ og $B(x)$ er vanskelige. (Bokstaven s betegner et kvadratfritt tall ved konvensjon.) Problemet om tupler av kvadratfrie tall ble løst av Leon Mirsky i 1947. Han fant at visse kongruensbetingelser, som trivielt er nødvendige, er tilstrekkelige. Beviset er elementært.

Det kan virke som problemet vedrørende tupler av summer av to kvadrat ligger mellom de tilsvarende problemene for primtall og for kvadratfrie tall i vanskelighetsgrad, og antakelig nærmere de kvadratfrie tallene enn primtallene.

Til slutt skal vi gi løsningen på oppgaven. Triplet $8, 9, 10$ består av summer av to kvadrat. Forutsett at triplet $n-1, n, n+1$ består av summer av to kvadrat. Da består også triplet n^2-1, n^2, n^2+1 av summer av to kvadrat. For $n^2 = 0^2 + n^2$ og $n^2+1 = 1^2+n^2$. Videre er $n^2-1 = (n-1)(n+1)$ produkt av summer av to kvadrat etter forutsetning, dermed selv sum av to kvadrat. Dette gir uendelig mange konsekutive tripler av summer av to kvadrat ved gjentatt kvadrering.

Referanser

[1] R. P. Bambah and S. Chowla, *On numbers which can be expressed as sums of two squares.* Proc. Nat. Inst. Sci. India **13** (1947), no. 2, 101–103.

[2] L. Euler, Novi Comm. Acad. Petropolitensis **5** (1751), 3 et seq.

[3] P. de Fermat, *Oeuvres.* 3 vols., Gauthiers-Villars, Paris (1841,1894,1896), I 293, II 213, III 243–246.

[4] J. B. Friedlander, *Sifting short intervals.* Math. Proc. Cambridge Philos. Soc. **91** (1982), 9–15.

[5] J. B. Friedlander, *Sifting short intervals, II.* Math. Proc. Cambridge Philos. Soc. **92** (1982), 381–384.

[6] C. F. Gauss, *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig (1801), §182.

[7] C. F. Gauss, *Werke.* 12 vols., Dieterichschen Universitätsdruckerei, Göttingen (1863-1933), II 272–275.

[12] G. H. Hardy, *On the Expression of a Number as the Sum of Two Squares.* Quart. J. Math. **46** (1915), 263–283.

[9] D. R. Heath-Brown, *Fermat's two squares theorem.* Invariant **11** (1984), 3–5.

[10] C. Hooley, *On the Intervals between Numbers that are Sums of Two Squares, II.* J. Number Theory **5** (1973), 215–217.

[11] C. Hooley, *On the Intervals between Numbers that are Sums of Two Squares, IV.* J. Reine Angew. Math. **452** (1994), 79–109.

[12] M. N. Huxley, *Integer points, exponential sums and the Riemann zeta function.* Number theory for the millennium, II (Urbana, IL 2000) (Natick, MA) (M. A. Bennett, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand and W. Philipp eds.), A K Peters (2002), 275–290.

[13] C. G. J. Jakobi, *Fundamenta Nova Theoriae Functionum Ellipticarum.* Bornträger, Königsberg (1829), 103, 106–107, 184.

[14] N. M. Korobov, *Estimates of trigonometric sums and applications.* Uspekhi Mat. Nauk **13** (1958), no. 4, 185–192 (Russian).

[15] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate.* Arch. Math. Phys. **13** (1908), 305–312.

[16] *Mathematical Questions, 14955.* Educ. Times (2) **3** (1903), 41–43.

[17] L. Mirsky, *Note on an asymptotic formula connected with r-free integers.* Quart. J. Math., Oxford Ser. **18** (1947), 178-182.

[18] L. Mirsky, *Arithmetical pattern problems relating to divisibility by rth powers.* Proc. London Math. Soc. (2) **50** (1949), 497–508.

[19] W. Sierpiński, *On a problem of the theory of asymptotic functions.* Prace mat.-fiz. **17** (1906), 77–118 (Polish).

[20] S. Stevin, *L'Arithmétique.* (Reueuë, corrigee & augmentee de plusieurs traictez et annotations par A. Girard), Elzevier, Leide (1625), 622.

[21] I. M. Vinogradov, *A new estimate of the function $\zeta(1+it)$.* Iz. Akad. Nauk. SSSR Ser. Mat. **22** (1958), 161–164 (Russian).