UPPSALA UNIVERSITET
Institutionen för informationsteknologi

NUMERISK TALTEORI

Eva-Lotta Högberg
Daniel Norin
Linn Stengård
Joakim Widén

INLEDNING

Vi skall i detta arbete belysa den numeriska talteorins utveckling under de senaste århundradena samt datorernas och beräkningsalgoritmernas förfining. Detta åstadkoms genom att redogöra för och analysera försöken till bevis till och lösning av fyra talteoretiska problem som alla bygger på primtalsbegreppet; Mersennes tal, Fermats tal, Goldbachs förmodan samt problemet med primtalstvillingar. Ett primtal är som bekant ett tal som endast är jämnt delbart med sig självt och ett. De utgör alla heltals byggstenar på så sätt att man genom multiplikation av entydigt valda primtal kan uttrycka alla heltal. Alla primtal är udda utom talet 2 som också är det minsta primtalet.

Fastän man redan på de gamla grekernas dagar bevisade att antalet primtal är oändligt så har man än idag inte funnit något sätt att representera ett godtyckligt stort primtal. Det vill säga man har inte funnit någon praktiskt användbar formel för vilken man kan sätta in ett godtyckligt tal och få ut ett primtal. För att lära sig mer om primtalens natur och kanske någon gång hitta en allmän formel med vilken man kan uttrycka primtal är det viktigt att finna nya primtal samt studera deras fördelning över tallinjen.

MERSENNES TAL

I försöken att hitta en formel på vilken man kan representera alla primtal ställde munken Marin Mersenne (1588-1648) upp följande formel:

$$M_n = 2^n - 1$$

Det skulle dock visa sig att detta inte var någon allmängiltig formel för primtal. Trots att det är bevisat att om $2^n - 1$ är ett primtal så är också n ett primtal så gäller dock inte det omvända. Det behöver alltså inte vara så att $2^n - 1$ är ett primtal även om n är det. Men fastän Mersenne misslyckades i sin egentliga föresats så lever formeln kvar. Detta då det visade sig att av de kända formerna för primtal är denna den på vilken man lättast kan bevisa att ett, mycket stort, tal

är ett primtal.[1] Följaktligen är det också tal av denna typ som ligger högst på listorna över de största kända primtalen. Detta trots att det egentligen rör sig om ganska liten andel av de tal som man kan representera på formeln $2^n - 1$ som verkligen är primtal. Man känner idag endast 39 stycken tal på formen som är primtal!

Letandet efter Mersennetal är också kopplat till en annan del av talteorin, sökandet efter så kallade *perfekta tal*. Ett perfekt tal är det som är lika med summan av sina delare, det vill säga de tal som delar talet utan rest. Exempelvis så är 6 det första perfekta numret då dess delare 1, 2 och 3 blir talet 6 vid addition. Nästa är 28 = 1 + 2 + 4 + 7 + 14. Sedan blir steget längre, de två efterföljande är 496 och 8128. I partiellt faktoriserad form blir dessa

$$2 \cdot 3,\ 4 \cdot 7,\ 16 \cdot 31 \text{ och } 64 \cdot 127.$$

Om man tittar lite närmare på de perfekta talen inser man att alla kan skrivas på formen

$$2^{n-1}(2^n - 1).$$

I vart och ett av dessa fall är också $2^n - 1$ ett Mersenneprimtal. Det går att bevisa att ett jämnt tal är ett perfekt tal om och endast om det kan skrivas på formen

$$2^{n-1}(2^n - 1)$$

och $2^n - 1$ är ett primtal.

FERMATS TAL

Pierre de Fermat levde under 1600-talet i Paris där han livnärde sig som juridisk ämbetsman. Hans stora intresse var matematik och han korresponderade med flera av dåtidens stora matematiker som Carcavi, Huygens och Mersenne. Här ska vi titta närmare på ett av de problem som även Fermat funderade över;

[1] Beviset går ut på att man gör det s.k. Lucas-Lehmertestet där man kan sluta sig till att M_n är ett primtal om och endast om det delar u_{n-2} jämnt, där $u_0 = 4$ och $u_i = u^2_{i-1} - 2$.

nämligen om och i så fall hur man ska kunna finna en allmängiltig formel för primtal. Fermats förslag på lösning av problemet formulerade han så här:

$$F_n = 2^{2^n} + 1$$

Enligt Fermat skulle alla lösningar till formeln vara primtal. För n = 0, 1, 2, 3, 4, 5, 6 är Fermattalen 3, 5, 17, 257, 65537 och 4294967297. Som synes blir Fermattalen stora redan vid små värden på n. Därför har man inte kunnat bevisa särskilt många Fermattal. Den schweiziske matematikern Leonhard Euler var 1732 den förste att motbevisa Fermats anmodan då han fann faktorn

$$641 = 5 \cdot 2^7 + 1$$

i F_5. F_5 var alltså ej något primtal.

Sedan Eulers tid har man med olika metoder försökt att finna ytterligare F_n, något som visat sig vara en tuff utmaning. 1880 fick Landry fram

$$F_6 = 274177 \cdot p$$

(p = primtal med 14 decimalsiffror) men för ytterligare framgångar krävdes datorer och effektivare algoritmer. Fördelen vid datorexperimenterande är att Fermattal representeras som enkla binära tal. De börjar alltid med en etta som följs av nollor för att sedan återigen avslutas med en etta. Med hjälp av datorer är det enkelt att empiriskt undersöka förekomsten av primtal skrivna på binär form. 1970 tog Morrison och Brillhart fram faktorerna i F_7 Sedan följde (med olika metoder) F_8 1980, F_{11} 1988, F_9 1990, F_{10} 1995. F_{12} till F_{22} har man också försökt lösa.

Fram till 1999 kände man dock fortfarande inte till något primtal större än F_4 vilket ger grund för en argumentation för att det enbart finns ett begränsat antal F_n som är primtal. Det minsta Fermattal som man fortfarande inte lyckats faktorisera fullständigt är F_{12} som man vet består av minst sju primtal.

GOLDBACHS FÖRMODAN

Vi har redan berört att primtalen är de hela talens byggstenar i meningen att alla heltal kan uttryckas som produkter av ett antal primtal. För varje heltal går det alltså att hitta ett entydigt antal primtalsfaktorer som via multiplikation bygger

upp talet. Kan vi på liknande vis göra en uppdelning med avseende på addition, eller med andra ord: är det möjligt att uttrycka alla heltal som en addition av ett antal primtal? Det är lätt att inse att det för ett godtyckligt tal alltid går att hitta sådana primtal om vi får välja hur många som helst. Den relevanta frågan är snarare *hur många* primtal som behövs. Svaret på detta problem anses sammanfattas i *Goldbachs förmodan*, som egentligen består av *två* hittills obevisade påståenden.

Goldbachs förmodan i dess ursprungliga form uttrycks i ett brev från Christian Goldbach till Leonhard Euler 1742. Goldbach skriver där att varje heltal kan skrivas som summan av tre primtal. Man kan då göra påståendet att *varje jämnt heltal är summan av två primtal*, och det är det påståendet, vanligen benämnt ”the Binary Goldbach Conjecture”, som oftast avses då man talar om Goldbachs förmodan. När vi i fortsättningen talar om Goldbachs förmodan är det detta vi hänvisar till. Det andra, svagare påståendet säger att *varje udda heltal är summan av tre primtal,* vilket allmänt kallas för ”the Ternary Goldbach Conjecture”. Bilaga 1 visar de största och minsta primtal som behövs för att additivt bygga upp de första 24 heltalen. Det visar sig att för allt större heltal blir möjligheterna att kombinera ihop två primtal i summan större. Exempelvis kan talet 100 byggas upp av 6 olika par av primtal. Alltså bör det för större heltal bli mer sannolikt att Goldbachs förmodan är riktig.

Arbetet med att bekräfta riktigheten i Goldbachs förmodan har länge utförts utifrån två angreppssätt. Dels görs försök att utarbeta ett strikt matematiskt bevis för påståendet, vilket visat sig vara mycket svårt. Dels görs försök att verifiera det för allt större tal, något som underlättats i hög grad av de ökade möjligheterna att utföra avancerade datorberäkningar. När det gäller bevisen har inget fullständigt sådant framkommit, men man har kommit en bit på väg. Under förutsättning att den så kallade Riemannhypotesen (en annan talteoretisk förmodan som anses vara riktig) är sann så är ”the Ternary Goldbach Conjecture” bevisad. Ett steg mot ett bevis för den starkare förmodan togs 1973 då det bevisades att varje tillräckligt stort jämnt heltal kan skrivas som en summa av ett primtal och ett annat tal som antingen är ett primtal eller en

produkt av två primtal. Det har även bevisats att varje jämnt tal är summan av högst 18 primtal.

Den verifierande sidan av verksamheten har rönt större framgångar på senare år. Bilaga 2 visar tillsammans med tidsangivelser de största tal *k* sådana att Goldbachs förmodan visat sig stämma för tal mindre än *k*. De höga siffrorna för senare år är en produkt av den accelererande datorkapaciteten. Det senaste stordådet utfördes av Jörg Richstein, vars verifiering vi skall undersöka lite närmare. Att verifiera Goldbachs förmodan för stora tal innebär vissa praktiska problem. Ett stort intervall kräver på grund av minneshanteringen uppdelning i mindre delar på vilka de möjliga primtalskombinationerna sedan testas. Richsteins program höll för varje heltal också reda på det minsta primtalet i summan. Arbetet delades upp på femton olika datorer: sju Sun Ultra1- och sex Sun4-workstations tillsammans med två Linuxbaserade PC-datorer. Ändå tog beräkningarna lång tid: hela 130 dagar med processerna lågprioriterade i bakgrunden krävdes för att slutföra verifieringen.

PRIMTALSTVILLINGAR

De primtal som dyker upp som par av på varandra följande udda heltal, exempelvis 3 och 5, 5 och 7, 11 och 13, 17 och 19, kallas primtalstvillingar. Alla dessa kan skrivas på formen $6 \cdot k +/- 1$. Liksom alla andra mönster som kan skönjas bland primtalen så har dessa tvillingar länge rönt stort intresse bland matematiker och anses idag vara ett av de mest betydelsefulla olösta problemen inom talteorin.

Trots att många har ägnat mycket tid åt att studera detta fenomen har ingen ännu kunnat bevisa det som är den stora frågan angående primtalstvillingarna – nämligen om det finns oändligt många eller inte. Euklides fastslog som tidigare nämnts med ett enkelt bevis att det finns oändligt många primtal. Att sedan bevisa att det även finns oändligt många primtalstvillingar verkar inte vara mycket svårare, men ändå har ingen lyckats! Författarna av två artiklar från 1964[2] respektive 2001[3] uttrycker samma sak; det tycks ju så lätt och ändå har

[2] Stanislaw Ulam ”Computers” *Scientific American* 1964

ingen lyckats! Matematikerna verkar dock överens om att det faktiskt finns oändligt många, för ingen har ju heller lyckats bevisa det motsatta.

Då man inte har lyckats formulera något matematiskt bevis för att det finns oändligt många primtalstvillingar arbetar man liksom när det gäller andra former av primtal med att verifiera teorin för allt större tal. Som hjälp i jakten på allt större primtal och primtalstvillingar har man idag datorer och man slår ständigt nya rekord. På 80-talet påbörjades en lista över ”titanic primes” med 1000 eller fler siffror och de som bevisade att dessa existerade fick titulera sig ”titans”. Listan var från början inte lång, men idag känner man till tiotusentals titaniska primtal och man talar även om gigantiska och megastora primtal. Det största kända tvillingparet idag (eller i alla fall i somras) är

$$318032361 \cdot 2^{107001} +/- 1.$$

Dessa tal har 32 220 siffror och hittades i år av ett team lett av Jörg Richstein. Rekordet på antalet funna par av ett och samma team låg i juni på 8 494 836 459 690 stycken och de största var då i storleksordningen $1 \cdot 10^6$ och att finna alla dessa tog bara två år, något som ansågs vara en relativt kort tid i sammanhanget.

Något som skiljer primtalstvillingarna från de andra primtalen är det faktum att summan av deras inverser ((1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/13)) konvergerar till ett känt tal som kallas Bruns konstant. Den är idag fastställd till 1.9021605820 +/– 0.0000000024. Om denna summa hade divergerat liksom summan av alla primtals inverser gör, så hade det varit ett bevis för primtalstvillingarna är oändligt många, men nu är inte så fallet. Arbetet med att finna allt större tvillingar och att slå allt fler rekord fortsätter dock.

”Twin primes continue to fascinate.”[4]

AVSLUTNING

Trots problemens skenbara trivialitet och trots beräkningsalgoritmernas utveckling och datorernas exponentiellt ökande kapacitet så har man ännu inte lyckats fullständigt bevisa de olika problemens förmodade lösningar. Men ju

---

[3] Ivars Peterson ”Prime twins” *Science News Online* www.sciencenews.org/20010602/mathtrek

[4] Peterson

större beräkningar man klarar av att göra desto större tal kan man verifiera att teorierna stämmer för. Då blir också sannolikheten hos teorierna allt större, medan även lösningar som falsifierar felaktiga teorier lättare kan finnas.

EXTRA! EXTRA!

Efter detta arbetes slutförande har stora händelser skett i primtalsvärlden. Mersennetal nummer 39, $2^{13466917} - 1$, upptäcktes alldeles nyligen av organisationen GIMPS, Great Internet Mersenne Prime Search. Organisationen är uppbyggd av medlemmar som via Internet kopplat ihop sina datorer till ett distribuerat nätverk. Detta skapar en datorkraft som är mycket stor och följaktligen så står organisationen registrerad för de hittills fem största kända primtalen.

REFERENSER

Brent, Richard P, ”Factorization of the tenth fermat number”, *Mathematics of computation*, volume 68, number 225. 1999 American Mathematical Society.

Colqiutt, W.N. och Welsh, L Jr., ”A new Mersenne prime”, *Mathematics of computation*, volume 56, number 194. 1991 American Mathematical Society.

Peterson Ivars, ”Prime Twins” *Science News Online* www.sciencenews.org/20010602/mathtrek.asp

Richstein, Jörg, ”Verifying the Goldbach Conjecture up to $4*10^{14}$”, *Mathematics of Computation*, volume 70, number 236. 2000 American Mathematical Society.

Ulam, Stanislaw M, ”Computers”, *Scientific American*, nr 9 1964.

Singh, Simon, *Fermats gåta*, pan 1997.

www.aalkat-gym.dk/UV/MFK/tal/fermat.html, Aalborg Katedralskoles websida, december 2001.

www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html, School of Mathematics and Statistics University of St Andrews, Scotland, december 2001.

www.mathworld.wolfram.com/GoldbachConjecture.html, 2001.

www.sciencenews.org, Science news websida, december 2001

www.utm.edu/research/primes, Prime pages websida december 2001

BILAGA 1

De tal *k* sådana att Goldbachs förmodan verifierats för alla heltal < *k*.

k	År
1×10^4	1885
1×10^5	1938
1×10^8	1965
2×10^{10}	1989
4×10^{11}	1993
1×10^{14}	1998
4×10^{14}	2001

BILAGA 2

De jämna heltalen mellan 4 och 50 uttryckta som summan av två primtal. De största respektive minsta möjliga primtalen har använts i varje summa.

2	+	2	=	4
3	+	3	=	6
3	+	5	=	8
3	+	7	=	10
5	+	7	=	12
3	+	11	=	14
3	+	13	=	16
5	+	13	=	18
3	+	17	=	20
3	+	19	=	22
5	+	19	=	24
3	+	23	=	26
5	+	23	=	28
7	+	23	=	30
3	+	29	=	32
3	+	31	=	34
5	+	31	=	36
7	+	31	=	38
3	+	37	=	40
5	+	37	=	42
3	+	41	=	44
3	+	43	=	46
5	+	43	=	48
3	+	47	=	50