SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Gaussiska primtal och andra prima faktorer

av

Jenny Arthur

2016 - No 13

Gaussiska primtal och andra prima faktorer

Jenny Arthur

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torbjörn Tambour

2016

Sammanfattning

Alla heltal kan entydigt faktoriseras i primtal enligt aritmetikens fundamentalsats. Men går det att faktorisera primtal på något sätt? I den här uppsatsen undersöks hur vi, genom att utvidga mängden till de gaussiska heltalen, kan faktorisera en del av våra vanliga primtal. Vi undersöker vilka olika typer av gaussiska primtal det finns och hur vi känner igen dem. I uppsatsens sista del ser vi ett exempel på att det även går att faktorisera i andra ringar.

Innehåll

1 Inledning

Den här uppsatsen handlar om heltal och hur dessa kan faktoriseras i primtal. Alla heltal kan entydigt faktoriseras i primtal enligt aritmetikens fundamentalsats. Entydigheten innebär dock inte att faktoriseringen bara kan se ut på ett sätt, utan att vissa uttryck anses vara lika eller tillräckligt lika enligt definitionen. Räkneoperationer med heltal är i vissa fall, som med addition och multiplikation, okomplicerade, men vi kommer att titta närmare på hur divison med heltal utförs. Med hjälp av divisionsalgoritmen och Euklides algoritm kommer vi att räkna ut största gemensamma delare av två tal.

En del primtal i $\mathbb{Z}$ kan anmärkningsvärt nog faktoriseras om vi utvidgar mängden till de gaussiska heltalen $\mathbb{Z}[i]$. Gaussiska heltal är tal på formen $a + bi$, där a och b är heltal i $\mathbb{Z}$. De gaussiska heltalen är alltså en delmängd av de komplexa talen. Vi går igenom vilka kriterier som gäller för att ett primtal i $\mathbb{Z}$ ska kunna faktoriseras i $\mathbb{Z}[i]$ och vilka som förblir primtal i $\mathbb{Z}[i]$. Här har vi bland annat Fermats tvåkvadratsats till vår hjälp som säger att ett udda primtal p kan skrivas som en summa av två heltalskvadrater om och endast om $p \equiv 1 \mod 4$.

Den sista delen handlar om faktoriseringar i $\mathbb{Z}[\omega]$, där ω definieras som en rot till $z^3 = 1$ och $\omega \neq 1$. Vi tittar på egenskaper hos dessa tal och hur primtal i $\mathbb{Z}$ ska vara beskaffade för att kunna faktoriseras i $\mathbb{Z}[\omega]$.

I mitt arbete med uppsatsen har jag främst använt mig av två böcker i talteori, *A Classical Introduction to Modern Number Theory* av Ireland & Rosen [4] och *An Introduction to the Theory of Numbers* av Hardy & Wright [3] samt en artikel av Conrad, *The Gaussian Integers* [1]. För att sätta mig in i ämnet har jag också haft hjälp av *Algebra for Computer Science* av Gårding & Tambour [2] och skaffat mig en översiktlig bild av Gauss, mannen som fått namnge de gaussiska primtalen, genom boken *A Concise History of Mathematics* av Struik [5].

2 Heltalen

2.1 Primtal och enheter

Primtal definieras ofta i grundläggande kurser som tal större än 1 som har de enda positiva delarna sig själv och 1. Det går även att tala om negativa primtal och här utvidgas definitionen till att primtal är tal som bara kan delas med sig själva och enheter.

Ett tal u är en enhet om och endast om det finns ett tal v så att $u \cdot v = 1$. Vi kan även kalla v multiplikativ invers till u och skriver då $v = u^{-1}$. De enda enheterna i $\mathbb{Z}$ är 1 och -1, eftersom $u \cdot v = 1$ ger att $u = 1/v$ och eftersom vi befinner oss i $\mathbb{Z}$ måste såväl $1/v$ som v vara heltal och då är enda möjligheten att $v = \pm 1$, vilket ger att $u = \pm 1$. Enheter i $\mathbb{Z}$ är alltså ± 1.

Om p är ett primtal är därmed även $-p$ ett primtal. Om två tal endast skiljer sig åt med en faktor av en enhet kallas talen associerade, vilket innebär att p och $-p$ är associerade.

2.2 Divisionsalgoritmen

Divisionsalgoritmen vid divsion med heltal är helt enkelt vanlig division med rest.

Sats 1 *Till varje heltal a och b, där $b \neq 0$ finns ett unikt heltal q (kvot), och ett unikt heltal r (rest), så att $a = qb + r$ där $0 \leq r < |b|$.*

Exempel
Vi delar 23 med 7. Då får vi kvoten 3 och resten 2.

$$\frac{23}{7} = 3 + \frac{2}{7}$$

Med divisionsalgoritmen skriver vi således:

$$23 = 3 \cdot 7 + 2$$

Ett sätt att tänka på uttrycket $a = qb + r$ är att sätta ut talet a och alla multipler av b på en tallinje. Då ser vi att det finns precis ett heltal q sådant att $q|b| \leq a < (q+1)|b|$. Det finns alltså precis en heltalskvot, q och en rest, r, där $r = a - q|b|$.

2.3 Euklides algoritm

Det största heltal som delar de båda heltalen a och b kallas största gemensamma delare, $SGD(a, b)$.

Lemma 1 *Om ett tal d delar två tal, a och b, så delar d också varje linjärkombination av a och b.*

Bevis
Om $d|a$ och $d|b$ kan vi skriva $a = a_1 d$ och $b = b_1 d$. Då är $ka+lb = (ka_1+lb_1)d$, vilket innebär att det finns ett tal c så att $ka + lb = cd$. Alltså ser vi att $d|(ka + lb)$. □.

Med hjälp av Euklides algoritm kan vi räkna ut $SGD(a, b)$, vilket i princip innebär att vi använder oss av divisonsalgoritmen upprepade gånger. Vi utgår från talen a och b och börjar med att dividera a med b och skriver med hjälp av divisionsalgoritmen

$$a = kb + r$$

. Sedan gör vi samma sak med b och r och skriver

$$b = k_1 r + r_1$$

Vi fortsätter på samma sätt och får på så sätt hela tiden nya rester. Resterna blir hela tiden mindre och mindre, $r > r_1 > r_2 ... > r_n$ och därför kommer vi så småningom att komma fram till en rest som är lika med 0.

$$\begin{aligned} a &= kb + r \\ b &= k_1 r + r_1 \\ r &= k_2 r_1 + r_2 \\ &... \\ r_{n-2} &= k_n r_{n-1} + r_n \\ r_{n-1} &= (k_{n+1}) r_n \end{aligned}$$

Bevis för Euklides algoritm
Vi dividerar a med b och skriver med hjälp av divisionsalgoritmen uttrycket som $a = bq + r$ Med hjälp av lemma 1 kan vi se att alla tal som delar a och b delar r och omvänt att de tal som delar b och r delar a. Alltså har a och b samma gemensamma delare som b och r. Speciellt har de samma största gemensamma delare, $SGD(a, b) = SGD(b, r)$. Om vi upprepar detta så får

vi $SGD(a,b) = SGD(b,r) = SGD(r,r_1) = SGD(r_{n-1},r_n) = r_n$ $\square$

Exempel
Beräkna $SGD(221, 1976)$ Vi delar det större talet med det mindre:

$$1976 = 8 \cdot 221 + 208$$

Vi skriver nu om 221 med hjälp av resten:

$$221 = 208 + 13$$
$$208 = 16 \cdot 13$$

Vi ser att här är vår sista nollskilda rest är 13 och enligt satsen är den sista nollskilda resten vår största gemensamma delare. Alltså är $SGD(232, 1797) = 13$. Om vi löser ut resterna får vi

$$208 = 1976 - 8 \cdot 221$$
$$13 = 221 - 208$$

När vi sedan skriver om vår sista nollskilda rest med hjälp av de andra resterna får vi fram ett uttryck på formen $d = xa + yb$, där $d = SGD(a, b)$. I vårt exempel blir det:

$$13 = 221 - 208$$
$$13 = 221 - (1976 - 8 \cdot 221)$$
$$13 = 9 \cdot 221 - 1976$$

Två tal vars största gemensamma delare är 1 kallas relativt prima.

Lemma 2 *Låt d vara den största gemensamma delaren till a och b. Då finns heltal x och y sådana att $d = xa+yb$. Speciellt gäller att om a och b är relativt prima, så finns heltal x och y sådana att $xa + yb = 1$.*

Att vi kan skriva $xa + yb = d$ följer från beviset för Euklides algoritm. Om a och b är relativt prima är deras största gemensamma delare 1 och därav följer att vi kan skriva $xa + yb = 1$.

2.4 Entydig faktorisering

Alla heltal, förutom 0 och ± 1, kan faktoriseras i primtal på precis ett sätt, sånär som på ordning och associering. Alla dessa heltal är således produkter av primtal, eftersom vi tillåter produkter att bestå av endast en faktor.

Exempel

$$363 = 11 \cdot 11 \cdot 3$$

Att ordningen inte spelar någon roll innebär att primtalsfaktoriseringen

$$66 = 11 \cdot 3 \cdot 2$$

och

$$66 = 3 \cdot 11 \cdot 2$$

anses vara samma faktorisering.

Associering innebär multiplikation med enheter. I $\mathbb{Z}$ har vi enheterna 1 och -1. Ett exempel på associerade tal är således -3 och 3. Faktoriseringar får skilja sig åt med avseende på associering, det vill säga vi kan multiplicera med enheter och få samma produkt. Exempel:

$$66 = 11 \cdot 3 \cdot 2 = 11 \cdot (-3) \cdot (-2)$$

Vi noterar att när vi gör förändringar och multiplicerar med enheter förekommer de alltid i par. Här har vi multiplicerat två faktorer med enheten -1.

Lemma 3 *Om $p|ab$ delas minst en av faktorerna av p.*

Bevis
Låt p vara ett primtal som delar ab, det vill säga $p|ab$. Vi antar att p inte delar a och vill visa att p då delar b. Eftersom p inte delar a är $SGD(p, a) = 1$ och enligt Euklides algoritm kan vi skriva $xp + ya = 1$. Vi multiplicerar med b och får $bxp + bya = b$. Givetvis delar p talet p och vi har fått givet att p delar ab. Därmed vet vi att vi kan dela vänsterledet med p och således måste även högerledet delas av p. Alltså $p|b$.[4] □

Nu har vi allt som behövs för att genomföra beviset för aritmetikens fundamentalsats.

Sats 2 (Aritmetikens fundamentalsats) *Varje heltal $a>1$ kan skrivas som en produkt av primtal på ett och endast ett sätt.*

Bevis
Vi börjar med att visa att ett tal $a > 1$, det vill säga ett positivt a som

inte är en enhet, alltid kan faktoriseras i primtal. Vi har två olika fall. Antingen är $a = p_1$ och primtalsfaktoriseringen är redan klar. (Vi tillåter alltså att faktoriseringen består av ett enda tal.) I det andra fallet är a inte ett primtal. Då låter vi p_1 vara ett primtal som delar a och skriver $a = p_1q_1$. Om q_1 är ett primtal är faktoriseringen klar, annars är $q_1 = p_2q_2$. Om q_2 inte är något primtal får vi $a = p_1p_2q_3$ och fortsätter på samma sätt så att $a = p_1p_2...q_n$. Eftersom $a > q_1 > ... > q_n$ måste till slut något q_n bli 1 och vi har faktoriserat a.

Vi behöver också bevisa att faktoriseringen är entydig. Vi börjar med talet $n = 2$. Eftersom 2 är ett primtal, vet vi att faktoriseringen är trivialt unik. Vi tittar nu på ett tal n som är större än 2. Vi antar att det finns tal som kan faktoriseras på olika sätt och att vårt tal n är det minsta talet med olika faktoriseringar: $n = p_1...p_r = q_1...q_s$ där alla faktorer är primtal. Vi vill nu visa att dessa faktoriseringar inte kan vara olika. Vi delar med p_1 och enligt lemma 3 vet vi att p_1 delar minst en av faktorerna i högerledet,

$$\frac{n}{p_1} = p_2...p_r = \frac{q_1...q_s}{p_1}$$

Eftersom alla faktorer är primtal måste p_1 vara lika med en av faktorerna i högerledet. Vilken faktor det är spelar ingen roll, vi numrerar om dem så att $p_1 = q_1$. Vi betraktar nu talet

$$\frac{n}{p_1} = p_2...p_r = q_2...q_s$$

Här skrivs talet $\frac{n}{p_1}$, som uppenbarligen är mindre än n, som ett tal med olika primtalsfaktoriseringar, men n skulle ju vara det minsta tal som skulle gå att faktorisera på olika sätt. Alltså kan det inte finnas några tal som går att faktorisera på olika sätt. □

3 De gaussiska heltalen

Nu har vi kommit fram till de gaussiska heltalen, som är tal på formen $a+bi$, där a och b är heltal i $\mathbb{Z}$ och där $i = \sqrt{-1}$. Talen är uppkallade efter Carl Friedrich Gauss, som levde 1777-1855 och anses vara en av historiens största matematiker. Han visade att många områden i talteorin blev enklare genom att använda beräkningar med komplexa tal och utformade en ny primtalsteori där en del primtal kunde faktoriseras i komplexa tal, så kallade gaussiska

primtal. [5]

Mängden av gaussiska heltal betecknas $\mathbb{Z}[i]$. Summor och produkter av gaussiska heltal är gaussiska heltal, det vill säga mängden $\mathbb{Z}[i]$ är sluten under addition och multiplikation, vilket följer omedelbart av regler för addition och multiplikation av komplexa tal:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

3.1 Norm och enheter

Normen av ett gaussiskt heltal, z (där $z=a+bi$) skrivs $N(z)$ och definieras som a^2+b^2, det vill säga $N(z)=z\overline{z}=(a+bi)(a-bi)$. Vi kan också tänka på normen som kvadraten på absolutbeloppet

$$N(z)=|a+bi|^2=(\sqrt{a^2+b^2})^2=a^2+b^2$$

Normen är multiplikativ, det vill säga $N(u)N(v)=N(uv)$.

Bevis
Om $u=a+bi$ och $v=c+di$, så är $uv=(ac-bd)+(ad+bc)i$

$$\begin{aligned}N(u)N(v)&=(a^2+b^2)(c^2+d^2)=(ac)^2+(ad)^2+(bc)^2+(bd)^2\\N(uv)&=(ac-bd)^2+(ad+bc)^2=\\&=(ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2=\\&=(ac)^2+(bd)^2+(ad)^2+(bc)^2=\\&=N(u)N(v)\end{aligned}$$

□

Som vi tidigare sagt i $\mathbb{Z}$, kallas ett tal som har en multiplikativ invers för en enhet. Detta kan generaliseras till $\mathbb{Z}[i]$ och ett gaussiskt heltal, $u=a+bi$, är alltså en enhet om det finns ett gaussiskt heltal v så att $u\cdot v=1$. Således är v den multiplikativa inversen till u och vi kan skriva $v=u^{-1}$. 1 och -1 är alltså sina egna inverser och i och $-i$ är varandras inverser. Vi kontrollerar om ±1 och $\pm i$ är de enda enheterna i $\mathbb{Z}[i]$. Vi räknar med normen på båda sidor:

$$N(uu^{-1})=1^2$$

$$N(u)N(u^{-1})=1$$

Normen är ett icke-negativt heltal, så $N(u) = 1$. Normen av u kan vi också skriva som

$$N(u) = a^2 + b^2$$

och vi får ekvationen $a^2 + b^2 = 1$, vilken har lösningarna

$$a = \pm 1 \text{ och } b = 0$$

$$a = 0 \text{ och } b = \pm 1$$

De enda enheterna i $\mathbb{Z}[i]$ är alltså: $1, -1, i$ och $-i$.

3.2 Delbarhet

Delbarhet i $\mathbb{Z}[i]$ definieras likadant som i $\mathbb{Z}$, enda skillnaden är att vi nu räknar med komplexa tal.

Ett tal w delar z, om $z = wu$ för något $u \in \mathbb{Z}[i]$.

Exempel:
Eftersom $(5 + i)(3 + 2i) = 13 + 13i$, ser vi att $3 + 2i$ delar $13 + 13i$.

Sats 3 *För $w, z \in \mathbb{Z}[i]$ gäller att om $w|z$ så $N(w)|N(z)$.*

Bevis
Vi skriver $z = wu$ där $z, w, u \in \mathbb{Z}[i]$. När vi tar normen på båda sidor, får vi $N(z) = N(w)N(u)$ och vi ser därmed att $N(w)|N(z)$ i $\mathbb{Z}$.

Detta är användbart för att undersöka när ett gaussiskt heltal inte delar ett annat. Delas inte normen vet vi att inte heller det gaussiska heltalet delas och vi har besparat oss räkningar med komplexa tal. Däremot är det motsatta fallet oftast falskt. Normerna av talen kan mycket väl vara delbara med varandra utan att de gaussiska heltalen delar varandra.

3.3 Divisionsalgoritmen

För att utföra division i $\mathbb{Z}[i]$ börjar vi med att multiplicera med nämnarens konjugat för att få ett heltal i nämnaren och ser sedan om täljaren kan delas med detta heltal och utför i så fall divisionen .

$$\frac{8+12i}{5+i} = \frac{(8+12i)(5-i)}{(5+i)(5-i)} = \frac{52+52i}{26} = 2+2i$$

I det här fallet blev resultatet ett gaussiskt heltal, men oftast kommer täljaren inte att vara delbar med nämnaren och resultatet blir då således inte ett gaussiskt heltal.

I divionsalgoritmen i $\mathbb{Z}$ använde vi oss av icke-negativa rester, $0 \leq r < w$ där r är resten och w är divisorn. I $\mathbb{Z}[i]$ kommer vi istället att använda *absolut minsta rester*, det vill säga vi har valt resten så att den ligger så nära 0 som möjligt. Vi skulle förstås kunna räkna med absolut minsta rester i $\mathbb{Z}$ också och då tillåta negativa rester, så att $|r| \leq w/2$. För att avgöra storleken på ett tal i $\mathbb{Z}[i]$ räknar vi med normen. Att resten ligger så nära 0 som möjligt kan vi uttrycka som att $N(r) \leq (1/2)N(w)$.

Sats 4 (Divisionsalgoritmen för de gaussiska heltalen) *För $z, w \in \mathbb{Z}[i]$ där $w \neq 0$, finns det $u, v \in \mathbb{Z}[i]$, så att $z = uw+v$ och där $N(v) \leq (1/2)N(w)$.*

Här är vår kvot u och resten kallar vi v.

Bevis
Vi har $z, w \in \mathbb{Z}[i]$ där $w \neq 0$ och vi vill konstruera $u, w \in \mathbb{Z}[i]$ så att $z = wu + v$ där $N(v) \leq (1/2)N(w)$.

Vi skriver

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{z\overline{w}}{N(w)} = \frac{a+bi}{N(w)}$$

Vi delar a och bi med $N(w)$ och låter

$$a = N(w)q_1 + r_1$$

$$b = N(w)q_2 + r_2$$

$$q_1, q_2 \in \mathbb{Z} \text{ och } 0 \leq |r_1|, |r_2| \leq (1/2)N(w)$$

Då blir

$$\frac{z}{w} = \frac{N(w)q_1 + r_1 + (N(w)q_2 + r_2)i}{N(w)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(w)}$$

Sätt nu $u = q_1 + q_2 i$, vilken blir vår eftersökta kvot. Då får vi:

$$\begin{aligned} \frac{z}{w} &= u + \frac{r_1 + r_2}{w\overline{w}} \\ z &= uw + \frac{r_1 + r_2}{\overline{w}} \\ z - uw &= \frac{r_1 + r_2}{\overline{w}} \end{aligned}$$

Vi vill visa att $N(z - wu) \leq (1/2)N(w)$, så vi använder $v = z - wu$. Vi tar normen av båda sidorna och använder oss av att $N(\overline{w}) = N(w)$ och får

$$N(z - wu) = \frac{(r_1)^2 + (r_2)^2}{N(w)}$$

Vi använder nu att $0 \leq |r_1|, |r_2| \leq (1/2)N(w)$ och får

$$N(z - wu) \leq \frac{(1/4)(N(w))^2 + (1/4)(N(w))^2}{N(w)} = \frac{1}{2}N(w).$$

□

Exempel
Låt $z = 25 + 18i$ och $w = 3 - i$. Då är $N(w) = 10$. Vi vill dela z med w. Det vill säga skriva $z = qw + r$, där q är kvoten och r är resten och där $N(r) < N(w)$

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{(25 + 18i)(3 + i)}{10} = \frac{57 + 79i}{10}$$

Av detta tal vill nu hitta den kvot som ger oss den *absolut minsta resten*. Observera att vi inte kommer att räkna med denna absolut minsta rest, vi använder bara resonemanget om den för att hitta rätt kvot. I realdelen har vi $\frac{57}{10}$ vilket ger kvoten 6 (och resten -3, vilken vi alltså inte använder oss av) och i imaginärdelen har vi $\frac{79i}{10}$, vilket ger kvoten $8i$ (och resten $-i$) Vi sätter

ihop dessa och får vårt $q = 6 + 8i$. Vi vill nu få fram vårt r. Vi använder formeln $z = wq + r$ och löser ut $r = z - wq$ och får:

$$25 + 18i - (3 - i)(6 + 8i) = -1 = r$$

Vi kontrollerar så att $N(r) < N(w)$. Eftersom $N(r) = 1$ och $N(w) = 10$, så ser vi att olikheten är uppfylld.

3.4 Euklides algoritm

Vi definierar en största gemensam delare till två tal z och w (där z och w är skilda från 0) i $\mathbb{Z}[i]$, som en delare som har maximal norm. Det innebär att det kan finnas flera största gemensamma delare i $\mathbb{Z}[i]$. Associerade tal har samma norm, så om $SGD(z, w) = u$, så är även $-u, iu$ och $-iu$ största gemensamma delare till z och w.

Euklides algoritm fungerar på samma sätt som i $\mathbb{Z}$ och beviset utförs analogt. Låt z och w vara tal i $\mathbb{Z}[i]$ som är skilda från 0.

$$\begin{aligned} z &= wq_1 + r_1, N(r_1) < N(w) \\ w &= r_1q_2 + r_2, N(r_2) < N(r_1) \\ r_1 &= r_2q_3 + r_3, N(r_3) < N(r_2) \\ &.... \\ r_{n-2} &= r_{n-1}q_n + r_n, N(r_n) < N(r_{n-1}) \end{aligned}$$

I $\mathbb{Z}$ var resten alltid mindre än kvoten, men när vi räknar med komplexa tal är det inte meningsfullt att tala om vilket tal som är minst. Därför räknar vi istället med normerna av resterna så att $N(r_{n+1}) < N(r_n) < ... < N(r_1)$. Eftersom normerna av resterna kommer att minska successivt kommer vi alltid så småningom fram till en rest som är 0. Liksom i $\mathbb{Z}$ ser vi att alla delare till z och w är delare även till r_n. Alla delare har därför normer som är mindre än eller lika med $N(r_n)$. Å andra sidan ser vi också att r_n är en delare till z och w, och då måste r_n vara en största gemensam delare.

Sats 5 *Om $SGD(z, w) = d$, där $z, w \in \mathbb{Z}[i]$ är övriga gemensamma delare d multiplicerat med enheter.*

Bevis
Vi såg ovan att r_n i Euklides algoritm är en största gemensam delare till z och w. Låt d vara en annan. Då är d, också enligt vad vi såg ovan, en

delare till r_n. Skriv $r_n = de$. Tar vi normerna så får vi $N(r_n) = N(d)N(e)$. Men r_n och d har samma norm eftersom de är största gemensamma delare, så $N(e) = 1$ och e är således en enhet. Alltså är alla största gemensamma delare associerade till r_n och därmed till varandra. □

Exempel
Vi utför Euklides algoritm för att hitta $SGD(z, w)$, där $z = 32 + 9i$ och $w = 4 + 11i$.

För att utföra divisionen $\dfrac{32+9i}{4+11i}$ förlänger vi först med konjugatet och får

$$\frac{(32+9i)(4-11i)}{(4+11i)(4-11i)} = \frac{128-352i+36i-99i^2}{16-121i^2} = \frac{227-316i}{137}$$

Den kvot som ger den minsta resten blir i det här fallet $2-2i$. Vi skriver om $32+9i = (4+11i)(2-2i)+r_1$ och räknar ut att r_1 måste vara $2-5i$. 1:a raden i Euklides algoritm blir alltså:

$$32 + 9i = (4 + 11i)(2 - 2i) + 2 - 5i$$

Räkningarna sker sedan på samma sätt och vi får vidare:

$$\begin{aligned} 4 + 11i &= (2 - 5i)(-2 + i) + 3 - i \\ 2 - 5i &= (3 - i)(1 - i) - i \\ 3 - i &= (-i)(1 + 3i) + 0 \end{aligned}$$

Vår sista nollskilda rest är alltså $-i$, vilket innebär att z och w är relativt prima, vilket är fallet när vår rest är en enhet. Vi kan jämföra med när vi kommer fram till $SGD(a, b) = 1$ i $\mathbb{Z}$. [1]

Sats 6 (Bezouts sats) *Låt δ vara en största gemensam delare av två gaussiska heltal α,$\beta \neq 0$. Då är $\delta = \alpha x + \beta y$ för några $x, y \in \mathbb{Z}[i]$. Speciellt gäller att de gaussiska heltalen α och β är relativt prima om och endast om vi kan skriva $1 = \alpha x + \beta y$ för några $x, y \in \mathbb{Z}$.*

Bevis
Att vi kan skriva $x\alpha + y\beta = \delta$ följer från beviset för Euklides algoritm. Om α och β är relativt prima innebär det att 1 är en största gemensam delare till α och β och vi kan skriva $1 = \alpha x + \beta y$ för $x, y \in \mathbb{Z}$. Omvänt gäller att om $\alpha x + \beta y = 1$ så måste alla delare till α och β vara delare till 1, vilket endast enheter kan vara och därmed är α och β relativt prima. □

3.5 Gaussiska primtal

Ett gaussiskt primtal är ett gaussiskt heltal som inte kan delas upp i faktorer, således motsvarigheten i $\mathbb{Z}[i]$ till primtal i $\mathbb{Z}$. En faktor måste vara en äkta delare och inte bara en enhet. Vi ska nedan se samband mellan primtal i $\mathbb{Z}$ och i $\mathbb{Z}[i]$.

Sats 7 *Ett gaussiskt heltal vars norm är ett primtal i $\mathbb{Z}$, är ett primtal i $\mathbb{Z}[i]$.*

Bevis
Antag att $N(w) = p$ och att $w = uz$. Då är $p = N(w) = N(u)N(z)$. Därmed är antingen $N(u) = 1$ eller är $N(z) = 1$ och antingen u eller z är en enhet, vilket innebär att w är ett primtal. □

Exempel
Vi har $N(3+2i) = (3+2i)(3-2i) = 13$, där 13 är ett primtal i $\mathbb{Z}$ och $3+2i$ är ett primtal i $\mathbb{Z}[i]$. Vi ser också att $N(1+i) = (1+i)(1-i) = 2$ och 1+i är ett gaussiskt primtal, vilket följer av sats 7. Detta är ett sätt att med relativt enkla beräkningar kontrollera om ett gaussiskt heltal är ett primtal.

Däremot fungerar satsen inte i andra riktningen, dvs om $N(u)$ inte är ett primtal kan ändå u vara ett primtal. Till exempel är $N(3) = 9$. Antag att $3 = (a+bi)(c+di)$. Då är $9 = (a^2+b^2)(c^2+d^2)$. Eftersom 9 kan faktoriseras som $9 = 3 \cdot 3$ så måste $a^2 + b^2$ vara lika med $c^2 + d^2$, men det är omöjligt eftersom 3 inte är summan av två kvadrater. [3]

Vilka delare finns det till ett gaussiskt primtal, z? Talet z delas av sig själv, sina enheter, eller sig själv multiplicerat med enheter, det vill säga associeringar av z. Därmed finns det 8 delare: $1, -1, i, -i, z, -z, iz, -iz$.

Att känna till ett gaussiskt heltal upp till multiplikation med en enhet, är jämförbart med att känna till ett heltal i $\mathbb{Z}$ upp till dess tecken (enheterna i $\mathbb{Z}$ är ju 1 och -1).

3.6 Entydig faktorisering

Ett gaussiskt heltal, z, är sammansatt om det kan faktoriseras i icke-triviala faktorer, annars är det ett gaussiskt primtal. Trivial faktorisering är när en faktor är en enhet, det vill säga en faktor som har normen 1. Ett exempel på

trivial faktorisering är $7+i = i(1-7i)$. Exempel på icke-trivial faktorisering: $7 + i = (1 - 2i)(1 + 3i)$. Ett sammansatt gaussiskt heltal kan skrivas som $z = wu$, där $N(w) > 1$ och $N(u) > 1$.

För att kunna bevisa aritmetikens fundamentalsats i $\mathbb{Z}[i]$ behöver vi en sats till, vi vill undersöka om det är möjligt att faktorisera. För att kunna genomföra beviset behöver vi följande sats:

Sats 8 *Låt π vara ett primtal i $\mathbb{Z}[i]$ och låt $\alpha_1, ..., \alpha_r$ vara gaussiska heltal. Om $\pi|\alpha_1, ..., \alpha_r$ delar π någon av faktorerna.*

Bevis
Vi låter $\pi|\alpha_1\alpha_2$. Antag att π inte delar α_1, vilket implicerar att π och α_1 är relativt prima, annars skulle de ha en största gemensam delare som skulle vara en multipel av π. Eftersom α_1 och π är relativt prima, så kan vi enligt Bezouts sats skriva $x\pi+y\alpha_1 = 1$. Vi förlänger med α_2 och får $\alpha_2 x\pi+\alpha_2 y\alpha_1 = \alpha_2$. Vi har fått givet att $\pi|\alpha_1\alpha_2$ och π delar förstås π. Därmed ser vi att vänsterledet delas av π, vilket innebär att även högerledet måste delas av π. □

Sats 9 (Aritmetikens fundamentalsats) *Varje tal $z \in \mathbb{Z}[i]$ med $N(z) > 1$ kan faktoriseras i $\pi_1\pi_2 \ldots \pi_n$ där varje π är ett primtal. Denna representation är unik med undantag för ordningen av primtalen och variationer mellan associerade primtal.*

Bevis
Vi börjar med att visa att ett tal z kan alltid faktoriseras i primtal om $N(z) > 1$, det vill säga när z inte är en enhet. Vi har liksom i $\mathbb{Z}$ två olika fall. Antingen är $z = \pi_1$ och primtalsfaktoriseringen är redan klar. I det andra fallet är z inte ett primtal. Då låter vi π_1 vara ett primtal som delar a och skriver $z = \pi_1 q_1$. Om q_1 är ett primtal, det vill säga $q_1 = \pi_2$, är faktoriseringen klar annars fortsätter vi så att $z = \pi_1\pi_2...q_n$. Eftersom $N(z) > N(q_1) > N(q_2) > ... > N(q_n)$ kommer vi så småningom fram till $q_n = 1$ och primfaktoriseringen är klar.

Att faktoriseringen är unik kan visas på samma sätt som i $\mathbb{Z}$. Om $N(z) = 2$, så är z ett primtal och faktoriseringen trivialt unik. Antag att det finns gaussiska heltal som inte har unik primfaktorisering och låt z vara ett sådant tal med minimal norm. Vi har två faktoriseringar $z = \pi_1...\pi_r = q_1...q_s$, där alla faktorer är gaussiska primtal. Primtalet π_1 delar $q_1...q_s$ och enligt

sats 8 delar det då någon av faktorerna. Efter omnumrering kan vi anta att $\pi_1|q_1$. Men båda talen här är primtal, så de måste vara associerade. Säg att $q_1 = u\pi_1$, där u är en enhet. Då får vi $w = \frac{z}{\pi_1} = \pi_2...\pi_r = uq_2...q_s = q_2'q_3...q_s$, där $q_2' = uq_2$ också är ett primtal. Talet w har mindre norm än z och har därför unik primfaktorisering. Alltså är $r = s$ och efter en eventuell omnumrering är π_i och q_i associerade för $i = 2, ..., r$. Tydligen har även z en unik primfaktorisering och det finns inga tal med olika primfaktoriseringar. □

Trots att faktoriseringen är entydig är det inte alltid uppenbart vid en första anblick att primfaktoriseringarna är lika.

Exempel

$$-4 + 7i = (2 + 3i)(1 + 2i)$$

$$-4 + 7i = (3 - 2i)(-2 + i)$$

$$(2 + 3i)(1 + 2i) = (2 + 3i)(-i)(1 + 2i)i = (3 - 2i)(-2 + i)$$

Vi kan jämföra med faktoriseringen i $\mathbb{Z}$ där $140 = 7 \cdot 5 \cdot 2 \cdot 2$ anses vara samma faktorisering som $140 = 7 \cdot (-5) \cdot 2 \cdot (-2)$, där det enda som skiljer är att vi har multiplicerat två faktorer med enheten -1.

3.7 Tvåkvadratsatsen

Vilka primtal i $\mathbb{Z}$ är även gaussiska primtal? För att besvara denna fråga kommer vi att använda Fermats tvåkvadratsats.

Sats 10 (Fermats tvåkvadratsats) *Ett positivt udda primtal p kan skrivas som en summa av två heltalskvadrater om och endast om $p \equiv 1 \mod 4$.*

Vi väntar med beviset och börjar med att titta på ett par exempel. Vi vet att $5 \equiv 1 \mod 4$, och mycket riktigt är 5 en summa av två heltalskvadrater: $5 = 2^2 + 1^2$. Likaså är $13 \equiv 1 \mod 4$, och $13 = 3^2 + 2^2$.

Om $p \equiv 1 \mod 4$, så har vi enligt tvåkvadratsatsen att $p = a^2 + b^2$ för några heltal a och b. I $\mathbb{Z}[i]$ kan högerledet faktoriseras som $a^2 + b^2 = (a + bi)(a - bi)$ varav följer att p inte är ett gaussiskt primtal. Eftersom $N(a + ib) = N(a - ib) = p$, så är talen $a \pm ib$ gaussiska primtal, vilket följer av sats 7.

Vi tittar också på de fall när primtal i $\mathbb{Z}$ inte kan faktoriseras i $\mathbb{Z}[i]$, vilket är de primtal där $p \equiv 3 \mod 4$. Ty antag att $p = zw$, där varken z eller w är en enhet. Då är $p^2 = N(p) = N(z)N(w)$ och eftersom både $N(z)$ och $N(w)$ är > 1, så måste $N(z) = p$. Om $z = a + ib$, så betyder detta att $p = a^2 + b^2$, där $z = a + bi$. Men då ger tvåkvadratsatsen att $p \equiv 1 \mod 4$. Primtal i $\mathbb{Z}$ som är kongurenta med 3 mod 4 är tydligen gaussiska primtal.

Nu har vi bara ett primtal i $\mathbb{Z}$ kvar att studera, nämligen det enda jämna primtalet, 2. Som vi redan sett går det att faktorisera

$$2 = (1 + i)(1 - i)$$

De tre olika typerna av gaussiska primtal som vi har hittat är alltså:

- $a + bi$, där $a, b \in \mathbb{Z}$ och $a^2 + b^2 = p$, där p är ett primtal i $\mathbb{Z}$ som är kongruent med 1 modulo 4
- tal som är associerade med p, där $p \equiv 3 \pmod 4$
- tal som är associerade med 1+i

Kan det finnas fler än dessa tre typer? Vi antar att $z = a + bi$ är av en annan typ. Talet z kan omöjligen vara reellt för då skulle det vara av den andra typen, alltså ett vanligt primtal kongruent med 3 modulo 4. Vi låter p vara ett primtal i $\mathbb{Z}$ som delar $N(z) = z\overline{z}$. Då kan vi skriva $mp = z\overline{z}$ för något m och p är då associerat med $z, \overline{z}$ eller $z\overline{z}$. Om p är associerat med z eller $\overline{z}$, så har vi det andra fallet ovan där $p \equiv 3 \mod 4$. Annars måste $p = N(z) = a^2 + b^2$ och z är alltså av den första typen ovan. Det finns alltså inga ytterligare typer av primtal i $\mathbb{Z}[i]$.

Beviset för tvåkvadratssatsen utförs i flera steg och vi börjar med följande sats:

Sats 11 *Om p är ett udda primtal är kongruensen $x^2 \equiv -1 \mod p$ lösbar om och endast om $p \equiv 1 \mod 4$.*

Bevis
Först antar vi att $p \equiv 1 \mod 4$. Fermats lilla sats säger att $a^{p-1} - 1 \equiv 0 \mod p$, om a och p är relativt prima. Med hjälp av konjugatregeln skriver vi:

$$x^{p-1} - 1 = (x^{(p-1)/2} + 1)(x^{(p-1)/2} - 1)$$

Ett polynom har alltid högst så många nollställen modulo ett primtal p, som sin grad. Alltså har $x^{(p-1)/2}-1$ högst $(p-1)/2$ nollställen modulo p, varav det följer att $x^{(p-1)/2}+1$ har minst 1 nollställe. Vi låter a vara ett nollställe till faktorn

$$x^{(p-1)/2}+1$$

så att

$$a^{(p-1)/2}+1 \equiv 0 \mod p,$$

vilket vi skriver om som

$$(a^{(p-1)/4})(a^{(p-1)/4}) \equiv -1 \mod p.$$

Eftersom $\frac{p-1}{4} \in \mathbb{Z}$ har kongruensen $x^2 \equiv -1 \mod p$ en lösning, nämligen

$$x = a^{(p-1)/4}.$$

Vi går vidare med att bevisa att detta gäller just när $p \equiv 1 \mod 4$. Vi antar att $b^2 \equiv -1 \mod p$. ($x = b$ är här en lösning till vår kongruens). Vi låter m vara det minsta positiva heltalet sådant att $b^m \equiv 1 \mod p$. Exponenten 4 fungerar uppenbarligen, men vi måste utesluta $m = 3$. Om b^3 vore kongruent med 1 mod p skulle vi få:

$$1 \equiv b^3 = b^2 \cdot b = -1 \cdot b = -b$$

vilket skulle ge $b = -1$ och då skulle $b^2 = (-1)^2 = 1$, men det innebär en motsägelse, så m måste vara lika med 4.

Enligt Fermats lilla sats är $b^{p-1} \equiv 1 \mod p$. Vi delar $p-1$ med 4.

$$p - 1 = 4q + r, \text{ där } 0 \leq r < 4$$

$$1 = b^{p-1} = b^{4q+r} = (b^4)^q b^r = b^r$$

Eftersom $1 = b^r$, måste $r = 0$ och vi ser att 4 verkligen delar $p-1$. Nu har vi förutsättningarna klara för att kunna genomföra beviset för tvåkvadratsatsen, som alltså sa att ett udda primtal p kan skrivas som en summa av två heltalskvadrater om och endast om $p \equiv 1 \mod 4$.

Bevis tvåkvadratsatsen
Vi antar att $p \equiv 1 \mod 4$. Ovan kom vi fram till att det finns ett heltal α sådant att $p|\alpha^2+1$. Om vi faktoriserar i $\mathbb{Z}[i]$ innebär det att $p|(\alpha+i)(\alpha-i)$.

Om p vore ett gaussiskt primtal så skulle p dela $\alpha + i$ eller $\alpha - i$. Vi antar att $p|\alpha + i$ och skriver $\alpha + i = pw$, där w är ett gaussiskt primtal. Vi konjugerar båda sidor och får $\alpha - i = \overline{pw}$. Eftersom $p \in \mathbb{Z}$ är $p = \overline{p}$ får vi $\alpha - i = p\overline{w}$. Då måste p även dela differensen: $p|(\alpha + i) - (\alpha - i)$, alltså $p|2i$. Detta innebär att p måste dela 2. Vi skriver $2 = pq$ där $q = x + yi$. Vi tar normen och får $4 = p^2(x^2 + y^2)$, vilket är omöjligt. Primtalet p kan alltså inte vara ett gaussiskt primtal, utan måste kunna faktoriseras i $\mathbb{Z}[i]$ som $p = (a + bi)(c + di)$, där ingen av faktorerna är en enhet.

Vi tittar på normen av p: $N(p) = p^2 = (a^2 + b^2)(c^2 + d^2)$. Eftersom ingen av faktorerna är en enhet har ingen av faktorerna normen 1, vilket innebär att $p = a^2 + b^2 = c^2 + d^2$.

För omvändningen, antag att $p = a^2 + b^2$. Då måste a vara jämnt och b udda, eller tvärtom. Kvadraten på ett jämnt tal är $\equiv 0 \mod 4$ och kvadraten på ett udda tal är $\equiv 1 \mod 4$, vilket innebär att $p \equiv 1 \mod 4$. □

4 Tal i $\mathbb{Z}[\omega]$

I förra avsnittet betraktade vi vilka primtal i $\mathbb{Z}$ som går att faktorisera i $\mathbb{Z}[i]$ och vilka som förblir primtal. Nu inför vi en ny mängd och byter ut i mot ω. I $\mathbb{Z}[i]$ hade vi de gaussiska heltalen $a + bi$. I $\mathbb{Z}[\omega]$ ingår talen $a + b\omega$, där $a, b \in \mathbb{Z}$ och där ω är en rot till ekvationen $z^3 = 1$ och $\omega \neq 1$. Om vi utför polynomdivision med roten $\omega = 1$ får vi en andragradsekvation ur vilken vi kan hitta de resterande rötterna.

$$\frac{z^3 - 1}{z - 1} = z^2 + z + 1$$

De resterande rötterna blir alltså

$$\omega = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$$

Vi kan använda vilken som helst av dem eftersom de är varandras konjugat.

Vi ser också att ω har egenskapen att $\overline{\omega} = \omega^2 = -1 - \omega$.
Vi väljer $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Då är

$$\omega^2 = (-\frac{1}{2} + \frac{i\sqrt{3}}{2})(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = \frac{1}{4} - \frac{i\sqrt{3}}{2} - \frac{i\sqrt{3}}{2} + \frac{i^2 3}{4} = -\frac{1}{2} - \frac{i\sqrt{3}}{2} = \overline{\omega}$$

och

$$-1-\omega = -1-(-\frac{1}{2}+\frac{i\sqrt{3}}{2}) = -\frac{1}{2}-\frac{i\sqrt{3}}{2} = \overline{\omega}$$

När vi nu känner till ovanstående egenskaper, kommer vi i fortsättningen att räkna med ω direkt.

Mängden $\mathbb{Z}[\omega]$ är precis som $\mathbb{Z}[i]$ sluten under addition, subtraktion och multiplikation. Delbarhet, enheter, associerade tal och primtal definieras också som för de gaussiska heltalen. Även normen definieras precis som förut: $N(z) = z\overline{z}$ och det gäller att $N(zw) = N(z)N(w)$. Vi använder oss av att $\omega^2 = \overline{\omega} = -1-\omega$ och räknar ut normen.

$$\begin{aligned} N(z) &= (a+\omega b)(a+\overline{\omega}b) = a^2 + ab(\omega+\overline{\omega}) + b^2\omega\overline{\omega} \\ &= a^2 + (\omega+\omega^2)ab + \omega^2\omega b^2 = a^2 - ab + b^2 \end{aligned}$$

Vi säger att $u = a + b\omega$ är en enhet om det finns ett v så att $u \cdot v = 1$. Vi kan även kalla v för multiplikativ invers till u och skriver då $v = u^{-1}$. Vi tar normen på båda sidor och får

$$N(uu^{-1}) = N(1)$$

$$N(u)N(u^{-1}) = 1^2$$

och ser att normen av en enhet alltid är 1. Vi kan också skriva $N(u) = u\overline{u}$, som vi sett tidigare är $N(u) = a^2 - ab + b^2$ Med hjälp av detta kan vi ta reda på vilka enheterna i $\mathbb{Z}[\omega]$ är.

Vi antar att $z = a + \omega b$ är en enhet, så $a^2 - ab + b^2 = 1$. Vi kvadratkompletterar, men måste tänka på att vi arbetar med heltal och förlänger med 4.

$$(2a-b)^2 + 3b^2 = 4$$

Eftersom a och b är heltal är de enda möjligheterna:

$$\begin{aligned} &a = 1 \text{ och } b = 0 \\ &a = -1 \text{ och } b = 0 \\ &a = 0 \text{ och } b = 1 \\ &a = 0 \text{ och } b = -1 \\ &a = b = 1 \\ &a = b = -1 \end{aligned}$$

Alltså finns det sex stycken enheter, nämligen $\pm 1, \pm\omega, \pm(1+\omega)$. Vi kan också observera att $\pm(1+\omega) = \pm\omega^2$.

4.1 Division

Divisionsalgoritmen ser likadan ut som i $\mathbb{Z}[i]$, det enda som skiljer är hur talen vi räknar med ser ut. Liksom i $\mathbb{Z}[i]$ multiplicerar vi med nämnarens konjugat för att få tal i $\mathbb{Z}$ i nämnaren.

Sats 12 (Divisionsalgoritmen) *Låt $z, u \in \mathbb{Z}[\omega]$, $z \neq 0$. Då finns $q, r \in \mathbb{Z}[\omega]$ sådana att $u = qz + r$ och N(r)<N(z).*

Bevis
Antag att $z = a + b\omega, u = c + d\omega$. Division ger

$$\frac{u}{z} = \frac{c+d\omega}{a+b\omega} = \frac{(c+d\omega)(a+b\overline{\omega})}{(a+b\omega)(a+b\overline{\omega})} = \frac{ac+bd-bc+(ad-bc)\omega}{a^2-ab+b^2}$$

Vi ser att det finns rationella tal x, y sådana att $\dfrac{u}{z} = x + y\omega$. Vi väljer nu heltal α, β sådana att $|x-\alpha| \leq 1/2$ och $|y-\beta| \leq 1/2$ och skriver:

$$u = z(x+y\omega) = z(\alpha+\beta\omega) + z((x-\alpha)+(y-\beta)\omega) = qz + r$$

Då är

$$\begin{aligned} N(r) &= N(z((x-\alpha)+(y-\beta)\omega)) \\ &= N(z)((x-\alpha)^2 - (x-\alpha)(y-\beta) + (y-\beta)^2) \\ &\leq N(z)(1/4+1/4+1/4) < N(z). \end{aligned}$$

□

I $\mathbb{Z}[i]$ såg vi att om normen av ett gaussiskt heltal var ett primtal, var det gaussiska heltalet ett gaussiskt primtal. Detta kan generaliseras i $\mathbb{Z}[\omega]$. För talet $z \in \mathbb{Z}[\omega]$ gäller att om $N(z)$ är ett primtal måste även z vara ett primtal.

Exempel
Med $z = 1-\omega$, så är $N(z) = 3$ eftersom

$$\begin{aligned} N(1-\omega) = (1-\omega)(1-\overline{\omega}) &= 1 - (\omega+\overline{\omega}) + \omega\overline{\omega} = \\ &= 1 - (\omega+\omega^2) + |\omega|^2 = 1 - (-1) + 1 = 3 \end{aligned}$$

och således är $z = 1-\omega$ ett primtal.

Euklides algoritm fungerar som i $\mathbb{Z}$ och $\mathbb{Z}[i]$. Vi får fram största gemensamma delare och Bezouts sats gäller.

4.2 Primtal och entydig faktorisering

Vi ska nu reda ut vilka vanliga primtal, p, som går att faktorisera i $\mathbb{Z}[\omega]$. Vi har redan undersökt talet 3 så nu tittar vi på primtal $\neq 3$. Då måste p vara kongurent med 1 eller 2 modulo 3.

Vi vill visa att p kan skrivas på formen $p = a^2 - ab + b^2$ om och endast om $p \equiv 1 \mod 3$. Endast om är enkelt:

$$a^2 - ab + b^2 \equiv a^2 - ab + b^2 + 3ab \equiv a^2 + 2ab + b^2 \equiv (a + b)^2$$

Vi vet att en kvadrat $\equiv 0$ eller $1 \mod 3$, så p kan inte vara kongurent med 2.

För att bevisa Fermats tvåkvadratsats skulle kongurensen $x^2 \equiv -1 \mod p$ visas vara lösbar. Här är motsvarigheten att visa att kongurensen $x^2 \equiv -3$ mod p är lösbar, om och endast om $p \equiv 1 \mod 3$. Först visar vi att om $p > 3$ och $x^2 \equiv -3 \mod p$ är lösbar, så är $p = a^2 - ab + b^2$.

Antag att $a^2 \equiv -3 \mod p$, vilket innebär att $p|a^2 + 3$ (p delar alltså ett tal i $\mathbb{Z}$). Som vi sett tidigare är $3 = (1 - \omega)(1 - \omega^2)$ vilket är lika med $-\omega^2(1 - \omega)^2$ och eftersom $\omega^3 = 1$ och $\omega^2 + \omega + 1 = 0$ blir

$$\omega^2(1-\omega)^2 = \omega^2(1-2\omega+\omega^2) = \omega^2-2\omega^3+\omega^4 = \omega^2-2+\omega = \omega^2+\omega+1-3 = -3$$

Nu ska vi kontrollera om p är ett primtal i $\mathbb{Z}[\omega]$. Vi skriver

$$a^2 + 3 = a^2 - \omega^2(1 - \omega)^2 = (a + \omega(1 - \omega))(a - \omega(1 - \omega)).$$

Om p vore ett primtal i $\mathbb{Z}[\omega]$ skulle det dela en av faktorerna, till exempel $p|(a+\omega(1-\omega))$, eftersom $\overline{\omega(1-\omega)} = \overline{\omega - \omega^2} = \omega^2 - \omega = -\omega(1-\omega.)$ Därför ger konjugering att $p|(a - \omega(1 - \omega))$. Om vi nu adderar $a + \omega(1 - \omega)$ och $a-\omega(1-\omega)$ får vi att $p|2a$ och tar vi sedan normen får vi $p^2|4a^2$. Det innebär att p antingen delar 2 eller delar p talet a. Eftersom vi i början antog att $p > 3$, kan p inte dela 2. Inte heller kan p dela a eftersom p också måste dela $a^2 + 3$ enligt vårt antagande och då måste p även dela 3. Därför kan inte p vara ett primtal i $\mathbb{Z}[\omega]$, så vi skriver att $p = (a + b\omega)(c + d\omega)$ där ingen av faktorerna är en enhet. Om vi nu tar normen får vi $p^2 = N(a+b\omega)N(c+d\omega)$. Eftersom vi har en likhet i $\mathbb{Z}$ måste $p = N(a + b\omega)$, vilken vi tidigare sett är lika med $a^2 - ab + b^2$. Det är alltså de primtal som är kongurenta med 1 modulo 3 som kan faktoriseras i $\mathbb{Z}[\omega]$, alltså de tal som går att skriva på formen $p = a^2 - ab + b^2$. [4]

Sats 13 (Aritmetikens fundamentalsats) *Varje tal $z \in \mathbb{Z}[\omega]$ med $N(z) > 1$ kan faktoriseras i $\pi_1\pi_2....\pi_n$ där varje π är ett primtal. Denna representation är unik med undantag för ordningen av primtalen och variationer mellan associerade primtal.*

Bevis
Liksom i $\mathbb{Z}$ och i $\mathbb{Z}[i]$ vill vi visa att det går att faktorisera varje $z \in \mathbb{Z}[\omega]$ vars norm är större än 1 i primtal. Antingen är z=π_1, där π_1 är ett primtal och faktoriseringen är redan klar. Om a inte är ett primtal delar vi a med primtalet π_1 och skriver $z = \pi_1\delta_1$. Om δ_1 är ett primtal är vi klara annars fortsätter vi så att $z = \pi_1\pi_2...\delta_n$. Eftersom $N(z) > N(\delta_1) > ... > N(\delta_n)$ kommer vi så småningom fram till ett $\delta_n = 1$ och primfaktoriseringen är klar.

Entydighet visas genom induktion på $N(z)$. Vi vet att vi kan faktorisera ett tal z med norm 3 entydigt, eftersom 3 är ett primtal i $\mathbb{Z}$ och då vet vi att z är ett primtal i $\mathbb{Z}[\omega]$ och z har en trivialt unik faktorisering. Antag nu att det finns heltal i $\mathbb{Z}[\omega]$ som inte har unik primfaktorisering och låt z vara ett sådant tal med minmal norm. Vi har i så fall två faktoriseringar $z = \pi_1...\pi_r = q_1...q_s$, där alla faktorer är primtal i $\mathbb{Z}[\omega]$. Primtalet π_1 delar $q_1...q_s$ och vi visade i $\mathbb{Z}$ och $\mathbb{Z}[i]$ att π_1 då måste då dela någon av faktorerna, vilket genraliseras här. Vi numrerar om faktorerna och antar att $\pi_1|q_1$. Men båda talen är primtal, så de måste vara associerade, säg att $q_1 = u\pi_1$, där u är en enhet. Då får vi $w = \frac{z}{\pi_1} = \pi_2...\pi_r = uq_2...q_s = q_2'q_3...q_s$, där $q_2' = uq_2$ också är ett primtal. Talet w har mindre norm än z och har därför unik primfaktorisering. Alltså är $r = s$ och efter en eventuell omnumrering är π_i och q_i associerade för $i = 2, ..., r$. Således har även z en unik primfaktorisering.□

4.3 Kvadratiska rester

Ett primtal $p \neq 3$ är kongruent med antingen 1 eller 2 modulo 3. Nu ska vi visa att om $p \equiv 1 \mod 3$, så är kongruensen $x^2 \equiv -3 \mod p$ lösbar. Vi börjar med att betrakta kongruensen $x^2 \equiv a \mod p$ för a som inte är delbart med p. Ett tal a som innebär att kongruensen är lösbar kallas kvadratisk rest modulo p. Om ett tal a innebär att kongruensen inte är lösbar kallas a en kvadratisk icke-rest. Om a är en kvadratisk rest så har $x^2 \equiv a \mod p$ två lösningar:

$$x_1 = u$$
$$x_2 = -u = p - u \mod p$$

Dessa två lösningar måste vara olika modulo p eftersom annars skulle

$u \equiv p-u$ och därmed $2u \equiv 0 \mod p$. Detta ger att $p|u$, därmed delar även p talet u^2 och eftersom $u^2 \equiv a \mod p$ skulle p även dela a, vilket är omöjligt eftersom det strider mot de givna förutsättningarna.

Vi betraktar alla tal $1, 2, ..., p-1$ och ser att hälften, det vill säga $(p-1)/2$ stycken är kvadratiska rester och lika många är icke-kvadratiska rester.

Exempel
För att få en kvadratisk rest skulle $x^2 \equiv a \mod p$ vara lösbar och vi ser att för $p = 11$ är

$$1^2 \equiv 10^2 \equiv 1$$
$$2^2 \equiv 9^2 \equiv 4$$
$$3^2 \equiv 8^2 \equiv 9$$
$$4^2 \equiv 7^2 \equiv 5$$
$$5^2 \equiv 6^2 \equiv 3$$

Vi ser att för ett primtal p och $1 \leq n \leq p-1$ är

$$n^2 \equiv (p-n)^2 \mod p$$

Om vi nu tittar på alla tal mellan 1 och $p-1 = 10$ ser vi att de tal som kan skrivas som kvadrater modulo 11 är $1, 3, 4, 5, 9$. De tal som är icke-kvadratiska rester är således: $2, 6, 7, 8$ och 10. Eftersom $n^2 = (p-1)^2$ ser vi att endast hälften av alla n ger olika kvadratiska rester modulo p.

Enligt Fermats lilla sats är alla tal $1, 2, ..., p-1$ nollställen modulo p till polynomet $x^{p-1} - 1$. Vi faktoriserar det som

$$x^{p-1} - 1 = (x^{(p-1)/2} + 1)(x^{(p-1)/2} - 1)$$

Nu låter vi a vara en kvadratisk rest modulo p, vi säger att $a \equiv u^2 \mod p$. Då är

$$a^{(p-1)/2} - 1 = (u^2)^{(p-1)/2} - 1 = u^{(p-1)} - 1 \equiv 0 \mod p.$$

Alla kvadratiska rester är således nollställen till $x^{(p-1)/2} - 1$. Eftersom deras antal är lika med graden $(p-1)/2$ utgör de samtliga nollställen. Till faktorn $(x^{(p-1)/2} + 1)$ är det således de kvadratiska icke-resterna som utgör samtliga nollställen.

- a är en kvadratisk rest modulo p om och endast om $a^{(p-1)/2} \equiv 1 \mod p$
- a är en kvadratisk icke-rest modulo p om och endast om $a^{(p-1)/2} \equiv -1 \mod p$.

Vi tittar nu på talen $a{\cdot}1, a{\cdot}2, ..., a{\cdot}(p-1)/2$. Vi dividerar dem med p och väljer de absolut minsta resterna, alltså de rester som ligger närmast 0 på tallinjen, vilket ger att resterna är tal mellan $-p/2$ och $p/2$. Vi säger att $r_1, ...r_\mu$ är de positiva resterna och att $-s_1, ..., -s_\nu$ är de negativa resterna. (Observera att s_i är positiv.) Antalet rester är $(p-1)/2$, det vill säga $\mu + \nu = (p-1)/2$. Alla r är olika, liksom alla s. Om två r vore lika skulle $ai \equiv aj \mod p$ för några $i \neq j$, så $p|a(i-j)$. Eftersom p inte delar a, så $p|i-j$ och eftersom i och j ligger mellan 1 och $(p-1)/2$, så måste $i - j = 0$. På samma sätt ser vi att alla s är olika. Skulle r_i kunna vara lika med s_j? I så fall skulle $ak \equiv -al \mod p$ för några k och l. Men i så fall skulle $p|a(k+l)$ och $p|(k+l)$. Eftersom $0 < k+l \leq \mu + \nu = (p-1)/2$ så ser vi att detta är omöjligt. Alltså är alla talen r_i, s_j olika. Eftersom antalet rester är $(p-1)/2$ stycken måste r_i, s_j utgöra alla talen $1, 2..., (p-1)/2$. Därmed kan vi säga att r_i, s_j är en permutation av $1, 2, ..., (p-1)/2$. Vi multiplicerar ihop alla r_i, s_j. Då är

$$r_1 \cdot ... \cdot r_\mu \cdot s_1 \cdot ... \cdot s_\nu = 1 \cdot 2 \cdot ... \cdot (p-1)/2 = ((p-1)/2)!$$

Detta kan vi skriva eftersom vi vet att alla r_i, s_j är olika och att antalet är $(p-1)/2$.
Vi kan också skriva

$$\begin{aligned} r_1 \cdot ... \cdot r_\mu \cdot s_1 \cdot ... \cdot s_\nu &= (-1)^\nu r_1 \cdot ... \cdot r_\nu \cdot (-s_1) \cdot ... \cdot (-s_\nu) \\ &\equiv (-1)^\nu (a \cdot 1 \cdot ... \cdot a \cdot (p-1)/2)) \\ &\equiv (-1)^\nu a^{(p-1)/2} ((p-1)/2)! \mod p \end{aligned}$$

Därmed kan vi skriva $(-1)^\nu a^{(p-1)/2}((p-1)/2)! \equiv ((p-1)/2)! \mod p$
Vi dividerar med $(p-1)/2)!$ (vilket vi kan göra eftersom $(p-1)/2$ inte är delbart med p) och får

$$(-1)^\nu a^{(p-1)/2} \equiv 1 \mod p$$

vilket vi inser är samma sak som

$$a^{(p-1)/2} \equiv (-1)^\nu \mod p.$$

Denna kongruens brukar kallas Gauss lemma och används när kvadratiska rester studeras. Vi vet sedan tidigare att

- a är en kvadratisk rest modulo $p \Leftrightarrow a^{(p-1)/2} \equiv 1 \mod p$

- a är en kvadratisk icke-rest modulo $p \Leftrightarrow a^{(p-1)/2} \equiv -1 \mod p$

Därmed kan vi slå fast att

- a är en kvadratisk rest modulo p om ν är jämnt

- a är en kvadratisk icke-rest modulo p om ν är udda.

För att avgöra om ett tal a är en kvadratisk rest eller ej, behöver vi alltså undersöka hur många av de absolut minsta resterna som är negativa. Vi börjar med att undersöka $a = -1$, vilket är ett exempel på Gauss lemma och är en uppvärmning inför fallet (-3) som är det vi egentligen behöver. För $a = -1$ har vi talen $-1 \cdot 1, -1 \cdot 2, ..., -1((p-1)/2)$, vilka alla redan ligger i området mellan $-(p/2)$ och $p/2$ och alltså redan är sina egna absolut minsta rester. Därmed ser vi att antalet negativa rester är $(p-1)/2$ och vi får att -1 är en kvadratisk rest om $(p-1)/2$ är jämnt, vilket inträffar när $p \equiv 1 \mod 4$.

Lite mer omständligt är det att undersöka fallet $a = -3$. Vi undersöker nu talen $-3 \cdot 1, -3 \cdot 2, -3 \cdot ..., -3 \cdot ((p-1)/2)$. Vi skriver detta istället som $-3 \cdot k$ där $1 \leq k \leq (p-1)/2$. De tal som är större än $-p/2$ är redan sina egna absolut minsta rester. De talen får vi när $k < p/6$. Det finns $[p/6]$ sådana tal. Vi går vidare och tittar på olikheten $-p < -3k < -p/2$. Vi adderar p och får den ekvivalenta olikheten $0 < -3k + p < p/2$. Vi ser alltså att den absolut minsta resten kommer att bli positiv. För att få den absolut minsta resten måste vi dividera med p. Med hjälp av divisionsalgoritmen skriver vi: $-3k = (-1)p + (-3k + p)$, där -1 är vår kvot och $(-3k + p)$ är vår rest. Att denna rest måste vara positiv har vi redan konstaterat. Vi går vidare med vårt sista intervall som måste undersökas, $\frac{-3p}{2} < -3k < -p$. Vi adderar p och får olikheten $\frac{-3p}{2} + p < -3k + p < 0$, vilket är ekvivalent med $\frac{-p}{2} < -3k + p < 0$, följaktligen kommer våra absolut minsta rester att vara negativa. Vilka k är det som uppfyller det här? Vi delar med -3 och får den ekvivalenta olikheten $\frac{p}{3} < k < \frac{p}{2}$. Här är resterna redan sina egna

absolut minsta rester. Antalet måste vara $[\frac{p}{2}] - [\frac{p}{3}]$. Talet $[\frac{p}{2}]$ kan vi skriva om som närmsta mindre heltal som $\frac{p-1}{2}$. Det totala antalet negativa rester blir alltså sammanlagt:

$$[\frac{p}{6}] + \frac{p-1}{2} - [\frac{p}{3}] = \nu$$

Nu måste vi också kontrollera de olika fallen när $p \equiv 1 \mod 3$ och när $p \equiv 2 \mod 3$. Vi tittar först på fallet när $p \equiv 1 \mod 3$. Eftersom p är udda, så är $p-1$ jämnt. Vi vet att $p-1$ är delbart med 3 och eftersom det är jämnt är det även delbart med 2. Alltså är det delbart med 6. Vi skriver $p = 6m+1$. När vi sätter in detta i vårt uttryck för ν ovan får vi:

$$\nu = [m + \frac{1}{6}] + 3m - [2m + \frac{1}{3}]$$

vilket i heltal motsvarar

$$\nu = m + 3m - 2m = 2m$$

ν är alltså jämnt och a har visat sig vara en kvadratisk rest.

I fallet när $p \equiv 2 \mod 3$, kan vi lika väl skriva $p \equiv -1 \mod 3$. Då är $p+1$ jämnt och delbart med 6. Om vi skriver $p = 6m-1$, så får vi

$$\nu = [m - \frac{1}{6}] + 3m - 1 - [2m - \frac{1}{3}]$$

och omskrivet till heltal får vi

$$\nu = (m-1) + 3m - 1 - (2m-1) = 2m - 1$$

vilket ger oss en kvadratisk icke-rest. Således har vi rett ut när ett tal a är en kvadratisk rest eller inte. [4]

4.4 Vilka är primtalen?

Nu ska vi undersöka vilka primtalen i $\mathbb{Z}[\omega]$ är. Om q är ett primtal i $\mathbb{Z}$ sådant att $q \equiv 2 \mod 3$, så är q ett primtal i $\mathbb{Z}[\omega]$. Vi tar ett primtal $q \equiv 2 \mod 3$ och antar att $q = (a+b\omega)(c+d\omega)$, där ingen av faktorerna är en enhet. Sedan tar vi normen: $q^2 = N(a+b\omega)N(c+d\omega)$. Eftersom ingen av faktorerna i högerledet är 1, så måste $q = N(a+b\omega) = a^2 - ab + b^2$, vilket vi tidgare sett är omöjligt och q måste alltså vara ett primtal i $\mathbb{Z}[\omega]$.

Nu låter vi p vara ett primtal > 3 som är $\equiv 1 \mod 3$ och vi skriver $p = a^2 - ab + b^2 = (a + b\omega)(a + b\omega^2)$. Då är $a + b\omega$ och $a + b\omega^2$ primtal i $\mathbb{Z}[\omega]$. För om vi skulle kunna skriva $a + b\omega = zu$, så vore $p = N(a + b\omega) = N(z)N(u)$, vilket innebär att antingen z eller u är en enhet.

Vi undersöker nu talet 3, som kan faktoriseras som $3 = -\omega^2(1 - \omega)^2$, vilket innebär att 3 är en enhet multiplicerat med en kvadrat. Vi kan jämföra med 2 som i $\mathbb{Z}[i]$ kan faktoriseras som $(1 - i)(1 + i) = i(1 - i)^2$.

Alla tal som är associerade med de primtal vi hittat är förstås också primtal. Kan det finnas fler? Vi låter $z = a + b\omega$ vara ett godtyckligt primtal i $\mathbb{Z}[\omega]$. Om $b = 0$, så är a ett primtal i $\mathbb{Z}$. Om $a \equiv 1 \pmod 3$, så är a inte ett primtal i $\mathbb{Z}[\omega]$. Alltså är $a \equiv 2 \pmod 3$, vilket är en av de typer av primtal som vi redan har hittat. Antag alltså att $b \neq 0$ och låt p vara ett primtal i $\mathbb{Z}$ som delar $N(a + b\omega)$, det vill säga $p | (a + b\omega)(a + b\omega^2)$. Om $p \equiv 2 \pmod 3$, så är p ett primtal i $\mathbb{Z}[\omega]$ och skulle därför vara associerat till någon av faktorerna exempelvis till $a + b\omega$, säg $p = u(a + b\omega)$, vilket är en av de typer vi hittat tidigare.

Vi tittar slutligen på fallet då $p \equiv 1 \mod 3$ och $p | (\alpha + \beta\omega)(\alpha + \beta\omega^2)$. Vi faktoriserar $p = (a + b\omega)(a + b\omega^2)$ och ser att $\alpha + \beta\omega$ eller $\alpha + \beta\omega^2$ är associerat med $a + b\omega$, vilket också är en av de typer vi har hittat tidigare. Vi har alltså hittat alla primtal i $\mathbb{Z}[\omega]$.

Referenser

[1] Keith Conrad, *The Gaussian Integers.* http://www.math.uconn.edu/ ∼kconrad/blurbs/ugradnumthy/Zinotes.pdf (hämtad 2016-02-20).

[2] Lars Gårding Torbjörn Tambour, *Algebra for Computer Science.* New York: Springer-Verlag, 1988.

[3] G. H. Hardy & E. M. Wright, *An Introduction to the theory of numbers.* Oxford: At the Clarendon Press, 1954.

[4] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory.* New-York: Springer-Verlag, 1990.

[5] Dirk J. Struik, *A Concise History of Mathematics.* New York: Dover, 1987.