Bengt Ulin

Primtal

Författaren gör några nedslag bland upptäckter som olika matematiker gjort om primtal och formulerar några av de frågor som lett till dessa upptäckter.

Ett av de viktigaste kapitlen inom aritmetiken handlar om primtal. De har varit och är fortfarande ett motiv för många matematiker att fördjupa kunnandet om.

Primtal och multipler av talet 6

Efter primtalen 2 och 3 följer närmast primtalen 5, 7, 11, 13, 17, 19, 23, 29. Alla dessa har en multipel av 6 som granne, antingen närmast under eller närmast över, nämligen 6, 6, 12, 12, 18, 18, 24 och 30.

Kan det vara så att alla multipler av 6 har ett primtal som granne? Vi utvidgar den nyss angivna raden med 36, 42, 48, 54, 60. Alla dessa tal har ett primtal som granne: 37, 43, 47, 53 och 59. Vi fortsätter med 6-multiplerna 66, 72, 78, 84, 90, 96, 102, 108, 114 och 120. De nio första av dessa tal har primtalen 67, 73, 79, 83, 89, 97, 101, 109 och 113 som granne. Men – vid 120 tar det slut eftersom man har såväl $119 = 7 \cdot 17$ som $121 = 11^2$.

Omvänd fråga

Vi kan omvänt fråga: Har varje primtal p en multipel av 6 som granne? Talet 5 har 6 som granne. Vidare: låt oss säga att vi har $6n < p < 6(n+1)$ för något n-värde ≥ 1. $p = 6n + 2$ är inget primtal eftersom $6n + 2$ är delbart med 2. Av samma skäl är $p = 6n + 4$ inte något primtal. Inte heller kan $p = 6n + 3$ vara ett primtal eftersom p då är delbart med 3. Följden blir att två fall återstår: antingen gäller $p = 6n + 1$ eller $p = 6n + 5$. I båda dessa fall har p en multipel av 6 som granne. Vi kan alltså besvara frågan med JA.

Något om primtalens positioner

Var finns primtalen bland de naturliga talen 1, 2, 3 ...? Om man tar ett stort primtal och sedan tittar på de konsekutiva talen efter detta primtal måste man gå långt tills nästa primtal dyker upp eftersom de konsekutiva talen precis efter primtalen är delbara med faktorerna i talet.

Låt oss bilda talen $1 \cdot 2 \cdot 3 \cdot 5 + 1 = 31$ och $1 \cdot 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Båda dessa tal är primtal. Även talet $1 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ är ett primtal. Som vi ser blir avstånden mellan dessa primtal allt större. Vi kan fråga oss: Kan avstånden bli hur stora som helst?

För att undersöka det bildar vi produkten $N = 2 \cdot 3 \cdot 4 \ldots m$ av alla naturliga tal från 2 till ett stort tal m. Med exempelvis $m = 1000$ kan vi konstatera att alla tal $N + 2, N + 3 \ldots 1000$ kan faktoriseras, nämligen med 2, 3 ... respektive 1000.

Eftersom talet m kan väljas hur stort som helst inser vi att vi kan finna hur många faktoriserbara tal i rad som helst. Det finns alltså hur långa ”öknar” som helst utan primtal.

Några resultat rörande primtal

I boken *Primzahlen* av Ernst Trost finner man många intressanta resultat rörande primtal. Bland dem finns exempelvis:

- Varje naturligt tal har en entydig framställning som produkt av primtal.
- Antalet primtal är oändligt. Detta bevisade redan Euklides i sitt berömda verk *Elementa*.
- Ett udda tal i formen $4m+1$ ($m>0$) är ett primtal om och endast om talet på endast ett sätt kan skrivas som summan av två kvadrattal utan gemensam faktor.
- Varje tillräckligt stort udda tal är summan av tre primtal.
- Särskilt berömda bland primtalen är Fermats primtal: $F_n = 2^{2^n}+1$. För $n=2$ erhåller man talet 17, det berömda tal, om vilket Gauss bevisade att en cirkel kan delas i 17 lika stora delar med de klassiska hjälpmedlen passare och linjal.
- Om både p och $p+2$ är primtal, så har man en så kallad primtalstvilling. Exempelvis är 5 och 7, 11 och 13, 17 och 19 primtalstvillingar. Frågan om det finns oändligt många tvillingpar lär fortfarande vara obesvarad.
- Med framställningarna $6n-1$ och $6n+1$ ($n>1$) kan man visa att det inte finns någon primtalstrilling utöver 3, 5, 7. Man finner att ett av talen $p+2$ och $p+4$ är delbart med 3.
- År 1742 formulerade Christian Goldbach i ett brev till den berömde matematikern Leonhard Euler hypotesen att varje jämnt tal ≥ 4 är summan av två primtal. Trots att hypotesen är enkelt formulerad är frågan om dess giltighet hittills obesvarad.

Ur boken *The man who mistook his wife for a hat*

Oliver Sacks var en världsberömd psykoneurolog bland annat känd från filmen Awakenings. I avsnitt 23 i boken med den märkliga titeln ovan, om mannen som förväxlade sin fru med en hatt, finner man fascinerande ord om tvillingparet John och Michael som Sacks blev bekant med 1966. Tvillingarna var då 26 år gamla och hade fått en diagnos som utvisade autism och någon annan psykisk defekt. De hade stora bekymmer med mycket enkla räkneproblem men ägde trots detta en sällsynt förmåga rörande bland annat primtal. När en ask med tändstickor råkade få sitt innehåll tömt på bordet utbrast tvillingarna samtidigt ”111!”. Sacks kontrollräknade antalet tändstickor och det stämde, 111. Är det då något speciellt med detta tal? Jo, 111 är 3 gånger 37, det vill säga tre gånger ett primtal.

En annan gång då Sacks besökte tvillingarna utväxlade de åttasiffriga tal med varandra. Sacks antecknade talen och kunde väl hemma konstatera att talen var primtal. Tvillingarna kunde senare utvidga sin förmåga till 20-siffriga tal, så stora att Sacks inte på egen hand kunde avgöra om talen verkligen var primtal. Men de var primtal.

Varför primtal?

Primtal kan användas för kryptering. Om man multiplicerar två mycket stora primtal med varandra får man en så stor produkt att det kan vara mycket svårt för en utomstående att finna dess faktorer. Läs mer om primtal och kryptering i *Sophie Germains identitet* och *RSA-kryptering i Ma 5* i detta nummer.

LITTERATUR

Hall, T. (1965). *Gauss, matematikerns konung*. Prisma.
Sacks, O. (1985). *The man who mistook his wife for a hat*. Picador.
Trost, E. (1968). *Primzahlen*. Birkhäuser.