KTH Matematik

KTHs Matematiska Cirkel

Talteori

Andreas Enblom
Alan Sola

Institutionen för matematik, 2008
Finansierat av Marianne och Marcus Wallenbergs Stiftelse

Innehåll

Några ord på vägen

Detta kompendium är skrivet för att användas som litteratur till KTHs Matematiska Cirkel under läsåret 2008–2009 och består av sju avsnitt samt ett inledande avsnitt om mängdlära. Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju träffarna.

Som den mesta matematik på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Övningsuppgifterna är fördelade i två kategorier. De med udda nummer har facit, och syftet med dessa är att eleverna ska kunna räkna dem och på egen hand kontrollera att de förstått materialet. De med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa även dessa uppgifter även om man inte examineras på dem. Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av författarna.

Vi bör också nämna att få av uppgifterna är helt enkla. Kika därför inte i facit efter några få minuter, om du inte löst uppgiften, utan prata först med kompisar eller försök litet till. Alla uppgifter ska gå att lösa med hjälp av informationen i detta kompendium.

KTHs Matematiska Cirkel finansieras av Marianne och Marcus Wallenbergs Stiftelse. Vi tackar Dan Laksov och Roy Skjelnes, båda från Institutionen för Matematik vid KTH, för deras givande kommentarer om denna skrift.

Några ord om Cirkeln

KTHs Matematiska Cirkel, i dagligt tal benämnd Cirkeln, startade 1999. Dess ambition är att sprida kunskap om matematiken och dess användningsområden utöver vad eleverna får genom gymnasiekurser, och att etablera ett närmare samarbete mellan gymnasieskolan och högskolan. Cirkeln skall särskilt stimulera elevernas matematikintresse och inspirera dem till fortsatta naturvetenskapliga studier. Lärarna på cirkeln kan vid behov ge eleverna förslag på ämnen till projektarbeten vid gymnasiet.

Till varje kurs skrivs ett kompendium som distribueras gratis till eleverna. Detta material, liksom övriga uppgifter om KTHs Matematiska Cirkel, finns tillgängligt på

`http://www.math.kth.se/cirkel`

Cirkeln godkänns ofta som en gymnasiekurs eller som matematisk breddning på gymnasieskolorna. Det är upp till varje skola att godkänna Cirkeln som en kurs och det är lärarna från varje skola som sätter betyg på kursen. Lärarna är självklart också välkomna till Cirkeln och många har kommit överens med sin egen skola om att få Cirkeln godkänd som fortbildning eller som undervisning. Vi vill gärna understryka att föreläsningarna är öppna för alla gymnasieelever och lärare.

Vi har avsiktligt valt materialet för att ge eleverna en inblick i matematisk teori och tankesätt och presenterar därför både några huvudsatser inom varje område och bevisen för dessa resultat. Vi har också som målsättning att bevisa alla satser som används om de inte kan förutsättas bekanta av elever från gymnasiet. Detta, och att flera ämnen är på universitetsnivå, gör att lärarna och eleverna kan uppleva programmet som tungt, och alltför långt över gymnasienivån. Meningen är emellertid inte att lärarna och eleverna skall behärska ämnet fullt ut och att lära in det på samma sätt som gymnasiekurserna. Det viktigaste är att eleverna kommer i kontakt med teoretisk matematik och får en inblick i *matematikens väsen*. Vår förhoppning är att lärarna med denna utgångspunkt skall ha lättare att upplysa intresserade elever om KTHs Matematiska Cirkel och övertyga skolledarna om vikten av att låta både elever och lärare delta i programmet.

Några ord om betygssättning

Ett speciellt problem tidigare år har varit betygssättningen. Detta borde emellertid bara vara ett problem om lärarna använder sig av samma standard som de gör när de sätter betyg på ordinarie gymnasiekurser. Om utgångspunkten istället är att eleverna skall få insikt i matematiken genom att gå på föreläsningarna och att eleven gör sitt bästa för att förstå materialet och lösa uppgifterna, blir betygsättningen lättare. Självklart betyder det mycket vad eleverna har lärt av materialet i kursen, men lärarna kan bara förvänta sig att ett fåtal elever behärskar ämnet fullt ut. I det perspektivet blir det lätt att använda de officiella kriterierna:

Godkänd: Eleven har viss insikt i de moment som ingår i kursen och kan på ett godtagbart sätt redovisa valda delar av kursen såväl muntligt som skriftligt. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Väl godkänd: Eleven har god insikt i flera moment från kursen. Eleven kan redovisa dessa moment både skriftligt och muntligt och dessutom uppvisa lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Mycket väl godkänd: Eleven har mycket god insikt i flera moment av kursen och lämnar skriftliga redovisningar av flera delar av kursen eller lämnar lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Det är också möjligt att skolorna samarbetar, så elever från en skola redovisar eller lämnar rapport för en lärare i en annan skola.

Författarna, september 2008

0 Mängdlära

0.1 Mängder

Låt oss börja med att titta på ett av de mest grundläggande begreppen i matematiken, nämligen mängder. En mängd är en samling matematiska objekt, som till exempel tal, och dessa objekt kallar vi för *element* i mängden. Det enklaste sättet att beskriva en mängd är att räkna upp dess element. Ett sådant exempel är

$$A = \{1, 3, a, 7\}.$$

Detta betyder att A är en mängd som innehåller elementen $1, 3, a$ och 7. Ett annat sätt att beskriva en mängd är att skriva $\{x \in D : \text{villkor på } x\}$. Med detta menar man mängden av alla element i D som uppfyller de givna villkoren. Som exempel tar vi

$$B = \{n \in \{1, 2, 3, \ldots\} : n \text{ är udda}\}$$

och

$$C = \{y \in \{1, 2, 3, 4\} : y > 2\}.$$

Mängden B innehåller alla udda positiva heltal, medan C innehåller alla element från mängden $\{1, 2, 3, 4\}$ som är större än 2. Alltså har vi

$$B = \{1, 3, 5, 7, 9, 11, \ldots\} \quad \text{och} \quad C = \{3, 4\}.$$

Vi bryr oss inte om i vilken ordning eller hur många gånger elementen räknas upp och därmed gäller till exempel

$$\{1, 2, 3, 4\} = \{3, 1, 4, 2\} = \{1, 3, 3, 1, 2, 4, 4, 1, 3, 2, 4\}.$$

Om A är en mängd och x är ett element i mängden A så skriver vi $x \in A$ och säger att x *tillhör* A. Exempelvis gäller $17 \in \{n : n \text{ är ett udda heltal}\}$ och $b \in \{a, b, 10, 3\}$. Att ett element x inte tillhör mängden A skrivs $x \notin A$. Den *tomma mängden* innehåller ingenting och betecknas $\varnothing$.

Exempel 0.1.1. Låt $A = \{4, 5, 8, 4711, 12, 18\}$ och $B = \{x \in A : x > 10\}$. Då är $B = \{12, 18, 4711\}$ medan $\{x \in A : x < 3\} = \varnothing$. Vidare har vi att $4 \in A$ men $4 \notin B$. ▲

Definition 0.1.2. Låt A och B vara mängder. Om alla element i mängden A också är element i mängden B så sägs A vara en *delmängd* till B. Detta betecknas $A \subseteq B$.

Exempel 0.1.3. Mängden $\{1, a\}$ är en delmängd till $\{1, 3, a\}$, eftersom alla element i $\{1, a\}$ finns i mängden $\{1, 3, a\}$. Vi skriver $\{1, a\} \subseteq \{1, 3, a\}$. ▲

Definition 0.1.4. Antag att A och B är mängder. *Unionen* av A och B består av de element som ligger i någon av mängderna och betecknas $A \cup B$. *Snittet* av A och B består av de element som ligger i båda mängderna och betecknas $A \cap B$.

Exempel 0.1.5. Låt $A = \{1, 3, 5, 6\}$ och $B = \{5, 8, 3, 4711\}$. Då har vi $A \cup B = \{1, 3, 5, 6, 8, 4711\}$ och $A \cap B = \{3, 5\}$. ▲

Det är dags att titta på några viktiga talmängder. Den mängd vi använder för att räkna föremål är de *naturliga talen* $\{0, 1, 2, 3, \ldots\}$. Denna mängd betecknas $\mathbb{N}$. Tar vi med negativa tal får vi heltalen $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Beteckningen kommer från tyskans *zahl* som betyder tal. Slutligen betecknar vi med $\mathbb{R}$ de *reella talen*, det vill säga alla tal på tallinjen, exempelvis $0, -1, 3/2, -527/3, \sqrt{2}$ och π. Notera att $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}$.

Exempel 0.1.6. Vi har att $\mathbb{N} = \{n \in \mathbb{Z} : n \geqslant 0\}$. ▲

Exempel 0.1.7. Mängden $\{n \in \mathbb{Z} : n = 2 \cdot k \text{ för något } k \in \mathbb{Z}\}$ är mängden av alla jämna heltal. Denna mängd kan också skrivas som $\{2 \cdot k : k \in \mathbb{Z}\}$, eller som $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$. ▲

Exempel 0.1.8. Låt oss påpeka att en mängd även kan ha andra mängder bland dess element. Exempelvis kan vi låta

$$A = \{2, 3, \{-1, 1\}, 4\},$$

och vi har att $\{-1, 1\} \in A$, det vill säga mängden $\{-1, 1\}$ är ett element i mängden A. ▲

0.2 Funktioner

Innan vi gör en allmän definition av vad en funktion är kan det vara på sin plats att titta på något välbekant, nämligen en formel som $f(x) = x^2 + 1$. Detta är ett exempel på en funktion. Formeln säger att om vi tar ett tal $x \in \mathbb{R}$ så får vi ett nytt tal $f(x) \in \mathbb{R}$ genom att göra beräkningen $x^2 + 1$; till exempel får vi $f(2) = 2^2 + 1 = 5$. Vi säger att f är en funktion från de reella talen till de reella talen, eftersom både det vi stoppar in, x, och det vi får ut, $f(x)$, är reella tal. Vi brukar beteckna detta med $f : \mathbb{R} \to \mathbb{R}$.

Definition 0.2.1. Låt X och Y vara mängder. En *funktion* $f : X \to Y$ är ett sätt att till varje element $a \in X$ tilldela ett välbestämt element $b \in Y$. Vi skriver $f(a) = b$. Vi säger att a *avbildas* på b och att b är *bilden* av a.

Anmärkning 0.2.2. Ofta säger man att f är en funktion från X till Y istället för att använda beteckningen $f : X \to Y$. Ett vanligt alternativ till ordet funktion är *avbildning*.

Exempel 0.2.3. Betrakta mängderna $A = \{1, 2, 3\}$ och $B = \{1, 2, \ldots, 100\}$. Ett exempel på funktion $f : A \to B$ ges av $f(n) = 2n$ för $n \in A$. Vi har alltså att $f(1) = 2$, $f(2) = 4$ och $f(3) = 6$. Per definition måste vi ha $f(x) \in B$ för alla $x \in A$, och detta gäller ju här eftersom

$$f(1) = 1 \in B, \quad f(2) = 4 \in B, \quad \text{och} \quad f(3) = 6 \in B.$$

I detta exempel definieras funktionen f av formeln $f(n) = 2n$, men det är inte alls nödvändigt att det finns en formel som beskriver hur funktionen verkar. Om vi som här har en funktion från en den *ändliga* mängden $A = \{1, 2, 3\}$ kan man till exempel definera funktionen med hjälp av en tabell:

n	$f(n)$
1	2
2	4
3	6

▲

Exempel 0.2.4. Låt $h(x) = 3/2 \cdot x^2 - x^3$. Detta definierar en funktion h från $\mathbb{R}$ till $\mathbb{R}$. Vi har exempelvis att

$$h(1) = \frac{1}{2}, \quad \text{och} \quad h(-2) = 14.$$ ▲

0.3 Träning i mängdlära och bevisföring

Här kommer fyra tips på hur man visar saker om mängder:

1. Visa att $x \in A$.

   Här ska man alltså visa att x uppfyller de villkor som definierar vilka element som tillhör mängd A. Om exempelvis $A = \{1, 2, 3\}$ är det uppenbart att $2 \in A$, men om $A = \{x : \text{villkor på } x\}$ så måste man visa att x uppfyller de nämnda villkoren. Om $A = B \cap C$ så måste man visa att $x \in B$ och $x \in C$, medan om $A = B \cup C$ så räcker det att visa att $x \in B$ eller $x \in C$ (eller båda).

2. Visa att $A \subseteq B$.

   Tag ett godtyckligt element $x \in A$. Använd nu definitionen för mängden A för att skriva ner vilka villkor som finns på x. Visa sedan att $x \in B$. Eftersom x var godtyckligt så betyder detta att alla $x \in A$ uppfyller $x \in B$, det vill säga $A \subseteq B$.

3. Visa att $A = B$.

   Vi visar först $A \subseteq B$ och sedan $B \subseteq A$. Då har vi visat att alla element i A ligger i B och att alla element i B ligger i A. Det följer då naturligtvis att $A = B$.

4. Visa att $A = \varnothing$.

   Minns att $\varnothing$ betecknar denna tomma mängden, det vill säga en mängd som inte innehåller några element alls. Det som ska visas är alltså att det inte kan finnas några element i A.

   Antag till att börja med att $x \in A$. Använd definitionen av A för att skriva ner vilka villkor som då ställs på x. Visa att dessa villkor är

omöjliga, det vill säga de leder till en motsägelse. Alltså kan det inte vara så att $x \in A$, oavsett vilket x vi väljer. Alltså innehåller inte A några element.

Låt Ω vara en godtycklig mängd. Vi kommer i följande exempel antaga att alla mängder $A, B, C, \ldots$ är delmängder till Ω. Låt oss göra följande definitioner:

1. $A \setminus B = \{x \in A : x \notin B\}$
2. $A^c = \Omega \setminus A = \{x \in \Omega : x \notin A\}$
3. $A \Delta B = \{x \in \Omega : x \text{ tillhör en av } A \text{ och } B \text{ men inte båda}\}$

Följande åtta exempel har lösningar, men läsaren bör försöka göra bevisen utan att titta på lösningarna först.

Exempel 0.3.1. Visa att $A \setminus B \subseteq A \Delta B$.

Lösning. Tag $x \in A \setminus B$. Det betyder att $x \in A$ och att $x \notin B$. Alltså tillhör x en av A och B, men inte båda, och därmed gäller $x \in A \Delta B$. Eftersom x var godtycklig betyder detta att $x \in A \Delta B$ för alla $x \in A \setminus B$, det vill säga att $A \setminus B \subseteq A \Delta B$. ▲

Exempel 0.3.2. Visa att $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Lösning. Tag $x \in A \Delta B$. Det betyder att x tillhör en av A och B men inte båda. Vi har två fall:

Till att börja med kan $x \in A$ och $x \notin B$. Då gäller per definition $x \in A \setminus B$. Eftersom $A \setminus B$ är en delmängd till $(A \setminus B) \cup (B \setminus A)$ så gäller även $x \in (A \setminus B) \cup (B \setminus A)$.

Det andra fallet är att $x \in B$ och $x \notin A$, det vill säga att $x \in B \setminus A \subseteq (A \setminus B) \cup (B \setminus A)$.

I båda fallen får vi alltså att $x \in (A \setminus B) \cup (B \setminus A)$, och eftersom x var godtycklig så betyder detta att $A \Delta B \subseteq (A \setminus B) \cup (B \setminus A)$.

Omvänt, tag $x \in (A \setminus B) \cup (B \setminus A)$. Det betyder att $x \in A \setminus B$ eller $x \in B \setminus A$. I båda fallen tillhör x en av A och B men inte båda. Alltså gäller $x \in A \Delta B$. Eftersom x var godtycklig så följer det att $(A \setminus B) \cup (B \setminus A) \subseteq A \Delta B$.

Nu har vi visat att $A \Delta B \subseteq (A \setminus B) \cup (B \setminus A)$ och att $(A \setminus B) \cup (B \setminus A) \subseteq A \Delta B$. Det betyder att $A \Delta B = (A \setminus B) \cup (B \setminus A)$. ▲

Exempel 0.3.3. Två mängder B och C sägs vara *disjunkta* om de inte har några gemensamma element. Visa att B och C är disjunkta om och endast om $B \cap C = \varnothing$.

Lösning. Antag att B och C är disjunkta. Antag att $x \in B \cap C$, det vill säga att $x \in B$ och $x \in C$. Men detta betyder att B och C har x som gemensamt element, vilket motsäger att B och C är disjunkta. Alltså måste $B \cap C = \varnothing$.

Omvänt, antag att $B \cap C = \varnothing$. Det betyder att det inte finns något element som tillhör både B och C. Alltså har B och C inga gemensamma element, det vill säga att B och C är disjunkta.

Nu har vi alltså visat två saker, dels att om B och C är disjunkta så gäller $B \cap C = \varnothing$, dels att om $B \cap C = \varnothing$ så är B och C disjunkta. Tillsammans betyder detta att B och C är disjunkta om och endast om $B \cap C = \varnothing$. ▲

Exempel 0.3.4. Visa att A och A^c är disjunkta.

Lösning. Enligt föregående exempel är det vi ska visa att $A \cap A^c = \varnothing$. Antag att $x \in A \cap A^c$. Det betyder att $x \in A$ och att $x \in A^c$. Det senare betyder per definition att $x \notin A$, vilket är en motsägelse. Alltså måste $A \cap A^c = \varnothing$. ▲

Exempel 0.3.5. Symbolen $n!$ definieras som $n! = 1 \cdot 2 \cdot 3 \cdots n$ och kallas *n-fakultet*. Exempelvis har vi att $1! = 1$, $2! = 2$, $3! = 6$ och $5! = 120$. Låt $A_n = \{kn : k = 1, 2, 3, \ldots\}$. Visa att $n! \in A_1 \cap A_2 \cap \cdots \cap A_n$, för varje heltal $n \geqslant 1$, men att $A_1 \cap A_2 \cap A_3 \cap \cdots = \varnothing$.

Lösning. Låt n vara ett heltal med $n \geqslant 1$. Tag ett heltal i med $1 \leqslant i \leqslant n$. Notera att $n! = ki$ där $k = 1 \cdot 2 \cdots (i-2) \cdot (i-1) \cdot (i+1) \cdot (i+2) \cdots (n-1) \cdot n \geqslant 1$. Alltså gäller $n! \in A_i$, och eftersom i var godyckligt så gäller $n! \in A_i$ för alla $i = 1, 2, \ldots, n$, det vill säga $n! \in A_1 \cap A_2 \cap \cdots \cap A_n$. Nu, eftersom n var godtyckligt så gäller $n! \in A_1 \cap \cdots \cap A_n$, för alla heltal $n \geqslant 1$.

Vidare, antag att $x \in A_1 \cap A_2 \cap \cdots$. Det betyder att $x \in A_n$ för alla heltal $n \geqslant 1$. I synnerhet gäller $x \in A_1 = \{1, 2, 3, \ldots\}$, det vill säga x är ett positivt heltal. Låt $m = x + 1$. Då gäller $x < m < 2m < 3m < \cdots$, och i synnerhet $x \neq km$ för $k = 1, 2, \ldots$, så $x \notin A_m$. Men detta motsäger ju att $x \in A_n$ för alla heltal $n \geqslant 1$. Alltså gäller $A_1 \cap A_2 \cap \cdots = \varnothing$. ▲

Övningar

Övning 0.1. Låt $A = \{1, 2, 3, 4, \ldots\}$, $B = \{1, 3, 5, 7, \ldots\}$, $C = \{2, 4, 6, 8, \ldots\}$ och $D = \{1, 4, 19, 36, 101\}$. Bestäm mängderna

1. $B \cup C$,
2. $B \cap C$,
3. $D \cap C$,
4. $\{x \in D : x \in B\}$,
5. $\{x \in A : x = y + 1 \text{ för något } y \in D\}$,
6. $\{x + 1 : x \in D\}$.

Övning 0.2. Låt $\mathbb{N} = \{0, 1, 2, \ldots\}$ och $B_n = \{1, 2, \ldots, n\}$ för $n = 1, 2, 3, \ldots$. Visa att $\mathbb{N} \setminus \{0\} = B_1 \cup B_2 \cup B_3 \cup \cdots$.

Övning 0.3. Låt Ω vara en mängd och $A, B, C \subseteq \Omega$. Visa att

$$((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c).$$

Övning 0.4. Låt Ω vara en mängd och $A \subseteq \Omega$. Visa att $\Omega = A \cup A^c$.

1 Heltal

1.1 Grundläggande egenskaper för heltalen

Heltal är tal som 1, 0, -17 och 4712. Vi kommer som tidigare nämnts att använda beteckningen $\mathbb{Z}$ för heltalen. Detta är alltså den mängd som består av alla heltal:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

När man beskriver matematisk teori, måste man alltid utgå från någonting. Inom talteorin utgår man från heltalen tillsammans med räknesätten addition ($+$) och multiplikation ($\cdot$), samt jämförelserelationerna $<$, $=$ och $>$. Vi bestämmer oss alltså för att ta existensen av heltal, samt addition, multiplikation och jämförelse av dessa, för givna. Det kan påpekas att dessa saker faktiskt kan bevisas, om man utgår från ännu enklare förutsättningar.

> I fortsättningen anses läsaren känna till heltalen $\mathbb{Z}$ samt hur man adderar, multiplicerar och jämför dem.

Det kan vara på sin plats att kommentera räknesätten subtraktion och division. Subtraktion är bara ett specialfall av addition, givet att man vet hur man utifrån ett tal $a \in \mathbb{Z}$ bildar talet $-a$. Vi har ju att

$$3 - 8 = 3 + (-8)$$

så för att kunna utföra subtraktionen med 8 räcker det att känna till addition samt hur man bildar talet -8. Division är lite mer komplicerat och det kommer vi till om en sida eller två.

Trots att alla läsare känner till det om heltal, addition och så vidare som vi förväntar oss, kan det ändå vara intressant att skriva upp några av de allra viktigaste egenskaperna för heltalen, och det görs här, utan bevis:

Sats 1.1.1. *Heltalen $\mathbb{Z}$ tillsammans med operationerna $+$ och $\cdot$ uppfyller följande egenskaper för alla $a, b, c \in \mathbb{Z}$:*

1. $a + b \in \mathbb{Z}$
2. $a \cdot b \in \mathbb{Z}$.
3. $a + b = b + a$
4. $a \cdot b = b \cdot a$.
5. $a + (b + c) = (a + b) + c$.

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
7. $a \cdot (b + c) = a \cdot b + a \cdot c$.
8. *Heltalet* $0 \in \mathbb{Z}$ *uppfyller* $a + 0 = a$.
9. *Heltalet* $1 \in \mathbb{Z}$ *uppfyller* $a \cdot 1 = a$.
10. *För varje heltal* a *finns ett heltal* $-a$ *sådant att* $a + (-a) = 0$.

Av intresse är att notera att om vi har någon godtycklig mängd, antingen $\mathbb{Z}$ eller någon annan mängd, för vilken man definierat några operationer, betecknade med $+$ och $\cdot$, som uppfyller punkterna 1–10 ovan, så kallas den mängden för en *kommutativ ring*, eller ibland *kommutativ talring* eller bara *ring*. Sådana ringar finns det massor av exempel på. Senare ska vi få stifta bekantskap med de *Gaussiska heltalen* som utgör just en kommutativ ring.

Följande egenskaper kan kännas självklara, men är i själva verket några oerhört centrala egenskaper för heltalen. De är tre av de egenskaper som gör tal så unika inom matematiken.

Sats 1.1.2. *För heltalen* $\mathbb{Z}$ *gäller följande:*

1. *Om* $a, b \in \mathbb{Z}$ *så gäller exakt en av* $a < b$, $a = b$ *och* $a > b$.
2. *Om* $k \neq 0$ *är ett heltal och* $a \cdot k = b \cdot k$ *så gäller* $a = b$, *för* $a, b \in \mathbb{Z}$.
3. *Antag att* $A \subseteq \mathbb{Z}$, *att* $A \neq \varnothing$ *samt att det finns en* övre begränsning *för* A, *det vill säga ett tal* $m \in \mathbb{Z}$ *sådant att* $m \geqslant x$ *för alla* $x \in A$. *Då innehåller* A *ett* största element. *Med andra ord finns då ett* $a \in A$ *sådant att* $a \geqslant x$ *för alla* $x \in A$.

Observera att det i punkt 3 *inte* behöver vara så att $m = a$. Talet m behöver inte ligga i mängden A, utan det räcker att det är *någon* övre begränsning för A. Slutsatsen är att det finns en övre begränsning a som ligger i själva mängden A.

Exempel 1.1.3. Låt $A = \{-3, 0, 1, 2, 5, 10, 12\}$. Eftersom exempelvis $57 \geqslant x$ för alla $x \in A$ så är 57 en övre begränsning för A. Talet 12 är ett största element i A eftersom det både är en övre begränsning för A och tillhör A. ▲

1.2 Delbarhet

Av stor vikt inom talteorin är egenskapen för tal att dela andra tal. Exempelvis: eftersom $12 = 4 \cdot 3$ så vet vi att 4 delar 12. Det är just på detta sätt vi definierar *delbarhet*:

Definition 1.2.1. Låt a och b vara heltal. Om det finns ett heltal q sådant att $a = b \cdot q$ så säger vi att b *delar* a, och skriver

$$b \mid a.$$

Om b inte delar a så skriver vi $b \nmid a$.

Exempel 1.2.2. Vi har att

$$3 \mid 24 \quad \text{eftersom} \quad 24 = 8 \cdot 3.$$

Men delbarhet fungerar också för negativa tal. Det gäller att

$$-3 \mid 24 \quad \text{eftersom} \quad 24 = (-8) \cdot (-3).$$

och också att

$$3 \mid -24 \quad \text{samt} \quad -3 \mid -24.$$

Däremot gäller inte $5 \mid 24$. Detta skriver vi alltså som $5 \nmid 24$. ▲

Enligt definitionen av delbarhet delar alla heltal talet 0. Att $0 = a \cdot 0$ innebär ju att $a \mid 0$ för alla $a \in \mathbb{Z}$.

1.3 Division

Nu är det dags att fundera på hur man dividerar heltal. Det är viktigt att tänka på att det är just heltal vi dividerar, och att vi som resultat vill få heltal.

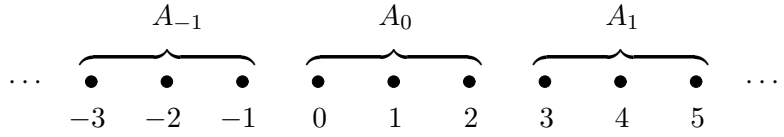
Alla vet att $6/3 = 2$, men var betyder detta egentligen? Och hur utför man divisionen $7/3$ om man bara får använda heltal? Svaren ges av följande sats:

Sats 1.3.1. *Låt a, b vara heltal. Antag att $b > 0$. Då finns unika heltal q och r, där $0 \leqslant r < b$, sådana att*

$$a = b \cdot q + r.$$

Vi skriver inte ner alla detaljer i beviset för denna sats, utan nöjer oss med att beskriva den grundläggande idén.

Bevisidé. För betrakta mängderna $A_n = \{b \cdot n + m \,:\, 0 \leqslant m < b\}$, där $n \in \mathbb{Z}$. För exempelvis $b = 3$ ser mängderna ut så här:



Man inser nu att det för varje $a \in \mathbb{Z}$ finns ett unikt n sådant att $a \in A_n$. Och enligt definitionen av A_n finns ett unikt m med $0 \leqslant m < b$ sådant att $a = b \cdot n + m$. Låt $q = n$ och $r = m$ och saken är klar. □

Satsen säger faktiskt att vi alltid kan utföra det som brukar kallas för *heltalsdivision*. Vi har exempelvis att

$$7 = 3 \cdot 2 + 1,$$

och då säger vi att heltalsdivision av 7 med 3 ger kvoten 2 och resten 1. Termen r i satsen ovan brukar alltså kallas *rest* eller *restterm*.

Men hur är det med divisionssymbolen / då? Vad betyder $6/3 = 2$? Jo, det är helt enkelt så att

$$6 = 3 \cdot 2 + 0$$

och därför kan vi skriva $6/3 = 2$. Så fort ett tal b delar ett tal a, kommer resttermen r i satsen ovan att vara 0, precis som i fallet $a = 6$ och $b = 3$. I sådana fall skriver vi att $q = a/b$.

Definition 1.3.2. Antag att a, b är heltal där $b \neq 0$, och att $b \mid a$. Enligt definitionen av delbarhet finns då ett heltal q sådant att $a = b \cdot q$. Vi kallar q *kvoten mellan* a *och* b och skriver

$$q = \frac{a}{b}.$$

Övningar

Övning 1.1. Hitta talen q och r i formeln $a = b \cdot q + r$, där $0 \leqslant r < b$, i fallen då

1. $a = 32$, $b = 13$,
2. $a = -24$, $b = 7$,
3. $a = 1762$, $b = 10$,
4. $a = 10$, $b = 1726$,
5. $a = -70$, $b = 35$.

Övning 1.2. Låt a och b vara heltal, där $b \neq 0$. Visa att om $a \cdot b = 0$ så måste $a = 0$.

Övning 1.3. Betrakta några heltal a och b, där $b \neq 0$. Antag att heltalen q, r och $\tilde{r}$ uppfyller

$$a = b \cdot q + r \quad \text{och} \quad a = b \cdot q + \tilde{r}.$$

Visa att $r = \tilde{r}$.

Övning 1.4. Låt a och b vara heltal där $b \neq 0$. Antag att det finns heltal $q, \tilde{q}$ och r sådana att

$$a = b \cdot q + r \quad \text{och} \quad a = b \cdot \tilde{q} + r.$$

Visa att $q = \tilde{q}$.

Anmärkning: Detta betyder att kvoten q vid heltalsdivision är unikt bestämd.

Övning 1.5. Visa följande egenskaper hos delarrelationen:

1. För alla heltal a gäller $a \mid a$.
2. Låt a, b, c vara heltal. Om $a \mid b$ och $b \mid c$ så gäller $a \mid c$.
3. Det är inte så att om $a \mid b$ så gäller $b \mid a$, för alla heltal a, b.

2 Gemensamma delare

2.1 Största gemensamma delare

Vi ska nu göra en precis definition av vad vi menar med den *största gemensamma delaren* till två tal. Inutitivt är det klart vad som menas. Betrakta exempelvis talen 8 och 12. Talet 8 har följande positiva delare:

$$1, \quad 2, \quad 4, \quad 8,$$

och talet 12 har följande positiva delare.

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 12.$$

Det största talet som är en delare till både 8 och 12 är alltså 4. Vi säger alltså att 4 är den största gemensamma delaren till 8 och 12, och skriver $4 = \text{sgd}\,(8, 12)$. Låt oss nu göra en allmän definition av detta.

Definition 2.1.1. Låt n vara ett heltal. Betrakta mängden

$$D(n) = \{a \in \mathbb{Z} \,:\, a > 0,\ a \mid n\}.$$

Denna mängd kallar vi *delarmängden till* n.

Mängden $D(n)$ innehåller alltså alla positiva delare till n. Vi har exempelvis att $D(12) = \{1, 2, 3, 4, 6, 12\}$.

Definition 2.1.2. Låt a, b vara heltal, där inte både a och b är 0. Det största talet i mängden $D(a) \cap D(b)$ kallar vi för *den största gemensamma delaren till* a *och* b. Vi betecknar detta tal med $\text{sgd}\,(a, b)$.

När man ger en definition som denna måste man fundera på om mängden $D(a) \cap D(b)$ verkligen innehåller ett största element, för alla val av a och b, så att definitionen har en innebörd. Detta bevisas här:

Sats 2.1.3. *Låt* a *och* b *vara heltal som inte båda är* 0*. Då innehåller mängden* $D(a) \cap D(b)$ *ett största element.*

Bevis. Enligt påstående 3 i Sats 1.1.2 räcker det att visa att $D(a) \cap D(b) \neq \varnothing$ samt att $D(a) \cap D(b)$ har en övre begränsning.

Observera att $1 \in D(n)$ för varje heltal n. Alltså kommer även $1 \in D(a) \cap D(b)$. Detta betyder att $D(a) \cap D(b) \neq \varnothing$.

Att $D(a) \cap D(b)$ har en övre begränsning följer om vi kan visa att minst en av mängderna $D(a)$ och $D(b)$ har en övre begränsning. Vi vet att minst ett av talen a och b inte är 0. Antag utan inskränkning att $a \neq 0$ (fallet $b \neq 0$ hanteras på samma sätt). Låt

$$M = \begin{cases} a & \text{om } a > 0 \\ -a & \text{om } a < 0, \end{cases}$$

Vi väljer alltså M sådant att $M > 0$. Tag ett godtyckligt $x \in D(a)$. Då är x en delare till a, och därmed också en delare till M. Detta betyder att det finns ett tal q sådant att $M = xq$, och eftersom $M > 0$ så måste $x \leqslant M$. Alltså är M en övre begränsning till $D(a)$. □

Definition 2.1.4. Låt a, b vara heltal, inte båda 0. Om $\operatorname{sgd}(a, b) = 1$ så säger vi att a och b är *relativt prima*.

Exempel 2.1.5. Betrakta talen $9 = 3 \cdot 3$, $10 = 2 \cdot 5$, och $12 = 2 \cdot 2 \cdot 3$. Klart är att

$$D(9) = \{1, 3, 9\}, \quad D(10) = \{1, 2, 5, 10\}, \quad D(12) = \{1, 2, 3, 4, 6, 12\}.$$

Alltså gäller

$$\operatorname{sgd}(9, 10) = 1, \quad \operatorname{sgd}(9, 12) = 3, \quad \operatorname{sgd}(10, 12) = 2.$$

Detta betyder att talen 9 och 10 är relativt prima, medan varken 9 och 12 eller 10 och 12 är relativt prima. ▲

Exempel 2.1.6. Det kan vara intressant att fundera på vad största gemensamma delaren till ett positivt tal och 0 är. Låt $a > 0$. Enligt definitionen är det faktiskt så att

$$D(0) = \{1, 2, 3, \ldots\},$$

och därmed får vi

$$D(a) \cap D(0) = D(a).$$

Observera nu att det största talet i $D(a)$ är a, och därför är

$$\operatorname{sgd}(a, 0) = a.$$ ▲

2.2 Euklides algoritm

Sats 2.2.1. *Låt a, b vara heltal där $b \neq 0$. Antag att heltalen p, q uppfyller*

$$a = b \cdot q + r.$$

Då gäller

$$\operatorname{sgd}(a, b) = \operatorname{sgd}(b, r).$$

Bevis. Tag $x \in D(b) \cap D(r)$. Då gäller $x \mid b$ och $x \mid r$. Det betyder att det finns heltal m_1, m_2 sådana att $b = xm_1$ och $r = xm_2$. Vi får att

$$a = bq + r = xm_1q + xm_2 = x(m_1q + m_2).$$

Alltså gäller $x \mid a$ och därmed $x \in D(a)$. Eftersom $x \in D(b)$ så får vi $x \in D(a) \cap D(b)$. Vi har alltså visat att

$$D(b) \cap D(r) \subseteq D(a) \cap D(b).$$

Omvänt, tag $y \in D(a) \cap D(b)$. Då finns heltal k_1 och k_2 sådana att $a = yk_1$ och $b = yk_2$. Nu får vi

$$r = a - bq = yk_1 - yk_2q = y(k_1 - k_2q).$$

Alltså gäller $y \mid r$ och därmed $y \in D(r)$. Eftersom $y \in D(b)$ så följer $x \in D(b) \cap D(r)$. Detta visar att

$$D(a) \cap D(b) \subseteq D(b) \cap D(r).$$

Eftersom vi nu har visat att $D(b) \cap D(r) \subseteq D(a) \cap D(b)$ och $D(a) \cap D(b) \subseteq D(b) \cap D(r)$, så följer

$$D(a) \cap D(b) = D(b) \cap D(r). \qquad \square$$

Denna sats kan användas för att räkna ut största gemensamma delaren till två tal. Denna uträkningsmetod, som här illustreras med ett exempel, brukar kallas *Euklides algoritm*.

Exempel 2.2.2 (Euklides algoritm)**.** Låt oss bestämma $\operatorname{sgd}(6\,396, 525)$. Eftersom

$$6\,396 = 525 \cdot 12 + 96$$

så följer

$$\operatorname{sgd}(6\,396, 525) = \operatorname{sgd}(525, 96).$$

Vidare, vi har att

$$525 = 96 \cdot 5 + 45,$$

och därmed

$$\operatorname{sgd}(525, 96) = \operatorname{sgd}(96, 45).$$

Fortsätt på detta sätt så ser det ut så här:

$$\begin{array}{rl|l} 6\,396 = & 525 \cdot 12 + 96 & \operatorname{sgd}(6\,396, 525) = \operatorname{sgd}(525, 96) \\ 525 = & 96 \cdot 5 + 45 & = \operatorname{sgd}(96, 45) \\ 96 = & 45 \cdot 2 + 6 & = \operatorname{sgd}(45, 6) \\ 45 = & 6 \cdot 7 + 3 & = \operatorname{sgd}(6, 3) \\ 6 = & 3 \cdot 2 + 0 & = \operatorname{sgd}(3, 0) = 3. \end{array}$$

Vi ser alltså att $\operatorname{sgd}(6\,396, 525) = 3$. Algoritmen går alltså ut på att utföra heltalsdivision ett antal gånger tills den går jämnt ut (det vill säga att resten blir 0), och sedan använda det faktum att $\operatorname{sgd}(n, 0) = n$ för alla $n > 0$, vilket diskuterades i Exempel 2.1.6. ▲

Sats 2.2.3. *Låt a, b vara heltal som är relativt prima. Då finns heltal x, y sådana att*

$$1 = xa + yb.$$

Bevis. Vi kan utan inskränkning anta att $b > 0$. Använd nu Sats 1.3.1 för att utföra heltalsdivision om och om igen, tills resttermen blir 0, och få:

$$\begin{aligned}
a &= b \cdot q_1 + r_1 && \text{där} && 0 < r_1 < b \\
b &= r_1 \cdot q_2 + r_2 && \text{där} && 0 < r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3 && \text{där} && 0 < r_3 < r_2 \\
r_2 &= r_3 \cdot q_4 + r_4 && \text{där} && 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n && \text{där} && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n \cdot q_{n+1} + r_{n+1} && \text{där} && r_{n+1} = 0
\end{aligned} \tag{2.1}$$

Att denna process verkligen tar slut, och att resten på den sista raden blir 0 inser man eftersom

$$b > r_1 > r_2 > \cdots > r_n > 0.$$

En sådan följd av heltal, som blir mindre och mindre hela tiden måste så småningom nå 0. Enligt Sats 2.2.1 vet vi att

$$\begin{aligned}
1 &= \operatorname{sgd}(a, b) \\
&= \operatorname{sgd}(b, r_1) \\
&= \operatorname{sgd}(r_1, r_2) \\
&= \operatorname{sgd}(r_2, r_3) \\
&\;\;\vdots \\
&= \operatorname{sgd}(r_{n-1}, r_n) \\
&= \operatorname{sgd}(r_n, 0) \\
&= r_n,
\end{aligned}$$

det vill säga att $r_n = 1$. Använd nu (2.1) baklänges och få

$$\begin{aligned}
1 &= r_n \\
&= r_{n-2} - q_n \cdot r_{n-1} = r_{n-2} - q_n \cdot (r_{n-3} - r_{n-2} \cdot q_{n-1}) \\
&= -q_n \cdot r_{n-3} + (1 - q_{n-1} q_n) \cdot r_{n-2} \\
&\;\;\vdots \\
&= x \cdot a + y \cdot b
\end{aligned}$$

för några heltal x, y. □

Exempel 2.2.4. Talen 4 712 och 585 är relativt prima. Det visas på följande sätt:

$$\begin{array}{rl|l}
4\,712 = 585 \cdot 8 + 32 & & \operatorname{sgd}(4\,712, 585) = \operatorname{sgd}(585, 32) \\
585 = 32 \cdot 18 + 9 & & \qquad\qquad = \operatorname{sgd}(32, 9) \\
32 = 9 \cdot 3 + 5 & & \qquad\qquad = \operatorname{sgd}(9, 5) \\
9 = 5 \cdot 1 + 4 & & \qquad\qquad = \operatorname{sgd}(5, 4) \\
5 = 4 \cdot 1 + 1 & & \qquad\qquad = \operatorname{sgd}(4, 1) \\
4 = 1 \cdot 4 + 0 & & \qquad\qquad = \operatorname{sgd}(1, 0) = 1.
\end{array} \tag{2.2}$$

Detta visar att $\operatorname{sgd}(4\,712, 585) = 1$, men uträkningarna kan också användas för att hitta de tal x, y som enligt satsen ovan finns och gör

$$1 = 4\,712 \cdot x + 585 \cdot y.$$

Använd (2.2) baklänges och få

$$\begin{aligned} 1 &= 5 - 4 \cdot 1 && = 5 - (9 - 5 \cdot 1) \cdot 1 \\ &= -9 + 5 \cdot 2 && = -9 + (32 - 9 \cdot 3) \cdot 2 \\ &= 32 \cdot 2 - 9 \cdot 7 && = 32 \cdot 2 - (585 - 32 \cdot 18) \cdot 7 \\ &= -585 \cdot 7 + 32 \cdot 128 && = -585 \cdot 7 + (4\,712 - 585 \cdot 8) \cdot 128 \\ &= 4\,712 \cdot 128 - 585 \cdot 1\,031. \end{aligned}$$

Alltså gäller

$$x = 128 \quad \text{och} \quad y = -1\,031. \qquad \blacktriangle$$

Sats 2.2.5. *Låt a, b vara relativt prima heltal, och c ett godtyckligt heltal. Om $a \mid bc$ så gäller $a \mid c$.*

Bevis. Enligt Sats 2.2.3 finns heltal x, y sådana att $1 = xa + yb$. Multiplicera detta med c och få

$$c = xac + ybc.$$

Eftersom $a \mid bc$ så finns ett heltal q sådant att $bc = aq$. Nu följer

$$c = xac + ybc = xac + yaq = a(xc + yq),$$

vilket visar att $a \mid c$. □

Övningar

Övning 2.1. Låt a, b vara heltal. Antag att heltalet $d > 0$ uppfyller

$$d \mid a \quad \text{och} \quad d \mid b.$$

Antag att $x \mid d$ för varje $x \in D(a) \cap D(b)$. Visa att $d = \operatorname{sgd}(a, b)$.

Övning 2.2. Använd Euklides algoritm för att bestämma $\operatorname{sgd}(8\,860, 1\,075)$.

Övning 2.3. Talen 139 och 117 är relativt prima. Enligt Sats 2.2.3 finns heltal x och y sådana att $1 = x \ \cdot 139 + y \cdot 117$. Använd tekniken i Exempel 2.2.4 för att bestämma x och y.

Övning 2.4. Låt a och b vara relativt prima heltal. Antag att heltalet c uppfyller att

$$a \mid c \quad \text{och} \quad b \mid c.$$

Visa att $ab \mid c$.

3 Primtal

I detta avsnitt kommer vi definiera primtal och visa hur varje positivt heltal kan skrivas som en produkt av sådana primtal.

3.1 Grundläggande definitioner

Definition 3.1.1. Ett heltal $p > 1$ sägs vara ett *primtal* om de enda positiva heltal som delar p är 1 och p. Ett heltal som inte är ett primtal kallas *sammansatt*.

Det kan vara värt att poängtera att *alla* heltal delas av 1 och sig själv. Om n är ett heltal har vi ju att $n = n \cdot 1$, vilket enligt definitionen av delare betyder både att $n \mid n$ och att $1 \mid n$. Men primtalen är alltså de enda heltalen, större än 1, som inte delas av något annat positivt heltal än just dessa två.

Exempel 3.1.2. De första tio primtalen är:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29. \qquad \blacktriangle$$

Om ett tal n kan *faktoriseras*, det vill säga skrivas som en produkt av andra positiva heltal än 1 och n, är det inte ett primtal. Exempelvis är inte 12 ett primtal eftersom $12 = 3 \cdot 4$, vilket bland annat betyder att talen 3 och 4 delar 12. Tal som kan faktoriseras är alltså sammansatta.

Exempel 3.1.3. Följande tal är *inte* primtal, eftersom de kan faktoriseras:

$$6 = 2 \cdot 3, \quad 36 = 4 \cdot 9, \quad 64 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2. \qquad \blacktriangle$$

3.2 Primtalsfaktorisering

Låt oss nu titta på hur man kan faktorisera sammansatta tal. Betrakta talet 60. Det finns ett antal olika sätt att faktorisera det på, exempelvis:

$$60 = 6 \cdot 10, \quad 60 = 3 \cdot 20, \quad 60 = 3 \cdot 4 \cdot 5, \quad 60 = 2 \cdot 2 \cdot 3 \cdot 5.$$

Observera särskilt den sista faktoriseringen. Den består bara av primtal. Försök nu hitta en faktorisering av 60 som består av andra primtal än dessa. Försök dock inte för länge, för det går inte. Detta är inget speciellt för talet 60, utan en egenskap som alla heltal har.

Det visar sig nämligen att alla heltal, förutom 0, 1 och -1, inte bara kan skrivas som en produkt av primtal, utan dessutom att det bara finns ett enda sätt att göra detta på. Visserligen är det så att

$$60 = 2 \cdot 5 \cdot 3 \cdot 2 = 5 \cdot 3 \cdot 2 \cdot 2,$$

vilket betyder att man kan ordna om primtalsfaktorerna i talet 60 för att få faktoriseringar som ser olika ut. Men det väsentliga är att det alltid är samma

primtalsfaktorer som förekommer (i fallet med 60 är primtalsfaktorerna 2, 3 och 5), och antalet gånger varje primtal förekommer är också detsamma (för talet 60 förekommer 2 två gånger, medan 3 och 5 förekommer en gång vardera). Låt oss nu bevisa detta.

Vi börjar med följande hjälpsats:

Lemma 3.2.1. *Låt p vara ett primtal, och $x_1, x_2, x_3, \ldots$ godtyckliga heltal. Välj ett heltal $n \geqslant 1$. Om*

$$p \mid x_1 x_2 \cdots x_n$$

så är det också så att

$$p \mid x_j$$

för något j med $1 \leqslant j \leqslant n$.

Bevis. Om $n = 1$ så är påståendet uppenbarligen sant. Antag nu för ett ögonblick att påståendet också är sant om $n = k$, där $k \geqslant 1$ är ett heltal. Utifrån detta antagande försöker vi nu visa att påståendet också gäller för $n = k + 1$.

Låt $m = x_1 x_2 \cdots x_k$. Det vi har antagit är alltså att om $p \mid m$ så har vi att $p \mid x_j$ för något j med $1 \leqslant j \leqslant k$. Det vi vill visa är att om $p \mid m x_{k+1}$ så följer det att $p \mid x_j$ för något j med $1 \leqslant j \leqslant k + 1$.

Antag alltså att $p \mid m x_{k+1}$. Vi har två fall: $p \mid x_{k+1}$ och $p \nmid x_{k+1}$. I det första fallet är det uppenbarligen så att $p \mid x_j$ för något j med $1 \leqslant j \leqslant k+1$ (eftersom det gäller för $j = k + 1$).

Låt oss därför titta på det andra fallet, det vill säga där $p \nmid x_{k+1}$. Eftersom p är ett primtal gäller per definition $D(p) = \{1, p\}$. Eftersom $p \nmid x_{k+1}$ så gäller $p \notin D(x_{k+1})$. Alltså måste $D(p) \cap D(x_{k+1}) = \{1\}$. Detta betyder att $\operatorname{sgd}(p, x_{k+1}) = 1$, så p och x_{k+1} är relativt prima. I och med att $p \mid x_{k+1} m$ så följer det enligt Sats 2.2.5 att $p \mid m$. Men enligt vårt första antagande följer då att $p \mid x_j$ för något j med $1 \leqslant j \leqslant k$.

Vi har alltså visat att $p \mid x_j$ för något j med $1 \leqslant j \leqslant k+1$ både i fallet $p \mid x_{k+1}$ och $p \nmid x_{k+1}$. Alltså har vi visat det vi föresatte oss: att om $p \mid m x_{k+1}$ så följer $p \mid x_j$ för något j med $1 \leqslant j \leqslant k + 1$.

Det som har hänt nu är att vi har visat att så fort påståendet i lemmat gäller för $n = k$, där $k \geqslant 1$, så gäller det också för $n = k + 1$. Men vi vet ju från första raden i beviset att det gäller för $n = 1$. Alltså följer det att påståendet gäller också för $n = 2$. Och därmed måste påståendet gälla för $n = 3$, och för $n = 4$, $n = 5$, $n = 6$, och så vidare i all evighet. Alltså gäller påståendet för alla heltal $n \geqslant 1$. □

Med hjälp av Lemmat kan vi visa att alla heltal har en unik primtalsfaktorisering, något som brukar kallas för *aritmetikens fundamentalsats*:

Sats 3.2.2 (Aritmetikens fundamentalsats)**.** *Varje heltal $m \geqslant 2$ kan skrivas som*

$$m = p_1 p_2 \cdots p_n,$$

där $p_1, p_2, \ldots, p_n$ är primtal. Denna faktorisering är unik, bortsett från ordningen av faktorerna.

Bevis. Vi börjar med att visa att varje $m \geqslant 2$ verkligen har en primtalsfaktorisering. Antag motsatsen, det vill säga det finns tal $m \geqslant 2$ som inte kan faktoriseras i primtal. Låt M vara det minsta sådana talet. Det kan inte vara så att M är ett primtal, för då är det redan faktoriserat i primtal ($M = p$, där p är ett primtal). Alltså är M inte ett primtal, vilket betyder att det finns en delare a till M som inte är 1 eller M. Enligt definitionen av delare finns också b sådant att $M = ab$. Uppenbarligen kan inte heller b vara 1 eller M. Vi kan utan inskränkning anta att $a, b > 0$. Alltså gäller $2 \leqslant a < M$ och $2 \leqslant b < M$. Men eftersom M är det minsta tal $\geqslant 2$ som inte har en primtalsfaktorisering, så måste både a och b ha primtalsfaktoriseringar. Vi kan alltså skriva

$$a = q_1 q_2 \cdots q_k \quad \text{och} \quad b = r_1 r_2 \cdots r_l,$$

där $q_1, q_2, \ldots, q_k, r_1, r_2, \ldots, r_l$ är primtal. Men nu gäller ju

$$M = ab = q_1 q_2 \cdots q_k r_1 r_2 \cdots r_l,$$

vilket betyder att även M har en primtalsfaktorisering. Detta är en motsägelse, vilket betyder att det inte kan finnas tal $m \geqslant 2$ som saknar primtalsfaktorisering.

Nu återstår det att visa att faktoriseringen av m är unik. Antag även här motsatsen, det vill säga att det finns tal $m \geqslant 2$, som visserligen kan faktoriseras i primtal, men på olika sätt. Låt M vara det minsta sådana talet. Skriv upp två godtyckliga primtalsfaktoriseringar av M enligt:

$$M = q_1 q_2 \cdots q_k \quad \text{och } M = r_1 r_2 \cdots r_l,$$

där $q_1, q_2, \ldots, q_k, r_1, r_2, \ldots, r_l$ är primtal.

Vi måste ha $k \geqslant 2$ och $l \geqslant 2$, för om exempelvis $k = 1$ så skulle $M = q_1$ vara ett primtal. Och primtal har naturligtvis en unik faktorisering bestående av ett enda primtal: talet själv.

Vi har att

$$q_1 \mid M = r_1 r_2 \cdots r_l,$$

vilket enligt lemmat ovan betyder att

$$q_1 \mid r_j$$

för något j med $1 \leqslant j \leqslant l$. Men eftersom både q_1 och r_j är primtal så måste $q_1 = r_j$. Alltså gäller

$$q_1 \cdot (q_2 q_3 \cdot q_k) = M = q_1 \cdot (r_1 r_2 \cdots r_{j-1} r_{j+1} \cdots r_l)$$

och därmed

$$q_2 q_3 \cdot q_k = r_1 r_2 \cdots r_{j-1} r_{j+1} \cdots r_l.$$

Men eftersom detta tal är mindre än M så har det en *unik* primtalsfaktorisering, vilket betyder att primtalsfaktoriseringarna

$$q_2 q_3 \cdot q_k \quad \text{och} \quad r_1 r_2 \cdots r_{j-1} r_{j+1} \cdots r_l.$$

är desamma, förutom möjligtvis ordningen på faktorerna. Och eftersom $p_1 = q_j$ så är också fakoriseringarna

$$M = q_1 q_2 \cdots q_k \quad \text{och} \quad M = r_1 r_2 \cdots r_l$$

desamma, förutom möjligtvis ordningen på faktorerna. Detta betyder att alla sätt att faktorisera M på är desamma, vilket är en motsägelse. Alltså kan det inte finnas tal $m \geqslant 2$ som har olika primtalsfaktoriseringar. □

3.3 Existens av primtal

En sak som återstår att fråga sig om primtal är hur många det finns. Detta besvaras av följande sats, vars bevis var känt redan av Euklides:

Sats 3.3.1. *Det finns oändligt många primtal.*

Bevis. Antag att det bara finns ändligt många primtal $p_1, p_2, \ldots, p_n$. Skriv

$$m = 1 + p_1 p_2 \cdots p_n.$$

Enligt aritmetikens fundamentalsats finns primtal $q_1, q_2, \ldots, q_k$ sådana att

$$m = q_1 q_2 \cdots q_k.$$

Eftersom $p_1, p_2, \ldots, p_n$ enligt antagandet är alla primtal som finns, så måste q_1 vara ett av dessa. Vi har alltså $q_1 = p_j$ där $1 \leqslant j \leqslant n$. Låt

$$a = p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_n \quad \text{och} \quad b = q_2 q_3 \cdots q_n.$$

Då har vi $m = 1 + p_j a$ och $m = q_1 b$, och eftersom $q_1 = p_j$

$$q_1 \cdot b = m = 1 + q_1 \cdot a,$$

vilket i sin tur betyder att

$$q_1 \cdot (b - a) = 1.$$

Detta är omöjligt eftersom $q_1 \geqslant 2$ och $b - a$ är ett heltal. Alltså kan det inte finnas ändligt många primtal. □

Övningar

Övning 3.1. Primtalsfaktorisera talen

$$12, \quad 26, \quad 55, \quad 98, \quad 150, \quad 210, \quad 315, \quad 455.$$

Ledning: Prova att successivt dela talet med primtalen $2, 3, 5, 7, 11, \ldots$. Om ett primtal p delar talet a, så är det ett av primtalfaktorerna, och resten av faktoriseringen hittar man genom att faktorisera kvoten a/p på samma sätt. Exempelvis ser vi att $105/3 = 35$. Så för att hitta faktoriseringen av 105 återstår nu att faktorisera 35. Men $35/5 = 7$ så $105 = 3 \cdot 5 \cdot 7$.

Övning 3.2. Låt p och $\tilde{p}$ vara primtal. Visa att om $p \mid \tilde{p}$ så måste $p = \tilde{p}$.

Övning 3.3. Låt a vara ett heltal och p vara ett primtal. Visa att antingen gäller $\operatorname{sgd}(a, p) = 1$ eller så gäller $p \mid a$.

Övning 3.4. Låt $n \geqslant 1$ vara ett heltal. Antag att talen $a_1, a_2, \ldots, a_m$ alla är relativt prima med n. Låt

$$a = a_1 a_2 \cdots a_m.$$

Visa att a och n är relativt prima.

4 Kvadratiska talringar

Eftersom vi är så vana vid att arbeta med vanliga heltal är det ibland svårt för oss att verkligen uppskatta elegansen i våra resultat från de första kapitlen. Vi tar exempelvis ofta entydig faktorisering av heltal för given, men som vi har sett är det inte helt lätt att visa detta faktum på ett matematiskt tillfredsställande sätt. I det här kapitlet ska vi sätta våra tidigare kunskaper i ett nytt perspektiv.

Vi ska definiera så kallade *kvadratiska talringar* med hjälp av de tidigare kända heltalen. Elementen i dessa ringar påminner rätt mycket om heltal, men de uppför sig ibland på oväntade sätt. Vi inför operationer som motsvarar addition och multiplikation, och vi definierar ett slags minimala faktorer som motsvarar primtal. Till slut kommer vi att se att vi i vissa fall kan skriva elementen i våra talringar som produkten av minimala faktorer på *flera olika sätt*.

4.1 Gaussiska heltal

När man försöker lösa andragradsekvationer av typen

$$x^2 + bx + c = 0 \quad \text{där} \quad b, c \in \mathbb{R}$$

finner man ibland att dessa ekvationer saknar lösningar, det vill säga, att inte inte finns *något* $x \in \mathbb{R}$ som uppfyller ekvationen.

Exempel 4.1.1. Ett känt exempel är ekvationen

$$x^2 + 1 = 0. \tag{4.1}$$

Eftersom $x^2 \geqslant 0$ för alla $x \in \mathbb{R}$ och summan av ett icke-negativt tal och ett positivt tal alltid är positiv, ser vi att ekvationen saknar reella lösningar. ▲

Den här situationen dyker ofta upp i matematiken: man arbetar med en mängd som är för liten för att man ska kunna lösa vissa problem, och för att kunna gå vidare ändå gör man därför mängden större genom att lägga till element. Vi har redan sett något liknande när vi införde de reella talen efter att vi märkte att kvadratrötter inte alltid kan hittas bland de rationella talen.

Vi bildar nu ett nytt talsystem med hjälp av heltalen och en symbol i, som vi kan tänka på som ett slags "skiljetecken" mellan två hela tal. Vi utrustar detta talsystem med addition och multiplikation på följande sätt.

Definition 4.1.2. Mängden av *Gaussiska heltal* består av uttryck på formen

$$z = a + b\mathrm{i}, \quad a, b \in \mathbb{Z}.$$

Summan $z + w$ av två Gaussiska heltal $z = a + b\mathrm{i}$ och $w = c + d\mathrm{i}$ definieras som

$$z + w = a + c + (b + d)\mathrm{i}, \tag{4.2}$$

medan produkten $z \cdot w$ ges av

$$z \cdot w = ac - bd + (ad + bc)\mathrm{i}. \tag{4.3}$$

Mängden av Gaussiska heltal, tillsammans med de bägge operationerna addition och multiplikation, betecknas med $\mathbb{Z}[\mathrm{i}]$.

Exempel 4.1.3. Talen

$$2,\ 3\mathrm{i},\ 2+4\mathrm{i},\ -2+7\mathrm{i},\ 5-2\mathrm{i}$$

är Gaussiska heltal. ▲

Det är viktigt att först vi övertygar oss om att definitionen ovan är vettig. Eftersom summor av heltal är heltal följer det i alla fall att summan $z + w$ är på formen $A + B\mathrm{i}$ för heltalen $A = a + c$, $B = b + d$. Motsvarande gäller för produkten $z \cdot w$: uttrycken $C = ac - bd$ och $D = ad + bc$ är heltal, så $z \cdot w = C + D\mathrm{i}$. Vi ser alltså att vi inte kan lämna mängden av Gaussiska heltal genom att utföra räkneoperationer på dem; man säger att mängden $\mathbb{Z}[\mathrm{i}]$ är sluten under addition och multiplikation. I en av övningarna får läsaren bekanta sig med några andra viktiga egenskaper hos de Gaussiska heltalen.

Vi inser alltså att definitionerna ovan inte leder till några motsägelser, men frågan varför vi har valt just dessa regler för addition och multiplikation kvarstår. Innan vi diskuterar detta ska vi bekanta oss lite med hur konkreta räkningar i $\mathbb{Z}[\mathrm{i}]$ kan se ut.

Exempel 4.1.4. Vi sätter $z = 2 + \mathrm{i}$ och $w = -2 + \mathrm{i}$ och har då

$$z + w = (2 + \mathrm{i}) + (-2 + \mathrm{i}) = 2 - 2 + (1 + 1)\mathrm{i} = 0 + 2\mathrm{i}.$$

Produkten zw får vi genom att beräkna

$$zw = (2 + \mathrm{i})(-2 + \mathrm{i}) = 2 \cdot (-2) - 1 \cdot 1 + [2 \cdot 1 + 1 \cdot (-2)]\,\mathrm{i} = -5 + 0\mathrm{i}.$$

Om vi istället låter $z = 7 - 3\mathrm{i}$ och $w = -\mathrm{i}$ ser vi att

$$z - w = (7 - 3\mathrm{i}) - (-\mathrm{i}) = (7 - 3\mathrm{i}) - (0 - 1\mathrm{i}) = 7 + 0 + (-3 + 1)\mathrm{i} = 7 - 2\mathrm{i},$$

medan vi får

$$zw = (7 - 3\mathrm{i})(0 - \mathrm{i}) = 7 \cdot 0 - (-3) \cdot (-1) + [(-3) \cdot 0 + 7 \cdot (-1)]\,\mathrm{i} = 3 - 7\mathrm{i}$$

▲

För att förenkla notationen skriver vi 0 istället ofta för $0 + 0\mathrm{i}$, a istället för $a + 0\mathrm{i}$ och $b\mathrm{i}$ istället för $0 + b\mathrm{i}$. Talet $0 = 0 + 0\mathrm{i}$ har den speciella egenskapen att $0 + z = z$ och $0 \cdot z = 0$ för alla $z \in \mathbb{Z}[\mathrm{i}]$, det fungerar på precis samma sätt som den vanliga nollan för heltalen.

Exempel 4.1.5. Vi skriver 3 istället för $3 + 0\mathrm{i}$ och $5\mathrm{i}$ istället för $0 + 5\mathrm{i}$. ▲

Vi ska nu försöka förstå varifrån vi har fått idén som ligger bakom definitionerna av addition och multiplikation av Gaussiska heltal. En jämförelse med multiplikation av polynom kan vara nyttig. Tag två polynom $a+bx$ och $c+dx$, där $a, b, c, d \in \mathbb{Z}$ och x är en variabel. Om vi adderar polynomen, och samlar ihop termerna som innehåller variabeln x får vi

$$(a + bx) + (c + dx) = a + c + (b + d)x,$$

ett nytt polynom på samma form. Om vi istället multiplicerar polynomen och samlar ihop alla termer som innehåller x och x^2 får vi:

$$(a + bx)(c + dx) = ac + adx + bcx + bdx^2 = ac + (ad + bc)x + bdx^2.$$

Nu har vi en term med x^2 med också, så produkten är inte på samma form som de två ursprungliga polynomen. Vi gör nu samma sak med $a + b\mathrm{i}$ och $c + d\mathrm{i}$ (vi byter bara x mot i) och får

$$(a + b\mathrm{i})(c + d\mathrm{i}) = ac + ad\mathrm{i} + bc\mathrm{i} + bd\mathrm{i}^2 = ac + (ad + bc)\mathrm{i} + bd\mathrm{i}^2.$$

Om vi här helt fräckt byter ut i^2 mot -1 får vi precis vår Gaussiska produkt, där resultatet är ett nytt Gaussiskt heltal!

Vi gör nu en avgörande observation: om vi låter $z = 0+\mathrm{i}$ får vi från räknereglerna för Gaussiska heltal att

$$z^2 = z \cdot z = -1 + 0\mathrm{i},$$

vilket betyder att talet $z = 0 + \mathrm{i}$ löser ekvationen $z^2 + 1 = 0$, i alla fall om vi använder konventionen $0 = 0+0\mathrm{i}$. Vi har alltså lyckats hitta en lösning till vår olösbara ekvation genom att utvidga vårt talsystem! Talet i kallas för övrigt den *imaginära enheten*. Det här faktumet har motiverat vår definition av multiplikation i $\mathbb{Z}[\mathrm{i}]$: tanken är att man ska "räkna på som vanligt" med uttryck på formen $3 + 7\mathrm{i}$ och $-2 + 5\mathrm{i}$ genom att tillämpa de vanliga räknereglerna för heltal, men byta ut en förekomst av uttrycket i^2 mot -1.

Det är viktigt att notera att vi återfinner mängden av vanliga heltal bland de Gaussiska heltalen: de är helt enkelt Gaussiska heltal $z = a+b\mathrm{i}$ med $b = 0$. Om man tillämpar räknereglerna för $\mathbb{Z}[\mathrm{i}]$ finner man att mängden av tal $z = a+0\mathrm{i}$ beter på samma sätt som heltalen, så vi har i alla fall inte förstört några av våra tidigare resultat genom att utvidga vårt talsystem.

Anmärkning 4.1.6. Man kan definiera division för Gaussiska heltal också, men vi avstår från det här.

Vi inför däremot begreppet *delare* för Gaussiska heltal.

Definition 4.1.7. Låt z och z_1 vara Gaussiska heltal. Om det finns ett Gaussiskt heltal w_1 sådant att $z = z_1 \cdot w_1$ säger vi att z_1 *delar* z, och vi skriver $z_1 \mid z$. Vi kallar då z_1 för en *delare* till z. Om z_1 inte delar z skriver vi $z_1 \nmid z$.

Ett begrepp som vi kommer att använda flitigt är *normen* av ett Gaussiskt heltal. Normen av ett Gaussiskt heltal är ett mått på hur stort talet är.

Definition 4.1.8. *Normen* $N(z)$ av ett tal $z = a + b\mathrm{i}$ definieras som

$$N(z) = a^2 + b^2.$$

Det är värt att notera följande egenskaper hos normen:

Lemma 4.1.9. *Normen av ett Gaussiskt heltal är ett icke-negativt heltal, och* $N(z) = 0$ *om och endast om* $z = 0$*. Vidare gäller*

$$N(a + b\mathrm{i}) = N(a - b\mathrm{i}),$$

samt

$$N(z \cdot w) = N(z) \cdot N(w) \tag{4.4}$$

Bevis. Normen av $z = a + b\mathrm{i}$ är ett heltal eftersom $a^2 + b^2 = a \cdot a + b \cdot b$ och vi har visat att summor och produkter av heltal är heltal. Vi vet även att kvadraten av ett heltal är icke-negativt, och således gäller $N(z) \geqslant 0$ för alla Gaussiska heltal z. Om $N(z) = 0$ har vi

$$a^2 + b^2 = 0,$$

och den enda möjliga heltalslösningen till denna ekvation är $a = b = 0$.

Definitionen av norm ger att

$$N(a - b\mathrm{i}) = N(a + (-b)\mathrm{i}) = a^2 + (-b)^2 = a^2 + b^2,$$

vilket är lika med $N(a + b\mathrm{i})$.

Vi bildar sedan produkten

$$zw = (a + \mathrm{i}b)(c + \mathrm{i}d) = ac - bd + (ad + bc)\mathrm{i}.$$

Från definitionen för normen får vi

$$N(zw) = N(ac - bd + (ad + bc)\mathrm{i}) = (ac - bd)^2 + (ad + bc)^2.$$

Genom att utveckla kvadraterna i högerledet får vi

$$\begin{aligned} N(zw) &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2. \end{aligned}$$

Å andra sidan ser vi att

$$N(z) \cdot N(w) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2,$$

och därmed är den sista likheten i satsen visad. □

Det är emellertid *inte sant* att $N(z+w) = N(z) + N(w)$, vi återkommer till detta i en av övningarna.

Exempel 4.1.10. Vi har att

$$N(1+\mathrm{i}) = 1^2 + 1^2 = 2$$

medan

$$N(-3\mathrm{i}) = 0^2 + 3^2 = 9. \qquad \blacktriangle$$

Från egenskaperna hos normen följer nu speciellt att $z \cdot w = 0$ om och endast om $z = 0$ eller $w = 0$.

Nästa lemma beskriver en viktig egenskap hos normen: normen av en produkt är större eller lika med var och en av faktorernas normer.

Lemma 4.1.11. *Låt z och w vara nollskilda Gaussiska heltal. Då gäller*

$$N(z \cdot w) \geqslant N(z) \quad \textit{och} \quad N(z \cdot w) \geqslant N(w).$$

Vi har sträng olikhet såvida inte någon av faktorerna är en enhet.

Vi ger det som en övning att visa detta.

Vi ska nu titta närmare mot motsvarigheterna till heltalen 1 och -1 i $\mathbb{Z}[\mathrm{i}]$.

Definition 4.1.12. Vi säger att $z \in \mathbb{Z}[\mathrm{i}]$ är en *enhet* om $N(z) = 1$.

Alla tal i $\mathbb{Z}[\mathrm{i}]$ är på formen $z = a + b\mathrm{i}$, och om z ska vara en enhet måste vi ha $N(a + b\mathrm{i}) = 1$, det vill säga

$$a^2 + b^2 = 1$$

Summan av två icke-negativa heltal är alltid större än ett om a och b båda är skilda från 0. Om ekvationen $a^2 + b^2 = 1$ ska vara uppfylld måste således antingen $a = 0$ eller $b = 0$. Vi inser nu att $a = \pm 1, b = 0$ och $a = 0, b = \pm 1$ är de enda möjliga lösningarna till ekvationen. Alltså ges enheterna i $\mathbb{Z}[\mathrm{i}]$ av

$$1, -1, \mathrm{i}, -\mathrm{i}.$$

4.2 Entydig faktorisering

Vårt mål är att undersöka huruvida vi kan skriva varje Gaussiskt heltal som en produkt av en minimala faktorer, det vill säga Gaussiska heltal som själva inte kan skrivas som produkter. Man observerar emellertid att det för varje $z \in \mathbb{Z}[\mathrm{i}]$ gäller att $z = 1 \cdot z$, och även att $z = \mathrm{i} \cdot \mathrm{i} \cdot (-z)$, så vi kommer aldrig ifrån att vi kan skjuta in enheter i faktoriseringen av Gaussiska heltal. Vi tar hänsyn till detta i vår nästa definition.

Definition 4.2.1. Vi säger att det Gaussiska heltalet z är *irreducibelt* om det enda sättet att skriva z som en produkt av Gaussiska heltal är att bara använda enheter och z som faktorer.

Exempel 4.2.2. Talet $1 + \mathrm{i}$ är irreducibelt. Om så inte vore fallet skulle vi ha $1 + \mathrm{i} = z \cdot w$ för några tal $z, w \in \mathbb{Z}[\mathrm{i}]$ som inte är enheter. Vi har emellertid $N(1+\mathrm{i}) = 2$, vilket skulle medföra att $N(z \cdot w) = N(z) \cdot N(w) = 2$. Eftersom 2 är ett primtal måste därför antingen $N(z) = 1$ eller $N(w) = 1$, vilket motsäger att z och w inte är enheter. ▲

Exempel 4.2.3. Talet 2 är inte irreducibelt eftersom $2 = (1 + \mathrm{i})(1 - \mathrm{i})$, och $1 + \mathrm{i}$ samt $1 - \mathrm{i}$ inte är enheter. Vi säger istället att 2 är *reducibelt.* ▲

Här ser vi att något lite överraskande har inträffat. Talet 2 som är ett primtal i $\mathbb{Z}$ och inte kan skrivas som en produkt av heltal, har i $\mathbb{Z}[\mathrm{i}]$ blivit reducibelt!

Definition 4.2.4. Vi säger att ett Gaussiskt heltal z har en *irreducibel faktorisering* om z kan skrivas som en ändlig produkt av irreducibla element i $\mathbb{Z}[\mathrm{i}]$.

Sats 4.2.5. *Varje element i talringen* $\mathbb{Z}[\mathrm{i}]$ *som är skilt från* 0 *har en irreducibel faktorisering.*

Bevis. Antag att satsen är falsk, det vill säga, att det finns ett Gaussiskt heltal z som inte är noll, men som inte kan skrivas som en ändlig produkt av irreducibla element.

Vi noterar först att z självt inte kan vara irreducibelt, ty då skulle vi ju ha en irreducibel faktorisering bestående av bara z. Vi måste alltså kunna skriva z som en produkt

$$z = z_1 \cdot w_1$$

av Gaussiska heltal z_1 och w_1 som är skilda från 0 och som inte är enheter. Det är vidare omöjligt att både z_1 och w_1 har irreducibla faktoriseringar. Om så vore fallet skulle vi ju få en irreducibel faktorisering för z genom att multiplicera ihop dessa två irrededucibla faktoriseringar för z_1 och w_1. Alltså måste åtminstone något av z_1 och w_1, säg z_1, ha samma egenskap som det Gaussiska heltalet z. Vi har alltså att $z = z_1 \cdot w_1$, att z_1 inte är noll och inte är irreducibelt, och att z_1 inte kan skrivas som en produkt av irreducibla element.

Vi upprepar ovanstående resonemang för z_1. Detta ger oss att $z_1 = z_2 \cdot w_2$ för några tal z_2 och w_2, där z_2 och w_2 inte är enheter och där z_2 saknar en irreducibel faktorisering. Vi fortsätter på samma sätt och erhåller en oändlig följd $z_1, z_2, z_3 \ldots$ av element i $\mathbb{Z}[\mathrm{i}]$ där z_{j+1} är en faktor i z_j och inte är en enhet eller noll. För varje j gäller vidare att $z_j = z_{j+1} \cdot w_j$, där talen w_j är Gaussiska heltal som inte är enheter.

Relationen (4.4) samt det faktum att inget av w_j:na är en enhet medför då att

$$N(z_j) = N(z_{j+1} \cdot w_j) > N(z_{j+1})$$

Eftersom detta gäller i varje steg j får vi en oändlig, strängt avtagande följd av heltal

$$N(z_1) > N(z_2) > N(z_3) > \cdots .$$

Men detta leder till att $N(z_j) \leqslant 0$ för något j, vilket motsäger att $N(z) > 0$ för alla nollskilda $z \in \mathbb{Z}[\mathrm{i}]$. Alltså har varje element z i $\mathbb{Z}[\mathrm{i}]$ som inte är 0 en entydig faktorisering. □

Anmärkning 4.2.6. Observera noga att vi inte uttalar oss om att faktoriseringen ska vara entydig. Vi säger bara att det finns *minst en* irreducibel faktorisering av varje Gaussiskt heltal.

En fråga som kvarstår är hur de irreducibla elementen i $\mathbb{Z}[\mathrm{i}]$ egentligen ser ut. Eftersom de vanliga heltalen kan identifieras med Gaussiska heltal $z = a + b\mathrm{i}$ med $b = 0$ skulle en gissning kunna vara att åtminstone primtalen i $\mathbb{Z}$ skulle kunna vara irreducibla. Detta är emellertid inte sant, vi har ju sett att $2 = (1+\mathrm{i})(1-\mathrm{i})$. Det ligger ändå nära till hands att misstänka att primtalen borde dyka upp i beskrivningen av de irreducibla Gaussiska heltalen – vi har ju skapat dessa med hjälp av vanliga heltal! Vi avstår från att ge en precis beskrivning av alla irreducibla Gaussiska tal, men med hjälp våra tidigare exempel kan vi i alla fall observera att om $N(z)$ är ett primtal, så är z irreducibelt.

Vi har nu kommit fram till en av höjdpunkterna i det här kapitlet.

Sats 4.2.7. *Varje nollskilt element i talringen $\mathbb{Z}[\mathrm{i}]$ har en entydig faktorisering i irreducibla faktorer om vi bortser från förekomsten av enheter och faktorernas ordning.*

Liksom i heltalsfallet behöver vi i beviset använda ett lemma.

Lemma 4.2.8. *Låt z vara ett irreducibelt element i $\mathbb{Z}[\mathrm{i}]$. Om $z \mid y_1 y_2 \cdots y_n$ så gäller $z \mid y_j$ för något j med $1 \leqslant j \leqslant n$.*

Vi avstår ifrån att ge ett fullständigt bevis här. Bevisidén är samma som i heltalsfallet, och bygger något som liknar divisionalgoritmen för heltal.

Bevis av Sats 4.2.7. Låt oss anta motsatsen, det vill säga, att det existerar Gaussiska heltal med två olika irreducibla faktoriseringar. Låt z vara ett sådant Gaussiskt heltal, med egenskapen att normen av z är minimal. Det vill säga, vi har $N(\tilde{z}) \geqslant N(z)$ för varje tal $\tilde{z}$ som har mer än en irreducibel faktorisering.

Vi har alltså antagit att

$$z = x_1 x_2 \cdots x_N \quad \text{och} \quad z = y_1 y_2 \cdots y_M, \tag{4.5}$$

där både x_j:na och y_j:na är irreducibla element. Vi antar också att inga av x_j:na och y_j:na är enheter.

Det måste gälla att $N \geqslant 2$ och $M \geqslant 2$. Annars är z självt irreducibelt med $z = x_1$ och $z = y_1$, vilket medför $x_1 = y_1$.

Eftersom $x_1 \mid z$ måste vi ha $x_1 \mid y_1 y_2 \cdots y_M$, och från lemmat ovan följer det att $x_1 \mid y_k$ för något $1 \leqslant k \leqslant M$. Vi kan alltså skriva

$$y_k = e \cdot x_1$$

för något Gaussiskt heltal e. Vi vet å andra sidan att y_k är irreducibelt, så det enda sättet att skriva y_k som en produkt är att bara använda y_k och enheter. Detta innebär att x_1 och y_k bara kan skilja sig på en enhet. Vi drar slutsatsen att talet e ovan är en enhet, $N(e) = 1$.

Vi sätter in relationen $y_k = ex_1$ i (4.5) och får

$$x_1 x_2 \cdots x_N = z = ex_1 \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdots y_M.$$

Vi låter nu $w = x_2 x_3 \cdots x_N$; vi har alltså $z = x_1 \cdot w$. Vi vet att x_1 inte är noll, vilket innebär att

$$x_2 x_3 \cdots x_N = w = e \cdot y_1 \cdots y_{j-1} y_{j+1} \cdots y_M.$$

Inget av talen y_j är en enhet, och w är ju en produkt av y_j:na med y_k utbytt mot en enhet. Vi drar slutsatsen att $N(y_k) > N(e)$, vilket i sin tur medför $N(w) < N(z)$.

Talet z var ju det Gaussiska heltal med minst norm bland dem som inte hade entydig faktorisering. Det betyder att talet w *har* en entydig faktorisering, vilket betyder att alla x_j och y_j är lika, bortsett från talens ordningen och att vi kan skjuta in eventuella enheter. Slutligen har vi $z = x_1 \cdot w$ samt $z = y_1 \cdot w$, och det följer därmed att även z har en entydig faktorisering, om man bortser från ordningen på faktorerna och förekomsten av enheter. □

4.3 Andra talringar och avsaknad av entydig faktorisering

I föregående avsnitt definierade vi ett talsystem och räkneoperationer för detta som var skräddarsydda så att ekvationen $x^2 + 1 = 0$ skulle gå att lösa. Detta innebar väsentligen att vi införde en symbol i med egenskapen $\mathrm{i}^2 = -1$.

Låt oss nu istället betrakta ekvationen

$$x^2 + 5 = 0.$$

Denna saknar också reella lösningar; det finns inga $x \in \mathbb{R}$ som satisfierar ekvationen. Vi inför därför symbolen $\sqrt{-5}$ som har egenskapen att $(\sqrt{-5})^2 + 5 = 0$.

Definition 4.3.1. Talringen $\mathbb{Z}[\sqrt{-5}]$ består av mängden av uttryck på formen

$$z = a + b\sqrt{-5}, \quad a, b \in \mathbb{Z},$$

tillsammans med två operationer: addition och multiplikation. Vi låter summan $z + w$ av $z = a + b\sqrt{-5}$ och $w = c + d\sqrt{-5}$ vara

$$z + w = a + c + (b + d)\sqrt{-5}$$

medan produkten $z \cdot w$ definieras som

$$z \cdot w = ac - 5bd + (ad + bc)\sqrt{-5}$$

Exempel 4.3.2. Ett exempel på en uträkning i $\mathbb{Z}[\sqrt{-5}]$ är beräkningen av produkten $z \cdot w$ för $z = 1 + \sqrt{-5}$ och $w = 1 - \sqrt{-5}$:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 \cdot 1 - 5 \cdot (-1) \cdot 1 + [1 \cdot (-1) + 1 \cdot 1]\sqrt{-5} = 6. \quad \blacktriangle$$

Definition 4.3.3. *Normen* $N(z)$ av ett element $z \in \mathbb{Z}[\sqrt{-5}]$ ges av

$$N(z) = a^2 + 5b^2.$$

Normen i $\mathbb{Z}[\sqrt{-5}]$ skiljer sig alltså från normen i $\mathbb{Z}[\mathrm{i}]$. Man kan dock observera att vi definierat de två normerna så att $N(z) = (a + b\mathrm{i})(a - b\mathrm{i})$ respektive $N(z) = (a + b\sqrt{-5})(a - b\sqrt{-5})$.

Om man funderar och räknar lite inser man att normen i $\mathbb{Z}[\sqrt{-5}]$ har egenskaper som motsvarar de för normen i $\mathbb{Z}[\mathrm{i}]$, speciellt gäller det liksom tidigare att

$$N(z \cdot w) = N(z) \cdot N(w)$$

och $N(z) = 0$ om och endast om $z = 0$.

Exempel 4.3.4. Talet $z = 2$ har norm $N(2) = 2^2 + 5 \cdot 0^2 = 4$ medan talet $z = \sqrt{-5}$ har norm $N(\sqrt{-5}) = 0^2 + 5 \cdot 1^2 = 5$. $\blacktriangle$

Definition 4.3.5. Vi säger att $z \in \mathbb{Z}[\sqrt{-5}]$ är en enhet om $N(z) = 1$.

Vi kan bestämma alla enheter i $\mathbb{Z}[\sqrt{-5}]$. Att $z = a + \sqrt{-5}b$ är en enhet betyder definitionsmässigt att

$$a^2 + 5b^2 = 1$$

Vi noterar att $5b^2 \geqslant 5 > 1$ om $b \neq 0$. Eftersom a^2 och $5b^2$ är positiva saknar alltså ekvationen lösningar om $b \neq 0$. Vi drar slutsatsen att

$$1, -1$$

är enheterna i $\mathbb{Z}[\sqrt{-5}]$.

Definition 4.3.6. Vi säger att $z \in \mathbb{Z}[\sqrt{-5}]$ är *irreducibelt* om det enda sättet att skriva z som produkten av element i $\mathbb{Z}[\sqrt{-5}]$ är att enbart använda enheter och z självt.

Exempel 4.3.7. Talet $6 + \sqrt{-5}$ är irreducibelt eftersom $N(6 + \sqrt{-5}) = 41$ är ett primtal. $\blacktriangle$

Exempel 4.3.8. Talet $-5 + 2\sqrt{-5}$ är *inte* irreducibelt eftersom

$$-5 + 2\sqrt{-5} = \sqrt{-5}\,(2 + \sqrt{-5})$$

och $\sqrt{-5}$ och $2 + \sqrt{-5}$ inte är enheter. $\blacktriangle$

Sats 4.3.9. *Varje element i talringen* $\mathbb{Z}[\sqrt{-5}]$ *har en irreducibel faktorisering.*

Beviset är mycket likt motsvarande bevis för Gaussiska heltal och utelämnas därför.

Vi ska nu visa att $\mathbb{Z}[\sqrt{-5}]$ inte tillåter oss att faktorisera element i irreducibla faktorer på ett entydigt sätt. Först observerar vi att

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{4.6}$$

Vi har $N(1 + \sqrt{-5}) = 6 = 2 \cdot 3$, men inga element i $\mathbb{Z}[\sqrt{-5}]$ har norm 2 eller 3. Alltså kan inga element i $\mathbb{Z}[\sqrt{-5}]$ förutom enheter eller talet självt dela $1 + \sqrt{-5}$, vilket betyder att $1 + \sqrt{-5}$ är irreducibelt. På samma sätt får vi att även $1 - \sqrt{-5}$ är irreducibelt. Vi har vidare $N(2) = 2^2$ och $N(3) = 3^2$, och detta betyder att även dessa tal är irreducibla. Ett tal i $\mathbb{Z}[\sqrt{-5}]$ som skulle dela 2 skulle ju behöva ha en norm som delar 2^2, och därmed skulle detta tals norm behöva vara lika med 2, eftersom 2^2 är en potens av primtalet 2. Vi vet emellertid att inga tal i $\mathbb{Z}[\sqrt{-5}]$ har norm 2. Motsvarande argument visar därefter att även 3 är irreducibelt. Detta visar att vi i (4.6) har gett ett exempel på två *skilda* irreducibla faktoriseringar av talet 6 i $\mathbb{Z}[\sqrt{-5}]$!

Det här visar att irreducibel faktorisering faktiskt är en rätt subtil sak!

Anmärkning 4.3.10. Vi avslutar det här kapitlet med en liten utblick. Den uppmärksamme läsaren kanske har märkt att det som kännetecknar både $\mathbb{Z}[\mathrm{i}]$ och $\mathbb{Z}[\sqrt{-5}]$ är att vi har infört ett speciellt tal, talet i respektive $\sqrt{-5}$, som vi låter uppfylla en andragradsekvation, och att vi sedan anpassar additionen och multiplikationen i våra talringar så att de tar hänsyn till detta. I själva verket kan man skapa mer allmänna så kallade *kvadratiska talringar* $\mathbb{Z}[\xi]$ på likartade sätt: vi låter då symbolen ξ vara en lösning till någon allmän ekvation på formen

$$x^2 + Bx + C, \quad B, C \in \mathbb{Z}.$$

Elementen i $\mathbb{Z}[\xi]$ låter vi vara på formen $z = a + b\xi$, och i alla räkningar byter vi ut ξ^2 mot $-C - B\xi$. Vi har studerat fallen som svarar mot $C = 1$ och $C = 5$. Mer omfattande studier av allmänna kvadratiska talringar brukar man bedriva i högre kurser i algebra.

Övningar

Övning 4.1. Visa att mängden $\mathbb{Z}[\mathrm{i}]$ av Gaussiska heltal satisfierar följande räkneregler.

1. $z + w \in \mathbb{Z}[\mathrm{i}]$
2. $z \cdot w \in \mathbb{Z}[\mathrm{i}]$.
3. $z + w = w + z$
4. $z \cdot w = w \cdot z$.
5. $z + (w + v) = (z + w) + v$.

6. $z \cdot (w \cdot v) = (z \cdot w) \cdot v$.
7. $z \cdot (w + v) = z \cdot w + z \cdot v$.
8. Talet $0 = 0 + 0\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ uppfyller $z + 0 = z$.
9. Talet $1 = 1 + 0\mathrm{i} \in \mathbb{Z}$ uppfyller $z \cdot 1 = z$.
10. För varje Gaussiskt heltal z finns ett Gaussiskt heltal som vi betecknar med $-z$ sådant att $z + (-z) = 0$.

Använd dig av motsvarande regler för heltal där det behövs!

Anmärkning: Som vi tidigare nämnts, visar detta att $\mathbb{Z}[\mathrm{i}]$ är en *kommutativ ring*.

Övning 4.2. Beräkna $z + w$, $z - w$ och zw för

1. $z = 3 + \mathrm{i}$ och $w = -1 + 4\mathrm{i}$
2. $z = -2\mathrm{i}$ och $w = 2 - 5\mathrm{i}$.

Övning 4.3. Visa att $N(a+b\mathrm{i}) = (a+b\mathrm{i})(a-b\mathrm{i})$ för normen i $\mathbb{Z}[\mathrm{i}]$. Visa också att vi har $N(z + w) = N(z) + N(w) + 2(ac + bd)$ för alla Gaussiska heltal z och w.

Övning 4.4. Låt z och w vara Gaussiska heltal skilda från 0 och bilda $\zeta = z \cdot w$. Visa att $N(\zeta) \geqslant N(z)$ och $N(\zeta) \geqslant N(w)$. När inträffar likhet?

Anmärkning: Detta bevisar Lemma 4.1.11.

5 Modulär aritmetik

5.1 Moduloräkning

Vi kommer nu fram till moduloräkning. Detta är ett lite annorlunda sätt att räkna med heltal på, även om det egentligen bygger på de vanliga räknesätten. Allt utgår från följande definition:

Definition 5.1.1. Låt $n \geqslant 1$ vara ett heltal. Vi säger att heltalen a och b är *kongruenta modulo* n, och skriver

$$a \equiv b \pmod{n},$$

om $n \mid (a - b)$.

Exempel 5.1.2. Låt $n = 12$. Exempelvis har vi att

$$16 \equiv 4 \pmod{12}, \quad -27 \equiv -3 \pmod{12} \quad \text{och} \quad 22 \equiv -2 \pmod{12},$$

eftersom 12 är en delare till alla tre talen $16 - 4 = 12$, $(-27) - (-3) = -24$ och $22 - (-2) = 24$. ▲

När man räknar modulo ett tal, exempelvis 12, kan man se det som att man betraktar alla tal som är kongruenta med varandra som samma tal. Enligt exemplet ovan är 16 och 4 ”samma tal” modulo 12, liksom 22 och -2. Därför verkar det inte alldeles orimligt, så länge man räknar modulo 12, att $16 + 22$ borde bli ”samma tal” som $4 - 2$. Mer korrekt kan vi skriva detta som

$$16 + 22 \equiv 4 - 2 \pmod{12}.$$

Denna kongruens gäller eftersom

$$16 + 22 - (4 - 2) = 36 = 12 \cdot 3.$$

Detta beteende är ingen speciellt för $n = 12$, utan gäller i allmänhet, vilket visas nedan.

Sats 5.1.3. *Låt n vara ett positivt heltal. Antag att heltalen $a, \tilde{a}$ samt $b, \tilde{b}$ uppfyller*

$$a \equiv \tilde{a} \pmod{n} \quad \textit{och} \quad b \equiv \tilde{b} \pmod{n}.$$

Då gäller

$$a + b \equiv \tilde{a} + \tilde{b} \pmod{n}$$

samt

$$a \cdot b \equiv \tilde{a} \cdot \tilde{b} \pmod{n}.$$

Bevis. Per definition vet vi att $n \mid (a - \tilde{a})$ och $n \mid (b - \tilde{b})$. Det betyder att det finns heltal x och y sådana att

$$a - \tilde{a} = nx \quad \text{och} \quad b - \tilde{b} = ny.$$

Nu följer

$$\begin{aligned}(a+b)-(\tilde{a}+\tilde{b}) &= (a-\tilde{a})+(b-\tilde{b})\\ &= nx+ny\\ &= n\cdot(x+y).\end{aligned}$$

Alltså gäller $n \mid (a+b)-(\tilde{a}+\tilde{b})$, vilket betyder att

$$a+b \equiv \tilde{a}+\tilde{b} \pmod{n}.$$

Vidare,

$$\begin{aligned}ab-\tilde{a}\tilde{b} &= ab-a\tilde{b}+a\tilde{b}-\tilde{a}\tilde{b}\\ &= a\cdot(b-\tilde{b})+(a-\tilde{a})\cdot b\\ &= a\cdot ny+nx\cdot b\\ &= n\cdot(ya+xb),\end{aligned}$$

och därmed $n \mid (ab-\tilde{a}\tilde{b})$, det vill säga

$$ab \equiv \tilde{a}\tilde{b} \pmod{n}. \qquad \square$$

Denna sats visar en av de stora fördelarna med moduloräkning. Genom att använda den kan vissa beräkningar förenklas väsentligt. Låt oss illustrera detta med ett par exempel.

Exempel 5.1.4. Låt $a = 228 \cdot 115$. Vi vet att det finns heltal q och r sådana att $a = 8 \cdot q + r$, där $0 \leqslant r < 8$. Bestäm r.

Lösning. Börja med att utföra heltalsdivision med 8 av talen 228 och 115:

$$228 = 8 \cdot 28 + 4 \quad \text{och} \quad 115 = 8 \cdot 14 + 3.$$

Detta betyder att $228 - 4 = 8 \cdot 28$ och $115 - 3 = 8 \cdot 14$, det vill säga att $8 \mid (228-4)$ och $8 \mid (115-3)$. Alltså gäller

$$228 \equiv 4 \pmod{8} \quad \text{och} \quad 115 \equiv 3 \pmod{8}.$$

Enligt satsen ovan får vi

$$a = 228 \cdot 115 \equiv 4 \cdot 3 = 12 \pmod{8}.$$

Men eftersom det uppenbarligen är så att $12 \equiv 4 \pmod{8}$ så följer

$$a \equiv 4 \pmod{8}$$

Alltså har vi $8 \mid (a-4)$, vilket per definition betyder att det finns ett heltal q sådant att $a - 4 = 8 \cdot q$. Vi får alltså

$$a = 8 \cdot q + 4, \quad \text{och därmed} \quad r = 4. \qquad \blacktriangle$$

Poängen med ovanstående exempel är att det är mycket enklare att heltalsdividera talen 228 och 115 med 8 än vad det är att utföra heltalsdivisionen med deras produkt $a = 228 \cdot 115 = 26\,200$.

Exempel 5.1.5. Låt $a = 3^{100}$. Det finns heltal q och r, där $0 \leqslant r < 6$ sådana att $a = 6 \cdot q + r$. Bestäm r.

Lösning. Observera att

$$3^3 = 27 = 6 \cdot 4 + 3 \equiv 3 \pmod{6}.$$

Alltså gäller

$$a = 3^{100} = 3 \cdot 3^{99} = 3 \cdot (3^3)^{33} \equiv 3 \cdot 3^{33} = 3 \cdot (3^3)^{11} \equiv 3 \cdot 3^{11} = 3^{12} \pmod{6}.$$

Vidare följer

$$a \equiv 3^{12} = (3^3)^4 \equiv 3^4 = 3 \cdot 3^3 \equiv 3 \cdot 3 = 9 \equiv 3 \pmod{6},$$

vilket betyder att vi kan skriva

$$a = 6 \cdot q + 3,$$

för något heltal q. Alltså får vi att $r = 3$. ▲

I detta exempel får vi en väldigt stor vinst. Talet $a = 3^{100}$ är enormt stort, om man skriver ut det så består det av 48 siffror, och antagligen alldeles för stort för de flesta miniräknare. Så utan moduloräkning blir det mycket svårt att bestämma r.

Sats 5.1.6. *Låt $n \geqslant 1$ vara ett heltal. För varje heltal a som är relativt prima med n gäller följande:*

1. *Det finns ett heltal x som löser ekvationen $ax \equiv 1 \pmod{n}$.*
2. *Om heltalen b, c uppfyller $ab \equiv ac \pmod{n}$ så måste $b \equiv c \pmod{n}$.*

Bevis. Eftersom a och n är relativt prima finns enligt Sats 2.2.3 heltal x, y sådana att

$$1 = xa + yn.$$

Detta betyder att $1 - xa = n \cdot y$, det vill säga att $n \mid (1 - xa)$, och därmed gäller $1 \equiv xa \pmod{n}$, vilket visar punkt 1.

För att visa punkt 2, antag att heltalen b, c uppfyller $ab \equiv ac \pmod{n}$. Per definition gäller

$$n \mid (ab - ac) = a \cdot (b - c).$$

Men eftersom n och a är relativt prima följer det från Sats 2.2.5 att $n \mid (b - c)$. Alltså får vi

$$b \equiv c \pmod{n}.$$ □

5.2 Ringen $\mathbb{Z}_n$

Låt oss nu införa ett alternativt sätt att se på moduloräkning. Detta sätt kan i vissa fall vara behändigare. Låt $n \geqslant 1$ vara ett fixerat heltal.

Givet ett heltal a, vet vi enligt Sats 1.3.1 att det finns heltal q och r, där r uppfyller $0 \leqslant r < n$, sådana att

$$a = n \cdot q + r.$$

Talet r är alltså resten vid heltalsdivision av a med n. Notera att

$$a \equiv r \pmod{n},$$

eftersom n uppenbarligen delar $a - r = nq$. I själva verket är r det enda tal som uppfyller både $a \equiv r \pmod{n}$ och $0 \leqslant r < n$. Vi kallar hädanefter r för *resten av a modulo n* och skriver

$$r = \mathrm{R}_n(a).$$

Det är alltså skillnad på att skriva $\mathrm{R}_n(a)$ och $a \equiv b \pmod{n}$. Det första uttrycket, $\mathrm{R}_n(a)$ är ett tal r som uppfyller $0 \leqslant r < n$, medan det andra uttrycket beskriver en relation mellan talen a och b.

Exempel 5.2.1. Låt $n = 13$ och $a = 15$. Vi har att

$$\mathrm{R}_n(a) = 2,$$

eftersom

$$a = n \cdot 1 + 2.$$

Observera igen att $\mathrm{R}_n(a)$ är ett tal r som uppfyller *både* $0 \leqslant r < n$ *och* $a \equiv r \pmod{n}$. Det finns oändligt många tal b som uppfyller $a \equiv b \pmod{n}$, exempelvis har vi att

$$15 \equiv -11 \pmod{13}, \quad 15 \equiv 81 \pmod{13}, \quad \text{och} \quad 15 \equiv 11\,015 \pmod{13}.$$

Men det är bara talet 2 bland dessa tal som ligger i intervallet $0 \leqslant b < n$. ▲

Exempel 5.2.2. Låt $n = 15$. Då gäller

$$\mathrm{R}_n(19) = 4, \quad \mathrm{R}_n(-27) = 3, \quad \mathrm{R}_n(11) = 11, \quad \mathrm{R}_n(30) = 0. \qquad ▲$$

Ännu enklare blir det för tal som 10 och 100:

Exempel 5.2.3. Vi har att

$$\mathrm{R}_{10}(67) = 7, \quad \mathrm{R}_{10}(4\,711) = 1, \quad \mathrm{R}_{10}(-118) = 2 \,(= 10 - 8).$$

Dessutom gäller

$$\mathrm{R}_{100}(1\,234) = 34, \qquad \mathrm{R}_{100}(-256) = 44 \,(= 100 - 56). \qquad ▲$$

Nu inför vi *ringen* $\mathbb{Z}_n$. Vi låter helt enkelt detta vara mängden

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Observera att $\mathrm{R}_n(a)$ är ett element i ringen $\mathbb{Z}_n$ för alla heltal a, eftersom $\mathrm{R}_n(a)$ per definition uppfyller $0 \leqslant \mathrm{R}_n(a) < n$. Mängden $\mathbb{Z}_n$ innehåller helt enkelt alla "rester modulo n".

Den stora vinsten med att införa dessa begrepp är att det förenklar språket för oss. Vi tillåter oss nämligen att "räkna", det vill säga utföra addition och multiplikation, *i ringen* $\mathbb{Z}_n$. Detta fungerar som vanlig addition och multiplikation, men resultatet av uträkningarna väljs *modulo* n.

Alltså: när vi räknar i ringen $\mathbb{Z}_n$ menar vi med $a+b$ egentligen talet $\mathrm{R}_n(a+b)$, och med $a \cdot b$ menar vi talet $\mathrm{R}_n(a \cdot b)$. På detta sätt kommer vi att som resultat av uträkningarna få ett tal r som uppfyller $0 \leqslant r < n$, det vill säga $r \in \mathbb{Z}_n$, och som är kongruent modulo n med det "vanliga" resultatet av uträkningen.

Exempel 5.2.4. Låt $n = 5$. Eftersom exempelvis

$$3 + 8 = 11 \equiv 1 \pmod{n},$$

så säger vi att

$$3 + 8 = 1 \text{ i ringen } \mathbb{Z}_n.$$

På samma sätt säger vi att

$$3 \cdot 8 = 4 \text{ i ringen } \mathbb{Z}_n,$$

eftersom $3 \cdot 8 = 24 \equiv 4 \pmod{n}$. ▲

En av de allra mest självklara matematiska identiteterna är $1 + 1 = 2$. Det visar sig dock när man använder moduloräkning att denna identitet kanske inte är så självklar när allt kommer omkring:

Exempel 5.2.5. Observera att

$$1 + 1 \equiv 0 \pmod{2}.$$

Utan att vara det minsta inkorrekt kan man alltså säga att

$$1 + 1 = 0,$$

om vi bara lägger till "i ringen $\mathbb{Z}_2$". ▲

5.3 Satser av Euler och Fermat

Nu kommer vi till en av matematikens mest berömda satser: *Fermats lilla sats*. Vi börjar med att bevisa *Eulers sats*, från vilken Fermats lilla sats följer.

Definition 5.3.1. Låt $n \geqslant 1$ vara ett heltal, och $\phi(n)$ vara antalet tal x med $1 \leqslant x < n$ som är relativt prima med n. Vi kallar ϕ *Eulers ϕ-funktion.*

Exempel 5.3.2. Om $n = 12$, så tittar vi på talen $x = 1, 2, \ldots, 11$. Vi observerar följande:

$$\begin{array}{llll} \text{sgd}\,(1,12) = 1, & \text{sgd}\,(2,12) = 2, & \text{sgd}\,(3,12) = 3, & \text{sgd}\,(4,12) = 4, \\ \text{sgd}\,(5,12) = 1, & \text{sgd}\,(6,12) = 6, & \text{sgd}\,(7,12) = 1, & \text{sgd}\,(8,12) = 4, \\ \text{sgd}\,(9,12) = 3, & \text{sgd}\,(10,12) = 2, & \text{sgd}\,(11,12) = 1. & \end{array}$$

Alltså är det precis de fyra talen 1, 5, 7 och 11 som är relativt prima med 12. Detta betyder att $\phi(12) = 4$. ▲

Exempel 5.3.3. Om p är ett primtal kommer alltid $\phi(p) = p - 1$, eftersom alla talen $1, 2, 3, \ldots, p-1$ är relativt prima med p. ▲

Sats 5.3.4 (Eulers sats)**.** *Let $n \geqslant 1$ vara ett heltal. Låt a vara ett heltal sådant att a och n är relativt prima. Då gäller*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Bevis. Låt $m = \phi(n)$. Enligt definitionen av ϕ-funktionen, finns det m tal bland $1, 2, \ldots, n-1$ som är relativt prima med n. Kalla dessa tal $b_1, b_2, \ldots, b_m$. Låt

$$c_1 = ab_1, \quad c_2 = ab_2, \quad \ldots, \quad c_m = ab_m.$$

Vi vet enligt Sats 1.3.1 att det finns tal $r_1, r_2, \ldots, r_m$ med $0 \leqslant r_j < n$, och tal $q_1, q_2, \ldots, q_m$ sådana att

$$c_j = n \cdot q_j + r_j, \quad j = 1, 2, \ldots, m.$$

Detta betyder bland annat att

$$c_j \equiv r_j \pmod{n}, \quad j = 1, 2, \ldots, m. \tag{5.1}$$

Till att börja med måste alla talen $r_1, r_2, \ldots, r_m$ vara olika, ty om $r_j = r_k$, där $j \neq k$, så får vi att $c_j - c_k = n \cdot q_j - n \cdot q_k = n \cdot (q_j - q_k)$, vilket betyder att

$$n \mid (c_j - c_k) = a \cdot (b_j - b_k),$$

och eftersom n och a är relativt prima måste enligt Sats 2.2.5 $n \mid (b_j - b_k)$, vilket är omöjligt eftersom både $1 \leqslant b_j \leqslant n-1$ och $1 \leqslant b_k \leqslant n-1$, och dessutom $b_j \neq b_k$.

Vidare, låt oss visa att r_j och n är relativt prima. Antag motsatsen, det vill säga att $\text{sgd}\,(r_j, n) > 1$. Då finns det ett tal $x > 1$ som delar både r_j och n. Vi kan skriva $r_j = x\tilde{r}$ och $n = x\tilde{n}$, för några heltal $\tilde{r}$ och $\tilde{n}$. Vi har att $\text{sgd}\,(x, a) = 1$ eftersom om det fanns ett tal $y > 1$ som delade både x och a så skulle det talet också dela $n = x\tilde{n}$, vilket skulle betyda att y vore en gemensam delare till a och n och detta är omöjligt eftersom a och n är relativt prima. Nu har vi

$$c_j = n \cdot q_j + r_j = x \cdot (\tilde{n} q_j + \tilde{r}),$$

vilket betyder att x är en delare till $c_j = ab_j$. Eftersom a och x är relativt prima måste $x \mid b_j$, enligt Sats 2.2.5. Men detta är omöjligt, eftersom $x > 1$ i så fall skulle vara en gemensam delare till n och b_j. Men vi vet från definitionen av b_j att n och b_j är relativt prima. Alltså är det inledande antagandet omöjligt, vilket betyder att r_j och n är relativt prima, för varje $j = 1, 2, \ldots, m$.

Notera i förbifarten att detta innebär att $r_j \neq 0$, eftersom om det vore så att $r_j = 0$ så skulle $\text{sgd}\,(r_j, n) = n$ (se Exempel 2.1.6), men vi vet ju nu att $\text{sgd}\,(r_j, n) = 1$.

Vi har alltså visat att $r_1, r_2, \ldots, r_m$ är m stycken olika tal som alla uppfyller $1 \leqslant r_j \leqslant n-1$, och att r_j och n är relativt prima. Men enligt definitionen av talen $b_1, b_2, \ldots, b_m$ var dessa alla tal som uppfyllde detta. Alltså har vi att

$$r_1, r_2, \ldots, r_m \quad \text{är precis talen} \quad b_1, b_2, \ldots, b_m,$$

även om ordningen på talen möjligtvis skiljer sig i de två fallen. Det följer att

$$b_1 b_2 \cdots b_m = r_1 r_2 \cdots r_m.$$

Från (5.1) får vi nu att

$$\begin{aligned} b_1 b_2 \cdots b_m \cdot a^m &= (ab_1)(ab_2)\cdots(ab_m) \\ &= c_1 c_2 \cdots c_m \\ &\equiv r_1 r_2 \cdot r_m = b_1 b_2 \cdots b_m \pmod{n}, \end{aligned}$$

det vill säga att

$$b_1 b_2 \cdots b_m \cdot a^m \equiv b_1 b_2 \cdots b_m \cdot 1 \pmod{n}.$$

Eftersom b_j och n är relativt prima, för alla $j = 1, 2, \ldots, m$, så kommer också talen $b_1 b_2 \cdots b_m$ och n vara relativt prima (att visa detta var Övning 3.4). Nu följer det från Sats 5.1.6 att

$$a^m \equiv 1 \pmod{n}. \qquad \square$$

Följdsats 5.3.5 (Fermats lilla sats)**.** *Låt p vara ett primtal. Då gäller*

$$a^{p-1} \equiv 1 \pmod{p},$$

för alla heltal a som inte delas av p.

Bevis. Eftersom a och p är relativt prima så fort p inte delar a, och eftersom $\phi(p) = p - 1$ så följer detta från Eulers sats. $\square$

Övningar

Övning 5.1. Beräkna $4 + 3$ i ringen $\mathbb{Z}_5$, $8 \cdot 7$ i ringen $\mathbb{Z}_9$ och 3^{100} i ringen $\mathbb{Z}_{10}$.

Övning 5.2. Fixera ett heltal $n \geqslant 1$. Visa följande egenskaper för modulorelationen:

1. För varje heltal a gäller $a \equiv a \pmod{n}$.
2. Låt a och b vara heltal. Om $a \equiv b \pmod{n}$ så gäller också $b \equiv a \pmod{n}$.
3. Antag att heltalen a, b, c uppfyller $a \equiv b \pmod{n}$ och $b \equiv c \pmod{n}$. Då gäller $a \equiv c \pmod{n}$.

Anmärkning: Detta visar att modulorelationen är en så kallad *ekvivalensrelation.*

Övning 5.3. Låt $n \geqslant 1$ vara ett heltal. Antag att $a \equiv b \pmod{n}$. Visa att $-a \equiv -b \pmod{n}$.

Övning 5.4. Bevisa följande variant av Fermats lilla sats:

Låt p vara ett primtal, och $a \in \mathbb{Z}$. Då gäller

$$a^p \equiv a \pmod{n}.$$

6 RSA-kryptering

Under det senaste århundradet har elektroniska apparater och datorer fått en allt mer framskjuten ställning i vårt samhälle, och därmed har även behovet av snabba algoritmer och effektiv kodning av information vuxit starkt. Även om dagens datorer har stor processorkraft krävs det nästan alltid att man inte bara skriver bra kod utan även utvecklar bra metoder inom exempelvis dataöverföring. Dåligt skriven kod eller långsamma algoritmer kan leda till program som inte kan lösa sina uppgifter på rimlig tid och som därmed är värdelösa! Kunniga dataloger och matematiker som förmår att analysera och lösa dessa problem fyller en mycket viktig funktion.

En stor del av informationen som överförs via datorer vill vi hålla hemlig. Vi vill ju undvika att vem som helst kan få tag på våra kontonummer eller lösenord, eller kan ta del av våra känsliga personuppgifter. Ett sätt att se till att det bara är den avsedde mottagaren som kan läsa våra meddelanden eller tolka den information vi skickar elektroniskt är att kryptera den. I det här kapitlet ska vi visa hur grundläggande resultat inom talteorin, som exempelvis Fermats lilla sats, kan utnyttjas för att skapa säkra krypteringssystem.

6.1 Krypteringssystem

Låt oss börja med att diskutera vad en matematiker menar med ett *krypteringssystem*.

Definition 6.1.1. Ett krypteringssystem består av två ändliga mängder M_1 och M_2 tillsammans med två funktioner $E : M_1 \to M_2$ och $D : M_2 \to M_1$ sådana att

$$D\left(E(x)\right) = x \quad \text{för} \quad x \in M_1. \tag{6.1}$$

Här tänker vi oss att M_1 utgör mängden av meddelanden som vi kan tänkas vilja skicka, och att mängden M_2 består av möjliga krypterade meddelanden. Funktionen E kallas för *krypteringsnyckel* medan D kallas *dekrypteringsnyckel*. Kravet (6.1) betyder helt enkelt att om vi är utrustade med rätt dekrypteringsnyckel, det vill säga, om vi är behöriga att läsa meddelandet, så kan vi dekryptera meddelandet $E(x)$ och återfå det ursprungliga meddelandet x.

Vi ska välja $M_1 = M_2 = \mathbb{Z}_N$ för något heltal N och arbeta med modulär aritmetik. Detta innebär ingen väsentlig inskränkning i vilka meddelanden vi kan skicka och ta emot. Vi kan ju exempelvis konvertera bokstäver till ASCII-kod och använda denna när vi krypterar.

Exempel 6.1.2. Vi börjar med ett enkelt exempel. Låt $M_1 = M_2 = \mathbb{Z}_2$ och sätt $E(x) = \mathrm{R}_2\left(x+1\right)$ och $D(y) = \mathrm{R}_2\left(y+1\right)$. Vi kan då skicka två meddelanden: 0 (”nej”) och 1 (”ja”). Låt oss anta att vi vill svara ”ja” på en hemlig fråga. Vi krypterar och får

$$E(1) = \mathrm{R}_2\left(1+1\right) = 0,$$

så mottagaren tar emot 0, det vill säga, ett "nej". En behörig mottagare dechiffrerar vårt meddelande

$$D\left(E(1)\right) = \mathrm{R}_2\left(0+1\right) = 1,$$

och tolkar vårt meddelande helt korrekt som ett "ja".

Ett ännu enklare exempel vore att låta $E(x) = \mathrm{R}_2\left(x\right)$ och $D(y) = \mathrm{R}_2\left(y\right)$. Detta motsvarar att vi inte krypterar alls, utan skriver vårt meddelande i klartext. ▲

Exemplet ovan illustrerar principen bakom kryptering, men systemet är alldeles för enkelt. Vi kanske kan lura någon som avlyssnar oss en eller två gånger, men sedan kan han eller hon eventuellt observera att vår motpart alltid handlar precis tvärtemot vad vi har skrivit till honom eller henne. Vår kryptering är sedan knäckt.

Följande typ av krypteringssystem brukar kallas *Caesarchiffer* eftersom det sägs ha använts redan av Julius Caesar.

Exempel 6.1.3. Vi låter $M_1 = M_2 = \mathbb{Z}_{28}$ eftersom alfabetet har 28 bokstäver; vi låter 0 motsvara "a", 1 motsvara "b" och så vidare. Sedan fixerar vi ett heltal $t \in \mathbb{Z}$ och inför $E_t : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$ genom

$$E(x) = \mathrm{R}_{28}\left(x+t\right).$$

Vi förskjuter alltså varje bokstav med t positioner och räknar modulärt. Om exempelvis $t = -2$ ser vi att "ja" krypteras till "hä" och "nej" krypteras till "lch". Vi lämnar det som en övning att bestämma dekrypteringsfunktionen $D_t : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$. ▲

Det senaste exemplet är lite mer raffinerat än det första, men vi inser ändå att det finns vissa nackdelar med systemen vi har behandlat hittills. Ett problem är att om man i något av de ovanstående fallen känner till krypteringsnyckeln så kan man även hitta dekrypteringsnyckeln. Det är ju inte så bra: vi vill ju eventuellt kunna ta emot meddelanden från många olika avsändare, som inte ska kunna läsa varandras meddelanden (om vi till exempel är en bank). För att folk ska kunna skicka krypterade meddelanden måste vi dela ut krypteringsnyckeln. Detta betyder att om vi som del av ett krypteringsnätverk måste komma överrens med varje annan deltagare om en kryperingsnyckel och en dekrypteringsnyckel, för att sedan hålla dessa hemliga för alla andra i nätverket. Tyvärr innebär detta att vi måste hålla reda på många olika krypteringssystem samtidigt.

Caesarchiffret lider dessutom också av att det är lättknäckt. Man kan genom att observera att vissa bokstäver och ord förekommer oftare än andra försöka sig på att knäcka krypteringen om man vet att det är just Caesarkryptering som har använts. Man försöker till exempel gissa sig till vilka krypterade ord som kommer från "en" eller "ett", och då kan man gissa vilken bokstav "e" skickas på av funktionen E. Sedan kan man helt enkelt testa om man har gissat rätt. Det finns naturligtvis mer sofistikerade metoder för att komma åt andra, mer komplicerade, krypteringssystem.

6.2 RSA-systemet

W. Diffie och M. Hellman lade 1976 i en uppsats fram idén om ett *krypteringssystem med offentlig krypteringsnyckel*. Istället för att varje par av deltagare ska dela på krypterings- och dekrypteringsnycklar, föreslår Diffie och Hellman att varje användare istället delar ut *en* krypteringsnyckel till alla som vill ha den, men att användarens dekrypteringsnyckel hålls hemlig. Det förutsätts att systemet är uppbyggt så att kunskap om krypteringsfunktionen E ger ingen, eller i varje fall mycket liten, information om dekrypteringsfunktionen D. Speciellt betyder det att man inte kan läsa de meddelanden man har krypterat, men det gör kanske inte så mycket. Om man kan uppnå detta blir fördelarna att krypteringssystemet blir svårknäckt, samt att varje användare nu bara måste hålla reda på sina egna funktioner, samt *en* funktion för varje annan användare. Vi ska i nästa avsnitt visa hur man kan använda sig av talteori för att konstruera svårknäckta krypteringssystem.

Ett mycket populärt, och relativt enkelt, krypteringssystem med offentlig nyckel beskrevs 1978 av R. Rivest, A. Shamir och L. Adleman. Det har fått namnet *RSA-kryptering* efter upphovsmännens efternamn. Det har senare visat sig att en engelsman, C. Cocks, runt samma tid hade upptäckt RSA-kryptering oberoende av Rivest, Shamir och Adleman, men eftersom han arbetade för brittiska försvaret förblev hans forskningsrapporter hemligstämplade fram tills nyligen!

Som deltagare i ett krypteringssystem väljer vi först två primtal p och q. Dessa primtal ska vara mycket stora, minst 100-siffriga, och de hålls hemliga för alla andra användare. Vi inför sedan de båda talen

$$n = pq \quad \text{och} \quad m = (p-1)(q-1). \tag{6.2}$$

Vi finner därefter två heltal e och d med $1 < e, d < m$ sådana att

$$ed \equiv 1 \pmod{m}. \tag{6.3}$$

Vi tar $M_1 = M_2 = \mathbb{Z}_n$ och inför krypteringsfunktionen $E : \mathbb{Z}_n \to \mathbb{Z}_n$ genom att låta

$$E(x) = \mathrm{R}_n\left(x^e\right)$$

och dekrypteringsfunktionen $D : \mathbb{Z}_n \to \mathbb{Z}_n$ genom

$$D(y) = \mathrm{R}_n\left(y^d\right).$$

Talparet (n, e) delas ut till alla användare som vill skicka krypterade meddelanden till oss. Eftersom vi vill hålla d hemlig, måste vi se till att p, q och m förblir hemliga. Man kan nämligen visa att det går att bestämma d, och därmed knäcka krypteringen, om man känner något av dessa tal.

Vi ska nu visa att systemet vi beskrivit ovan verkligen är ett krypteringssystem. I beviset använder vi Fermats lilla sats från det föregående kapitlet.

Sats 6.2.1. *Vi har $D\left(E(x)\right) = x$ och $E\left(D(y)\right) = y$ för alla $x, y \in \mathbb{Z}_n$.*

Bevis. Vi ska visa att $D\left(E(x)\right) = x$, det vill säga, att

$$(x^e)^d \equiv x^{ed} \equiv x \pmod{n},$$

vilket även kan skrivas

$$x^{ed} - x \equiv 0 \pmod{n}.$$

Vi måste alltså visa att n delar differensen $x^{ed} - x$. Vi vet att p och q är primtal och att $n = pq$, så det räcker att visa att p och q delar $x^{ed} - x$.

Eftersom $ed \equiv 1 \pmod{m}$ följer det att $ed - 1$ är en multipel av $m = (p-1)(q-1)$, det vill säga, att

$$ed = 1 + k(p-1)(q-1) \tag{6.4}$$

för något heltal k. Vidare medför Fermats lilla sats att

$$x^{p-1} \equiv 1 \pmod{p}. \tag{6.5}$$

Vi använder först (6.4) och sedan (6.5) och får

$$x^{ed} \equiv x^{1+k(p-1)(q-1)} \equiv x \cdot \left(x^{p-1}\right)^{k(q-1)} \equiv x \cdot 1^{k(q-1)} \equiv x \pmod{p},$$

vilket visar att p delar $x^{ed} - x$. Genom att byta plats på p och q erhåller vi att även q delar $x^{ed} - x$, och nu följer $D\left(E(x)\right) = x$.

Beviset för att $E\left(D(y)\right) = y$ är snarlikt och vi uppmanar läsaren att utföra detaljerna. □

Som vi har observerat är det mycket viktigt att övriga användare inte kan ta reda på primtalen p och q utgående från n. Vi vill alltså välja mycket stora primtal p och q. Det är nämligen oerhört tidskrävande att faktorisera ett stort, säg 200-siffrigt, sammansatt n tal i primtalsfaktorer. Ett naivt sätt är att testa med alla heltal som är mindre än $\sqrt{n}$-fundera gärna på varför det räcker med detta! för att se om något av dem delar n. Det finns mycket bättre algoritmer, men inte heller dessa är tillräckligt effektiva för att RSA-krypteringen ska kunna knäckas: även med snabb dator finns det i nuläget inget hopp att genomföra en sökning i rimlig tid-det skulle snarare ta tusentals år. Vi vill dessutom helst se till att de primtalen vi väljer inte finns i tabeller över kända primtal. Lyckligtvis finns det olika metoder för att hitta nya, stora primtal. Ofta bygger dessa metoder på att man använder Fermats lilla sats och sannolikhetsteori, men vi går inte in på hur dessa fungerar här.

Slutsatsen är att RSA-kryptering är relativt säker. Nu måste vi fundera på om systemet går att implementera på ett bra sätt. Att utföra multiplikationerna $n = pq$ och $m = (p-1)(q-1)$ är oproblematiskt. Eftersom vi, men inte de övriga RSA-användarna, känner p och q kan vi välja e så att $\operatorname{sgd}(e, m) = 1$, och sedan kan Euklides algoritm användas för att hitta inversen $d \equiv e^{-1} \pmod{m}$. När vi nu vill börja kryptera kommer vi att behöva beräkna uttryck av typen $x^e \pmod{n}$, där de ingående talen är mycket stora, så det är viktigt

att utföra dessa beräkningar på ett effektivt sätt. Ett bra sätt är att utföra succesiva kvadreringar.

Vi kan nämligen alltid skriva talet e på formen

$$e = e_N 2^N + e_{N-1} 2^{N-1} + \cdots + e_0,$$

där e_j:na är antingen 0 eller 1. Exempelvis har vi

$$9 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1, \quad 31 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1.$$

Vi observerar sedan att

$$x^e = x^{e_N 2^N} x^{e_{N-1} 2^{N-1}} \cdots x^{e_0}$$

Alla ingående faktorer är nu på formen x^{2^j}, så vi behöver bara beräkna $x, x^2 x^4, \cdots$ modulo n och multiplicera ihop de potenser vi behöver. Om vi använder denna metod i vår implementering av RSA kan de nödvändiga beräkningarna utföras tillräckligt snabbt.

Det finns naturligtvis risker med att förlita sig på RSA-kryptering. Det är inte omöjligt att någon en dag kommer att konstruera en faktoriseringsalgoritm som är väsentligt mycket snabbare än de nu kända, och att man då kommer att kunna bestämma p och q från n på kort tid. Om detta inträffar skulle RSA-kryptering med en gång vara värdelöst.

Exempel 6.2.2. Vi går nu igenom ett exempel på RSA-kryptering i detalj. För att kunna räkna för hand låter vi de ingående talen vara orealistiskt små.

Vi låter $p = 7$ och $q = 13$. Detta ger

$$n = 7 \cdot 13 = 91, \quad m = 6 \cdot 12 = 72.$$

Vi sätter därefter $e = 23$, vilket är ett lämpligt val då $(e, m) = (23, 72) = 1$. För att bestämma d använder vi Euklides algoritm och får att

$$\begin{aligned} 72 &= 3 \cdot 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Detta ger att

$$\begin{aligned} 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (23 - 7 \cdot 3) &= 8 \cdot 3 - 1 \cdot 23 \\ &= 8 \cdot (72 - 3 \cdot 23) - 1 \cdot 23 = -25 \cdot 23 + 8 \cdot 72. \end{aligned}$$

Vi väljer därför $d = 47 \equiv -25 \pmod{72}$. Vi har nu bestämt alla parametrar vi behöver för att kunna börja kryptera.

Låt oss anta att vi vill skicka meddelandet 24. Vi har då att beräkna $E(24) = 24^{23} \pmod{91}$. Vi har

$$24^{23} = 24^{16+4+2+1} = 24^{16} \cdot 24^4 \cdot 24^2 \cdot 24,$$

och vi beräknar

$$\begin{aligned} 24^2 = 576 &\equiv 30 \pmod{91} \\ 24^4 = 30^2 = 900 &\equiv 81 \pmod{91} \\ 24^8 = 81^2 &\equiv 9 \pmod{91} \\ 24^{16} = 9^2 &\equiv 81 \pmod{91}. \end{aligned}$$

Detta ger tillsammans $24^{23} = 81 \cdot 81 \cdot 30 \cdot 24 \equiv 19 \pmod{91}$, och vår mottagare erhåller meddelandet 19. ▲

6.3 Övningar

Övning 6.1. Bestäm dekrypteringsfunktionen $D_t : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$ för Caesarchiffret med krypteringsfunktionen $E_t(x) = \mathrm{R}_{28}(x + t)$. Testa ditt svar för $t = -2$ genom att först kryptera och sedan dekryptera $x_1 = 10$ samt $x_2 = 1$, det vill säga ordet ”ja”.

Övning 6.2. Betrakta ett RSA-krypteringssystem med offentliga nycklar n och e. Visa att man kan bestämma d, och därmed knäcka krypteringssystemet, om man känner någon av m, p eller q.

Övning 6.3. Betrakta krypteringssystemet i det avslutande exemplet. Dekryptera meddelandet 2 och kryptera meddelandet 3.

Övning 6.4. Skriv talen 73 och 91 på formen

$$e_N 2^N + e_{N-1} 2^{N-1} + \cdots + e_1 2^1 + e_0 2^0.$$

7 Kvadratisk reciprocitet

Det här avslutande kapitlet ägnar vi åt ett resultat som brukar kallas *lagen om kvadratisk reciprocitet* och som visades 1798 av C.F. Gauss i hans doktorsavhandling *Disquisitiones arithmeticae* ("Aritmetiska undersökningar"). Gauss var bara 21 år gammal när han skrev detta sitt mästerverk, som ofta anses vara den första moderna framställningen av talteorin. Gauss avhandling var för övrigt ett av de sista viktiga vetenskapliga verken i Europa som skrevs uteslutande på latin!

Kvadratisk reciprocitet handlar, som namnet antyder, om kvadrater. Mer precist ska vi undersöka hur man kan avgöra om ett heltal är en kvadrat modulo ett primtal.

7.1 Kvadratiska rester

Utgångspunkten för våra undersökningar i det här kapitlet är följande problem. Låt a vara ett givet heltal. För vilka primtal p existerar då ett heltal x sådant att

$$x^2 \equiv a \pmod{p}?$$

Denna frågeställning härrör från det mer allmänna problemet att bestämma vilka heltal a som har kvadratrötter (som också är heltal) när vi räknar modulo något heltal n. Man kan nämligen visa (men vi avstår från det här) att ekvationen

$$x^2 \equiv a \pmod{n}$$

har heltalslösningar x om och endast om

$$x^2 \equiv a \pmod{p_j}$$

har lösningar för alla primtal p_j ingår i faktoriseringen av n!

Definition 7.1.1. Vi säger att ett heltal a med $\gcd(a, n) = 1$ är en *kvadratisk rest* modulo n om det finns ett heltal x sådant att $x^2 \equiv a \pmod{n}$. Vi betecknar mängden av kvadratiska rester modulo n med Q_n.

Exempel 7.1.2. Låt oss först studera det enklaste fallet: $n = 2$. Om a är ett udda tal, $a = 2k+1$ för något heltal k, och x är ett annat udda tal, $x = 2l+1$, så har vi

$$a \equiv 1 \pmod{2}$$

och

$$(2l+1)^2 = 4l^2 + 2l + 1 = 2(2l^2 + l) + 1 \equiv 1 \pmod{2}.$$

Vi ser alltså att alla udda tal är kvadratiska rester modulo 2. ▲

Vi vet sedan tidigare att det finns heltal som inte har kvadratrötter som är heltal; två exempel är talen 2 och -1. Samma sak kan inträffa i modulär aritmetik också: vissa tal har inga kvadratrötter. Låt oss titta på ett exempel när detta inträffar.

Exempel 7.1.3. Betrakta ringen $\mathbb{Z}_5$. Vi beräknar kvadraterna av alla element i ringen och får

$$1^2 \equiv 1 \pmod 5, \quad 2^2 \equiv 4 \pmod 5,$$
$$3^2 = 9 \equiv 4 \pmod 5, \quad 4^2 = 16 \equiv 1 \pmod 5.$$

Alltså är talen 1 och 4 kvadratiska rester, medan 2 och 3 inte är det. ▲

Låt oss studera ett exempel till.

Exempel 7.1.4. Vi kvadrerar alla elementen i $\mathbb{Z}_7$ och får

$$1^2 \equiv 1 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 3^2 = 9 \equiv 2 \pmod 7,$$
$$4^2 = 16 \equiv 2 \pmod 7, \quad 5^2 = 15 \equiv 4 \pmod 7, \quad 6^2 = 36 \equiv 1 \pmod 7.$$

Våra räkningar visar att 1, 2 och 4 är kvadratiska rester, medan 3, 5 och 6 inte är det. ▲

Eftersom $1^2 = 1$ är 1 en kvadratisk rest modulo alla primtal, men redan för talet 2 blir det svårare att avgöra om det är en kvadratisk rest modulo p.

Ett naivt sätt att angripa problemet är att beräkna kvadraterna av alla element i $\mathbb{Z}_p$ och göra en lista över de kvadratiska resterna för varje primtal p, precis som vi har gjort i våra exempel. Den här metoden är inte särskilt elegant, och om primtalet p är stort blir de nödvändiga beräkningarna omfattande. Det vi istället vill ha är någon slags allmän beskrivning av primtalen p för vilka a är en kvadratisk rest.

7.2 Legendresymboler och lagen om kvadratisk reciprocitet

Vi inför nu den mycket praktiska *Legendresymbolen* som hjälper oss att hålla reda på om a är en kvadratisk rest eller inte.

Definition 7.2.1. Låt a vara ett heltal och låt p vara ett udda primtal. Vi definierar *Legendresymbolen* för a som

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{om} \quad p \mid a, \\ 1 & \text{om} \quad p \nmid a,\ a \in Q_p, \\ -1 & \text{om} \quad p \nmid a,\ a \notin Q_p. \end{cases} \tag{7.1}$$

Heltalet a är alltså en kvadratisk rest modulo p om $\left(\frac{a}{p}\right) = 1$. Fördelen med Legendresymbolen är att vi kan räkna med den!

Lemma 7.2.2. *För alla heltal a och b gäller*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \tag{7.2}$$

samt, om $a \equiv b \pmod p$,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \tag{7.3}$$

Beviset för lemmat bygger på en speciell egenskap hos $\mathbb{Z}_p$ när p är ett primtal.

Sats 7.2.3. *Låt p vara ett primtal. Då existerar ett tal ζ_p i $\mathbb{Z}_p$, en så kallad* primitiv rot*, sådant att varje z i $\mathbb{Z}_p$ kan skrivas på formen*

$$z = \zeta_p^j = \zeta_p \cdot \zeta_p \cdots \zeta_p$$

för något heltal $j \geqslant 0$.

Den primitiva roten ger oss faktiskt även alla element i Q_p: de är på formen ζ_p^{2j}. Vi ska förklara varför detta är sant. De a i $\mathbb{Z}_p$ som kan skrivas som $a = \zeta_p^{2k} \pmod p$ är ju kvadratiska rester enligt definitionen, och om $a = \zeta_p^k$ är en kvadratisk rest modulo p har vi $x^2 \equiv a \pmod p$ för något x i $\mathbb{Z}_p$. Även x kan skrivas med hjälp av den primitiva roten, säg $x = \zeta_p^j$, och detta ger oss

$$a = x^2 = (\zeta_p^j)^2 = \zeta_p^k \pmod p$$

vilket betyder att $k \equiv 2j \pmod p$, så k är jämnt.

Vi ger det som en övning att visa att om ζ_p är en primitiv rot så gäller

$$\left(\frac{\zeta_p^j}{p}\right) = (-1)^j, \tag{7.4}$$

och det är detta faktum som vi ska utnyttja i beviset för lemmat.

Bevis av Lemma 7.2.2. Vi börjar med det första påståendet. Om p delar a eller b delar ju p även deras produkt, så från Legendresymbolens definition följer

$$\left(\frac{ab}{p}\right) = 0.$$

Å andra sidan är minst en av $\left(\frac{a}{p}\right)$ och $\left(\frac{b}{p}\right)$ lika med 0, så likheten gäller i detta fall.

Vi antar nu att p inte delar a eller b. Om ζ_p är en primitiv rot har vi $a = \zeta_p^j$ och $b = \zeta_p^k$ för några heltal j och k. Vi har då $ab = \zeta_p^{j+k}$, och det följer att

$$\left(\frac{ab}{p}\right) = (-1)^{j+k} = (-1)^j(-1)^k = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Vi har således visat det första påståendet.

Nu ska visa att om $a = b \mod p$ så har a och b:s Legendresymboler samma värde. Att a och b är kongruenta modulo p betyder att $a = b + kp$ för något heltal k. Om p delar a delar p även $a - kp$ och därmed b. Om p inte delar a och a är en kvadratisk rest gäller $x^2 \equiv a \equiv b \mod p$, så b att även b är en kvadratisk rest. På samma sätt följer att b inte kan vara en kvadratisk rest om a inte är det. □

I våra exempel såg vi att det fanns lika många kvadratiska rester som tal som inte är kvadratiska rester. Det visar sig att detta alltid är sant om man bortser från fallet $p = 2$ som vi redan har behandlat. Kom ihåg att $p-1$ alltid är jämnt om p är ett primtal större än 2.

Sats 7.2.4. *För varje p gäller att antalet tal som är kvadratiska rester är lika med antalet tal som inte är kvadratiska rester.*

Satsen följer i själva verket direkt från likheten (7.4).

Att bestämma huruvida talet a är en kvadratisk rest modulo p är samma sak som att beräkna Legendresymbolen för a. Från ovanstående lemma följer att om vi skriver a som en produkt

$$a = q_1 q_2 \cdots q_N \tag{7.5}$$

av primtal q_j, så räcker det att evaluera de N Legendresymbolerna

$$\left(\frac{q_1}{p}\right), \left(\frac{q_2}{p}\right), \ldots, \left(\frac{q_N}{p}\right)$$

och sedan beräkna deras produkt. Om produkten är lika med 1 är a en kvadratisk rest modulo p, annars inte.

Vi kan nu formulera den berömda *lagen om kvadratisk reciprocitet*. Detta resultat förmodades av A.M. Legendre och bevisades av Gauss.

Sats 7.2.5. *Låt p och q, $p \neq q$, vara två udda primtal. Då gäller*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \tag{7.6}$$

såvida inte $p \equiv q \equiv 3 \mod 4$. Om $p \equiv q \equiv 3 \mod 4$ gäller istället

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right). \tag{7.7}$$

Beviset är ganska invecklat, så vi måste dessvärre avstå ifrån det i det här kompendiet.

En alternativ, och lite kortare, formulering av Gauss sats är

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}. \tag{7.8}$$

Vi kan nu förklara varför satsen heter som den gör. Ordet ”reciprocitas” betyder ömsesidighet på latin: Legendresymbolen för p med avseende på q är (upp till ett eventuellt minustecken) lika med Legendresymbolen för q med avseende på p. Frågorna om q är en kvadratisk rest modulo p och om p är en kvadratisk rest modulo q besvarar alltså varandra!

Vi ger nu några exempel på hur man kan använda lagen om kvadratisk reciprocitet.

Exempel 7.2.6. Är $a = 83$ en kvadratisk rest modulo $p = 103$? Alternativet att kvadrera alla element i $\mathbb{Z}_{103}$ känns inte särskilt lockande, så vi använder Gauss resultat istället.

Vi observerar först att $83 \equiv 3 \pmod 4$ och att $103 \equiv 3 \pmod 4$, så om vi vill tillämpa lagen om kvadratisk reciprocitet måste vi använda (7.7). Vi får att

$$\left(\frac{83}{103}\right) = -\left(\frac{103}{83}\right) = -\left(\frac{20}{83}\right),$$

efter att vi i andra steget utnyttjat att $103 \equiv 20 \pmod{83}$. Vi faktoriserar sedan $20 = 2^2 \cdot 5$ och använder räknereglerna för Legendresymbolen för att få

$$\left(\frac{83}{103}\right) = -\left(\frac{2}{83}\right)^2 \cdot \left(\frac{5}{83}\right).$$

Nu skulle vi kunna beräkna $\left(\frac{2}{83}\right)$, men det räcker i det här fallet att notera att

$$\left(\frac{2}{83}\right)^2 = [\pm 1]^2 = 1.$$

Vi använder detta, tillämpar lagen om kvadratisk reciprocitet en gång till, samt reducerar modulo 5, för att få

$$\left(\frac{83}{103}\right) = -\left(\frac{5}{83}\right) = -\left(\frac{83}{5}\right) = -\left(\frac{3}{5}\right).$$

Notera att $5 \equiv 1 \pmod 4$, så vi kan tillämpa (7.6). Vi har i andra exemplet i detta kapitel observerat att 3 inte är en kvadratisk rest modulo 5, så vi får till slut

$$\left(\frac{83}{103}\right) = -\left(\frac{3}{5}\right) = -(-1) = 1,$$

vilket visar att $83 \in Q_p$. ▲

Exempel 7.2.7. För vilka primtal p har vi $3 \in Q_p$?

Vi börjar med att notera att $3 \equiv 3 \pmod 4$, så vi kommer att behöva vara försiktiga när vi använder lagen om kvadratisk reciprocitet. Vi ser att $3 \in Q_2$ och att $3 \notin Q_3$, så vi kan i fortsättningen anta att $p > 3$.

Vi skiljer på två fall: $p \equiv 1 \pmod 4$ och $p \equiv 3 \pmod 4$. Om det första fallet inträffar har vi

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right),$$

och den enda kvadratiska resten i $\mathbb{Z}_3$ är 1. Alltså är 3 en kvadratisk rest om $p \equiv 1 \pmod 4$ och $p \equiv 1 \pmod 3$, det vill säga, vi måste ha $p \equiv 1 \pmod{12}$.

Om vi istället har $p \equiv 3 \pmod 4$ använder vi (7.7) och får

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right),$$

och uttrycket i högerledet är positivt om p *inte* är en kvadratisk rest modulo 3. Detta inneträffar om $p \equiv 2 \pmod 3$, vilket medför att vi måste ha $p \equiv 11 \pmod{12}$.

Alltså är $3 \in Q_p$ om $p = 2$, om $p \equiv 1 \pmod{12}$ eller $p \equiv 11 \pmod{12}$. Detta stämmer överrens med de exempel vi tittade på i början, vi såg ju att $3 \notin Q_5$ och $3 \notin Q_7$. ▲

Det är viktigt att notera att satsen om kvadratisk reciprocitet, som vi har formulerat den, kräver att både p och q är udda primtal. Vi kompletterar satsen med följande resultat som tar hand om fallet $q = 2$.

Sats 7.2.8. *Om p är ett udda primtal gäller*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

och speciellt är 2 en kvadratisk rest om och endast om $p \equiv \pm 1 \pmod 8$.

Bevis. Vi avstår från att ge beviset här. □

Tyvärr kan lagen om kvadratisk reciprocitet bara hjälpa oss att besvara frågan om det överhuvudtaget existerar x sådant att

$$x^2 \equiv a \pmod p,$$

den säger ingenting om hur man kan beräkna det sökta talet x. Detta kräver andra metoder, som vi inte kan ta upp här.

Övningar

Övning 7.1. Bestäm samtliga kvadratiska rester modulo 11 och 13.

Övning 7.2. Visa att om p är ett primtal, ζ_p är en primitiv rot och $a = \zeta_p^j$ för något j så gäller

$$\left(\frac{a}{p}\right) = (-1)^j$$

Övning 7.3. Är 43 en kvadratisk rest modulo 923?

Ledning: Är 923 ett primtal? Om så inte är fallet kan det vara till hjälp att läsa igenom inledningen till kapitlet.

Övning 7.4. För vilka primtal p har vi $5 \in Q_p$?

Lösningar till udda övningsuppgifter

Övning 0.1.

1. $B \cup C = A$.
2. $B \cap C = \emptyset$.
3. $D \cap C = \{4, 36\}$.
4. $\{x \in D : x \in B\} = D \cap B = \{1, 19, 101\}$.
5. $\{x \in A : x = y + 1 \text{ för något } y \in D\} = \{2, 5, 20, 37, 102\}$.
6. $\{x + 1 : x \in D\} = \{2, 5, 20, 37, 102\}$.

Övning 0.3. Tag $x \in ((A \cap C) \cup (B \cap C^c))^c$. Det betyder att $x \in \Omega$ och $x \notin (A \cap C) \cup (B \cap C^c)$. Alltså har vi att $x \notin A \cap C$ och $x \notin B \cap C^c$. Det finns nu två möjligheter: $x \in C$ och $x \notin C$.

I det första fallet, det vill säga $x \in C$, måste $x \notin A$ eftersom om $x \in A$ så skulle $x \in A \cap C$ vilket är falskt. Alltså gäller $x \in A^c$, vilket tillsammans med $x \in C$ ger att $x \in A^c \cap C$ i detta fall. I synnerhet har vi att $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I det andra fallet gäller $x \in C^c$ och då måste $x \in B^c$ eftersom om $x \in B$ så skulle $x \in B \cap C^c$ vilket är falskt. Alltså gäller $x \in B^c \cap C^c$, och i synnerhet $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I båda fallen gäller alltså $x \in (A^c \cap C) \cup (B^c \cap C^c)$, och eftersom x var godtycklig så visar detta att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$.

Omvänt, tag $x \in (A^c \cap C) \cup (B^c \cap C^c)$. Då gäller $x \in A^c \cap C$ eller $x \in B^c \cap C^c$ (eller båda). Vi har alltså dessa två fall.

I det första fallet, det vill säga $x \in A^c \cap C$, har vi att $x \notin A$ och $x \notin C^c$. I synnerhet har vi att $x \notin A \cap C$ (eftersom $x \notin A$) och att $x \notin B \cap C^c$ (eftersom $x \notin C^c$). Alltså tillhör x varken $A \cap C$ eller $B \cap C^c$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I det andra fallet, det vill säga $x \in B^c \cap C^c$ har vi att $x \notin B$ och att $x \notin C$. Det följer att $x \notin A \cap C$ och att $x \notin B \cap C^c$. Alltså gäller $x \notin (A \cap C) \cup (B \cap C^c)$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I båda fallen har det alltså visats att $x \in ((A \cap C) \cup (B \cap C^c))^c$, och eftersom x var godtycklig visar detta att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$.

Vi har alltså visat att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$ och att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$ och därmed att $((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c)$.

Övning 1.1.

1. $q = 2$, $r = 6$ eftersom $32 = 13 \cdot 2 + 6$.

2. $q = -4$, $r = 4$ eftersom $-24 = 7 \cdot (-4) + 4$.

3. $q = 176$, $r = 2$ eftersom $1762 = 10 \cdot 176 + 2$.

4. $q = 0$, $r = 10$ eftersom $10 = 1762 \cdot 0 + 10$.

5. $q = -2$, $r = 0$ eftersom $-70 = 35 \cdot (-2) + 0$.

Övning 1.3. Vi har att

$$0 = a - a = (b \cdot q + r) - (b \cdot q + \tilde{r}) = r - \tilde{r}.$$

Att $r - \tilde{r} = 0$ medför att $r = \tilde{r}$ (eftersom $r = r + (\tilde{r} - \tilde{r}) = (r - \tilde{r}) + \tilde{r} = 0 + \tilde{r} = \tilde{r}$).

Övning 1.5.

1. Låt a vara ett godtyckligt heltal. Vi har att $a = a \cdot 1$, vilket per definition betyder att $a \mid a$.

2. Antag att $a \mid b$ och $b \mid c$. Per definition finns då heltal q_1 och q_2 sådana att $b = a \cdot q_1$ och $c = b \cdot q_2$. Nu har vi att $c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot q_1 q_2$, vilket per definition betyder att $a \mid c$, eftersom $q_1 q_2$ är ett heltal.

3. Vi ska alltså visa att det finns heltal a och b sådana att $a \mid b$ men $b \nmid a$. Låt $a = 1$ och $b = 2$. Då gäller uppenbarligen detta.

Övning 2.1. Per definition gäller $d \in D(a)$ och $d \in D(b)$. Alltså har vi $d \in D(a) \cap D(b)$. Det återstår att visa att d är en övre begränsning för $D(a) \cap D(b)$. Tag $x \in D(a) \cap D(b)$. Enligt uppgiftslydelsen gäller $x \mid d$. Alltså finns ett heltal q sådant att $d = x \cdot q$. Eftersom både $d > 0$ och $x > 0$ så måste $q > 0$. I och med att q är ett heltal följer det att $q \geqslant 1$. Nu gäller

$$d = x \cdot q \geqslant x \cdot 1 = x.$$

Alltså har vi att $d \geqslant x$, för alla $x \in D(a) \cap D(b)$, vilket betyder att d är en övre begränsning för $D(a) \cap D(b)$. Saken är klar.

Övning 2.3. Vi har att

$$\begin{aligned} 139 &= 117 \cdot 1 + 22 \\ 117 &= 22 \cdot 5 + 7 \\ 22 &= 7 \cdot 3 + 1. \end{aligned}$$

Använd dessa uträkningar baklänges och få

$$\begin{aligned} 1 &= 22 - 7 \cdot 3 \\ &= 22 - (117 - 22 \cdot 5) \cdot 3 = -117 \cdot 3 + 22 \cdot 16 \\ &= -117 \cdot 3 + (139 - 117 \cdot 1) \cdot 16 = 139 \cdot 16 - 117 \cdot 19. \end{aligned}$$

Alltså är $x = 16$ och $y = -19$.

Övning 3.1. Vi har att

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3, \\ 26 &= 2 \cdot 13, \\ 55 &= 5 \cdot 11, \\ 98 &= 2 \cdot 7 \cdot 7, \\ 150 &= 2 \cdot 3 \cdot 5 \cdot 5, \\ 210 &= 2 \cdot 3 \cdot 5 \cdot 7, \\ 315 &= 3 \cdot 3 \cdot 5 \cdot 7, \\ 455 &= 5 \cdot 7 \cdot 13. \end{aligned}$$

Övning 3.3. Sätt $d = \text{sgd}\,(a, p)$. Då är d en delare till både a och p. Eftersom $d > 0$ är en delare till p och eftersom p är ett primtal så måste antingen $d = 1$ eller $d = p$. I det första fallet gäller $\text{sgd}\,(a, p) = d = 1$. I det andra fallet noterar vi att eftersom d är en delare till a och $d = p$ så gäller $p \mid a$.

Övning 4.1. Vi går igenom var och en av punkterna i tur och ordning. Vi sätter genomgående $z = a + b\text{i}$, $w = c + d\text{i}$ och $v = e + f\text{i}$.

1. Enligt definitionen får vi $z + w = a + c + (b + d)\text{i}$ och eftersom summan av två heltal är ett heltal följer att $a + c$ och $b + d$ är heltal. Därmed är $z + w$ ett nytt Gaussiskt heltal.

2. Produkten zw beräknas enligt definitionen av multiplikation som $zw = ac - bd + (ad + bc)\text{i}$. Produkten av två vanliga heltal är ett nytt heltal, och således är ac, bd, ad och bc heltal. Vi utnyttjar sedan att summor och differenser av heltal är heltal för att kunna dra slutsatsen att zw är ett Gaussiskt heltal.

3. Vi har $z + w = a + c + (b + d)\text{i}$, och eftersom ordningen inte spelar någon roll vid addition av heltal kan vi istället skriva $z + w = c + a + (d + b)\text{i}$. Detta är enligt definitionen lika med $w + z$, och därmed är likheten bevisad.

4. Vi har enligt definitionen av multiplikation att $zw = ac - bd + (ad + bc)\text{i}$ och $wz = ca - db + (da + cb)\text{i}$. Vi vet emellertid att $ac = ca$, $bd = db$, $ad = da$ och $bc = cb$ för heltal a, b, c och d. Genom att utnyttja detta finner vi att $zw = wz$.

5. Vi adderar först w och v och lägger därefter till z, och får

   $$z + (w + v) = a + b\text{i} + (c + e + (d + f)\text{i}) = a + (c + e) + (b + (d + f))\text{i}.$$

   Addition av vanliga heltal satisfierar associativa lagen, och detta betyder att högerledet ovan är lika med

   $$(a + c) + e + ((b + d) + f)\text{i},$$

   men detta är precis vad man får om man först beräknar $z+w$ och därefter adderar v. Likheten följer nu.

6. Vi beräknar först $wv = ce - df + (cf + de)\mathrm{i}$ och därefter

$$z \cdot (w \cdot v) = a(ce - df) - b(cf + de) + [a(cf + de) + b(ce - df)]\mathrm{i}.$$

Vi utvecklar sedan parenteserna och finner att

$$\begin{aligned} z \cdot (w \cdot v) = ace - adf - bcf - bde \\ +(acf + ade + bce - bdf)\mathrm{i}. \end{aligned}$$

Om vi istället först räknar ut $zw = ac - bd + (ad + bc)\mathrm{i}$ och därefter multiplicerar med v får vi

$$(z \cdot w) \cdot v = e(ac - bd) - f(ad + bc) + [e(ad + bc) + f(ae - bd)]\mathrm{i}.$$

Vi multiplicerar ut parenteserna och finner att

$$\begin{aligned} (z \cdot w) \cdot v = ace - bde - adf - bcf \\ +(ade + bce + acf - bdf)\mathrm{i}. \end{aligned}$$

Vi påminner oss om att ordningen inte spelar någon roll när vi adderar vanliga heltal och med detta i åtanke jämför vi nu uttrycken för $z \cdot (w \cdot v)$ och $(z \cdot w) \cdot v$ som vi har räknat ut. Vi finner att $z \cdot (w \cdot v) = (z \cdot w) \cdot v$, vilket skulle visas.

7. Vi räknar först ut högerledet i likheten vi ska visa. Vi har $zw = ac - bd + (ad + bc)\mathrm{i}$ och $zv = ae - bf + (af + be)\mathrm{i}$, vilket ger oss

$$zw + zv = ac + ae - bd - bf + (ad + bc + af + be)\mathrm{i}.$$

Därefter beräknar vi $w + v = c + e + (d + f)\mathrm{i}$ och får

$$z \cdot (w + v) = a(c + e) - b(d + f) + [a(d + f) + b(c + e)]\mathrm{i},$$

och efter att ha utvecklat parenteserna ser vi att $z \cdot (w + v)) = zw + zv$.

8. Denna punkt följer direkt från egenskapen $0 + a = a$ för varje heltal a: vi får $z + 0 = a + b\mathrm{i} + 0 + 0\mathrm{i} = a + 0 + (b + 0)\mathrm{i} = a + b\mathrm{i}$.

9. Vi vet att $a \cdot 1 = a$ för varje heltal a, och detta ger oss att $z \cdot 1 = (a + b\mathrm{i})(1 + 0\mathrm{i}) = a - 0 + (b + 0)\mathrm{i} = a + b\mathrm{i} = z$.

10. Om $z = a + b\mathrm{i}$ är $-z = -a - b\mathrm{i}$ ett Gaussiskt heltal eftersom $-a$ och $-b$ är heltal. Vidare gäller ju $a - a = 0$ för heltalet a, och motsvarande är ju även samt för b. Definitionen av addition medför nu att $z + (-z) = a - a + (b - b)\mathrm{i} = 0 + 0\mathrm{i} = 0$, vilket var precis vad vi skulle visa.

Övning 4.3. Vi börjar med det första påståendet. Vi beräknar

$$(a + b\mathrm{i})(a - b\mathrm{i}) = a^2 - ab\mathrm{i} + ab\mathrm{i} + b^2 = a^2 + b^2,$$

och enligt definitionen är det sista uttrycket till höger lika med $N(a + b\mathrm{i})$.

Vi sätter $z = a + b\mathrm{i}$ och $w = c + d\mathrm{i}$, tillämpar identiteten ovan på $N(z + w) = N(a + c + (b + d)\mathrm{i})$ och får

$$N(a + c + (b + d)\mathrm{i}) = (a + c + (b + d)\mathrm{i})(a + c - (b + d)\mathrm{i}).$$

Nu utvecklar vi produkten i högerledet och får

$$\begin{aligned}
&(a + c + (b + d)\mathrm{i})(a + c - (b + d)\mathrm{i}) \\
&= a^2 - iab + ac - iad + iab + b^2 + ibc + bd \\
&+ac - ibc + c^2 - icd + iad + bd + icd + d^2 \\
&= a^2 + b^2 + c^2 + d^2 + 2ac + 2bd \\
&= N(z) + N(w) + 2(ac + bd).
\end{aligned}$$

Detta visar likheten i uppgiften.

Övning 5.1.

1. Eftersom $4 + 3 = 7 = 5 \cdot 1 + 2 \equiv 2 \pmod 5$ så har vi att $4 + 3 = 2$ i ringen $\mathbb{Z}_5$.

2. Notera att $8 \cdot 7 = 56 = 9 \cdot 6 + 2 \equiv 2 \pmod 9$. Detta betyder att $8 \cdot 7 = 2$ i ringen $\mathbb{Z}_9$.

3. Till sist har vi att $3^3 = 9 \equiv -1 \pmod{10}$. Nu följer

   $$3^{100} = 3 \cdot 3^{99} = 3 \cdot (3^3)^{33} \equiv 3 \cdot (-1)^{33} = 3 \cdot (-1) = -3 \equiv 7 \pmod{10}.$$

   Alltså har vi att $3^{100} = 7$ i ringen $\mathbb{Z}_{10}$.

Övning 5.3. Per definition gäller $n \mid (a - b)$, det vill säga det finns ett heltal q sådant att $a - b = n \cdot q$. Nu följer

$$(-a) - (-b) = -(a - b) = -(n \cdot q) = n \cdot (-q),$$

vilket betyder att $n \mid ((-a) - (-b))$, och därmed $-a \equiv -b \pmod n$.

Övning 6.1. $D_t(y) = \mathrm{R}_{28}(y - t)$ är den sökta dekrypteringsfunktionen. För att visa att detta är fallet noterar vi först att

$$\begin{aligned}
D_t(\mathrm{R}_{28}(x + t)) &= \mathrm{R}_{28}(\mathrm{R}_{28}(x + t) - t) \\
&= \mathrm{R}_{28}(\mathrm{R}_{28}(x + t)) + \mathrm{R}_{28}(-t).
\end{aligned}$$

Därefter utnyttjar vi att $\mathrm{R}_n(\mathrm{R}_n(a)) = \mathrm{R}_n(a)$ och får

$$\begin{aligned}
&\mathrm{R}_{28}(\mathrm{R}_{28}(x + t)) + \mathrm{R}_{28}(-t) \\
&= \mathrm{R}_{28}(x + t) + \mathrm{R}_{28}(-t) \\
&= \mathrm{R}_{28}(x + t - t) = x,
\end{aligned}$$

vilket visar att $D(E(x)) = x$.

Vi sätter nu $t = -2$ och krypterar:

$$E(10) = \mathrm{R}_{28}\,(10-2) = \mathrm{R}_{28}\,(8) = 8$$

$$E(1) = \mathrm{R}_{28}\,(1-2) = \mathrm{R}_{28}\,(-1) = 27.$$

Vi skickar alltså det krypterade meddelandet ”hä”.

Vi dekrypterar detta och får

$$D(8) = \mathrm{R}_{28}\,(8+2) = \mathrm{R}_{28}\,(10) = 10$$

$$D(27) = \mathrm{R}_{28}\,(27+2) = \mathrm{R}_{28}\,(29) = 1,$$

vilket mycket riktig är det urspungliga meddelandet ”ja”.

Övning 6.3. Vi ska först dekryptera meddelandet 2, det vill säga, vi ska beräkna

$$D(2) = \mathrm{R}_{91}\left(2^{47}\right).$$

Vi använder metoden med upprepad kvadrering. Vi noterar att $47 = 32+8+4+2+1$, vilket medför att

$$2^{47} = 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2^2 \cdot 2.$$

Vi räknar ut att $2^2 \equiv 4 \pmod{91}$, $2^4 = 4^2 \equiv 16 \pmod{91}$, $2^8 = 16^2 = 256 \equiv 74 \pmod{91}$, $2^{16} = 74^2 = 5476 \equiv 16 \pmod{91}$ och $2^{32} = 16^2 \equiv 74 \pmod{91}$.

Vi multiplicerar ihop dessa tal och får

$$2^{47} \equiv 2 \cdot 4 \cdot 16 \cdot 74 \cdot 74 = 700928 \equiv 46 \pmod{91},$$

vilket ger oss $D(2) = 46$.

Vi krypterar nu meddelandet 3. Vi ska beräkna $\mathrm{R}_{91}\left(3^{23}\right)$, och vi utnyttjar här att

$$3^{23} = 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3.$$

Vi räknar ut att $3^2 \equiv 9 \pmod{91}$, $3^4 \equiv 81 \pmod{91}$, $3^8 \equiv 9 \pmod{91}$ och $3^{16} \equiv 81 \pmod{91}$, vilket ger oss

$$3^{23} \equiv 3 \cdot 9 \cdot 81 \cdot 81 = 177147 \equiv 61 \pmod{91}.$$

Därmed är $E(3) = 61$.

Övning 7.1. I första fallet prövar vi oss fram genom att kvadrera alla tal mellan 1 och 10 och reducera modulo 11. Eftersom exempelvis $1^1 \equiv 1 \pmod{11}$, $5^5 = 25 \equiv 3 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $4^2 = 16 \equiv 5 \pmod{11}$ och $8^2 = 64 \equiv 9 \pmod{11}$ finner vi att

$$1, \quad 3, \quad 4, \quad 5, \quad 9$$

är kvadratiska rester modulo 11.

Vi går till väga på precis samma sätt för att bestämma de kvadratiska resterna modulo 13. Då $1^2 \equiv 1 \pmod{13}$, $4^2 = 16 \equiv 3 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $3^2 \equiv 9 \pmod{13}$, $6^2 = 36 \equiv 10 \pmod{13}$ och $5^2 = 25 \equiv 12 \ (13)$ finner vi att

$$1, \quad 3, \quad 4, \quad 9, \quad 10, \quad 12$$

är kvadratiska rester modulo 13.

Övning 7.3. Vi följer ledningen och konstaterar först att 923 inte är ett primtal eftersom $923 = 13 \cdot 71$. I inledningen till kapitlet såg vi att $x^2 \equiv a \pmod{p}$ har lösningar för ett sammansatt tal p om $x^2 \equiv a \pmod{p_j}$ har lösningar för alla primtalsfaktorer p_j som ingår i p. Problemet reduceras alltså till att bestämma om 43 är en kvadratisk rest modulo 13 och modulo 71.

Vi ser att $43 \equiv 4 \pmod{13}$ och eftersom $2^2 \equiv 4 \pmod{13}$ drar vi slutsatsen att $43 \in Q_{13}$.

Vi tillämpar därefter lagen om kvadratisk reciprocitet för att undersöka huruvida 43 är en kvadratisk rest modulo 71. Notera här att $43 \equiv 3 \pmod{4}$ och att $71 \equiv 3 \pmod{4}$. Vi får först att

$$\left(\frac{43}{71}\right) = -\left(\frac{71}{43}\right)$$

och efter en reduktion modulo 43 följer att

$$\left(\frac{43}{71}\right) = -\left(\frac{28}{43}\right).$$

Vi använder nu att $28 = 4 \cdot 7$ samt att 4 är en kvadratisk rest modulo 43 eftersom $2^2 \equiv 4 \pmod{43}$. Vi får

$$-\left(\frac{28}{43}\right) = -\left(\frac{4}{43}\right)\left(\frac{7}{43}\right) = (-1) \cdot 1 \cdot \left(\frac{7}{43}\right).$$

En ny tillämpning av lagen om kvadratisk reciprocitet, även denna gång varianten med minustecken, ger oss därefter

$$-\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right),$$

och efter en reduktion modulo 7 finner vi att

$$\left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

Våra uträkningar visar därmed att $43 \in Q_{71}$.

Alltså är 43 en kvadratisk rest modulo 923.

Förslag till vidare läsning

[1] N. L. Biggs. *Discrete Mathematics.* Second Edition. Oxford University Press, 2002.

[2] G. Jones, J.M. Jones. *Elementary Number Theory.* Springer-Verlag London, 1998.

[3] A. Thorup. *Algebra.* 2. udgave. Kobenhavns Universitet, 1998.

Böckerna ovan, och många andra böcker, finns att låna på Matematikbiblioteket, Lindstedtsvägen 25 (bottenvåningen). Biblioteket är öppet för alla.