SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Gaussiska heltal, entydig faktorisering och tvåkvadratsatsen

av

Katayoon Khosraviani

2020 - No K28

Gaussiska heltal, entydig faktorisering och tvåkvadratsatsen

Katayoon Khosraviani

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2020

Sammanfattning

I detta arbete visas att ringen av Gaussiska heltal har entydig faktorisering, genom att först ge bevis på att en större klass av ringar kallade Euklidiska ringar har unik faktorisering i primtalsfaktorer, och sedan visas både algebraiskt och geometriskt att ringen av Gaussiska heltal är Euklidisk. Vi undersöker även hur primtalselement bland Gaussiska heltal kan beskrivas, och vidare visar vi Fermats tvåkvadratsats som en följdsats av satsen om entydigt faktorisering för Gaussiska heltal.

Abstract

This paper aims to demonstrate that the ring av Gaussisan integers is uniq factorisation, by provide first evidence on that a larger class of rings, namely Euclidean rings are unique factorization rings, and than Gaussian integer is Euclidean. Further investigations focused to understand how prime elements can be clarified among Gaussian integers. Likewise, the result of the effort provided evidences on Fermats sum of two square theorem as a consequence of the theorem of unique factorization for Gaussian integer.

Innehåll

1 Introduktion **4**

2 Historia **5**

3 Ringar **5**

4 Kroppar **10**

5 Euklidiska ringar och entydig faktorisering **11**

6 Gaussiska heltal **16**

7 Tvåkvadratsatsen **22**

8 Gaussiska primtal **24**

9 Faktorisering av Gaussiska heltal **27**

1 Introduktion

Uppsatsen inleds med en introduktion till några av de mest grundläggande begreppen som studeras inom den abstrakt algebran, nämligen ringar och kroppar. Kortfattat kan man säga att en ring är en mängd som är sluten med avseende på addition, och multiplikation. I detta arbete antas alla ringar vara kommutativa ringar med etta (om inget annat anges). En kommutativ ring med ett enhetselement, där varje nollskilt element är inverterbart är en kropp. Mängderna av komplexa tal respektive reella tal är två kroppar som vi känner till sedan länge, men det finns många andra kroppar till exempel ändliga kroppar, kroppar med ändligt många element. Vi kommer att undersöka när mängden $\mathbb{Z}_n$, den kommutativa ringen med etta av heltalen modulo ett heltal n är en kropp. Ett sätt att konstruera kroppar är att utvidga redan kända kroppar. Till exempel den kvadratiska talkroppen $\mathbb{Q}(\sqrt{m})$ är en kroppsutvidgning av $\mathbb{Q}$, som fås genom att lägga till roten ur ett kvadratfritt heltal $m \neq 1$. Ett kvadratfritt heltal är ett heltal som inte är delbart med kvadraten på något primtal.

Det är välkänt att ringen av heltal har entydig faktorisering, varje positivt heltal kan skrivas entydigt, upp till ordning, som en produkt av primtal. Vi ska undersöka om en större klass av ringar, kallade Euklidiska ringar, också har entydig faktorisering. Vi kommer att bevisa ett antal satser i referensboken [1], för att sedan visa att ringen av Gaussiska heltal, tal på formen $a + bi$ där a och b är vanliga heltal, är Euklidisk. Det senare visas både algebraiskt, enligt [1], och genom ett geometriskt bevis.

Vissa heltal k kan skrivas som $k = x^2 + y^2$, summan av två heltalskvadrater. Till exempel talen $1, 2, 4, 5, 8, 9$ och 10 är heltalen mellan $1 \leq k \leq 10$ som kan skrivas som summan av två kvadrater. Här finns inget uppenbart mönster, förutom kanske att vi undviker tal på formen $4n + 3$. Vi kan även konstatera att av alla primtal i samma intervall är det bara 2 och 5 som kan skrivas som summan av två heltalkvadrater. Detta är vad Fermats tvåkvadratsats handlar om. Enligt Fermats tvåkvadratsats kan ett udda primtal skrivas som summan av två heltalskvadrater, om och endast om p är kongruent 1 mod 4. Vi kommer att använda satsen om entydig faktorisering för Gaussiska heltal för att bevisa Fermats tvåkvadratsats.

Ett Gaussiskt heltal z är ett Gaussiskt primtal om $z = \alpha\beta$ medför att exakt en av α eller β är $+1, -1, i, -i$. Vi kommer att undersöka närmare hur man kan hitta Gaussiska primtal. Slutligen visar vi hur man primtalfaktoriserar ett givet Gaussiskt heltal.

I denna uppsats används främst tre referenser,[1], [2], och [3]. Varje avsnitt följs av relevanta exempel.

2 Historia

Ordet algebra sträcker sig så långt tillbacka i tiden som ungefär 1200 år sedan till Al-Khwarizms (c.780-c.850) bok om ämnet "ALGEBER". Ämnet i sig användes av de tidiga civilisationernas folk, Babylonier och Egypten för 4000 år sedan i det dagliga livet för att lösa numeriska problem som vi nu skulle identifiera som linjära och kvadratiska ekvationer. Dock visade sig att lösningar till ekvationer av högre grader länge skulle förbli ett bekymmer för matematiker.

I slutet av 1800-talet och början av 1900-talet genomgick matematiken enorma förändringar. Abstrakt algebra uppstod omkring början av 1900-talet under namnet modern algebra. Ursprungligen tog antagandena i klassisk algebra, som hela matematiken och stora delar av naturvetenskapen beror på, form av axiomatiska system [6]. Matematikerna började inte längre nöja sig med att fastställa egenskaper hos konkreta föremål utan började rikta uppmärksamheten mot allmänna teorier. Formella definitioner av vissa algebraiska strukturer började dyka upp på 1800-talet. Frågor om struktur och klassificering av olika matematiska objekt kom i fokus inom hela matematiken, men blev särskilt uttalade i algebra.

Intresset i abstrakt algebra gällde främst strukturen som helhet snarare än att göra beräkningar inom den strukturen. Några av dessa strukturer är ringar och kroppar.

3 Ringar

En av de grundläggande strukturer som används i abstrakt algebra är ringar. Konceptualiseringen av ringar började på 1870-talet och slutfördes på 1920-talet. Viktiga bidragsgivare inkluderar Richard Dedekind (1831-1916), David Hillbert (1862-1943), Adolf Frankel (1891-1965) och Emmy Noether (1892-1935)[5].

En ring R kan vi definiera som följer.

Definition 3.1. En kommutativ ring med etta är en mängd R med två binära operationerna $\cdot$ och $+$, kallade multiplikation respektive addition, och med följande egenskaper:

Den är associativ vid addition. För alla $a, b, c \in R$ gäller att

$$a + (b + c) = (a + b) + c.$$

Den är kommutativ vid addition. För alla a och $b \in R$ gäller att

$$a + b = b + a.$$

Det finns ett neutral element $0 \in R$ vid addition så att för alla $a \in R$ så att

$$a + 0 = 0 + a = a,$$

och för varje element $a \in R$ finns ett additiv invers element $-a \in R$ så att

$$a + (-a) = (-a) + a = 0.$$

Distributiva lagar gäller, så att

$$a(b + c) = ab + ac, (a + b)c = ac + bc \quad \text{för alla } a, b, c \in R$$

Den är associativ vid multiplikation. För alla $a, b, c \in R$ gäller att

$$(ab)c = a(bc).$$

Den är kommutativ vid multiplikation. För alla $a, b \in R$ gäller att

$$ab = ba.$$

För all element $a \in R$ finns ett neutralt element 1 vid multiplikation så att

$$1 \cdot a = a \cdot 1.$$

Exempel 3.2. Ett exempel på en ring är mängden av heltalen, $\mathbb{Z}$ tillsammans med de två binära operationerna addition och multiplikation.

Exempel 3.3. Vi ska undersöka om mängden $\mathbb{Z}[\sqrt{2}]:=\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ är en kommutativ ring. Vi börjar med att visa att delmängden $\mathbb{Z}[\sqrt{2}]$ av $\mathbb{R}$ är sluten under addition och multiplikation.

För alla a, b och c i $\mathbb{Z}$ gäller att,

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

och $a + c$ och $b + d$ är heltal så $(a + b\sqrt{2}) + (c + d\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$, så mängden $\mathbb{Z}[\sqrt{2}]$ är sluten under addition.

Det gäller för alla a, b och c i $\mathbb{Z}$ så att,

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}),$$

och av den orsaken att $(ac + 2bd)$ och $(ad + bc)$ är heltal så är även $(a + b\sqrt{2})(c + d\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$, så är mängden $\mathbb{Z}[\sqrt{2}]$ sluten också under multiplikation.

För alla element $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ finns additiv invers, eftersom

$$(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0.$$

Eftersom delmängden $\mathbb{Z}[\sqrt{2}]$ är en delringen av de reella talen, så alla egenskaper för en ring enligt definition 3.1 är uppfyllda. Därmed mängden $\mathbb{Z}[\sqrt{2}]$ är en kommutativ ring.

Nu skall vi undersöka om ringen Z_n, heltal modulo en heltal n är en kommutativ ring. Först några viktiga begrepp.

Kongruens började användas systematiskt av den framstående tyska matematikern Carl Fredrich Gauss (1777-1855). Sedan dess har det spelat en viktig roll i talteori, och även modern algebra. Innan vi definierar kongruens behöver vi erinra oss begreppet delbarhet[1].

Definition 3.4. Ett heltal m är delbart med ett heltal n om det finns ett heltal k så att $m = nk$. Då säger vi att n delar m eller att n är delare till m, och skriver $n \mid m$.

Varje heltal m är delbart med $\pm m$ och ± 1. Dessa delare kallas triviala. Delbarhet har många egenskaper, nedan bevisar vi en av dessa egenskaper.

Om $n \mid m$ och $n \mid b$ så gäller att $n \mid (a + b)$. Detta bevisar vi så att eftersom n delar både m och n så har vi att $a = nk_1$ och $b = nk_2$ för två heltal k_1 och k_2. Vi får då att $(a + b) = n(k_1 + k_2)$, eftersom k_1 och k_2 är heltal, är även summan av $k_1 + k_2$ är heltal, vilket leder till att $n \mid (a + b)$. På samma sätt kan vi visa att om $n \mid a$ och $b \in \mathbb{Z}$, så följer det att $n \mid ab$, ty produkten av två heltal är ett heltal.

Med hjälp av begreppet delbarhet definiera vi nu begreppet kongruens.

Definition 3.5. Låt n vara ett positivt heltal. Heltalen a och b säges vara kongruent modulo n om $a - b$ är delbart med n. Vi skriver $a \equiv b \pmod{n}$.

Mängden av heltal a som är kongruent med ett givet tal b modulo n kallas för en kongurensklass eller restklass modulo n med representanten b och skrivs $[b]_n$. I detta arbete skriver vi inga index, när det framgår klart vad n är.

Exempel 3.6. Kongurensklassen modulo 10 med representanten 7 är,

$$[7]_{10} = \{\ldots, -13, -3, 7, 17, 27, \ldots\}.$$

Exempel 3.7. Kongurensklassen modulo 10 med representanten -7 är,

$$[-7]_{10} = \{\ldots, -27, -17, -7, 3, 13, \ldots\}.$$

Om n är ett positivt heltal, då är varje heltal kongruent modulo n exakt ett av heltalen $0, 1, \ldots, (n - 1)$.

Vi definiera $\mathbb{Z}_n$ som en mängd bestående av restklasserna modulo n, det vill säga,

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n - 1]_n\}.$$

Vi kan definiera två binära operationer $+$ och $\cdot$ på $\mathbb{Z}_n$ som vanliga addition och multiplikation genom:

$$[x] + [y] := [x + y],$$

och

$$[x] \cdot [y] := [x \cdot y].$$

Enligt kongruenslagarna, se [3], gäller att om $x \equiv x_1 \pmod{n}$ och $y \equiv y_1 \pmod{n}$, så är $x + y \equiv x_1 + y_1 \pmod{n}$ och $xy \equiv x_1 y_1 \pmod{n}$. Av den anledning är dessa operationer väldefinierade.

Så $\mathbb{Z}_n$ uppfyller följande egenskaper:

Associativa lagar gäller för alla $[x], [y], [z] \in \mathbb{Z}_n$

$$[x] + ([y] + [z]) = [x] + [y + z] =$$

$$= [x + (y + z)] = [(x + y) + z] =$$

$$= [x + y] + [z] = ([x] + [y]) + [z]$$

och på motsvarande sätt fås

$$[x] \cdot ([y] \cdot [z]) = ([x] \cdot [y]) \cdot [z].$$

Det finns ett neutral element $[0] \in \mathbb{Z}_n$ vid addition så att för alla $[x] \in \mathbb{Z}_n$ gäller att

$$[x] + [0] = [0] + [x] = [x].$$

För alla $[x]$ i $\mathbb{Z}_n$ existera ett additiv invers $[-x] \in \mathbb{Z}_n$ som uppfyller att

$$[x] + [-x] = [-x] + [x] = [0].$$

Det existera ett neutral element $[1] \in \mathbb{Z}_n$ vid multiplikation, sådant att för alla $[x] \in \mathbb{Z}_n$ gäller att

$$[x] \cdot [1] = [1] \cdot [x] = [x].$$

Kommutativa lagar vid addition och multiplikation gäller för alla $[x], [y], [z] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] = [y + x] = [y] + [x]$$

och

$$[x] \cdot [y] = [x \cdot y] = [y \cdot x] = [y] \cdot [x].$$

Distributiva lagar gäller för alla $[x], [y], [z] \in \mathbb{Z}_n$,

$$[x] \cdot [y + z] = [x \cdot y] + [x \cdot z]$$

och

$$[y] + [z] \cdot [x] = [y] \cdot [x] + [z] \cdot [x].$$

Vi fortsätter med flera användbara definitioner.

Definition 3.8. Ett positivt heltal $n > 1$ kallas sammansatt, om det är en produkt $n = ab$ av två positiva heltal $a, b > 1$. Om $n > 1$ inte är sammansatt, kallas det för ett primtal [3].

Vi kan säga att ett heltal p är ett primtal i $\mathbb{Z}$ om $p > 1$ och p är enbart delbart med ± 1, eller $\pm p$.

Definition 3.9. Ett element $a \neq 0$ i en kommutativ ring R kallas nolldelare i R om det finns ett element $b \neq 0$ i R så att $a \cdot b = 0$.

Observera att definitionen begränsas till elementen i en kommutativ ring, vad kan vi säga om nolldelare i en icke kommutativ ring? I en icke kommutativ ring skiljer man på vänsternolldelare och högernolldelare, som vi tänker inte tar upp i denna uppsats.

Definition 3.10. En kommutativ ring som saknar nolldelare kallas ett integritesområde.

Exempel 3.11. Vi ska nu studera multiplikationstabellerna för $\mathbb{Z}_5$ och $\mathbb{Z}_6$.

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Tabell 1: multiplikation tabell för $\mathbb{Z}_5$

*	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[1]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Tabell 2: multiplikation tabell för $\mathbb{Z}_6$

Vid en noggran undersökning av multiplikationstabellen för $\mathbb{Z}_5$ finner vi att produkten av två nollskilda element är nollskilt. Det vill säga att $\mathbb{Z}_5$ saknar nolldelare och därmed är ett integritetsområde. Motsvarande undersökning av multiplikationstabellen för ringen $\mathbb{Z}_6$ visar att produkten av två nollskilda elementen [2] och [3] är [0], det vill säga att ringen $\mathbb{Z}_6$ har nolldelare och därmed inte är ett integriteteområde.

Det kommer att visa sig i nästa avsnitt att det som är avgörande är om n är primtal eller inte.

4 Kroppar

En kropp är en kommutativ ring med det extra kravet att för varje element $q \neq 0$ i ringen R finns ett element q' så att $q \cdot q' = 1$, det vill säga att varje nollskilt element har en multiplikativ invers. Vi kan se att i multiplikationstabellen för $\mathbb{Z}_5$ (Tabell 1), att varje element utom noll har en multiplikativ invers, ty varje rad utom [0]-raden innehåller [1]. Denna egenskap saknas i fallet $n = 6$.

Vi kan definiera en kropp enligt följande.

Definition 4.1. En ring med etta i vilken varje element utom noll har en multiplikativ invers kallas en kropp [1].

Exempel 4.2. Mängden $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, exempel 3.3 är en ring men inte en kropp. Exempelvis har vi $-2 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, och $(-2 + \sqrt{2})^{-1} = (-1 - \frac{1}{2}\sqrt{2}) \notin \mathbb{Z}[\sqrt{2}]$. Med detta ser vi att $\mathbb{Z}[\sqrt{2}]$ saknar multiplikativ invers och därmed är inte en kropp.

Observera att om vi istället studera ringen $\mathbb{Q}[\sqrt{2}]$, har vi en kropp.

Det framgått av exempel 3.3 att $\mathbb{Z}_6$ saknar nolldelare och därmed inte är ett integritetesområde. Medan $\mathbb{Z}_5$ är ett integeritisomrsåde med multiplikativ invers, så enligt definition 4.1 är $\mathbb{Z}_5$ en kropp. Det här händer för att 6 inte är ett primtal. Detta kan vi generalisera i följande sats.

Sats 4.3. *Ringen $\mathbb{Z}_n$ är en kropp om och endast om n är ett primtal.*

Bevis. Antag att n inte är primtal då finns en faktorisering $n = a \cdot b$ med $1 < a, b < n$. I ringen $\mathbb{Z}_n$ är restklassen $[a] \neq [0]$ och $[b] \neq [0]$, men $[a] \cdot [b] = [a \cdot b] = [n] = [0]$, vilket är omöjligt i en kropp enligt definition 4.1. Därmed $\mathbb{Z}_n$ inte är en kropp när n inte är primtal.

Antag nu att n är primtal och restklassen $[a] \neq [0]$, vi söker ett b sådant att $[a] \cdot [b] = [1]$. Eftersom n är primtal och $n \neq a$, har vi att a och n är relativt prima, så enligt Bezouts sats i [3] finns heltal b och y sådana att $ab + ny = 1$. Detta innebär att $a \cdot b \equiv 1 \pmod{n}$ så $[a] \cdot [b] = [1]$, det vill säga att $[b]$ är multiplikativ invers till $[a]$. Därmed har vi visat att Z_n är en kropp om n är ett primtal. □

Nu ska vi undersöka lite närmare så kallade kvadratiska talkroppar. För att förstå kvadratiska kroppar behöver vi först bekanta oss med begreppet kroppsutvidgning.

En kroppsutvidging inom matematik är en kropp K som innehåller en annan kropp F som en delkropp [4].

Till exempel, de komplexa talen $\mathbb{C}$ är kropputvidgning av de reella talen $\mathbb{R}$. En kvadratiska talkropp, kan vi definiera enligt följande.

Definition 4.4. Mängden $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ är en kvadratiskt talkropp, om $m \neq 1$ är ett kvadratfritt heltal.

Ett kvadratfritt heltal är ett heltal m som inte är delbart med kvadraten på något primtal. Till exempel 6 är kvadratfritt heltal, medan 18 inte är kvadratfritt för att 18 är delbart med $9 = 3^2$.

Vi skall nu visa att $\mathbb{Q}(\sqrt{m})$ är en kropp. Först visar vi att den är sluten under addition och multiplikation, slutligen visar vi att varje element i $\mathbb{Q}(\sqrt{m})$ har multiplikativ invers.

Den är sluten under addition, efterson för alla a, b och $c, d \in \mathbb{Q}$ gäller att

$$(a + b\sqrt{m}) + (c + d\sqrt{m}) = (a + c) + (b + d\sqrt{m}).$$

Den är sluten under multiplikation, eftersom för alla a, b och $c, d \in \mathbb{Q}$ gäller att

$$(a + b\sqrt{m})(c + d\sqrt{m}) = (ac) + (ad\sqrt{m} + bc\sqrt{m} + (bd\sqrt{m}\sqrt{m})$$

$$= (ac + mbd) + (ad + bc)\sqrt{m}) \in \mathbb{Q}\sqrt{m}.$$

För alla $a + b\sqrt{m} \in \mathbb{Q}$ existera additiv invers eftersom

$$(a + b\sqrt{m}) + (-a - b\sqrt{m}) = 0.$$

Nu kvarstår att kontrollera om varje nollskilt element i ringen har multiplikativ invers. Låt $a, b \in \mathbb{Q}$ och $(a, b) \neq (0, 0)$, vi måste hitta en c och $d \in \mathbb{Q}$ så att $(a + b\sqrt{m}) \cdot (c + d\sqrt{m}) \neq 0$.

Den multiplikativa inversen till $(a + b\sqrt{m})$ kan skrivas som $\frac{1}{(a+b\sqrt{m})}$ och vi får

$$\frac{1}{a + b\sqrt{m}} = \frac{1}{(a + b\sqrt{m})} \cdot \frac{a - b\sqrt{m}}{(a - b\sqrt{m})} = \frac{a}{(a^2 - mb^2)} + \frac{-b}{(a^2 - mb^2)}\sqrt{m} \in \mathbb{Q}(\sqrt{m}).$$

Med detta har vi visat att $a + b\sqrt{m}$ har multiplikativ invers. Därmed $\mathbb{Q}(\sqrt{m})$ är en kropp.

5 Euklidiska ringar och entydig faktorisering

Ringen $\mathbb{Z}$ är en ring där varje element kan skrivas entydigt som en produkt av primtal. Detta visade man med hjälp av Euklides algoritm, en känd algoritm som används för att finna största gemensamma delare till två heltal utan faktorisering. Euklides algoritm beskrevs i Elementa av den Grekisk matematikern Euklides

(325-265 f.kr.). Ringar i vilka Euklides algoritm kan användas utgör en speciell klass av ringar känd som Euklidiska ringar. Vi ska visa att Euklidiska ringar har entydig faktorisering.

Men första några viktiga definitioner.

Definition 5.1. Ett element u i en ring R med etta är en enhet om u är inverterbart i R, det vill säga att det finns ett element $v \in R$ så att $uv = 1$.

De enda enheter, element med multiplikativ invers i integritetsområdet $\mathbb{Z}$ är 1 och -1. I en kropp varje nollskilt element är en enhet.

Definition 5.2. Två nollskilda element a och b i en ring R med etta sägs vara associerade, om det finns en enhet $u \in R$ sådan att $a = bu$.

Två nollskillda element $a, b \in \mathbb{Z}$ är associerade om och endast om $a = \pm b$, däremot i en kropp är alla nollskilda element associerade.

Definition 5.3. Låt R vara en ring med etta. Elementet $\pi \in R$ är ett irreducibelt element i R om $\pi = \sigma \cdot \delta$ med $\sigma, \delta \in R$ medför att precis en av σ och δ är en enhet.

Definition 5.3 säger att π är ett element som inte kan skrivas som en produkt av två andra element utan att något av dem är en enhet. Exempelvis har vi att de irreducibla elementen bland heltalen är alla p och $-p$, där p är primtal.

Definition 5.4. Låt R vara ett integritetsområde och antag att $a, n \in R$. Ett element a kallas delare till ett element n, om det finns ett element $b \in R$, sådant att $n = ab$. Vi skriver detta som $a \mid n$ [4].

Största gemensamma delaren av två eller flera heltal, där minst ett av talen är nollskilt är, enligt den klassiska definitionen, det största heltal som delar alla talen. Till exempel 2 är den största gemensam delaren till 4 och 6 i ringen $\mathbb{Z}$. I en mer allmän definition kommer en största gemensam delare inte längre vara unik. Till exempel räknas både $+2$ och -2 som största gemensamma delaren till 4 och 6 i integritetsområdet $\mathbb{Z}$ enligt följande definition:

Definition 5.5. Om a, b är element i ett integritetsområde R, och $ab \neq 0$ då är $d \in R$ en största gemensam delare till a och b förutsatt att:

1. $d \mid a$ och $d \mid b$,
2. om $c \mid a$ och $c \mid b$ för något $c \in R$ så gäller $c \mid d$.

Första egenskapen innebär att d är en gemensam delare till a och b medan den andra egenskapen innebär att d är även största bland sådana delare, varför kallas den största gemensam delaren till a och b.

Nu ska vi visa att de största gemensamma delare är associerade genom att bevisa följande sats.

Sats 5.6. *Om d_1 och d_2 båda är största gemensamma delare till a och b i ett integritesområde R, då är d_1 och d_2 associerade i R.*

Bevis. Antag att båda d_1 och d_2 är största delare till a och b. Då vet vi att d_2 delar a och b. Eftersom d_1 är största delaren gäller då $d_2 \mid d_1$. Enligt definition av delbarhet 5.4, gäller $d_1 = d_2u$ för något $u \in R$. Samma argument kan används för att visa att $d_2 \mid d_1$. Nu ska vi visa att d_1 och d_2 är associerade. Det gäller att $d_1 = d_2u$ och $d_2 = d_1v$ för några $u, v \in R$, så $d_1 = d_2u = (d_1v)u = d_1(vu)$, och därmed får vi $d_1(1 - uv) = 0$. Notera att $d_1 \neq 0$ och eftersom det i ett integritetsområde inte finns några nolldelare, så måste $1 - uv = 0$, eller $uv = 1$. Eftersom v alltså är en enhet i R och $d_2 = d_1v$, så är d_1 och d_2 associerade enligt definition 5.2. □

Definition 5.7. Ett integritetsområde R har entydig faktorisering om det har följande egenskaper:

1. Varje element $a \in R$ som inte är noll eller enhet kan skrivas som produkt av irreducibla element i R.

2. Om $a \in R$ och $a = p_1p_2 \dots p_s = q_1q_2 \dots q_t$, där alla p_i, q_j är irreducibla, så är $s = t$ och det finns en permutation π av $\{1, 2, \dots, s\}$ så att p_i och $q_{\pi(i)}$ är associerade för alla i med $1 \leq i \leq s$.

Definition 5.8. Ett integritesområde R är en Euklidisk ring om för varje nollskilt element $a \in R$ finns ett positivt heltal $d(a)$ med följande egenskaper:

1. om a,$b \in R$ och a,$b \neq 0$ så är $d(a) \leq d(ab)$,

2. om a,$b \in R$ och $b \neq 0$, då finns två element q,$r \in R$ så att $a = bq + r$ med $r = 0$ eller $d(r) < d(b)$.

I fortsättning betecknar vi en Euklidisk ring med D, för att betona skillnaden mellan ett integritetsområde R och en Euklidisk ring D.

Exempel 5.9. Vi ska vis att ringen av heltal $\mathbb{Z}$ är en Euklidisk ring enligt definition 5.8, om $d(a) = |a|$ för alla $a \neq 0$. Vi vet att ringen av heltal $\mathbb{Z}$ är en kommutativ ring med etta. Om $b \neq 0$ så är $|b| \geq 1$, alltså vi får $|a| \leq |a||b| = |ab|$. Därmed gäller första egenskapen. Det andra egenskapen följer ur divisionalgoritmen för $\mathbb{Z}$, se [3]. Därmed har vi påvisat att $\mathbb{Z}$ är en Euklidisk ring [4].

Vi skall nu visa att varje Euklidisk ring har entydig faktorisering. Låt oss först gå igenom några nödvändiga hjälpsatser och definitioner. Formulering av satserna kommer från [1], där de ges utan bevis. Arbetets tyngdpunkt har varit att arbeta med att formulera bevis för dessa satser.

Sats 5.10. *Två nollskilda element a,b i en Euklidisk ring D har en största gemensam delare $c \in D$ och $c = ar + bs$ för några r,s $\in D$.*

Bevis. Euklides algoritm är välkänd för ringen av heltal. Nu ska vi undersöka om denna algoritm kan generaliseras till Euklidiska ringar. Låt $a, b \in D$. Då finns $q_1, r_1 \in D$ så att:

$$a = q_1 b + r_1, \qquad d(r_1) < d(b).$$

Vi fortsätter och får,

$$\begin{aligned}
b &= q_2 r_1 + r_2, & d(r_2) &< d(r_1) \\
r_1 &= q_3 r_2 + r_3, & d(r_3) &< d(r_2) \\
&\vdots \\
r_{i-3} &= q_{i-1} r_{i-2} + r_{i-1}, & d(r_{i-1}) &< d(r_{i-2}) \\
r_{i-2} &= q_i r_{i-1} + r_i, & d(r_i) &< d(r_{i-1}) \\
r_{i-1} &= q_{i+1} r_i
\end{aligned}$$

Eftersom alla $d(r_i)$ är heltal, och följden $d(r_1), d(r_2), \ldots$, är strikt avtagande, så måste till slut någon rest r_{i+1} vara 0.

Nu skall vi visa att den sista nollskilda resten r_i är en största gemensam delare till a och b. Vi börja med att visa att r_i är en gemensam delare till a och b genom att skriva Euklides algoritmen från sista raden och uppåt. Eftersom $r_{i-1} = q_{i+1} r_i$ får vi att r_i delar r_{i-1}. Men r_i delar även r_{i-2} ty $r_{i-2} = q_i r_{i-1} + r_i$. Fortsätter vi på samma sätt genom varje rad, får vi $r_i \mid r_{i-1}$, $r_i \mid r_{i-2}$, $\ldots$, $r_i \mid r_1$, slutligen att $r_i \mid b$ och $r_i \mid a$. Detta betyder att r_i är en gemensam delare till a och b. Återstå att visa att r_i även är en största delare till a och b. Antag nu att det finns ett $d \in D$ sådant att $d \mid a$ och $d \mid b$. Vi får att $d \mid r_1$ eftersom $r_1 = a - q_1 b$, men om $d \mid b$ och $d \mid r_1$ så $d \mid r_2$ eftersom $r_2 = b - q_2 r_1$. Vi fortsätter på samma sätt genom varje rad, får vi slutligen att $d \mid r_i$, därmed har vi visat att r_i är även en största delare till a och b.

Nu kan vi visa det sista påståendet, genom att skriva Euklides algoritmen baklänges. Sätt $c = r_i$. Omskrivning av näst sista raden ger oss nämligen att $c = r_i = q_i r_{i-1} - r_{i-2}$, detta är r_i som linjärkombination av r_{i-1} och r_{i-2}. Vi förtsätter till föregående rad och då ser vi att c kan skrivas som en linjärkombination av r_{i-2}

och r_{i-3}. Vi försätter och till slut får vi c som linjärkombination av a och b med koefficienter r, s i ringen D, alltså

$$c = ar + bs$$

för några $r,\ s \in\ D$. □

Definition 5.11. Två element a och b i en Euklidisk ring D är relativt prima om alla största gemensamma delare till a och b är enheter.

Sats 5.12. *Antag att a, b, c är element i en Euklidisk ring D och $a, b, c \neq 0$. Om a och b är relativt prima och $a \mid bc$, så gäller att $a \mid c$.*

Bevis. Vi antar att a och b är relativt prima. Enligt sats 5.10, har vi att

$$ar + bs = 1 \tag{5.13}$$

för några r, s i D. Multipliceras båda leden i ekvationen 5.13 med c, får vi $acr + bcs = c$. Givetvis gäller $a \mid acr$, och vi har att $a \mid bc$, så $a \mid bcs$. Alltså $a \mid (acr+bcs)$, men $(acr + bcs) = c$, så $a \mid c$. □

Sats 5.14. *Låt π vara irreducibelt element i en Euklidisk ring D. Antag att $\pi \mid \sigma\delta$ för några σ,δ i D. Då gäller att $\pi \mid \sigma$ eller $\pi \mid \delta$.*

Bevis. Om $\pi \mid \sigma$ så är vi klara med beviset. Antag därför att π inte delar σ. Vi vill visa att π delar δ. Om π inte delar σ, är π och σ relativt prima och $\pi \mid \sigma\delta$, så enligt sats 5.12, får vi $\pi \mid \delta$. □

Satsen kan generaliseras till en produkt av flera faktorer än två. Om ett irreducibelt element π delar en produkt $\alpha_1\alpha_2 \ldots \alpha_k$ i en Euklidisk ring, så måste π dela någon av faktorerna α_i. Detta påstående följer genom induktion över k.

Ett viktigt lemma är följande.

Lemma 5.15. *Om a och b är nollskilda element i D, så gäller att $d(a) = d(ab)$ om och endast om b är en enhet.*

Bevis. Antag att b är en enhet i D, då gäller $bc = 1$ för något element c i D. Enligt definition 5.8, första villkoret gäller, $d(a) \leq d(ab)$ och $d(ab) \leq d((ab)c) = d(a(bc)) = d(a)$. Alltså vi har visat att $d(a) = d(ab)$ om b är en enhet.

Antag nu att b inte är en enhet. Vi vill visa att $d(a) < d(ab)$. Enligt andra villkoret i definition 5.8, gäller $a = qab + r$ för några r och q i D, med $r = 0$ eller $d(r) < d(ab)$. Om $r = 0$ då $a = qab$, så $a(1 - qb) = 0$, och eftersom a är nollskilt då måste $qb = 1$, det vill säga att b är en enhet. Detta är en motsägelse mot vårt antagande. Och om $d(r) < d(ab)$ och r nollskilt, så $r = a - qab = a(1 - qb)$. Vi vet att $d(a) \leq d(a(1 - qb))$, men $a(1 - qb) = r$. Genom substitutionen får vi att, $d(a) \leq d(r) < d(ab)$. Därmed har vi visat att om b inte är en enhet så är $d(a) < d(ab)$. □

Sats 5.16. *Varje element i en Euklidisk ring som är skilt från noll och inte är en enhet kan skrivas som produkter av irreducibla element.*

Bevis. Antag att det finns element som inte kan skrivas som produkter av irreducibla element. Låt $s \neq 0$ vara sådant med minsta möjliga $d(s)$. Detta innebär att vi kan skriva $s = ab$ för något a och b i D, där varken a eller b är enhet. Enligt lemma 5.15 gäller att $d(a) < d(ab) = d(s)$ och $d(b) < d(ab) = d(s)$. Eftersom både $d(a)$ och $d(b)$ är mindre än $d(s)$, så måste dessa element kunna skrivas som produkt av irreducibla. Men detta betyder också att s kan skrivas som produkt av irreducibla, varvid vi har en motsägelse. Det vi har visat att det inte finns något element som inte kan skrivas som produkt av irreducibla. □

Sats 5.17. *Varje Euklidisk ring har entydig faktorisering.*

Bevis. Vi har visat att faktorisering i irreducibla element är möjligt, nu behöver vi visa att den är entydig. Antag att vi har två faktorisering $s = \pi_1\pi_2 \dots \pi_k = \theta_2 \dots \theta_l$. Det irreducibla elementet $\pi_1 \mid \theta_1\theta_2 \dots \theta_l$, så enligt sats 5.14 så gäller att $\pi_1 \mid \theta_j$ för något $j \in \{1, 2, \dots, l\}$. Efter omnumrering kan vi anta att $\pi_1 \mid \theta_1$, eftersom båda elementen är irreducibla, måste de vara associerade. Låt $\theta_1 = \pi_1 u$. Dela båda leden med π_1. Kvar står, då $\pi_2\pi_3 \dots \pi_k = u\theta_2\theta_3 \dots \theta_l$. Upprepas resonemanget, får vi till slut att villkor 2 i definition 5.7 är uppfyllt. Därmed har vi visat att varje Euklidisk ring har entydig faktorisering. □

6 Gaussiska heltal

Gaussiska heltal är komplexa tal $a+bi$, där a och b är heltal. Mängden av Gaussiska heltal betecknas med $\mathbb{Z}[i]$. Carl Fredrich Gauss (1777-1855) införde Gaussiska heltal (1832) i hans andra monografi om kvadratisk reciprocitets. Den kvadratisk reciprocitetssatsen relatera lösbarheten av kongruensen $x^2 \equiv q \pmod{p}$ till den för $x^2 \equiv p \pmod{q}$ [8]. Han introducerade även termerna norm, enhet, och associerad som nu är standard i algebraisk talteori.

Huvudmålet i detta kapitel är att visa att ringen av Gaussiska heltal är Euklidisk och därmed enligt sats 5.17 har unik faktorisering.

Mängden $\{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, betecknas med $\mathbb{Z}[i]$, är en delmängd av $\mathbb{C}$ som bildar en ring, eftersom summan och produkten av två godtyckliga Gaussiska heltal $z = a + bi$ och $w = c + di$ är också ett Gaussiskt heltal. Således är $\mathbb{Z}[i]$ ett integritets område ty $\mathbb{C}$ är ett integitetsområde.

Konjugat av ett komplex tal $z = a+bi$ definieras av $\overline{z} = a-ib$. Vi kan definiera normen för Gaussiska heltal som följande.

Definition 6.1. Normen $N : \mathbb{Z}[i] \mapsto \mathbb{Z}$ definieras för $z = a + bi \in \mathbb{Z}[i]$ som $N(z) = z\overline{z} = (a + bi) \cdot (a - bi) = a^2 + b^2$.

Med denna definition är normen en funktion från ringen av Gaussiska heltal till ringen av heltal.

Exempel 6.2. Vi ska räkna normen av Gaussiskt heltalet $z = (3 + 4i)$ det vill säga $N(z)$. Enligt definition 6.1 är $N(z) = N(3 + 4i) = |3^2 + 4^2| = 25$.

Sats 6.3. *Normen är multiplikativ, det vill säga att för w och z i $\mathbb{Z}[i]$ gäller att $N(zw) = N(z)N(w)$.*

Bevis. Vi får

$$N(zw) = (zw)(\overline{zw}) =$$
$$= (z\overline{z})(w\overline{w}) = N(z)N(w).$$

Därmed har vi visat att normen är multiplikativ. □

Normen för varje Gaussiskt heltal är ett icke-negativt heltal, men alla icke-negativa heltal är inte en norm. Eftersom enligt definition 6.1 normen är ett heltal av formen $a^2 + b^2$, och inte varje positivt heltal är summan av två kvadrater. Exempelvis talen $3, 7, 11, 15, 19$ och 21 är inte summan av två heltals kvadrater.

Vi har konstaterat att ringen av Gaussiska heltal är ett integritetsområde, och enligt definition 5.1 är en enhet i ett integritetsområde ett element som har multiplikativ invers. Vi skall nu bestämma enheterna i ringen av Gaussiska heltal.

Sats 6.4. *Ett element $\alpha \in \mathbb{Z}[i]$ är en enhet om och endast om $\alpha \in \{-1, 1, -i, i\}$.*

Bevis. Vi kan enkelt se att -1 och 1 är sina egna inverser, och i och $-i$ är varandras inverser.

Antag nu att $\alpha = a+bi$ är en enhet i $\mathbb{Z}[i]$, så $\alpha\omega = 1$ för något ω i $\mathbb{Z}[i]$.Vi vill visa att $\alpha \in \{-1, 1, i, -i\}$. Vi räknar normen av båda sidor och får $N(\alpha\omega) = N(1) = 1$. Enligt sats 6.3 är normen multiplikativ, så $N(\alpha)N(\omega) = 1$. Vi vet att normen är ett positivt heltal, så $N(\alpha) = N(\omega) = 1$. Enligt definition 6.1 är $N(\alpha) = |a^2 + b^2|$, det vill säga att $a^2 + b^2 = 1$, så enda möjligheterna är

$$a = \pm 1 \qquad b = 0$$

eller

$$a = 0 \qquad b = \pm i,$$

och därmed $\alpha \in \{1, -1, +i, -i\}$. □

Delbarhet i $\mathbb{Z}[i]$ definieras av definition 5.4.

Exempel 6.5. Det Gaussiska heltalet $14 - 3i$ är delbart med $4 + 5i$, ty $14 - 3i = (4 + 5i)(i - 2i)$.

Exempel 6.6. Vi ska undersöka om Gaussiskt heltalet $14+3i$ är delbart med $4+5i$.

$$\frac{(14+3i)}{(4+5i)} = \frac{(14+3i)(4-5i)}{(4+5i)(4-5i)} = \frac{71}{41} - \frac{58i}{41} \notin \mathbb{Z}[i].$$

Med detta har vi visat att Gaussiskt heltalet $14+3i$ inte är delbart med $4+5i$.

Med hjälp av normen $N : \mathbb{Z}[i] \mapsto \mathbb{Z}$, kommer vi att kunna relatera delbarhet i $\mathbb{Z}[i]$ med delbarhet i $\mathbb{Z}$, enligt följande.

Sats 6.7. *Låt z och $w \in \mathbb{Z}[i]$. Om $w \mid z$ så gäller att $N(w) \mid N(z)$.*

Bevis. Antag att ω delar z, så $w = z\alpha$ för något α i $\mathbb{Z}[i]$. Vi tar normen av båda sidor, och enligt sats 6.3 är normen multiplikativ, så

$$N(w) = N(z\alpha) = N(z)N(\alpha).$$

Därmed ser vi att $N(w) \mid N(z)$ i $\mathbb{Z}$. □

Satsen kan användas som ett snabbt sätt att undersöka om ett Gaussiskt heltal är delbart med ett annat Gaussiskt heltal.

Exempel 6.8. Vi skall undersöka om $\alpha = 3+7i$ delar $\omega = 10+3i$ i $\mathbb{Z}[i]$. Vi börjar med att beräkna normerna $N(3+7i) = 58$ och $N(10+3i) = 109$. Enligt sats 6.7, måste $58 \mid 109$ i $\mathbb{Z}$ om $\omega \mid \alpha$, vilket inte är sant, så $\omega \nmid \alpha$. Det vill säga att α delar inte ω.

Notera att vanligtvis gäller inte omvändningen, det vill säga att normen av Gaussiska heltal kan dela varandra utan att de Gaussiska heltalen är delbara med varandra. Fallet med dom två Gaussiska heltalen $\alpha = 14+3i$ och $\omega = 4+5i$ i exempel 6.6 är ett sådant fall. Vi såg att α inte är delbart med ω i $\mathbb{Z}[i]$, men $N(\omega) \mid N(\alpha)$ i $\mathbb{Z}$, ty $N(\alpha) = 205 = 41 \cdot 5$ och $N(\omega) = 41$.

Det vanliga divisionalgoitm i $\mathbb{Z}$ säger att för ett heltal a och ett nollskilt heltal b finns ett unikt heltal q kallad kvot och ett unikt heltal r kallad rest, där $0 \leq r < |b|$. I följande rader kommer vi att bevisa divisionalgoritmen för de Gaussiska heltalen. Först ger vi algebraiskt bevis enligt referensboken [1] och sedan ett geometriskt bevis.

Sats 6.9. *Låt z och w vara två nollskillda element i $\mathbb{Z}[i]$ då finns q och $r \in \mathbb{Z}[i]$ så att $z = wq + r$ och $N(r) < N(w)$.*

Bevis. Antag $z, w \in \mathbb{Z}[i]$ är nollskilda. Antag nu att $\frac{z}{w} = a + bi$, med a och b i $\mathbb{Q}$ och låt m, n i $\mathbb{Z}$ vara närmaste heltal till a respektive b, det vill säga att sådana att $|a-m| \leq \frac{1}{2}$, och $|b-n| \leq \frac{1}{2}$. Då är

$$\frac{z}{w} = a + bi = m + ni + [(a-m) + (b-n)i],$$

och därmed

$$z = (m + ni)w + [(a - m) + (b - n)i]w = qw + r,$$

där $q = m + ni$ och $r = [(a - m) + (b - n)i]w$. Här är $r \in \mathbb{Z}[i]$ eftersom båda qw och z är i $\mathbb{Z}[i]$.

För att visa att $N(r) \leq N(w)$ börjar vi med att ta normen av r,

$$N(r) = N[(a - m) + (b - n)i]N(w),$$

och enligt definition 6.1,

$$N(r) = ((a - m)^2 + (b - n)^2)N(w),$$

via substitution får vi

$$N(r) \leq \left(\frac{1}{4} + \frac{1}{4}\right) N(w) = \frac{1}{2}N(w) < N(w),$$

alltså $N(r) < N(w)$, vilket skulle visas. □

Exempel 6.10. Betrakta $z = 1 + 8i$ och $w = 2 - 4i$ i $\mathbb{Z}[i]$. Först räknar vi,

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{-30}{20} + i\frac{20}{20}.$$

Sedan väljer vi -2 ett närmaste heltalet till $\frac{-30}{20}$, och från $\frac{20}{20}$ får vi heltalet 1. Detta ge upphov till $q = -2 + i$. Vidare hittar vi resten från

$$r = z - wq = (1 + 8i) - ((-2 + i) \cdot (2 - 4i)) = 1 - 2i,$$

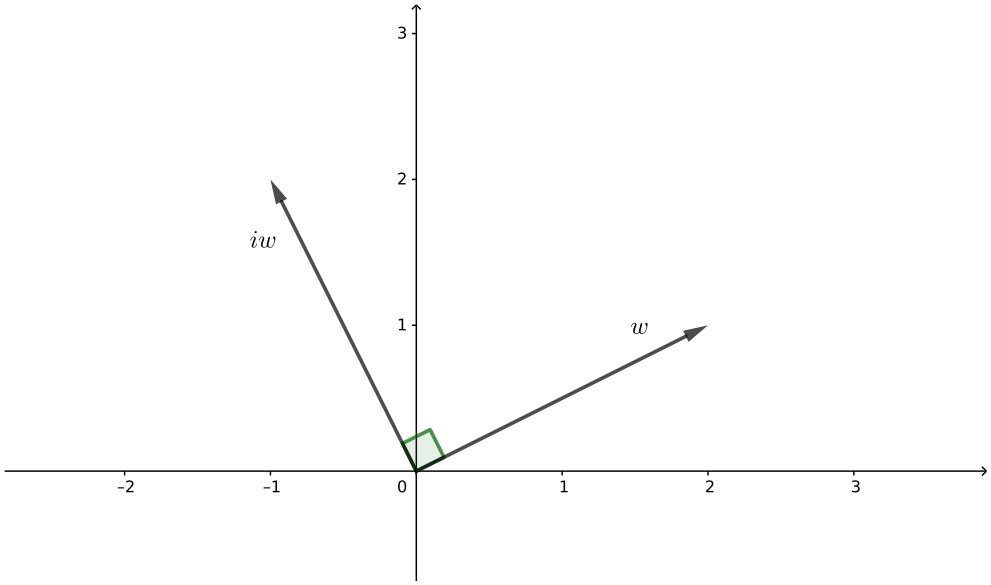
och

$$N(r) = r\overline{r} = (1 - 2i)(1 + 2i) = 5 \leq N(w) = 20,$$

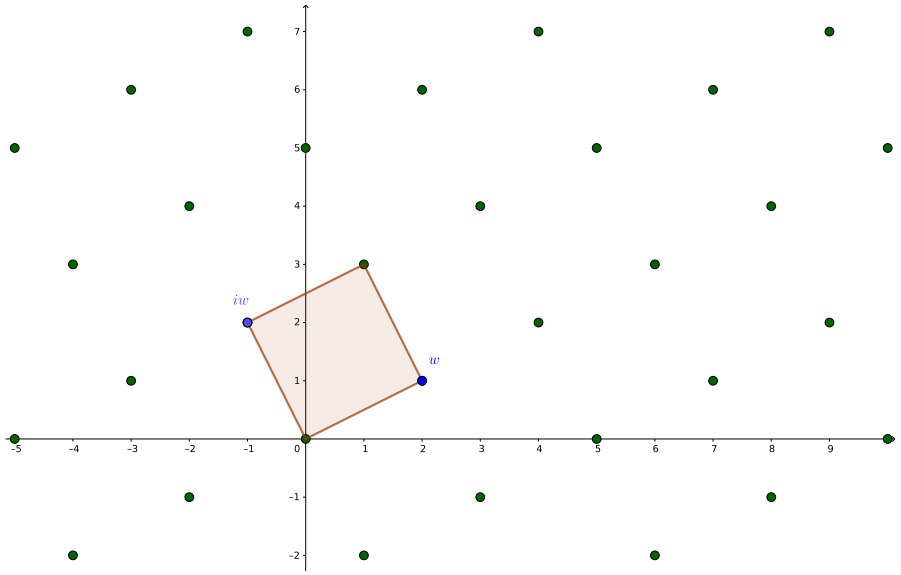
så val av $q = -2 + i$ och $r = 1 - 2i$ funkar för att få $N(r) < N(w)$.

I exempel 6.10 valde vi -2 som ett närmaste heltal till $\frac{-30}{20}$, vad händer om vi väljer den andra möjligheten , det vill säga -1 ? Vi får $q = -1+i$ och $r = -1-2i$, och $N(r) = 3 < 20 = N(w)$. Vi ser att detta val av q och r också skulle fungera. Detta är ett exempel på att kvoten och resten inte är unika för de Gaussiska heltalen.

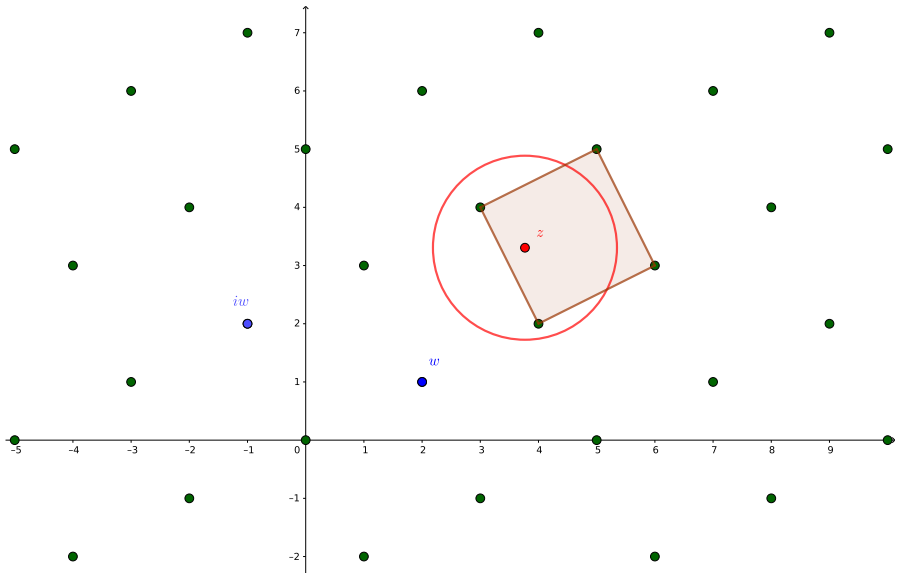
Härnäst kommer ett geometriskt bevis av divisionalgoritmen för Gaussiska heltal i det komplexa talplanet, formulerat på förslag av min handledare.



Figur 1: Komplexa talen w och iw som vektorer.



Figur 2: Ett kvadratiskt gitter



Figur 3: En cirkelskiva med center z och radie $\frac{|w|}{\sqrt{2}}$.

Bevis. Man kan betrakta ett Gaussiskt heltal som en vektor w från origo till punkten w. Om man multiplicerar w med i så motsvarar det en rotation med 90 grader moturs runt origo. Alltså de två vektorerna w och wi är ortogonala, figur 1.

Mängden $w \cdot \mathbb{Z}[i] = \{w \cdot q \mid q \in \mathbb{Z}[i]\} = \{aw + biw \mid a, b \in \mathbb{Z}\}$ är mängden av heltalliga linjärkombinationer av w och iw, som bildar ett kvadratiskt gitter med sidolängd $|w|$, det vill säga att de Gaussiska multiplerna av q bildar ett kvadratiskt gitter med sidolängd $|w|$. Figur 2 visar ett sådant kvadratiskt gitter.

Betrakta nu en given punkt z, vilken måste tillhöra någon av gitterkvadraterna. I en kvadrat är det längsta möjliga avståndet från en punkt till närmaste hörn i mitten av kvadraten. Alltså, i en kvadrat med sidolängd $|w|$ är $\frac{|w|}{\sqrt{2}}$ det längsta avståndet som någon punkt i kvadraten kan få från närmaste hörnet. Detta betyder att ett cirkelskiva med radie $\frac{|w|}{\sqrt{2}}$ och center z innehåller minst ett gitterpunkt wq, se Figur 3.

Låt $r = z - wq$, som alltså har längden $\frac{|w|}{\sqrt{2}}$ som mest. Det vill säga att

$$|r| = |z - wq| \leq \frac{|w|}{\sqrt{2}}. \tag{6.11}$$

Genom att kvadrera båda sidor i ekvation 6.11 får vi, $|r|^2 \leq \frac{|w|^2}{2}$, så

$$N(r) \leq \frac{1}{2}N(w) < N(w),$$

ty $N(r) = |r|^2$ och $N(w) = |w|^2$.

Det var det som skulle visas. □

Vi avslutar det här avsnittet med den viktigaste satsen i uppsatsen.

Sats 6.12. *Ringen $\mathbb{Z}[i]$ är en Euklidisk ring.*

Bevis. Enligt definition 5.8 behöver vi visa att, för alla $w, z \in \mathbb{Z}[i]$ om $w \mid z$ gäller $N(w) \leq N(z)$, och det finns två element $q, r \in \mathbb{Z}[i]$ så att $z = wq + r$ och $N(r) < N(w)$.

Låt $Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Låt $z = wq$ för några $z, w, q \in \mathbb{Z}[i]\backslash\{0\}$ och $w \mid z$. Enligt Sats 6.3 är normen multiplikativ, så,

$$N(w) \leq N(w)N(q) = N(wq) = N(z).$$

Alltså, $N(w) \leq N(z)$.

Enligt sats 6.9, finns $q, r \in \mathbb{Z}[i]$ så att $z = wq + r$ och $N(r) < N(w)$. Alltså är ringen av Gaussiska heltal en Euklidisk ring. □

Sats 6.13. *Ringen $\mathbb{Z}[i]$ har entydigt faktorisering i primtalsfaktorer.*

Bevis. Enligt sats 5.17 och sats 6.12 följer att ringen av Gaussiska heltal har entydigt faktorisering i primtalsfaktorer. □

7 Tvåkvadratsatsen

Fermats tvåkvadratsats, som säger att varje primtal p med resten 1 vid division med 4 kan skrivas som en summa av två heltalskvadrater, presenterades först 1625 av Girard (1595–1632) och 15 år senare 1640 återigen av Fermat (1601–1655), utan bevis [7]. I det kommande avsnittet kommer Fermats tvåkvdratsats visas som en följdsats av satsen om entydig faktorisering för Gaussiska heltal. Innan vi ger beviset för Fermats tvåkvadratsats, behöver vi ett lemma och nästkommande sats.

Lemma 7.1. *Låt p vara ett primtal med $p \equiv 1 \pmod 4$. Det finns ett heltal y så att $y^2 \equiv -1 \pmod p$.*

Bevis. Vi antar att $p \equiv 1 \pmod 4$ är ett primtal. Låt

$$F(x) = x^{\frac{p-1}{2}} - 1$$

vara ett polynom med koefficienter i $\mathbb{Z}_p$. Enligt sats 4.3 är $\mathbb{Z}_p$ en kropp. Vi ska undersöka polynomet och dess nollställen i $\mathbb{Z}_p$.

Polynomet $F(x)$ har högst $\frac{p-1}{2}$ nollställen i $\mathbb{Z}_p$, ty ett polynom över en kropp har högst så många nollställen som sin grad, se [1]. Välj ett nollskilt element i $\mathbb{Z}_p$, det vill säga en restklass $[y] \neq [0]$. Nu låter vi $x = [y^2]$. Enligt Fermats lilla sats är alla heltal $1, 2, \ldots, p-1$ nollställen modulo p till polynomet $x^{p-1} - 1$, så

$$[x^{\frac{p-1}{2}} - 1] = [y^2]^{\frac{p-1}{2}} - [1] = [y^{p-1} - 1] = [0],$$

det vill säga att alla kvadrater av nollskilda element i $\mathbb{Z}_p$ är alltså nollställen till polynomet $F(x)$. Nu vill vi veta hur många kvadratiska rester som finns. Om vi tittar på ekvationen $[y_1^2] = [y_2^2]$, vi kan skriva den som

$$[y_1 + y_2][y_1 - y_2] = [0].$$

Eftersom $\mathbb{Z}_p$ är en kropp, och därmed saknar nolldelare, så måste $[y_1] = [\pm y_2]$. Vi får därmed precis $\frac{p-1}{2}$ kvadratiska rester. Därmed är de kvadratiska resterna alla nollställen till $F(x)$.

Om vi tar nu $x = -1$, får vi $F(-1) = (-1)^{\frac{p-1}{2}} - 1 = 0$, eftersom $p = 4k + 1$. Det vill säga $y^2 \equiv -1 \pmod p$ har lösning om $p \equiv 1 \pmod 4$. Vilket var det som vi skulle visa.

□

Sats 7.2. *Ett primtal $p \in \mathbb{Z}$ är sammansatt i $\mathbb{Z}[i]$ om och endast om det är en summa av två kvadrater.*

Bevis. Vi låter att p vara primtal i $\mathbb{Z}$ och $p = \alpha\beta$ vara icke-trivial faktorisering av p. Normen av p är $p^2 = N(\alpha)N(\beta)$ och eftersom faktorisering av p är icke-trivial så måste $N(\alpha) = p$. Vi låter nu $\alpha = a + bi$, normekvationen säger att $p = a^2 + b^2$.

För omvändningen antar vi att ett primtal p är summan av två kvadrater alltså $p = a^2 + b^2$ i $\mathbb{Z}$. En icke-trivial faktorisering av p i $\mathbb{Z}[i]$ blir då $p = (a + bi)(a - bi)$, så p är sammansatt. □

Nu har vi allt vi behöver för att bevisa Fermats tvåkvadratsats.

Sats 7.3. *(Fermats tvåkvadratsats). Ett udda primtal p kan skrivas som summan av två heltalskvadrater om och endast om $p \equiv 1 \pmod 4$.*

Bevis. Vi kommer att bevisa satsen med hjälp av lemma 7.1 och entydig faktorisering av Gaussiska heltal. Vi antar att $p \equiv 1 \pmod 4$. Enligt lemma 7.1, finns ett heltal y sådant att $y^2 \equiv -1 \pmod p$. Vi får att $p \mid y^2 + 1$ som kan faktoriseras till

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

och därmed får vi

$$p \mid (y + i)(y - i).$$

Nu ska vi visa att p är sammansatt i $\mathbb{Z}[i]$. Antag att p är irreducibelt, då måste $p \mid (y + i)$ eller $p \mid (y - i)$. Det finns därmed något Gaussiskt heltal $z = a + bi$ så att $p(a + bi) = y + i$ eller $p(a + bi) = y - i$. Den imaginära delen ger att $pb = 1$ respektive $pb = -1$, vilket är omöjligt. Alltså delar p varken $(y + i)$ eller $(y - i)$ det vill säga att p inte är irreducibelt. Därmed p kan faktoriseras i $\mathbb{Z}[i]$ och ingen av de faktorena är enhet, det vill säga att p är sammansatt och enligt sats 7.2, p kan skrivas som summan av två heltalkvadrater.

Omvänt, antag nu att p är udda och $p = a^2 + b^2$. Då måste antingen a eller b vara jämnt, eftersom kvadraten på ett jämnt tal ger resten 0, medan kvadraten på ett udda tal ger resten 1, vid division med 4. Alltså a och b har olika rester vid division med 2. Låt $a = 2s$ och $b = 2s' + 1$ för några $s, s' \in \mathbb{Z}$. Vi får $p = a^2 + b^2 = 4(s^2 + s'^2 + s') + 1$ som ger resten 1 vid division med 4. Alltså $p \equiv 1 \pmod 4$. □

Därmed har vi bevisat Fermats tvåkvadratsatsen som följdsats av satsen om entydig faktorisering för Gaussiska heltal.

8 Gaussiska primtal

Att säga att ett heltal är primtal, betyder att man inte kan faktorisera det talet utan att ett av faktorer måste vara 1 eller -1. Man kan till exempel skriva

$$3 = 1 \cdot 3 = 3 \cdot 1 = (-1) \cdot (-3) = (-3) \cdot (-1),$$

men inte på något annat sätt med heltal. Medan heltalet 22 kan faktoriseras till faktorer,

$$22 = 2 \cdot 11 = 11 \cdot 2 = (-2) \cdot (-11) = (-11) \cdot (-2),$$

och ingen av de faktorer är enhet i $\mathbb{Z}$.

I ringen $\mathbb{Z}[i]$, kan några primtal i $\mathbb{Z}$ faktoriseras på nytt sätt. Till exempel primtalen 2 och 13 i $\mathbb{Z}$, kan faktoriseras i $\mathbb{Z}[i]$ till,

$$2 = (1 + i)(1 - i), \qquad 13 = (3 + 2i)(3 - 2i),$$

och primtalet 3 som kan skrivas

$$3 = 1 \cdot 3 = (-1) \cdot (-3) = (i)(-3i) = (-i)(3i),$$

kan faktoriseras med trivial faktorer $1, -1, i, -i$. Detta kapitel har till ändamål att undersöka vilka Gaussiska heltal är Gaussiska primtal, och speciellt vilka primtal i $\mathbb{Z}$ som även är Gaussiska primtal.

Definition 8.1. Låt α vara ett nollskilt Gaussiskt heltal. Vi kallar α ett Gaussiskt primtal om α är irreducibelt i ringen $\mathbb{Z}[i]$.

Ett tal α är sammansatt om det har icke-triviala faktorer.

Till exempel är $i(1-7i)$ en trivial faktorisering och $(1-2i)(1+3i)$ en icke-trivial faktorisering av $7+i$. En icke-trivial faktorisering till 5 är $(1+2i)(1-2i)$. Det intressanta är att 5 är ett primtal i $\mathbb{Z}$ men sammansatt i $\mathbb{Z}[i]$, även 2 är sammansatt i $\mathbb{Z}[i]$, dock 3 är irreducibelt i $\mathbb{Z}[i]$, så några primtal i $\mathbb{Z}$ är primtal i $\mathbb{Z}[i]$ medan andra inte är. Det vi vill säga är att begreppet primtal inte är ovillkorligt och beror på vilken ring man relaterar det till.

Sats 8.2. *Ett Gaussiskt heltal vars norm är ett primtal i $\mathbb{Z}$, är ett Gaussiskt primtal.*

Bevis. Låt normen av α vara ett primtal p, och antag att $\alpha = \beta\gamma$ med $\beta, \gamma \in \mathbb{Z}[i]$. Vi vill visa att α bara har triviala faktoriseringar. Vi får att $p = N(\alpha) = N(\beta)N(\gamma)$, alltså måste antingen $N(\beta) = 1$ eller $N(\gamma) = 1$. Detta betyder att antingen β eller γ är en enhet, alltså α är irreducibelt i $\mathbb{Z}[i]$, så enligt definition 8.1 är α ett Gaussiskt primtal. □

Exempel 8.3. Låt oss undersöka om talet $z = 4 + 5i$ med normen $N(z) = (4 + 5i)(4 - 5i) = 41$ är ett Gaussiskt primtal. Vi ser att normen 41 är ett primtal i $\mathbb{Z}$, så enligt sats 8.2 är talet z ett Gaussiskt primtal.

Exempel 8.4. Låt oss nu att undersöka några intressanta Gaussiska heltal nämligen $z = 1 + i$, $\gamma = 1 - i$, $w = -1 - i$ och $\alpha = -1 + i$. Beräknar vi normen, får vi primtalet 2. Alltså enligt sats 8.2, är z, γ, w, och α Gaussiska primtal.

Vid en närmare undersökning av exempel 8.4, ser vi att $z, \gamma, w, \alpha \in \mathbb{Z}[i]$ är associerade med $1 + i$, ty $1 + i = 1(1 + i)$, $1 - i = -i(1 + i)$, $-1 - i = -1(1 + i)$, och $-1 + i = i(1 + i)$.

Sats 8.5. *Låt $p \in \mathbb{Z}$ vara ett primtal. Då är p ett Gaussiskt primtal om och endast om $p \equiv 3 \pmod 4$.*

Bevis. Antag att $p \equiv 3 \pmod 4$, och p kan faktoriseras i $\mathbb{Z}[i]$. Vi får att $p = (a + bi)(c + di)$, och $p^2 = N(p) = N(a + bi)N(c + di)$. Om både $N(a + bi)$ och $N(c+di)$ är större än 1, så måste $p = a^2+b^2$. Ett tal på formen a^2+b^2 vid division med 4 kan ge bara 0 och 1, så vi får att $a^2 + b^2$ modulo 4 är kongruent med en av,

$$0^2 + 0^2 = 0, \qquad 0^2 + 1^2 = 1, \qquad 1^2 + 0^2 = 1, \qquad \text{eller} \qquad 1^2 + 1^2 = 1,$$

men aldrig 3. Därmed drar vi slutsatsen att p är ett primtal i $\mathbb{Z}[i]$.

Omvänt, antag nu att p inte är 3 modulo 4. Antingen är $p = 2$ eller $p \equiv 1 \pmod 4$.

Fallet där $p = 2$, det enda jämna primtalet. Primtalet 2 kan faktoriseras till $2 = (1-i)(1+i)$. Vi får att $N(1-i) = N(1+i) = 2$, och enligt sats 8.2 är $1+i$ och $1-i$ Gaussiska primtal.

För fallet där $p \equiv 1 \pmod 4$, finns enligt sats 7.3, heltal a och b sådana att $p = a^2 + b^2$. Man kan faktoriseras högerledet till $(a+bi)(a-bi)$, vilket visar att p inte är Gaussiskt primtal. Eftersom $N(a+bi) = N(a-bi) = p$ följer av sats 8.2, att talen $a+bi$ och $a-bi$ måste vara Gaussiska primtal.

□

Vi har kommit fram till att ett primtal p på formen $4k+3$ för något heltal k är även primtal i den större ringen $\mathbb{Z}[i]$. I exempel 8.4 såg vi att tal som är associerad med $(1+i)$ är Gaussiska primtal. Det primtal som har formen $4k+1$ för något heltal k och $p = a^2 + b^2$, kan faktoriseras till två Gaussiska heltal som måste vara primtal i $\mathbb{Z}[i]$. Vi kan sammanfatta Gaussiska primtal enligt nedan i tre typer:

1. Element som är associerade med $1+i$.
2. Element som är associerade med primtal p, om $p \equiv 3 \pmod 4$.
3. Element $a+bi$, där a och b är heltal med $p = a^2 + b^2$ är primtal, med $p \equiv 1 \pmod 4$.

Nu skall vi undersöka om det finns några andra Gaussiska primtal.

För detta endamål, låter vi w i $\mathbb{Z}[i]$ vara ett Gaussiskt primtal. Vi ska visa att w antingen är associerat med ett vanligt primtal på formen $4k+3$, eller $N(w)$ är ett primtal.

Vi antar att $p \mid N(w)$, där p är primtal på formen $4k+3$ för någon $k \in \mathbb{Z}$. Enligt sats 8.5, är p ett Gaussiskt primtal. Eftersom $p \mid N(w) = w\overline{w}$, måste p dela antingen w eller $\overline{w}$. Låt oss att titta på fallet där $p \mid w$. Eftersom det Gaussiska primtalet w saknar icke-triviala faktorisering, så är p och w associerade.

Fallet där $p \mid \overline{w}$, så har man $ps = \overline{w}$ för något s i $\mathbb{Z}[i]$. Eftersom $p\overline{s} = \overline{p}\ \overline{s} = \overline{ps} = w$, och återigen får vi att p och w associerade. Alltså vi har visat att w är associerat med ett vanlig primtal på formen $4k+3$.

Vi antar nu att $N(w)$ har en primtalsfaktor p som inte är på formen $p = 4k+3$. Vi låter att $p = s\overline{s}$, där normen av både $s = a+bi$ och $\overline{s}$, är ett primtal p, och $p \mid N(w) = w\overline{w}$, således $s \mid w\overline{w}$, så antingen $s \mid w$ eller $s \mid \overline{w}$. I båda fallen är w associerat med ett tal $a+bi$, där $a, b \in \mathbb{Z}$ och $p = a^2 + b^2$. Alltså är $N(w) = p$ är ett primtal.

Därmed har vi visat att det inte finna flera andra Gaussiska primtal utöver de tre ovannämnda typer.

9 Faktorisering av Gaussiska heltal

I det förra avsnittet bekantade vi oss med Gaussiska primtal. Nu skall vi se hur man kan faktorisera ett Gaussiskt heltal. Vi gör ett exempel som visar principerna för hur sådana faktoriseringar går till.

Exempel 9.1. Vi ska primfaktorisera det Gaussiska heltalet $z = 17+331i$. Vi börjar med att beräkna normen av z och primfaktorisera den. Vi får,

$$N(z) = N(17 + 331i) = 17^2 + 331^2 = 109850 = 2 \cdot 5^2 \cdot 13^3.$$

Normens primtalfaktorer kan faktoriseras i $\mathbb{Z}[i]$ och vi får,

$$2 = -i(1 + i)^2, \qquad 5 = (2 - i)(2 + i), \qquad \text{och} \qquad 13 = (3 - 2i)(3 + 2i).$$

Detta ger alla möjliga tänkbara primfaktorer till z, ty $N(z) = z\overline{z}$ så $z \mid 2 \cdot 5^2 \cdot 13^3$. Det betyder att z kan primtalfaktoriseras för något enhet q i $\mathbb{Z}[i]$, som

$$z = q(1 + i)^a(2 + i)^b(2 - i)^c(2 + 3i)^d(2 - 3i)^e, \tag{9.2}$$

för naturliga tal a, b, c, d och e.

För att veta vilka av de faktorerna som verkligen är primfaktorer till z fortsätter vi enligt följande. Beräknar vi normen av båda sidor i (9.2), får vi

$$2 \cdot 5^2 \cdot 13^3 = 2^a \cdot 5^{b+c} \cdot 13^{d+e},$$

så $a = 1$, $b + c = 2$ och $d + e = 3$. Vi får första faktorn $1 + i$ av $a = 1$. Vi fortsätter till nästa faktorn, alltså $(2 + i)^b(2 - i)^c$, där $b + c = 2$. Här får vi tre möjliga fall. Fallet $b = c = 1$ är omöjligt eftersom $(2 + i)(2 - i) = N(2 + i) = 5$, men talet z är inte delbart med 5, så antingen är $b = 0$ eller $c = 0$. Vi avgör om z är delbart med $2 + i$ eller $2 - i$ genom prövning.

$$\frac{17 + 331i}{2 - i} = \frac{(17 + 331i)(2 + i)}{(2 - i)(2 + i)} = \frac{-277 + 679i}{5} \notin \mathbb{Z}[i].$$

Eftersom talet $17 + 331i$ inte är delbart med $2 - i$, så måste $17 + 331i$ vara delbart med $2 + i$, så vi har $b = 2$ och $c = 0$.

Samma procedur gäller för faktorn $(2 + 3i)^d(2 - 3i)^e$. Med samma resonemang som tidigare om normen, fall $d = 1$ och $e = 2$ liksom $d = 2$ och $e = 1$ utesluts, så antingen måste $d = 0$ eller $e = 0$. Vi testar om z är delbart med $2 + 3i$ eller $2 - 3i$ genom prövning:

$$\frac{17 + 331i}{2 + 3i} = \frac{(17 + 331i)(2 + 3i)}{(2 - 3i)(2 - 3i)} = \frac{1027 + 661i}{13} = 79 + 47i \in \mathbb{Z}[i].$$

Eftersom talet $17+331i$ är delbart med $2+3i$, så vi har $d = 3$ och $e = 0$. Beräknar vi alla primfaktorer som vi har fått ihop, får vi $z = q(1+i)(2+i)^2(2+3i)^3 = q(-17-331i)$. Detta bestämmer $q = -1$ i $\mathbb{Z}[i]$. Slutligen får vi primtalsfaktoriseringen,

$$z = 17 + 331i = -1(1 + i)(2 + i)^2(2 + 3i)^3.$$

.

Referenser

[1] John R. Durbin, *Modern algebra, an introduction*, 3:rd edition, John Wiley & sons, 1992

[2] Keith Conrad, The Gaussian integers, (hämtad 2019-11-16)

[3] Rikard Bøgvad, Qimh Xantcha, Håkan Granath, *Algebra 1*, 10:e tryckningen, Stockholms universitet, 2018

[4] Per-Anders Svensson, *Abstrakt algebra*, 1:a upplagan, Studentlitteratur, 2001

[5] Wikipedia, Ring (mathematics), (hämtad 2020-01-18)

[6] Wikipedia, Abstract Algebra, (hämtad 2020-02-08)

[7] Wikipedia, Fermat's theorem sum of two squares, (hämtad 2020-04-27)

[8] Wikipedia, Gaussian integer, (hämtad 2020-01-25)