Per-Eskil Persson

Sophie Germains identitet

Algebraiska förenklingar och faktoriseringar är en del i gymnasiekurserna som kan behandlas på flera intressanta sätt. Ett inslag kan vara att titta bakåt på matematikers arbeten och se hur deras resultat kan komma till användning i nutid.

I Nämnaren 2013:2 behandlade jag i en artikel olika typer av faktoriseringar och jag utgick då från uttrycket x^4+1. Där visade jag hur man i reella tal får identiteten $x^4+1=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$. Men detta är egentligen bara ett specialfall av det som brukar kallas Sophie Germains identitet.

Sophie Germain levde 1776–1831 och hon räknas som Frankrikes första kvinnliga matematiker. Hon levde i en tid då kvinnor inte ansågs kunna förstå matematik och naturvetenskap, inte ens efter revolutionen då jämlikhet var ett slagord. Under sin uppväxt fick hon studera i smyg eftersom hennes föräldrar försökte hindra henne. Men hon hade en oerhört stark drivkraft att lära sig behärska matematiken och lånade bland annat anteckningar från föreläsningar. Hon var i princip helt självlärd, men kom att göra betydande insatser inom talteorin och teorin för elastiska ytor. Hennes brevväxling med den tidens stora matematiker, som Gauss, Lagrange, Legendre och Fourier, var omfattande och hon hade en stor rival i Poisson vad gäller elastiska ytor. Läs mer om henne i exempelvis *Stora matematiker – Från Fibonacci till Wiles*.

Sophie Germain-primtal

En stor utmaning inom matematiken har varit att bevisa Fermats stora sats. Den säger att ekvationen $x^n+y^n=z^n$ inte har några heltalslösningar för x, y och z om $n>2$. För $n=2$ finns det oändligt många lösningar i form av pythagoreiska taltrippler, exempelvis (3, 4, 5), (5, 12, 13) och (20, 21, 29). Germain arbetade under en period mycket med att lägga fram delbevis för Fermats sats, och lyckades också för vissa typer av tal n, speciellt primtal. Fermats stora sats bevisades slutligen i sin helhet av Andrew Wiles 1993.

Ett primtal p som har egenskapen att även $2p+1$ är ett primtal, kallas för ett *Sophie Germain-primtal*. Talet $2p+1$ kallas för ett *säkert primtal*. Talet 2 är ett SG-primtal, eftersom $2\cdot 2+1=5$. På samma sätt är 3 och 5 SG-primtal, men inte 7, eftersom $2\cdot 7+1=15$, som inte är ett primtal. De första SG-primtalen är:

2 3 5 11 23 29 41 53 83 89 113 131 173 179 ...

Germain bevisade att Fermats stora sats var sann för sådana primtal. Hon genomförde även bevis för andra delar av satsen.

Sophie Germain-primtal och säkra primtal har i modern tid fått betydelse för avancerade krypteringssystem, så kallad RSA-kryptering, som använder sig av stora primtal. Speciellt är Cunninghamkedjor av intresse.

Dessa består av en räcka SG- och säkra primtal. En kort sådan är 3, 7 (15 är inget primtal) och en lite längre är 89, 179, 359, 719, 1439, 2879 (5759 är inget primtal). Det sista talet i kedjan är alltså inget SG-primtal. Prova gärna att bilda egna Cunninghamkedjor.

Att förenkla bevis

Så kommer vi då till Sophie Germains identitet, vilken hon utnyttjade i vissa av sina bevis. Den säger att:

$$a^4+4b^4=(a^2+2ab+2b^2)(a^2-2ab+2b^2)=((a+b)^2+b^2)((a-b)^2+b^2)$$

Om man kan skriva om ett uttryck på något av sätten, så kan man utnyttja identiteten för att förenkla bevis. För uttrycket jag inledde med gäller att:

$$x^4+1=x^4+4\cdot(\frac{1}{\sqrt{2}})^4=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1).$$

I följande exempel visas hur identiten används för att primtalsfaktorisera talet 629 och hur uttrycket $x^{36}+64y^8$ kan skrivas om:

$$629=625+4=5^4+4\cdot1^4=((5+1)^2+1^2)((5-1)^2+1^2)=(36+1)(16+1)=37\cdot17$$

$$x^{36}+64y^8=(x^9)^4+4\cdot(2y^2)^4=$$
$$((x^9)^2+2\cdot x^9\cdot2y^2+2\cdot(2y^2)^2)((x^9)^2-2\cdot x^9\cdot2y^2+2\cdot(2y^2)^2)=$$
$$(x^{18}+4x^9y^2+8y^4)(x^{18}-4x^9y^2+8y^4)$$

Har talet 5 en särställning?

Man kan fråga sig hur många primtal det finns som kan skrivas a^4+4b^4, där a och b är naturliga tal. Sophie Germains identitet säger att:

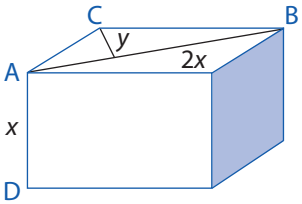
$$a^4+4b^4=(a^2+2ab+2b^2)(a^2-2ab+2b^2)$$

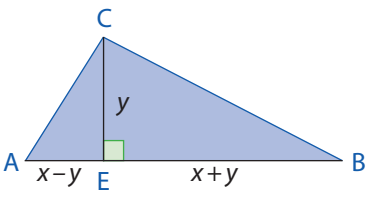
Men om detta är ett primtal måste den minsta faktorn, vilket är den andra parentesen, vara lika med 1. Det kan den bara bli om $b=1$ och $a-b=0$, vilket ger $a=b=1$. Det enda primtalet som kan skrivas så är alltså 5, vilket ger talet en slags särställning.

En läsarutmaning

Följande uppgift återfinns på webbplatsen Brilliant, utan medföljande lösning.

> Ett rätblock har höjden $AD=x$ och diagonalen på ovansidan är $2x$. Halva ovansidan bildar en rätvinklig triangel ABC. Triangelns höjd mot hörnet C är $CE=y$, och den delar AB i två delar, som är $x-y$ respektive $x+y$ långa (se figurerna).





> Bestäm x och y, om man vet att rätblockets volym är 108. Ledning: Sophie Germains identitet är till stor nytta.

En lösning på volymproblemet

Ett förslag på lösning där Sophie Germains identitet används är följande:
Med Pythagoras sats fås att ”lockets” kanter är:

$BC = \sqrt{(x+y)^2+y^2}$ och $AC = \sqrt{(x-y)^2+y^2}$

Rätblockets volym blir då:

$$V = x \cdot \sqrt{(x+y)^2+y^2} \cdot \sqrt{(x-y)^2+y^2} =$$
$$= x\sqrt{((x+y)^2+y^2)((x-y)^2+y^2)}$$

Enligt Sophie Germains identitet får man volymen $V = x \cdot \sqrt{x^4+4y^4}$. Men ABC är en rätvinklig triangel och CE bildar rät vinkel med AB. Det betyder att de två trianglarna CEB och AEC är likformiga.

Alltså har man förhållandet: $\frac{(x+y)}{y} = \frac{y}{(x-y)}$, vilket ger att $x^2 = 2y^2$.

Det medför att $x^4 = 4y^4$ och volymen $V = x \cdot \sqrt{x^4+x^4} = x\sqrt{2 \cdot x^4} = \sqrt{2} \cdot x^3$.

Volymen är enligt förutsättningen 108, vilket ger ekvationen $\sqrt{2} \cdot x^3 = 108$.

Lösningen till utmaningen är att $x = 3\sqrt{2}$ och $y = 3$.

Förslag för undervisningen

Vid arbete med algebraiska förenklingar och faktoriseringar i gymnasiekurserna kan man ge extra uppgifter som innebär användning av Sophie Germains identitet. Här är möjligheterna oändliga.

- När primtal diskuteras kan eleverna söka efter Sophie Germain-primtal och Cunninghamkedjor. Eftersom talen i sådana snabbt kan bli ganska stora, kan man använda funktionen Primfaktorer(*x*) i CAS-delen av Geogebra för att kontrollera om de är primtal. Det går också att använda primtalslistor av olika slag.
- Är talet 5 alltid en faktor till ett av talen i en pythagoreisk taltrippel? Man kan bilda sådana trippler med några enkla formler. Låt $x > y$ vara två heltal. Då bildas en pythagoreisk taltrippel (a, b, c) av:
  $a = x^2 - y^2 \qquad b = 2xy \qquad c = x^2 + y^2$
  Exempel: $x = 8$ och $y = 3$ ger taltrippeln (55, 48, 73).

På sidan 56 i detta nummer finns ett bevis för att minst ett tal i en pythagoreisk taltrippel måste vara delbart med 5.

LITTERATUR

Brilliant (2021). *Sophie Germain identity.* https://brilliant.org/wiki/sophie-germain-identity

Dalmedico, A. D. (2000). Sophie Germain. I E. Picutti m fl, *Stora matematiker – Från Fibonacci till Wiles*, 100–116. Studentlitteratur.

Persson, P-E. (2013). *Visst kan man faktorisera* $x^4 + 1$. Nämnaren 2013:2.