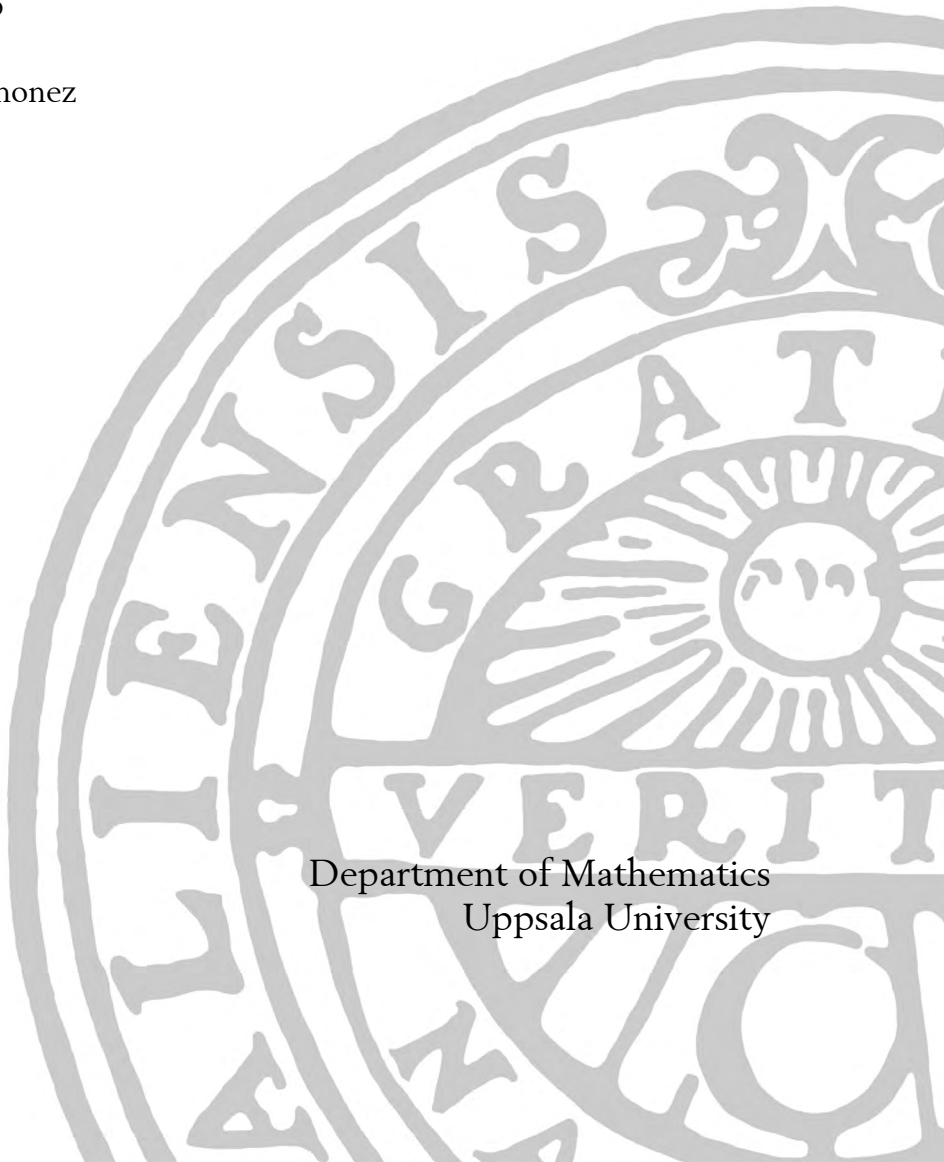
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2019:20

Fermats lilla sats – dess historia och några tillämpningar

Daniel Backeman

Examensarbete i matematik, 15 hp
Handledare: Gunnar Berg
Examinator: Veronica Crispin Quinonez
Juni 2019



Department of Mathematics
Uppsala University

Innehåll

Historia om Fermat och hans satser

Pierre de Fermat föddes 1607 i Beaumont de Lomagne i södra Frankrike, nära Toulouse.[1] Till yrket var han jurist och matematiken var hans sysselsättning på fritiden. Han levde under en tid när matematik inte ansågs vara ett yrke att dedikera sitt liv åt, vilket innebar att det inte fanns en tydlig definition av vad matematik är, hur det bör studeras eller hanteras.[2] Det skulle kunna vara en förklaring till varför det inte finns några nerskrivna bevis av Fermat för de två satserna som han idag är mest känd för; Fermats lilla sats och Fermats stora, alternativt sista, sats. Många matematiker har genom åren försökt att bevisa satserna med varierad framgång. Den stora satsen har sannolikt ett rekord för antal felaktiga bevis och det dröjde till 1995 innan Andrew Wiles publicerade ett bevis som godtogs av övriga matematiker. Det är dock väldigt osannolikt att Fermat behärskade den matematik Wiles använde, vilket fortfarande får matematiker att ställa sig frågan huruvida Fermat verkligen hade bevisat satsen själv eller om han bara hade tur när han formulerade den.[3] I kontrast kom den lilla satsen att bevisas relativt snabbt, redan på 1700-talet, och det anses vara rimligt att anta att Fermat behärskade den matematik som krävs för att bevisa satsen, vilket gör det troligt att han faktiskt hade formulerat ett eget bevis som helt enkelt är spårlöst borta.[4]

Fermats lilla sats på två sätt

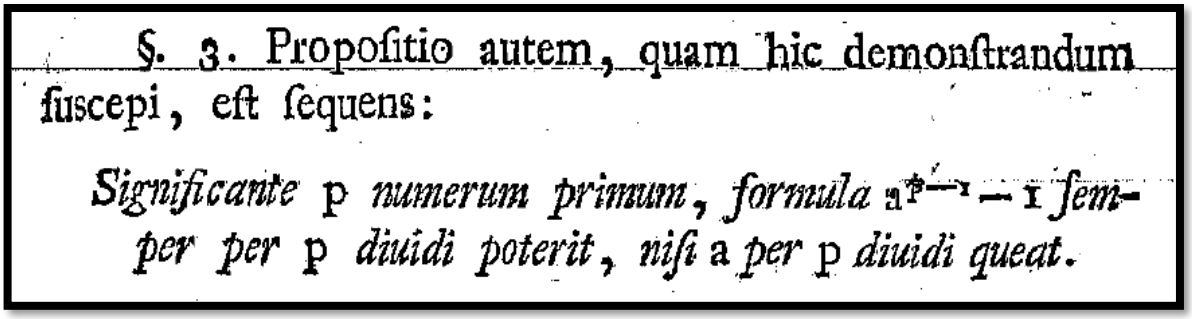
18:e oktober 1640 skrev Fermat följande i ett brev till Frénicle de Bessy;

Givet ett primtal p, och valfri geometrisk talföljd av slaget $1, a, a^2, etc.,$ *så måste p dela ett tal* $a^n - 1$ *för vilket n delar* $p - 1$*; om N sedan är en multipel av det minsta möjliga n så delar p även* $a^N - 1$.[5] [Min översättning]

Det är den första kända formuleringen av vad som komma att kallas för Fermats lilla sats. Fermat kom dock aldrig, till vår vetskap, att bevisa satsen, varken i brevet till de Bessy eller senare. I brevet påstår han sig ha ett formulerat bevis, men att det är för långt för att skickas med. Med tiden har satsen generaliserats av både Leibniz och Euler, varav den senare var först med att publicera ett bevis 1736 i en text vid namn *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio*.[6]

---

[1] Weil 1983, s. 39.
[2] Mahoney 1994, s. 1–2.
[3] Stewart & Tall 2002, s. 6.
[4] Weil 1983, s. 56.
[5] Weil 1983, s. 56.
[6] Weil 1983, s. 56.



§. 3. Propoſitio autem, quam hic demonſtrandum ſuscepi, eſt ſequens:

Significante p *numerum primum, formula* $a^{p-1} - 1$ *ſemper per* p *diuidi poterit, niſi* a *per* p *diuidi queat.*

Utdrag ur Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio där Fermats lilla sats är formulerad av Euler.

Dagens matematiker skulle dock snarare känna igen satsen enligt följande formulering;

$$Om\ p\ \text{är}\ ett\ primtal\ och\ a\ \text{är}\ ett\ heltal\ sådant\ att\ p \nmid a, \text{så}\ gäller\ att$$
$$a^{p-1} \equiv 1\ (mod\ p).$$

Alternativt denna formulering som är vanligt förekommande;

$$Om\ p\ \text{är}\ ett\ primtal, \text{så}\ gäller\ för\ alla\ heltal\ a\ att$$
$$a^p \equiv a\ (mod\ p).$$

Vilken formulering som kom först, och vilken som är en följd av den andra, verkar inte vara helt klart. I *Elementary Number Theory* av Kenneth H. Rosen benämns båda som Fermats lilla sats utan att på något sätt särskilja dem åt. Med det sagt härleder Rosen den andra formuleringen utifrån den första.[7]

I dag brukar man bevisa Fermats lilla sats på två olika sätt; antingen via modulo-räkning eller induktion. Nedan följer två härledningar kopplade till respektive tidigare nämnda formuleringar av satsen.

Härledning med hjälp av modulo-räkning

$$Sats\ 1. Om\ p\ \text{är}\ ett\ primtal\ och\ a\ \text{är}\ ett\ heltal\ sådant\ att\ p \nmid a, \text{så}\ gäller\ att$$
$$a^{p-1} \equiv 1\ (mod\ p).$$

Betrakta heltalen $a, 2a, \dots, (p-1)a$. Inget av dessa tal är delbart med p, för om $p \mid ja$ och $p \nmid a$ så måste $p \mid j$. Det går inte då $1 \leq j \leq p-1$. Dessutom är inga par av talen $a, 2a, \dots (p-1)a$ kongruenta modulo p. För att förstå det så börjar vi med att anta $ja \equiv ka\ (mod\ p)$, där $1 \leq j \leq k \leq p-1$. Eftersom SGD$(a,p) = 1$ så är $j \equiv k\ (mod\ p)$, vilket inte går då både j och k är positiva heltal som är mindre än $p-1$.

[7] Rosen 2010, s. 219–220. Jämför sats 6.3 med 6.4.

Utifrån detta och eftersom $a, 2a, \dots, (p-1)a \not\equiv 0 \ (mod\ p)$ så vet vi att resterna av talen $a, 2a, \dots, (p-1)a$ modulo p måste vara heltalen $1, 2, \dots, (p-1)$. Det innebär också att produkten av heltalen $a, 2a, \dots, (p-1)a$ måste vara kongruent med produkten av heltalen $1, 2, \dots, (p-1)\ (mod\ p)$.

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1)\ (mod\ p)$$

Detta kan skrivas om till

$$a^{p-1}(p-1)!\ \equiv (p-1)!\ (mod\ p)$$

Eftersom $SGD((p-1)!, p) = 1$ så kan vi dividera båda sidorna med $(p-1)!$ för att få satsen.

$$a^{p-1} \equiv 1\ (mod\ p)$$

Härledning med hjälp av induktion

Vi kan börja med att observera att föregående formulering av Fermats lilla sats inte kan härledas med induktion på grund av det villkor som finns för relationen mellan a och p. Den kommande formuleringen har inget villkor alls för relationen mellan a och p, och på det sättet mer generell, vilket möjliggör induktion som härledningsmetod.

Sats 2. Om p är ett primtal, så gäller för alla naturliga tal a att

$$a^p \equiv a\ (mod\ p)$$

Satsen gäller för $a = 1$ eftersom $1^p \equiv 1\ (mod\ p)$ betyder att $p \mid 0$, vilket alltid är sant, och därmed har vi vår induktionsbas.

$$1^p \equiv 1\ (mod\ p)$$

Vi antar nu att satsen gäller för valfritt positivt heltal $a = b$ och vi behöver då visa att den även gäller för $b + 1$. Vi introducerar binomialkoefficienten

$$\binom{p}{k} = \frac{p(p-1) \cdot \dots \cdot (p-k+1)}{k!}$$

där det gäller att p och k är naturliga tal samt att $1 \leq k \leq p-1$. Vi kan då notera två saker. För det första så är $\binom{p}{k}$ också är ett naturligt tal, nämligen antalet delmängder med k element valda ur p element. För det andra delar p täljaren men inte nämnaren efter som $0 < k < p-1 < p$ och p är ett primtal. Med det i åtanke får vi att

$$(b+1)^p = \sum_{k=0}^{p} \binom{p}{k} b^k 1^{p-k} = \sum_{k=0}^{p} \binom{p}{k} b^k = b^p + b^0 + \sum_{k=1}^{p-1} \binom{p}{k} b^k$$

Men eftersom $\binom{p}{k}$ alltid är delbart med p då p är ett primtal som inte delar $k!$ så är $\binom{p}{k} \equiv 0\ (mod\ p)$. Då kan vi förenkla uttrycket enligt följande

$$b^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} b^k \equiv b^p + 1 \equiv b + 1\ (mod\ p)$$

Enligt induktionsantagandet

Då vi har visat att induktionsbasen och induktionssteget är sanna så följer det av induktionsaxiomet att satsen gäller för alla naturliga tal och att den därmed är bevisad med hjälp av induktion.

Vi avrundar detta avsnitt om Fermats lilla sats genom att illustrera den i två exempel.

$$Om\ a = 4\ och\ p = 5\ så\ säger\ satsen\ att$$

$$4^4 - 1 \equiv 1\ (mod\ 5)$$

$$4^4 = 256 = \ 51 \cdot 5 + 1 \equiv 1\ (mod\ 5)$$

$$eller$$

$$4^5 \equiv 4\ (mod\ 5)$$

$$4^5 = 1024 = \ 204 \cdot 5 + 4 \equiv 4\ (mod\ 5)$$

Olika versioner av originalformulering

Hur Fermat formulerade sig i sitt brev till Frénicle de Bessy verkar inte helt entydigt. Den tidigare översättningen utgick ifrån Weils tolkning av brevet. Bob Burn, professor i matematik vid University of Exeter, presenterar en annan tolkning i artikeln *Fermat's little theorem – proofs that Fermat might have used* från 2002 publicerad i *The Mathematical Gazette*, en tidskrift som ges ut av University of Cambridge. Den lyder som följer;

Utan undantag så måste varje primtal dela en av potenserna -1 *i valfri talföljd, och den exponenten delar det givna primtalet* -1.

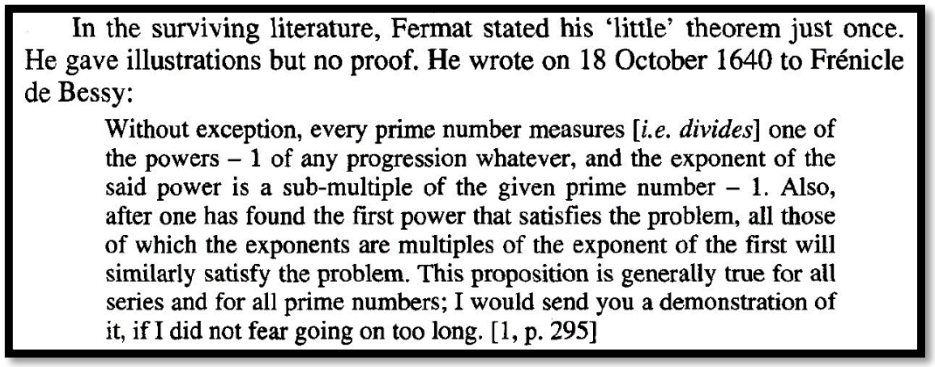
Vidare, om man har funnit den första exponenten som uppfyller ovanstående kriterier, så följer det *att alla multipler av exponenten också uppfyller ovanstående kriterier. Denna sats gäller för alla talföljder och alla primtal.*

Jag skulle skicka en redovisning av beviset om jag inte fruktade att det är för långt.

[Min översättning][8]

[8] Burn 2002, s. 415.

Direkt kan man notera att denna formulering är markant mycket längre än den som presenterats av Weil tidigare i detta arbete. Vi kan också notera att Burns tolkning är mycket mer sparsam med tecken och notationer vilket går i linje med hur matematiken antagligen såg ut på Fermats tid när det kommer till allmänna konventioner i det matematiska språket.



In the surviving literature, Fermat stated his 'little' theorem just once. He gave illustrations but no proof. He wrote on 18 October 1640 to Frénicle de Bessy:

> Without exception, every prime number measures [*i.e. divides*] one of the powers – 1 of any progression whatever, and the exponent of the said power is a sub-multiple of the given prime number – 1. Also, after one has found the first power that satisfies the problem, all those of which the exponents are multiples of the exponent of the first will similarly satisfy the problem. This proposition is generally true for all series and for all prime numbers; I would send you a demonstration of it, if I did not fear going on too long. [1, p. 295]

Burns tolkning av Fermats formulering till de Bessy.

I samarbete med min handledare har även jag översatt originaltexten för att jämföra med de två översättningarna av Burn och Weil. Den lyder som följande;

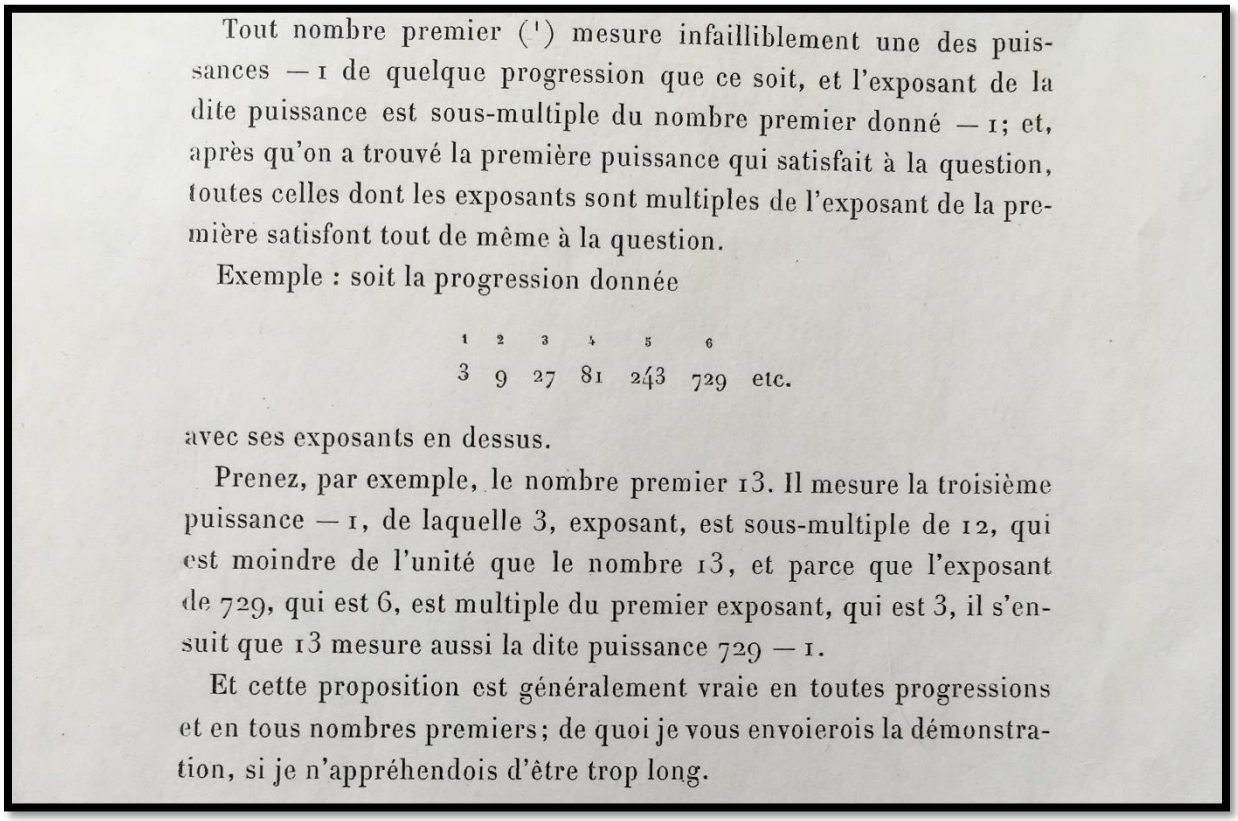
Nu synes det mig vara viktigt att jag berättar för Er om den grund på grund jag stöder mina bevis av allt som har att göra med geometriska följder, nämligen: Varje primtal mäter [*delar*] *nödvändigtvis en av potenserna* -1 *i vilken följd som helst och exponenten i denna potens är submultipel* [*delar*] *det givna primtalet* -1*; och sedan man hittat den första potensen som uppfyller villkoret kommer de vars exponenter är multipler av exponenten till den första alla att uppfylla villkoret.* [...] *Och denna proposition är generellt sann för alla följder och för alla primtal; jag skulle skicka en redovisning av beviset om jag inte fruktade att det är för långt.* [Min översättning][9]

Vår översättning är tydligt mycket mer lik Burns tolkning än Weils. Det är förbryllande att en sådan stor matematiker som Weil var så slarvig med sin historiska framställning av satsen. Det är inte uppenbart att exponent-notationen som vi känner till idag är något Fermat använde sig av, eller ens kände till. Därför blir det farligt att Weil använder sig av den notationen när han använder sig utav citattecken och refererar till originalbrevet, vilket kan leda läsaren till att tro att det är Fermat själv som har uttryckt sig så. Inom den historiska disciplinen är man extremt noga med hur citat används av respekt för källan och hade aldrig tillåtit ett sådant felcitat. Det som gör

[9] Fermat 1894, s. 209.

detta lite intressant är att Weil har ett eget kapitel i boken *Proceedings of the International congress of mathematicians, Helsinki 1978, volume 1* om relationen mellan matematik och matematisk historia och vilka som är mest kvalificerade och därmed bör studera matematisk historia.[10] I kapitlet framhäver han vikten av matematisk kunskap för att studera matematisk historia och därför menar han att matematiker är mer lämpad. Samtidigt tyder en sådan relevant miss som denna att historikerns noggrannhet när det kommer till källhantering är nödvändig och något man bör ta efter om man ska exkludera dem från arbetet kring matematisk historia.

Det ska även påpekas att även Burns citat inte är helt korrekt då Fermat har med ett exempel i sin formulering. Den uppmärksamme har noterat att i vår översättning så är något bortklippt, vilket



Tout nombre premier (') mesure infailliblement une des puissances — 1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné — 1; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.

Exemple : soit la progression donnée

1	2	3	4	5	6	
3	9	27	81	243	729	etc.

avec ses exposants en dessus.

Prenez, par exemple, le nombre premier 13. Il mesure la troisième puissance — 1, de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance 729 — 1.

Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Fermats lilla sats av Fermat själv. Notera exemplet i mitten av formuleringen som varken Weil eller Burn tar upp.

är det exemplet, något som inte framgår i Burns citat. Troligtvis beror det på att Burn inte fann exemplet intressant, men ur ett källhanteringsperspektiv är det viktigt att vara noga med saker som dessa för att läsaren inte ska vilseledas eller få en felaktig bild av hur originalet ser ut.

Avslutningsvis kan man också notera att Fermat, utifrån det brevet han skriver till de Bessy, verkar missar villkoret att p ej får dela a, något som Weil inte heller påpekar i sin text om detta.

[10] Lehto 1980, s. 227-236.

Däremot tar Euler upp detta villkor i sitt bevis av satsen som framgår av texten överst på sidan 2.[11]

Eulers φ-funktion

Som nämnts kom Euler att bevisa Fermats lilla sats knappt 100 år efter att Fermat formulerade den till de Bessy, men han kom även att generalisera satsen till att inkludera sammansatta tal 1760.[12] För att gå igenom generaliseringen behöver vi dock först förstå Eulers φ-funktion som definieras enligt följande;

$$Definition\ 1.\ Förutsatt\ att\ n\ är\ ett\ naturligt\ tal\ så\ gäller\ det\ att\ \varphi(n)\ betecknar\ antalet\ naturliga\ tal\ \leq n\ som\ är\ relativt\ prima\ med\ n.$$ [13]

Att två tal, exempelvis a och b, är relativt prima innebär att $\text{SGD}(a, b) = 1$. Det betyder till exempel att $\varphi(12) = 4$ då talen $2, 3, 4, 6, 8, 9$ och 10 alla har en gemensam delare med 12 som är > 1 medan $1, 5, 7$ och 11 har 1 som SGD. Observera att den gemensamma delaren kan vara olika för de olika talen.

Det finns några intressanta följdsatser till Eulers φ-funktion. Den första, och kanske mest intuitiva, är

$$Korollarium\ 1.\ Givet\ att\ p\ är\ ett\ primtal\ så\ gäller\ \varphi(p) = p - 1.$$

I och med att p är ett primtal kan inga av talen $1, 2, \ldots, p - 1$ ha en gemensam delare med p som är > 1. Nästa sats är inte lika intuitiv och lyder som följande;

$$Korollarium\ 2.\ Givet\ att\ p\ är\ ett\ primtal\ så\ gäller\ \varphi(p^{\alpha}) = p^{\alpha-1}(p - 1).$$

Vi kan notera att mellan 1 och p^{α} så finner vi multiplerna av p;

$$1 \cdot p, 2 \cdot p, \ldots p^{\alpha-1} \cdot p$$

Åter igen så gör det faktum att p är ett primtal det uppenbart att dessa multipler är de enda naturliga talen $\leq p^{\alpha}$ som kan dela p^{α}. Således får vi att $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p - 1)$ och följdsatsen är därmed bevisad.

[11] Euler 1741, s. 143.
[12] Rosen 2010, s. 234.
[13] Nagell 1950, s. 23.

Något som inte är så intuitivt är att Eulers φ-funktion är multiplikativ. Men innan vi kan härleda det måste förstå restklasser och restsystem, något som även behövs när vi ska förstå Eulers generalisering av Fermats lilla sats.

Restklasser och restsystem

Två tal, a och b, tillhör samma restklass modulo n om de har samma rest modulo n, det vill säga $a \equiv b \ (mod\ n)$. Notera att det finns $n-1$ antal restklasser för ett godtyckligt positivt heltal n, nämligen resterna $1, 2, \dots, n-1$. Exempelvis tillhör 13 och 6 samma restklass modulo 7 då $13 = 7 + 6 \equiv 6 \ (mod\ 7)$.

Det finns två typer av restsystem; fullständiga och reducerade. Ett fullständigt restsystem består av n olika heltal som representerar de olika restklasserna modulo n. Ett exempel på ett fullständigt restsystem är mängden $\{2, 6, 10\}$ modulo 3 då $2 \equiv 2 \ (mod\ 3)$, $6 \equiv 0 \ (mod\ 3)$ och $10 \equiv 1 \ (mod\ 3)$.

Ett reducerat restsystem är en talmängd som består av $\varphi(n)$ tal som representerar alla olika restklasser till modulo n som även är relativt prima till n. Exempelvis är talmängden $\{1, 5\}$ ett reducerat restsystem av modulo 6 då $\varphi(6) = 2$ eftersom $\text{SGD}(1, 6) = 1$ och $\text{SGD}(5, 6) = 1$. Utifrån denna definition är det inte svårt att komma till insikten att om n är ett primtal p så kan ett reducerat restsystem bestå utav talen $1, 2, \dots, p-1$ och därför är $\varphi(p) = p - 1$. För ett reducerat restsystem modulo n gäller det även att alla talen i talmängden är parvis inkongruenta modulo n.

Eulers φ-funktion och multiplikativitet

Nu är vi redo för att härleda att Eulers φ-funktion är multiplikativ och vi formulerar det som en sats;

$$Sats\ 3. Om\ SGD(m_1, m_2) = 1\ och\ m = m_1 \cdot m_2\ så\ gäller\ det\ att$$
$$\varphi(m) = \varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

Låt $F(m)$, $F(m_1)$ och $F(m_2)$ beteckna de tre fullständiga restsystemen för m, m_1 och m_2. I och med att $m = m_1 \cdot m_2$ så måste $F(m)$ och den cartesiska produkten $F(m_1) \times F(m_2)$ innehålla lika många element, det vill säga m stycken. Med hjälp av ett tal $x \in F(m)$ och $j = 1$ eller 2 så kan vi ta fram ett unikt tal ur m_j som uppfyller att $x_j \equiv x \ (mod\ m_j)$. Vi introducerar sedan funktionen $\omega: F(m) \to F(m_1) \times F(m_2)$ och definierar den till att $\omega(x) = (x_1, x_2)$.

För att illustrera hur detta byggs upp och hur funktionen används så tar vi hjälp av ett exempel. Vi inleder med att sätta $m_1 = 3, m_2 = 5$ och således blir då $m = 3 \cdot 5 = 15$. Då kan vi ta valfritt tal $x \in F(m)$, exempelvis 8, och se att för $j = 1$ så får vi $x_1 \equiv 8 \ (mod\ 3)$ vilket ger oss att $x_1 = 2$. För $j = 2$ får vi istället att $x_2 \equiv 8 \ (mod\ 5)$ vilket ger oss $x_2 = 3$. Därmed blir $\omega(8) = (2, 3)$. På samma sätt kan vi bilda ett talpar för varje restklass modulo 15 med hjälp av vår funktion ω.

Nästa steg är att visa att avbildningen mellan mängderna $F(m)$ och $F(m_1) \times F(m_2)$ är en bijektion, men då mängderna har lika många element räcker det med att visa att avbildningen är surjektiv. Surjektiviteten följer dock direkt från den kinesiska restsatsen[14] i och med att $(x_1, x_2) \in F(m_1) \times F(m_2)$ och då säger satsen att det finns ett unikt $x \in F(m)$ sådant att $x \equiv x_1 \ (mod\ m_1)$ och $x \equiv x_2 \ (mod\ m_2)$. Med andra ord så är $\omega(x) = (x_1, x_2)$ och avbildningen ω är således bijektiv.

Nu ska vi istället betrakta vad som händer med avbildningen ω på det reducerade restsystemet $R(m)$. För det första vet vi att om $SGD(x, m) = 1$ så följer det att $SGD(x, m_1) = SGD(x, m_2) = 1$. För det andra vet vi att om $x \equiv x_1 \ (mod\ m_1)$ så gäller ekvivalensen $SGD(x, m_1) = 1 \Leftrightarrow SGD(x_1, m_1) = 1$ samt att om $x \equiv x_2 \ (mod\ m_2)$ så gäller ekvivalensen $SGD(x, m_2) = 1 \Leftrightarrow SGD(x_2, m_2) = 1$.

Åter igen illustrerar vi detta med ett exempel och använder samma mängder som i förra exemplet. Vi har alltså $m_1 = 3$ och $m_2 = 5$ vilket ger oss $m = 15$, och vi kan ta talet $x = 14$ och se att $SGD(14, 15) = SGD(14, 3) = SGD(14, 5) = 1$. Vi kan även se att $14 \equiv 2 \ (mod\ 3)$ och då gäller att $SGD(14, 3) = SGD(2, 3) = 1$ och på samma sätt se att $14 \equiv 4 \ (mod\ 5)$ vilket ger att $SGD(11, 5) = SGD(4, 5) = 1$.

Vi har nu visat ekvivalensen $x \in R(m) \leftrightarrow \ \omega(x) \in R(m_1) \times R(m_2)$ och som visar att avbildningen därmed är bijektiv. I och med att $R(m)$ har $\varphi(m)$ element och $R(m_1) \times R(m_2)$ har $\varphi(m_1) \cdot \varphi(m_2)$ element samt det faktum att en bijektion kräver att båda mängderna har samma antal element, har vi därmed visat att satsen stämmer.

[14] För en härledning av den kinesiska restsatsen rekommenderar jag Lars-Åke Lindahls kompendium *Elementär Talteori*, s. 30–32.

Eulers sats

Med hjälp av Eulers φ-funktion och restsystem kan vi även förstå Eulers generalisering av Fermats lilla sats. Euler lyckades nämligen visa att;

$$\textit{Sats } 4. \textit{ Om } n \text{ är } \textit{ett positivt heltal och } a \textit{ ett heltal som } \text{är } \textit{relativt prima med } n$$
$$\textit{så gäller det att } a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Till skillnad från Fermats lilla sats så har inte Eulers sats något villkor om att a eller n behöver vara primtal. Det ska samtidigt påpekas att det faktum att Fermats lilla sats förutsätter ett primtal i exponenten används inom vissa delar av talteorin, något som vi kommer att ta upp senare.

För att återgå till beviset av generaliseringen så inleder vi med att konstruera ett reducerat talsystem $a_1, a_2, \dots, a_\varphi$ modulo n, där $\varphi = \varphi(n)$. Vi kan även betrakta restsystemet $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_\varphi$ och konstatera att även det är reducerat. För att förstå detta får vi börja med att påminna oss om att a och n är relativt prima enligt satsens definition, vilket då leder till att $\text{SGD}(a \cdot a_i, n) = 1$. Vidare så måste talen $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_\varphi$ parvis vara inkongruenta modulo n eftersom $a \cdot a_i \equiv a \cdot a_j \ (mod\ n)$, vilket medför att $a_i \equiv a_j \ (mod\ n)$. Utifrån detta kan vi således konstatera följande;

$$a \cdot a_1, a \cdot a_2, \dots, a \cdot a_\varphi \ \equiv a_1 \cdot a_2 \cdot \ \dots \cdot \ a_\varphi \ (mod\ n)$$

Om vi nu dividerar båda sidorna med produkten av talen $a_1, a_2, \dots, a_\varphi$ så får vi att

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Generaliseringen, och då även satsen, är därmed bevisad.

Pseudoprimtal

Pseudoprimtal är sammansatta tal som uppfyller ett eller flera specifika ”kriterium” som primtal uppfyller. Det finns olika typer av pseudoprimtal-grupper beroende på vilka kriterier de uppfyller. Den mängd som är i fokus för detta arbete är kanske en av de viktigaste, nämligen Fermats pseudoprimtal. De definieras enligt följande;

$$\textit{Definition } 2. \textit{ Låt } b \textit{ vara ett positiv heltal och } n \textit{ ett sammansatt positivt heltal.}$$
$$\textit{Då kallas } n \textit{ ett pseudoprimtal till basen } b \textit{ om } b^n \equiv b \ (mod\ n).$$

För att illustrera vad det betyder kan vi betrakta talet $n = 341 = 11 \cdot 31$. Enligt Fermats lilla sats vet vi att $2^{10} \equiv 1 \ (mod\ 11)$ vilket vi kan utnyttja för att se $2^{340} = (2^{10})^{34} \equiv 1 \ (mod\ 11)$.

Dessutom kan vi se att $2^{340} = (2^5)^{68} = (32)^{68} \equiv 1\ (mod\ 31)$. Således vet vi att $2^{340} \equiv 1\ (mod\ 341)$ trots att 341 inte är ett primtal och därmed kallar vi 341 för ett pseudoprimtal till basen 2 och tillhör talmängden Fermats pseudoprimtal.

För att förstå det sista steget får vi ta hjälp av följande lemma:

$$Lemma\ 1. Om\ a \equiv b\ (mod\ p_1)\ och\ a \equiv b\ (mod\ p_2), där\ p_1\ och\ p_2\ är\ olika\ primtal,$$
$$så\ gäller\ det\ att\ a \equiv b\ (mod\ p_1 \cdot p_2).$$

För det första så måste p_1 och p_2 vara inkongruenta med varandra i och med att de är olika primtal. För det andra så kan vi notera att $a \equiv b\ (mod\ p_1)$ är ekvivalent med $p_1 \mid (a - b)$, vilket innebär att det finns ett tal k_1 sådant att $a - b = p_1 \cdot k_1$. Samtidigt så gäller det att $p_2 \mid (a - b)$ och således gäller det även att $p_2 \mid p_1 \cdot k_1$, och då måste $p_2 \mid k_1$. Sammantaget betyder det att $a - b = p_1 \cdot p_2 \cdot k_2$ och vi ser att $p_1 \cdot p_2 \mid (a - b)$ som kan skrivas om till $a \equiv b\ (mod\ p_1 \cdot p_2)$ och lemmat är därmed bevisat.

Det går att visa att det finns oändligt många pseudoprimtal till basen 2. Först behöver vi dock konstatera att

$$Lemma\ 2. Om\ d \mid n\ så\ gäller\ att\ 2^d - 1 \mid 2^n - 1$$

I och med att d delar n så måste det finnas ett positivt heltal t som ger $dt = n$. Vi kan även notera att

$$(2^d)^t - 1 = 2^{dt} - 1 = (2^d - 1)\left(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 1\right)$$

samt att $2^{dt} = 2^n$, vilket kan skrivas om till $2^n - 1 = (2^d - 1)(2^{d(t-1)} + \cdots + 1)$ och därmed kan vi till slut se att $(2^d - 1)|(2^n - 1)$.

Låt nu n vara ett udda pseudoprimtal till basen 2, som vi ska använda för att konstruera ett större udda pseudoprimtal. Enligt definitionen av pseudoprimtal är n sammansatt och uppfyller att $2^{n-1} \equiv 1\ (mod\ n)$. I och med att n är sammansatt kan vi skriva $n = dt$ där $1 < d < n$ och $1 < t < n$. Nu ska vi se att utifrån dessa förutsättningar så gäller det även att $m = 2^n - 1$ också är ett pseudoprimtal, genom att visa att m är sammansatt men också att det uppfyller $2^{m-1} \equiv 1\ (mod\ m)$.

För det första så måste m vara sammansatt då det redan har visats att $2^d - 1 \mid 2^n - 1$ och därmed måste det finnas ett tal u sådant att $u(2^d - 1) = 2^n - 1 = m$.

För att förstå att $2^{m-1} \equiv 1\ (mod\ m)$ kan vi börja med att notera att $2^n \equiv 2\ (mod\ n)$ enligt definitionen av ett pseudoprimtal till basen 2. Det kan vi skriva om till $2^n - 2 \equiv 0\ (mod\ n)$ och det måste då finnas ett k som ger $2^n - 2 \equiv kn\ (mod\ n)$, vilket är ekvivalent med att

$2^n - 2 = kn$. Vidare kan vi konstatera att $m = 2^n - 1$, vilket innebär att $m - 1 = 2^n - 2$.

Med hjälp av det kan vi skriva om $2^{m-1} = 2^{2^n-2} = 2^{kn}$, vilket gör att vi kan konstatera att $2^n - 1 \mid 2^{kn} - 1$. Då $2^n - 1 = m$ så följer det att $m \mid 2^{m-1} - 1$, vilket är ekvivalent med $2^{m-1} - 1 \equiv 0\ (mod\ m)$, och kan således skrivas om till $2^{m-1} \equiv 1\ (mod\ m)$

Därmed har vi visat att m också är ett pseudoprimtal som är konstruerat ur n. På samma sätt kan vi konstruera ett nytt pseudoprimtal p utifrån m. Det som saknas är ett första pseudoprimtal att konstruera ifrån men det kan vi finna i början av detta avsnitt, nämligen 341.

Robert Daniel Carmichael

Robert föddes 1879 i Goodwater, Alabama, och vigde hela sitt liv åt matematiken. Vid 30-års ålder hade han hunnit med 170 publikationer i *American Mathematical Monthly*, idag en av världens största tidskrifter inom matematik, en tidskrift han kom att vara redaktör för 1918. Utöver det hade han även publicerat 13 artiklar i *Annals of Mathematics* och *Bulletin of the American Mathematical Society*, två andra tidskrifter inom matematik som funnits sedan slutet av 1800-talet. 1910 blev han tilldelad Porter Ogden Jacubus-stipendiet, Princeston Universitys finaste akademiska utmärkelse och året därpå fick han en Ph.D. för sin avhandling *Linear Difference Equations and their Analytic Solutions*. Han kom att arbeta som assisterande professor inom matematik på Indiana University, för att byta till University of Illinois 1915 där han 1920 befordrades till professor och arbetade till han gick i pension 1947.[15]

Carmichael-tal

I början av 1900-talet studerade Carmichael en undergrupp till Fermats pseudoprimtal som kallas för Carmichael-tal, eller absoluta pseudoprimtal. De definieras enligt följande;

$$Definition\ 3.\ Om\ det\ för\ ett\ positivt\ sammansatt\ tal\ n\ gäller\ att$$
$$b^{n-1} \equiv 1\ (mod\ n), för\ alla\ positiva\ heltal\ b\ som\ uppfyller$$
$$SGD(b,n) = 1, kallas\ n\ för\ ett\ Carmichael - tal.\ [16]$$

[15] O'Connor & Robertson 2010.
[16] Rosen 2010, s. 227.

Se exempelvis det första av dessa tal som Carmichael hittade redan 1910, $561 = 3 \cdot 11 \cdot 17$.[17] I och med att $\text{SGD}(b, 561) = 1$ är en förutsättning så följer det att

$$\text{SGD}(b, 3) = \text{SGD}(b, 11) = \text{SGD}(b, 17) = 1.$$

Vidare kan vi notera att Fermats lilla sats ger oss

$$b^2 \equiv 1 \ (mod\ 3), b^{10} \equiv 1 \ (mod\ 11), b^{16} \equiv 1 \ (mod\ 17)$$

Vi kan samtidigt observera att b^{560} kan skrivas om på följande sätt;

$$b^{560} = (b^2)^{280} = (b^{10})^{56} = (b^{16})^{35}$$

Slår vi ihop dessa observationer får vi att

$$b^{560} \equiv 1 \ (mod\ 561)$$

för alla b som uppfyller $\text{SGD}(b, n) = 1$.

Robert antog att det finns oändligt många av dessa typer av pseudoprimtal, något som skulle ta 80 år innan Alford, Granville och Pomerance bevisade. Det beviset är aningen för långt och komplext för detta arbete[18], så istället kommer det nu presenteras en sats som kan användas för att hitta Carmichael-tal.

> *Sats* 5. *Om* $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ *där* q_j *är olika primtal som uppfyller att* $(q_j - 1) \mid (n - 1)$ *för alla* j *och* $k > 2$, *då är* n *ett Carmichael − tal.*

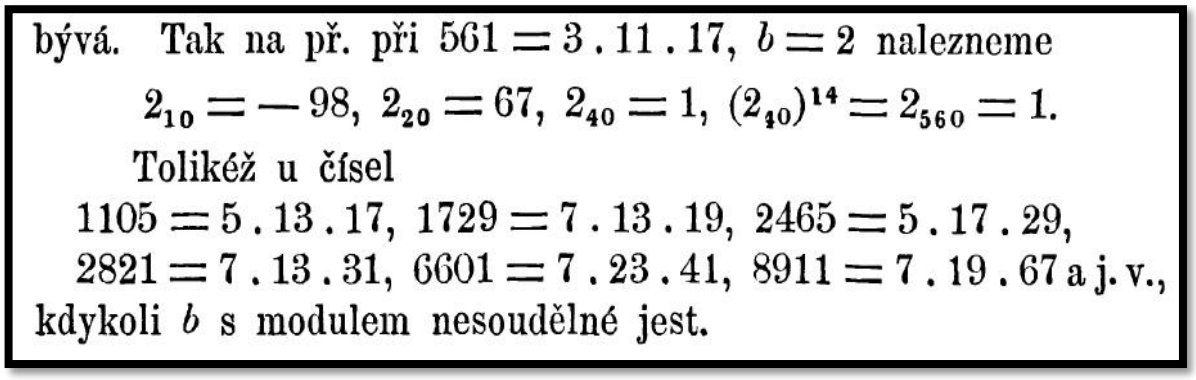
Se exempelvis talet $6601 = 7 \cdot 23 \cdot 41$. Vi kan notera att $(7 - 1) = 6 \mid 6600 = (6601 - 1)$, och på samma sätt kan vi se att $(23 - 1) \mid 6600$ och $(41 - 1) \mid 6600$. Således är 6601 ett Carmichael-tal enligt satsen ovan.

För att bevisa satsen så börjar vi med att låta b vara ett positivt heltal som uppfyller att $SGD(b, n) = 1$. I och med att $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ så betyder det att $SGD(b, q_k) = 1$ för $k = 1, 2, \ldots, k$. Enligt Fermats lilla sats så gäller då att $b^{q_k - 1} \equiv 1 \ (mod\ q_k)$. Eftersom $(q_k - 1) \mid (n - 1)$ så måste det för varje k finnas ett tal t_k sådant att $t_k(q_k - 1) = (n - 1)$. Således vet vi att för varje k så gäller det att $b^{n-1} = b^{t_k(q_k - 1)}$, samtidigt som vi enligt Fermats lilla sats att $b^{q_k - 1} \equiv 1 \ (mod\ q_k)$, vilket ger oss att $b^{n-1} \equiv 1 \ (mod\ q_k)$ och n måste således vara ett Carmichael-tal.

[17] O'Connor & Robertson 2010.
[18] Introduktionen till beviset finns som appendix i slutet för den intresserade.

Trots namnet var Carmichael inte först med att upptäcka denna undergrupp av Fermats pseudoprimtal. Redan på slutet av 1800-talet publicerade den tjeckiska matematikerna Václav Šimerka en artikel i en tjeckisk tidskrift där han presenterade de första sju Carmichael-talen.[19]

Utöver det så formulerade den tyska matematikern Alwin Reinhold Korselt det berömda Korselt's kriterium, en ekvivalent variant av sats 5. Korselt lyckades dock inte hitta några egna tal som uppfyller hans kriterium.[20]



bývá. Tak na př. při $561 = 3 . 11 . 17$, $b = 2$ nalezneme

$$2_{10} = -98,\ 2_{20} = 67,\ 2_{40} = 1,\ (2_{40})^{14} = 2_{560} = 1.$$

Tolikéž u čísel

$1105 = 5 . 13 . 17$, $1729 = 7 . 13 . 19$, $2465 = 5 . 17 . 29$,
$2821 = 7 . 13 . 31$, $6601 = 7 . 23 . 41$, $8911 = 7 . 19 . 67$ a j. v.,

kdykoli b s modulem nesoudělné jest.

Utdrag ur Šimerkas artikeln från 1885 där han listar de 7 första Carmichael-talen.

Man kan fråga sig varför denna undergrupp av Fermats pseudoprimtal inte kallas för Šimerka-tal, alternativt Korselt-tal. En förklaring skulle kunna vara att den tjeckiska tidskriften Šimerka publicerade sin upptäckt i inte var så utbredd, medan Korselt, som nämnt, aldrig hittade konkreta exempel. Carmichael var således först med att både hitta exempel men också att definiera talmängden. En andra förklaring skulle kunna vara så enkel att Carmichael publicerade sina upptäcker i större och mer utbredda tidskrifter, så när det väl blev mer välkänt att både Šimerka och Korselt hade varit före Carmichael så var denna talmängd så starkt förknippat med honom att man inte bytte namn på den.

RSA-algoritmen

Kommunikation har varit en central del av mänsklighetens existens och överlevnad. Med tiden har det även blivit viktigt att kunna kommunicera med människor utan att någon annan kan förstå det, inte minst genom meddelanden, vilket är varför kryptering har växt fram. Kryptering kan dock ske på en mängd sätt, exempelvis använde Julius Caesar ett tämligen enkelt system där han bytte ut varje bokstav i meddelandet mot bokstaven tre steg fram i alfabetet.[21]

Vanlig text	a	b	c	d	e	f	g	h	i	j	k	l	m

[19] Šimerka 1885, s. 224.
[20] Conrad, s. 2.
[21] Mollin 2003, s. 1.

Krypterad text	D	E	F	G	H	I	J	K	L	M	N	O	P

Vanlig text	n	o	p	q	r	s	t	u	v	w	x	y	z
Krypterad text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabell över Julius Caesars kryptering.

Men av samma anledning som att man vill dölja meddelandet för fel mottagare, så vill de personerna försöka tyda meddelandet trots krypteringen, med andra ord vill de dekryptera meddelandet. Därför är kryptering alltid en tävling mellan de som försöker dölja meddelandet och de obehöriga som vill tolka meddelandet. Används ett krypteringssystem av Caesars karaktär allt för länge är det inte osannolikt att någon kan komma på nyckeln och därmed dekryptera meddelandet. Betrakta istället följande exempel av ett krypteringssystem;

Vanlig text	a	b	c	d	e	f	g	h	i	j	k	l	m
Krypterad text	1	2	3	4	5	6	7	8	9	10	11	12	13

Vanlig text	n	o	p	q	r	s	t	u	v	w	x	y	z
Krypterad text	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabell över ett enkelt sätt att omvandla bokstäver till tal.

Vi har nu ett meddelande skrivet med tal istället. Det öppnar upp möjligheten att kryptera meddelandet ytterligare genom att utföra olika matematiska operationer för att på så sätt öka svårighetsgraden att dekryptera meddelandet. Vi kan börja med att notera att Caesars kryptering kan uttryckas med hjälp av matematik på följande sätt; $\beta = \alpha + 3\ (mod\ 26)$ där β är den dekrypterade siffran och α är ursprungsbokstaven översatt till motsvarande siffra.

Men med hjälp av matematiken kan vi göra mer avancerade system, framför allt för de som inte kan systemet. Vi skulle exempelvis kunna tänka oss att vi använder oss av följande funktion;

$$\beta(\alpha) = \begin{cases} 2\alpha + 1, & \alpha \equiv 0\ (mod\ 2) \\ 3\alpha + 2, & \alpha \equiv 1\ (mod\ 2) \end{cases}$$

Vi får således ett villkor på krypteringen utifrån om talet är udda eller jämnt som i sin tur påverkar hur vi krypterar siffran. Men på grund av datorernas intåg under 1900-talet har det blivit svårare att kryptera då datorerna blir bättre och bättre på att dekryptera allt för enkla system. Det blir extra tydligt att det är en kapplöpning mellan de som krypterar och de, oftast obehöriga, som vill dekryptera. Därför har det utvecklats metoder som inte bara ska göra det svårt för en människa att dekryptera meddelanden, utan även datorerna.

På 1980-talet kom Ronald Rivest, Adi Shamir och Leonard Adleman på ett av de mest använda krypteringssystemen idag, RSA-algoritmen.[22] Men innan vi kan förstå den behöver vi lära oss följande sats;

$$Sats\ 6. Konstruera\ ett\ tal\ m, sådant\ att\ m = p_1 \cdot p_2 \cdot \ldots \cdot p_i, där\ p_1, p_2 \ldots p_i\ är\ olika\ primtal, samt\ m > 0. Välj\ sedan\ ut\ ett\ positivt\ talpar\ d\ och\ e\ som\ uppfyller\ att\ d \cdot e \equiv 1\ (mod\ \varphi(m)). Då\ gäller\ \text{det}\ för\ varje\ heltal\ a\ att\ a^{de} \equiv a\ (mod\ m).$$

Tack vare lemma 1 räcker det med att vi visar att kongruensen $a^{de} \equiv a\ (mod\ p)$ gäller för alla primtal $p = p_1, p_2 \ldots, p_i$ som delar m. Det är ganska lätt att se att detta gäller för $a = 0$ eftersom $0^{de} \equiv 0\ (mod\ p)$ oavsett vad d och e är, således kan vi utgå ifrån att $a \neq 0$.

Utifrån förutsättningarna i satsen är $d \cdot e = 1 + n \cdot \varphi(m)$ för något heltal $n \geq 1$. Samtidigt gäller det att $\varphi(m) = \varphi\left(p \cdot \frac{m}{p}\right)$ eftersom m består utav primtal $p = p_1, p_2, \ldots, p_i$, vilket vi kan skriva om enligt följande $\varphi\left(p \cdot \frac{m}{p}\right) = \varphi(p) \cdot \varphi\left(\frac{m}{p}\right)$ tack vare att Eulers φ-funktion är multiplikativ.

När vi nu har $\varphi(p) \cdot \varphi\left(\frac{m}{p}\right)$ så kan vi påminna oss om att $\varphi(p) = p - 1$ när p är ett primtal, vilket det är enligt förutsättningarna, och vi kan skriva om vårt uttryck till $(p-1)\varphi\left(\frac{m}{p}\right)$. Med andra ord är alltså $d \cdot e = 1 + n(p-1)\varphi\left(\frac{m}{p}\right)$. Eftersom både n och $\varphi\left(\frac{m}{p}\right)$ är heltal ≥ 0 så kan vi multiplicera ihop dem till ett positivt heltal N och vårt uttryck blir således $d \cdot e = 1 + (p-1)N$. Nu kan vi med hjälp av Fermats lilla sats avrunda beviset;

$$a^{de} = a^{1+(p-1)N} = a \cdot a^{(p-1)N} = a \cdot (a^{p-1})^N \equiv a \cdot 1^N = a\ (mod\ p)$$

När man använder RSA-kryptering så behövs det två nycklar; en publik krypteringsnyckel och en hemlig dekrypteringsnyckel. Krypteringsnyckeln består utav ett talpar (m, e), där m är en modul och e en exponent. m konstrueras genom att ta produkten av två olika primtal, p och q, medan e konstrueras utifrån att det måste vara relativt prima mot $\varphi(m)$ vilket som tidigare visat är ekvivalent med att det måste vara relativt prima mot $\varphi(p) \cdot \varphi(q) = (p-1)(q-1)$.

Dekrypteringsnyckeln består utav ett talpar (m, d), där d ska uppfylla att $d < \varphi(m)$ och

[22] Rosen 2010, s. 323.

$ed \equiv 1\ (mod\ \varphi(m))$. Notera att dessa två villkor gör att det finns endast finns ett tal som d kan anta.

För att kryptera ett meddelande så börjar man med att konvertera det till ett heltal a i intervallet $[0, m-1]$. Sedan krypteras heltalet genom att omvandla a till b, där b är det tal som uppfyller att $0 < b < m-1$ och $b \equiv a^e\ (mod\ m)$. Talet b skickas sedan till den avsedda mottagaren för dekryptering.

När mottagaren har fått talet b så använder hen talet d för att hitta det tal c som uppfyller att $0 \leq c < m$ och $c \equiv b^d\ (mod\ m)$. Tack vare sats 6 så vet vi att $c = a$ och således kan mottagaren omvänt omvandla talet till bokstäver och tecken för att läsa meddelandet.

Vi illustrera hur detta kan gå till i praktiken med ett exempel. Säg att vi väljer $p = 5$ och $q = 11$, då blir $m = 55$ samt $\varphi(m) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = 4 \cdot 10 = 40$. Sedan måste vi välja e sådant att $SGD(e, 4) = SGD(e, 10) = 1$, exempelvis $e = 3$. För dekrypteringsnyckeln gäller då för d att $d < 40$ och $ed = 3 * d \equiv 1\ (mod\ 40)$, det vill säga $d = 27$ då $27 \cdot 3 = 81 = 2 \cdot 40 + 1 \equiv 1\ (mod\ 40)$. Således blir krypteringsnyckeln $(m, e) = (55, 3)$ och dekrypteringsnyckeln $(m, d) = (55, 27)$.

Om vi nu vill skicka meddelandet ”FERMAT” så måste vi först omvandla det till ett tal a som uppfyller $0 < a < 54$. Den observante kommer nu notera att det kan bli svårt, och vi får dela upp ”FERMAT” i block och omvandla till $a_1, a_2, \dots, a_i$. Vi gör det enkelt för oss och översätter varje bokstav till motsvarande siffra där $A = 1, B = 2, \dots$ Ö $= 29$. Då blir vårt omvandlade meddelande följande sex block;

$$a_1 = F = 6$$
$$a_2 = E = 5$$
$$a_3 = R = 18$$
$$a_4 = M = 13$$
$$a_5 = A = 1$$
$$a_6 = T = 20$$

Vi får nu översätta dessa block till $b_1, b_2, \dots, b_6$ där $0 < b_i < 54$ och $b_i \equiv a_i^e\ (mod\ 55)$. Till exempel får vi $b_1 = 6^3 = 216 = 3 \cdot 55 + 51 \equiv 51\ (mod\ 55)$. På samma sätt får vi att $b_2 = 15, b_3 = 2, b_4 = 52, b_5 = 1, b_6 = 25$.

Vi skickar iväg strängen $51\ 15\ 02\ 52\ 01\ 25$ till vår mottagare, som sitter på dekrypteringsnyckeln $(40, 27)$, som i sin tur tar varje block och löser kongruensen $c \equiv b_i^{27}\ (mod\ 55)$. Med hjälp av digitala verktyg kan vi få fram att $c_1 = 51^{27} \equiv 6 = a_1 (mod\ 55)$. På samma sätt får vi att $c_2 = a_2 = 5$, och så vidare. Avslutningsvis får mottagaren omvandla tillbaka siffrorna till bokstäver och vårt meddelande ”FERMAT” har kommit fram.

Ovanstående dekrypteringsnyckel hade antagligen varit ganska lätt att ta reda på eftersom de valda primtalen var så små. I verkligheten bör primtalen vara större än 2^{512} för att vara relativt säkra. Det har sin förklaring i processen av vad man måste göra för att kunna dekryptera meddelandet. Ponera att någon obehörig får tag på talet b. Då behöver denne lösa kongruensen $a^e \equiv b\ (mod\ m)$, med andra ord måste man beräkna $\sqrt[e]{b}$. Det finns dock inget känt sätt att göra det utan att känna till d. Men för att beräkna d behöver man veta $\varphi(m)$ vilket kräver att man kan faktorisera m. Givet att m består av två olika primtal som är större än 2^{512} betyder det att m är större än 2^{1024}, ett tal så stort att det inte finns några algoritmer eller datorer idag som kan faktorisera det.[23]

Sammanfattning

Fermat är känd för två satser; den lilla och den stora. I detta arbete har vi bekantat oss mer med den lilla satsen, både hur den härleds, men också hur den har tillämpats och utvecklats genom åren. Den har användning i dagens samhälle genom att möjliggöra en av den vanligaste krypteringssätten, RSA-kryptering. Den här även gett upphov till en egen grupp pseudoprimtal, som i sin tur har bearbetats till den grad att det finns undergrupper, bland annat Carmichael-talen.

Däremot är det fortfarande ett mysterium huruvida Fermat själv lyckades bevisa satsen, och i sådana fall hur han bevisade den, eller om han hade ren tur när han formulerade den. Oavsett verkar han ha ansett själv att det var en viktig upptäckt och det vore intressant om någon annan kunde granska huruvida han faktiskt använde satsen i sitt framtida arbete inom geometriska talföljder, och i sådana fall i vilken utsträckning.

[23] Lindahl 2012, s. 38.

Käll- och litteraturförteckning

Tryckta källor

Fermat, Pierre de, 1894, *Ouvres de Fermat. T. 2, Correspondence*, Paris.

Litteratur

Burn, Bob, 2002, "Fermat's little theorem, proofs that Fermat might have used", i *The Mathematical Gazette,* Volume 86, Issue 507, Cambridge.

Conrad, Keith, "Carmichael Numbers and Korselt's Criterion". https://kconrad.math.uconn.edu/blurbs/ (Hämtad 2019-05-17)

Euler, Leonhard, 1741, *Theorematum quorundam ad numeros primos spectantium demonstratio.* https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1053&context=euler-works (Hämtad 2019-06-06)

Lehto, Olli, 1980, *Proceedings of the International congress of mathematicians, Helsinki 1978, volume 1*, Helsinki.

Lindahl, Lars Åke, 2012, *Elementär talteori*, Uppsala.

Mahoney, Michael Sean, 1994, *The Mathematical Career of Pierre de Fermat, 1601-1665*, Princeton.

Mollin, Richard A., 2003, *RSA and public-key cryptography,* Florida.

Nagell, Trygve, 1950, *Elementär talteori*, Stockholm.

O'Connor, J J, Robertson, E. F., 2010, *Robert Daniel Carmichael*, St Andrew. http://www-history.mcs.st-and.ac.uk/Biographies/Carmichael.html (Hämtad 2019-04-28)

Rosen, Kenneth H., 2010, *Elementary number theory and its applications*, Boston.

Šimerka, Václav, 1885, "Zbytky z arithmetické posloupnosti", i *Časopis pro pěstování mathematiky a fysiky*, Volume 14, Issue 5. https://dml.cz/handle/10338.dmlcz/122245 (Hämtad 2019-06-07)

Stewart, Ian, Tall, David Orme, 2002, *Algebraic number theory and Fermat's last theorem*, Natick.

Weil, André, 1983, *Number Theory: an approach through history from Hammurapi to Legendre*, Boston.

Appendix

Appendix 1, Introduktionssida till beviset för oändligt antal Carmichael-tal.

Annals of Mathematics, **140** (1994), 703–722

There are infinitely many Carmichael numbers

By W.R. Alford, Andrew Granville and Carl Pomerance*

Dedicated to Paul Erdős on the occasion of his 80^{th} birthday

Introduction

On October 18th, 1640, Fermat wrote in a letter to Frenicle, that whenever p is prime, p divides $a^{p-1}-1$ for all integers a not divisible by p, a result now known as Fermat's 'little theorem.' An equivalent formulation is the assertion that p divides a^p-a for all integers a, whenever p is prime. The question naturally arose as to whether the primes are the only integers exceeding 1 that satisfy this criterion, but Carmichael [Ca1] pointed out in 1910 that 561 $(=3\times 11\times 17)$ divides $a^{561}-a$ for all integers a. In 1899, Korselt [Ko] had noted that one could easily test for such integers by using (what we will call)

Korselt's criterion. n divides a^n-a for all integers a if and only if n is squarefree and $p-1$ divides $n-1$ for all primes p dividing n.

In a series of papers around 1910, Carmichael began an in-depth study of composite numbers with this property, which have become known as *Carmichael numbers.* In [Ca2], Carmichael exhibited an algorithm to construct such numbers and stated, perhaps somewhat wishfully, that "*this list* (of Carmichael numbers) *might be indefinitely extended.*" Indeed, until now, no one has been able to prove that there are infinitely many Carmichael numbers, though it has long seemed highly likely.

---

*The idea for this paper came to us after seeing a preprint of Zhang Mingzhi [Zh] in which a technique proposed by Erdős is modified to give numerical examples of Carmichael numbers with many prime factors. We are indebted to Ed Azoff, Roger Baker, Brian Boe, Enrico Bombieri, Paul Erdős, John Friedlander, Roger Heath-Brown, Sergei Konyagin, Helmut Maier, Greg Martin, Hugh Montgomery, François Morain, Gary Mullen, Jean-Louis Nicolas, Richard Pinch, John Selfridge, Jeff Shallit, Bob Vaughan and Richard Warlimont for their comments and advice concerning this paper. The second and third authors wish to acknowledge support from NSF grant DMS 90-02538. The second author is an Alfred P. Sloan Research Fellow.