UPPSALA UNIVERSITET
Matematiska Institutionen
Sten Kaijser

Pythagoreiska trianglar

Inledning. Pythagoreiska trianglar har varit kända i minst 4000 år och kanske ännu längre. De utgör därmed ett av de äldsta vittnesbörden om matematisk aktivitet. Uppsatsens syfte är att öka intresset för den moderna matematikens strukturer genom att visa hur de kan användas för att förstå matematiska problem som fascinerat människan sedan urminnes tider, problem som dessutom ofta kan fascinera ungdomar även idag.

Kort historik. Pythagoras sats tillhör de äldsta vittnesbörden om mänsklig matematisk aktivitet. Vi får alla i skolan lära oss om den *Egyptiska triangeln* med sidorna 3, 4 och 5, och vi får ibland höra att egypterna använde denna triangel för att åstadkomma räta vinklar när de byggde sina pyramider. Även om detta förmodligen inte är sant, helt enkelt för att de antagligen föredrog att tillverka vinkelhakar, så är det förvisso sant att egypterna redan för tre och ett halvt årtusende sedan kände till både denna triangel och andra rätvinkliga trianglar vars sidor är heltal. Det som förmodligen också är sant är att antingen PYTHAGORAS själv[1], eller någon i hans skola, faktiskt bevisade både satsen och dess omvändning.

PYTHAGORAS SATS. *Om T är en rätvinklig triangel med kateterna a och b och med hypotenusan c så råder sambandet $a^2 + b^2 = c^2$.*

OMVÄNDNINGEN TILL PYTHAGORAS SATS. *Om T' är en triangel med sidorna a, b och c sådan att $a^2 + b^2 = c^2$ så är T' rätvinklig med kateterna a och b och med hypotenusan c.*

Det är däremot inte sant att Pythagoras eller pythagoréerna *upptäckte* satsen. Av bevarade kilskrifter framgår att babylonierna i Mesopotamien kände till ett flertal s.k. pythagoreiska taltripplar, d.v.s. taltripplar av **naturliga tal** $(a,\ b,\ c)$ sådana att $a^2 + b^2 = c^2$. Sådana tripplar var kända även i Indien vid ungefär samma tid som Pythagoras var verksam i Grekland, och möjligen hade de redan då varit kända i tusentals år.

Vi kommer i fortsättningen att säga att en rätvinklig triangel T vars alla tre sidor har heltalslängd är pythagoreisk (eller en pythagoreisk triangel). Vi kommer likaså att säga att en taltrippel (av naturliga tal) $(a,\ b,\ c)$ är pythagoreisk om $a^2 + b^2 = c^2$. Samtidigt bör det påpekas att vi inte skiljer mellan taltripplarna $(a,\ b,\ c)$ och $(b,\ a,\ c)$ eller mellan en viss triangel och dess spegelvändning.

Som vi också får lära oss ledde Pythagoras sats till upptäckten av irrationella tal — något som fick stor betydelse för den grekiska matematiken. (Ännu större betydelse lär denna upptäckt ha haft för den som gjorde den, eftersom han som straff kastades överbord vid nästa sjöresa — kom sedan inte och påstå att matematisk forskning är riskfri.)

Pythagoreiska taltripplar har varit kända i två och ett halvt årtusende och även generella metoder att konstruera dem har varit kända, åtminstone sedan 300-talet (e.Kr.) av både kinesiska och västerländska matematiker. Den som i väst angav en metod var Diofantos. Även om metoder att konstruera dem alltså varit kända dröjde det länge innan man kunde ge en fullständig teori som direkt kunde beskriva mängden av alla möjliga pythagoreiska trianglar. Den som löste problemet var PIERRE FERMAT (1601 - 1665) som bevisade följande vackra resultat.

[1]Pythagoras kom till staden Kroton i södra Italien omkring år 530 f.Kr.och var verksam där till sin död ungefär 30 år senare.

SATS 3. *Ett primtal p kan skrivas som en summa av två (heltals-)kvadrater om och endast om $p = 4n + 1$.*

Vi ska senare se vilken roll denna sats (och dess konsekvenser) spelar för beskrivningen av pythagoreiska trianglar.

Ett viktigt bidrag till förståelsen av pythagoreiska trianglar gavs av GAUSS (1777 - 1855), som med introduktionen av det komplexa planet och de s.k. Gaussiska heltalen skapade nya möjligheter att använda algebraiska metoder för studiet av pythagoreiska trianglar.

Några förberedande observationer. Innan vi övergår till att studera pythagoreiska trianglar med algebraiska metoder ska vi börja med några enkla observationer. Låt oss till att börja med införa ett slags ordning på mängden av dem, så att vi kan tala om att en triangel är mindre än en annan, genom att i första hand gå efter längden av hypotenusan och i andra hand efter längden av den kortaste kateten. Detta innebär t.ex. att (12, 16, 20) är mindre än (7, 24, 25) och att (7, 24, 25) är mindre än (15, 20, 25).

1. Visa att de tre minsta pythagoreiska trianglarna, med avseende på denna ordning, är (3, 4, 5), (6, 8, 10) och (5, 12, 13).

En första naiv fråga som man kan ställa sig när det gäller pythagoreiska trianglar är om alla (naturliga) tal kan vara sida i någon sådan. Svaret på denna fråga får ni genom att lösa följande uppgifter.

2. Låt u vara ett udda tal (≥ 3). Visa att det finns ett tal b så att triangeln $(u,\ b,\ b+1)$ är pythagoreisk. Bestäm också sambandet mellan b och u.
3. Låt j vara ett jämnt tal (≥ 4). Visa att det finns ett tal a så att $(j,\ a-1, a+1)$ är pythagoreisk. Bestäm sambandet mellan a och j.
4. Kan 1 eller 2 vara sidor i en pythagoreisk triangel.

Dessa uppgifter visar att alla naturliga tal, utom 1 och 2, kan förekomma som kateter i en pythagoreisktriangel, så att den naturliga följdfrågan är därför om alla tal också kan vara hypotenusor. För att få en idé om svaret på denna fråga bör ni innan ni läser vidare lösa följande uppgift.

5. Det finns 10 pythagoreiska trianglar med en hypotenusa ≤ 29. Bestäm dessa.
   Ledning: Alla utom en av dessa pythagoreiska trianglar kan erhållas med hjälp av de två föregående problemen. Om ni inte kan hitta den sista nu kommer ni säkert att göra det då ni läst lite längre.

Räkning med tal. När vi som barn började med räkning eller matematik i skolan så fick vi börja med att räkna från 1 till 10. Snart fick vi lära oss addera dessa tal och vi fick räkna längre och längre tills vi så småningom fick en känsla av att det fanns (*nästan*?) hur stora tal som helst. Detta innebär att vi hade en aning om mängden $\mathcal{N}$ av naturliga tal. Innan vi kom så långt hade vi ju naturligtvis börjat med subtraktion och som ett resultat av denna började de negativa talen tränga in i vårt medvetande. Vi fick också lära oss multiplikation och även division. I samband med att vi lärde oss multiplikation upptäckte vi också att vissa tal ständigt dök upp i svaren medan andra aldrig gjorde det, vilket förklarades (i samband med divisionen) av att vissa tal hade många delare medan andra hade få eller ibland inga alls. På så sätt fick vi lära oss om primtalen. Sedan visade det sig att division inte alltid gick jämnt upp, så att vi blev tvungna att lära oss att räkna med bråk. Vi lärde oss att multiplicera och dividera bråk, vilket var lätt så snart vi lärt oss att förkorta bråk. Det var svårare att addera och subtrahera bråken och för det tvingades vi lära oss begrepp som *minsta gemensam multipel* och *största gemensamma delare*. En viktig egenskap hos de naturliga talen som vi fick lära oss, men som vi aldrig fick se något bevis för var *satsen om entydig primtalsfaktorisering.*

Efter några år i skolan kunde vi därför handskas med om inte mängderna själva så åtminstone elementen i dem för såväl mängden av alla hela tal **Z** som mängden av rationella tal (kvoterna, **q**uotients) $\mathbf{Q}$. Något senare lärde vi oss funktioner och började därmed lära oss att arbeta med reella tal, och t.o.m. mängder av reella tal. Eftersom vi också fick lära oss att lösa andragradsekvationer så fick vi åtminstone höra talas om det mystiska talet i, d.v.s. kvadratroten ur -1, och om de komplexa talen.

6. Ett komplext tal $z = a + bi$ kan skrivas som $z = r(\cos\theta + i\sin\theta)$, varvid $r = |z| = \sqrt{a^2 + b^2}$ och $\tan\theta = b/a$.

$$\begin{aligned} \text{Om} \quad & z = a + bi = r(\cos\theta + i\sin\theta) \\ \text{och} \quad & w = c + di = s(\cos\varphi + i\sin\varphi) \end{aligned}$$

så är

$$zw = (a + bi)(c + di) = (ac - bd) + (ad + bc)i = R(\cos\psi + i\sin\psi).$$

Bevisa att
(i) $zw = wz$ och att
(ii) $R = rs$ och $\psi = \theta + \varphi$.

På universitetet får man lära sig mer om komplexa tal, men eftersom de oftare förekommer i samband med analys än med algebra, så ägnas *de hela komplexa talen* ingen större uppmärksamhet. Ändå är dessa, mängden av s.k. *Gaussiska heltal*, en både viktig och intressant matematisk struktur. Denna mängd brukar skrivas som $\mathbf{Z}(i)$ för att ange att den innehåller dels mängden av heltal $\mathbf{Z}$, dels talet $i = \sqrt{-1}$. Den grundläggande egenskapen är att $\mathbf{Z}(i)$ är en *Ring* vilket betyder att man kan både addera och subtrahera och dessutom multiplicera två gaussiska heltal med varandra (och resultatet blir på nytt ett gaussiskt heltal). Mängden $\mathbf{Z}(i)$ och operationerna på den definieras på följand sätt:

Låt a, b, c och d vara heltal. Då är $a + bi$ och $c + di$ gaussiska heltal.
Vidare definieras summan och produkten som för vanliga komplexa tal, d.v.s. genom att

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \quad \text{och} \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i. \end{aligned}$$

Innan vi fortsätter kan det vara lämpligt att antyda sambandet mellan gaussiska heltal och det problem som vi egentligen håller på med d.v.s. att på något sätt beskriva mängden av alla pythagoreiska trianglar. Vi ska göra detta genom att införa ännu en tolkning av dessa genom att säga att gaussiskt heltal $z = a + bi$ är pythagoreiskt om $|z|$ $(= \sqrt{a^2 + b^2})$ är ett (vanligt) heltal. Vi kommer i fortsättningen helt enkelt att tala om pythagoreiska tal, varvid det är underförstått att talet är ett (pythagoreiskt) gaussiskt heltal. Detta ger oss tre sätt att uppfatta pythagoreiska trianglar, som trianglar, som taltripplar eller som gaussiska heltal. Vi ska snart se att den algebraiska strukturen hos $\mathbf{Z}(i)$ gör det möjligt att ge en enkel och tilltalande beskrivning av de pythagoreiska *talen*. Eftersom vi inte skiljer på de pythagoreiska tripplarna (a, b, c) och (b, a, c) är det värt att notera att talen $a + bi$ och $b + ai$ ger samma pythagoreiska *triangel*. Dessutom är det praktiskt att även tillåta att *realdelen* och/eller *imaginärdelen* av ett pythagoreiskt tal är negativ. (Om $z = a + bi$, så är realdelen $\Re(z) = a$ och imaginärdelen $\Im(z) = b$.) Sammantaget innebär detta att alla de (vanligen) åtta talen $\pm a \pm bi$ och $\pm b \pm ai$ svarar mot samma pythagoreiska triangel.

De Gaussiska heltalen. Det vi närmast ska ägna oss åt är primtal och primtalsfaktorisering i $\mathbf{Z}(i)$. Vi ska börja med några definitioner.

DEFINITION 1: Om x och z är gaussiska heltal så sägs x vara en **delare** i z om det finns ett gaussiskt heltal y sådant att $xy = z$.

Definition 2: En delare i talet 1 kallas för en **enhet** (i $\mathbf{Z}(i)$).

Definition 3: Två gaussiska heltal x och y sägs vara **associerade** om det finns en enhet ε i $\mathbf{Z}(i)$ så att $x = \varepsilon y$ d.v.s. om kvoten mellan dem är en enhet.

Vi ska använda den vanliga beteckningen $x|z$ för att ange att x är en delare i z. Om $x|z$ och varken x eller $y = z/x$ är enheter så sägs x vara en *äkta* delare.

För att kunna tala om primtalsfaktorisering måste vi naturligtvis först och främst veta vad ett primtal (i $\mathbf{Z}(i)$) är.

Definition 4: Ett gaussiskt heltal p kallas för ett **primtal** (i $\mathbf{Z}(i)$) om det inte har någon äkta delare i $\mathbf{Z}(i)$.

Ett viktigt hjälpmedel för att bevisa satser om naturliga tal är induktionsprincipen, d.v.s. det faktum att en icke-tom mängd av naturliga tal har ett minsta element. Induktionsprincipen kan användas även vid studiet av hela tal eftersom $|n|$ alltid är positivt (eller åtminstone icke-negativt), så att varje mängd av hela tal innehåller något (möjligen t.o.m. 2) tal med minsta belopp. För att på motsvarande sätt kunna använda induktion även vid studiet av $\mathbf{Z}(i)$, så behöver vi en lämplig funktion som till varje gaussiskt heltal tillordnar ett (välvalt) naturligt tal. För detta behöver vi ytterligare ett par nya begrepp.

Definition 5: Om $z = a + bi$ är ett gaussiskt heltal (eller mer allmänt ett komplext tal) kallas talet $z^* = a - bi$ för det **konjugerade talet** till z, eller för z-**konjugat**.

7. Visa att $(z^*)^* = z$ och att $z = xy$ om och endast om $z^* = x^* y^*$.
8. Visa att z är ett (gaussiskt) primtal om och endast om z^* är det.
9. Låt x vara ett gaussiskt heltal och låt n vara ett naturligt tal. Visa att $x|n$ medför att $x^*|n$ och att $n|x$ medför att $n|x^*$.

Definition 6: Om $z = a + bi$ är ett gaussiskt heltal, så kallas talet

$$N(z) = |z|^2 = z^* z = z z^* = a^2 + b^2$$

för **normen** av z.

Anmärkning. Vanligen används ordet norm i modern matematik för något som snarare motsvarar $|z|$ än $|z|^2$ men för gaussiska heltal infördes benämningen redan av Gauss och det har därför förblivit den gängse beteckningen.

10. Visa att $N(z^*) = N(z)$

Eftersom normen av ett gaussiskt heltal alltid är ett naturligt tal så innehåller varje (icke tom) mängd av gaussiska heltal, något element med minimal norm. En annan viktig egenskap framgår av följande uppgift.

11. Visa att normen är *multiplikativ* d.v.s. att $N(zw) = N(z)N(w)$.
    Detta innebär att om $x|z$ i $\mathbf{Z}(i)$, så är $N(x)|N(z)$ i $\mathbf{Z}$.
12. Visa att z är ett primtal i $\mathbf{Z}(i)$ om $N(z)$ är ett primtal i $\mathbf{Z}$.
13. Visa att z är en enhet i $\mathbf{Z}(i)$ om och endast om $N(z) = 1$ och bestäm alla enheter i $\mathbf{Z}(i)$.
14. Visa att om $z \neq 0$ är ett gaussiskt heltal, så finns det någon enhet ε (i $\mathbf{Z}(i)$), sådan att om $w = \varepsilon z$ så är
    (i) realdelen av w positiv, och
    (ii) antingen är beloppet av imaginärdelen *strikt mindre* än realdelen eller så är den *lika med* realdelen (och därmed positiv). Detta innebär att

$$(\star) \qquad -\Re(w) < \Im(w) \leq \Re(w).$$

RITA FIGUR!

(Vi ska säga att ett primtal är skrivet på *normalform* om ($\star$) gäller.)

Innan vi fortsätter ska vi göra en enkel observation som omedelbart kommer att ge oss ett lätt sätt att konstruera pythagoreiska trianglar.

15. Visa att det nödvändiga och tillräckliga villkoret för att ett gaussiskt heltal z ska vara pythagoreiskt är att dess norm $N(z)$ är en jämn kvadrat.

ANMÄRKNING. Detta innebär att om $w = z^2$ så är $N(w) = N(z^2) = N(z)N(z) = N(z)^2$ så att talet w är pythagoreiskt (om det inte är rent reellt eller rent imaginärt).

16. Av de 10 pythagoreiska trianglar med hypotenusa högst 29, som du (förhoppningsvis) hittat, så kan alla utom två erhållas som kvadrater. Bestäm vilka som inte är det.

Den entydiga primtalsfaktoriseringen i $\mathbf{Z}(i)$. Vi ska börja med att formulera och bevisa den lätta delen av satsen om entydig primtalsfaktorisering, nämligen att en faktorisering existerar.

SATS 4. *(Existensen av primtalsfaktorisering.) Varje gaussiskt heltal, som inte är en enhet i $\mathbf{Z}(i)$, kan skrivas som en produkt av primtal.*

BEVIS: Vi ska använda induktion och börjar med att observera att om $N(z) = 2$ så är z ett primtal, helt enkelt därför att om 2 är en produkt av två naturliga tal så måste något av dem vara 1. Vi antar nu att alla gaussiska heltal med en norm som är mindre än n har en primtalsfaktorisering och att z är ett gaussiskt heltal med normen n. Om z är ett primtal så är det sin egen primtalsfaktorisering och då finns det inget mer att bevisa. Om z inte är ett primtal kan vi skriva $z = xy$ där både x och y är äkta delare. Eftersom $N(z) = N(x)N(y)$ (och båda är större än 1) så är $2 \leq N(x) < N(z)$ och $2 \leq N(y) < N(z)$, så enligt antagandet har båda primtalsfaktoriseringar och produkten av dessa är vår sökta faktorisering av z. $\square$

17. Bestäm alla gaussiska heltal med normen 2 och visa att de är associerade.
18. Är 2 ett primtal i $\mathbf{Z}(i)$?

Medan existensen av en primtalsfaktorisering som regel är lätt att bevisa, så brukar entydighet vara ett betydligt svårare problem. Den centrala egenskapen hos primtalen i $\mathbf{Z}$, och som också måste bevisas i $\mathbf{Z}(i)$ är att om ett primtal delar en produkt så delar det också en av faktorerna.

Utgångspunkten för alla undersökningar av entydigheten av faktoriseringen i $\mathbf{Z}(i)$ är följande

SATS 5. *(Divisionsalgoritmen) Om a och b är gaussiska heltal, så finns det gaussiska heltal q och r sådana att*

$$\begin{aligned} &(i) \quad a = bq + r \text{ och} \\ &(ii) \quad 0 \leq N(r) \leq \frac{N(b)}{2}. \end{aligned}$$

Innan vi bevisar divisionsalgoritmen för *gaussiska heltal* kan det vara lämpligt att ge motsvarande sats för (vanliga heltal).

SATS 5'. *(Divisionsalgoritmen) Om a och b är heltal, så finns det heltal q och r sådana att*

$$\begin{aligned} &(i) \quad a = bq + r \text{ och} \\ &(ii) \quad -|b|/2 < r \leq |b|/2. \end{aligned}$$

(Denna sats är självklar om vi helt enkelt väljer q så att $|a - bq|$ blir så liten som möjligt. Rita figur!)

Bevis av divisionsalgoritmen för gaussiska heltal: Vi antar först att talet b är ett naturligt tal, och för att göra beteckningarna klarare ska vi skriva n istället för b. Detta innebär att vi har ett gaussiskt heltal $a = \alpha + \beta i$ och ett naturligt tal n och enligt divisionsalgoritmen för hela tal finns det hela tal q_1, r_1, q_2 och r_2 sådana att $|r_1| \leq n/2$ och $|r_2| \leq n/2$ och dessutom gäller

$$a = \alpha + \beta i = (q_1 n + r_1) + (q_2 n + r_2)i = (q_1 + q_2 i)n + (r_1 + r_2 i) = qn + r.$$

Eftersom vidare

$$N(r) = r_1^2 + r_2^2 \leq 2\frac{n^2}{4} = \frac{n^2}{2} = \frac{N(n)}{2}$$

så gäller satsen i detta fall.

Om nu b inte är ett naturligt tal så börjar vi med att multiplicera både a och b med b^* vilker ger talen $A = ab^*$ och $N = bb^*$. Enligt vad vi nyss såg kan finns q och r' så att

$$A = qN + r' \quad \text{med} \quad N(r') \leq N(N)/2 = N(b)^2/2.$$

Vi kan nu definiera $r = a - bq$ och eftersom

$$r' = (A - qN) = (ab^* - qbb^*) = (a - qb)b^* = rb^*,$$

så är

$$N(r) = \frac{N(r)N(b^*)}{N(b^*)} = \frac{N(r')}{N(b^*)} \leq \frac{N(b)^2}{2N(b)} = \frac{N(b)}{2}. \qquad \square$$

Förutom att den möjliggör induktion är normen användbar också på andra sätt, bl.a. genom att den gör det möjligt att tala om att ett gaussiskt heltal är "större" än ett annat (trots att det egentligen inte finns någon *ordning* i $\mathbf{Z}(i)$). Vi kan därför definiera t.ex. **en största gemensam delare** $\text{sgd}(x, y)$ till två gaussiska heltal x och y som en delare med största möjliga norm. Med hjälp av divisionsalgoritmen kan vi nu bevisa följande viktiga

Sats 6. *Låt a och b vara gaussiska heltal, som inte båda är 0, och låt d vara en största gemensam delare. Då finns det gaussiska heltal x och y sådana att*

$$d = xa + yb.$$

Bevis: Bilda mängden $M = M(a, b)$ av alla gaussiska heltal m som kan skrivas på formen $m = xa + yb$ för något val av talen x och y. Det är lätt att se att varje gemensam delare till a och b är en delare till varje tal i M. Speciellt är d en gemensam delare för hela mängden M. Låt nu $d' = x'a + y'b$ vara något tal i M med den minsta möjliga (strikt positiva) normen. Vi vill bevisa att d' är en delare till alla tal i M och väljer ett godtyckligt $m = xa + yb$ i M. Med hjälp av divisionsalgoritmen kan vi skriva $m = qd' + r$, där $0 \leq N(r) < N(d')$. Då är

$$r = m - qd' = (xa + yb) - q(x'a + y'b) = (x - qx')a + (y - qy')b$$

vilket innebär att $r \in M$. Eftersom enligt förutsättningen $N(d')$ är den minsta möjliga normen, så innebär detta att $N(r) = 0$, d.v.s. att $d'|m$. Eftersom både a och b tillhör M så är d' en gemensam delare till dem, och eftersom d har den största möjliga normen av alla delare så är $N(d') \leq N(d)$. Å andra sidan är d en gemensam delare till a och b, vilket innebär att det finns gaussiska heltal s och t så att $a = sd$ och $b = td$. Men då är

$$d' = x'a + y'b = x'sd + y'td = (x's + y't)d = zd.$$

Detta innebär att $N(d') = N(z)N(d)$ och eftersom $N(d') \leq N(d)$ så är $N(z) = 1$. Detta innebär att $d = z^*d' = (z^*x')a + (z^*y')b$. □

ANMÄRKNING. Av beviset följer att det finns tal x och y sådana att $d = xa + yb$ men beviset ger ingen metod för att hitta varken dem eller den största gemensamma delaren. Det finns dock en *konstruktiv* metod som finns beskriven redan i EUKLIDES ELEMENTA. Enligt denna metod (som brukar kallas *Euklides Algoritm)* konstrueras $\text{sgd}(a, b)$ för två hela tal a och b genom upprepad användning av divisionsalgoritmen. Om vi antar att $|a| > b$ så får vi en följd $r_1 > r_2 > \ldots r_{n-1} > r_n = 0$ genom att

$$\begin{aligned}
r_1 &= a - bq_1 \quad \text{med } |r_1| \leq b/2 \\
r_2 &= b - r_1q_2 \quad \text{med } |r_2| \leq r_1/2 \\
r_3 &= r_1 - r_2q_3 \quad \text{med } |r_3| \leq r_2/2 \\
&\vdots \\
0 = r_n &= r_{n-2} - r_{n-1}q_n.
\end{aligned}$$

Det är uppenbart att processen tar slut efter ett ändligt antal steg. Av konstruktionen följer också att $r_1 \in M$ (där M är mängden av alla $xa + by$).

19. Visa (med induktion) att varje $r_i (\neq 0)$ som erhålles i denna följd är av formen $xa+yb$, där x och y är heltal.
20. Visa att den sista resten r_{n-1} är en gemensam delare till a och b. (Euklides algoritm ger alltså en metod att hitta element av formen $xa + by$ med allt mindre belopp.
21. Visa att Euklides algoritm kan användas även i $\mathbf{Z}(i)$, och att den ger en konstruktiv metod för att hitta den största gemensamma delaren till två givna gaussiska heltal.
22. Bestäm (exempelvis med användning av Euklides algoritm) den största gemensamma delaren till
    a) $21 + 20i$ och $5 + 2i$
    b) $15 + 10i$ och $13 - 26i$
    c) $47 + 4i$ och $26 + 6i$

Därmed är vi färdiga för det viktigaste lemmat i beviset av den entydiga primtalsfaktoriseringen i $\mathbf{Z}(i)$.

LEMMA 1. *Om ett gaussiskt primtal p delar en produkt $z = b_1b_2 \ldots b_n$ så är p en delare i någon av faktorerna b_k.*

BEVIS: Vi ska använda induktion och noterar först att påståendet är trivialt om $n = 1$. Vi antar därför att det gäller för varje produkt med högst $n - 1$ faktorer. Vi sätter $a = b_1b_2 \ldots b_{n-1}$. Om $p|a$ så följer det av induktionsantagandet att p delar någon av faktorerna b_k, $1 \leq k \leq n - 1$ vilket var vad vi ville veta. Vi antar därför att p inte är en delare i a. Eftersom ett primtal inte har några andra delare än enheter och associerade tal (som inte kan vara delare i a) så är 1 en största gemensam delare till a och p. Enligt föregående sats finns det tal x och y sådana att $1 = xa + yp$ vilket innebär att $b_n = 1 \cdot b_n = xab_n + ypb_n$. Enligt förutsättningen är p en delare till båda termerna i högerledet, och därmed också till deras summa, vilket betyder att $p|b_n$. □

Äntligen är vi framme vid den stora satsen.

SATS 7. (ARITMETIKENS FUNDAMENTALSATS FÖR GAUSSISKA HELTAL). *Varje gaussiskt heltal har en primtalsfaktorisering. Denna är entydig bortsett från faktorernas ordning (och förekomst av associerade primtal).*

BEVIS: Eftersom vi redan bevisat existensen behöver vi bara visa entydigheten. Om satsen inte är sann så finns det ett gaussiskt heltal med minimal norm för vilket den inte gäller.

Låt x vara ett sådant tal. Vi antar alltså att $x = p_1p_2\dots p_n$ och $x = q_1q_2\dots q_m$ båda är primtalsfaktoriseringar av x. Eftersom p_1 är ett primtal och dessutom $p_1|x$ så gäller enligt lemma 1, att $p_1|q_k$ för något k, $1 \le k \le m$. Eftersom även q_k är ett primtal så är $q_k = \varepsilon p_1$ där ε är en enhet. Men då är $y = p_2\dots p_n = (\varepsilon q_1)q_2\dots q_{k-1}q_{k+1}\dots q_m$ och efterson $N(y) < N(x)$ så följer det av induktionsantagandet att dessa två primtalsfaktoriseringar av y är lika bortsett från faktorernas ordning, vilket naturligtvis innebär detsamma för faktoriseringarna av x, och därmed har vi fått en motsägelse som bevisar satsen. □

23. Visa att varje gaussiskt heltal z har en kanonisk primtalsfaktorisering av formen $z = \varepsilon p_1p_2\dots p_n$ där ε är en enhet och alla p_k är skrivna på normalform.

Bestämning av primtalen i $\mathbf{Z}(i)$. För att riktigt kunna utnyttja de gaussiska heltalen för att studera pythagoreiska trianglar, räcker det inte med att känna till satsen om entydig primtalsfaktorisering, vi måste också kunna använda den, varmed menas att vi ska kunna utföra en faktorisering.

Om vi förutsätter att vi kan faktorisera naturliga tal (något som vi med en programmerbar fickräknare kan göra åtminstone för tal upp till 100 000) så vill vi om möjligt utnyttja faktoriseringen av $N(z)$ för att faktorisera z. Vi vill alltså veta om en faktorisering av $N(z)$ som en produkt av naturliga tal på något sätt svarar mot en faktorisering av z som en produkt av gaussiska heltal och hur vi i så fall ska använda den. För att se hur detta ska gå till ska vi börja med att bestämma primtalen i $\mathbf{Z}(i)$ (givet de naturliga primtalen).

Vi börjar med att notera att $j_0 = 1 + i$ och alla med detta tal associerade tal är primtal. Det är naturligt att säga att ett gaussiskt heltal är jämnt om och endast om det är delbart med j_0.

24. Bevisa att ett gaussiskt heltal z är jämnt om och endast $s = \Re(z) + \Im(z)$ är ett jämnt heltal.

25. Bestäm alla primtal p i $\mathbf{Z}(i)$, sådana att $0 < \Re(p) \le 5$ och $0 \le \Im(p) \le \Re(p)$. (Det finns 7 stycken.)

Anmärkning. Eftersom $N(1 + i) = 1 + 1 = 2$ så är talet $j_0 = 1 + i$ i och för sig ett specialfall av vår tidigare observation att z är ett primtal (i $\mathbf{Z}(i)$) om $N(z)$ är ett primtal (i $\mathbf{Z}$), men det är samtidigt speciellt eftersom $j_0^* = -ij_0$ så att j_0 och j_0^* är associerade.

Utöver talet $1 + i$ så är alltså alla gaussiska heltal z, sådana att $N(z)$ är ett *naturligt* primtal, primtal i $\mathbf{Z}(i)$. Frågan är om det finns några andra. Låt därför p vara ett primtal i $\mathbf{Z}(i)$, och antag att $N(p)$ *inte* är ett primtal. Vi kan då skriva $N(p) = kl$ varvid vi antar att k är den minsta primfaktorn i $N(p)$. Detta innebär att $N(k) = k^2 \le kl = N(p)$. Nu finns det två möjligheter, för antingen är k ett primtal även i $\mathbf{Z}(i)$ eller så är det inte det. Om k är ett primtal så är det en faktor i antingen p eller p^* och därmed i båda, vilket (eftersom p är ett primtal) innebär att $p = \varepsilon k$ där ε är en enhet och att $N(p) = k^2$ (där k är ett primtal i $\mathbf{Z}$). Om k inte är ett primtal i $\mathbf{Z}(i)$, så innehåller det en primfaktor q, och eftersom q då är en delare i antingen p eller p^*, så är antingen q eller q^* en faktor i p, men eftersom $N(q) < N(k) \le N(p)$ så ger detta en motsägelse mot antagandet att p är ett gaussiskt primtal. Sammanfattningsvis har vi därmed bevisat följande

Sats 8. *Om p är ett Gaussiskt primtal så är $N(p)$ antingen ett primtal eller en primtalskvadrat i $\mathbf{Z}$.*

Därmed har vi återfört problemet att bestämma primtalen i $\mathbf{Z}(i)$ till ett problem för primtal i $\mathbf{Z}$. Det vi gjort är nämligen att uppdela de gaussiska primtalen i två klasser, som exempelvis kan beskrivas av att $p \ne p^*$ (om $N(p)$ är ett primtal) eller $p = p^*$ (annars) och därmed har vi också delat in de vanliga primtalen i två klasser, nämligen dels de som kan faktoriseras i $\mathbf{Z}(i)$, dels de som inte kan det. Frågan är nu om denna uppdelning kan beskrivas på något annat sätt. Vi observerar därför först att om det naturliga primtalet

q innehåller den gaussiska primfaktorn $p = a + bi$ så är $q = N(p) = p^*p = a^2 + b^2$, vilket innebär att q kan skrivas som en summa av två kvadrater. Omvänt är det uppenbart att om $q = a^2 + b^2$ så är $q = (a + bi)(a - bi)$ vilket innebär att q inte är ett gaussiskt primtal. För att bestämma primtalen i $\mathbf{Z}(i)$ så gäller det alltså att ta reda på vilka naturliga primtal som kan skrivas som en summa av två kvadrater. Som ett första steg mot detta noterar vi att om vi bortser från talet 2 är alla naturliga primtal udda, så att om q är en summa av två kvadrater är den ena av dessa jämn och den andra udda. Detta innebär då att q kan skrivas som $(2k)^2 + (2l + 1)^2 = 4k^2 + 4l^2 + 4l + 1 = 4n + 1$. Ett nödvändigt villkor för att q ska kunna faktoriseras i $\mathbf{Z}(i)$ är därför att det är av formen $4n + 1$. Därmed vet vi alltså att alla naturliga primtal av formen $4n + 3$ är primtal också i $\mathbf{Z}(i)$ vilket alltså gäller för talen 3, 7, 11, 19, 23 o.s.v.

Fermats sats. Frågan är nu om alla primtal av formen $4n + 1$ verkligen kan faktoriseras i $\mathbf{Z}(i)$, (d.v.s. skrivas som en summa av två kvadrater) och nu kommer äntligen Fermats sats till användning.

Sats 9. *Varje primtal av formen $4n + 1$ är en summa av två kvadrater.*

Eftersom beviset för denna sats innehåller helt andra begrepp än de som annars ingår i detta specialarbete, så hoppar vi över det.[2] Ett bevis finns i Le Veque [1956, volym I, kapitel 7]. Däremot finns det all anledning att övertyga sig om att satsen förefaller vara sann genom att utföra följande uppgift.

26. Det finns 11 primtal av formen $4n + 1$ som är mindre än 100. Skriv dem som summor av två kvadrater och faktorisera dem i $\mathbf{Z}(i)$.
27. Skriv ett datorprogram som tar reda på om ett givet naturligt tal kan skrivas som en summa av två kvadrater, och på hur många sätt det kan ske. (Kan du se något mönster?)

Kombinerar vi Fermats sats med sats 7 ovan får vi följande beskrivning av primtalen i $\mathbf{Z}(i)$.

Sats 8. *Primtalen i $\mathbf{Z}(i)$ är dels talen $\{\pm 1 \pm i\}$, dels alla tal av formen $\pm a \pm bi$ sådana att $a^2 + b^2 = p$ där p är ett primtal (i $\mathbf{Z}$) av formen $4n + 1$ dels alla tal av formen $i^k p$ där p är ett primtal av formen $4n + 3$.*

Beskrivning av mängden av alla pythagoreiska trianglar.. Med hjälp av sats 8 kan vi nu ge en fullständig beskrivning av mängden av alla pythagoreiska trianglar, genom att ge ett kriterium för när $z = a + bi$ är pythagoreiskt. För att göra det så observerar vi först att varje gaussiskt heltal kan skrivas som ett naturligt tal gånger en produkt av "icke-reella primfaktorer", d.v.s. som $K \cdot (a' + b'i)$ där $(a' + b'i)$ inte innehåller någon "reell" primfaktor. Vi vet att z är pythagoreiskt om $N(z)$ är en jämn kvadrat och eftersom $N(z) = K^2((a')^2 + (b')^2) = K^2 P$ så gäller detta om och endast om $P = (a')^2 + (b')^2$ är en jämn kvadrat. Nu är P en kvadrat om och endast om alla dessa primfaktorer förekommer ett jämnt antal gånger, vilket innebär att $a' + b'i$ är en jämn kvadrat. Sammanfattningsvis ger detta

Sats 9. *Ett gaussiskt heltal z är pythagoreiskt om och endast om det är av formen $N \cdot w^2$ där N är ett naturligt tal och w^2 varken är reellt eller rent imaginärt.*

[2]Fermats intresse för detta problem tycks till stor del ha berott på ett intresse för det vi håller på med i detta specialarbete, nämligen pythagoreiska trianglar. De algebraiska strukturer, *ändlig grupp* och *ändlig talkropp* som beviset bygger på fanns inte utvecklade på Fermats tid. Därför studerade Fermat vissa specialfall av dem, men de satser han bevisade spelade stor roll för de matematiker, främst Lagrange, (1736 1813) och Galois, (1811-1832) som senare utvecklade strukturerna.

Sats 9 är naturligtvis perfekt som beskrivning av mängden och den ger en utmärkt metod för att konstruera pythagoreiska trianglar. Däremot är det inte så lätt att omedelbart besvara frågan om vilka naturliga tal som kan vara hypotenusa eller hur många olika pythagoreiska trianglar, som har en viss hypotenusa. För att ge ett svar på denna fråga (som är en fråga om naturliga tal) så ska vi dela upp de vanliga primtalen i två klasser $\mathcal{P}_1$ och $\mathcal{P}_2$ där den första består av alla primtal av formen $4n+1$ medan den andra består av 2 och alla primtal av formen $4n+3$. Vi har då följande

Sats 10. *Ett naturligt tal H kan vara hypotenusa i en pythagoreisk triangel om och endast om det innehåller någon primfaktor av formen $4n+1$.*
Om $H = K \cdot h$ där $h = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ är produkten av alla primtal av formen $4n+1$ så ges antalet N av olika trianglar med hypotenusan h av formeln

$$N = \frac{\mathcal{P}-1}{2} = \frac{(2k_1+1)(2k_2+1)\dots(2k_n+1)-1}{2}.$$

Bevis: Ett gaussiskt heltal z med beloppet H, d.v.s. normen H^2 kan faktoriseras som

$$z = K(a_1+b_1 i)^{l_1}(a_1+b_1 i)^{2k_1-l_1}\dots(a_n+b_n i)^{l_n}(a_n-b_n i)^{2k_n-l_n},$$

där $a_i^2 + b_i^2 = p_i$, och där $0 \leq l_i \leq 2k_i$. Det finns $\mathcal{P}$ stycken val av talen l_i och alla val utom det där alla $l_i = k_i$ ger ett gaussiskt heltal med imaginärdel $\neq 0$. Om vi sedan påminner oss att z och z^* ger samma triangel, så är det lätt att inse att det totala antalet är $(\mathcal{P}-1)/2$. □

28. Bestäm alla naturliga tal $h < 100$ sådana att det finns mer än en pythagoreisk triangel med hypotenusan h, och bestäm alla de till dessa h hörande pythagoreiska trianglarna.

    Ledning: Det finns fem sådana tal h, tre av dem har två tillhörande trianglar, de övriga har fyra.

29. Bestäm det minsta tal h för vilket det finns fler än 4 pythagoreiska trianglar med hypotenusan h och bestäm de tillhörande trianglarna.

Den inskrivna cirkeln. Om T är en godtycklig triangel så har den som bekant en inskriven cirkel. Medelpunkten för denna kan erhållas som skärningen för triangelns bisektriser. (En bisektris är en linje från ett hörn in i triangeln sådan att vinkeln till båda de bredvidliggande sidorna är lika stora. Rita figur.) Alla tre bisektriserna möts i en punkt, och denna punkt ligger lika långt från alla sidorna. De tre bisektriserna delar därför in T i tre deltrianglar med varsin sida som bas och den inskrivna cirkelns radie som höjd. Eftersom summan av dessa tre trianglars ytor är ytan av den ursprungliga så ger detta att

$$2|T| = r(a+b+c),$$

där $|T|$ är ytan, a, b och c är sidorna och r är den inskrivna cirkelns radie. Det är vanligt att summan $a+b+c$ kallas för $2p$, och då ger ovanstående formel att

$$r = \frac{|T|}{p}.$$

I en rätvinklig triangel (a, b, c) är $2|T| = ab$ och $2p = a+b+c$ så att

$$r = \frac{ab}{a+b+c}.$$

Förlänger vi detta bråk med *konjugatkvantiteten* $a+b-c$ får vi den vackra formeln

$$r = \frac{ab(a+b-c)}{(a+b)^2 - c^2} = \frac{ab(a+b-c)}{2ab} = \frac{a+b-c}{2}.$$

I en pythagoreisk triangel är $a+b-c$ alltid jämnt, så att den inskrivna cirkelns radie är alltid ett heltal. Om $z = a+bi$ är ett gaussiskt heltal i den första kvadranten så ska vi identifiera z med den rätvinkliga triangel som har hörnen i punkterna $0, a, a+bi$.

30. Bestäm den inskrivna cirkelns radie och medelpunkt för alla pythagoreiska trianglar med hypotenusa högst 29.
31. När du bestämde medelpunkterna för cirklarna i de trianglar, som kunde skrivas som jämna kvadrater $A+Bi = (a+bi)^2$ så upptäckte du säkert att medelpunkten var en heltalsmultipel av $(a+bi)$ (exempelvis var $2+i$ medelpunkt i den inskrivna cirkeln i triangeln $3+4i$). Bevisa att detta alltid gäller för sådana trianglar, och bestäm n (som funktion av a och b) sådant att den inskrivna cirkelns medelpunkt i den triangel som ges av $(a+bi)^2$ är $n(a+bi)$. (Härvid förutsättes att såväl $a+bi$ som $a+bi)^2$ ligger i första kvadranten, d.v.s. att $0 < b < a$.)

Som avslutning kan det vara värt att påpeka att det finns andra intressanta egenskaper hos pythagoreiska taltripplar än att hypotenusan är av en speciell form. De intressantaste egenskaperna finns hos de trianglar vars sidor inte innehåller någon gemensam delare större än 1. Sådana trianglar kallas primitiva och ges av alltid av kvadrater i $\mathbf{Z}(i)$.

32. Visa att i en primitiv pythagoreisk triangel är hypotenusan udda, liksom en av kateterna, medan den andra kateten är jämn.
33. Försök att bevisa att i varje pythagoreisk triangel är en av kateterna delbar med 3 och att ytan är delbar med 6.
    bigskip

Litteraturhänvisningar

Lennart Carleson. *Matematik för vår tid.* Stockholm: Prisma 1968

G. H. Hardy & E. M. Wright. An Introduction to the Theory of Numbers. Oxford 1979.

W. J. LeVeque. *Topics in Number Theory, I & II.* Addison-Wesley 1956.

C. Stanley Ogilvy och John T. Andersson. *Talteori för alla.* Prisma 1968.

Hans Riesel. En bok om primtal. Odense 1968.

Frfattarens adress: Matematiska institutionen, Thunbergsvgen 3, 752 38 Uppsala