FAKULTETSOMRÅDET FÖR
NATURVETENSKAPER OCH TEKNIK

PRO GRADU-AVHANDLING

Elementära bevis för primtalens egenskaper

Skribent:
Marius KRAUFVELIN,
37919

Handledare:
Anne-Maria
ERNVALL-HYTÖNEN

2020

Sammanfattning

I denna avhandling studerades primtalens egenskaper. Syftet med avhandlingen var att belysa och bevisa dessa egenskaper. Här användes endast elementära bevis, vilket inte betyder att bevisen är enkla utan att de saknar komplex analys. Arbetet begränsades till talteoretiska satser med betoning på primtal, d.v.s. heltal som endast är delbara med sig själva och med 1. Primtalen är oändliga och de fascinerade redan matematiker i antikens Grekland. Det söks än idag efter allt större primtal.

I inledningen berättades i korthet om personerna bakom denna matematik, i synnerhet om Paul Erdös, som bland annat står bakom det mest kända beviset till Bertrand-Tjebysjovs sats. Dessutom gavs definitionen på ett Erdöstal. I Förkunskaper behandlades klassisk matematik, Bezouts identitet (som bygger på de diofantiska ekvationerna, d.v.s. klassisk matematik) och Fermats lilla sats. Det redogjordes för aritmetikens fundamentalsats (som visar att varje heltal har en entydig primtalsuppdelning). Även Erasthosthenes såll, som var den första metoden som avgjorde vilka tal som är primtal eller inte, omnämndes.

Det finns tre centrala satser angående primtal i gradun. Den första är Bertrands postulat (eller Bertrand-Tjebysjovs sats) som säger att det alltid finns åtminstone ett primtal p mellan ett godtyckligt heltal n och $2n$. Den andra är en utveckling av Bertrands postulat som visar att detta också gäller i intervallet mellan $2n$ och $3n$. Den tredje viktiga satsen är primtalssatsen som stipulerar att det existerar en precis asymptotisk formel som visar att antalet primtal mindre än ett godtyckligt tal x är approximativt lika med $\frac{x}{\ln x}$ för stora x. Av dessa tre viktiga resultat vad gäller primtal fascinerade i synnerhet primtalssatsen många matematiker, och det har krävts flera försök av flera olika matematiker innan den kunnat bevisas.

Metoden i avhandlingen var, förutom att räkna och bevisa, att använda sig av det matematiska programpaketet Mathematica, där det kodats fram en lista på de första primtalen, samt en figur som visar de 1 000 första primtalen. I kapitlet om hjälpsatserna till Bertrands postulat tillämpades (och det finns dessutom en figur över) Pascals triangel, som var mycket användbar vid bevisandet. Det finns även ett extra kapitel som kort behandlar övriga talteoretiska satser, bl.a. det

matematiska problem som anses vara det svåraste av dem alla, men som har blivit löst, Fermats stora sats.

I avslutningen redogjordes för lite extra information om de viktiga satserna och deras tillämpningar. Den mest intressanta egenskapen för primtalen är att de alltid finns åtminstone relativt nära varandra, vilket också var den huvudsakliga slutsatsen för detta arbete. Det finns mycket i matematiken kvar att upptäcka, så även i talteorin. Även om primtalens egenskaper numera är (relativt) välkända, finns det än idag ännu flera talteoretiska satser som inte blivit bevisade eller motbevisade.

Innehåll

Kapitel 1

Inledning

Denna magistersavhandling berör flera upptäckter inom talteorin, som enligt mig är den mest intressanta grenen inom universitetsmatematiken.

Matematiken är egentligen ett eget språk, och med hjälp av universella formler och beteckningar kan matematiker från hela världen kommunicera, och ibland t.o.m. samarbeta, med varandra utan att ens ha något gemensamt språk.

Att ett bevis är elementärt behöver inte betyda att beviset är enkelt utan man brukar säga att ett bevis i analytisk talteori är elementärt om det inte innehåller komplex analys. I själva verket kan alltså ett elementärt bevis vara svårt.

Avhandlingen handlar främst om talteoretiska satser med bevis, inklusive tillhörande hjälpsatser.

Ett viktigt tema som tas upp är Bertrands postulat, som säger att det för varje heltal $n > 3$ finns åtminstone ett primtal p som uppfyller $n < p < 2n$. [1] Postulatet formulerades 1845 av den franske matematikern Joseph Bertrand (1822-1900). Förutom matematiker var Bertrand professor i fysik och matematisk fysik, specialiserad på termodynamik. Dessutom var han även känd för att främja matematiken och matematiker, och han blev medlem av såväl den franska vetenskapsakademin som den litterära franska akademin. [2]

Efter att Bertrands postulat beskrivits och bevisats, utvecklas satsen ännu vidare. Denna upptäckt är relativt ny, och är samtidigt ett ypperligt bevis på att det upptäcks nya saker inom matematiken än idag, eller åtminstone i vår tid, bland matematiker i hela världen. Många icke-matematiker tror att all, eller åtminstone all väsentlig matematik, redan är upptäckt för länge sedan, men utvecklingen av Bertrands postulat bevisades av Mohamed El Bachraoui så sent

som 2006.

Bertrands postulat bevisades dock redan 1850 av ryssen Pafnutij Tjebysjov (1821-1894), och därför går postulatet även under namnet Bertrand-Tjebysjovs sats. Ryska namn kan dock transkriberas på många olika sätt beroende på språk. Oftast är det den engelska varianten Chebyshev som används, men jag håller mig till den officiella svenska transkriberingen, alltså Tjebysjov. [3]

Sannolikt diskuterade Bertrand och Tjebysjov satsen med varandra, eftersom Tjebysjov kunde franska samt besökte Frankrike flera gånger, och de träffade t.o.m. varandra. [3]

Det var i talteori, sannolikhetslära och matematisk statistik som Tjebysjov gjorde sina mest kända upptäckter. Han hör till de mest kända ryska matematikerna, och han är speciellt känd för sin olikhet som är mycket viktig i sannolikhetsläran:

Definition 1.1. *Tjebysjovs olikhet.*

Låt X vara en stokastisk variabel med väntevärdet μ och standardavvikelsen σ (och variansen σ^2). Då gäller att sannolikheten, alltså $P\ |X - \mu| \geq k\sigma \leq \frac{1}{k^2}$ för alla $k > 0$.

Det kan alternativt formuleras P $|X - \mu| \geq a \leq \frac{\sigma^2}{k^2}$ för alla $a > 0$. Olikheten gäller oavsett vilken sannolikhetsfördelning den stokastiska variabeln X följer.

Det mest kända beviset, som samtidigt också är ett elementärt bevis, och betydligt enklare och mer välkänt än Tjebysjovs bevis, är utfört av den ungerske matematikern Paul Erdös (1913-1996). Beviset som används i detta arbete baserar sig på Erdös bevis, som hittas på nätet i sin originalform skrivet på tyska. [4] Erdös var bara 18 år gammal när han 1931 bevisade och 1932 publicerade detta.

Ett primtal är ett tal som endast är delbart med sig självt och med 1. Många grekiska vetenskapsmän kände till deras existens redan för ca 2 500 år sedan. De visste exempelvis med säkerhet att 2 är det enda jämna talet som är ett primtal. En ”gammal grekisk” metod är Erasthosthenes såll. Genom att stryka alla tal som är delbara med 2 (d.v.s. alla jämna), delbara med 3, delbara med 5, 7 osv kunde Erasthosthenes avgöra vilka tal som var primtal eller inte. Ingen vet hur långt han avgjorde detta, men garanterat undersökte han åtminstone de hundratals första talen eftersom Erasthosthenes såll kan användas för godtyckligt stora tal. Grekerna kunde också bevisa att det finns oändligt många primtal.

Erdös visade väldigt tidigt begåvning i och intresse för matematik. Bägge hans föräldrar var matematiklärare och de hade väldigt tidigt introducerat honom till ämnet, långt innan han började skolan. Han var son till två judiska ungrare, och hans pappa dog i förintelsen. Själv hade han lyckats emigrera till Storbritannien och senare USA, och han bodde även största delen av sitt liv utanför Ungern. Även om han aldrig avsade sig sitt ungerska medborgarskap såg han sig som en världsmedborgare, vilket han också sade när han t.o.m. erbjöds ett israeliskt medborgarskap. Han bodde aldrig längre tider på samma plats. Så gott som alla timmar han var vaken ägnade han sig åt matematik. Han är känd för sina talteoretiska upptäckter i allmänhet och för sina utvecklingar av primtalssatsen i synnerhet, men han bidrog till det mesta som behandlas i universitetsmatematiken, d.v.s. även till matematisk analys, grafteori, kombinatorik, approximationsteori, mängdlära och sannolikhetslära. Han har författat mer än 1 500 vetenskapliga artiklar. Leonhard Euler (1707-1783) är den enda matematikern som överträffat detta. Det finns även Erdöstal, Erdös själv är den enda som har Erdöstalet 0, och de personer som har Erdöstalet 1 är sådana som har samarbetat med Erdös, de som har Erdöstalet 2 har samarbetat med någon som har samarbetat med Erdös, o.s.v. I och med att det gjorts väldigt många tvärvetenskapliga arbeten finns det också väldigt många icke-matematiker med ett lågt Erdöstal. Han trodde själv mycket på tvärvetenskap, och han arbetade även med unga förmågor, t.o.m. med barn. [5] Han hade en speciell humor, exempelvis ett eget matematiskt språk där han t.ex. kallade barn för epsilon som man i matematiken kallar godtyckligt små tal, och kallade exempelvis sin enda publikation på ryska (hans kunskaper i det var i det närmaste obefintliga, han levde inte många år i Ungern under östblockets tid) skämtsamt för det ryska pappret [6]. Han pratade förutom ungerska även flytande engelska, tyska och franska och hade även lärt sig latin och klassisk grekiska, vilket säkerligen gjorde det lätt för honom att såväl arbeta som umgås med matematiker från nästan hela världen. [7]

Han fortsatte att umgås i matematikkretsar samt med att delta på konferenser så länge han levde, och han dog 83 år gammal av en hjärtattack mitt under en konferens i Warszawa. [5]

Peter Frankl (född 1953) är en ungersk matematiker som är verksam i Japan sedan 1988. Han skrev hela sju vetenskapliga artiklar tillsammans med Erdös. Han forskar främst inom kombinatorik och mängdlära. Han är mycket språkkun-

nig och talar bl.a. svenska. [8]

I kapitel 2 behandlas förkunskaper och delbarhetssatserna, och mycket av detta är sådant som inte direkt anknyter till bevisen men som kan hjälpa till för att förstå dem. I kapitel 3 behandlas hjälpsatserna till Bertrands postulat, och i kapitel 4 själva postulatet, baserat på Erdös bevis. I kapitel 5 behandlas en utveckling av Bertrands postulat, som redan nämndes, och i kapitel 6 behandlar jag primtalssatsen, som är en mycket viktig sats i talteorin. Den visar hur tätt primtalen ligger, och det var många matematiker som bidrog till att bevisa detta. Flera matematiker har funderat över primtalssatsen ända sedan 1700-talet, men den som slutgiltigt elementärt bevisade den år 1948 var den norske matematikern Atle Selberg (1917-2007). Den hade dock blivit bevisad komplext redan 1896.

Kapitel 2

Förkunskaper

Här behandlas sådant som inte direkt finns med i de viktiga satserna, men som kan hjälpa till för att förstå dem samt bevisen till dem.

Lemma 2.1. *Om p är ett primtal och n är ett positivt heltal, definieras exponenten av p i n som det största naturliga tal k, för vilket $p^k \mid n$, alltså för vilket p^k delar n. Alltså, om m och n är positiva heltal, gäller det att exponenten, som betecknas $l_p(mn)$, $l_p(mn) = l_p(m) + l_p(n)$ och om $m \mid l$ gäller dessutom att $l_p(\frac{m}{n})$ $= l_p(m) - l_p(n)$.*

Lemmat följer från aritmetikens fundamentalsats. Den säger att alla heltal större än 1 kan delas upp i primtalsfaktorer, och primtalsuppdelningen är entydig för varje tal oavsett om talet är ett primtal eller inte. I beviset av primtalsfaktoriseringen används Bezouts identitet. Denna olikhet upptäcktes av den franske matematikern Étienne Bézout (1730-1783) även om liknande resultat som Euklides algoritm och de diofantiska ekvationerna var kända redan i den grekiska världen under antiken. (Såväl Euklides som Diofantos levde i Alexandria i dagens Egypten på 300-200-talet f.Kr respektive 200-talet e.Kr).

Lemma 2.2. *Bézouts identitet. Om två heltal a och b har en största gemensam delare c, går det att hitta sådana heltal x och y att $ax + by = c$ där c är det minsta positiva heltalet som skrivs på formen $ax + by$. Talen x och y kan sedan beräknas med hjälp av Euklides algoritm.*

Bevis. a och b är olika noll, och då betecknas mängden med $ax + by$, och det krävs att $ax + by > 0$ och att x och y är heltal. Då är mängden icke-tom och har ett minsta element enligt välordningsprincipen, som kan kallas c, där $c = as + bt$.

För att visa att c är SGD (största gemensamma delare), eller GCD (greatest common divisor), tas också ett tal $d \leq c$.

Via divisionsalgoritmen fås då att $a = cq + r$ då $0 \leq r < c$. Resten, r, är då i mängden eller i nollan för $r = a - qc$, dvs $a - q(as + bt)$, som är $a(1 - qs) - bqt$. Då c är det minsta positiva heltalet i mängden, som kan kallas S, är det klart att $r = 0$ måste gälla, för c delar a, och c delar även b.

Antag att d är en gemensam delare till både a och b. Då finns det tal u, v i en annan mängd, som kan kallas Z, så att $a = du$ och $b = dv$. Då fås att $c = as + bt = dus + dvt = d(us + vt)$, så d är en delare till c och då gäller att $d \leq c$. □

Sats 2.3. *Aritmetikens fundamentalsats. Varje heltal har en primtalsuppdelning som är entydig så när som på funktionens ordning.*

Bevis. Först bevisas existensen av primtalsuppdelningen. Använder beteckningen A = mängden av alla positiva heltal som har en primtalsfaktorisering. Sedan görs ett motsägelsebevis; antag att A inte är mängden av alla positiva heltal. Då finns det positiva heltal som inte tillhör A. Då tillhör dessa tal en annan mängd, som kan kallas B.

Enligt välordningsaxiomet gäller det att varje icke-tom mängd av positiva heltal innehåller ett minsta element, som kan betecknas m. Då kan inget element i mängden B vara ett primtal. Då m inte är ett primtal så kan det skrivas som en produkt av två mindre positiva heltal p och q.

Då finns det två alternativ; antingen är p ett element i B eller så är p inte ett element i B. Att p är ett element i B leder direkt till en motsägelse, för det antogs redan att m är det minsta elementet i B.

Annars är p ett element i A. Varje element i A kan skrivas som en produkt av primtal, och då kan även p skrivas som en produkt av primtal. Detsamma gäller givetvis också för q.

Detta leder slutligen också till en motsägelse för i så fall kan både p och q skrivas som en produkt av primtal, och m är i så fall också en produkt av primtal, och därmed är ett motbevis konstruerat. Ifall p är ett primtal som delar en produkt av flera heltal så delar p minst en av dessa faktorer.

Induktion med en produkt av två positiva heltal a och b:

Talet p delar produkten ab. Om p inte delar a så kommer p att dela b. Om p inte delar a så är 1 talens största gemensamma delare och då kan man med

hjälp av Bezouts identitet skriva $xp + ya = 1$, och då erhålls $xpb + yab = b$ efter multiplikation med b. Nu delar p både xpb och yab, och p delar därför också b.

Om p delar heltalet c är satsen bevisad, om inte måste p dela produkten av alla positiva heltal c_2, c_3... c_n. För något m måste primtalet p dela ett av de positiva heltalen c_m.

Antag att det finns något, eller flera, positiva heltal $n > 1$ som kan primtalsfaktoriseras på två eller flera sätt.

Antag att talet n kan framställas som både p_1,p_2...p_r och q_1,q_2...q_s där $r \leq s$.

p_1 delar en av faktorerna q_1,...q_s t.ex. p_1 delar q_1.

Men p_1 och q_1 är primtal så $p_1 = q_1$. Dessa kan förkortas bort till

$p_2...p_r = q_2...q_s$.

På detta sätt fås att $p_2 = q_2$ och $p_r = q_r$ så p_2,...p_r och q_2,...q_s kan förkortas bort eftersom $r \leq s$. Om $r < s$ leder det till att $1 = q_{r+1}...q_s$, vilket är omöjligt.

Alltså $r = s$ och satsen är bevisad.

Vissa av primtalen p kan vara desamma som de i q, och om de divideras bort fås att ingen av faktorerna p_{iv} är lika med någon av faktorerna q_{js}.

Nu ska hjälpsatsen tillämpas på primtalet p_{i_1} och produkten av alla q. Då måste primtalet p_{i_1} eftersom det delar ett tal n, dela åtminstone något av primtalen i "q-kedjan". Men det är omöjligt enligt det som tidigare antogs, och därmed är det bevisat att alla positiva heltal har en entydig primtalsuppdelning. [1] □

Pierre de Fermat (1607-1665) var en fransk matematiker och fysiker. Hans egentliga yrke var domare, så matematiken var huvudsakligen ett intresse för honom och han publicerade nästan ingenting. Det lilla han faktiskt publicerade, publicerades dessutom utan bevis, vilket överlag inte gillas av matematiker.

Förutom talteoretiker var han en av de första sannolikhetsteoretikerna.

Han är främst känd för sin stora sats, men också bl.a. för sin lilla sats. Här i Förkunskaper presenteras Fermats lilla sats, medan hans stora sats, som brukar kallas sista sats, Last theorem, på engelska, presenteras kort i avslutningen.

Sats 2.4. *Fermats lilla sats. Om p är ett primtal gäller det för varje heltal a att*

$$a^p \equiv a \mod p$$

d.v.s. att a^p är kongruent med a. Kongruensräkning som också kallas modulär aritmetik eller moduloräkning är ett område inom aritmetiken. Två tal a och b är kongruenta modulo n om n delar differensen mellan a och b.

Ett exempel på kongruens är att 7 är kongruent med 3 modulo 4, vilket är trivialt, och ett annat exempel är att 98 är kongruent med 53 modulo 15 eftersom 98-53 är 45 som är delbart med 15.

Om man tar ett tal a och multiplicerar det p gånger med sig självt och subtraherar a så är resultatet delbart med p. Ett specialfall, $a = 2$, var välkänt i Kina långt innan det bevisades för alla tal.

Fermat själv bevisade inte satsen, men den bevisades istället så tidigt som 1683 av Gottfried Wilhelm Leibnitz (1646-1716).

Satsen kan både bevisas med matematisk induktion samt med hjälp av gruppteori. Det räcker att bevisa påståendet för positiva heltal ty i det här fallet är det analogt och trivialt för negativa tal.

Bevis med matematisk induktion:

Bevis. Om $a = 1$ så är

$$1^p \equiv 1 \mod p$$

och satsen gäller.

Antag att satsen gäller för alla $a \leq n$, då erhålls att

$$n^p \equiv n \mod p$$

Om $a = n + 1$ så är $a^p = (n + 1)^p$ som är kongruent med

$$\begin{aligned} & n^p + \binom{p}{1} n^{p-1} \cdot 1 + \binom{p}{2} n^{p-2} \cdot 1^2 + ... + \binom{p}{p-1} n^1 \cdot 1^{p-1} + 1^p \mod p \\ & \equiv n^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} \cdot n^{p-k} + 1 \\ & \equiv n^p + p \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)! \cdot p} \cdot n^{p-k} + 1 \mod p \end{aligned}$$

Koefficienten är $\frac{p!}{k!(p-k)!\cdot p}$. Om p är ett primtal så delas inte p av varken faktorn $k!$ eller $(p-k)!$.

Eftersom $\frac{p!}{k!(p-k)!}$ är ett heltal måste också $\frac{p!}{k!(p-k)!\cdot p}$ vara ett heltal. Det är kongruent med $n^{p+1}(\mod p)$ om p är ett primtal, d.v.s. kongruent med $n+1(\mod p)$ d.v.s.

$$a^p \equiv a \mod p$$

och satsen gäller. □

Satsen kan också bevisas med gruppteori:

Bevis. Antag att p är ett primtal och G gruppen som består av elementen 1, 2, ..., $p-1$ under operationen multiplikation $\mod p$.

Gruppen är då av ordningen $p-1$. Tag ett element a i G (a ligger mellan 1 och $p-1$) och låt k vara a:s ordning (d.v.s. det minsta k så att a^k är 1). Enligt Lagranges sats (Om G är en ändlig grupp och F en delgrupp i G är F:s ordning en delare till G:s ordning) är k en delare i G:s ordning, som är $p-1$, så $p-1 = kn$ för något heltal n.

Då erhålls att a^{p-1} är kongruent med a^{kn} som är kongruent med $(a^k)^n$ som är kongruent med 1^n som är kongruent med 1 modulo p. Om båda sidorna multipliceras med a fås att a^p är kongruent med $a \mod p$ vilket skulle bevisas. □

Fermats lilla sats kan även generaliseras till Eulers sats som i sin tur kan generaliseras till Carmichaels sats.

Kapitel 3

Bertrands postulat; hjälpsatserna

Detta kapitel behandlar hjälpsatserna till Bertrands postulat, som är ett mycket centralt resultat i denna gradu.

Sats 3.1. *Bertrands postulat. För varje heltal $n > 3$, finns det åtminstone ett primtal p som uppfyller $n < p < 2n - 2$.*

När postulatet betraktas ser det enkelt ut, och det kan antas att det nästan säkert gäller (även om Bertrand inte bevisade postulatet, bevisade han att det gäller för alla $n < 3\ 000\ 000$), men beviset är relativt långt och inte särdeles enkelt. Här framläggs följande elementära bevis, som inte är originalbeviset. För beviset krävs flera hjälpsatser. Här följs en tyskspråkig video på Youtube. [9].

Hjälpsatserna är betydligt längre än själva beviset.

Sats 3.2. *Bertrands postulat i svag form: Om n är ett positivt heltal finns det åtminstone ett primtal p så att $n < p \leq 2n$.*

Lemma 3.3. *Olikheten $\frac{2^x}{x^2} > x^{\sqrt{x}}\ 2^{\frac{2x}{3}}$, $x \geq 1024$ gäller.*

Anmärkning. $1024 = 2^{10}$

Bevis. Olikheten kan omskrivas till

$$f(x) = x \ln 2 - 2 \ln x - \sqrt{x} \ln x - \frac{2x \ln 2}{3}, f(x) > 0, x \geq 1024$$

genom att ta logaritmen, för den är växande.

Efter derivering fås, efter förlängning av $x \ln 2$ till $3x\ \frac{\ln 2}{3}$

$$f'(x) = \frac{\ln 2}{3} - \frac{2}{x} - \frac{2 + \ln x}{2\sqrt{x}}$$

Deriveras det en gång till fås

$$f''(x) = \frac{2}{x^2} + \frac{\ln x}{4x\sqrt{x}} \geq 0$$

ty $\frac{\ln 2}{3}$ är en konstant.

Eftersom $f''(x) \geq 0$ för alla x då $x > 1$ är derivatan växande och $f'(1024) > 0$. f är växande för $x \geq 1024$ och följaktligen fås att $f(x) > 0$ då $x \geq 1024$. Det gäller även att $f(1024) \geq 0$. □

Även i Youtube-videon nämns det att det inte är något enkelt bevis, den är en timme lång och där berättas också att Erdös elementära bevis följs, åtminstone är det väldigt starkt byggt på Erdös bevis, och videons bevis inleds på samma sätt som Erdös själv inledde beviset, med binomialsannolikheten. [4], [9]

Kom ihåg att:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Talet n är alltid större än eller lika med k. n och k måste givetvis vara positiva heltal eftersom operationen fakultet endast är definierad för positiva heltal. I Pascals triangel finns varje binomialkoefficient, och triangeln är följaktligen oändlig. För det första elementet i varje rad är $k = 0$ och $n = n$ vilket n är i alla element på raden n, och i det sista elementet är dessutom $k = n$. Det första och det sista elementet på varje rad blir alltid en etta.

Först ska Pascals triangel tillämpas, vilken, precis som exempelvis Fermats satser, är ett exempel på renässansmatematik eftersom Blaise Pascal levde 1623-1662. Han var en av sannolikhetslärans fäder, och funderade bl.a. på vad som det lönar sig att spela på i hasardspel. Hasardspel har spelats i åtminstone hundratals år och det var även via dem som sannolikhetsläran överhuvudtaget växte fram. Till en början handlade det om tärningsspel och slantsinglingar, men senare handlade det även om andra sorters spel. Pascal var även fysiker, uppfinnare och teolog, det sistnämnda något som inte var ovanligt bland naturvetare på 1600- och 1700-talen.

Pascals triangel väcker och har väckt mycket fascination, och med hjälp av den kan binomialsannolikheter beräknas och summan av elementen på varje rad är alltid i potenser av talet 2. I Pascals triangel är alla binomialiteter utskrivna.

Till exempel vid slantsingling är det alltså relativt osannolikt, $\frac{252}{1024}$ (24.6 procent), att exakt 5 kronor på 10 försök erhålls, även om det är väntevärdet. Men

att kronorna skulle bli nära 5, alltså 4, 5 eller 6, är däremot sannolikt, $\frac{672}{1024}$ (65.6 procent).

Som följande visas de 10 första raderna i Pascals triangel.

$n = 0$					1					
$n = 1$				1		1				
$n = 2$			1		2		1			
$n = 3$		1		3		3		1		
$n = 4$	1		4		6		4		1	
$n = 5$	1	5		10		10		5		1
$n = 6$	1	6	15		20		15	6		1
$n = 7$	1	7	21		35		35	21	7	1
$n = 8$	1	8	28	56		70		56	28	8	1
$n = 9$	1	9	36	84	126		126	84	36	9	1
$n = 10$	1	10	45	120	210	252	210	120	45	10	1

Det gäller alltså att

Lemma 3.4. $n, k \in !$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \leq \binom{2n}{n} = \frac{2n!}{n!(n)!}$$

Bevis. Erdös ställde upp det med $\binom{2n}{n} = \frac{2n!}{n!(n)!}$ på samma sätt, det ska senare bevisas att det mellan alla heltal $n > 3$ finns minst ett primtal p sådant att $n < p < 2n - 2$. Detta påstående är ekvivalent med $(n!)^2 \leq (2n - k)!k!$, som är ekvivalent med $\frac{n!}{k!} \leq \frac{(2n-k)!}{n!}$.

Denna olikhet kan omskrivas till $n(n-1)(n-2)...(n-(n-k-1) \leq (2n-k)(2n-k-1)...(2n-k-(n-k-1))$ så olikheten är giltig för $(n-i) \leq (2n-1)$. Olikheten är också uppenbar genom att betrakta Pascals triangel. I videon ringades det mittersta elementet i rad 2, rad 4, rad 6, rad 8, o.s.v., alltså alla de första jämna raderna. I rad 1, 3, 5, o.s.v., d.v.s. alla udda rader, är alltid två tal de största, d.v.s. de två talen som är i mitten av raden. (Ettan på toppen anses vara rad 0). Det vill säga det största elementet är alltid det mittersta i de jämna raderna och i de udda raderna kan inte ens n bli ett heltal från $2n$ för ett udda tal blir alltid ett halvt tal om man delar det. □

Lemma 3.5. *För alla $n \in N$ gäller dessutom*

$$\frac{4^n}{2n} \leq \binom{2n}{n},$$

som också fungerar som en underskattning.

Det kan också omskrivas till

$$4^n \leq \binom{2n}{n} \cdot 2n.$$

Även här är Pascals triangel till stor hjälp. Innan beviset kommer det visas ett exempel.

Exempel 3.6. *Som induktionsbevis kan t.ex. den sjätte raden väljas, där $2n$ är 6 och n därmed 3. På den åttonde raden är siffersumman 256 d.v.s. 4^4, och på den sjätte raden är siffersumman 64 d.v.s. 4^3. Den sjätte radens mittersta objekt är 20, och 20 är större än $\frac{64}{6}$, och likväl är 70 större än $\frac{256}{8}$, 252 är större än $\frac{1024}{10}$ o.s.v. Det är endast på den andra raden som likhet gäller, annars är det alltid mindre. $\binom{2n}{n}$ kan följaktligen underskattas med hjälp av alla andra element som finns på raden $2n$ i Pascals triangel.*

Bevis.

$$4^n = 2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k},$$

det kan också skrivas

$$\sum_{k=0}^{2n} \binom{2n}{k} = \binom{2n}{0} + \binom{2n}{2n} + \sum_{k=1}^{2n-1} \binom{2n}{k},$$

vilket är uppenbart genom att betrakta Pascals triangel, eftersom $\binom{2n}{0}$ är elementet längst till vänster på raden $2n$, $\binom{2n}{2n}$ elementet längst till höger på rad $2n$ och den sista termen är summan av alla de övriga elementen. Och eftersom de båda yttersta elementen alltid är 1 på alla rader kan uttrycket förenklas till

$$2 + \sum_{k=1}^{2n-1} \binom{2n}{k} \leq \binom{2n}{n} + \sum_{k=1}^{2n-1} \binom{2n}{n} = 2n \cdot \binom{2n}{n},$$

och hjälpsatsen är bevisad. □

Detta gav följaktligen en underskattning för $\binom{2n}{n}$. Nästa hjälpsats kommer i sin tur vara en av satserna som ger en överskattning.

Nästa hjälpsats är mer komplicerad och innehåller en produkt.

Lemma 3.7. *För varje reellt tal $x \geq 2$ gäller:*

$$\prod_{p \leq x} p \leq 4^{x-1},$$

d.v.s. produkten av alla primtal som är mindre än eller lika med talet x tas. Det är alltså en exponentialfunktion som det ska överskattas med, och den andra funktionen kallas för en trappfunktion, som även delas upp i olika intervall för olika primtal. Funktionen är en konstant ifall talet som passeras inte är ett primtal, eftersom det endast ska multipliceras med primtalen.

Grafen visar att exponentialfunktionen ökar exponentiellt hela tiden medan primtalsfunktionen endast ökar i språngpunkterna.

Som redan tidigare nämnts behöver denna olikhet endast bevisas för naturliga tal. Om påståendet gäller för ett udda tal $x > 1$, då gäller det även för $x + 1$ eftersom produkten av alla primtal upp till x är lika med produkten av alla primtal upp till $x + 1$ i det här fallet. $x + 1$ är jämnt, och kan följaktligen inte vara ett primtal.

Bevis. Ansats: För $p = 2$ och $x = 2$ fås att $2 < 4$, och för $p = x = 3$ fås att $6 < 16$, så den ser ut att stämma. (Likhet gäller bara för $p = 1$ och 1 anses dessutom i regel inte vara ett primtal och hör inte till definitionsmängden heller).

Induktionsbevis: Låt $x = 2m + 1$ där m är ett naturligt tal, och det är redan känt att utsagan gäller för $2, ..., 2m$, alltså för alla jämna rader, vilket visades i en hjälpsats. Nu ska det bevisas för alla udda rader också.

Det antas att

$$\prod_{p \leq x} p \leq \prod_{p \leq x+1} p$$

om $x + 1$ jämnt, $x + 1 > 2$. Då erhålls

$$\prod_{p \leq 2m+1} p,$$

där produkten av alla primtal fram till rad $2m + 1$ bildas och dessutom sätts $2m + 1$ in i exponenten till potensen 4.

Det betyder att

$$\prod_{p \leq 2m+1} p \leq 4^{2m}.$$

Sedan delas produkten (produkten för primtalen upp till $m+1$ och produkten av primtalen större än $m+1$ upp till $2m+1$ tas) och då erhålls att:

$$\prod_{p\leq 2m+1} p = \prod_{p\leq m+1} p \cdot \prod_{m+1<p\leq 2m+1} p \leq 4^m \cdot \prod_{m+1<p\leq 2m+1} p \leq 4^{2m}.$$

4^{2m} fås genom att sätta in $2m+1$ på x:s plats i exponenten. Talen upp till $m+1$ ligger bland dem som redan har bevisats eftersom de ligger mellan m och $2m$, därifrån kom termen 4^m. Varför denna olikhet gäller fås genom att skatta uttrycket med binomialkoefficienten för $2m+1$. Det betyder alltså att det erhålls

$$\prod_{m+1<p\leq 2m+1} p \leq \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m}$$

eftersom det finns ett primtal $p \in [m+1, 2m+1]$ där p är delbart med $(2m+1)!$ men inte med $m!$ och $m+1!$. $\binom{2m+1}{m}$ är alltid något av elementen i mitten på de udda raderna, och därmed är det det största talet på raden ifråga. Primtalen är som bekant odelbara så fakulteten kan aldrig vara ett primtal. Fakulteten är för övrigt alltid ett jämnt tal för $n \geq 2$ och ett jämnt tal som slutar på åtminstone en nolla fr.o.m. $n \geq 5$. De första 15 fakulteterna är för övrigt 1, 2, 6, 24, 120, 720, 5 040, 40 320, 362 880, 3 628 800, 39 916 800, 479 001 600, 6 227 020 800, 87 178 291 200 och 1 307 674 368 000, så det handlar om en operation som växer mycket snabbt.

Återigen finns Pascals triangel till hjälp och det kunde lika gärna ha skrivits $\binom{2m+1}{m+1}$ eftersom m och $m+1$ alltid är samma tal på de udda raderna. Summan på de udda raderna är dessutom alltid $2 \cdot 4^m$.

Beviset fortsätter med:

$$2\cdot 4^m = (1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2\binom{2m+1}{m} + \sum_{k=0,k\neq m,k\neq m+1}^{2m+1} \binom{2m+1}{k},$$

ty de två mittersta raderna $\binom{2m+1}{m}$ och $\binom{2m+1}{m+1}$ är alltid samma sak,

och därför erhålls att

$$\binom{2m+1}{m} \leq 4^m.$$

Det följer alltså att

$$\prod_{p\leq 2m+1} p \leq 4^m \cdot 4^m = 4^{2m}.$$

□

Detta bevis kommer att behövas också senare.

Till näst används Legendres identitet. Den ger en övre uppskattning för $\binom{2n}{n}$.

Lemma 3.8. *Legendres identitet. Låt n vara ett naturligt tal. Då gäller för multipliciteten av ett primtal p i n!, att:*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

där klamrarna anger det största heltal som är mindre än eller lika med talet, d.v.s. heltalsdelen. T.ex. talet 120, som också är 5!, eller $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ (ettan är egentligen överflödig) har primtalsfaktoriseringen $2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$. Multipliciteten av 2 är 3, multipliciteten av 3 är 1 och multipliciteten av 5 är 1 i det här fallet.

Låt x vara multipliciteten av ett primtal p. Då delar p^x $n!$, men p^{x+1} delar inte $n!$.

Bevis. Om p är större än n så delas inte $n!$ av p så svaret är 0. Därför kan det antas att $p \leq n$. Låt k vara den största potensen av p så att $p^k \leq n$. För varje $1 \leq i \leq k$, är antalet heltal från 1 till n som är delbara med p^i men inte delbara med p^{i+1} lika med

$$\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor.$$

Om inga tal är delbara med p^i så är $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$, analogt för $\left\lfloor \frac{n}{p^{i+1}} \right\rfloor$.

$\left\lfloor \frac{n}{p^{i+1}} \right\rfloor$ motsvarar antalet heltal som är större än och delbara med p^{i+1}. Så antalet heltal som är entydigt delbara med p^i är alltså skillnaden av dessa två golvfunktioner.

Värdet av p^x som delar $n!$ motsvarar produkten av alla potenser p som delar vilka som helst av heltalen i följden från 1 till n.

Därför kan värdet av x beräknas med

$$x = \sum_{k=1}^{k} i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor \right).$$

Genom att sätta ihop detta erhålls följande mönster:

$$x = 1 \cdot \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 2 \cdot \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + 3 \cdot \left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor \right) + \ldots$$

eftersom för $k = 1$ fås $\left\lfloor \frac{n}{p} \right\rfloor$, för $k = 2$ $\left\lfloor \frac{n}{p^2} \right\rfloor$ o.s.v. [10] □

Dessa klamrar kan alltså också kallas för en golvfunktion. Golv- och takfunktionerna är två viktiga funktioner inom talteorin, där värdet av golvfunktionen för ett reellt tal x är det största heltal som är mindre eller lika med x. För positiva tal x ger golvfunktionen heltalsdelen av x.

Det finns även takfunktioner, som i sin tur ger det minsta heltal som är större eller lika med x. Men de används inte i beviset till Bertrands postulat.

Lemma 3.9. *Låt $n \geq 5$, och*

$$\binom{2n}{n} = \prod_p p^{\nu_p(\binom{2n}{n})}.$$

Nu upphöjs alltså alla primtal med den multiplicitet som $\binom{2n}{n}$ förekommer.

Då gäller det för alla primtal p att:

$$p^{\nu_p\binom{2n}{n}} \leq 2n.$$

Det betyder att de har en multiplicitet på högst $2n$.

Ett exempel: Tag ett stort tal, $n = 500$. Då blir $\binom{2n}{n}$ till $\binom{1000}{500}$. Multipliciteten ska alltså bli högst 500 i detta exempel. I beviset i videon motsvarades detta av 1800 och 3600.

2^9 och 3^6 är båda över 500, alltså kan högst 2^8 eller 3^5 komma ifråga.

Bevis. Låt n vara ett naturligt tal och p ett primtal. Då är

$$\nu_p\binom{2n}{n} = \nu_p\binom{(2n)!}{n!n!} = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \leq \log_p 2n.$$

Varje summa är exakt 0 eller exakt 1 eftersom det gäller att:

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2(\frac{n}{p^k} - 1) = 2.$$

$p^k > 2n$ blir alltid 0 om

$$k > \frac{\log 2n}{\log p}.$$

Detta ger utsagan

$$p^{\nu_p\binom{2n}{n}} \leq 2n.$$

genom omformning av de tidigare uttrycken. Det betyder att varje primtalsfaktor finns högst $2n$ gånger.

Om $\sqrt{2n} < p < \frac{2n}{3}$ är summorna för $k \geq 2$ tillsammans exakt 0, eftersom

$$\nu_p\binom{2n}{n} = \nu_p\left(\frac{(2n)!}{n!n!}\right) = \sum_{k=1}^{\infty}\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor \leq \log_p 2n.$$

Alltså

$$\nu_p\binom{2n}{n} \leq 1.$$

Om $\frac{2n}{3} < p \leq n$ erhålls summeringen

$$\left\lfloor\frac{2n}{p}\right\rfloor - \left\lfloor\frac{n}{p}\right\rfloor = 2 - 2 \cdot 1 = 0$$

och då följer

$$\nu_p\binom{2n}{n} = 0.$$

I fallet $n < p \leq 2n$ fås summeringen

$$\left\lfloor\frac{2n}{p}\right\rfloor - \left\lfloor\frac{n}{p}\right\rfloor = 1 - 2 \cdot 0 = 1$$

och då följer

$$\nu_p\binom{2n}{n} = 1.$$

□

Detta var alla hjälpsatser, och nu kan Bertrands postulat bevisas.

Kapitel 4

Bertrands postulat, med tillägg

Nu bevisas Bertrands postulat.

Bevis. Låt $n \geq 5$.

Nu används den sista hjälpsatsen för att bevisa postulatet. Antag att Bertrands postulat inte gäller.

Det gäller att

$$\frac{4^n}{2n} \leq \binom{2n}{n} = \prod_p p^{\nu_p\binom{2n}{n}} \leq 2n \leq \prod_{p\leq\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}<p<\frac{2n}{3}} p \cdot \prod_{n<p\leq 2n} p,$$

$\prod_{\frac{2n}{3}<p\leq n} p$ är en onödig produkt att ha med när primtalen mellan $\frac{2n}{3}$ och n förkortades bort. Därmed följer

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}-1},$$

och formas det om erhålls

$$4^{\frac{n}{3}+1} \leq (2n)^{\sqrt{2n}+1}.$$

Det fås alltså en överskattning eftersom basen $2n$ är en linjär funktion, men denna överskattning gäller inte för stora tal.

Det är givet att

$$2n = (\sqrt{2n}^{\frac{1}{6}})^6 < (\lfloor\sqrt{2n}^{\frac{1}{6}}\rfloor + 1)^6 \leq 2^{6\sqrt{2n}^{\frac{1}{6}}}.$$

ty $(k+1) < 2^k$.

Då har detta överskattats.

Nu erhålls

$$2^{2n} < 2^{2n+6} = (4^{\frac{n}{3}+1})^3 \leq ((2n)^{\sqrt{2n}+1})^3 < 2^{18\sqrt{2n}^{\frac{1}{6}}(\sqrt{2n}+1)}$$

För $n \geq 41$ gäller att $18 < 2\sqrt{2n}$. Genom att logaritmera fås

$$2n < 18\sqrt{2n}^{\frac{1}{6}}(\sqrt{2n}+1) = 18(2n)^{\frac{2}{3}} + 18\sqrt{2n}^{\frac{1}{6}} < 18(2n)^{\frac{2}{3}} + 2\sqrt{2n}\sqrt{2n}^{\frac{1}{6}} = 20(2n)^{\frac{2}{3}}.$$

Detta gäller ty 18 är en konstant och kvadratroten i högra ledet växer.

$(2n)^{\frac{1}{3}} < 20$ ger att $2n < 8000$, alltså följer det att $n < 4000$.

Genom att ställa om ekvationen följer slutligen att $n < 4000$. Detta visar alltså att Bertrands postulat gäller också för $n \geq 4000$.

Nu behöver bara tal mindre än 8 000 undersökas. Det kan beräknas att talen 2, 3, 5, 7, 13, 23, 45, 83, 163, 317, 631, 1 259, 2 503 och 5 003 är primtal.

Därmed är det bevisat att Bertrands postulat gäller för alla naturliga tal. □

Erdös formulerade det hela på samma sätt men använde andra tal som exempel.

Kapitel 5

En utveckling av Bertrands postulat

Det kan även bevisas att en utveckling av Bertrands postulat gäller i intervallet mellan $2n$ och $3n$, d.v.s. att det alltid finns ett primtal p sådant att $2n < p < 3n$.

Lemma 5.1. *Dessa fyra olikheter gäller:*

1. *Om n är jämnt så är*

$$\binom{\frac{3n}{2}}{n} < (\sqrt{6.75})$$

2. *Om n är ett jämnt tal sådant att $n > 152$ så gäller*

$$\binom{\frac{3n}{2}}{n} > (\sqrt{6.5})^n$$

3. *Om n är udda och $n > 7$ så är*

$$\binom{\frac{3n+1}{2}}{n} < (\sqrt{6.75})^{n-1}$$

4. *Om $n > 945$ så är*

$$(\frac{6.5}{\sqrt{27}})^n > (3n)^{\frac{3n}{2}}$$

Bevis. Nu bevisas 1 och 2 med induktion på n. För $n = 2$ erhålls att

$$\binom{3}{2} < 6.75$$

och

$$\binom{\frac{3\cdot 154}{2}}{154} > \sqrt{6.5}^{154}$$

ty $231!/(154! \cdot 77!) = 3.995^{62}$ medan $\sqrt{(6.5)^{154}}$ eller 6.5^{77} är 3.929^{62}.

För $n = 153$ är det odefinierat ty då erhålls $229,5!$ i täljaren vilket inte existerar.

För $n = 152$ fås $228!/(152! \cdot 76!)$ vilket är $5,958^{61}$ medan 6.5^{76} är $6,045^{61}$, så där gäller det inte.

Antag att dessa två olikheter gäller för $\binom{3}{2}$. Då är

$$\begin{aligned}\binom{3n+3}{2n+2} &= \binom{3n}{2n}\frac{(3n+1)(3n+2)(3n+3)}{(n+1)(2n+1)(2n+2)} \\ &= \binom{3n}{2n}\frac{3(3n+1)(3n+2)}{(2n+1)(2n+2)} \\ &= \binom{3n}{2n}\frac{27n^2+27n+6}{4n^2+6n+2}\end{aligned}$$

Det är nu lämpligt att notera att för alla n gäller (1)

$$\frac{27n^2+27n+6}{4n^2+6n+2} < 6.75$$

och för alla $n > 12$ gäller (2)

$$6.5 < \frac{27n^2+27n+6}{4n^2+6n+2}$$

Bevis av (1). Genom att förlänga 6.75 med nämnarens uttryck fås uttrycket liknämnigt.

$$\frac{27n^2+27n+6}{4n^2+6n+2} < \frac{6.75(4n^2+6n+2)}{4n^2+6n+2}$$

När nämnaren multiplicerats med 6.75 och efter att detta har satts in i täljaren fås

$$\frac{27n^2+27n+6}{4n^2+6n+2} < \frac{27n^2+40.5n+13.5}{4n^2+6n+2}$$

vilket tydligt och klart alltid gäller.

Bevis av (2). Nu förlängs 6.5 med nämnarens uttryck och då fås

$$\frac{6.5 \cdot (4n^2+6n+2)}{4n^2+6n+2} < \frac{27n^2+27n+6}{4n^2+6n+2}$$

$$\frac{26n^2+39n+13}{4n^2+6n+2} < \frac{27n^2+27n+6}{4n^2+6n+2}$$

Efter subtraktion av täljarna fås

$$-n^2+12n+7$$

vilket alltid är mindre än 0 för heltal $n > 12$, vilket skulle bevisas.

(3) bevisas med induktion på n. Använder $n = 9$ med induktion och erhåller då $\binom{14}{9} < (6.75)^4$. Antag nu att det gäller för $\binom{3n+2}{2n+1}$. Då är

$$\binom{3n+5}{2n+3} = \binom{3n+2}{2n+1}\frac{3(3n+4)(3n+5)}{2(n+2)(2n+3)} < (6.75)^n \cdot 6.75 = 6.75^{n+1},$$

ty

$$\frac{3(3n+4)(3n+5)}{2(n+2)(2n+3)} = \frac{27n^2+81n+60}{4n^2+14n+12} < \frac{6.75(4n^2+14n+12)}{4n^2+14n+12} = \frac{27n^2+94.5n+81}{4n^2+14n+12}.$$

(4) Notera att de följande tre olikheterna är ekvivalenta:

$$(\frac{6.5}{\sqrt{27}}) > (3n)^{\frac{\sqrt{3n}}{2}}$$

$$n \ln \frac{6.5}{\sqrt{27}} > \frac{\sqrt{3n}}{2} \ln 3n$$

$$\frac{2}{\sqrt{3}} \ln \frac{6.5}{\sqrt{27}} > \frac{\ln 3n}{\sqrt{n}}.$$

Resultatet följer eftersom funktionen $\frac{\ln 3x}{\sqrt{x}}$ är avtagande och genom prövning fås

$$\frac{2}{\sqrt{3}} \ln \frac{6.5}{27} > \frac{\ln(3 \cdot 946)}{\sqrt{946}}.$$

□

Lemma 5.2. *1. Om n är jämnt så är*

$$\prod_{\frac{n}{2} < p \leq \frac{3n}{4}} p \cdot \prod_{n < p \leq \frac{3n}{2}} p < \binom{\frac{3n}{2}}{n}.$$

2. Om n är udda så är

$$\prod_{\frac{n+1}{2} < p \leq \frac{3n}{4}} p \cdot \prod_{n < p \leq \frac{3n+1}{2}} p < \binom{\frac{3n+1}{2}}{n}.$$

Bevis. Del 1, med jämna tal:

$$\binom{\frac{3n}{2}}{n} = \frac{\frac{3n!}{2}}{\frac{n!}{2} \cdot n!}$$

Då gäller det att

$$\binom{\frac{3n}{2}}{n} = \frac{(n)...\frac{3n}{2}}{\frac{n!}{2}}$$

Med hjälp av det ses att $\prod_{n<p\leq\frac{3n}{2}} p$ delar $\binom{\frac{3n}{2}}{n}$. Om $\frac{n}{2} < p \leq \frac{3n}{4}$ finns $2p$ i täljaren av uttrycket men p finns inte i nämnaren. Efter en förkortning av $2p$ (ett jämnt tal från nämnaren) fås en primtalsfaktor p i $\binom{\frac{3n}{2}}{n}$. Då delar $\prod_{\frac{n}{2}<p\leq\frac{3n}{4}} p$ $\binom{\frac{3n}{2}}{n}$ också och den krävda olikheten följer från detta.

Beviset till del 2 funkar på ett liknande sätt.

$$\binom{\frac{3n+1}{2}}{n} = \frac{\frac{3n+1!}{2}}{\frac{n+1!}{2} \cdot n!}$$

Det gäller att

$$\binom{\frac{3n+1}{2}}{n} = \frac{(n+1)...\frac{3n+1}{2}}{\frac{n+1!}{2}}$$

Med hjälp av det ses att $\prod_{n<p\leq\frac{3n+1}{2}} p$ delar $\binom{\frac{3n+1}{2}}{n}$. Om $\frac{n+1}{2} < p \leq \frac{3n}{4}$ finns $2p$ i täljaren av uttrycket men p finns inte i nämnaren. Efter en förkortning med $2p$ (ett jämnt tal från nämnaren) fås en primtalsfaktor p i $\binom{\frac{3n+1}{2}}{n}$. Då delar $\prod_{\frac{n}{2}<p\leq\frac{3n}{4}} p$ $\binom{\frac{3n+1}{2}}{n}$ också och den krävda olikheten följer från detta.

[11]

□

Det ska först bevisas för alla tal n upp till 945 och sedan för alla tal större än 946. Med hjälp av Mathematica [12] fås att de första primtalen är 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609,

1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889 och 1901, så det finns alltid något primtal p mellan $2n$ och $3n$ för alla tal $n < 946$.

Låt nu $n > 945$. Eftersom

$$\binom{3n}{2n} = \frac{(2n+1)(2n+2)...3n}{1 \cdot 2 \cdots n},$$

delas $\binom{3n}{2n}$ av produkten av primtalen mellan $2n$ och $3n$, om de existerar. Nu används beteckningarna

$$T_1 = \prod_{p \leq \sqrt{3n}} p^{\beta(p)}, T_2 = \prod_{\sqrt{3n} \leq p \leq 2n} p^{\beta(p)}, T_3 = \prod_{2n+1 \leq p \leq 3n} p^{\beta(p)}$$

så att

$$\binom{3n}{2n} = T_1 T_2 T_3.$$

T_1 : Eftersom $p \leq \sqrt{3n}$ gäller det att $p^2 \leq 3n$, och det gäller för alla $n \geq 2$ att det finns åtminstone ett primtal där, ty $2^2 = 4 < 6$.

T_2 : Nu betraktas T_2. Det är känt att $n < p < 2n$ gäller (Bertrands postulat). För alla tal $n > 3$ är dessutom $\sqrt{3n} < n$. Det behöver alltså bara visas att detta gäller för $n \leq 3$. Eftersom det mellan $\sqrt{3}$ och 2 finns primtalet 2, mellan $\sqrt{6}$ och 4 finns primtalet 3, samt mellan 3 och 6 finns primtalen 3 och 5, är det klart att det i detta intervall alltid finns minst ett primtal.

T_3 : $\beta(p) = 1$ då $2n + 1 \leq p \leq 3n$. Då $n = 1$ fås att $3 \leq p \leq 3$ och 3 är ett primtal, och när $n = 2$ fås $5 \leq p \leq 6$ och 5 är ett primtal, när $n = 3$ fås $7 \leq p \leq 9$, och 7 är ett primtal, när $n = 4$ fås $9 \leq p \leq 12$ och 11 är ett primtal. Mellan 11 och 15 finns 13 som är ett primtal, mellan 13 och 18 finns 13 och 17 som båda är primtal, och mellan 15 och 21 finns primtalen 17 och 19.

Mellan $2n$ och $2n + 1$ behöver detta inte gälla ty om $n = 4$ är $2n = 8$ och $2n + 1 = 9$ och varken 8 eller 9 är något primtal.

Om $p \in [2n + 1, 3n]$ så är $2p > 3n$ och p delar $(3n)!$.

$\binom{3n}{2n} = \frac{3n!}{2n! \cdot n!}$. Mellan $2n + 1$ och $3n$ finns alltid n stycken tal liksom mellan $n + 1$ och $2n$. Om $p \in [2n + 1, 3n]$ dvs $2p > 3n$ så delar p $(3n)!$.

Nu undersöks om p kan dela $1 \cdot 2 \cdot 3 \cdot n$.

Nej, p kan inte dela $1 \cdot 2 \cdot 3 \cdot n$ eftersom ett primtal p endast är delbart med sig själv och med 1 och talen i serien $1 \cdot 2 \cdot 3 \cdot n$ är alltid mindre än talet p och inget av dem är därmed delbara med p och därför kan inte p dela produkten.

I produkten $(2n+1)(2n+2)...3n$ finns alltid minst ett primtal, enligt vad som tidigare bevisades.

Det kan finnas flera primtal i intervallet, t.ex. om $n = 5$ finns både 11 och 13 i intervallet.

Primtalsupplösningen av $\binom{3n}{2n}$ visar att potenserna till T_2 är mindre än 2 för primtalsupplösningen av $\binom{n}{j}$. Dessutom gäller det att om ett primtal p satisfierar $\frac{3n}{4} < p \leq n$ så är dess potens i T_2 lika med 0. Det är även klart att ett primtal p med detta villkor finns i nämnaren av $\binom{3n}{2n}$ men $2p$ finns inte där, och $3p$ finns i täljaren av $\binom{3n}{2n}$. På grund av detta gäller påståendet. Om $\frac{3n}{2} < p \leq 2n$ så är potensen i T_2 dessutom också 0 eftersom ett sådant primtal p varken finns i nämnaren eller i täljaren och $2p > 3n$. Enligt informationen om $\binom{3n}{2n}$ som finns från tidigare och faktumet att $\prod_{p \leq x} p < 4^x$, som finns i beviset av Bertrands postulat, så gäller, om n är jämnt, att

Lemma 5.3.

$$\begin{aligned} T_2 &< \prod_{\sqrt{3n}<p<\frac{n}{2}} p \cdot \prod_{\frac{n}{2}<p\leq\frac{3n}{4}} p \cdot \prod_{n<p\leq\frac{3n}{2}} p \\ &< 4^{\frac{n}{2}} \binom{\frac{3n}{2}}{n} \\ &< 4^{\frac{n}{2}} (6.75)^{\frac{n}{2}} \\ &= \sqrt{27}^n. \end{aligned}$$

Om n är udda fås att

$$\begin{aligned} T_2 &< \prod_{\sqrt{3n}<p<\frac{n+1}{2}} p \cdot \prod_{\frac{n+1}{2}<p\leq\frac{3n}{4}} p \cdot \prod_{n<p\leq\frac{3n+1}{2}} p \\ &< 4^{\frac{n+1}{2}} \binom{\frac{3n+1}{2}}{n} \\ &< 4^{\frac{n+1}{2}} (6.75)^{\frac{n-1}{2}} \\ &4 \cdot \sqrt{27}^{n-1} \\ &= \sqrt{27}^n. \end{aligned}$$

Med hjälp av dessa två resultat fås att övre gränsen för T_2 är

$$T_2 < \sqrt{27}^n.$$

I T_2 finns det primtal i intervallet $\prod_{\sqrt{3n}\leq p\leq 2n} p^{\beta(p)}$ så $4p$ finns säkert i nämnaren/täljaren.

Nu ska det slutligen bevisas att det finns åtminstone ett primtal p i intervallet $2n < p < 3n$.

Bevis. Primtalsnedbrytningen av $\binom{3n}{2n}$ är sådan att den bryter ut den följande övre gränsen för T_1:

$$T_1 < (3n)^{\pi(\sqrt{3n})}$$

Då erhålls

$$(6.5)^n < T_1T_2T_3 < (3n)^{\pi(\sqrt{3n})}\sqrt{27}^n T_3$$

som implicerar att

$$T_3 > (\frac{6.5}{\sqrt{27}})^n \frac{1}{(3n)^{\pi(\sqrt{3n})}}$$

Dock gäller att antalet primtal mindre eller lika med $\sqrt{3n}$, d.v.s. $\pi(\sqrt{3n}) \leq \frac{\sqrt{3n}}{2}$.

$$T_3 > (\frac{6.5}{\sqrt{27}})^n \frac{1}{(3n)^{\pi(\sqrt{3n})/2}} > 1$$

där den andra olikheten följer från olikhet 4, alltså om $n > 945$ så är

$$(\frac{6.5}{\sqrt{27}})^n > (3n)^{\frac{3n}{2}}.$$

Följaktligen är produkten T_3 av primtal mellan $2n$ och $3n$ större än 1 och därför följer existensen av åtminstone ett primtal p i intervallet $2n < p < 3n$. □

Sats 5.4. *(Extra sats). För varje positivt heltal n finns det åtminstone ett primtal p sådant att*

$$n < p < \frac{3(n+1)}{2}.$$

Det är klart för $n = 2$ (induktion). För jämna tal $n > 2$ följer det från satsen att det finns ett primtal mellan $2n$ och $3n$. Antag nu att $n = 2k + 1$ för ett positivt heltal $k \geq 1$. Då fås från samma sats att det finns ett primtal p som satisfierar olikheten

$$2(k+1) < p < 3(k+1) = \frac{3(n+1)}{2},$$

och resultatet följer från detta.

Kapitel 6

Primtalssatsen med en skiss till ett elementärt bevis

Primtalssatsen är en annan känd talteoretisk sats. Den uppskattar hur tätt primtalen ligger.

Som källor har jag använt D. Goldfields essä The Elementary Proof of the Prime Number Theorem, samt Atle Selbergs bevis från 1948.

Studiet av primtalens fördelning har fascinerat matematikerna alltsedan antiken. Redan i antikens Grekland var det välkänt bland vetenskapsmännen att det finns oändligt många primtal. Men det är först i för matematiken relativt modern tid som matematiker lyckats upptäcka och senare också bevisa en precis asymptotisk lag för antalet primtal i godtyckligt långa intervall.

Teoremet,

$$\lim_{x\to\infty} \pi(x)/\frac{x}{\log x} = 1$$

förmodades av både Carl Friedrich Gauss (1777-1855) och Adrien-Marie Legendre (1752-1833) oberoende av varandra. Approximationen

$$\pi(x) = \frac{x}{A\log(x) + B}$$

formulerades av Legendre år 1798 och han fick fram värdena $A = 1$ och $B = -1.08366$.

Även den norske matematikern Niels Henrik Abel (1802-1829) förundrades över primtalssatsen och tyckte att den t.o.m. kunde vara den mest anmärkningsvärda satsen i hela matematiken. Han karaktäriserade primtalssatsen 1823 genom att referera till Legendre.

Gauss hade skrivit ett brev till en astronom på julafton 1849 att han redan 1792-1793 (då han var endast 15 eller 16 år gammal) försökte hitta en asymptotisk formel baserad på$\frac{1}{log(x)}$ och att det skulle leda till approximationen, så förutsatt att han mindes rätt var han den förste att förmoda detta samband. Han refererade även till Legendre. Han antog att approximationen skulle följa

$$\pi(x) \approx Li(x) = \int_2^x \frac{dt}{log(t)}.$$

Tjebysjov var 1848 den förste att komma fram till den rätta uppskattningen för den asymptotiska fördelningen av primtal.

Han bevisade att om approximationen till $\pi(x)$ av ordning $\frac{x}{log(x)}^N$ med något fixt heltal N gäller, måste approximationen vara $Li(x)$ och det följde från Legendres förmodan att $\lim_{x\to\infty} A(x) = 1.08366$ var falsk och att om gränsen existerade måste den vara 1. $\pi(x)$ betyder produkten av antalet primtal som är mindre eller lika med x.

För ett reellt heltal $x > 1$ betecknas det $\pi(x)$.

Betecknas antalet primtal som är mindre än eller lika med x med $\pi(x)$ sägs det att $\pi(x)$ är ungefär lika med $\frac{x}{\ln x}$ för stora x.

Tjebysjov var också den förste att visa 1852 att $\pi(x)$ har magnituden $\frac{x}{\log(x)}$. Hans argument var helt och hållet elementärt och han löste det med hjälp av faktorernas egenskaper. Den högsta potensen av ett primtal p som delar $x!$ är

$$\lfloor\frac{x}{p}\rfloor + \lfloor\frac{x}{p^2}\rfloor + \lfloor\frac{x}{p^3}\rfloor + ..,$$

och från detta följer att

$$x! = \prod_{p\leq x} p^{[x/p]+[x/p^2]+...}$$

samt

$$\log(x!) = \lfloor\frac{x}{p}\rfloor + \lfloor\frac{x}{p^2}\rfloor + \lfloor\frac{x}{p^3}\rfloor \log(p).$$

Enligt Stirlings asymptotiska formel, som är en approximation för mycket stora fakulteter (och som även har tillämpningar i fysiken, närmare bestämt i den statistiska mekaniken i termodynamiken) är $\log(x!)$ asymptotisk till $x\log(x)$ och eftersom kvadrater, kuber etc. på primtal är relativt ovanliga och $\lfloor\frac{x}{p}\rfloor$ nästan samma som $\frac{x}{p}$, ses att

$$\prod_{\frac{log(p)}{p}} = x\log(x) + O(x)$$

varifrån det erhålls att $\pi(x)$ är av ordning $\frac{x}{\log(x)}$.

Tjebysjovs metod visade egentligen att

$$B < \pi(x)/\frac{x}{\log(x)} < \frac{6B}{5}$$

för alla tillräckligt stora tal x där

$$B = \frac{\log 2}{2} + \frac{\log 3}{3} + \frac{\log 5}{5} - \frac{\log 30}{30} \approx 0.92129$$

och $\frac{6B}{5} \approx 1.10555$

Men Tjebysjov kunde inte bevisa hela primtalssatsen själv på det sättet.

James Joseph Sylvester (1814-1897) kom närmare 1892 med 0.956 och 1.045 som gränser för $\pi(x)/\frac{x}{\log(x)}$.

År 1896 bevisades satsen av fransmannen Jacques Hadamard (1865-1963) och belgaren Charles de la Vallée Poussin (1866-1962), och det anmärkningsvärda är att såväl förmodandet som beviset till satsen tillskrivs två olika matematiker oberoende av varandra. Dessutom bevisade bägge satsen med hjälp av samma metod (Riemanns zeta funktion). Riemanns zeta-funktion hör till den komplexa analysen och tillskrivs den tyske matematikern Bernhard Riemann (1826-1866), och den definieras av absolut konvergenta serier

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

för $Re(s) > 1$.

Det första elementära beviset gjordes 1948 av den norske matematikern Atle Selberg (1917-2007) och Paul Erdös.

Det finns många olika sätt att bevisa primtalssatsen på, och här kommer endast en skiss av ett elementärt bevis, formulerat av Selberg år 1948. Det elementära beviset för primtalssatsen är för övrigt hans största upptäckt.

Detta elementära bevis använder varken reell eller komplex analys, utan endast logaritmens simplaste egenskaper.

Selberg hade följande skiss för sitt bevis (detta är alltså inte hans fullständiga bevis med alla detaljer).

Det bevisar primtalssatsen på formen

$$\lim_{x\to\infty} \frac{\nu(x)}{x} = 1$$

när $x > 0, \nu(x)$ definieras som vanligt av

$$\nu(x) = \sum_{p \leq x} \log p$$

där p betecknar primtalen.

Det under- och överskattas med

$$a = \liminf \frac{v(x)}{x}$$

och

$$A = \limsup \frac{v(x)}{x}.$$

Selberg kom fram till att $a + A = 2$.

Bevis. Välj ett x så stort att $\nu(x) = ax + o(x)$.

Eftersom $\nu(x) < Ax + o(x)$ följer från Selbergs fundamentala formel att

$$ax \log(x) + \sum A \frac{x}{p} \log(p) \geq 2x \log(x) + o(x \log(x)).$$

Å andra sidan kan det väljas ett x så stort att $\nu(x) = Ax + o(x)$

Eftersom $\nu(x)$ alltid är större än $ax + o(x)$ följer det alltid, som tidigare, att

$$Ax \log(x) + \sum a \frac{x}{p} \log(p) \leq 2x \log(x) + o(x \log(x)).$$

Den huvudsakliga formeln i beviset är en asymptotisk formel som kan skrivas

$$\nu(x) \log x + \sum_{p \leq x} \log p \nu(\frac{x}{p}) = 2x \log x + O(x)$$

Från denna formel finns det många sätt att bevisa primtalssatsen.

Erdös har konstruerat ett bevis även för denna sats, och det går ut på epsilon-deltakalkyl.

Selbergs bevis fortsätter genom att introducera beteckningarna

$$\lim \frac{\nu(x)}{x} = a$$

och

$$\lim \frac{\nu(x)}{x} = A$$

och från dem ses att

$$\sum_{p\leq x}\frac{\log p}{p}=\log x+O(1),$$

så att $a+A=2$.

Härnäst tas ett stort x så att

$$\nu(x)=ax+o(x),$$

och från detta kan den modifierade formen

$$(\nu(x)-ax)\log x+\sum_{p\leq x}\log p\nu(\frac{x}{p})-A(\frac{x}{p})=O(x),$$

skrivas, vilken visar att för ett fixt tal δ erhålls

$$\nu(\frac{x}{p})>(A-\delta)\frac{x}{p},$$

med undantag för en särskild mängd av primtal $\leq x$ med

$$\sum\frac{\log p}{p}=o(\log x).$$

Det kan därmed avgöras att det finns ett x' i intervallet $\sqrt{x}<x'<x$ med

$$\nu(x')=Ax'+o(x').$$

Från

$$(\nu(x)-ax)\log x+\sum_{p\leq x}\log p\nu(\frac{x}{p})-A(\frac{x}{p})=O(x),$$

ses, om a byts till A och x' istället för x, att

$$\nu(\frac{x'}{p})<(a+\delta)\frac{x'}{p},$$

med undantag för en särskild mängd primtal $\leq x'$ med

$$\sum\frac{\log p}{p}=o(\log x).$$

Från Erdös resultat är det möjligt att visa att man kan välja primtalen p och p' som inte hör till någon av de övriga mängderna med

$$\frac{x}{p}<\frac{x'}{p'}<(1+\delta)\frac{x}{p}.$$

Då fås från

$$\nu(\frac{x}{p}) > (A-\delta)\frac{x}{p},$$

och

$$\nu(\frac{x'}{p'}) < (a+\delta)\frac{x'}{p},$$

att

$$(A-\delta)\frac{x}{p} < \nu(\frac{x}{p}) \leq (\frac{x'}{p'}) < (a+\delta)(1+\delta)\frac{x}{p},$$

så att

$$A-\delta < (a+\delta)(1+\delta).$$

genom att försöka få δ att närma sig noll.

$A \leq a$. Eftersom också $A \geq a$ och $a + A = 2$ fås att $a = A = 1$, vilket bevisar satsen. [13] □

På det sättet bevisades att gränsen är 1, men Selbergs fullständiga elementära bevis var betydligt längre, och där tillämpade han primtalens basformler samt summerade dem och använde resttermer, så kallad ordokalkyl. Han använde sig även av partiell summering. [14]

Några tidiga närmanden mot primtalssatsens gränsvärde var för övrigt att antalet primtal mindre än 1 000 är 168, medan $\frac{x}{\log x}$ är 145 då $x = 1000$, antalet mindre än 1000000 är 78 498 medan $\frac{x}{\log x}$ är 72 382, antalet primtal mindre än 10 000 000 är 664 579 och $\frac{x}{\log x}$ blir 620 421 och antalet primtal mindre än 1 000 000 000 är 50 847 478 medan $\frac{x}{\log x}$ då blir 48 254 942. Dessa fyra kvoter är 1.159, 1.084, 1.071 och 1.053, så det är inte så konstigt att 1700- och 1800-talsmatematikerna antog att det skulle konvergera mot 1, men eftersom konvergensen är långsam fanns det givetvis också ett visst tvivel - det räcker inte med att något är nästan säkert, det måste vara helt säkert ty matematiken är en exakt vetenskap.

Det största primtalet som har hittats utan hjälp av datorer har 44 siffror, och redan i början av 1950-talet, då datorer var något alldeles nytt, hittades med hjälp av dator ett primtal med nästan 700 siffror [15]

De facto är konvergensen mot 1 i primtalssatsen så långsam att kvoten är 1.019 för $\pi(10^{24})$, d.v.s. alla primtal mindre än 10^{24}, en kvadriljon, ett tal så stort att det motsvarar en biljon biljoner, en triljon miljoner eller en biljard miljarder. Svenskan och de flesta andra språk använder sig av den s.k. långa skalan men på engelska, där den korta skalan (d.v.s. den som endast innehåller

-joner, men inga -jarder) huvudsakligen används (det är även den som gör att en svensk miljard är en engelsk billion), heter detta stora tal som har ytterst få vardagliga tillämpningar septillion. Primtalsfördelningen för detta stora tal visades först 2013 av David J. Platt. Platt nämner dessutom i sin vetenskapliga artikel att det 1870 beskrevs en kombinatorisk modell av den tyske matematikern och astronomen Ernst Meissel (1826-1895) för 10^9, och Meissel lyckades med denna metod nästan beräkna antalet primtal mindre än 10^9, d.v.s. $\pi(10^9)$ korrekt. Denna algoritm förbättrades senare av sex andra matematiker. År 2007 användes denna algoritm för att beräkna $\pi(10^{23})$. [16]

Kapitel 7

Andra talteoretiska satser

Här beskrivs andra talteoretiska satser, som påminner om eller bygger vidare på de centrala resulaten.

En matematiker som var samtida med Bertrand och Tjebysjov, dansken Ludvig Oppermann (1817-1883), förmodade att en sats som påminner om Bertrands postulat gäller. Detta antagande, som han dock aldrig själv bevisade, går under namnet Oppermanns förmodan. Förutom matematiker var han filolog (professor i tyska), samt matematisk direktör vid en livränteanstalt, som kunde klassas som en 1800-talsversion av ett försäkringsbolag. Han förmodade att det för varje heltal $x > 1$ finns åtminstone ett primtal mellan $x(x-1)$ och x^2 och åtminstone ett annat primtal mellan x^2 och $x(x+1)$. På samma sätt kom han fram till att det måste gälla för $\pi(x^2-x) < \pi(x^2) < \pi(x^2+x)$ för $x > 1$ där $\pi(x)$ betecknar antalet primtal som är mindre än eller lika med x. Ändpunkterna av dessa två intervall är en kvadrat mellan två rektangeltal där båda rektangeltalen är dubbelt så stora som ett par av triangulära siffror. Summan av paren av de triangulära siffrorna är kvadraten. Hans förmodan är bevisad nu men beviset är mycket komplicerat och tas inte upp här. Den brasilianske matematikern Edigles Guedes bevisade denna sats elementärt 2013. [17]

Så gott som alla matematiker har hört om Fermats stora sats, eller Fermats sista sats som den brukar kallas på många andra språk. Det anses vara det svåraste matematiska problem som har blivit löst.

Den säger att ekvationen, $a^n + b^n + c^n$ som bygger på den mest kända matematiska satsen, Pythagoras sats, inte har några lösningar för positiva heltal $n > 2$. Alltså att det inte finns några andra heltalslösningar än för det mycket

välbekanta specialfallet $n = 2$. (Pythagoras sats)

Pierre de Fermat formulerade satsen 1637. Fermat hade skrivit på en lapp: "Jag har ett i sanning underbart bevis för detta påstående, men marginalen är alltför trång för att rymma detsamma."("Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet"). Fermats bevis, om det någonsin överhuvudtaget formulerades, har inte hittats, men det är i praktiken klart att Fermat inte har bevisat detta. Så gott som all matematik som behövs för beviset har uppfunnits av matematiker som levt långt efter Fermat. Till slut bevisades satsen av engelsmannen Andrew Wiles 1995. Det tog åtta år för Wiles att bevisa detta, och 1993 trodde han t.o.m. att han hade bevisat satsen, men beviset visade sig innehålla ett fel så han var tvungen att omarbeta beviset. Två år senare var satsen till slut bevisad. Fermats stora sats är en talteoretisk sats men det mesta i Wiles bevis hade inte med talteori att göra. Wiles metoder var inte kända på 1600-talet - många av metoderna (som exempelvis utvecklingarna av de modulära formlerna) uppfanns först på 1900-talet. Redan som tioåring bekantade han sig med satsen på det lokala biblioteket.

Fermats stora sats är en sats vars formulering är mycket enkel men beviset är 150 sidor långt och kan i sin helhet förstås av endast en handfull matematiker i hela världen. [18]

Eulers förmodan bygger på Fermats stora sats, men den har motbevisats vid flera tillfällen. T.ex. är $27^5 + 84^5 + 110^5 + 133^5 = 144^5$. [19]

Inom analytisk talteori, ett delområde av matematiken, är Friedlander–Iwaniecs sats ett resultat som säger att det finns oändligt många primtal av formen $a^2 + b^4$. De första primtalen av den typen är

2, 5, 17, 37, 41, 97, 101, 137, 181, 197, 241, 257, 277, 281, 337, 401, 457, 577, 617, 641, 661, 677, 757, 769, 821, 857, 881, 977, ... Satsen bevisades 1997 av John Friedlander och Henryk Iwaniec genom Enrico Bombieris metoder och tekniker. Satsen säger dock inte att det finns oändligt många primtal av formen $a^2 + 1$. Det är fortfarande okänt om det finns oändligt många sådana primtal eller inte. De första primtalen av den formen är

2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101, 8837, 12101, 13457, 14401 och 15377. [20]

Ännu är det inte klart (även om det anses mycket osannolikt) om det finns något udda tal som är ett perfekt tal, d.v.s. ett tal som är lika med summan av

alla sina delare, ej heller om det finns oändligt många primtalstvillingar, d.v.s. två primtal som bara skiljer med 2, t.ex. 3 och 5, 5 och 7, samt 17 och 19. [21]

Kanske någon av dessa är någon av de följande matematiska, eller åtminstone talteoretiska satser, som kommer att bli bevisade eller motbevisade.

Kapitel 8

Avslutning

Avslutningsvis kan det konstateras att flera intressanta och viktiga talteoretiska satser nu har blivit bevisade. Liknande, kanske t.o.m. just dessa satser, har matematikerna garanterat funderat på långt innan Bertrands, Tjebysjovs och Erdös tid.

Bertrands postulat är för övrigt ett svagt resultat, för oftast finns det betydligt fler än ett primtal mellan ett godtyckligt tal n och $2n$. T.ex. mellan 100 och 200 finns 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, alltså hela 21 stycken. Mellan 500 och 1 000 är 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997 primtal, d.v.s. 73 stycken.

När det kommer till tillämpningen av Bertrands postulat, är det ännu inte bevisat om detta också gäller i intervallet $3n < p < 4n$. Det är däremot klart att det inte gäller i intervallet $4n < p < 5n$, inte heller om $4n \leq p \leq 5n$ ty om $n = 2$ fås $8 < p < 10$ och inget utav 8, 9 eller 10 är något primtal.

Primtalssatsen var ett mycket stort matematiskt problem men numera en viktig sats med många tillämpningar. Detsamma gäller även Bertrands postulat och andra elementära bevis för primtalens egenskaper.

Eulers sats är en generalisering av Fermats lilla sats och den används i RSA-kryptering, som kryptering i datorer baserar sig på. Carmichaels sats i sin tur påstår att det n:te Fibonaccitalet har en eller flera primtalsdelare som inte delar

något av de föregående Fibonaccitalen.

Än idag söks det efter allt större primtal med hjälp av superdatorer. De största kända primtalen är alla Mersennetal, eftersom det finns en effektiv metod som avgör om ett Mersennetal är ett primtal eller inte. Ett Mersennetal är ett heltal på formen $2^n - 1$. [21] Alla Mersennetal är udda, och några triviala exempel på Mersennetal är 1, 3, 7, 15, 31 och 63.

Det största hittills kända primtalet är $2^{82589933} - 1$, och är följaktligen ett Mersennetal. Det upptäcktes i december 2018, och innehåller hela 24 862 048 siffror. [22]

Kapitel 9

Appendix: Mathematica-koder och skiss över de 1 000 första primtalen

PrimeQ[Range[2, 10000]] för att få fram vilka tal mellan 2 och 10000 som är primtal

l = Table[i, PrimeQ[i], i, 2, 10000] för att få fram vilka tal mellan 2 och 10000 som är primtal, med siffrorna med

primes = Cases[l, , True][[All, 1]] för att skriva ut alla primtal inom 2 och 10000

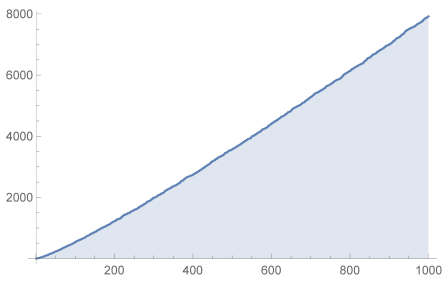
Min[primes] För att få det minsta primtalet

Table[Prime[n], n, 10000] För att få de 10 000 första primtalen

Table[Prime[n], n, 1000] För att få de 1 000 första primtalen

DiscretePlot[Prime[n], n, 1000] För att rita en graf $\frac{p}{n}$ för de 1 000 första primtalen

(Räcker till 7 919).



Figur 9.1: Skiss över de 1000 första primtalen.

Litteraturförteckning

[1] Bertrands postulat , https://mathworld.wolfram.com/BertrandsPostulate.html Hämtad 12.3.2020

[2] Joseph Bertrand, https://www.britannica.com/biography/Joseph-Bertrand Hämtad 12.3.2020

[3] Pafnuty Chebyshev, B.N.Delone, The St. Petersburg School of Number Theory, Hämtad 8.4.2020

[4] Erdös bevis, Erdös, P : Beweis eines Satzes von Tschebyschef, 1932. https://users.renyi.hu/ perdos/1932-01.pdf Erdös bevis. Hämtad 25.10.2018 Här är för övrigt en länk till många av Erdös verk: https://users.renyi.hu/ perdos/Erdos.html

[5] Paul Erdös, https://www.britannica.com/biography/Paul-Erdos Hämtad 12.3.2020

[6] Graham, R. L. m.fl. : A Algorithms and Combinatorics 13 Editorial Board https://epdf.tips/the-mathematics-of-paul-erds-i-algorithms-and-combinatorics.html Hämtad 3.10.2018

[7] Bollobas, B. "Journal of the Royal Statistical Society. Series D (The Statistician), Vol. 48, No. 2 (1999) https://www.jstor.org/stable/2681192?seq=1 metadatainfotabcontents Hämtad 3.10.2018

[8] Peter Frankl, https://peoplepill.com/people/peter-frankl-1/

[9] Youtube-videon, https://www.youtube.com/watch?v=DyzF54pyiA8 Hämtad 3.10.2018

[10] Mathrefresher, Multiplicity of prime factor http://mathrefresher.blogspot.com/2009/11/multiplicity-of-prime-factor.html Hämtad 21.11.2018

[11] El Bacraoui, M., : Primes in the Interval [2n, 3n] https://pdfs.semanticscholar.org/2c0c/af5bbaa02dcb7eeeebc5044a9079fc21abfe.pdf Hämtad 4.12.2018

[12] Primtal.nb, Mathematica

[13] Goldfield, D. (2003) : The Elementary Proof of the prime number theorem, an historical perspective. I Chudnovsky, D, Chudnovsky, G, Nathanson, M: Number Theory", New York Seminar, Spengler, s 179-192

[14] Selberg, A (1948) : An Elementary Proof of the Prime-Number Theorem. Annals of Mathematics, Second Series, Vol. 50, No. 2 (Apr. 1949), s. 305-313

[15] Hardy, G. H, Wright, E. M., The Theory of Numbers, 1938, tryckt 1954, s. 6-10, 340-370

[16] Platt, David J., : Computing $\pi(x)$ analytically, 2013, s 1-12 Hämtad 29.5.2020

[17] Oppermanns förmodan, Guedes, E : An Elementary Proof of Oppermann's Conjecture https:/vixra.org/pdf/1303.0047v1.pdf, http://vixra.org/pdf/1502.0134v1.pdf Hämtad 8.10.2018

[18] Singh, S. : Fermats gåta, 2005, 352 s.

[19] https://mathworld.wolfram.com/EulersSumofPowersConjecture.html Hämtad 3.6.2020

[20] https://www.theoremoftheday.org/NumberTheory/FI/TotDFI.pdf Hämtad 3.6.2020

[21] http://www.axler.net/MathVsSilicon.pdf Hämtad 3.6.2020

[22] https://www.npr.org/2018/12/21/679207604/the-world-has-a-new-largest-known-prime-number?t=1590334890113 Hämtad 24.5.2020