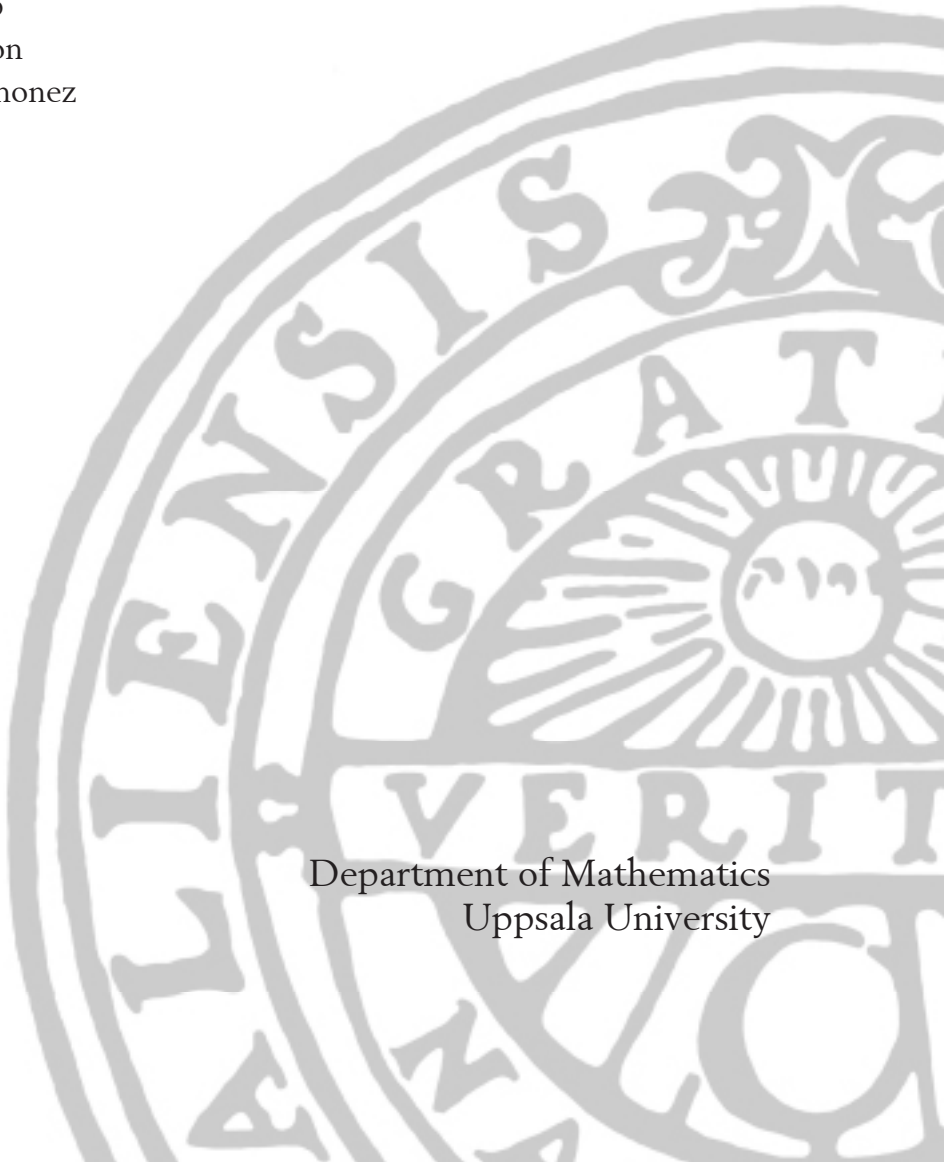
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2022:20

Euklides och primtal

Jakob Adabanian

Examensarbete i matematik, 15 hp
Handledare: Andreas Strömbergsson
Examinator: Veronica Crispin Quinonez
Juni 2022



Department of Mathematics
Uppsala University

Sammanfattning

I denna uppsats presenteras några av Euklides upptäckter inom matematiken med fokus på talteori och i synnerhet primtal. Dessa upptäckter har haft stor betydelse för dagens matematik - men tas ibland för givna och ses som självklara. Vi kommer att se närmare på några av Euklides upptäckter för att diskutera hur de såg ut då och hur de ser ut idag, med fokus på den matematiska teorin.

Innehåll

1 Introduktion

I denna uppsats diskuterar vi vad Euklides gjorde för upptäckter inom aritmetiken och talteorin, främst primtal. Vilken betydelse dessa upptäckter haft för talteorin kommer även att diskuteras.

1.1 Euklides *Elementa*

Euklides var en grekisk matematiker som verkade i Alexandria omkring 300 - 200 år före vår tideräkning. Om Euklides är inte mycket känt, mer än att han ska ha författat *Elementa*. *Elementa* är en av de mest spridda texterna i världen och kom att ha enorm betydelse för matematiken. Skrifterna är uppdelade i tretton olika böcker, I - XIII. Dessa behandlar främst geometri, men böckerna VII - IX handlar om aritmetik. Dessa kommer vi att fokusera på i denna uppsats. [5, s. 161][6, s. 64-65]

1.2 Primtal

Ett primtal är ett heltal a där

$$a \geq 2$$

som enbart är delbart med sina triviala delare, det vill säga 1 och sig självt. Exempelvis är 7 ett primtal eftersom enbart $1 \mid 7$ och $7 \mid 7$.

Med talet 9 är det däremot annorlunda. Detta eftersom 9 inte bara är delbart med sina triviala delare, $1 \mid 9$ och $9 \mid 9$, utan även följande gäller:

$$3 \mid 9.$$

Då 3 inte är en trivial delare till 9 följer alltså att 9 inte är ett primtal. De 20 första primtalen är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.$$

Primtal kan vid första anblick verka vara så oregelbundna att de skulle vara utplacerade slumpmässigt, men så är ej fallet eftersom det är entydigt hur ett primtal är uppbyggt. [6, s. 2] Att det verkar finnas något mönster kring primtalen kan ses om man exempelvis inspekterar *Ulams spiral*. När man organiserar alla heltal i en kvadratisk spiral tycks primtalen hamna i diagonala linjer på ett fascinerande sätt. [6, s. 232]

Primtalen och dess slumpmässighet - fast ändå inte slumpmässighet har länge förbryllat matematiker. Gång på gång har försök gjorts för att förklara alla mysterier kring primtalen, ibland har de lyckats och ibland ej. Än idag finns flera obevisade förmodanden kring primtalen. [6, s. 2]

> ”Prime numbers have always fascinated mathematicians. They appear among the integers seemingly random, and yet not quite: there

> seems to be some order or pattern, just a little below the surface, just a little out of reach."
>
> -*Underwood Dudley*

[1, s. 163]

> "God may not play dice with the universe, but something strange is going on with the prime numbers."
>
> -*Paul Erdös*

[2, s. 759]

2 Aritmetikens fundamentalsats

Aritmetikens fundamentalsats lyder:

Varje positivt heltal kan primtalsfaktoriseras på ett och endast ett sätt, bortsett från ordningen.

Fundamentalsatsen är avgörande för mycket av matematiken, särskilt inom talteorin. Att den kallas *fundamentalsats* beror på dess oerhört viktiga betydelse. Det finns dock vissa matematiska system där aritmetikens fundamentalsats inte gäller, vilket kommer att diskuteras senare i detta avsnitt.

2.1 Bevis

Satsen bevisar Euklides på följande vis:

2.1.1 Del I

Här följer vi [5, s. 234-236], vi har ett tal A. Om A är ett primtal är det redan primtalsfaktoriserat av sig självt och går ej att bryta upp i fler faktorer. Men om A inte är ett primtal (och $A > 1$) är det ett sammansatt tal. Detta tal har då icketriviala delare; låt oss kalla den minsta av dessa för M. Detta tal M måste vara ett primtal, ty annars hade det funnits ett tal N där $1 < N < M$ så att $N \mid M$, och därmed också $N \mid A$, vilket är en motsägelse mot att M är den minsta icketriviala delaren till A.

Om A alltså inte är ett primtal kan det faktoriseras av sin minsta delare, som vi kan kalla d_1, då kan vi faktorisera A

$$A = d_1 \cdot k_1.$$

Nu följer två alternativ. Antingen är k_1 ett primtal eller ej. *Om* det är ett primtal har vi primtalsfaktoriserat A. Annars är k_1 ett sammansatt tal, då kan vi fortsätta faktorisera A genom att faktorisera k_1

$$k_1 = d_2 \cdot k_2.$$

Om k_2 är ett primtal har vi primtalsfaktoriserat A

$$A = d_1 \cdot d_2 \cdot k_2.$$

Om k_2 inte är ett primtal kan man ändå faktorisera A genom att upprepa denna procedur. Det kan man göra genom att fortsätta faktorisera k_n

$$A = k_1 \cdot k_2 \cdots k_n$$

tills alla faktorer är primtal. Alltså kan vi för varje tal A finna en uppdelning av primtal. Det visar sig dock att denna primtalsuppdelning är unik för varje tal A. Beviset för det kommer i del II.

2.1.2 Del II

Denna del av beviset behandlar entydigheten, alltså varför primtalsfaktoriseringen endast kan se ut på ett sätt, bortsett från ordningen.

Till detta bevis behöver vi två lemman:

Lemma 1. *Om p är ett primtal där*

$$p \mid a \cdot b$$

kommer p även att dela åtminstone en av faktorerna a och b.

Observera att Lemma 1 även kallas *Euklides Lemma*.

Lemma 2. *Om p är ett primtal och $p \mid a_1 \cdot a_2 \cdots a_n$, så är minst en av faktorerna a_1, a_2 ... delbar med p.*

Observera att Lemma 2 följer direkt genom upprepad användning av Lemma 1 (först med $a = a_1$ och $b = a_2 \cdots a_n$; om $p \mid a_1$ så är vi klara; i annat fall ger Lemma 1 att $p \mid a_2 \cdot a_3 \cdots a_n$, och vi använder då Lemma 1 med $a = a_2$ och $b = a_3 \cdots a_n$, osv). Beviset av Euklides Lemma kommer i 3.2.6. Vi ger nu beviset av entydigheten i aritmetikens fundamentalsats med hjälp av lemmana.

Vi inleder med att anta att vi skulle kunna dela upp A i två olika primtalsfaktoriseringar

$$A = v_1 \cdot v_2 \cdots v_n = q_1 \cdot q_2 \cdots q_m.$$

Vi kan från början anta att de två primtalsfaktoriseringarna är ordnade så att $v_1 \leq v_2 \leq \cdots \leq v_n$ och $q_1 \leq q_2 \leq \cdots \leq q_m$. Här vill vi visa att primtalen $v_1, v_2, \ldots, v_n$ är precis desamma som primtalen $q_1, q_2, \ldots, q_m$, förutom att de kan vara ordnade på olika sätt.

Enligt lemma 2 följer att en av faktorerna q_1, q_2 ... är delbar med v_1. Eftersom dessa är primtal måste v_1 även vara lika med faktorn q_x som är delbar med v_1. Alltså finns v_1 som en faktor bland q_x, därför måste v_1 vara större eller lika med q_1, som i sin tur är minst bland faktorerna q_x. På samma vis som vi gjort med v_1 i förhållande till q_x kan vi göra med q_1 i förhållande till v_y. Detta ger $v_1 = q_1$. Nu skriver vi istället om A som

$$v_2 \cdot v_3 \cdots v_n = q_2 \cdot q_3 \cdots q_m.$$

På samma vis kommer vi att kunna visa likheterna $v_2 = q_2$, $v_3 = q_3$ och så vidare. Varje q_x paras ihop med ett korresponderande v_y. Av det får vi att $v_n = q_m$ och även att $n = m$. Därmed är aritmetikens fundamentalsats bevisad.

2.2 Exempel

Det som följer av aritmetikens fundamentalsats, att varje tal kan primtalsfaktoriseras på ett och endast ett sätt kan låta väldigt uppenbart vid en första anblick, men det visar sig inte vara så självklart. Om vi tar talet 60 som exempel så gäller:

$$60 = 2 \cdot 30$$

samtidigt som

$$60 = 6 \cdot 10$$

vilket inte alls verkar vara unika faktoriseringar. Dock kan talen 30 och 10 faktoriseras ytterligare eftersom de är sammansatta tal och ej primtal

$$2 \cdot 30 = 2 \cdot 2 \cdot 3 \cdot 5$$

och

$$6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5$$

dessa faktoriseringar är som tidigare nämnt inte olika, eftersom faktorerna är samma. De kommer bara i olika ordning, vilket aritmetikens fundamentalsats tillåter.

2.3 Gaussiska heltal

Gaussiska heltal är alla tal på formen $a+bi$ där $a, b \in \mathbb{Z}$ samt $i^2 = -1$. Då dessa tal har både en reell och en imaginär del kan de betraktas i det 2-dimensionella *komplexa talplanet*. Den Euklidiska divisionsalgoritmen kan inte bara användas på heltal utan även på gaussiska heltal. Detta gör att de gaussiska heltalen utgör en *Euklidisk ring*. Detta kan användas för att bevisa entydigheten i primtalsfaktoriseringar, eftersom det bland de gaussiska heltalen finns primtal.

Det finns 4 enheter i denna ring, dessa är $i, -i, 1$ och -1. Ett exempel på hur Euklides algoritm kan användas på gaussiska heltal kommer i avsnitt 3.2.3.

Gaussiska heltal är ett tydligt exempel på Euklides påverkan på senare matematik, eftersom denna typ av komplexa ”heltal” kopplats samman med exempelvis primtal och Euklides algoritm.

2.4 När aritmetikens fundamentalsats inte gäller

2.4.1 Exempel I

Här följer vi [3, s. 21-23], det finns alltså exempel på när aritmetikens fundamentalsats inte gäller, exempelvis när man betraktar vissa multiplikativa system. Vi låter det multiplikativa systemet A innehålla alla jämna, positiva heltal, alltså $A = 2, 4, 6, 8...$ Produkten av två tal i A kommer fortfarande alltid att vara ett tal i A. Om de enda talen man känner till är talen som finns i A kommer vi att få nya primtal. Exempelvis är 4 ett sammansatt tal, $4 = 2 \cdot 2$. Men 6 blir nu ett

primtal eftersom vi inte kan faktorisera 6 med något tal i A. Om vi som i det tidigare exemplet betraktar talet 60 så har vi $60 = 2 \cdot 30 = 6 \cdot 10$. Men eftersom alla dessa faktorer är primtal i A har vi funnit två olika primtalsfaktoriseringar, vilket går emot aritmetikens fundamentalsats.

2.4.2 Exempel II

Ett annat exempel på när aritmetikens fundamentalsats inte gäller är exempelvis $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Exemplet kan vid en första anblick verka *påhittat*, eftersom $\sqrt{-5}$ är ett komplext tal, men exemplet är taget ur den algebraiska talteorin som är ett viktigt område inom matematiken. Här betraktar vi en klass B innehållandes alla tal på formen $a + b\sqrt{-5}$ där $a, b \in \mathbb{Z}$. Summan och produkten av två tal i B kommer alltid att vara ett tal i B, alltså är B slutet under addition och multiplikation.

2.5 $\sqrt{2}$ är irrationellt

Euklides använde aritmetikens fundamentalsats för att visa att $\sqrt{2}$ är ett irrationellt tal. Han resonerade på följande vis: oavsett hur många primtalsfaktorer ett positivt heltal n har kommer n^2 att ha ett jämnt antal primtalsfaktorer. Det medför att kvoten av två jämna kvadrater också har ett jämnt antal primtalsfaktorer. Aritmetikens fundamentalsats omöjliggör att detta kan ändras till ett udda antal primtalsfaktorer så inget tal med ett udda antal primtalsfaktorer kan vara kvadratroten ur ett rationellt tal. Alltså är $\sqrt{2}$ irrationellt. Samma metod kan naturligtvis användas för att visa att fler kvadraträtter är irrationella, vilket fler grekiska matematiker gjorde efter Euklides. Av någon anledning slutade man dock efter $\sqrt{17}$. Man kan även visa att $\sqrt[n]{p}$ är irrationellt även för $n > 2$ för vissa heltal p med denna metod. [6, s. 65]

3 Relativt prima tal

3.1 Relativt prima

Att två tal är relativt prima innebär att 1 är den största gemensamma delaren, *SGD*, till båda talen. Två tal som inte är primtal kan alltså vara relativt prima, så länge de inte har en större *gemensam* delare än 1. De är alltså prima i förhållande till varandra. Euklides upptäckte en metod för att ta reda på om två tal är relativt prima genom *Euklides algoritm*. [6, s. 68] Exempelvis är talen 10 och 21 relativt prima, eftersom det största talet som delar de båda är 1. Däremot är 10 och 15 inte relativt prima, detta eftersom 5 är deras största gemensamma delare.

3.2 Euklides algoritm

3.2.1 Algoritmen

Med *Euklides algoritm* kan man beräkna SGD för två tal. Algoritmen går ut på att man subtraherar det mindre talet från det större, tills vi får en rest. Sedan subtraheras resten upprepade gånger från det mindre av de två ursprungliga talen. Då finner vi till slut en ny, mindre rest. Den sista nollskilda resten är alltid SGD. I de fall SGD = 1 är talen relativt prima. Givet två heltal a och $b > 0$ ser algoritmen ut som följer

$$a - bk_1 = r_1$$

k står här för kvoten mellan a och b, r står för resten. Vi fortsäter algoritmen

$$b - r_1k_2 = r_2$$

$$r_1 - r_2k_3 = r_3$$

$$...$$

$$r_{x-2} - r_{x-1}k_x = r_x$$

$$r_{x-1} - r_xk_{x-1} = 0.$$

Som sagt är SGD lika med den sista nollskilda rest vi får när vi upprepar denna procedur (alltså lika med r_x i ovanstående uppställning, om vi antar $r_x \neq 0$).

3.2.2 Exempel

Om vi vill hitta den största gemensamma delaren till 1180 och 482 använder vi Euklides algoritm

$$1180 - 2 \cdot 482 = 216$$

Resten är alltså 216, vilket vi subtraherar från 482

$$482 - 2 \cdot 216 = 50$$

Vi fortsätter på samma vis

$$216 - 4 \cdot 50 = 16$$

$$50 - 3 \cdot 16 = 2$$

$$16 - 8 \cdot 2 = 0$$

Det visar sig att den sista nollskilda resten är 2. Alltså är 2 den största gemensamma delaren till 1180 och 482. Det kan även skrivas $\text{SGD}(1180, 482) = 2$. Av detta kan vi dra slutsatsen att talen inte är relativt prima.

3.2.3 Exempel på Euklides algoritm för gaussiska heltal

Som tidigare nämnt kan Euklides algoritm användas för gaussiska heltal. Vi tittar på ett exempel. Låt oss anta att $z = 5 - 14i$ och $w = 1 + 2i$. Vi vill nu hitta $\text{SGD}(z, w)$. Först vill vi hitta ett tal q så att $z - qw = r$. Detta kan vi finna genom att beräkna $\frac{z}{w}$

$$\frac{z}{w} = \frac{5 - 14i}{1 + 2i}.$$

Vi multiplicerar täljaren och nämnaren med nämnarens konjugat

$$\frac{5 - 14i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{-23 - 24i}{5} = -\frac{23}{5} - \frac{24i}{5}.$$

Av detta ser vi alltså att $w \nmid z$ eftersom koefficienterna inte är heltal, alltså är talet inte ett gaussiskt heltal. Vi kan då *uppskatta* ett q. 5 går nästan 5 gånger i både -23 och -24, så vi uppskattar q till $-5 - 5i$. Alltså, $z - qw = r$

$$5 - 14i - (-5 - 5i)(1 + 2i) = r$$

$$5 - 14i - 5 + 15i = r$$

$$r = i.$$

Här går Euklides algoritm ut på att man upprepar algoritmen tills man får en rest som är en enhet, vilket i är. Alltså är $\text{SGD}(5 - 14i, 1 + 2i) = i$.

3.2.4 Euklides algoritm *baklänges*

Euklides algoritm kan användas för att hitta lösningar till ekvationer på formen $as + bt = \text{SGD}(a, b)$ där s och t är heltal. Vi tar ett exempel, vi vill hitta heltal s och t som satisfierar ekvationen $1789s + 1456t = \text{SGD}(1789, 1456)$.

Det första vi gör är att hitta SGD(1456,1789). Det gör vi genom Euklides algoritm:

$$1789 - 1 \cdot 1456 = 333$$

$$1456 - 4 \cdot 333 = 124$$

$$333 - 2 \cdot 124 = 85$$

$$124 - 1 \cdot 85 = 39$$

$$85 - 2 \cdot 39 = 7$$

$$39 - 5 \cdot 7 = 4$$

$$7 - 1 \cdot 4 = 3$$

$$4 - 1 \cdot 3 = 1$$

$$3 - 3 \cdot 1 = 0$$

Eftersom den sista icke försvinnande resten är 1 betyder det att SGD(1789,1456) = 1. Alltså kommer vi att kunna finna heltalslösningar till ekvationen $1789s + 1456t = 1$. Detta uppnås genom att gå *baklänges*. Vi börjar då med att uttrycka 1 på samma vis som vi tidigare fick ut 1 som rest:

$$1 = 4 - 1 \cdot 3$$

Vi fortsätter genom att substituera 3 mot

$$3 = 7 - 1 \cdot 4$$

och sätter in det i ekvationen

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7$$

vi fortsätter sedan på samma vis substituera den mindre resten mot det vi fick ut under Euklides algoritm:

$$2 \cdot 4 - 7 = 2 \cdot (39 - 5 \cdot 7) - 7 = 2 \cdot 39 - 10 \cdot 7 - 7 = 2 \cdot 39 - 11 \cdot 7 =$$

$$2 \cdot 39 - 11 \cdot (85 - 2 \cdot 39) = 2 \cdot 39 - 11 \cdot 85 + 22 \cdot 39 = 24 \cdot 39 - 11 \cdot 85 =$$

$$24 \cdot (124 - 85) - 11 \cdot 85 = 24 \cdot 124 - 24 \cdot 85 - 11 \cdot 85 = 24 \cdot 124 - 35 \cdot 85 =$$

$$24 \cdot 124 - 35 \cdot (333 - 2 \cdot 124) = 24 \cdot 124 - 35 \cdot 333 + 70 \cdot 124 = 94 \cdot 124 - 35 \cdot 333 =$$

$$94 \cdot (1456 - 4 \cdot 333) - 35 \cdot 333 = 94 \cdot 1456 - 376 \cdot 333 - 35 \cdot 333 = 94 \cdot 1456 - 411 \cdot 333 =$$

$$94 \cdot 1456 - 411 \cdot (1789 - 1456) = 94 \cdot 1456 - 411 \cdot 1789 + 411 \cdot 1456 = 505 \cdot 1456 - 411 \cdot 1789.$$

Vi har nu slutligen hittat en lösning till $1789s + 1456t = \text{SGD}(1789, 1456)$. Euklides algoritm baklänges gav oss att $s = -411$ samt att $t = 505$ eftersom $505 \cdot 1456 - 411 \cdot 1789 = 1$.

Euklides Lemma (*Lemma 1* i 2.1.2) går att bevisa med hjälp av Euklides algoritm baklänges. Till detta inför vi först ett nytt Lemma.

Lemma 3. *Om $b \mid ac$ och SGD(b,c) = 1 gäller det att $b \mid a$.* Bevis för Lemma 3:

3.2.5 Bevis för Lemma 3

Eftersom SGD$(b, c) = 1$ innebär det att b och c är relativt prima. Då kan vi, genom att arbeta beklänges i Euklides algoritm, finna två heltal s och t så att $sb + tc = 1$. Eftersom $b \mid ac$ kan vi hitta ett tal m så att $bm = ac$. Eftersom det går att finna $sb + tc = 1$ går det att skriva om a som $a = a(sb + tc)$. Om vi multiplicerar in a i parentesen erhåller vi

$$a = asb + atc = asb + t(ac) = asb + tbm = b(as + tm)$$

vi har alltså

$$a = b(as + tm)$$

men eftersom $as + tm$ är ett heltal gäller det att $b \mid a$.

Nu när vi bevisat Lemma 3 kan vi slutligen gå vidare till att bevisa Euklides Lemma.

3.2.6 Bevis för Euklides Lemma

Antag att vi har tre tal p, a, $b \in \mathbb{Z}$ där p är ett primtal så att $p \mid ab$ gäller. Vi låter $d =$ SGD(p, a). Vi vet att p är ett primtal och att $d \mid p$. Alltså måste antingen $d = p$ eller $d = 1$ gälla. I fallet där $d = p$ kommer d att dela både p och a, eftersom SGD(p, a) delar båda. I fallet där $d = 1$ blir p och a relativt prima. Alltså, enligt lemmat ovan, eftersom $p \mid ab$ så gäller det att $p \mid b$. Oavsett delar p alltså åtminstone en av faktorerna och beviset är komplett.

4 Oändligt antal primtal

Sats: *Det finns oändligt många primtal.* Denna sats bevisades först av Euklides. Efter det har satsen bevisats många fler gånger på olika sätt. Några av dessa är varianter av Euklides bevis och kommer här att tas upp.

4.1 Euklides bevis

I *Elementa* definierar Euklides ett primtal som *"Ett tal som endast mäts av sig självt"*. Euklides använder uttrycket *mäter* i samma mening som vi säger *delar* idag. Han bevisar senare att det finns oändligt antal primtal. Här följer vi [6, s. 66][4, s. 2] och beviset lyder:

Vi har en ändlig uppsättning av primtal. Vi kan kalla dess produkt för D. Då är $D + 1$ antingen ett primtal eller ej. Om det är ett primtal har vi lyckats finna ett primtal utanför vår ändliga uppsättning av primtal. Om det inte är ett primtal är det ett sammansatt tal. Detta sammansatta tal är ej delbart med något av talen i vår uppsättning av primtal. Detta eftersom $D + 1$ ger resten 1 vid division med dessa. Alltså är detta sammansatta tal delbart med något primtal som inte ingår i vår ursprungliga uppsättning. Alltså har vi även här lyckats hitta ett primtal utanför vår ändliga uppsättning av primtal.

Av detta följer att för vilken ändlig uppsättning av primtal som helst, kan vi alltid hitta ett primtal som ligger utanför mängden. Alltså finns det oändligt många primtal.

4.1.1 Euklides-Mullin-följden

Den amerikanske matematikern Albert A. Mullin (1933-2017) använde Euklides bevis för att definiera en talföljd som är uppkallad efter både honom och Euklides. Följdens element består av den största primtalsfaktorn i det tal som är summan av produkten av alla primtal hittills och talet ett, alltså $D + 1$ i beviset ovan. Vi börjar med talet 2, eftersom det är det första primtalet. Det andra elementet i följden ges då av den största primtalsfaktorn i $2 + 1 = 3$, som är 3 eftersom det är ett primtal. Det tredje elementet är $2 \cdot 3 + 1 = 7$ och nästa tal i följden är $2 \cdot 3 \cdot 7 + 1 = 43$. Det femte elementet är 139, eftersom $2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$, som är ett sammansatt tal av primtalsfaktorerna 13 och 139, därför blir det femte elementet 139. Sekvensen växer snabbt och de första 9 elementen är

$$2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 4680225641471129.$$

Det har dock visat sig att följden inte är strikt växande, exempelvis är det tionde elementet mindre än det nionde. En annan fråga man ställde sig var huruvida alla primtal ingår i följden eller ej. Svaret har visat sig vara nej. Det finns en variant på följden, med samma namn. Om man istället låter följden byggas upp

av den *minsta* primtalsfaktorn som element är de 9 första elementen

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571.$$

Här ser vi hur exempelvis följdens femte element blir 13 istället för 139, eftersom vi här utgår från den minsta primtalsfaktorn. Följden är uppenbarligen inte strikt växande, den amerikanske matematikern Daniel Shanks (1917-1996) förmodade år 1991 att varje primtal förekommer som element i följden. Huruvida det stämmer eller ej får framtiden utvisa!

4.2 Charles Hermites bevis

Om vi följer [4, s. 4] visade den franske matematikern Charles Hermite (1822-1901) satsen med en mycket liknande metod. Han tänkte sig ett tal n där $n > 1$ och om $p \leq n$ kommer $p \mid n!$ men $p \nmid (n! + 1)$ eftersom vi då alltid kommer att få resten 1.

Precis som i Euklides bevis har vi nu två möjligheter. Antingen är $n! + 1$ ett primtal eller inte. Är det ett primtal finns det primtal $> n$. Är det inte ett primtal är det ett sammansatt tal. Alla primtal i primtalsfaktoriseringen av detta tal måste vara $> n$; alltså har vi, precis som i Euklides bevis, visat att det alltid kommer att finnas ett större primtal $\forall n$.

4.3 Jan Thomas Stieltjes bevis

Även den nederländske matematikern Jan Thomas Stieltjes (1856-1894) bevis av satsen liknar Euklides bevis. Han utgår också från en ändlig uppsättning av primtal. Om vi sätter K till produkten av alla dessa kan vi skriva $K = a \cdot b$ där a och b är två positiva heltal. Då gäller för varje primtal p i vår uppsättning att p delar *en* av a och b men *inte båda*. Detta medför att p inte delar $a + b$. Alltså: $a + b$ är inte delbart med något av primtalen i vår givna uppsättning. Vi har även $a + b > 1$. Alltså, genom att betrakta ett godtyckligt primtal i primtalsfaktoriseringen av $a + b$, får vi precis som i Euklides bevis ett *nytt* primtal som är utanför vår ändliga uppsättning primtal.

Man kan säga att Stieltjes bevis är en generalisering av Euklides bevis, för om vi väljer $a = 1$ och $b = K$ så gäller $a + b = K + 1$.

5 Avslutning

I denna uppsats har några olika resultat rörande primtal kopplat till Euklides presenterats. Vi inledde med beviset av den välkända aritmetikens fundamentalsats och dess tillämpning på de gaussiska heltalen. Sedan visade vi ett par talmängder där aritmetikens fundamentalsats inte gäller. Vi presenterade därefter hur Euklides bevisade att bland annat $\sqrt{2}$ är irrationellt.

Därefter diskuterade vi relativt prima tal och hur Euklides algoritm fungerar och hur den kan användas för att ta reda på om två tal är relativt prima. Exempel presenterades på Euklides algoritm, Euklides algoritm för gaussiska heltal, Euklides algoritm baklänges samt vilka användningsområden dessa har.

Slutligen presenterade vi olika bevis för Euklides sats, alltså att det finns ett oändligt antal primtal. Två varianter på detta bevis presenterades också samt en talföljd med nära koppling till Euklides bevis.

Referenser

[1] Underwood Dudley. *Elementary Number Theory.* Dover Publications, 2008.

[2] Dana Mackenzie. Homage to an itinerant master. *Science*, 275(5301):759–759, 1997.

[3] Ivan Niven Herbert S. Zuckerman Hugh L. Montgomery. *An introduction to the theory of numbers.* Wiley, 1991.

[4] Wladyslaw Narkiewicz. *The Development of Prime Number Theory.* Springer, 2000.

[5] Jan Thompson. *Matematiken i historien.* Studentlitteratur, 1996.

[6] David Wells. *Prime Numbers The Most Mysterious Figures in Math.* Wiley, 2005.