POLYNOM OCH GAUSSISKA HELTAL

Material till Diskret Matematik (SF1662),
Petter Brändén, KTH, 2018.

1. Ringar

Kom ihåg att en *ring* $(R, +, \cdot)$ är en mängd R tillsammans med två operationer *addition* $+$ och *multiplikation* $\cdot$, sådana att

- $(R, +)$ är en abelsk grupp (med identitetselement 0),
- multiplikationen är *associativ*, dvs
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
för alla $a, b, c \in R$,
- multiplikationen är *distributiv*, dvs
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{och} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$
för alla $a, b, c \in R$.

Ringen R kallas *kommutativ* om

$$a \cdot b = b \cdot a,$$

för alla $a, b \in R$. Vi säger att ringen R har en *etta* om det finns ett element i R, som vi benämner 1, som fungerar som en "vanlig etta", dvs

$$1 \cdot a = a \cdot 1 = a,$$

för alla $a \in R$.

Bekanta exempel på kommutativa ringar med etta är $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ och polynomringarna $(K[x], +, \cdot)$ i nästa avsnitt.

Precis som för $\mathbb{Z}$ säger vi att ett element $d \in R$ *delar* ett element $a \in R$ om det finns ett element $b \in R$ sådant att $a = d \cdot c$. Vi skriver då $d \mid a$.

Ett element a i en kommutativ ring R med etta är *inverterbart* om det finns ett element $b \in R$ sådant att

$$a \cdot b = 1.$$

De inverterbara elementen kallas också för *enheter*. I $\mathbb{Z}$ är endast 1 och -1 enheter. I $\mathbb{Z}_n$ är a inverterbart om och endast om $\text{sgd}(a, n) = 1$. I $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ och $\mathbb{Z}_p$, där p är ett primtal, är alla element förutom 0 enheter, dvs, dessa ringar är *kroppar*.

Ett element a i en kommutativ ring R med etta är *reducibelt* om vi kan skriva

$$a = b \cdot c$$

där varken b eller c är enheter. Ett element $a \in R$ är *irreducibelt* om det varken är reducibelt eller en enhet.

De irreducibla elementen i $\mathbb{Z}$ är precis alla p och $-p$, där p är ett primtal.

Vi ska i den här texten ge två exempel på ringar som delar en viktig egenskap som $\mathbb{Z}$ har, nämligen *entydig faktorisering*. Dessa ringar är polynomringar över kroppar och Gaussiska heltal.

2. Polynomringar

I detta kapitel betraktar vi polynom över en K. Kroppen K kan t. ex. vara

$\mathbb{Q}$: de rationella talen

$\mathbb{R}$: de reella talen, eller

$\mathbb{Z}_p$: heltalen modulo p, där p är ett primtal.

Ett *polynom* f över en kropp K är ett uttryck (serie) på formen

$$f = f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

där $a_0, a_1, \ldots, a_n \in K$ och $n \in \mathbb{N}$. Vi tolkar $0x^k = 0$ för alla $k \in \mathbb{N}$, så att $2+3x+0x^2$ är samma polynom som $2 + 3x$. Mängden av alla polynom över K betecknas med $K[x]$. Vi definerar nu addition och multiplikation av två polynom $f, g \in K[x]$. Genom att fylla ut med eventuella termer av formen $0x^k$ kan vi antaga att polynomen är på formen $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ och $g = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$. Addition, $f + g$ och multiplikation fg defineras av

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n, \text{ och}$$
$$fg = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n},$$

där koefficienten framför x^m i fg är

$$\sum_{k=0}^{m} a_k b_{m-k}.$$

Exempel 1. I $\mathbb{Z}_5[x]$,

$$\begin{aligned}(2 + 2x) + (2 + 3x + 3x^2) &= (2 + 2) + (2 + 3)x + (0 + 3)x^2 \\ &= 4 + 3x^2\end{aligned}$$

och

$$\begin{aligned}(2 + 2x)(2 + 3x + 3x^2) &= (2 \cdot 2) + (2 \cdot 3 + 2 \cdot 2)x + (2 \cdot 3 + 2 \cdot 3)x^2 + (2 \cdot 3)x^3 \\ &= 4 + 2x^2 + x^3.\end{aligned}$$

Polynomet $0 + 0x + 0x^2 + \cdots$ betecknas med 0. Med operationerna ovan är $K[x]$ en kommutativ ring med

$$0 + f = f + 0 = f \quad \text{och} \quad 1 \cdot f = f \cdot 1 = f,$$

för alla $f \in K[x]$. Enheterna i $K[x]$ är $K \setminus \{0\}$.

Graden för ett polynom $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$, där $f \neq 0$, är det största talet k sådant att $a_k \neq 0$. Graden för polynomet 0 defineras som $-\infty$. Vi betecknar graden för f med $\deg f$.

Liksom för heltalen så har vi en divisionsalgoritm för polynom. I gymnasiematten kallas den för *liggande stolen* eller *trappan*.

Sats 1 (Divisionsalgoritmen)**.** *Om $f, g \in K[x]$ och $g \neq 0$, så finns unika polynom q och r sådana att*

$$f = gq + r, \qquad \textit{där } \deg r < \deg g.$$

Bevis. Vi bevisar först existensen av q och r. Beviset följer precis liggande stolen (trappan).

Om $\deg f < \deg g$ så duger $q = 0$ och $r = f$. Antag att $\deg f \geq \deg g$, $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ och $g = b_m x^m + a_{m-1}x^{m-1} + \cdots + b_0$, där $a_n \neq 0$ och $b_m \neq 0$. Då kan vi uttrycka f som

$$f = a_n b_m^{-1} x^{n-m} g + (f - a_n b_m^{-1} x^{n-m} g).$$

Låt nu $q_1 = a_n b_m^{-1} x^{n-m}$ och $f_1 = f - a_n b_m^{-1} x^{n-m} g$ och notera att $\deg f_1 < \deg f$. Således

$$f = q_1 g + f_1, \quad \text{där} \quad \deg f_1 < \deg f.$$

Om $\deg f_1 < \deg g$ så kan vi låta $f_1 = r$ och vi är klara. Annars (om $\deg f_1 \geq \deg g$) så upprepar vi proceduren tills vi får $\deg f_k < \deg g$:

$$\begin{aligned} f &= q_1 g + f_1, \quad \text{där} \quad \deg f_1 < \deg f, \\ f_1 &= q_2 g + f_2, \quad \text{där} \quad \deg f_2 < \deg f_1, \\ &\vdots \\ f_{k-1} &= q_k g + f_k, \quad \text{där} \quad \deg f_k < \deg g. \end{aligned}$$

Då är $f = (q_1 + q_2 + \cdots + q_k)g + f_k$, där $\deg f_k < \deg g$, så vi kan låta

$$q = q_1 + q_2 + \cdots + q_k \quad \text{och} \quad r = f_k.$$

Det återstår att visa unikheten av q och r. Antag att vi kan skriva

$$f = qg + r = \tilde{q}g + \tilde{r}, \quad \text{där } \deg(r) < \deg g \text{ och } \deg(\tilde{r}) < \deg g.$$

Då är

$$(q - \tilde{q})g = r - \tilde{r}.$$

Vänsterledet är antingen lika med 0 eller av grad minst $\deg g$ och graden för högerledet är mindre än $\deg g$. Därför är högerledet 0, så $q = \tilde{q}$ och $r = \tilde{r}$. □

Vi har alltså att g delar f om och endast om $r = 0$ i Sats 1.

Ett polynom $f \in K[x]$ kallas *moniskt* om ledande koefficienten är lika med 1, dvs om $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. Precis som för heltal finns alltid en unik *största gemensam delare* till två givna polynom $f, g \in K[x]$ (förutsatt att båda inte är lika med 0). Den största gemensamma delaren betecknas $\operatorname{sgd}(f, g)$. Vi formulerar det som en sats:

Sats 2. *Om $f, g \in K[x]$ inte båda är lika med 0, så finns ett unikt moniskt polynom $d \in K[x]$ sådant att*

(1) *$d \mid f$ och $d \mid g$, samt* *(gemensam delare)*
(2) *om $c \in K[x]$ är sådant att $c \mid f$ och $c \mid g$, så $c \mid d$.* *(största)*

Polynomet d kallas största gemensamma delaren till f och g och betecknas $\operatorname{sgd}(f, g)$.

Beviset är analogt med motsvarande bevis gällande heltal och använder sig av Euklides algoritm. Låt $D(f, g)$ vara mängden av gemensamma delare till f och g, dvs

$$D(f, g) = \{h \in K[x] \mid \quad h \mid f \text{ och } h \mid g\}.$$

Notera att $D(f, 0) = \{h \in K[x] \mid \quad h \mid f\}$, dvs mängden av all delare till f. Precis som för heltal gäller

$$D(f, g) = D(f - qg, g) = D(f, g - qf) \tag{1}$$

för alla $f, g, q \in K[x]$.

Bevis av Sats 2. Vi visar först existensen av d genom att använda oss av divisionsalgoritmen och (1). Vi fortsätter att dela tills vi får en rest som är lika med 0.

$$\begin{aligned}
f &= q_1 g + r_1, && \text{där} \quad \deg r_1 < \deg f, && \Rightarrow D(f,g) = D(g,r_1)\\
g &= q_2 r_1 + r_2, && \text{där} \quad \deg r_2 < \deg r_1, && \Rightarrow D(g,r_1) = D(r_1,r_2)\\
r_1 &= q_3 r_2 + r_3, && \text{där} \quad \deg r_3 < \deg r_2, && \Rightarrow D(r_1,r_2) = D(r_2,r_3)\\
&\vdots\\
r_{k-2} &= q_k r_{k-1} + r_k, && \text{där} \quad \deg r_k < \deg r_{k-1}, && \Rightarrow D(r_{k-2},r_{k-1}) = D(r_{k-1},r_k)\\
r_{k-1} &= q_{k+1} r_k + 0. && && \Rightarrow D(r_{k-1},r_k) = D(r_k,0)
\end{aligned}$$

Antag nu att $r_k = a_0 + a_1 x + \cdots + a_n x^n$. Vi ser att $D(f,g) = D(r_k,0)$ så att $\operatorname{sgd}(f,g) = a_n^{-1} \cdot r_k$, eftersom vi kräver att sgd ska vara monisk. □

Genom att gå baklänges i Euklides algoritm (precis som för $\mathbb{Z}$) har vi:

Sats 3 (Bezouts sats)**.** *Om $f, g \in K[x]$ inte båda är lika med 0, så finns polynom $a, b \in K[x]$ sådana att*

$$\operatorname{sgd}(f,g) = a \cdot f + b \cdot g.$$

Med samma bevis som för $\mathbb{Z}$ får vi följande sats.

Sats 4. *Varje polynom $f \in K[x]$, som inte är en konstant, kan skrivas som*

$$f = a \cdot p_1 \cdot p_2 \cdots p_k, \tag{2}$$

där $a \in K$ är en nollskild konstant och $p_1, \ldots, p_k$ är moniska irreducibla polynom.
Uttrycket (2) är unikt, dvs om

$$f = b \cdot q_1 \cdot q_2 \cdots q_\ell,$$

där $b \in K$ är en nollskild konstant och $q_1, \ldots, q_\ell$ är moniska irreducibla polynom, så är $\ell = k$, $b = a$ och vi kan omnumrera $q_1, \ldots, q_k$ så att $q_i = p_i$ för alla $1 \le i \le k$.

För varje $K[x]$ och $a \in K$ gäller att $x - a$ är irreducibelt i $K[x]$. Faktorsatsen ger oss ett kriterium för när $(x-a) \mid f$.

Sats 5 (Faktorsatsen)**.** *Låt $f(x) \in K[x]$ och $a \in K$. Då är $f(a) = 0$ om och endast om $(x-a) \mid f(x)$.*

Bevis. Enligt divisionsalgoritmen är $f(x) = (x-a)q(x) + r(x)$ där $\deg r(x) < 1$, dvs $r(x) = r$ är en konstant. Om vi låter $x = a$, ser vi att

$$f(a) = r,$$

så $(x-a) \mid f$ om och endast om $f(a) = 0$. □

Exempel 2. Faktorisera polynomet $f(x) = x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ i irreducibla faktorer. Eftersom $f(1) = 0$ så är $x - 1 = x + 1$ en faktor. Vi delar $f(x)$ med divisionsalgoritmen (gör det) och får $f(x) = (x^3+1)(x+1)$. Polynomet $x^3 + 1$ har ett nollställe $x = 1$ så vi delar igen med $x + 1$ och får $x^3 + 1 = (x^2 + x + 1)(x + 1)$. Eftersom $x^2 + x + 1$ saknar nollställen så har det ingen faktor av grad 1. Men $x^2 + x + 1$ har grad 2 så det är irreducibelt. Således

$$x^4 + x^3 + x + 1 = (x+1)(x+1)(x^2 + x + 1).$$

Exempel 3. I $\mathbb{Z}_2[x]$ är x och $x+1$ de enda irreducibla polynomen av grad ett. Det finns totalt $2^2 = 4$ polynom av grad 2. De reducibla polynomen av grad 2 är $x \cdot x = x^2$, $x(x+1) = x + x^2$ och $(1+x)(1+x) = 1 + x^2$. Alltså är $1 + x + x^2$ det enda irreducibla polynomet av grad 2.

Det finns totalt $2^3 = 8$ polynom av grad 3. De reducibla polynomen är antingen av formen $(1 + x + x^2)x$, $(1 + x + x^2)(x + 1)$ eller en produkt av endast polynom av grad ett. Således finns exakt $2 + 4 = 6$ reducibla polynom av grad 3 och exakt $8 - 6 = 2$ irreducibla polynom av grad 3. Vilka då?

Hur många irreducibla polynom av grad 4 finns det i $\mathbb{Z}_2[x]$?

Gauss visade att i $\mathbb{C}[x]$ är de enda irreducibla moniska polynomen på formen $x - a$ där $a \in \mathbb{C}$:

Sats 6 (Algebrans fundamentalsats)**.** *Varje icke-konstant polynom $f \in \mathbb{C}[x]$ kan unikt (upp till ordningen av faktorerna) skrivas som*

$$f(x) = a \cdot (x - a_1)(x - a_2) \cdots (x - a_k),$$

där $a \in \mathbb{C}$ är en nollskild konstant och $a_j \in \mathbb{C}$ för alla $1 \leq j \leq k$.

Antag att $f(x) \in \mathbb{R}[x]$ är ett irreducibelt moniskt polynom. Om $f(a) = 0$ för något $a \in \mathbb{R}$, så $(x-a) \mid f(x)$ enligt faktorsatsen, så $f(x) = x - a$ eftersom f antogs vara irreducibelt. Om $f(a) \neq 0$ för alla $a \in \mathbb{R}$ så betrakta samma polynom f i $\mathbb{C}[x]$. Enligt Algebrans fundamentalsats är $f(z) = 0$ för något $z = a + ib \in \mathbb{C} \setminus \mathbb{R}$. Men då är $0 = \overline{f(z)} = f(\overline{z})$. Alltså delas $f(x)$ av polynomet $g(x) = (x - z)(x - \overline{z}) = x^2 - 2ax + (a^2 + b^2)$, vilket är ett reellt polynom. Därför $g(x) \mid f(x)$ och så $f(x) = g(x)$ eftersom $f(x)$ antogs vara irreducibelt. Vi sammanfattar:

Sats 7. *De irreducibla moniska polynomen i $\mathbb{R}[x]$ är precis*

- *$x - a$, där $a \in \mathbb{R}$, och*
- *$q(x) = x^2 + ax + b$, där $q(x)$ saknar reella nollställen.*

Kom ihåg att ett andragradspolynom $x^2 + ax + b$ saknar reella nollställen om och endast om $a^2 < 4b$.

Exempel 4. Betrakta polynomet $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$, där p är ett primtal. Enligt Fermats lilla sats är $f(a) = 0$ för varje $a \in \mathbb{Z}_p \setminus \{0\}$. Därför delar det irreducibla $x - a$ polynomet $f(x)$ för varje $a \in \mathbb{Z}_p \setminus \{0\}$. Eftersom det finns $p - 1$ sådana a och $\deg f(x) = p - 1$ är

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1)) \tag{3}$$

den unika faktoriseringen av $x^{p-1} - 1$ i irreducibla moniska polynom.

Om vi sätter $x = p$ i (3) får vi

$$(p - 1)! \equiv -1 \pmod{p}.$$

Detta resultat heter Wilsons sats.

3. Gaussiska heltal

De Gaussiska heltalen består av följande delmängd (delring) till de komplexa talen

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\},$$

där $i = \sqrt{-1}$ är den imaginära enheten. De Gaussiska heltalen är en kommutativ ring med etta (med den vanliga additionen och multiplikationen i $\mathbb{C}$). Ringen $\mathbb{Z}[i]$

är inte en kropp eftersom inte alla element är inverterbara. T.ex. $2 \in \mathbb{Z}[i]$, men $2^{-1} = 1/2 \notin \mathbb{Z}[i]$.

Kom ihåg att *konjugatet* till ett komplext tal $z = a + ib$ är $\bar{z} = a - ib$. Normen eller längden av ett element $z = a + ib$ i $\mathbb{Z}[i]$ (och i $\mathbb{C}$) är som bekant

$$|z| = \sqrt{z \cdot \bar{z}} = \sqrt{a^2 + b^2}.$$

Därför är $|z| \geq 1$ för alla $z \in \mathbb{Z}[i] \setminus \{0\}$, och $|z| = 1$ precis då $z \in \{1, -1, i, -i\}$. Kom ihåg att om $z, w \in \mathbb{C}$, så är $|z \cdot w| = |z| \cdot |w|$. Så om $z \in \mathbb{Z}[i]$ är inverterbart, så är $1 = |z \cdot z^{-1}| = |z| \cdot |z^{-1}|$, vilket betyder att $z \in \{1, -1, i, -i\}$. De inverterbara elementen i $\mathbb{Z}[i]$ är alltså precis $1, -1, i, -i$.

Nästa resultat är divisionsalgoritmen för $\mathbb{Z}[i]$. Istället, som i fallet med $K[x]$, använda oss a graden av ett polynom så använder vi $|a + ib|^2 = a^2 + b^2$ som ju alltid är ett heltal.

Sats 8 (Divisionsalgoritmen för Gaussiska heltal)**.** *Om $\alpha, \beta \in \mathbb{Z}[i]$ och $\alpha \neq 0$ så finns $\gamma, \rho \in \mathbb{Z}[i]$ sådana att*

$$\beta = \gamma\alpha + \rho$$

där $|\rho|^2 < |\alpha|^2$.

Vi kan till och med välja ρ sådant att $|\rho|^2 \leq |\alpha|^2/2$.

Bevis. Betrakta det komplexa talet β/α, vilket vi kan skriva som

$$\frac{\beta}{\alpha} = a + ib,$$

där $a, b \in \mathbb{Q}$. Välj heltal a', b' sådana att $|a - a'| \leq 1/2$ och $|b - b'| \leq 1/2$ och låt

$$\gamma = a' + ib' \quad \text{och} \quad \rho = \beta - \gamma\alpha.$$

Då är

$$\left|\frac{\beta}{\alpha} - \gamma\right|^2 = |(a - a') + i(b - b')|^2 = (a - a')^2 + (b - b')^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

så

$$|\rho|^2 = |\beta - \gamma\alpha|^2 = \left|\left(\frac{\beta}{\alpha} - \gamma\right)\alpha\right|^2 = \left|\frac{\beta}{\alpha} - \gamma\right|^2 |\alpha|^2 \leq \frac{1}{2}|\alpha|^2.$$

□

Notera att kvoten γ och resten ρ i divisionsalgoritmen för $\mathbb{Z}[i]$ inte är unika.

Exempel 5. Låt $\beta = 27 - 23i$ och $\alpha = 8 + i$. Då är

$$\frac{\beta}{\alpha} = \frac{\beta\overline{\alpha}}{\alpha\overline{\alpha}} = \frac{(27 - 23i)(8 - i)}{|\alpha|^2} = \frac{193}{65} - \frac{211}{65}i.$$

Eftersom $193/65 = 2.969...$ och $-211/65 = -3.246...$, så väljer vi $\gamma = 3 - 3i$. Då är

$$\rho = \beta - \gamma\alpha = 27 - 23i - (3 - 3i)(8 + i) = -2i.$$

Så $27 - 23i = (3 - 3i)(8 + i) + (-2i)$ och $4 = |-2i|^2 < |8 + i|^2 = 65$.

Vi säger att $z = a + ib \in \mathbb{C}$ är på *standardform* om $a > 0$ och $b \geq 0$. Om $\alpha = a + ib \neq 0$ så är precis ett av elementen

$$\{\alpha, -\alpha, i\alpha, -i\alpha\} = \{a + ib, -a - bi, -b + ai, b - ai\}$$

på standardform.

Eftersom vi har en divisionsalgoritm för $\mathbb{Z}[i]$ kan vi med Euklides algoritm visa existensen och unikheten av största gemensamma delare. Beviset är precis likadant som för heltal och polynom.

Sats 9. *Om $\alpha, \beta \in \mathbb{Z}[i]$ inte båda är lika med 0 så finns ett unikt element $\delta \in \mathbb{Z}[i]$ sådant att*

(1) *$\delta \mid \alpha$ och $\delta \mid \beta$, och* *(gemensam delare)*
(2) *om $\gamma \in \mathbb{Z}[i]$ är sådant att $\gamma \mid \alpha$ och $\gamma \mid \beta$, så $\gamma \mid \delta$, och* *(största)*
(3) *δ är på standardform.* *(unikt)*

Elementet δ kallas största gemensamma delaren till α och β och betecknas $\operatorname{sgd}(\alpha, \beta)$.

Exempel 6. Hitta $\operatorname{sgd}(11+3i, 1+8i)$. Vi utför Euklides algoritm.

$$\begin{aligned} 11+3i &= (1-i)(1+8i) + (2-4i) \qquad \text{(utför beräkningarna!)} \\ 1+8i &= (-1+i)(2-4i) + (-1+2i) \\ 2-4i &= (-2)(-1+2i) + 0 \end{aligned}$$

Den sista nollskilda resten är $-1+2i$, men den är inte på standardform så vi multiplicerar med det inverterbara elementet $-i$ och får $\operatorname{sgd}(11+3i, 1+8i) = 2+i$.

Genom att gå baklänges i Euklides algoritm (precis som för $\mathbb{Z}$) har vi:

Sats 10 (Bezouts sats)**.** *Om $\alpha, \beta \in \mathbb{Z}[i]$ inte båda är lika med 0, så finns $\gamma, \kappa \in \mathbb{Z}[i]$ sådana att*

$$\operatorname{sgd}(\alpha, \beta) = \gamma \cdot \alpha + \kappa \cdot \beta.$$

Exempel 7. Om $\alpha = 11+3i$ och $\beta = 1+8i$, då är enligt Exempel 6

$$\begin{aligned} -1+2i &= (1+8i) - (-1+i)(2-4i) \\ &= \beta - (-1+i)(\alpha - (1-i)\beta) \\ &= (1 + (-1+i)(1-i))\beta - (-1+i)\alpha \\ &= (1-i)\alpha + (1+2i)\beta. \end{aligned}$$

Så

$$\begin{aligned} \operatorname{sgd}(\alpha, \beta) = 2+i &= -i(-1+2i) = -i((1-i)\alpha + (1+2i)\beta) \\ &= (-1-i)\alpha + (2-i)\beta. \end{aligned}$$

De irreducibla elementen i $\mathbb{Z}[i]$ kallas för *Gaussiska primtal*. Senare, i Sats 13, ska vi fullständigt beskriva dessa.

Med samma bevis som för $\mathbb{Z}$ får vi följande sats.

Sats 11. *Varje nollskilt $\alpha \in \mathbb{Z}[i]$ kan skrivas som*

$$\alpha = u \cdot \pi_1 \cdot \pi_2 \cdots \pi_k, \tag{4}$$

där $u \in \{1, -1, i, -i\}$ och $\pi_1, \ldots, \pi_k$ är Gaussiska primtal på standardform.

Uttrycket (4) *är unikt, dvs om*

$$\alpha = v \cdot \sigma_1 \cdot \sigma_2 \cdots \sigma_\ell,$$

där $v \in \{1, -1, i, -i\}$ och $\sigma_1, \ldots, \sigma_\ell$ är Gaussiska primtal på standardform, så är $\ell = k$, $v = u$ och vi kan omnumrera $\sigma_1, \ldots, \sigma_k$ så att $\sigma_i = \pi_i$ för alla $1 \le i \le k$.

Inte alla vanliga primtal är Gaussiska primtal. T. ex.

$$2 = (1+i)(1-i), \quad 5 = (2+i)(2-i), \quad 13 = (2+3i)(2-3i).$$

Enligt följande sats är ett primtal p ett Gaussiskt primtal om och endast om $p \equiv 3 \mod 4$. T.ex. $3, 7, 11$ och 19.

Sats 12. *Låt p vara ett primtal i $\mathbb{Z}$. Följande påståenden är ekvivalenta:*

(1) $p = a^2 + b^2$ *för några* $a, b \in \mathbb{Z}$,
(2) $p = 2$ *eller* $p \equiv 1 \mod 4$,
(3) *Ekvationen* $x^2 + 1 = 0$ *har en lösning i* $\mathbb{Z}_p$,
(4) p *är ej ett Gaussiskt primtal.*

Bevis. Vi bevisar (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2): Antag att $p = a^2 + b^2$ är ett primtal. Eftersom $0^2 = 0, 1^2 = 1, 2^2 = 0, 3^2 = 1$ i $\mathbb{Z}_4$, så är summan av två kvadrater lika med $0, 1$ eller 2 i $\mathbb{Z}_4$. Så antingen är p jämn och då är $p = 2$, eller så är p udda och då är $p \equiv 1 \mod 4$, eftersom $p \equiv 3 \mod 4$ är uteslutet.

(2) $\Rightarrow$ (3): Om $p = 2$ är $x = 1$ en lösning, så antag att $p \equiv 1 \mod 4$, dvs $p = 4k + 1$ för något positivt heltal k.

Enligt Exempel 4 har ekvationen

$$x^{p-1} - 1 = 0$$

exakt $p - 1 = 4k$ rötter i $\mathbb{Z}_p$. Skriv

$$x^{p-1} - 1 = \left(x^{2k}\right)^2 - 1 = (x^{2k} - 1)(x^{2k} + 1) = 0.$$

Ekvationen $x^{2k} - 1 = 0$ har högst $2k$ rötter eftersom graden är $2k$. Därför måste ekvationen $x^{2k} + 1 = 0$ ha minst en rot, säg $a \in \mathbb{Z}_p$. Men då är $x = a^k$ en lösning till $x^2 + 1 = 0$.

(3) $\Rightarrow$ (4): Om $x^2 + 1 = 0$ i $\mathbb{Z}_p$, så finns $x \in \mathbb{Z}$ sådant att

$$p \mid (x^2 + 1) = (x + i)(x - i)$$

i $\mathbb{Z}[i]$. Antag för att få en motsägelse att p är ett Gaussiskt primtal. Då gäller $p \mid (x \pm i)$ enligt Sats 11, dvs $p \cdot (c + di) = x \pm i$ för något $c + di \in \mathbb{Z}[i]$ så $pd = \pm 1$. Men $p > 1$ (eftersom p är ett primtal) vilket är en motsägelse.

(4) $\Rightarrow$ (1): Om p ej är ett Gaussiskt primtal så är $p = \alpha \cdot \beta$ för två icke-inverterbara $\alpha, \beta \in \mathbb{Z}[i]$. Men då är $p^2 = |\alpha|^2 \cdot |\beta|^2$, vilket betyder att $p = |\alpha|^2 = |\beta|^2$. Om $\alpha = a + ib$ är alltså $p = a^2 + b^2$. □

Nu kan vi fullständigt beskriva de Gaussiska primtalen.

Sats 13. *Ett element $\alpha = a + ib \in \mathbb{Z}[i]$ är ett Gaussiskt primtal om och endast om*

(1) $a^2 + b^2 = 2$, *dvs* $\alpha \in \{1 + i, 1 - i, -1 + i, -1 - i\}$, *eller*
(2) $a^2 + b^2 = p$ *är ett primtal i* $\mathbb{Z}$ *sådant att* $p \equiv 1 \mod 4$, *eller*
(3) $\alpha \in \{p, -p, ip, -ip\}$, *där p är ett primtal i* $\mathbb{Z}$ *sådant att* $p \equiv 3 \mod 4$.

Bevis. Antag att $\alpha = a + ib$ är ett Gaussiskt primtal, vilket vi kan antaga är på standardform. Vi kan primtalsfaktorisera $|\alpha|^2$ (i $\mathbb{Z}$):

$$\alpha\overline{\alpha} = p_1 p_2 \cdots p_k$$

Eftersom α är ett Gaussiskt primtal, så måste $\alpha \mid p_j$ för något j. Kalla $p_j = p$. Vi har två fall:

Fall 1: Om $b = 0$, så är a ett positivt heltal eftersom α är på standardform. Eftersom $a \mid p$ så är $a = p$, så $\alpha = p$. Men då är $p \equiv 3 \mod 4$ enligt Sats 12, vilket motsvarar (3).

Fall 2: Om $b \neq 0$, så är $a > 0$ och $b > 0$ eftersom α är på standardform. Eftersom $\alpha \mid p$ finns ett icke-inverterbart element $c + di \in \mathbb{Z}[i]$ sådant att $(a+ib)(c+id) = p$. Men då är

$$p^2 = |p|^2 = |(a+ib)(c+id)|^2 = (a^2+b^2)(c^2+d^2)$$

och eftersom p är ett primtal är $p = a^2 + b^2 = c^2 + d^2$. Enligt Sats 12 är antingen $p = a^2 + b^2 = 2$, vilket motsvarar (1), eller så är $p = a^2 + b^2 \equiv 1 \mod 4$, vilket motsvarar (2). □

Exempel 8. Enligt Sats 12 kan ett primtal p skrivas som en summa av två kvadrater, dvs

$$p = a^2 + b^2, \qquad \text{för några } a, b \in \mathbb{Z}, a, b > 0, \tag{5}$$

om och endast om $p = 2$ eller $p \equiv 1 \mod 4$. Enligt Sats 13 är då $a+ib$ ett Gaussiskt primtal på standardform. Notera att

$$p = a^2 + b^2 = (a+ib)(a-ib) = (-i)(a+ib)(b+ia).$$

Den *unika* faktoriseringen av p i $\mathbb{Z}[i]$ är då

$$p = (-i)(a+ib)(b+ia).$$

Detta betyder att p endast kan skrivas på ett sätt som en summa av två kvadrater, dvs att a, b i (5) är unika. T. ex.

$$2 = 1^2 + 1^2 = (-i)(1+i)(1+i), \quad 5 = 1^2 + 2^2 = (-i)(1+2i)(2+i),$$
$$13 = 2^2 + 3^2 = (-i)(2+3i)(3+2i), \quad 17 = 1^2 + 4^2 = (-i)(1+4i)(4+i).$$

Hur finner vi den unika Gaussiska primtalsfaktoriseringen av ett tal $\alpha \in \mathbb{Z}[i]$? Om $\alpha = u \cdot \pi_1 \cdot \pi_2 \cdots \pi_k$ är den unika faktoriseringen av α och $|\alpha|^2 = p_1 \cdot p_2 \cdots p_\ell$ är primtalsfaktoriseringen av $|\alpha|^2$ (i $\mathbb{Z}$) så är

$$|\alpha|^2 = |\pi_1|^2 \cdot |\pi_2|^2 \cdots |\pi_k|^2 = p_1 \cdot p_2 \cdots p_\ell.$$

Enligt Sats 13 har vi

- Om $p_j = 2$ för något j, så $\pi_{j'} = 1 + i$ för något j'.
- Om $p_j \equiv 1 \mod 4$ för något j, så är $\pi_{j'} = a + ib$ där $a^2 + b^2 = p_j$ för något j'.
- Om $p_j \equiv 3 \mod 4$ för något j, så är $\pi_{j'} = p_j$ för något j.

På detta sätt kan vi få fram faktoriseringen.

Exempel 9. Är $2 + 3i$ ett Gaussiskt primtal? Ja eftersom $|2 + 3i|^2 = 13 \equiv 1 \mod 4$.

Faktorisera $1 + 3i$. Vi har $|1 + 3i|^2 = 10 = 2 \cdot 5$, så enligt ovan observation är

$$1 + 3i = u(1+i)(a+ib),$$

där $a^2 + b^2 = 5$ och u är en enhet. Därför är

$$1 + 3i = u(1+i)(1+2i) \text{ eller } 1 + 3i = u(1+i)(2+i)$$

där u är en enhet. Men $(1+i)(1+2i) = -1 + 3i$ och $(1+i)(2+i) = 1 + 3i$ så

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

är den unika faktoriserngen av $1 + 3i$.

Faktorisera $-15+9i$. Vi noterar först att $-15+9i = 3(-5+3i)$ och 3 är ett Gaussiskt primtal, så 3 ingår i faktoriseringen. Eftersom $|-5+3i|^2 = 34 = 2\cdot 17$ och $17 \equiv 1 \mod 4$, så är

$$-5+3i = u(1+i)(4+i) \text{ eller } -5+3i = u(1+i)(1+4i),$$

där u är en enhet. Vi har $(1+i)(4+i) = 3+5i = (-i)(-5+3i)$ så

$$-15+9i = i\cdot 3\cdot (1+i)\cdot (4+i)$$

är faktoriseringen av $-15+9i$.

4. Mer om unik faktorisering

Vi har sett tre exempel på ringar med entydig faktorisering, nämligen $\mathbb{Z}, K[x]$ och $\mathbb{Z}[i]$. Dessa ingår alla i familjen *Euklidiska ringar*. En Euklidisk ring R är en kommutativ ring med etta som dessutom har en så kallad *Euklidisk valuation*, vilket är en funktion $\nu : R \to \mathbb{N}\cup\{-\infty\}$, som uppfyller

(1) $\nu(s) \in \mathbb{N}$ om $s \in R\setminus\{0\}$ och $\nu(0) = -\infty$,
(2) för alla $s, d \in R$, $d \neq 0$, finns q, $r \in R$ med $s = qd + r$ och $\nu(r) < \nu(d)$,
(3) för alla $s, t \in R\setminus\{0\}$ gäller $\nu(s) \leq \nu(st)$.

De Euklidiska ringarna är alltså de som har en divisionsalgorithm. Ringarna $\mathbb{Z}, K[x]$ och $\mathbb{Z}[i]$ är alltså exempel på Euklidiska ringar. Med samma bevis som ovan kan man enkelt visa att Euklidiska ringar har entydig faktorisering.

Det finns exempel på ringar, som då inte är Euklidiska, där vi inte har entydig faktorisering i irreducibla element. Tag

$$\mathbb{Z}[\sqrt{5}i] = \{a+b\sqrt{5}i : a, b \in \mathbb{Z}\},$$

som är en delring till $\mathbb{C}$. Notera att

$$(a+b\sqrt{5}i)(c+d\sqrt{5}i) = ac - 5bd + (ad+bc)\sqrt{5}i,$$

så $\mathbb{Z}[\sqrt{5}i]$ är sluten under multiplikation. Om $z = a+b\sqrt{5}i$ är en enhet i $\mathbb{Z}[\sqrt{5}i]$, så är

$$1 = |a+b\sqrt{5}i|^2 = a^2 + 5b^2,$$

så $z = \pm 1$. Vi har

$$2\cdot 3 = 6 = (1+i\sqrt{5})\cdot(1-i\sqrt{5}),$$

och vi ska se att $2, 3, 1+i\sqrt{5}$ och $1-i\sqrt{5}$ är irreducibla. Notera att om $z = a+b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ inte är en enhet, så är antingen $|a| \geq 2$ eller $|b| \geq 1$ så $|z|^2 = a^2+5b^2 \geq 4$. Om z är reducibelt så är $z = z_1\cdot z_2$, där z_1 och z_2 ej är enheter. Så $|z|^2 = |z_1|^2\cdot|z_2|^2 \geq 4\cdot 4 = 16$. Men

$$|2|^2 = 4, |3|^2 = 9, |1+i\sqrt{5}|^2 = |1+i\sqrt{5}|^2 = 6,$$

så $2, 3, 1+i\sqrt{5}$ och $1-i\sqrt{5}$ är irreducibla.

Övningsexempel

Två element a och b i en kommutativ ring R med etta säges vara *associerade* om det finns en enhet u i R sådan att $a = u \cdot b$.

1a. Finn $a \in \mathbb{Z}$ så att $87 + 13i$ och $13 + ai$ är associerade i $\mathbb{Z}[i]$.

b. Finn $a, b, c \in \mathbb{Z}_5$ så att $2x^3 + 4x^2 + 3$ och $3x^3 + ax^2 + bx + c$ är associerade i $\mathbb{Z}_5[x]$.

2. Finn ett annat (än 6) element i $\mathbb{Z}[i\sqrt{5}]$ som har (minst) två olika faktoriseringar i irreducibla element.

3a. Finn i $\mathbb{Z}[i]$ $\text{sgd}(-3 + 11i, 8 - i)$ och uttryck den som $a(-3 + 11i) + b(8 - i)$.

b. Finn i $\mathbb{Z}[i]$ $\text{sgd}(1 + 47i, 26 + 12i)$.

4. Faktorisera $17 - 11i$ i irreducibla faktorer i $\mathbb{Z}[i]$, dvs skriv det som en produkt av gaussiska primtal.

5. Faktorisera $f(x) = x^3 + x + 1$ i irreducibla faktorer i $\mathbb{Z}_3[x]$.

6. Om modulär aritmetik i $\mathbb{Z}[i]$. Om $a \in \mathbb{Z}[i]$ kan vi räkna $\pmod a$ i $\mathbb{Z}[i]$ (dvs "räkna som vanligt, men ta resten vid division med a av resultatet") och den resulterande $\mathbb{Z}[i]/(a)$ är en kropp precis om a är ett gaussiskt primtal (liksom $\mathbb{Z}_p$ är en kropp precis om p är ett primtal).
Om elementen i $\mathbb{Z}[i]/(3)$ representeras som $\{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$, vad är $(2 + i) + (2 + 2i)$, $(2 + i)(2 + 2i)$, $-(2 + i)$ och $(1 + 2i)^{-1}$ i $\mathbb{Z}[i]/(3)$?

7. $x^2 + 1$ är ju ett irreducibelt polynom i $\mathbb{R}[x]$.
Om man som i förra uppgiften bildar $\mathbb{R}[x]/(x^2 + 1)$ och tar resterna vid division med $x^2 + 1$ som polynom av grad högst 1, vad är $(ax + b)(cx + d)$ i $\mathbb{R}[x]/(x^2 + 1)$? Vilken känd kropp är isomorf med $\mathbb{R}[x]/(x^2 + 1)$?

8*. Låt $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ och definiera $\nu : \mathbb{Z}[\sqrt{3}] \to \mathbb{N} \cup \{-\infty\}$ enligt $\nu(a + b\sqrt{3}) = |a^2 - 3b^2|$ om $a + b\sqrt{3} \neq 0$, $\nu(0) = -\infty$.

a. Visa att $\nu(\alpha\beta) = \nu(\alpha)\nu(\beta)$ då $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ ($k(-\infty) = -\infty$ för alla $k \in \mathbb{N} \cup \{-\infty\}$).

b. Visa att $\mathbb{Z}[\sqrt{3}]$ med detta ν är en euklidisk ring.

c. Visa att $\alpha \in \mathbb{Z}[\sqrt{3}]$ är en enhet omm $\nu(\alpha) = 1$.

d. Visa att $\alpha \in \mathbb{Z}[\sqrt{3}]$ är irreducibelt om $\nu(\alpha)$ är ett primtal.

e. Verifiera att $(3 + 2\sqrt{3})(4 + \sqrt{3}) = (5 - 2\sqrt{3})(12 + 7\sqrt{3})$ och visa att alla dess faktorer är irreducibla i $\mathbb{Z}[\sqrt{3}]$.

f. Har $\mathbb{Z}[\sqrt{3}]$ entydig faktorisering i irreducibla faktorer?

g.** Finn alla enheter i $\mathbb{Z}[\sqrt{3}]$.

Svar till övningsexemplen

1a. $13 + ai$ skall vara $u(87 + 13i)$ med u en av $1, i, -1, -i$. Enda möjligheten är $u = -i$, så $\boldsymbol{a = -87}$.

b. $3x^3 + ax^2 + bx + c$ måste vara $4(2x^3 + 4x^2 + 3)$, så $\boldsymbol{a = 1,\ b = 0,\ c = 2}$.

2. $\boldsymbol{9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})}$ och eftersom $1 < |3|^2, |2 \pm i\sqrt{5}|^2 < 16$ är alla faktorerna irreducibla element och 3 är uppenbarligen inte associerat med någon faktor i HL (de enda enheterna är ju ± 1).

3a. Euklides algoritm. $\frac{-3+11i}{8-i} = \frac{(-3+11i)(8+i)}{65} = -\frac{-7}{13} + \frac{17}{13}i \approx -1 + i$, $-3 + 11i = (-1 + i)(8 - i) + (4 + 2i)$, $\frac{8-i}{4+2i} = \frac{3}{2} - i \approx 1 - i$, $8 - i = (1 - i)(4 + 2i) + (2 + i)$ och $4 + 2i = 2(2 + i)$ ger $\boldsymbol{\mathrm{sgd}(-3 + 11i, 8 - i) = 2 + i} = (8 - i) + (-1 + i)(4 + 2i) = (8-i)+(-1+i)[(-3+11i)+(1-i)(8-i)] \boldsymbol{= (-1+i)(-3+11i)+(1+2i)(8-i)}$.

b. P.s.s. fås $\boldsymbol{\mathrm{sgd}(1 + 47i, 26 + 12i) = -3 - i}$ (eller $3 + i$ eftersom vi vill ha standardform).

4. $|17 - 11i|^2 = 17^2 + 11^2 = 410 = 2 \cdot 5 \cdot 41$. Faktorn 2 visar att $17 - 11i$ har en faktor $1 + i$ och man får $17 - 11i = (1 + i)(3 - 14i)$. Faktorn 5 visar att $17 - 11i$ (så $3 - 14i$) har en av $2 \pm i$ som faktor. Man finner $2 + i \nmid 3 - 14i$, men $3 - 14i = (2 - i)(4 - 5i)$, där $4 - 5i$ är ett gaussiskt primtal (ty $|4 - 5i|^2 = 41$, ett primtal). Så $\boldsymbol{17-11i = (1+i)(2-i)(4-5i) = (-1)(1+i)(1+2i)(5+4i)}$ är den önskade faktoriseringen.

5. Om $f(x)$ kan faktoriseras utan enheter, måste någon faktor ha grad 1 (eftersom dess grad är 3 och faktorer av grad 0 ju är enheter). Enligt faktorsatsen finns en sådan faktor precis om $f(x)$ har ett nollställe. $f(0) = 1$, men $f(1) = 1 + 1 + 1 = 0$, så $x - 1 = x + 2$ är en faktor. Polynomdivision ger $f(x) = (x + 2)(x^2 + x + 2)$. Om $g(x) = x^2 + x + 2$ kan faktoriseras utan enheter måste den ha ett nollställe (som inte kan vara 0), men $g(1) = 1$, $g(2) = 2$. Den sökta faktoriseringen är alltså $\boldsymbol{f(x) = (x + 2)(x^2 + x + 2)}$.

6. $(2 + i) + (2 + 2i) = 4 + 3i = 1 + 3(1 + i) \equiv_3 1$, så $\boldsymbol{(2 + i) + (2 + 2i) = 1}$.
$(2 + i)(2 + 2i) = 2 + 6i = 2 + 3 \cdot 2i \equiv_3 2$, så $\boldsymbol{(2 + i)(2 + 2i) = 2}$.
$-(2 + i) = -2 - i = 1 + 2i + 3(-1 - i) \equiv_3 1 + 2i$, så $\boldsymbol{-(2 + i) = 1 + 2i}$.
$(1 + 2i)^{-1}$ kan fås med Euklides algoritm (ty $\mathrm{sgd}(3, 1 + 2i) = 1$). Man finner $1 = (-1 - i)(1 + 2i) + 3i = (2 + 2i + 3(-1 - i))(1 + 2i) + 3i = (2 + 2i)(1 + 2i) + 3(1 - 2i)$, vilket ger $(2 + 2i)(1 + 2i) = 1$ och $\boldsymbol{(1 + 2i)^{-1} = 2 + 2i}$ i $\mathbb{Z}[i]/(3)$.

7. Eftersom $(ax+b)(cx+d) = acx^2+(ad+bc)x+bd = (ad+bc)x+(bd-ac)+ac(x^2+1) \equiv_{x^2+1} (ad + bc)x + (bd - ac)$ är $\boldsymbol{(ax + b)(cx + d) = (ad + bc)x + (bd - ac)}$ i $\mathbb{R}[x]/(x^2 + 1)$.
Eftersom också $(ax + b) + (cx + d) = (a + c)x + (b + d)$ ger $\varphi(ax + b) = b + ai$ en isomorfi mellan $\mathbb{R}[x]/(x^2 + 1)$ och $\mathbb{C}$**, de komplexa talen**.

8*a. Visa $(ac + 3bd)^2 - 3(ad + bc)^2 = (a^2 - 3b^2)(c^2 - 3d^2)$, tag $||$ av båda led.

b. Axiomen för en kommutativ ring med etta är uppfyllda i $\mathbb{Z}[\sqrt{3}]$.
ν en euklidisk valuation: (1) klart, (2) $s, d \in \mathbb{Z}[\sqrt{3}]$, $d \neq 0$ ger $\frac{s}{d} = q + (x + y\sqrt{3})$ med $q \in \mathbb{Z}[\sqrt{3}]$, $x, y \in \mathbb{Q}$, där $|x|, |y| \leq \frac{1}{2}$, så $-\frac{3}{4} \leq x^2 - 3y^2 \leq \frac{1}{4}$. Så $s = qd + r$, $r \in \mathbb{Z}[\sqrt{3}]$ och $\nu(r) < \nu(d)$ (som i a.), (3) ur a. ($\nu(t) \geq 1$ om $t \neq 0$).

c. $\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} \in \mathbb{Z}[\sqrt{3}]$ omm $a^2 - 3b^2 = 1$ ($a^2 - 3b^2 = -1$ omöjligt, ty $a^2 \equiv_3 0, 1$).

d. Om $\alpha = \beta\gamma$ och $\nu(\alpha)$ primt är $\nu(\alpha) = \nu(\beta)\nu(\gamma)$ och en av β, γ en enhet.

e. Beräkna och använd d.

f. Ja, enligt b. (I e. är $5 - 2\sqrt{3} = (2 - \sqrt{3})(4 + \sqrt{3})$, $12 + 7\sqrt{3} = (2 + \sqrt{3})(3 + 2\sqrt{3})$.)

g****.** Alla enheter ges av $\pm(2 + \sqrt{3})^n$, $n \in \mathbb{Z}$. ($(2 + \sqrt{3})^{-1} = 2 - \sqrt{3}$.)

(Om $a^2 = 3b^2 + 1$, $a, b \in \mathbb{Z}_+$ och $a_1 + b_1\sqrt{3} = (2 - \sqrt{3})(a + b\sqrt{3})$ är $0 < a_1 < a$, $0 \leq b_1 < b$ och $b_1 = 0$ omm $b = 1$ (så $a = 2$). Induktion över a för enheter med $a, b > 0$.)

Department of Mathematics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden

Email address: pbranden@kth.se