Pythagoreiska tripplar på sex olika sätt

Patrik Lundström

Institutionen för ingenjörsvetenskap
Högskolan Väst, Trollhättan
patrik.lundstrom@hv.se

Inledning

I den matematiska diskursen fyller beviset många funktioner varav den viktigaste naturligtvis är att säkerställa korrektheten hos matematiska påståenden. En annan funktion som inte alltid är lika uttalad, åtminstone inte hos ickematematiker, är bevisets roll som didaktiskt verktyg. När matematiker talar om att ett bevis är bra så menar de att resonemanget har en kvalitet som utifrån ett visst perspektiv tydligt belyser varför påståendet är sant. Matematikern Paul Erdös hävdade till och med att det finns perfekta bevis av alla satser (se t.ex. (11)). En något försiktigare och troligen vanligare hållning är att varierande infallsvinklar i bevis, till exempel användning av olika matematiska teorier, klargör olika aspekter på samma sats.

Det kanske mest kända exemplet på detta är Pythagoras sats som kan bevisas på flera hundra olikartade sätt med geometriska, algebraiska och analytiska metoder (se (16) för 378 bevis eller (3) för 78 bevis). Baserat på det arkeologiska fyndet Plimpton 322 har det konstaterats att man redan i det antika Babylonien kände till Pythagoras sats, även om den då naturligtvis inte kallades just så. Detta arkeologiska fynd består av en lertavla där man i kilskrift ristat in fyra kolumner med numerisk information. Kolumn två och tre innehåller bara naturliga tal och är överst namngivna med bredd respektive diagonal. Kontroll av tabellen ger vid handen att i varje rad är skillnaden mellan kvadraten på diagonalen och kvadraten på bredden lika med kvadraten på ett heltal. Detta innebär att Babylonierna konstruerade ett stort antal pythagoreiska tripplar, det vill säga tripplar (a, b, c) av heltal som uppfyller $a^2 + b^2 = c^2$. Ingen vet säkert varför Babylonierna var intresserade av sådan information, men utifrån det faktum att förhållandet mellan bredden och diagonalen minskar då man rör sig nedåt i tabellen har det formulerats en hypotes (13) om att det rör sig om en tidig trigonometrisk tabell. Denna och liknande hypoteser är dock starkt ifrågasatta (19). Det råder inte heller någon konsensus kring huruvida Babylonierna hittade sina tripplar genom någon form av parametrisering. Pythagoreiska tripplar har också studerats i andra kulturer, t.ex. i Kina och i Indien (14).

Syftet med denna artikel är att visa hur metoder som utvecklats i olika matematiska teorier kan användas för att hitta parametriseringar av pythagoreiska tripplar.

Den första metoden baseras på ett mycket elementärt talteoretiskt argument som leder fram till en parametrisering som Pythagoras och Platon kände till. Den andra metoden är hämtad från Euklides Elementa och grundar sig på elementär talteori. Den tredje metoden är ett algebraisk-geometriskt argument som är en utvidgning av en idé hämtad från Diophantos verk Arithmetica. Den fjärde metoden är ett resonemang som bygger på samband mellan trigonometriska funktioner. Den femte metoden är ett talteoretiskt argument som använder aritmetik för Gaussiska heltal. Den sjätte metoden är ett Galoisteoretiskt bevis som använder ett specialfall av Hilberts 90:e sats.

1 Pythagoras och Platon

Proclus påstår, i en kommentar till den första boken av Euklides Elementa, att både Pythagoras och Platon kände till varianter av pythagoreiska tripplar på formen

$$(a, b, c) = (2m^2 + 2m, 2m + 1, 2m^2 + 2m + 1)$$

där m är ett positivt heltal (8). Däremot vet vi ingenting om hur de hittade dessa tripplar. Ett folkloristiskt argument av okänt ursprung är följande. En geometrisk tolkning av likheten $c^2 - a^2 = b^2$ är att vi ska ta bort en mindre kvadrat från en större och sedan på något sätt stuva om det som är kvar till en kvadrat. Låt oss analysera det fall då vi får så lite kvar som möjligt att stuva om, det vill säga $c = n + 1$ och $a = n$ för något positivt heltal n. Då får vi att $b^2 = c^2 - a^2 = (n + 1)^2 - n^2 = 2n + 1$ vilket i sin tur implicerar att b måste vara lika med ett udda positivt heltal, säg $2m + 1$ för ett annat positivt heltal m. Då får vi att $(2m+1)^2 = 2n+1$ vilket efter omskrivning ger att $n = 2m^2+2m$ och vi har hittat de eftersökta pythagoreiska tripplarna. Notera att inte alla pythagoreiska tripplar har denna form, t.ex. $(8, 15, 17)$. För att hitta de resterande krävs därför ett annat angreppssätt.

2 Euklides

Beviset av Lemma 1 till Proposition 29 i den tionde boken av Euklides elementa (7) ger oss den äldsta kända metoden som genererar alla pythagoreiska tripplar. I nedanstående resonemang antar vi hela tiden att sådana tripplar består av olika naturliga tal.

Euklides använder i sitt resonemang flitigt begreppet *plana tal* vilket helt enkelt är areor av rektanglar med sidlängd i naturliga tal. Två plana tal kallar han *likformiga* om motsvarande rektanglar är likformiga med ett rationellt förhållande mellan sidorna. Han visar att två plana tal är likformiga om och endast om deras produkt är en kvadrat.

Euklides metod går till på följande sätt. Notera först att om vi har två naturliga tal u och v, $u > v$, av samma paritet, så gäller alltid likheten

$$uv = \left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2$$

och alla termer är naturliga tal. Om nu u och v också är likformiga, så är uv lika med en kvadrat, säg w^2, och därmed är

$$(a, b, c) = \left(\frac{u-v}{2}, w, \frac{u+v}{2}\right)$$

en pythagoreisk trippel. Omvänt, givet en pythagoreisk trippel (a, b, c), så är $u = c + a$ och $v = c - a$ två naturliga tal av samma paritet med $u > v$. Betraktat som plana tal är de också likformiga eftersom $uv = (c + a)(c - a) = c^2 - a^2 = b^2$ är en kvadrat. Euklides har därmed skapat en bijektion mellan mängden av alla pythagoreiska tripplar (a, b, c) och mängden av alla par (u, v), $u > v$, av likformiga plana tal av samma paritet.

Nu tittar vi på specialfallet då den pythagoreiska trippeln är primitiv, det vill säga då talen a, b och c är relativt prima. Genom att utnyttja Euklides resonemang ovan så kan vi faktiskt parametrisera alla sådana tripplar. Först konstaterar vi att a eller b är udda (annars är bägge jämna och då är c jämnt vilket strider mot antagandet att trippeln är primitiv). Kan både a och b vara udda? Nej, eftersom c då är jämnt vilket ger oss motsägelsen

$$2 = 1 + 1 \equiv \text{udda}^2 + \text{udda}^2 = \text{jämnt}^2 \equiv 0 \mod 4.$$

Av symmetriskäl kan vi nu anta att a och c är udda och att b är jämnt. Euklides metod ger oss nu två likformiga plana tal u och v, $u > v$, av samma paritet som uppfyller $c = (u + v)/2$, $a = (u - v)/2$ och $uv = b^2$. Av likformigheten följer det att $u = ds^2$ och $v = dt^2$ för några naturliga tal d, s och t där d är kvadratfri och $s > t$. Den största gemensamma delaren till u och v delar också $u + v = 2c$ och $u - v = 2a$. Men eftersom a och c inte har någon gemensam primfaktor, så betyder det att största gemensamma delaren till u och v är 1 eller 2. Eftersom u och v har samma paritet och $uv = b^2$ är jämnt, så är både u och v jämna. Alltså kan vi dra slutsatsen att $d = 2$ och att s och t är relativt prima. Eftersom a är udda så kan inte heller både s och t vara udda. Detta ger oss den välkända parametriseringen

$$(a, b, c) = (s^2 - t^2, 2st, s^2 + t^2)$$

av primitiva pythagoreiska tripplar där s och t, $s > t$, är relativt prima naturliga tal av olika paritet.

3 Diofantos

I lösningen till problem 8 i den andra boken av Diofantos verk Arithmetika redogörs för en metod att dela upp en kvadrat i två mindre kvadrater som med en modern tolkning (1) går ut på att göra en linjär ansats. Jag beskriver nu denna metod med hjälp av analytisk geometri.

Om vi i ekvationen $a^2 + b^2 = c^2$ dividerar med c, så kan den skrivas om på formen $x^2 + y^2 = 1$ där $x = a/c$ och $y = b/c$. För att lösa den ursprungliga ekvationen inser vi nu att det räcker att hitta alla rationella punkter på cirkeln $x^2 + y^2 = 1$.

Innan vi beskriver Diofantos metod gör vi en kort analys av problemet att hitta alla rationella punkter på allmänna kägelsnitt dvs kurvor av typen

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{1}$$

där A, B, C, D, E och F är rationella tal valda så att kurvan blir av andra graden, det vill säga så att någon av A, B och C är skild ifrån noll. Det är lätt att se att man genom en rationell koordinattransformation alltid kan få $A \neq 0$ (om $A = 0$ och $C \neq 0$, så använder vi $(x, y) \mapsto (y, x)$; om $A = C = 0$, så använder vi $(x, y) \mapsto (x, y + x)$). För att analysera (1) börjar vi med att skriva om den på formen

$$(2Ax + By + D)^2 - \Delta_1 y^2 - 2\Delta_3 y = \Delta_2 \tag{2}$$

där $\Delta_1 = B^2 - 4AC$, $\Delta_2 = D^2 - 4AF$ och $\Delta_3 = BD - 2AE$. Nu finns ett antal fall att beakta.

Fall 1: $\Delta_1 = \Delta_3 = 0$. Om Δ_2 ej är en rationell kvadrat, så har (2) inga rationella lösningar; Om $\Delta_2 = q^2$, $q \in \mathbb{Q}$, så blir (2) unionen av de två räta linjerna $2Ax + By + D = \pm q$.

Fall 2: $\Delta_1 = 0$ och $\Delta_3 \neq 0$. Då blir (2) en parabel.

Fall 3: $\Delta_1 \neq 0$. Då kan vi skriva om (2) på formen

$$\Delta_1(2Ax + By + D)^2 - (\Delta_1 y + \Delta_3)^2 = \Delta_1\Delta_2 - \Delta_3^2 \tag{3}$$

Om $\Delta_1 < 0$ och $\Delta_1\Delta_2 - \Delta_3^2 > 0$, så har (3) inga lösningar; Om $\Delta_1 < 0$ och $\Delta_1\Delta_2 - \Delta_3^2 = 0$, så har (3) en lösning; Om $\Delta_1 < 0$ och $\Delta_1\Delta_2 - \Delta_3^2 < 0$, så är (3) de rationella punkterna på en ellips; Om $\Delta_1 = q^2$, $q \in \mathbb{Q}\setminus\{0\}$ och $\Delta_1\Delta_2 - \Delta_3^2 = 0$, så är (3) unionen av två räta linjer. Om Δ_1 ej är en rationell kvadrat och $\Delta_1\Delta_2 - \Delta_3^2 = 0$, så har (3) inga rationella lösningar. Om $\Delta_1 > 0$ och $\Delta_1\Delta_2 - \Delta_3^2 \neq 0$, så är (3) de rationella punkterna på en hyperbel.

Av ovanstående analys framgår det att det är trivialt att hitta alla rationella punkter på kägelsnitt förutom i följande två fall: (i) $\Delta_1 < 0$ och $\Delta_1\Delta_2 < \Delta_3^2$ då vi måste hitta alla rationella punkter på en ellips; (ii) Δ_1 är ett positivt rationellt tal som ej är en rationell kvadrat och $\Delta_1\Delta_2 \neq \Delta_3^2$ då vi måste hitta alla rationella punkter på en hyperbel som ej genom en rationell koordinattransformation kan skrivas om på formen $xy = 1$.

Nu beskriver vi Diofantos metod för kurvorna av typen (i) eller (ii). Antag först att vi har hittat *en* rationell punkt (x_0, y_0) på kurvan. Om nu (x_1, y_1) är en annan rationell punkt på kurvan, så ligger den på linjen L_r: $y - y_0 = r(x - x_0)$ där r är det rationella talet $(y_1 - y_0)/(x_1 - x_0)$. Omvänt, så skär alla linjer L_r, där r är ett rationellt tal, kurvan i två rationella punkter. Varför? Jo, eftersom insättning av $y = y_0 + r(x - x_0)$ i kurvans ekvation ger oss en andragradsekvation i x med rationella koefficienter. Eftersom vi vet att en av rötterna, nämligen x_0, är rationell, så måste även den andra roten vara rationell. Varför? Jo, rötternas summa är ju lika med förstagradskoefficienten som är rationell. Detta resonemang ger oss faktiskt en bijektion mellan alla rationella tal r (samt ∞) och de rationella punkterna på kurvan (se t.ex. (12)).

Nu genomför vi den ovan beskrivna kalkylen explicit. Om vi låter L_r skära kurvan, så får vi ekvationen

$$Ax^2 + Bx(y_0 + r(x - x_0)) + C(y_0 + r(x - x_0))^2 + Dx + E(y_0 + r(x - x_0)) + F = 0$$

som, efter omskrivning, får utseendet

$$(x-x_0)\Big((A+Br+Cr^2)(x-x_0)+2Ax_0+By_0+Brx_0+2Cry_0+D+Er\Big)=0$$

Detta ger oss den andra skärningspunktens koordinater

$$\begin{cases} x = x_0 - \dfrac{2Ax_0+By_0+Brx_0+2Cry_0+D+Er}{A+Br+Cr^2} \\ \\ y = y_0 - \dfrac{r(2Ax_0+By_0+Brx_0+2Cry_0+D+Er)}{A+Br+Cr^2} \end{cases}$$

Nu bör man notera två saker. För det första är nämnaren nollskild i kvoterna ovan för alla r tack vare antagandet att Δ_1 ej är en rationell kvadrat. För det andra är täljaren noll precis då linjen L_r tangerar kurvan i punkten (x_0, y_0) (bilda skalärprodukten mellan gradienten till vänsterledet i (1) och vektorn $(1, r)$). Detta innebär att $x_0 \neq x_1$ för alla andra r.

I fallet med cirkeln är $A = C = 1$, $F = -1$ och $B = D = E = 0$. Vidare så kan vi t.ex. välja $x_0 = -1$ och $y_0 = 0$. Därför får vi följande parametrisering av cirkelns rationella punkter

$$\begin{cases} \dfrac{a}{c} = x = -1 + \dfrac{2}{1+r^2} = \dfrac{1-r^2}{1+r^2} = \dfrac{t^2-s^2}{t^2+s^2} \\ \\ \dfrac{b}{c} = y = \dfrac{2r}{1+r^2} = \dfrac{2st}{t^2+s^2} \end{cases}$$

där $r = s/t$ för heltal s och t där $t \neq 0$. Om vi nu, precis som tidigare, antar att a, b och c är relativt prima heltal med a och c udda och b jämnt, så kan vi dra slutsatsen att $a = t^2 - s^2$, $b = 2st$ och $c = t^2 + s^2$ för några relativt prima heltal s och t av olika paritet.

Den vetgirige läsaren undrar nu förstås om man kan avgöra om det till ett givet kägelsnitt finns minst en rationell punkt. Redan Legendre (se t.ex. (17)) hittade ett elegant sådant kriterium. Genom en rationell linjär transformation så kan varje kägelsnitt på homogen form beskrivas med en ekvation på formen

$$Ax^2 + By^2 + Cz^2 = 0$$

där koefficienterna är kvadratfria nollskilda heltal som är parvis relativt prima. Då finns det en icketrivial heltalspunkt på detta kägelsnitt om och endast om följande tre villkor är uppfyllda (i) $-AB$ är en kvadratisk rest till C; (ii) $-AC$ är en kvadratisk rest till B; (iii) $-BC$ är en kvadratisk rest till A. Beviset i (17) ger också en algoritm för att hitta en sådan lösning. Det finns naturligtvis andra, modernare algoritmer, se t.ex. (2).

4 Trigonometriska funktioner

Ända sedan trigonometrins barndom i det antika Grekland har det varit känt att alla *reella* lösningar till ekvationen $x^2 + y^2 = 1$ kan parametriseras med de trigonometriska funktionerna $x = \cos\theta$ och $y = \sin\theta$. Detta kan användas för att hitta

alla *rationella* lösningar till $x^2 + y^2 = 1$ genom att utnyttja tre välkända samband mellan sinus, cosinus och tangens halva vinkeln, nämligen:

$$\cos\theta = \frac{1 - \tan^2(\theta/2)}{1 + \tan^2(\theta/2)} \tag{4}$$

$$\sin\theta = \frac{2\tan(\theta/2)}{1 + \tan^2(\theta/2)} \tag{5}$$

$$\tan(\theta/2) = \frac{\sin\theta}{1 + \cos\theta} \tag{6}$$

Ifrån (4) och (5) kan vi dra slutsatsen att

$$(x, y) = \left(\frac{1 - r^2}{1 + r^2}, \frac{2r}{1 + r^2}\right) \tag{7}$$

är en rationell lösning till $x^2 + y^2 = 1$ om vinkeln θ är vald så att $r = \tan(\theta/2)$ är ett rationellt tal. Omvänt, ifrån (6) kan vi dra slutsatsen att r måste vara rationellt, givet att både $\sin\theta$ och $\cos\theta$ är rationella. Därför kan alla rationella lösningar till $x^2 + y^2 = 1$ parametriseras genom (7) där r löper över de rationella talen.

I det här sammanhanget är det värt att notera att en viktig ingrediens i det bevis av Fermats sista sats (FSS) till vilket Wiles lade den sista pusselbiten för en tid sedan också innehåller funktionsteori på ett analogt men samtidigt mycket mera komplicerat sätt. Beviset för FSS använder teorin för rationella elliptiska kurvor, dvs kurvor definierade av likheter på formen $y^2 = Ax^3 + Bx^2 + Cx + D$ där A, B, C och D är rationella tal och polynomet i högerledet har distinkta rötter. Enligt en förmodan av Taniyama och Shimura (TS) så kan varje sådan elliptisk kurva parametriseras $f(z)^2 = Ag(z)^3 + Bg(z)^2 + Cg(z) + D$ av s.k. modulära funktioner $f(z)$ och $g(z)$ båda i samma nivå N (se nedan). De modulära funktionerna är, precis som de trigonometriska funktionerna, invarianta med avseende på gruppverkan fast på ett mer komplicerat sätt. I fallet med sinus och cosinus så är det den additiva gruppen av alla heltal som verkar genom translation på argumentet. Funktionerna $f(z)$ och $g(z)$ är modulära i nivå N om de är invarianta med avseende på verkan av den multiplikativa matrisgruppen

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c \text{ och } d \text{ heltal med } ad - bc = 1 \text{ och } N|c \right\}$$

på argumenten, dvs så att

$$f\left(\frac{az + b}{cz + d}\right) = f(z) \quad \text{och} \quad g\left(\frac{az + b}{cz + d}\right) = g(z)$$

för a, b, c och d valda enligt ovan. Utöver denna invarians tillkommer ytterligare några villkor på funktionerna för att de ska vara modulära, men vi utelämnar här de tekniska detaljerna kring detta. Vad Wiles bevisade var att TS gäller för en speciell klass av elliptiska kurvor, de semistabila (ännu ett tekniskt villkor som vi väljer att

utelämna). Men vad har detta med FSS att göra? Jo, tidigare hade Ribet visat att om $a^p + b^p = c^p$ för positiva heltal a, b och c och primtal p större än 3, så har den semistabila elliptiska kurvan $y^2 = x(x - a^p)(x + b^p)$ så speciella egenskaper att den inte kan parametriseras av modulära funktioner vilket motsäger TS och beviset av FSS är klart. Efter Wiles har Breuil, Conrad, Diamond, och Taylor bevisat TS för alla elliptiska kurvor. Detta resultat har använts av flera matematiker för att visa att andra diofantiska ekvationer saknar icketriviala heltalslösningar. Som ett exempel på detta nämner vi här Darmon och Merel som med denna teknik bevisat att ekvationen $a^n + b^n = c^3$, $n > 2$, saknar heltalslösningar med a, b och c alla nollskilda. För mer detaljer kring detta och den allmänna TS, se t.ex. (4).

5 Gaussiska heltal

Nu ska vi använda ringen av de gaussiska heltalen $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ som introducerades av Gauss (9) under perioden 1829-1831 då han sökte efter kubiska och bikvadratiska reciprocitetssatser. Denna ring har unik primfaktoruppdelning. Notera att de gaussiska primtalen inte är desamma som primtalen i $\mathbb{Z}$. Till exempel är $2 = (1+i)(1-i)$ en äkta primfaktoruppdelning i $\mathbb{Z}[i]$. För detaljer kring gaussiska heltal, se t.ex. (20).

Antag att heltalen a, b och c i likheten $a^2 + b^2 = c^2$ inte har några gemensamma primfaktorer i $\mathbb{Z}[i]$ samt att a och c är udda men b är jämnt. Om vi skriver likheten som $(a + bi)(a - bi) = c^2$, så kan vi konstatera att faktorerna $a + bi$ och $a - bi$ inte har några gemensamma primfaktorer. Varför? Jo, om vi antar att z är ett gaussiskt primtal som delar båda dessa faktorer, så skulle z dela både deras summa $2a$ och deras differens $2bi$. Men eftersom c är udda så kan inte z vara en delare till 2. Därför delar z både a och b vilket är en motsägelse. Därför kan vi konstatera att $a + bi$ är en kvadrat gånger en enhet, det vill säga en delare till 1 i $\mathbb{Z}[i]$; Det är lätt att kolla att dessa är ± 1 och $\pm i$. Därför får vi nu

$$a + bi = \epsilon(s + ti)^2 = \epsilon(s^2 - t^2 + 2sti)$$

där $\epsilon = \pm 1$ eller $\epsilon = \pm i$ och $s, t \in \mathbb{Z}$. Möjligheterna $\epsilon = \pm i$ är uteslutna på grund av att att a är udda. Alltså är $\epsilon = \pm 1$. Fallet $\epsilon = 1$ ger oss att

$$\begin{cases} a = s^2 - t^2 \\ b = 2st \end{cases}$$

för några relativt prima heltal s och t av olika paritet. Fallet $\epsilon = -1$ kan återföras på det förra fallet genom transformationen $(s, t) \mapsto (-t, s)$.

6 Hilberts 90:e sats

Den 90:e satsen i Hilberts talteoretiska verk Zahlbericht från 1897 (se (10) för en engelsk översättning) säger att givet en ändlig cyklisk Galoisutvidgning K/k

av kroppar av grad n, med Galoigrupp genererad av automorphismen σ, så har alla lösningar i K till ekvationen $\prod_{i=0}^{n-1} \sigma^i(z) = 1$ formen $z = u/\sigma(u)$ för något $u \in K \setminus \{0\}$.

Nu redogör vi för ett folkloristiskt argument som visar att ett specialfall av Hilberts 90:e sats direkt ger oss en parametrisering av alla rationella lösningar till ekvationen $x^2 + y^2 = 1$. Argumentet kan hittas på flera ställen i litteraturen, se t.ex. (5), (6), (18) och (21). Om vi låter $K = \mathbb{Q}(i)$ och $k = \mathbb{Q}$, så är K/k en cyklisk Galoisutvidgning av grad två och σ är komplex konjugering. Av Hilberts 90:e sats följer nu att om det finns $x, y \in k$ som löser ekvationen $x^2+y^2 = (x+yi)(x-yi) = 1$ så måste det finnas $u = s + ti$, $s, t \in k$, sådant att

$$x + yi = u/\overline{u} = \frac{s + ti}{s - ti} = \frac{s^2 - t^2}{s^2 + t^2} + \frac{2st}{s^2 + t^2} i$$

En jämförelse av real- och imaginärdelar i likheten ovan ger oss samma parametrisering som vi fann med hjälp av de förra metoderna.

Varför gäller då Hilberts 90:e sats? Bevis för denna sats kan man hitta i många böcker i talteori eller algebra, se t.ex. (15). Vi nöjer oss med att bevisa satsen i det specialfall vi behöver, dvs då $K = \mathbb{Q}(i)$ och $k = \mathbb{Q}$. Låt $z \in K$ uppfylla $z\overline{z} = 1$. Då finns $w \in K$ sådant att $u = w + z\overline{w} \neq 0$. Varför? Jo, om $z = -1$ så väljer vi t.ex. $w = i$ och om $z \neq -1$ så väljer vi t.ex. $w = z$. Nu kontrollerar vi att elementet u duger för våra syften

$$u/\overline{u} = \frac{w + z\overline{w}}{\overline{w} + \overline{z}w} = z \cdot \frac{\overline{z}w + \overline{w}}{\overline{w} + \overline{z}w} = z$$

och beviset är klart

Elkies (6) har noterat att Hilberts 90:e sats på detta sätt kan användas för att parametrisera heltalslösningarna till alla ekvationer på formen

$$x^2 + Axy + By^2 = z^2,$$

där $A^2 - 4B$ ej är en rationell kvadrat, genom att studera den kvadratiska utvidgningen $\mathbb{Q}(\sqrt{A^2 - 4B})/\mathbb{Q}$.

Avslutningsvis... vill författaren uttrycka sin djupa tacksamhet gentemot refereen för dennes otaliga korrigeringar och förbättringsförslag på tidigare versioner av denna artikel.

Referenser

[1] I. G. Bashmakova, Diophantus and Diophantine Equations, MAA: Dolciani Math Expositions no 20 (1997).

[2] J. W. S. Cassels, Rational Quadratic Forms, Academic Press, London–New York–San Francisco (1978).

[3] Web page: Cut the Knot <http://www.cut-the-knot.org>

[4] H. Darmon, A Proof of the Full Shimura-Taniyama-Weil Conjecture Is Announced, Notices of the AMS, December 1999 **46** issue 11.

[5] D. S. Dummit och R. M. Foote, Abstract Algebra, Wiley (2003).

[6] N. D. Elkies, Pythagorean triples and Hilbert's Theorem 90, available at <http://www.math.harvard.edu/∼elkies/>.

[7] Euclid, The Thirteen Books of Euclid's Elements, T.L. Heath, Dover, New York (1956).

[8] J. Fauvel och J. Gray, The History of Mathematics: A Reader, MacMillan Press, London (1987).

[9] C. F. Gauss, Theoria residuorum biquadraticorum. Commentatio secunda., Comm. Soc. Reg. Sci. Gottingen 7, 1-34 (1832); reprinted in Werke, Georg Olms Verlag, Hildesheim,93-148 (1973).

[10] D. Hilbert, The theory of algebraic number fields, Springer-Verlag, Berlin (1998).

[11] P. Hoffman, The man who loved only numbers: the story of Paul Erdös and the search for mathematical truth, Hyperion (1999).

[12] D. Husemöller, Elliptic Curves, Springer (2004).

[13] D. E. Joyce, Plimpton 322 (1995), available at <http://aleph0. clarku.edu/∼djoyce/mathhist/plimpnote.html>.

[14] V. Katz, A History of Mathematics, Harper Collins, New York (1993).

[15] S. Lang, Algebra, Addison-Wesley (1993).

[16] E. S. Loomis, The Pythagorean Proposition, NCTM (1972).

[17] T. Nagell, Introduction to Number Theory, Almqvist & Wiksell, Uppsala (1951).

[18] T. Ono, Variations on a Theme of Euler: Quadratic Forms, Elliptic Curves and Hopf Maps, Springer (1994).

[19] E. Robson, Neither Sherlock Holmes nor Babylon: A Reassessment of Plimpton 322, Historia Mathematica 28, 167-206 (2001).

[20] I. N. Stewart och D. O. Tall, Algebraic Number Theory, Chapman and Hall (1987).

[21] O. Taussky, Sums of Squares, Amer. Math. Monthly, Vol. 77, 805-830 (1970).