

## Summan av två heltalskvadrater

HANS RIESEL

K T H

**Problemställning.** *Vissa tal kan skrivas som summan av två heltalskvadrater, andra inte!* Så är t.ex.  $13 = 2^2 + 3^2$ ,  $9 = 0^2 + 3^2$  medan  $n = 11$  inte kan skrivas som  $x^2 + y^2$ . Hur kan man övertyga sig om detta senare? Jo undersök vad  $n - x^2$  blir för  $x = 0, 1, 2, \dots$ . Uttrycket blir (fortfarande för  $n = 11$ ) 11, 10, 7, 2,  $-5 \dots$ , alltså aldrig en jämn kvadrat. Eftersom  $y^2$  alltid skall vara  $\geq 0$ , behöver vi tydligen inte gå längre. Egentligen hade vi bara behövt gå tills  $n - x^2 < n/2$ , ty om  $n = x^2 + y^2$ , är minst ett av talen  $x^2$  och  $y^2 \geq n/2$ . (Både  $x^2$  och  $y^2$  kan inte vara  $< n/2$ , ty då skulle ju summan bli  $< n$ .)

**Antalet framställningar.** Du kanske har lagt märke till, att vissa tal kan skrivas som  $x^2 + y^2$  på flera olika sätt, såsom  $25 = 3^2 + 4^2 = 0^2 + 5^2$  eller, tydligare,  $65 = 1^2 + 8^2 = 4^2 + 7^2$ . Man kan fråga sig, på hur många olika sätt ett givet tal kan skrivas som  $x^2 + y^2$ . I detta sammanhang är Lagranges identitet

$$(a^2 + b^2)(c^2 + d^2) = (ac \mp bd)^2 + (ad \pm bc)^2$$

av betydelse.

**En geometrisk tolkning.** En annan fråga är, hur många tal  $\leq N$ , som kan skrivas som  $x^2 + y^2$ . Titta på figur 1. Där ser Du att varje punkt med heltalskoordinater  $(x, y)$ , en s.k. gitterpunkt, i eller på cirkeln  $x^2 + y^2 = N$  med radien  $\sqrt{N}$  motsvarar en framställning av något heltal  $\leq N$  som  $x^2 + y^2$ .

De flesta gitterpunkterna i eller på cirkeln faller i grupper om 8. Om nämligen  $x \neq y$  och även  $xy \neq 0$ , får man ju framställningarna

$$n = (\pm x)^2 + (\pm y)^2 = (\pm y)^2 + (\pm x)^2,$$

som ger sammanlagt 8 olika möjliga framställningar av talet  $n$ . Är  $y = \pm x$  eller  $x = 0$  eller  $y = 0$ , får man endast 4 möjligheter, nämligen

$$n = (\pm x)^2 + (\pm x)^2 \quad \text{resp.} \quad n = (\pm x)^2 + 0^2 = 0^2 + (\pm x)^2.$$

För punkten  $(0, 0)$  slutligen har man den enda framställningen  $0 = 0^2 + 0^2$ .

Nu är antalet gitterpunkter i cirkeln med radien  $\sqrt{N}$  ungefär lika med cirkelns yta  $= \pi N$ . Därför måste det totala antalet framställningar av alla heltal  $\leq N$  som  $x^2 + y^2$  vara ungefär  $= \pi N$ , med ett fel som är av högst samma storleksordning som cirkelns omkrets  $2\pi\sqrt{N}$ . I figuren kan Du se hur enhetskvadraterna, en för varje gitterpunkt i eller på cirkeln, nära täcker över cirkeln.

UPPGIFTEN. Du skall med hjälp av dator undersöka ovan relaterade problemställningar. Skaffa Dig först en överblick över vilka tal  $n$ , som överhuvudtaget kan skrivas som  $x^2 + y^2$ . Till hjälp har Du nedanstående Pascal-program, som gör följande beräkningar: För varje tal  $n$  i ett givet intervall  $(nstart, nslut)$  skrivs talet  $n$  och antalet framställningar  $r(n)$  ut.  $r(n)$  beräknas på samma sätt som i ovan givna gitterpunktsbeskrivning av framställningarna. Vidare beräknas ytan av cirkelringen i vilken gitterpunkterna finns,  $\pi(n + 1 - nstart)$ , vilket skall jämföras med  $\sum_{nstart}^n r(i)$ , för att ge en uppfattning om hur väl gitterpunktsmodellen ovan stämmer. För att Du skall kunna uppskatta avvikelserna från gitterpunktsmodellen, beräknas även differensen, dividerad med  $\sqrt{n}$ . I programmet beräknas vidare, hur stor bråkdel  $f$  av talen i intervallet, som

överhuvudtaget kan framställas som  $x^2 + y^2$ . Slutligen skrivs primfaktoruppdelningen av talet  $n$  ut. — För att spara utskriftsutrymme, hoppas de tal över, som inte kan skrivas som en summa av två kvadrater.

**Några detaljer i datorprogrammet.** Ett sätt att känna igen en jämn kvadrat  $z$  är att undersöka om

$$z = \text{sqr}(\text{trunc}(\text{sqrt}(z) + 0.000001)).$$

(Tillägget 0.000001 har gjorts för att klara av fallet då  $\sqrt{x^2}$  i datorns aritmetik råkar bli en aning under  $x$ , varvid  $\text{trunc}(x)$  skulle ge  $x - 1$  i stället för  $x$ .)

Att hitta alla framställningar av  $n$  som  $x^2 + y^2$ , där  $0 \leq x \leq \sqrt{n/2}$  och  $\sqrt{n/2} \leq y \leq \sqrt{n}$ , görs snabbast genom att skriva

```
for y:=trunc(sqrt(n)+0.000001) downto ymin do ...,
```

där  $ymin = \sqrt{(n/2)}$ , och inte genom satsen

```
for x:=0 to ymin do ...
```

Antalet  $x$ -värden är nämligen ca.  $0.7\sqrt{n}$ , medan antalet  $y$ -värden är endast ca.  $0.3\sqrt{n}$  varför det första sättet går mer än dubbelt så snabbt som det senare.

Uppdelning av talet  $n$  i primtal och tryckning av faktorerna sker med hjälp av proceduren faktor i programmet, som utför ovan beskrivna beräkningar för alla tal  $n$  då  $nst \leq n \leq nsl$ .

```
Program x2y2(input,output);
```

```
Const pi=3.1416;
```

```
Var n,x2,x,r,y,ymin,sum,vx,sn,nst,ns1,n1 : Integer;
```

```
Procedure faktor(n:integer);
```

```

Var g,p,vg : integer;
Begin write(' ');
  while n Mod 2 = 0 do begin write(2:1); n:=n Div 2;
    if n>1 then write('*') end;
  while n Mod 3 = 0 do begin write(3:1); n:=n Div 3;
    if n>1 then write('*') end;
  p:=5; g:=trunc(sqrt(n)+0.000001); vg:=0;
  while p<=g do begin
    while n Mod p = 0 do begin write(p:1); n:=n Div p;
      vg:=1;
      if n>1 then write('*') end;
    while n Mod(p+2) = 0 do begin write(p+2:1);
      n:=n Div(p+2);
      vg:=1; if n>1 then write('*') end;
    p:=p+4; if vg=1 then begin g:=trunc(sqrt(n)+0.000001);
      vg:=0 end;
    end;
    if n>1 then write(n:1)
  end;

Begin
Write('Ge start- och slutvärden för tabellen: ');
read(nst,nsl); writeln;
Writeln(
'   n   r   sum pi(n-n0+1) diff/sqrt(n)   f   n=pqr...');
Writeln; sn:=0; sum:=0;
for n:=nst to nsl do begin
  r:=0; ymin:=trunc(sqrt(n div 2)+0.000001);
  if 2*sqr(ymin){n then ymin:=ymin+1; vx:=0;
  for y:=trunc(sqrt(n)+0.000001) downto ymin do begin

```

```

x2:=n-sqr(y); x:=round(sqrt(x2)+0.000001);
  if x2=sqr(x) then begin vx:=1;
    if (x=0) or (x=y) then r:=r+4 else r:=r+8 end end;
sum:=sum+r; if vx=1 then begin sn:=sn+1; n1:=n-nst+1;
  write(n:7,r:4,sum:7,pi*n1:7:1,(sum-pi*n1)/sqrt(n):12:2);
  write(sn/n1:8:2); faktor(n); writeln; end
end
end.

```

Provkör programmet, och se om Du kan finna några lagbundenheter i de värden som datorn matar ut. Lämpliga testintervall: (1, 400) och (1000, 1200).

Försök svara på följande frågor:

1. Eftersom Lagranges identitet visar, att en produkt av tal, som vart och ett kan skrivas som summan av två kvadrater, självt kan skrivas på detta sätt, kan Du börja med att titta på, vilka *primtal*, som kan skrivas som summan av två kvadrater. Ledning: Om det *udda* talet  $n = x^2 + y^2$ , så måste ett av talen  $x$  och  $y$  vara jämnt och det andra talet vara udda. Antag, att det är  $x = 2x'$  som är jämnt och  $y = 2y' + 1$  som är udda. Vad blir då  $x^2 + y^2 \pmod{4}$ ? Kan Du verifiera detta genom datorkörningar?
2. Trots att primtalen av formen  $4k + 3$  tydligen inte kan skrivas som en summa av två kvadrater, visar datorkörningarna att faktorerna 3, 7, 11, ... ibland förekommer i utskriften. Är det något som skiljer förekomsten av dessa faktorer i utskriften från förekomsten av primfaktorer av formen  $4k + 1$ ? Kan Du förklara fenomenet?
3. Försök nu komma underfund med, hur  $r(n)$  beror på antalet primfaktorer av formen  $4k + 1$  i talet  $n$ . Lämpliga testvärden: 5, 65, 1105, 32045 och dessa tal tagna gånger 2, 4 och 8. Pröva sedan multipla primfaktorer. Testa t.ex. talen 65, 325, 1625 och 8125.

4. Försök att formulera regler som ger  $r(n)$ , om primfaktoruppdelningen av  $n$  antas känd!
5. Som Du kan se av datorkörningarna, ligger värdet av  $\sum r(n)$  över en cirkelring nära cirkelringens yta. Man kan också uttrycka detta så, att den *genomsnittliga storleksordningen* hos funktionen  $r(n)$  är  $= \pi$ , i följande mer precisa formulering:

$$\lim_{n \rightarrow \infty} \frac{r(1) + r(2) + \dots + r(n)}{n} = \pi.$$

Om Du studerar den kolumn i datorutskriften, där skillnaden

$$\left( \sum_1^N r(n) - \pi N \right) / \sqrt{N}$$

har skrivits ut, vågar Du kanske gissa något om storleksordningen på avvikelserna mellan  $\sum r(n)$  och  $\pi N$ ?

6. Undersök nu hur *antalet tal*, som kan skrivas som en summa av två kvadrater, i ett litet intervall kring  $N$  ändrar sig, när  $N$  växer. Lämpliga testintervall: (50, 150), (950, 1050), (9900, 10100), (99800, 100200) o.s.v., så högt upp som Du kan köra. (Hur högt det går beror på vilket värde som `maxint` i Pascal har i Din dator.)
7. Som Du kan se på datorutskriften, så avtar medelvärdet  $f$  för antalet tal långsamt, när  $N$  växer. Kan Du finna någon lag för hur  $f$  avtar? Ledtråd: Eftersom alla tal, som överhuvudtaget kan skrivas som en summa av två kvadrater, har med primtalen av formen  $4k+1$  att göra, kanske det är den minskade primtalstätheten högre upp i talserien, som orsakar att  $f$  minskar, när  $N$  ökar? Avtar möjligen  $f$  i samma takt som primtalen?

Om Du vill veta mer om detta problem kan Du t.ex. läsa

Hardy, G.H., & Wright, E.M., *An Introduction to the theory of numbers*. Fifth edition, Oxford Univ. Press, Oxford 1979, s 241–243, 270–271 och 299–302.

Chandrasekharan, K., *Introduction to Analytic Number Theory*. Springer 1968, s 29.