Algebra I

Dan Strängberg

8 november 2016

Innehåll

1 Grundläggande logik

Innan vi sätter igång med matematiken kan det vara bra att bilda oss en uppfattning om vad matematiken som vetenskap sysslar med. Väldigt förenklat kan man säga att matematiken byggs upp av *definitioner*, *satser* och deras *bevis*. Definitionerna används för att bestämma vad man menar med ett visst ord och ska vara utformade på sådant sätt att det aldrig kan uppstå tvetydigheter i huruvida ett objekt uppfyller definitionen eller ej. Satserna innehåller ett antal *antaganden* och ett antal *påståenden* eller *utsagor*. Det är dessa påståenden som ska bevisas genom att utgå från de antagenden som angetts.[1] För att utföra beviset använder man sig av *logik*. Vi kommer därför börja med en genomgång av de grundläggande logiska reglerna som krävs för att genomföra de vanligaste logiska resonemangen i matematiken.

Vi börjar med att titta närmare på vad vi menar med en utsaga. Grovt sett kan man säga att en utsaga är något som ger en relation mellan två eller flera objekt, de säger något om något. I språkligt sammanhang skulle man kunna säga att en utsaga är en komplett mening. Till exempel är följande utsagor:

1. $1 > 0$,
2. mina skor är svarta,
3. $2x = 10$,
4. alla fåglar kan flyga,
5. det finns en fågel som kan flyga.

Däremot är följande inte utsagor:

1. 1,
2. mina skor,
3. alla fåglar,
4. $\int_a^b \sin(x)dx$.

Dessa är bara ”namn” på olika saker.

En utsaga kan vara *sann* eller *falsk*. Till exempel är utsagan ”alla fåglar kan flyga” falsk medans utsagan ”$1 > 0$” är sann. Till skillnad från dessa två utsagor, som alltid är antingen sanna eller falska, beror sanningsvärdet för utsagan ”mina skor är svarta” på vilka skor jag har på mig för tillfället och sanningsvärdet för ”$2x = 10$” beror på vad x är. Man brukar därför skilja på *öppna* utsagor, vars sanningsvärde beror på en eller flera

[1] Ofta pratar man också om lemman, propositioner och korollarier. Ett lemma är en hjälpsats, ett mindre resultat som används för att bevisa en större sats. En proposition är ett självständigt resultat som inte är tillräckligt viktigt för att kallas sats. Ett korollarium är en sats som är en direkt eller enkel följd av en annan sats.

variabler, och *slutna* utsagor, vars sanningsvärde är bestämt en gång för alla och aldrig ändras.

Vi ska nu titta på hur man kan kombinera utsagor för att skapa nya.

Definition 1.1. Låt A och B vara två utsagor. *Konjunktionen* av A och B, som vi betecknar $A \wedge B$, är den utsaga som är sann om och endast om både A och B är sanna.

Konjunktionen fungerar alltså på ungefär samma sätt som ordet "och" gör i vanligt språk. Om till exempel A är utsagan "mina skor är svarta" och B är utsagan "$2x = 10$" så är konjunktionen $A \wedge B$ utsagan "mina skor är svarta och $2x = 10$". Om $2x \neq 10$ eller om mina skor inte är svarta är alltså utsagan $A \wedge B$ falsk. Detta leder oss också in på nästa definition.

Definition 1.2. Låt A och B vara två utsagor. *Disjunktionen* av A och B, som vi betecknar med $A \vee B$, är den utsaga som är falsk om och endast om både A och B är falska.

Denna definition är inte lika lätt att genomskåda men om man funderar lite kan man inse att disjunktion fungerar ungefär som "eller" gör i vanligt språk. Om, som tidigare, A är utsagan "mina skor är svarta" och B är utsagan "$2x = 10$" så är $A \vee B$ utsagan "mina skor är svarta eller $2x = 10$". Utsagan $A \vee B$ är alltså sann om A och B är sanna, A är sann men B är falsk eller om A är falsk och B är sann. Notera att detta inte kan översättas med det språkliga "antingen ... eller ...".

När man använder till exempel konjunktion och disjunktion för att skapa sammansatta utsagor kan det vara lätt att tappa bort sig i alla sanningsvärden. Ett smidigt sätt att hålla koll på detta är genom att göra en så kallad *sanningsvärdestabell*. Vi illustrerar detta med några exempel.

Exempel 1.3. Låt A och B vara två utsagor. Vi vill nu undersöka sanningsvärdena för utsagorna $A \wedge B$ och $A \vee B$ genom att göra sanningsvärdestabeller. Låt S beteckna "sann" och F beteckna "falsk". Vi ställer upp det på följande vis:

A	B	$A \wedge B$
S	S	S
S	F	F
F	S	F
F	F	F

A	B	$A \vee B$
S	S	S
S	F	S
F	S	S
F	F	F

Figur 1: Sanningsvärdestabeller för konjunktion och disjunktion.

Låt nu C vara en tredje utsaga. Vi kan då titta på den lite mer komplicerade utsagan $(A \wedge B) \vee C$.

A	B	$A \wedge B$	C	$(A \wedge B) \vee C$
S	S	S	S	S
S	F	F	S	S
F	S	F	S	S
F	F	F	S	S
S	S	S	F	S
S	F	F	F	F
F	S	F	F	F
F	F	F	F	F

Figur 2: Sanningsvärdestabell för utsagan $(A \wedge B) \vee C$.

När man skriver utsagor är det några uttryck som ofta dyker upp. Exempel på sådana är ”för alla”, ”för varje” och ”det existerar”. Därför har man också infört beteckningar för dessa, de så kallade *kvantifikatorerna*. Uttrycket ”för alla” eller ”för varje” skrivs $\forall$. Uttrycket ”det existerar” eller ”det finns minst en” skrivs $\exists$. Om vi låter M vara mängden av alla fåglar kan vi då skriva utsagan ”alla fåglar kan flyga” som

$$\forall x \in M\colon x \text{ kan flyga}\,.$$

Uttrycket $x \in M$ betyder att x är ett element i M, d.v.s. i det här fallet att x är en fågel, och vi läser $:$ som ”gäller att” eller ”för vilket”. Skulle man läsa ut detta i mer vardagligt språk blir det ”för varje fågel x gäller att x kan flyga”. På liknande sätt kan man skriva utsagan ”det finns en fågel som kan flyga” som

$$\exists x \in M\colon x \text{ kan flyga}\,.$$

Vi läser detta som ”det existerar en fågel som kan flyga”. Man använder även $\exists!$ för att indikera att något existerar och att det är unikt och $\nexists$ för att indikera att något inte existerar. Till exempel skulle

$$\nexists x \in M\colon x \text{ kan flyga}$$

vara utsagan att det inte finns någon fågel som kan flyga. Jämför detta med utsagorna $x = y$ och $x \neq y$.

Anmärkning 1.4. När man i matematiken säger att ”det existerar en” eller ”det finns en” så menar man alltid att det finns *minst* en. Utsagan ”det finns ett jämnt tal” betyder alltså inte att det bara finns ett jämnt tal och inga fler utan bara att det finns minst ett jämnt tal.

Något annat som också dyker upp ofta är *negationen* eller *motsatsen* av en utsaga. Om vi har en utsaga A så ska negationen alltså vara falsk precis då A är sann och falsk precis då A är sann. Vi betecknar negationen av en utsaga A med $\neg A$. Vi kan beskriva förhållander mellan en utsaga A och dess negation $\neg A$ enkelt och koncist med en sanningsvärdestabell.

A	$\neg A$
S	F
F	S

Vi kan direkt se att någon av utsagorna A eller $\neg A$ alltid är sann, m.a.o. utsagan $A \vee \neg A$ är alltid sann. Detta är ett välkänt exempel på en tautologi.

Hur verkar då negationen på kvantifikatorerna $\forall$ och $\exists$? För att undersöka detta låter vi A vara en utsaga som beror på x i någon mängd M.

Vi börjar med att betrakta utsagan $\forall x \in M\colon A$, d.v.s. för varje element x i M är utsagan A sann. Vad är då negationen $\neg(\forall x \in M\colon A)$ av detta? Negationen är ju sann precis då utsagan i sig är falsk, så vi vill veta när utsagan $\forall x \in M\colon A$ är falsk. Om $\forall x \in M\colon A$ är falsk måste det finnas minst ett $x \in M$ för vilket A är falskt. Vi kan skriva detta som $\exists x \in M\colon \neg A$. Vi har alltså att $\neg(\forall x \in M\colon A)$ är utsagan $\exists x \in M\colon \neg A$

Anmärkning 1.5. Det här kan skilja sig från hur man använder ordet "motsats" i vardagligt språk. I vardagligt språk kan man säga att motsatsen till "alla fåglar kan flyga" är "ingen fågel kan flyga" men detta är inte den logiska motsatsen som istället är "det finns en fågel som inte kan flyga". I det här exemplet är detta extra tydligt eftersom båda utsagorna "alla fåglar kan flyga" och "ingen fågel kan flyga" är falska.

Vi betraktar nu istället utsagan $\exists x \in M\colon A$. Om denna utsaga ska vara falsk får det inte finnas något x för vilket A är sant, d.v.s. för varje x måste A vara falsk. Vi kan därför skriva $\neg(\exists x \in M\colon A)$ som $\forall x \in M\colon \neg A$.

Det finns liknande samband för negationen av en konjunktion och en disjunktion. Det lämnas som inlämningsuppgift att visa att för alla utsagor A, B gäller att $\neg(A \wedge B)$ är $\neg A \vee \neg B$ och att $\neg(A \vee B)$ är $\neg A \wedge \neg B$. Dessa relationer kallas för De Morgans lagar.

Det sista vi ska titta på innan vi går vidare från logiken är *implikationer* och *ekvivalenser*. Givet två utsagor A och B skapar vi utsagan $A \Rightarrow B$ som vi tolkar som "om A är sann så är B sann". Vi läser $A \Rightarrow B$ som "A implicerar B" eller "A medför B". Det är tydligt från tolkningen att om A är sann måste också B vara sann för att $A \Rightarrow B$ ska vara sann och att om A är sann men B är falsk så är även $A \Rightarrow B$ falsk. Däremot är det inte helt tydligt vad som gäller om A är falsk. För att råda bot på detta säger vi att en falsk utsaga kan implicera vad som helst, d.v.s. om A är falsk så är $A \Rightarrow B$ alltid sann oavsett B. Vi sammanfattar detta i en sanningsvärdestabell.

A	B	$A \Rightarrow B$
S	S	S
S	F	F
F	S	S
F	F	S

Denna sanningsvärdestabell gör det också tydligt vad som menas med $\neg(A \Rightarrow B)$, det måste nämligen vara utsagan $A \wedge \neg B$ eftersom endast då A är sann och B är falsk är $A \Rightarrow B$ falsk. Vi kan också tolka $\neg(A \Rightarrow B)$ som "visserligen A men trots det gäller inte B". En vanlig och ibland väldigt användbar omskrivning av implikationen $A \Rightarrow B$

är utsagan $\neg B \Rightarrow \neg A$. Denna omskrivning kallas *kontrapositionen* av $A \Rightarrow B$ och har alltså samma sanningsvärden. Kolla detta med en sanningsvärdestabell!

Anmärkning 1.6. Det förekommer ett stort missbruk av tecknet " $\Rightarrow$ ". Till exempel används det ibland istället för "=" och vice versa. Tänk på att implikationer bara kan användas mellan kompletta utsagor.

Givet två utsagor A och B skapar vi nu utsagan $A \Leftrightarrow B$ som betyder $(A \Rightarrow B) \wedge (B \Rightarrow A)$, d.v.s. de båda utsagorna implicerar varandra. Vi får därför följande saningsvärdestabell.

A	B	$A \Leftrightarrow B$
S	S	S
S	F	F
F	S	F
F	F	S

Om utsagan $A \Leftrightarrow B$ alltid är sann säger vi att utsagorna A och B är ekvivalenta. Vi har redan sett ett antal exempel på ekvivalenta utsagor, till exempel följande.

Exempel 1.7. Låt A och B vara två utsagor och låt M vara en mängd. Då är följande ekvivalenser sanna:

1. $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$,
2. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$,
3. $\neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$

Implikationer och ekvivalenser är väldigt viktiga vid ekvationslösning. En ekvation är i regel en öppen utsaga. Att lösa ekvationen betyder att man hittar samtliga värden på ingående variabler som gör att utsagan är sann. Detta gör man genom att skriva om den ursprungliga utsagan med hjälp av ekvivalenser och implikationer.

Om man kan lösa ekvationen med hjälp av enbart ekvivalenser så kan man vara säker på att man får rätt svar men om man vid något tillfälle måste använda en implikation är det inte längre säkert att de resultat man får faktiskt löser ekvationen. Ett typexempel på när sådana situationer upptsår är när man löser rotekvationer som till exempel

$$x = \sqrt{x+2}\,.$$

Vanligt är att man direkt kvadrerar båda leden för att bli av med rottecknet, men detta leder till en utsaga som inte är ekvivalent med den första. Det är bara en implikation. Anledningen till detta är att $a = b \Rightarrow a^2 = b^2$ men $a^2 = b^2 \not\Rightarrow a = b$. Utsagorna $a = b$ och $a^2 = b^2$ är alltså inte ekvivalenta. Ekvationen $a^2 = b^2$ har ju förutom lösningen $a = b$ också lösningen $a = -b$. Alltså är utsagan $a^2 = b^2$ ekvivalent med utsagan $(a = b) \vee (a = -b)$.

Exempel 1.8.

$$\begin{aligned} & x = \sqrt{x+2} \\ \Rightarrow\ & x^2 = x+2 \\ \Leftrightarrow\ & x^2 - x - 2 = 0 \\ \Leftrightarrow\ & x = -1 \ \vee\ x = 2 \end{aligned}$$

Notera att vi mellan första och andra utsagan har en implikation men inte en ekvivalens. Därför kan vi inte direkt dra slutsatsen åt andra hållet, d.v.s. om $x = -1 \ \vee \ x = 2$ så $x = \sqrt{x+2}$. Det kan hända att det är sant men det kan också hända att en eller båda dessa "lösningar" är falska. Det enda vi vet är att om en lösning finns måste den ha någon av formerna vi har hittat. Vi får helt enkelt undersöka om något av dessa förslag faktiskt är en lösning.

Om vi sätter in $x = -1$ får vi $-1 = \sqrt{1}$ vilket är falskt. Därför är $x = -1$ ingen lösning. Det är en så kallad *falsk rot*. Sätter vi in $x = 2$ får vi $2 = \sqrt{2+2} = \sqrt{4}$ vilket stämmer. Svaret blir alltså att $x = 2$ är den enda lösningen.

Exempel 1.9. Vi vill nu lösa ekvationen $(x-2)^2 = 8(x-2)$. Eftersom faktorn $x-2$ förekommer i båda leden är det frestande att helt enkelt dividera båda leden med $x-2$ men detta får man inte göra. Det kan ju hända att $x = 2$ och isåfall har vi dividerat med 0. Därför undersöker vi fallet $x = 2$ för sig och ser då att $x = 2$ är en lösning till ekvationen. Om $x \neq 2$ får vi utföra divisionen och får då

$$x - 2 = 8 \ \Leftrightarrow \ x = 10\,.$$

Vi har nu täckt in alla möjliga fall (eftersom antingen $x = 2$ eller $x \neq 2$) och kan därför dra slutsatsen att ekvationen har rötterna $x = 2$ och $x = 10$.

2 Grundläggande mängdlära

Vi har redan till viss del använt oss av vad vi kallar *mängder* men vi ska nu ta oss en närmare titt på vad det är och hur man kan arbeta med dem. *Mängdlära* är det område av matematik och logik som studerar mängder och används flitigt inom matematiken som språk för att formulera definitioner, satser, m.m. Man kan säga att mängdläran utgör ett fundament på vilket man kan bygga upp matematiken. Vi kommer inte oroa oss så mycket över hur man definierar mängder utan kommer fokusera på hur dessa kan användas i matematiska uttryck.

En *mängd* ser vi som en samling av objekt som kallas för mängdens *element*. Vi använder skrivsättet $x \in M$ för att indikera att x är ett element i mängden M. En mängd bestäms helt och hållet av dess element, d.v.s. om två mängder M och N har precis samma element så betraktar vi dem som samma mängd och skriver då $M = N$. Därför är det också vanligt att man beskriver en mängd genom att beskriva dess element. Man använder då klammerparenteser, som till exempel

$$A = \{1, 3, 5, 7\}\,.$$

Här säger vi alltså att A är mängden vars element är $1, 3, 5, 7$. Om antalet element är för många för att räkna upp får man istället använda sig av andra knep, till exempel kan man utnyttja en viss egenskap som alla elementen har.

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$
$$[0, 1] = \{x \in \mathbb{R} \colon 0 \leq x \leq 1\}$$

Mängden $[0, 1]$ är alltså mängden av alla reella tal som uppfyller den givna olikheten. Det är också vanligt att man använder $\mid$ istället för $:$ när man anger en mängd på detta sätt. Mer allmänt, om man har en utsaga A vars sanningsvärde beror på en variabel från en mängd B kan vi skapa mängden

$$S = \{x \in B \colon A\}$$

som alltså är mängden av alla $x \in B$ som uppfyller utsagan A.

Mängden $\mathbb{N}$ är en av *talmängderna*. Dessa mängder är så vanliga och viktiga att de har särskilda beteckningar:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\} = \text{mängden av alla } \textit{naturliga tal},$$
$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \text{mängden av alla } \textit{heltal},$$
$$\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0\right\} = \text{mängden av alla } \textit{rationella tal},$$
$$\mathbb{R} = \text{mängden av alla } \textit{reella tal},$$
$$\mathbb{C} = \text{mängden av alla } \textit{komplexa tal}.$$

Den andra mängden i exemplet ovan, $[0, 1]$, är ett så kallat *intervall*. Intervallen är viktiga mängder av reella tal som också dyker upp ofta i olika sammanhang och därför finns också en allmänt vedertagen notation för dessa. Låt $a, b \in \mathbb{R}$. Vi definierar då följande:

$$[a, b] = \{x \in \mathbb{R} \colon a \leq x \leq b\},$$
$$(a, b) = \{x \in \mathbb{R} \colon a < x < b\}.$$

Intervall på formen $[a, b]$ kallas *slutna* och intervall på formen (a, b) kallas öppna. Vi kan även tillåta intervall som är slutna i ena änden och öppna i andra, till exempel

$$[a, b) = \{x \in \mathbb{R} \colon a \leq x < b\}.$$

Vi tillåter också oändliga intervall. Vi skriver då till exempel

$$[a, \infty) = \{x \in \mathbb{R} \colon a \leq x\},$$
$$(-\infty, b) = \{x \in \mathbb{R} \colon x < b\},$$
$$(-\infty, \infty) = \mathbb{R}.$$

Anmärkning 2.1. Eftersom $-\infty, \infty$ ej är reella tal använder vi alltid beteckningen för ett öppet intervall åt det håll intervallet är oändligt. Däremot kallar vi ändå $[a, \infty)$ slutet och (a, ∞) öppet. Därför är också $(-\infty, \infty) = \mathbb{R}$ både öppet och slutet.

Intervallen har även egenskapen att varje element i ett intervall också är ett element i $\mathbb{R}$. De är så att säga inneslutna i $\mathbb{R}$. Vi ger denna egenskap en definition.

Definition 2.2. Låt A, B vara två mängder. Om $x \in B \Rightarrow x \in A$ så kallas B för en *delmängd* av A. Vi betecknar detta med $B \subseteq A$. Om det existerar ett $x \in A$ sådant att $x \notin B$ så kallas B en *äkta delmängd* och vi betecknar detta med $B \subset A$.

Anmärkning 2.3. Beteckningen $B \subset A$ används ibland också för vanlig delmängd. Här finns tyvärr ingen konsensus inom matematiken, man får helt enkelt vara uppmärksam på vad författaren egentligen menar när man ser $\subset$.

Vi ska nu titta på mängdoperationer, operationer på mängder, som givet två mängder A, B låter oss skapa nya mängder.

Definition 2.4.

1. *Unionen* eller *föreningsmängden* av A och B betecknas $A \cup B$ och består av alla element som tillhör A eller B, d.v.s.
$$A \cup B = \{x \colon x \in A \vee (x \in B)\}.$$
2. *Snittet* eller *skärningsmängden* av A och B betecknas $A \cap B$ och består av alla element som tillhör A och B, d.v.s.
$$A \cap B = \{x \colon x \in A \wedge x \in B\}.$$
3. *Mängddifferensen* av A och B betecknas $A \setminus B$ och består av alla element i A som inte är element i B, d.v.s.
$$A \setminus B = \{x \in A \colon x \notin B\}.$$

Exempel 2.5. Låt $A = [2, 4]$ och $B = (1, 3)$. Då har vi

$$A \cup B = (1, 4],$$
$$A \cap B = [2, 3),$$
$$A \setminus B = [3, 4].$$

Det kan vara väldigt illustrativt att rita upp hur detta ser ut på tallinjen.

Övning 2.6. Rita upp mängderna från föregående exempel på tallinjen.

En väldigt speciell mängd är den så kallade *tomma mängden* som skrivs $\varnothing$. Den karaktäriseras av att den inte har några element alls. Således är den också en delmängd av varje annan mängd. Tomma mängden ger oss också ett smidigt sätt att med hjälp av mängdoperationer avgöra om två mängder inte har några gemensamma element.

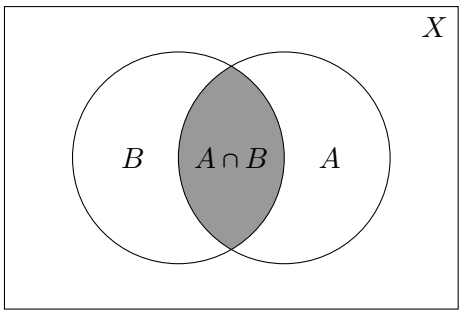
Definition 2.7. Låt A och B vara två mängder. Om $A \cap B = \varnothing$ säger vi att A och B är *disjunkta*: de har inga gemensamma element.

Ofta är mängderna man arbetar med delmängder av en större mängd X, ett så kallat *universum*. Om vi till exempel arbetar med intervall är vårat universum $\mathbb{R}$. Det kan då vara smidigt att prata om alla element i universumet som inte är element i en given delmängd.

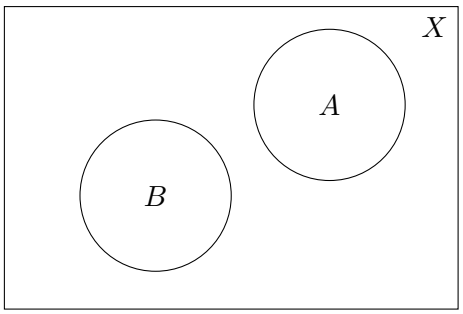
Definition 2.8. Låt $A \subseteq X$. *Komplementet av* A i X är mängden $A^c = X \setminus A$.

Ofta utelämnar man universumet X om det är underförstått. Om vi till exempel arbetar med intervall är det underförstått att universumet är $\mathbb{R}$ och att vi därför har, till exempel, $[0, \pi]^c = (-\infty, 0) \cup (\pi, \infty)$.

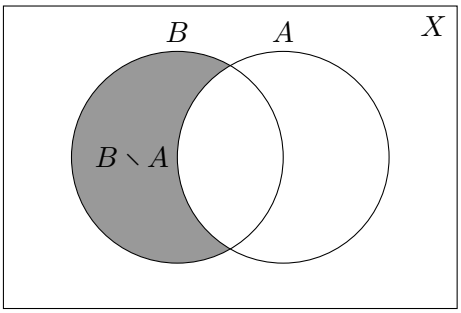
Innan vi lämnar mängdläran ska vi titta på hur man på ett enkelt sätt kan åskådliggöra mängdrelationer med så kallade Venndiagram. När man ritar ett Venndiagram börjar man med att rita en yttre kontur som symboliserar ens universum. Inom dessa konturer ritar man sedan in geometriska figurer, oftast cirklar, som symboliserar mängder i detta unviersum. Här följer några exempel.



(a) Venndiagram för $A \cap B$.



(b) Venndiagram för $A \cap B = \varnothing$.



(c) Venndiagram för $B \setminus A$.

3 Heltal

Vi ska nu ta en närmare titt på mängden av alla heltal, $\mathbb{Z}$, och vad heltalen har för egenskaper. Vi börjar med att notera att heltal kan adderas och multipliceras med varandra.

När det kommer till additionen gäller att $a + b = b + a$ för alla heltal a och b och därför kallar vi additionen *kommutativ*. Det finns ett speciellt heltal 0 som uppfyller att $a + 0 = 0 + a = a$ för varje heltal a. Vi kallar 0 för ett *neutralt element med avseende på additionen*. För varje heltal a finns dessutom ett annat heltal b som tillsammans uppfyller att $a + b = b + a = 0$, nämligen talet $b = -a$. Ibland säger man att $b = -a$ är *inversen av a med avseende på additionen*.

Multiplikationen är precis som additionen kommutativ, d.v.s. $a \cdot b = b \cdot a$ för alla heltal a och b. Det neutrala elementet med avseende på multiplikationen är talet 1, eftersom det uppfyller att $a \cdot 1 = 1 \cdot a = a$ för alla heltal a. Däremot är inversen med avseende på multiplikationen av ett heltal i regel inte ett heltal. Till exempel är $\frac{1}{2}$ den multiplikativa inversen av 2 men $\frac{1}{2}$ är inte ett heltal. Faktum är att endast 1 och -1 har inverser med avseende på multiplikationen, nämligen de själva:

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

För alla andra heltal a gäller alltid att $a \cdot b \neq 1$ oavsett vilket heltal b vi väljer. Detta gör också att det är intressant att undersöka vilka heltal som kan skrivas som en multiplikation av heltal som varken är 1 eller -1.[2]

3.1 Delbarhetsbegreppet

Delbarhetsbegreppet formaliserar idén att ett tal a kan skrivas som en produkt av heltal $a = b \cdot c$. Vi börjar i vanlig stil med att göra en definition som formaliserar vår intuition.

Definition 3.1. Låt $a, b \in \mathbb{Z}$. Vi säger att a är *delbart* med b om det finns ett heltal c sådant att $a = b \cdot c$. Vi säger då också att b *delar* a och att b är en *delare* till a. Vi betecknar detta med $b \mid a$. På motsvarande sätt låter vi $b \nmid a$ beteckna att b inte delar a, d.v.s. vi kan inte skriva a som en produkt av b med något annat heltal.

Exempel 3.2. Som exempel har vi att $7 \mid 56$ eftersom $56 = 7 \cdot 8$. Däremot har vi $3 \nmid 56$.

Exempel 3.3. Som vi redan har nämnt gäller alltid att $a = 1 \cdot a$ och $a = (-1) \cdot (-a)$ så vi kan dra slutsatsen att för alla heltal a gäller att $\pm 1 \mid a$ och $\pm a \mid a$. Dessa delare kallas för *triviala delare*. Delare som inte är triviala kallas *äkta*. Vi kommer titta närmare på detta senare.

Det är nu dags för vår första sats.

Sats 3.4. *Låt a, b, c vara heltal sådana att $a \mid b$ och $a \mid c$. Då gäller $a \mid (xb + yc)$ för alla heltal x, y.*

[2] Dessa kan ju alltid multipliceras med och vi kan få tillbaks talet vi hade från början, till exempel kan a skrivas som $(-1) \cdot (-a)$. Således är det bara multiplikation med andra tal som är intressant att undersöka.

När vi genomför beviset får vi utgå från de antaganden som finns i satsen, d.v.s. att $a \mid b$ och att $a \mid c$. Utifrån dessa antaganden ska vi sedan m.h.a. logik och vad vi vet sedan tidigare härleda att slutsatsen $a \mid (xb + yc)$ då också måste vara sann. Notera att satsen är formulerad som en implikation, $a \mid b \wedge a \mid c \;\Rightarrow\; \forall x, y \in \mathbb{Z}\colon a \mid (xb + yc)$.

Bevis. Eftersom vi enligt antagandet har att $a \mid b$ och $a \mid c$ finns det heltal d, e sådana att $b = ad$ och $c = ae$. Idén är nu att med hjälp av detta försöka skriva om $xb + yc$ så att vi kan bryta ut en faktor a. Vi kan göra detta på följande vis:

$$\begin{aligned} xb + yc &= xad + yae \\ &= a(xd + ye) \end{aligned}$$

Talet $f = xd + ye$ är också ett heltal eftersom x, y, d, e alla är heltal. Därför ser vi nu att vi kan skriva $xb + yc = af$ vilket är precis vad det betyder att $a \mid (xb + yc)$. Därför har vi nu bevisat det vi ville göra. □

Anmärkning 3.5. Symbolen □ betyder att beviset är färdigt. Andra vanliga symboler är ■, Q.E.D. och V.S.B. Q.E.D. är en förkortning av det latinska uttrycket "quod erat demonstrandum" vilket betyder "vilket skulle bevisas", som i sin tur har förkortningen V.S.B.

Vi går igenom ett exempel för att bekanta oss lite mer med delbarhetsbegreppet och hur bevis fungerar.

Exempel 3.6. Visa att om $4 \mid a - 1$ så gäller att $8 \mid a^2 + 7$.

Lösning. Enligt antagandet har vi att $a - 1 = 4b$ för något $b \in \mathbb{Z}$. Alltså har vi att $a = 4b + 1$. Vi tittar då på $a^2 + 7$. Eftersom $a = 4b + 1$ har vi att $a^2 = (4b + 1)^2 = 16b^2 + 8b + 1$. Det följer då att

$$\begin{aligned} a^2 + 7 &= 16b^2 + 8b + 8 \\ &= 8(2b^2 + b + 1) \end{aligned}$$

Vi ser alltså att $a^2 + 7 = 8c$ där $c = 2b^2 + b + 1$ vilket betyder att $8 \mid a^2 + 7$. □

Vad händer då om $a \mid b$ men $a \nmid c$? Detta beskrivs i följande sats.

Sats 3.7. *Låt $a, b, c \in \mathbb{Z}$ sådana att $a \mid b$ och $a \nmid c$. Då gäller att $a \nmid (b + c)$.*

Beviset för denna sats är ett så kallat *motsägelsebevis*. Ett motsägelsebevis går till så att man utöver de grundantaganden som finns i satsen även antar motsatsen av det man vill bevisa och sedan visar att detta extra antagande leder till motsägelser. Det följer då att vad satsen säger måste stämma.

Bevis. Vi vet att $b = ad$ för något $d \in \mathbb{Z}$ och att $a \nmid c$, d.v.s. vi kan inte skriva $c = ae$ för något heltal e. Vi antar nu motsatsen av $a \nmid (b + c)$, d.v.s. att $a \mid (b + c)$. Vi kan då även skriva $b + c = af$ för något $f \in \mathbb{Z}$. Eftersom vi dessutom har att $b = ad$ kan vi då skriva $b + c = ad + c = af \;\Leftrightarrow\; c = af - ad = a(f - d)$. Men vi har nu skrivit $c = ae$ med heltalet $e = f - d$ vilket motsäger att $a \nmid c$. Antagandet att $a \mid (b + c)$ har alltså ledit oss till en motsägelse och därför måste det gälla att $a \nmid (b + c)$. □

Vi kommer använda oss av motsägelsebevis emellanåt och kommer senare även att titta närmare på motsägelsebevis i allmänhet.

3.2 Divisionsalgoritmen och Euklides algoritm

Vi har nu sett några exempel på vad som händer om $a \mid b$ men finns det något man kan säga om $a \nmid b$? För enkelhetens skull begränsar vi oss, tills vidare, till heltal $b \geq 0$ och $a > 0$. Det visar sig att man alltid kan skriva $b = qa + r$ där $0 \leq r < a$. Vi kallar då q för *kvot* och r för *rest*. Detta bygger på *divisionsalgoritmen* som går ut på att man från b subtraherar så många multipler av a man kan utan att resultatet blir negativt. Det minsta tal man då får är resten och antalet multipler av a man har subtraherat är kvoten. Vi illustrerar detta i ett exempel.

Exempel 3.8. Vi vill dividera 971 med 46. Ett typiskt tillvägagångssätt med långdivision börjar med att man multiplicerar divisorn i divisionen med den högsta tiopotens man kan utan att det blir större än dividenden. Man drar sedan bort så många multipler man kan. I det här fallet kan vi dra bort 2 stycken $10 \cdot 46$. Kvar återstår 51.

$$\begin{array}{r} 2 \\ \hline 971 \mid 46 \\ -92 \\ \hline 51 \end{array}$$

Figur 4: Första steget i divisionsalgoritmen.

Vi upprepar sedan proceduren med dividenden 51, kvar blir 5.

$$\begin{array}{r} 21 \\ \hline 971 \mid 46 \\ -92 \\ \hline 51 \\ -46 \\ \hline 5 \end{array}$$

Figur 5: Divisionen är färdig.

Eftersom 5 är mindre än 46 kan vi inte fortsätta. Vi ser att kvoten är 21 och att resten är 5. Vi kan alltså skriva $971 = 21 \cdot 46 + 5$.

Givet två heltal a, b för vilka $a \nmid b$ och $b \nmid a$ kan det finnas tal c som uppfyller $c \mid a$ och $c \mid b$. Ett sådant tal kallas för en *gemensam delare* till a och b. Talen 1 och -1 är gemensamma delare till alla tal $a, b \in \mathbb{Z}$. Det största sådana talet kallas för den *största gemensamma delaren* av a och b och betecknas med $\mathrm{SGD}(a, b)$. Om $\mathrm{SGD}(a, b) = 1$ säger man att talen är *relativt prima*.

Exempel 3.9. Talet 20 har delarna $2, 4, 5, 10, 20$ och talet 36 har delarna $2, 3, 4, 6, 9, 12, 18, 36$. Vi ser därför att $\text{SGD}(36, 20) = 4$. Vi har också att $\text{SGD}(20, 9) = 1$ så talen 20 och 9 är relativt prima.

I föregående exempel bestämde vi $\text{SGD}(36, 20)$ genom att helt enkelt hitta alla talens delare. Denna metod för att hitta största gemensamma delare är dock väldigt opraktisk för stora tal som kan ha väldigt många delare. Som tur är finns det en metod som bygger på divisionsalgoritmen och som kan användas för att bestämma $\text{SGD}(a, b)$ för vilka heltal a, b som helst utan att faktiskt behöva undersöka deras delare. Denna metod kallas för *Euklides algoritm*. Vi beskriver den först abstrakt och ger sedan ett exempel.

Låt $a > b$ vara två heltal. Vi kan då skriva $a = q_1 b + r_1$ där $r_1 < b$. Vi vet nu från sats 3.7 att en gemensam delare till a och b därför också måste dela r_1. Dessutom, om ett tal delar både r_1 och b så måste det även dela a enligt sats 3.4. Det följer därför att $\text{SGD}(a, b) = \text{SGD}(b, r_1)$. Vi kan nu utnyttja samma trick igen och skriver $b = q_2 r_1 + r_2$ där $r_2 < r_1$. Om vi fortsätter använda samma resonemang kommer vi fram till formeln $r_{k-1} = q_{k+1} r_k + r_{k+1}$. Eftersom vi hela tiden har $r_{k+1} < r_k < r_{k-1} < \cdots < b$ måste denna procedur någon gång ta slut. Vi når en punkt då $r_{n+1} = 0$, d.v.s. vi kommer till en division som går jämnt ut och har då $r_{n-1} = q_{n+1} r_n$ och därmed också $\text{SGD}(r_{n-1}, r_n) = r_n$. Vi kan nu backa hela vägen tillbaks till $\text{SGD}(a, b)$ genom att använda oss av att $r_n = \text{SGD}(r_{n-1}, r_n) = \text{SGD}(r_{n-2}, r_{n-1}) = \cdots = \text{SGD}(r_2, r_1) = \text{SGD}(r_1, b) = \text{SGD}(a, b)$. Vi har således bestämt $\text{SGD}(a, b)$.

Exempel 3.10. Vi vill bestämma $\text{SGD}(4864, 752)$ Vi börjar därför med att skriva $4864 = q_1 \cdot 752 + r_1$ genom att använda oss av divisionsalgoritmen. Vi finner att $4864 = 6 \cdot 752 + 358$. Vi fortsätter nu med att skriva $752 = q_2 \cdot 358 + r_2$. Vi får följande uppställning:

$$
\begin{aligned}
4864 &= 6 \cdot 752 + 352 \\
752 &= 2 \cdot 352 + 48 \\
352 &= 7 \cdot 48 + 16 \\
48 &= 3 \cdot 16
\end{aligned}
$$

Här gick divisionen jämnt ut. Den sista nollsklida resten är 16 vilket då betyder att $\text{SGD}(4864, 752) = 16$. Vi kan nu använda detta för att förenkla kvoten $\frac{752}{4864}$. Genom att använda uppställngen av Euklides algoritm baklänges kan vi bryta ut 16 ur både 752

och 4864. Det ser då ut på följande vis:

$$\begin{aligned} 48 &= 3 \cdot 16 \\ 352 &= 7 \cdot 48 + 16 \\ &= 7 \cdot 3 \cdot 16 + 16 \\ &= 22 \cdot 16 \\ 752 &= 2 \cdot 352 + 48 \\ &= 2 \cdot 22 \cdot 16 + 3 \cdot 16 \\ &= 47 \cdot 16 \\ 4864 &= 6 \cdot 752 + 352 \\ &= 6 \cdot 47 \cdot 16 + 22 \cdot 16 \\ &= 304 \cdot 16 \end{aligned}$$

Vi kan därför skriva

$$\frac{752}{4864} = \frac{47 \cdot 16}{304 \cdot 16} = \frac{47}{304}$$

och eftersom vi nu har brytit ut den största gemensamma delaren vet vi också att bråket inte kan förenklas längre än så här.

3.3 Primtal

Vi har redan nämnt att ± 1 är delare till varje heltal a. Även $\pm a$ är delare till a för varje heltal a. Dessa delare kallas därför *triviala delare*. Alla andra delare kallas *äkta delare*. Vi har sett ett par exempel på äkta delare, till exempel såg vi i förra avsnittet att 16 är en äkta delare till både 4864 och 752. Det finns även heltal som saknar äkta delare. Ett exempel är talet 3. Sådana tal har ett speciellt namn.

Definition 3.11. Heltal $a \geq 2$ som saknar äkta delare kallas *primtal*.

Några av de första primtalen är $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$. Vi ser att vissa primtal dyker upp i par i meningen att både p och $p + 2$ är primtal. Till exempel ser vi detta med $5, 7$, $11, 13$ och $29, 31$. Sådana par av primtal kallas *primtalstvillingar*. Det är fortfarande en öppen fråga huruvida det finns oändligt många primtalstvillingar eller ej.

Vårat mål detta avsnitt kommer vara att bevisa *aritmetikens fundamentalsats* som säger att varje heltal $a \geq 2$ kan skrivas som en produkt av primtal och att denna produkt är unik om man bortser från faktorernas ordning. För att göra detta kommer vi först att bevisa ett antal *lemman*. Ett lemma är en mindre sats vars som främst används för att bevisa en större sats. Vi börjar med ett lemma vars bevis använder sig av Euklides algoritm.

Lemma 3.12. *För alla heltal a, b finns heltal x, y sådana att* $\mathrm{SGD}(a, b) = xa + yb$.

Bevis. Vi börjar med att använda Euklides algoritm för att hitta $\mathrm{SGD}(a,b)$. För att göra det mer överskådligt antar vi att r_3 är den sista nollskilda resten så att $\mathrm{SGD}(a,b) = r_3$. Vi får då följande uppställning:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 \end{aligned}$$

Genom att sedan gå igenom denna uppställning nerifrån och upp kan då skriva

$$\begin{aligned} r_3 &= r_1 - q_3 r_2 \\ &= r_1 - q_3(b - q_2 r_1) \\ &= a - q_1 b - q_3 b + q_3 q_2 (a - q_1 b) \\ &= (1 + q_3 q_2)a + (-q_1 - q_3 - q_3 q_2 q_1)b \\ &= xa + yb \end{aligned}$$

där $x = 1 + q_3 q_2$ och $y = -q_1 - q_3 - q_3 q_2 q_1$. På samma sätt kan man luckra upp sambanden om Euklides algoritm tar slut vid något annat r_n. □

Exempel 3.13. Vi vet sedan tidigare att $\mathrm{SGD}(4864, 752) = 16$ och att vi med Euklides algoritm får uppställningen

$$\begin{aligned} 4864 &= 6 \cdot 752 + 352 \\ 752 &= 2 \cdot 352 + 48 \\ 352 &= 7 \cdot 48 + 16 \end{aligned}$$

Vi kan då skriva

$$\begin{aligned} 16 &= 352 - 7 \cdot 48 \\ &= 352 - 7(752 - 2 \cdot 352) \\ &= 15 \cdot 352 - 7 \cdot 752 \\ &= 15(4864 - 6 \cdot 752) - 7 \cdot 752 \\ &= 15 \cdot 4864 - 97 \cdot 752 \end{aligned}$$

Lemma 3.14. *Låt a, b vara heltal och låt p vara ett primtal som delar ab. Då gäller att $p \mid a$ eller att $p \mid b$.*

Bevis. Vi vet att $p \mid a$ eller $p \nmid a$. Om $p \mid a$ är vi klara. Antag därför att $p \nmid a$. Vi vill visa att det då måste gälla att $p \mid b$. Eftersom p är ett primtal måste vi ha att $\mathrm{SGD}(p, a) = 1$. Enligt föregående lemma finns det då heltal x, y som uppfyller att $1 = xp + ya$. Multiplicerar vi med b får vi då $b = xpb + yab$. Eftersom $p \mid xpb$ och $p \mid ab$ får vi då enligt sats 3.4 att $p \mid (xpb + yab)$. Men $xpb + yab = b$ så vi har att $p \mid b$. □

Vi kan omedelbart generalisera detta lemma till större produkter av heltal.

Lemma 3.15. *Låt $a_1, a_2, \ldots, a_n$ vara heltal och låt p vara ett primtal som delar produkten $a_1 a_2 \ldots a_n$. Då finns ett k sådant att $1 \leq k \leq n$ och $p \mid a_k$.*

Bevis. Genom att sätta $a = a_1$ och $b = a_2 a_3 \ldots a_n$ säger vårat föregående lemma oss att $p \mid a_1$ eller $p \mid a_2 a_3 \ldots a_n$. Om $p \mid a_1$ är vi klara. Om $p \nmid a_1$ vet vi därför att $p \mid a_2 a_3 \ldots a_n$. Vi kan nu använda föregående lemma igen för att se att $p \mid a_2$ eller $p \mid a_3 a_4 \ldots a_n$. Genom att fortsätta på detta vis hittar vi förr eller senare ett tal a_k som delas av p: i värsta fall får vi hålla på tills vi ser att $p \mid a_{n-1}$ eller $p \mid a_n$ men då är vi också klara. □

Det här lemmat säger oss att om ett primtal delar en produkt av heltal så måste det också dela något av heltalen i sig.

Vi behöver nu ett sista lemma innan vi är redo att ge oss på beviset för aritmetikens fundamentalsats.

Lemma 3.16. *Om $a \geq 2$ inte är ett primtal så är den minsta positiva äkta delaren till a ett primtal.*

Bevis. Om a inte är ett primtal måste det ha äkta delare och därför också en minsta äkta delare. Kalla denna minsta äkta delare för b. Idén är nu att utföra ännu ett motsägelsebevis. Antag därför att b inte är ett primtal. Isåfall måste b också ha en äkta delare c. Vi kan då skriva $b = cd$ och $a = be = cde$. Men då ser vi ju att $c \mid a$ och eftersom c är en äkta delare till b måste vi dessutom ha att $1 < c < b$. c är alltså en äkta delare till a som är mindre än b, men b var den minsta äkta delaren. Har har vi motsägelsen vi behövde och som visar att b måste vara ett primtal. □

Vi är nu redo att formulera och bevisa aritmetikens fundamentalsats, som i någon mening är höjdpunkten på första delen och en väldigt viktig sats i allmänhet.

Sats 3.17 (Aritmetikens fundamentalsats)**.** *Varje heltal $a \geq 2$ kan skrivas som en produkt av primtal på ett sätt som är unikt om man bortser från faktorernas ordning.*

Bevis. Låt $a \geq 2$ vara ett heltal. Vi har nu två saker att visa: att a kan skrivas som en produkt av primtal och att detta bara kan göras på ett sätt bortsett från ordningen på faktorerna. Vi börjar med att visa att det kan skrivas som en produkt av primtal på något sätt.

Om a är ett primtal är vi färdiga. Om a inte är ett primtal vet vi från lemma 3.16 att det finns ett primtal p_1 sådant att $a = p_1 a_1$ där $a_1 < a$. Om nu a_1 är ett primtal är vi färdiga. Annars använder vi lemma 3.16 en gång till på a_1 och får då ett primtal p_2 som uppfyller $a_1 = p_2 a_2$ där $a_2 <_1$ och därför får vi också $a = p_1 p_2 a_2$. Om nu a_2 inte heller är ett primtal fortsätter vi. Vi får då en samling primtal $p_1, p_2, \ldots, p_n$ som uppfyller att $a = p_1 p_2 \ldots p_n a_n$ där $a_n < a_{n-1} < \cdots < a_2 < a_1 < a$. Eftersom talen a_k hela tiden minskar måste denna process ta slut vid något tillfälle och då har vi skrivit a som en produkt av primtal. Detta bevisar första halvan av satsen.

Antag nu att vi kan skriva a som en produkt av primtal på två olika sätt, $a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$. Vi kan också anta att $m \leq n$ eftersom det alltid måste gälla att

$m \leq n$ eller $n \leq m$ och om $n \leq m$ byter vi bara plats på bokstäverna så får vi vad vi vill ha. Eftersom $p_1 \mid a$ har vi också att $p_1 \mid q_k$ för något k. Eftersom vi inte bryr oss om ordningen kan vi lika gärna anta att $k = 1$ så att $p_1 \mid q_1$. Men p_1 och q_1 är primtal så de måste vara samma tal, $p_1 = q_1$. Vi gör sedan på samma sätt med $p_2 p_2 \dots p_m = q_2 q_3 \dots q_n$. Vi kan fortsätta tills vi får slut på p. Om $m < n$ får vi då $1 = q_{m+1} \dots q_n$ vilket är en motsägelse. Vi måste därför ha $m = n$, vilket avslutar beviset. □

3.4 Diofantiska ekvationer

Vi ska nu titta närmare på en typ av ekvationer som kallas *Diofantiska ekvationer*. En Diofantisk ekvation är en ekvation på formen

$$ax + by = c$$

där $a, b, c \in \mathbb{Z}$. När vi löser en Diofantisk ekvation letar vi efter $x, y \in \mathbb{Z}$ som uppfyller ekvationen. Våra tidigare resultat om delbarhet ger oss genast följande sats.

Sats 3.18. *Om* $\mathrm{SGD}(a, b) \nmid c$ *har den Diofantiska ekvationen* $ax + by = c$ *inga lösningar.*

Bevis. Eftersom $\mathrm{SGD}(a, b)$ delar både a och b vet vi från sats 3.4 att $\mathrm{SGD}(a, b) \mid ax + by$ för alla heltal x, y. Så om ekvationen $ax + by = c$ har en lösning x, y måste även $\mathrm{SGD}(a, b)$ dela c. Men detta är precis kontrapositionen av det vi ville visa, så vi är klara. □

Vi har nu visat att om den Diofantiska ekvationen $ax + by = c$ har en lösning så måste $\mathrm{SGD}(a, b)$ dela c. Det är nu naturligt att ställa sig följande fråga: Om $\mathrm{SGD}(a, b)$ delar c finns det då en lösning till den Diofantiska ekvationen $ax + by = c$? För att svara på denna fråga gör vi först iakttagelsen att om $\mathrm{SGD}(a, b) \mid c$ kan vi förkorta båda leden i den Diofantiska ekvationen och få en ekvivalent Diofantisk ekvation $\tilde{a}x + \tilde{b}y = \tilde{c}$ där $\mathrm{SGD}(\tilde{a}, \tilde{b}) = 1$. Vi kan därför utan inskränkning anta att $\mathrm{SGD}(a, b) = 1$ från början.

Innan vi ger oss i kast med den allmänna Diofantiska ekvationen tittar vi först på specialfallet då $c = 1$, d.v.s. ekvationen $ax + by = 1$ där $\mathrm{SGD}(a, b) = 1$. Vi kan då skriva om ekvationen som $ax + by = \mathrm{SGD}(a, b)$ och vi vet nu från lemma 3.12 att denna ekvation har en lösning (x_0, y_0) där x_0 och y_0 är heltal. Vi har också sett att vi kan bestämma en sådan lösning genom att använda oss av Euklides algoritm ”baklänges”.

Vi gör nu observationen att om vi i $ax + by$ sätter in värden $x = -bn$ och $y = an$ där får vi $ax + by = -abn + abn = 0$ för alla $n \in \mathbb{Z}$. Om nu (x_0, y_0) löser den Diofantiska ekvationen $ax + by = 1$ har vi då för $x = x_0 - bn$ och $y = y_0 + an$ att

$$\begin{aligned} ax + by &= a(x_0 - bn) + b(y_0 + an) \\ &= ax_0 - abn + by_0 + abn \\ &= ax_0 + by_0 \\ &= 1 \end{aligned}$$

så även $(x_0 - bn, y_0 + an)$ är en lösning för varje $n \in \mathbb{Z}$. Frågan blir då om det kan finnas fler lösningar. Vi noterar att om (x_0, y_0) är en lösning så måste varje annan lösning ha

formen $(x_0 + u, y_0 + v)$ där u, v är några heltal. Om vi sätter in detta i ekvationen får vi

$$\begin{aligned} ax + by &= ax_0 + au + by_0 + bv \\ &= 1 + au + bv \\ &= 1 \\ \Leftrightarrow\ au + bv &= 0 \\ \Leftrightarrow\ \qquad au &= -bv \end{aligned}$$

Eftersom $a \mid au$ måste vi också ha att $a \mid -bv \iff a \mid bv$. Dessutom vet vet vi att $\mathrm{SGD}(a, b) = 1$ så a måste dela v och på motsvarande vis ser vi att b måste dela u. Vi kan alltså skriva $v = an$ och $u = bk$ för några $n, k \in \mathbb{Z}$. Vi får då att $au = abk = -abn \iff k = -n$ och därför måste lösningen ha formen $x = x_0 + u = x_0 - bn$ och $y = y_0 + v = y_0 + an$, men detta är precis de lösningar vi redan hittat. Vi har därmed visat att den allmänna lösningen till den Diofantiska ekvationen $ax + by = 1$ med $\mathrm{SGD}(a, b) = 1$ ges av alla tal på formen $x = x_0 - bn$ och $y = y_0 + an$ där n är ett heltal och (x_0, y_0) är någon lösning till ekvationen.

Så vad händer då om högerledet inte är 1 utan vi istället har ekvationen $ax + by = c$ där $\mathrm{SGD}(a, b) = 1$? Vi kan fortfarande hitta heltal x_0, y_0 som uppfyller ekvationen $ax_0 + by_0 = 1$. Om vi multiplicerar båda leden av den senare ekvationen med c får vi då

$$\begin{aligned} c &= c(ax_0 + by_0) \\ &= acx_0 + bcy_0 \end{aligned}$$

så vi ser att (cx_0, cy_0) är en lösning. Den allmänna lösningen ges då av alla tal på formen $x = cx_0 - bn$ och $y = cy_0 + an$. Vi sammanfattar detta i följande sats.

Sats 3.19. *Den Diofantiska ekvationen*

$$ax + by = c$$

där $\mathrm{SGD}(a, b) = 1$ *har den allmänna lösningen*

$$x = cx_0 - bn, \quad y = cy_0 + an,$$

där n *är ett godtyckligt heltal och* (x_0, y_0) *löser ekvationen* $ax + by = 1$.

För att göra det hela mer konkret och skapa en allmän lösningsmetod går vi igenom ett exempel.

Exempel 3.20. Lös den Diofantiska ekvationen $10x - 14y = 4$.

Lösning. Vi börjar med att kolla att $\mathrm{SGD}(10, 14)$ delar 4. Vi kan se, t.ex. genom primtalsfaktorisering, att $\mathrm{SGD}(10, 14) = 2$ och $2 \mid 4$ så ekvationen har en lösning. Vi förkortar nu båda led med 2 och får $5x - 7y = 2$. Vi börjar nu med att lösa hjälpekvationen $5x - 7y = 1$. Vi ställer först upp Euklides algoritm.

$$\begin{aligned} 7 &= 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Vi går nu igenom denna baklänges för att skriva 1 som en kombination av 7 och 5.

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7 - 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \end{aligned}$$

Härifrån ser vi alltså att $x = 3$ och $y = 2$ löser ekvationen $5x - 7y = 1$. Den allmänna lösningen ges därför av alla tal x, y på formen $x = 2 \cdot 3 + 7n$ och $y = 2 \cdot 2 + 5n$ eftersom $a = 5$ och $b = -7$ i den förkortade ekvationen. □

3.5 Talbaser och positionssystemet

Hittills har vi undersökt de hela talens allmänna egenskaper. Innan vi lämnar heltalen ska vi nu ändra spår och titta närmare på hur vi representerar de hela talen i skrift och hur man kan representera dem på andra sätt.

Vad menar vi egentligen när vi skriver ut ett heltal, till exempel 5732? Vad man menar är $5 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0$. Man talar om entalssiffror, tiotalssiffror, hundratalssiffror, o.s.v. Vi har valt att skriva tal som en summa av potenser av 10 med koefficienter mellan 0 och 9. Varje tal kan skrivas på detta vis, något man kan visa med hjälp av divisionsalgoritmen. Vi säger att vi representerar talen i *bas* 10 eller i det *decimala talsystemet*. Men just siffran 10 har ingen speciell matematisk signifikans utan man kan lika gärna välja något annat heltal $B \geq 2$. På samma sätt kan man då visa att varje heltal x kan skrivas på formen

$$x = a_0 B^0 + a_1 B^1 + a_2 B^2 + \cdots + a_n B^n$$

där varje a_k uppfyller $0 \leq a_k < B$. Vi kan då skriva talet x som $x = (a_n a_{n-1} \ldots a_2 a_1 a_0)_B$. Vi kallar detta för *$x$:s representation i basen B*.

Exempel 3.21. Vi vill skriva talet $1990 = (1990)_{10}$ i bas 7. Vi tittar då först på alla potenser av 7, som är $1, 7, 49, 343, 2401$. Eftersom $2401 > 1990$ kan inte någon 4-potens av 7 förekomma i talets representation i bas 7. Vi använder nu divisions algoritmen för att bestämma koefficienten för $343 = 7^3$. Vi ser då att $1990 = 5 \cdot 343 + 275$. Koefficienten framför 7^3 är alltså 5. Vi fortsätter nu på samma sätt med resten 275 och ser då att

$$\begin{aligned} 275 &= 5 \cdot 49 + 30 \\ 30 &= 4 \cdot 7 + 2 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Vi får då att $(1990)_{10} = (5542)_7$.

Två talbaser som används flitigt inom datavetenskap är baserna 2 och 16 som kallas det *binära talsystemet* och det *hexadecimala talsystemet*. Notera att för det hexadecimala talsystemet stöter man på problemet att våra vanliga siffror tar slut. Därför tar man ofta till bokstäverna A, B, C, D, E, F för att representera $10, 11, 12, 13, 14, 15$.

4 Induktion och andra bevismetoder

4.1 Motsägelsebevis och kontraposition

Motsägelsebevis är en så pass vanlig bevisform att det kan vara värt att studera den lite närmare. Vi kommer göra detta genom att bevisa några resultat som vanligtvis bevisas med motsägelsebevis och som en utmärkt ursäkt att bevisa några viktiga resultat som inte riktigt passar in någon annanstans. Vi börjar med ett väldigt klassiskt resultat, känt sedan Euklides.

Sats 4.1. *Det finns oändligt många primtal.*

Bevis. Eftersom vi ska utföra ett motägelsebevis börjar vi med att anta motsatsen till det vi vill bevisa. Vi antar därför att det bara finns ändligt många primtal. Målet är nu att visa att detta antagande leder till en motsägelse. Eftersom det bara finns ändligt många primtal kan vi skriva dem som $p_1, p_2, \ldots, p_n$. Vi bildar nu talet $a = p_1 p_2 \ldots p_n + 1$. Eftersom $a \neq p_m$ för alla m kan inte a vara ett primtal. Därför måste det vara delbart med något av dem. Men om vi utför en division av a med något primtal får vi rest 1. Här har vi alltså hittat en motsägelse och beviset är då färdigt. □

Observera att talet $p_1 p_2 \ldots p_n + 1$ i sig inte behöver vara ett primtal. Till exempel gäller att $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, primtalsfaktorerna är större än de primtal som användes för att bilda talet.

Inför nästa sats påminner vi oss om att ett *irrationellt tal* x är ett reellt tal som inte är ett rationellt tal, d.v.s. det kan inte skrivas på formen $x = \frac{a}{b}$ för några heltal a, b.

Sats 4.2. $\sqrt{2}$ *är ett irrationellt tal.*

Bevis. Vi antar motsatsen, att $\sqrt{2}$ är ett rationellt tal. Då kan vi hitta heltal a, b sådana att $\mathrm{SGD}(a, b) = 1$, $b > 0$ och $\sqrt{2} = \frac{a}{b}$. Därför får vi att $2 = \frac{a^2}{b^2} \Leftrightarrow 2b^2 = a^2$. I synnerhet ser vi att a^2 är ett jämnt tal och därför måste även a vara ett jämnt tal. Vi kan alltså skriva $a = 2c$ för något heltal c. Då ser vi att $a^2 = (2c)^2 = 4c^2 \Rightarrow 2b^2 = 4c^2 \Leftrightarrow b^2 = 2c^2$ så även b måste vara ett jämnt tal. Men om både a och b är jämna tal så är 2 en gemensam delare vilket betyder att $\mathrm{SGD}(a, b) \neq 1$. Här har vi motsägelsen. □

Sats 4.3. $\sqrt[3]{2}$ *är ett irrationellt tal.*

Bevis. Vi kan göra som i förra beviset. Antag motsatsen, att $\sqrt[3]{2} = \frac{a}{b}$ med $\mathrm{SGD}(a, b) = 1$ och $b > 0$. Vi ser då att $2 = \frac{a^3}{b^3} \Leftrightarrow 2b^3 = a^3$. På precis samma sätt som i föregående bevis kan vi då inse att både a och b måste vara jämna tal, vilket motsäger att $\mathrm{SGD}(a, b) = 1$.

Vi kan också skriva $2b^3 = b^3 + b^3 = a^3$. Detta är också en motsägelse enligt Fermat's stora sats. □

Vi gör ett till bevis av liknande karaktär.

Sats 4.4. *Talet* $\log_2(3)$ *är irrationellt.*

Bevis. Precis som tidigare börjar vi med att anta att vi kan skriva $\log_2(3) = \frac{a}{b}$ där a, b är heltal, $\text{SGD}(a,b) = 1$ och $b > 0$. Vi har då följande:

$$\begin{aligned} 3 &= 2^{\log_2(3)} \\ &= 2^{\frac{a}{b}} \quad \Rightarrow \\ 3^b &= 2^a \,. \end{aligned}$$

Om $a > 0$ är detta omöjligt eftersom talen 3^b och 2^b saknar gemensamma delare och därför inte kan vara samma tal. Om istället $a \leq 0$ har vi $2^a \leq 1$ medans $3^b \geq 3$ vilket också gör att de omöjligt kan vara samma tal. Vi ser alltså att oavsett a, b får vi en motsägelse. □

Om en sats man vill bevisa är formulerad som en implikation och denna visar sig vara svår att bevisa kan det också vara värt att istället försöka bevisa kontrapositionen av påståendet. Eftersom en implikation och dess kontraposition är ekvivilenta utsagor har vi därför också bevisat den ursprungliga satsen. I beviset av sats 4.2 använde vi oss av att om a^2 är jämnt så är även a jämnt. Detta kan bevisas direkt men det är möjligen ännu enklare att bevisa det genom att bevisa dess kontraposition: om a inte är jämnt så är a^2 inte jämnt. Vi formulerar påståendet och ger båda bevisen för jämförelse.

Sats 4.5. *Låt a vara ett heltal. Om a^2 är ett jämnt tal så är även a ett jämnt tal.*

Bevis 1. Vi börjar med att bevisa satsen direkt. Om a^2 är ett jämnt tal har det en primtalsfaktorisering $a^2 = p_1 p_2 \dots p_n$ där något av $p_i = 2$. Vidare har a en primtalsfaktorisering $a = q_1 q_1 \dots q_m$. Vi måste därför ha att $a^2 = p_1 p_2 \dots p_n = (q_1 q_2 \dots q_m)(q_1 q_2 \dots q_m) = q_1 q_1 q_2 q_2 \dots q_m q_m$. Vi ser då att om 2 förekommer i primtalsfaktoriseringen av a^2 måste det även förekomma i primtalsfaktoriseringen av a och därför är även a ett jämnt tal. □

Bevis 2. Vi bevisar nu istället satsen kontraposition, d.v.s. om a inte är ett jämnt tal så är a^2 inte heller ett jämnt tal. Ett heltal som inte är jämnt måste vara udda så vi kan skriva $a = 2n+1$ för något heltal n. Då får vi $a^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$ så a^2 är också udda. □

Vi gör ett till bevis med hjälp av kontraposition.

Sats 4.6. *Låt x, y vara positiva reella tal. Om $xy \geq C$ så gäller att $x \geq \sqrt{C}$ eller $y \geq \sqrt{C}$.*

Bevis. Utsagan i satsen skrivs formellt som $\forall x, y \in \mathbb{R},\, x, y > 0$: $xy \geq C \;\Rightarrow\; x \geq \sqrt{C} \vee y \geq \sqrt{C}$. Dess kontraposition är därför $\forall x, y \in \mathbb{R},\, x, y > 0$: $(x < \sqrt{C}) \wedge (y < \sqrt{C}) \;\Rightarrow\; xy < C$. Vi låter därför $x, y \in \mathbb{R}$ uppfylla att $0 < x < \sqrt{C}$ och $0 < y < \sqrt{C}$. Det följer då att $xy < \sqrt{C}y < \sqrt{C}\sqrt{C} = C$. □

4.2 Summor

Vi ska nu införa ett smidigt sätt att skriva summor och sedan utforska några egenskaper som särskilda summor.

Låt $a_1, a_2, \ldots, a_n$ vara n stycken (komplexa) tal. Vi betecknar då deras summa med

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n.$$

Vi läser detta som "summan av a_k då k går från 1 till n". Bokstaven k används här för att numrera termerna i summan och kallas för *summationsindex*. Summationsindexet används enbart i summan och har ingen mening utanför den och precis som med variabler kan man använda sig av vilken ledig symbol som helst. Symbolen $\sum$ är en variant av den grekiska bokstaven för stora sigma och motsvarar på så vis den latinska bokstaven S.

Några konkreta exempel är

$$\sum_{k=0}^{5} k = 0 + 1 + 2 + 3 + 4 + 5$$
$$\sum_{j=1}^{4} \frac{1}{j^2} = \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16}$$
$$\sum_{l=3}^{8} 1 = 1 + 1 + 1 + 1 + 1 + 1$$

En summa kan också vara tom, som i fallet $\sum_{n=7}^{3} a_n$ och man brukar då ge den värdet 0

Notera att några räkneregler för summor följer automatiskt. Till exempel har vi följande

$$\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} a_k + b_k$$
$$\sum_{k=0}^{n} ca_k = c \sum_{k=0}^{n} a_k$$

för varje konstant c.

Om varje term i en summa har formen $a_k = ak + b$ där a, b är två fixa tal kallar man summan

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} ak + b$$

för en *aritmetisk summa*. Det som är speciellt för en aritmetisk summa är att differensen mellan två på varandra följande termer a_k, a_{k+1} alltid är samma, nämligen

$$\begin{aligned} a_{k+1} - a_k &= a(k+1) + b - ak - b \\ &= a. \end{aligned}$$

Det finns också en formel för att enkelt beräkna värdet av en aritmetisk summa. För att hitta denna formel fixerar vi $a, b, n \in \mathbb{Z}$ och betraktar summan

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} ak + b.$$

Vi observerar också att vi lika gärna kan summera i omvänd ordning, d.v.s.

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} a_{n-k}.$$

Med detta kan vi nu skriva

$$\begin{aligned} 2\sum_{k=0}^{n} a_k &= \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} a_k \\ &= \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} a_{n-k} \\ &= \sum_{k=0}^{n} a_k + a_{n-k}. \end{aligned}$$

För att komma längre behöver vi alltså undersöka termerna $a_k + a_{n-k}$. Eftersom vi vet att varje term $a_k = ak + b$ kan vi skriva

$$\begin{aligned} a_k + a_{n-k} &= ak + b + a(n-k) + b \\ &= an + 2b \\ &= a_n + b \\ &= a_n + a_0. \end{aligned}$$

Varje term har alltså ett konstant värde. Tillsammans med vad vi har sedan tidigare kan vi nu skriva

$$\sum_{k=0}^{n} a_k = \frac{(n+1)(a_n + a_0)}{2}.$$

Sats 4.7. *Värdet av en aritmetisk summa ges av*

$$\sum_{k=0}^{n} a_k = \frac{(n+1)(a_n + a_0)}{2}.$$

Vi kollar så att formeln stämmer i ett enkelt exempel:

$$\sum_{k=0}^{0} a_k = a_0 = 1 \cdot \frac{a_0 + a_0}{2}$$

så formeln stämmer för $n = 0$.

En annan speciell typ av summa är den *geometriska summan* där två på varandra följande termer har en konstant kvot (istället för differens som för aritmetiska summor).

Allmänt ser termerna i en geometrisk summa ut som $a_k = ar^k$ där a, r är två tal. Vi ser då att

$$\frac{a_{k+1}}{a_k} = \frac{ar^{k+1}}{ar^k} = r.$$

Även för geometriska summor kan man hitta en enkel formel för summans värde. För att hitta denna formel börjar vi med en geometrisk summa

$$\sum_{k=0}^{n} ar^k.$$

Om vi multiplicerar denna summa med r får v

$$\begin{aligned} r\sum_{k=0}^{n} ar^k &= \sum_{k=0}^{n} ar^{k+1} \\ &= \sum_{k=1}^{n+1} ar^k \,. \end{aligned}$$

Vi ser att denna summa innehåller nästan samma termer som den ursprungliga summan, fast alla har en grad högre. Om vi då tar differensen av de båda summorna får vi därför många cancellationer, alla termerna utom ar^k för $k = 0$ och $k = n + 1$ finns ju i båda summorna och tar därför ut varandra och bara $a - ar^{n+1}$ blir kvar:

$$\begin{aligned} (1-r)\sum_{k=0}^{n} ar^k &= \sum_{k=0}^{n} ar^k - \sum_{k=1}^{n+1} ar^k \\ &= a - ar^{n+1} \\ &= a(1 - r^{n+1}) \,. \end{aligned}$$

Om $r \neq 1$ kan vi då dividera båda sidorna med $1 - r$ och får du en formel för den geometriska summan. Om $r = 1$ ser vi att varje term i den geometriska summan blir $a_k = a \cdot 1^k = a$ så i detta fall blir värdet helt enkelt $(n + 1)a$. Vi sammanfattar detta i en till sats.

Sats 4.8. *Den geometriska summan $a_k = ar^k$ då k går från 0 till n har värdet*

$$\sum_{k=0}^{n} ar^k = \begin{cases} a\dfrac{1 - r^{n+1}}{1 - r} & \text{om } r \neq 1, \\ (n+1)a & \text{om } r = 1 \,. \end{cases}$$

Exempel 4.9. Den geometriska summan

$$\sum_{k=0}^{n} \frac{1}{2^k}$$

har $a = 1$ och $r = \frac{1}{2}$. Därför har den värdet

$$\begin{aligned}\sum_{k=0}^{n} \frac{1}{2^k} &= 1 \cdot \frac{1 - (\frac{1}{2})^{n+1}}{1 - \frac{1}{2}} \\ &= \frac{\frac{2^{n+1}-1}{2^{n+1}}}{\frac{1}{2}} \\ &= \frac{2^{n+1} - 1}{2^n} \\ &= 2 - \frac{1}{2^n}\,.\end{aligned}$$

För att avsluta vår diskussion om summor och leda oss in på nästa ämne ska vi nu undersöka om vi kan hitta ett annat sätt att bevisa formeln för värdet av en aritmetisk summa. Om vi vet att formeln stämmer upp till något naturligt tal p, d.v.s. vi vet att $\sum_{k=0}^{p} a_k = (n+1)\frac{a_p + a_0}{2}$ (till exempel $p = 0$ som vi har kontrollerat), kan vi då säga något om värdet för summan $\sum_{k=0}^{p+1} a_k$? Om vi kan göra detta är vi klara, för då vet vi att om formeln stämmer för något p så stämmer den också för $p + 1$. Men då måste den också stämma för $p + 2$ och $p + 3$, $p + 4$, o.s.v. och vi kan därför dra slutsatsen att den måste gälla för alla naturliga tal. Vi provar:

$$\begin{aligned}\sum_{k=0}^{p+1} a_k &= \sum_{k=0}^{p} a_k + a_{p+1} && \text{(bryt ut den sista termen} \\ &= \frac{(p+1)(a_p + a_0)}{2} + a_{p+1} && \text{(använd formeln för } p) \\ &= \frac{(p+1)(pa + b + b)}{2} + a(p+1) + b && \text{(skriv ut alla } a_k) \\ &= \frac{(p+1)(pa + 2b) + (p+1)2a + 2b}{2} \\ &= \frac{(p+1)(p+2)a + (p+2)2b}{2} \\ &= \frac{(p+2)((p+1)a + 2b)}{2} \\ &= \frac{(p+2)(a_{p+1} + a_0)}{2}\,.\end{aligned}$$

Vi lyckades alltså visa att om formeln gäller för p så måste den även gälla för $p + 1$.

4.3 Induktionsbevis

I vårt alternativa bevis för värdet av en aritmetisk summa hade vi en utsaga P_n för varje naturligt tal n som sade att en aritmetisk summa har ett värde som ges av

$$\sum_{k=0}^{n} a_k = \frac{(n+1)(a_n + a_0)}{2}\,.$$

Vi visste att utsagan P_n var sann för till exempel $n = 0$. Vi visade sedan att om utsagan P_p är sann för något naturligt tal p så är även P_{p+1} sann. Vi drog då slutsatsen att P_n är sann för alla naturliga tal n. Detta kallas för *induktionsprincipen*:

Induktionsprincipen: Låt P_n vara en utsaga om ett naturligt tal n. Låt följande utsagor vara sanna:

1. P_0 är sann,
2. för varje naturligt tal p gäller $P_p \Rightarrow P_{p+1}$.

Då är P_n sann för alla naturliga tal n.

Ett induktionsbevis går alltså till på följande vis:

1. Visa ett *basfall* (B), d.v.s. att P_0 är sann.
2. Antag att P_p är sann för något naturligt tal p. Detta kallas *induktionsantagande* (IA).
3. Skriv om P_{p+1} så att induktionsantagandet kan användas för att bevisa utsagan. Detta kallas *induktionssteg* (IS).
4. Enligt induktionsprincipen är då P_n sann för alla naturliga tal n.

Ett induktionsbevis jämförs ofta med ett oändligt antal dominobrickor uppställda så att om någon bricka välter så knuffar den till nästa bricka så att den också välter, o.s.v. Basfallet kan då ses som att man välter den första brickan och får därför varje annan bricka att välta förr eller senare.

Man behöver inte ha P_0 som basfall men om man väljer något annat basfall P_{n_0} med $n_0 > 0$ har man bara bevisat P_n för alla naturliga tal $n \geq n_0$.

Exempel 4.10. Vi vill visa att formeln

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}(2n^3 + 3n^2 + n)$$

är sann för alla naturliga tal $n \geq 1$.[3] Vi kan formulera detta på följande vis:

$$VL_n = \sum_{k=1}^{n} k^2, \quad HL_n = \frac{1}{6}(2n^3 + 3n^2 + n), \quad P_n \Leftrightarrow (VL_n = HL_n)\,.$$

Vi går nu igenom listan.

[3] Faktum är att den även är sann för $n = 0$ eftersom summan då är tom.

B: För $n = 1$ har vi

$$\begin{aligned} VL_1 &= \sum_{k=1}^{1} k^2 \\ &= 1 \\ HL_1 &= \frac{1}{6}(2 \cdot 1^3 + 3 \cdot 1^2 + 1) \\ &= 1 \end{aligned}$$

så vi ser att $VL_1 = HL_1$ så P_1 är sann.

IA: Antag att $VL_p = HL_p$ för något naturligt tal $p \geq 2$.

IS:

$$\begin{aligned} VL_{p+1} &= \sum_{k=1}^{p+1} k^2 \\ &= \sum_{k=1}^{p} k^2 + (p+1)^2 && \text{(bryt ut sista termen)} \\ &= \frac{2p^3 + 3p^2 + p}{6} + p^2 + 2p + 1 && \text{(använd IA)} \\ &= \frac{2p^3 + 9p^2 + 13p + 6}{6} \\ HL_{p+1} &= \frac{2(p+1)^3 + 3(p+1)^2 + p + 1}{6} \\ &= \frac{2p^3 + 6p^2 + 6p + 2 + 3p^2 + 6p + 3 + p + 1}{6} \\ &= \frac{2p^3 + 9p^2 + 13p + 6}{6} \end{aligned}$$

Vi ser alltså att $VL_p = HL_p \Rightarrow VL_{p+1} = HL_{p+1}$.

Vi drar nu slutsatsen att $VL_n = HL_n$ för alla naturliga tal n med hjälp av induktionsprincipen.

Föregående exempel visar på en av styrkorna (och svagheterna) med induktionsbevis: vi behöver inte ha någon aning om varifrån formeln $\frac{1}{6}(2n^3 + 3n^2 + n)$ kommer för att genomföra beviset.

Det finns också en annan formulering av induktionsprincipen som kan vara användbar.

Starka induktionsprincipen: Låt P_n vara en utsaga om ett naturligt tal n. Låt följande utsagor vara sanna:

1. P_0 är sann,
2. om P_n är sann för alla naturliga tal $n \leq p$ så är också P_{p+1} sann.

Då är P_n sann för alla naturliga tal n.

Namnet syftar till det till synes starkare antagandet att P_n ska vara sann för alla n upp till och med p men den starka induktionsprincipen är i själva verket ekvivalent med den vanliga induktionsprincipen. Man får alltså avgöra vilken av formuleringarna som lämpar sig bäst för vad man vill bevisa. Om man till exempel behöver använda både P_{n-1} och P_{n-2} för att bevisa P_n kan det vara på sin plats att använda den starka induktionsprincipen. Då behövs i regel också fler än ett basfall: för att bevisa P_2 måste vi först bevisa både P_1 och P_0.

Det kan även gå fel i induktionsbevis. Eftersom det är många steg i ett induktionsbevis finns också många tillfällen för misstag att smyga sig in i resonemanget. Om något steg i ett induktionsbevis faller så faller hela beviset. Här är ett ökänt exempel på ett felaktigt induktionsbevis.

Exempel 4.11. Vi ska bevisa att alla hus har samma färg.

B: Ett hus har automatiskt samma färg som sig självt.

IA: Varje mängd av p hus består av endast en färg.

IS: Betrakta en mängd med $p+1$ hus och numrerar dem med $1, 2, 3, \ldots, p, p+1$. Mängderna $\{1, 2, 3, \ldots, p\}$ och $\{2, 3, 4, \ldots, p+1\}$ består då vardera av p hus och enligt induktionsantagandet består båda mängderna av hus av samma färg, t.ex. alla hus i den första mängden är blåa och alla hus i den andra mängden är röda. Eftersom mängderna överlappar måste färgerna på husen i de två mängderna dessutom vara samma färg. Därför har alla hus i den urspungliga mängden samma färg.

Enligt induktionsprincipen kan vi därför dra slutsatsen att i varje mängd av godtyckligt många hus har alla hus samma färg. I synnerhet kan vi titta på mängden av alla hus och, eftersom denna mängd är ändlig, dra slutsatsen att alla hus har samma färg. Denna utsaga är uppenbarligen felaktig så någonstans finns ett fel i logiken. Kan du hitta det?[4]

4.4 Rekursion

Rekursion är en metod för att definiera en följd av objekt a_n där objekt a_{n+1} definieras i termer av objekten $a_n, a_{n-1}, \ldots, a_0$. Vi måste även bidra explicit med så många objekt som behövs för att starta rekursionen. Om till exempel varje objekt i följden definieras av de två föregående objekten behöver vi först definiera två objekt explicit för att kunna använda rekursionen för att definiera ett tredje, ett fjärde, o.s.v. Enligt induktionsprincipen leder detta till en väldefinierad oändlig följd av objekt. Objekten i fråga kan vara vad som helst. Vi ska titta närmare på rekursivt definierade talföljder, d.v.s. varje a_n är ett tal.

[4]Svar: De två mängderna $\{1, \ldots, p\}$ och $\{2, \ldots, p+1\}$ överlappar inte för $p = 1$.

Exempel 4.12. Talföljden $1, 2, 4, 8, 16, \ldots$ kan beskrivas med $a_n = 2^n$ men den kan också definieras rekursivt genom

$$\begin{aligned} a_0 &= 1, \\ a_{n+1} &= 2a_n \quad \text{för } n \geq 1. \end{aligned}$$

Man brukar säga att formeln $a_n = 2^n$ är en *sluten formel* för den rekursivt definierade talföljden a_n.

Exempel 4.13. En välkänd talföljd som är definierad rekursivt är *Fibonaccitalen*. De definieras på följande vis:

$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_{n+1} &= F_n + F_{n-1} \quad \text{för } n \geq 1. \end{aligned}$$

De 11 första Fibonaccitalen ges alltså av $0, 1, 1, 2, 3, 5, 8, 13, 21, 34$.

Induktion kan också användas för att bevisa egenskaper hos rekursiva talföljder.

Exempel 4.14. Betrakta talföljden $a_0 = 2$, $a_{n+1} = \sqrt{6 + a_n}$. Vi kan då bevisa att $a_n < 3$ för alla n.

B: Vi har $a_0 = 2 < 3$.

IA: Antag att $a_p < 3$ för något $p \in \mathbb{N}$.

IS: Vi har att

$$\begin{aligned} a_{p+1} &= \sqrt{6 + a_p} \\ &< \sqrt{6 + 3} \\ &= \sqrt{9} \\ &= 3. \end{aligned}$$

Induktionsprincipen säger oss därför att $a_n < 3$ för alla $n \in \mathbb{N}$.

5 Mer mängdlära

5.1 Funktioner

Vi lämnar nu heltalen för tillfället och utforskar andra koncept. Vi kommer börja med en informell definition av vad en funktion är för att få en bild av vad vi intuitivt ser som en funktion innan vi gör en formell definition av vad en funktion är.

För att informellt definiera vad en funktion är behöver vi först två mängder, X och Y. En funktion f från X till Y är då en regel som till varje element $x \in X$ associerar exakt

ett element $f(x) \in Y$. För att visa att f är en funktion från mängden X till mängden Y använder vi skrivsättet $f\colon X \to Y$. För enskilda element $x \in X$ skriver vi $x \mapsto f(x)$. Observera att två olika pilar används. Vi kallar mängden X för f:s *definitionsmängd* och betecknas ofta med D_f medans mängden Y kallas för f:s *målmängd*. Istället för att titta på vad f gör med enskilda element kan vi för en delmängd $C \subseteq X$ också definiera mängden

$$f(C) = \{f(x)\colon x \in C\} \subseteq Y.$$

Vi kallar denna mängd för *bilden av* C. Mängden $f(X)$ kallas för f:s *värdemängd* och betecknas ofta med V_f. I allmänhet behöver inte målmängden och värdemängden för en funktion vara samma.

När man arbetar med funktioner brukar man ofta också prata om funktioners *graf*, speciellt om man har en funktion $f\colon \mathbb{R} \to \mathbb{R}$. I det fallet är grafen alla punkter i ett koordinatsystem som uppfyller ekvationen $y = f(x)$. Punkter i ett koordinatsystem skrivs som (x, y) där x anger positionen på ena axeln och y anger positionen på den andra axeln. Eftersom $(x, y) \neq (y, x)$ i allmänhet kallar man detta för ett *ordnat par*. Begreppet ordnat par kan generaliseras till allmänna mängder, nämligen givet två mängder X, Y kan vi bilda mängden av alla ordnade par (x, y) där $x \in X$ och $y \in Y$. Vi betecknar denna mängd med $X \times Y$ och den kallas för den *Cartesiska produkten av* X *och* Y. Vi har alltså

$$X \times Y = \{(x, y)\colon x \in X \wedge y \in Y\}.$$

Till exempel kan vi betrakta mängden $\mathbb{R} \times \mathbb{R}$ som alltså består av alla ordnade par av reella tal. Denna mängd brukar kallas (det reella) *talplanet* och betecknas $\mathbb{R}^2$. Det är alltså denna mängd man representerar när man ritar upp ett koordinatsystem: man kan tänka sig den första mängden $\mathbb{R}$ som den horisontella axeln och den andra mängden $\mathbb{R}$ som den vertikala axeln.

Det är viktigt att skilja på (x, y) och $\{x, y\}$ eftersom vi i regel har $(x, y) \neq (y, x)$ (om inte $x = y$) medans det alltid gäller att $\{y, x\} = \{x, y\}$. Den Cartesiska produkten låter oss också göra en formell definition av begreppet funktion.

Definition 5.1. Låt X och Y vara två mängder. En funktion $f\colon X \to Y$ är en delmängd av den Cartesiska produkten $X \times Y$ med egenskapen att det för varje $x \in X$ finns ett unikt $y \in Y$ sådant att (x, y) är ett element i denna delmängd. Detta y betecknas med $f(x)$. Två funktioner f och g betraktas som lika och vi skriver $f = g$ om de har samma definitionsmängder och samma målmängder och $f(x) = g(x)$ för varje $x \in D_f = D_g$.

Med denna definition har vi alltså identifierat en funktion med dess graf. I övrigt används samma terminologi som vi har använt tidigare.

Ett vanligt sätt att ange funktioner är att ge ange $f(x)$ i termer av en ekvation som har en unik lösning för varje x, till exempel $f(x) = x^2$ eller $f(x) = e^x$.

Givet två funktioner $f\colon X \to Y$ och $g\colon Y \to Z$ kan man även skapa den *sammansatta funktionen* $g \circ f\colon X \to Z$ som ges av $(g \circ f)(x) = g(f(x)) \quad \forall x \in X$. Det är viktigt att målmängden för f sammanfaller med definitionsmängden för g för att vara säker på att sammansättningen $g \circ f$ är definierad.

Vi ska nu definiera några viktiga specialfall av funktioner som vi även kommer stöta på senare.

Definition 5.2. Låt $f\colon X \to Y$.

1. Funktionen f kallas *injektiv* om $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ för alla $x_1, x_2 \in X$. Vi säger att f är en *injektion*.
2. Funktionen f kallas *surjektiv* om $V_f = Y$. Vi säger att f är en *surjektion*.
3. Funktionen f kallas *bijektiv* om den är både injektiv och surjektiv. Vi säger att f är en *bijektion*.

Om en funktion är injektiv, surjektiv eller bijektiv kan bero på vad man väljer för definitionsmängd och målmängd. Vi visar detta med ett exempel.

Exempel 5.3. Låt funktionen $f\colon \mathbb{R} \to \mathbb{R}$ ges av $f(x) = x^2$. Funktionen f är inte injektiv eftersom ekvationen $y = x^2$ har lösningarna $x = \pm\sqrt{y}$ för $y \geq 0$ som dessutom är olika för $y > 0$. Vi kan alltså hitta två olika tal $x_1 = \sqrt{y}, x_2 = -\sqrt{y}$ som uppfyller $x_1 \neq x_2$ men $f(x_1) = f(x_2)$. Den är heller inte surjektiv eftersom dess värdemängd är alla ickenegativa reella tal. Till exempel har vi att $-1 \in \mathbb{R}$ men $-1 \notin V_f$ så $V_f \neq \mathbb{R}$.

Om vi däremot begränsar funktionen f till mängden $\mathbb{R}_{\geq 0}$, d.v.s. mängden av alla ickenegativa reella tal, får vi en funktion $f|_{\mathbb{R}_{\geq 0}}\colon \mathbb{R}_{\geq 0} \to \mathbb{R}$. Då är $f|_{\mathbb{R}_{\geq 0}}$ en injektiv funktion eftersom ekvationen $y = x^2$ nu bara har lösningen $x = \sqrt{y}$ i sin definitionsmängd. Den är dock fortfarande inte surjektiv.

Om vi dessutom ändrar målmängden för $f|_{\mathbb{R}_{\geq 0}}$ kan vi skapa funktionen $g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ som nu är både injektiv och surjektiv och därmed bijektiv eftersom den sedan tidigare var injektiv och vi nu har ändrat målmängden så att den sammanfaller med värdemängden.

Däremot är det fortfarande sant att $g(x) = f|_{\mathbb{R}_{\geq 0}}(x) = f(x) = x^2$ för alla $x \in \mathbb{R}_{\geq 0}$ fast att $g, f|_{\mathbb{R}_{\geq 0}}, f$ är tre olika funktioner. Det är alltså inte bara formen på ekvationen som bestämmer funktionen utan även vilka definitions- och målmängder man använder.

Eftersom en bijektion $f\colon X \to Y$ även är en surjektion kan vi för varje $y \in Y$ hitta något $x \in X$ som löser ekvationen $y = f(x)$. Eftersom det dessutom är en injektion vet vi att detta x är unikt. Detta låter oss då skapa en ny funktion

$$f^{-1}\colon Y \to X$$

som till varje $y \in Y$ associerar just detta x. Denna funktion kallas för *inversen av* f. Förhållandet mellan f och f^{-1} kan beskrivas med

$$y = f(x) \Leftrightarrow f^{-1}(y) = x.$$

Det följer härifrån att $f^{-1}(f(x)) = f^{-1}(y) = x$ och att $f(f^{-1}(y)) = f(x) = y$ så att funktionen $f^{-1} \circ f\colon X \to X$ associerar till varje $x \in X$ just x självt. Samma sak gäller för $f \circ f^{-1}\colon Y \to Y$. Funktionen $\mathrm{id}\colon X \to X$ som ges av $\mathrm{id}(x) = x$ kallas för *identitetsfunktionen*. Iblands skriver man även id_X för att markera vilken mängd identitetsfunktionen är definierad på. Vi kan nu skriva $f^{-1} \circ f = \mathrm{id}_X$ och $f \circ f^{-1} = \mathrm{id}_Y$.

Exempel 5.4. Vi såg nyss att funktionen $g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ är bijektiv. Den har därför en invers som ges av $g^{-1}(x) = \sqrt{x}$.

Funktionen $f\colon \mathbb{R} \to \mathbb{R}_+$ som ges av $f(x) = e^x$ där $\mathbb{R}_+$ är mängden av alla positiva reella tal är också bijektiv. Dess invers ges av $f^{-1}(x) = \ln(x)$.

5.2 Relationer

Vi ska nu titta på en enkel generalisering av funktioner. Vi börjar med en definition.

Definition 5.5. En *relation* R mellan två mängder X och Y är en delmängd $R \subseteq X \times Y$. Om $(x, y) \in R$ skriver vi xRy och säger då att "x står i relation R till y". Om $X = Y$ säger man att R är en relation på X.

Vi har helt enkelt slopat kravet på att det för varje $x \in X$ finns ett unikt $y \in Y$ sådant att xRy. Det betyder alltså att det kan finnas flera $y_1, y_2 \in Y$ sådana att xRy_1 och xRy_2.

Definitionen själv säger oss kanske inte så mycket om vad en relation är eller hur den beter sig. Vi kan direkt se att alla funktioner också är relationer men inte så mycket mer. Vi ska därför titta på några exempel.

Exempel 5.6.

1. Utsagan $a \,|\, b$ kan ses som en relation R på $\mathbb{Z}$ där $aRb \Leftrightarrow a \,|\, b$.

2. För reella tal x, y kan utsagan $x \leq y$ ses som en relation på $\mathbb{R}$ där x står i relation till y om och endast om $x \leq y$. Samma resonemang gäller även för andra olikheter.

3. Vi kan definiera en relation R på $\mathbb{R}^2$ genom $(x_1, y_1)R(x_2, y_2) \Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2$. De två punkterna (x_1, y_1) och (x_2, y_2) står alltså i relation till varandra om de ligger på en och samma cirkel runt origo.

Tre speciella egenskaper som många viktiga relationer på en mängd uppfyller har fått särskilda namn.

Definition 5.7. Låt R vara en relation på X.

1. R kallas *reflexiv* om xRx för alla $x \in X$.

2. R kallas *symmetrisk* om $xRy \Rightarrow yRx$ för alla $x, y \in X$.

3. R kallas *transitiv* om $xRy \wedge yRz \Rightarrow xRz$ för alla $x, y, z \in X$.

Exempel 5.8. Relationen $\leq$ på R är reflexiv och transitiv men inte symmetrisk. Till exempel har vi att $1 \leq 2$ men inte $2 \leq 1$. Om vi istället betraktar relationen $<$ så är den endast transitiv.

5.3 Ekvivalensrelationer

Ekvivalensrelationer är en särskild och mycket viktig klass av relationer på en mängd. Ekvivalensrelationer dyker upp i alla områden av matematiken och används bland annat för att avgöra om två objekt i någon mening är ”lika”.

Definition 5.9. En relation R på mängden X kallas för en *ekvivalensrelation* om den är reflexiv, symmetrisk och transitiv.

Vi går igenom några exempel.

Exempel 5.10.

1. Relationen $=$ kan ses som en ekvivalensrelation på en mängd. Den är reflexiv eftersom $x = x$ oavsett x. Den är symmetrisk eftersom om $x = y$ så måste vi även ha $y = x$. Slutligen, den är transitiv eftersom om $x = y$ och $y = z$ så har vi $x = y = z$ så $x = z$.

2. Låt X vara mängden av alla linjer i planet $\mathbb{R}^2$ och låt R vara relationen på X som ges av xRy om och endast om x och y är parallella. Då är R en ekvivalensrelation.

3. Relationen R på $\mathbb{R}^2$ som ges av $(x_1, y_1)R(x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$ är en ekvivalensrelation.

4. Låt M vara mängden av alla människor och låt R vara relationen på M som ges av xRy om och endast om x och y är födda samma år. Då är R en ekvivalensrelation på M.

Låt nu R vara en ekvivalensrelation på en mängd X och låt $x \in X$. Vi kan då betrakta mängden

$$[x] = \{y \in X \colon xRy\}$$

som kallas för *ekvivalensklassen av* x. Ekvivalensklasserna har en speciell egenskap som vi nu ska utforska och som kommer leda till en viktig sats.

Till att börja med vet vi att en ekvivalensrelation är reflexiv och därvid följer att $x \in [x]$ för varje $x \in X$. Alltså är ingen ekvivalensklass tom och varje $x \in X$ är också ett element i någon ekvivalensklass.

Låt nu $y \in [x]$. Vi kan så klart också betrakta $[y]$. Låt nu också $z \in [x]$. Vi vet då att xRz. Eftersom R är symmetrisk har vi även yRx och från transitiviteten följer att yRz eftersom yRx och xRz. Så $z \in [y]$. Men eftersom z var vilket element som helst i $[x]$ följer då att $z \in [y] \quad \forall z \in [x]$. Med andra ord, $[x] \subseteq [y]$. På grund av symmetrin kan vi även visa, på samma sätt, att $[y] \subseteq [x]$. Vi måste därför ha att $[x] = [y]$.

Antag nu att vi har $x, y \in X$ som inte står i relation till varandra. Vi vill nu visa att vi då måste ha $[x] \cap [y] = \varnothing$. Vi gör detta enklast genom att bevisa dess kontraposition, att $z \in [x] \cap [y] \implies xRy$. Eftersom $z \in [x] \cap [y]$ har vi xRz och $yRz \iff zRy$ eftersom R är symmetrisk. Enligt transitivitet har vi då xRy så kontrapositionen är bevisad. I själva verket har vi då $[x] = [y]$ enligt ovan.

Vi sammanfattar detta i följande mycket viktiga sats.

Sats 5.11. *Låt R vara en ekvivalensrelation på en mängd X. Då är ekvivalensklasserna för R parvis disjunkta och deras union är hela X.*

Vi går nu tillbaks till våra tidigare exempel och identifierar alla ekvivalensklasser.

Exempel 5.12.

1. Ekvivalensklasserna för relationen $=$ består enbart av elementet självt, d.v.s. $[x] = \{x\}$.

2. Ekvivalensklasserna består i det här fallet av alla linjer som är parallella med varandra, d.v.s. alla linjer med samma en och samma lutning.

3. Här består ekvivalensklasserna av alla punkter med ett och samma avstånd från origo. Om (x, y) har avståndet r från origo består alltså ekvivalensklassen $[(x, y)]$ av cirkeln med radie r centrerad i origo. Ekvivalensklasserna delar således upp planet $\mathbb{R}^2$ i koncentriska cirklar.

4. Ekvivalensklasserna utgörs av alla personer som är födda samma år.

5.4 Kongruenser

Vi ska nu titta ännu närmare på en speciell typ av ekvivalensrelationer. Dessa är de så kallade *kongruenserna*.

Vi börjar med ett givet positivt heltal n. Vi definierar nu en ekvivalensrelation $\equiv$ på $\mathbb{Z}$ genom $x \equiv y \Leftrightarrow n \mid x - y$. För att specificera att det är heltalet n vi använder skriver vi $x \equiv y \mod n$. Om $x \equiv y \mod n$ kallar vi x och y *kongruenta modulo* n. Vi måste nu visa att detta faktiskt är en ekvivalensrelation.

Reflexivitet: Eftersom $0 = 0 \cdot n$ har vi att $x - x = 0 = 0 \cdot n$ så $n \mid x - x \Leftrightarrow x \equiv x \mod n$ för alla $x \in \mathbb{Z}$.

Symmetri: Om $x \equiv y \mod n$ finns det ett heltal k så att $x - y = kn$. Vi har då att $y - x = -(x - y) = -kn = (-k)n$ så $y \equiv x \mod n$.

Transitivitet: Låt $x \equiv y \mod n$ och $y \equiv z \mod n$. Då finns det heltal k_1, k_2 sådana att $x - y = k_1 n$ och $y - z = k_2 n$. Genom att addera dessa får vi

$$\begin{aligned}(k_1 + k_2)n &= k_1 n + k_2 n \\ &= x - y + y - z \\ &= x - z\end{aligned}$$

så vi ser att $x \equiv z \mod n$.

Eftersom relationen $\equiv$ är reflexiv, symmetrisk och transitiv för alla heltal n är de ekvivalensrelationer allihopa. Som exempel kan nämnas att $20 \equiv 6 \mod 7$, $3 \equiv -2 \mod 5$ och $2044515854 \equiv 0 \mod 2$. De två första exemplen är ganska enkla att kontrollera för

hand men det sista kan verka svårare. Men om vi försöker inser vi något, nämligen $x \equiv 0 \mod n \iff n \mid x$. Att $x \equiv 0 \mod 2$ betyder alltså att talet x är jämnt, vilket vi direkt kan se i det sista exemplet. Från detta kan vi dra slutsatsen att ekvivalensklassen $[0]$ under relationen $\equiv$ utgörs av alla heltal som är delbara med n. Finns det ett liknande sätt att karaktärisera de andra ekvivalensklasserna?

Låt $x, n \in \mathbb{Z}$ vara givna. Vi kan då skriva $x = k_1 n + r_1$ där $0 \leq r < n$. Vi kan då direkt se att $x \equiv r \mod n$ och att om $y \in \mathbb{Z}$ har samma rest vid division med n, d.v.s. $y = k_2 n + r_1$ har vi $x - y = (k_1 - k_2)n$ så $x \equiv y \mod n$. Om däremot $z \in \mathbb{Z}$ har en annan rest vid division med n så att $z = k_3 n + r_2$ där $r_2 \neq r_1$ får vi istället $x - z = (k_1 - k_3)n + r_1 - r_2$ så $x \not\equiv z \mod n$. Vi ser alltså att ekvivalensklassen $[x]$, som oftast skrivs $\overline{x}$ när det handlar om kongruenser, karaktäriseras av vilken rest man får när x divideras med n. Ekvivalensklasserna $\overline{x}$ kallas därför för *restklasser modulo n*. En restklass $\overline{r}$ består alltså av alla heltal på formen $r + kn$ där $0 \leq r < n$. Det finns således n stycken restklasser modulo n, en för varje möjlig rest.

Det är nu naturligt att fråga sig vad som händer med restklasserna när man adderar och multiplicerar ett tal i en viss restklass med ett tal från en annan restklass. Det visar sig att detta kan beskrivas helt och hållet i termer av restklasserna själva.

Sats 5.13. *Låt n vara ett positivt heltal. Då gäller följande.*

1. *Om $x \equiv y \mod n$ och $c \in \mathbb{Z}$ så är $cx \equiv cy \mod n$.*
2. *Om $x_1 \equiv y_1 \mod n$ och $x_2 \equiv y_2 \mod n$ så är $x_1 + x_2 \equiv y_1 + y_2 \mod n$ och $x_1 x_2 \equiv y_1 y_2 \mod n$.*

Bevis.

1. Om $x \equiv y \mod n$ så finns ett $k \in \mathbb{Z}$ så att $x - y = kn$. Då gäller att $cx - cy = c(x-y) = ckn$ så $cx \equiv cy \mod n$.
2. Vi vet att det finns $a, b \in \mathbb{Z}$ sådana att $x_1 - y_1 = an$ och $x_2 - y_2 = bn$. Genom att addera dessa får vi nu

$$\begin{aligned} x_1 - y_1 + x_2 - y_2 &= (x_1 + x_2) - (y_1 + y_2) \\ &= an + bn \\ &= (a + b)n \end{aligned}$$

så vi ser att $x_1 + x_2 \equiv y_1 + y_2 \mod n$. Vi har dessutom att

$$\begin{aligned} x_1 x_2 - y_1 y_2 &= x_1 x_2 - x_1 y_2 + x_1 y_2 - y_1 y_2 \\ &= x_1(x_2 - y_2) + y_2(x_1 - y_1) \\ &= x_1 bn + y_2 an \\ &= (x_1 b + y_2 a)n \end{aligned}$$

och därför får vi att $x_1 x_2 \equiv y_1 y_2 \mod n$.

□

Vi ger nu ett par exempel på hur dessa räkneregler kan användas för att lösa vissa typer av uppgifter.

Exempel 5.14. Vi vill beräkna vilken rest vi får då 2^{461} divideras med 9. För att göra detta kan vi använda oss av att denna rest r uppfyller $2^{461} \equiv r \mod 9$. Vidare observerar vi att $2^6 = 64 = 7 \cdot 9 + 1$ så att $2^6 \equiv 1 \mod 9$. Eftersom $461 = 76 \cdot 6 + 5$ och kan därför skriva

$$\begin{aligned} 2^{461} &= 2^{76 \cdot 6 + 5} \\ &= 2^{76 \cdot 6} \cdot 2^5 \\ &= (2^6)^{76} \cdot 2^5 \\ &\equiv 1^{76} \cdot 2^5 \mod 9 \\ &\equiv 2^5 \mod 9 \\ &\equiv 5 \mod 9 \end{aligned}$$

där den sista kongruensen följer av att $2^5 = 32 = 3 \cdot 9 + 5$.

Exempel 5.15. Vi vill beräkna entalssiffran då talet 3^{85} skrivs i bas 7. Eftersom entalssiffran är precis den rest som uppstår då talet i fråga divideras med basen är målet alltså att bestämma denna rest. Vi använder oss av samma trick som i förra exemplet. Vi har till exempel att $3^3 = 27 = 4 \cdot 7 - 1$ så vi ser att $3^3 \equiv -1 \mod 7$. Vi kan då skriva

$$\begin{aligned} 3^{85} &= 3^{84} \cdot 3 \\ &= (3^3)^{28} \cdot 3 \\ &\equiv (-1)^{28} \cdot 3 \mod 7 \\ &\equiv 3 \mod 7. \end{aligned}$$

Vi ser alltså att entalssiffran är 3.

5.5 Kardinalitet

Vi ska nu titta på hur funktionsbegreppet kan användas för att jämföra mängders ”storlek”, d.v.s. hur många element de har. För att inte ta oss vatten över huvudet börjar vi med de ändliga mängderna.

Vi börjar med att notera att om det finns en injektion från en mängd X till en mängd Y så måste Y ha minst lika många element som X enligt Dirichlets lådprincip. På motsvarande sätt, om det finns en surjektion från X till Y måste X ha minst lika många element som Y. Vi ser därför att bijektioner är ett naturligt matematiskt verktyg för att avgöra om två ändliga mängder är lika stora eller inte. Det ger oss också ett sätt att klart och tydligt definiera vad vi menar med en ändlig mängd.

Definition 5.16. En mängd X kallas *ändlig* om det finns en bijektion från X till mängden $\{0, 1, 2, \ldots, n\}$ för något $n \in \mathbb{N}$.

Definition 5.17. Två mängder X och Y har samma *kardinalitet* om det finns en bijektion $f\colon X \to Y$. Vi betecknar detta med $X =_c Y$. Vi skriver också $X \leq_c Y$ om det finns en delmängd $Z \subseteq Y$ sådan att $X =_c Z$ och $X <_c Y$ om $X \leq_c Y$ och $X \neq_c Y$.

Övning 5.18. Visa att relationen $=_c$ har samma egenskaper som en ekvivalensrelation, d.v.s. den är reflexiv, symmetrisk och transitiv.[5]

Anmärkning 5.19. Här gäller det att vara försiktig eftersom ekvivalensrelationer är definierade på mängder. Kan vi hitta en mängd där vi kan definiera $=_c$ som en ekvivalensrelation? Man skulle vilja definiera relationen på mängden av alla mängder eller, i detta fall, kanske mängden av alla ändliga mängder men man kan visa att dessa inte kan vara mängder. De är "för stora". Man kan komma runt detta problem t.ex. genom att använda sig av så kallad axiomatisk mängdlära till skillnad från vad man kallar naiv mängdlära som vi använder oss av. Vi kommer inte titta närmare på detta problem här.

Sats 5.20. *Låt X och Y vara två mängder. Då gäller att $X \leq_c Y$ om och endast om det finns en injektion $f\colon X \to Y$.*

Bevis. Antag först att $X \leq_c Y$. Då finns det en delmängd $Z \subseteq Y$ och en bijektion $f\colon X \to Z$. Då är f också en injektion från X till Y. Omvänt, antag att det finns en injektion $f\colon X \to Y$. Vi har $f(X) \subseteq Y$ och f är en bijektion från X till $f(X)$ och därför har vi $X \leq_c Y$. □

Övning 5.21. Visa att $Y \leq_c X$ om och endast om det finns en surjektion från X till Y.

Anmärkning 5.22. Man kan visa att om $X \leq_c Y$ och $Y \leq_c X$ så gäller att $X =_c Y$. Detta resultat kallas *Schröder-Bernsteins sats*. Dess bevis är dock för komplicerat för att ges här.

En egenskap som är speciell för ändliga mängder är följande:

Sats 5.23. *Låt X vara en ändlig mängd och $Y \subset X$ en äkta delmängd. Då gäller att $Y <_c X$.*

Bevis. Låt $Y \subset X$ vara en äkta delmängd. Låt f vara en bijektion från X till $\{0, 1, 2, \ldots, n\}$. Då är $f(Y) \subset \{0, 1, 2, \ldots, n\}$ också en äkta delmängd. Enligt Dirichlets lådprincip kan det därför inte finnas en injektion från $\{0, 1, 2, \ldots, n\}$ till $f(Y)$. Antag nu att det finns en bijektion $g\colon X \to Y$. Då är $f|_Y \circ g \circ f^{-1}$ en bijektion mellan $\{0, 1, \ldots, n\}$ och $f(Y)$ men detta är en motsägelse och därför kan det inte finnas någon bijektion mellan X och Y. □

5.6 Oändliga mängder och uppräknelighet

En oändlig mängd är helt enkelt en mängd som inte är ändlig, d.v.s. för vilken det inte finns någon bijektion till $\{0, 1, 2, \ldots, n\}$ för något $n \in \mathbb{N}$. Det är inte lika naturligt för oss att avgöra om två oändliga mängder är lika stora eller inte, däremot fungerar

[5] Tips: Kom ihåg att om f är en bijektion så är också f^{-1} en bijektion.

definitionerna vi gjorde för ändliga mängder lika bra även för oändliga mängder. Vi kommer därför att använda oss av bijektioner för att avgöra om två oändliga mängder är lika stora eller inte.

Med detta kan vi se direkt att Sats 5.20 även gäller för oändliga mängder eftersom dess bevis aldrig använder sig av att mängderna skulle vara ändliga. Samma bevis fungerar alltså utan modifikation även för oändliga mängder. Däremot använder sig beviset för Sats 5.23 av att mängden X är ändlig så vi kan inte därifrån avgöra om satsen gäller eller inte. Faktum är att satsen inte gäller för oändliga mängder, något vi visar med ett motexempel.

Exempel 5.24. Mängden $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$, d.v.s. mängden av alla jämna heltal, är en äkta delmängd av de hela talen. Vi definierar nu en funktion $f\colon \mathbb{Z} \to 2\mathbb{Z}$ genom att sätta $f(n) = 2n$. Då är f en bijektion.

Den enklaste oändliga mängden är kanske de naturliga talen $\mathbb{N}$. Vi använder denna för att göra en definition.

Definition 5.25. En mängd X kallas *uppräknelig* om $X \leq_c \mathbb{N}$. Om X dessutom är oändlig kallas den även för *uppräkneligt oändlig*. En bijektion $f\colon \mathbb{N} \to X$ kallas för en uppräkning av X.[6] Om $\mathbb{N} <_c X$ kallas X för *överuppräknelig*.

Anmärkning 5.26. Uppräkneliga mängder kallas ibland även för *numrerbara* och överuppräkneliga mängder kallas ibland för *onumrerbara*. I samma anda kallas en uppräkning ibland också för en *numrering*.

Sats 5.27. *De hela talen $\mathbb{Z}$ är en uppräknelig mängd.*

Bevis. Vi konstruerar en bijektion f från $\mathbb{N}$ till $\mathbb{Z}$. Vi kan göra detta genom att sätta $f(0) = 0$, $f(1) = 1$, $f(2) = -1$, $f(3) = 2$, $f(4) = -2$, o.s.v. Konkret definierar vi f enligt följande:

$$f(n) = \begin{cases} -k & \text{om } n = 2k \\ k+1 & \text{om } n = 2k+1 \end{cases}.$$

Vi vill nu visa att detta faktiskt är en bijektion.

Injektion: Låt $n_1 \neq n_2$ vara två olika naturliga tal. Om det ena är udda och det andra jämnt kommer $f(n_1)$ och $f(n_2)$ ha olika tecken och därför vara olika. Antag att båda är jämna. Vi kan då skriva $n_1 = 2k_1$ och $n_2 = 2k_2$ där $k_1 \neq k_2$ eftersom $n_1 \neq n_2$. Då har vi $f(n_1) = -k_1 \neq -k_2 = f(n_2)$ så $f(n_1) \neq f(n_2)$. Antag slutligen att båda är udda. Vi kan då skriva $n_1 = 2k_1 + 1$ och $n_2 = 2k_2 + 1$ där $k_1 \neq k_2$ eftersom $n_1 \neq n_2$. Vi har då att $f(n_1) = k_1 + 1 \neq k_2 + 1 = f(n_2)$ så $f(n_1) \neq f(n_2)$. Vi kan därför dra slutsatsen att f är injektiv.

Surjektion: Låt $k \in \mathbb{Z}$. Om $k > 0$ har vi att $2(k-1)+1 > 0$ är ett udda tal och $f(2(k-1)+1) = k - 1 + 1 = k$. Om $k \leq 0$ har vi $-k \geq 0$ och $f(-2k) = k$. Vi drar slutsatsen att f är surjektiv.

[6] Namnet kommer av att man kan använda bijektionen för att införa en ordning på X, nämligen $f(0) < f(1) < f(2) < \ldots$, och därmed räkna upp X på samma vis som man räknar upp $\mathbb{N}$.

Eftersom f är både injektiv och surjektiv är den därför bijektiv och vi har därför att $\mathbb{N} =_c \mathbb{Z}$. □

Anmärkning 5.28. Notera att vi egentligen har visat mer än vad satsen säger. Vi har visat att $\mathbb{Z} =_c \mathbb{N}$ och inte bara $\mathbb{Z} \leq_c \mathbb{N}$.

Övning 5.29. Använd metoden från beviset ovan för att visa att om X och Y är uppräkneliga mängder så är även $X \cup Y$ uppräknelig.[7]

Vi har alltså ännu inget exempel på en överuppräknelig mängd. Vi kan därför försöka med nästa kända talmängd, de rationella talen $\mathbb{Q}$. Det visar sig dock att om man använder sig av en fiffig generalisering av metoden från vårt föregående bevis kan man konstruera en surjektion från $\mathbb{Z}$ till $\mathbb{Q}$.

Sats 5.30. *De rationella talen $\mathbb{Q}$ är en uppräknelig mängd.*

Bevis. Vi börjar med att notera att alla rationella tal kan skrivas som $\frac{p}{q}$ med $p \in \mathbb{Z}$ och $q \in \mathbb{Z}_+$, d.v.s. q är ett positivt heltal. Vi kan alltså skriva varje rationellt tal som ett ordnat par (p, q) av ett heltal och ett positivt heltal. Mängden av alla sådana par är $\mathbb{Z} \times \mathbb{Z}_+$. Om vi kan skapa en bijektion från $\mathbb{Z}$ till $\mathbb{Z} \times \mathbb{Z}_+$ är vi alltså klara. Faktum är att vi då har skapat en surjektion till de rationella talen eftersom till exempel $\frac{3}{2} = \frac{6}{4}$ som rationella tal men $(3, 2) \neq (6, 4)$ som ordnade par.

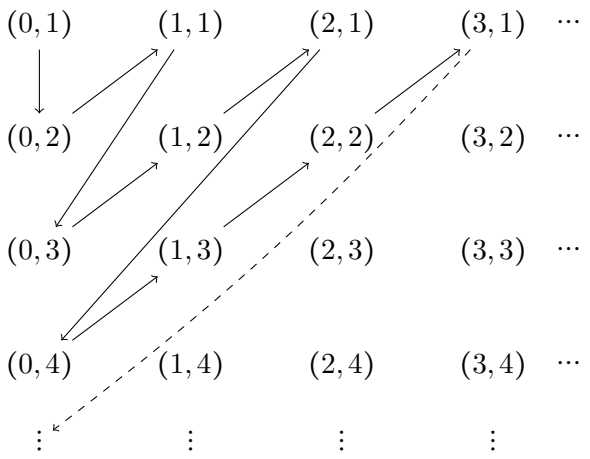
Vi börjar med att titta på de naturliga talen och skapa en bijektion från $\mathbb{N}$ till $\mathbb{N} \times \mathbb{Z}_+$. För att göra detta kommer vi använda oss av den naturliga ordningen på heltalen. Vi tänker oss också att vi ordnar alla ordnade par i $\mathbb{N} \times \mathbb{Z}_+$ enligt följande princip:

Om vi har två par (p_1, q_1) och (p_2, q_2) tittar vi först på $p_1 + q_1$ och $p_2 + q_2$. Om $p_1 + q_1 < p_2 + q_2$ säger vi att $(p_1, q_1) < (p_2, q_2)$. Om vi har $p_1 + q_1 = p_2 + q_2$ tittar vi istället på om $p_1 < p_2$ och säger isåfall att $(p_1, q_1) < (p_2, q_2)$. Ordningen ser alltså ut på följande vis:

$$\underbrace{(0,1)}_{p+q=1} < \underbrace{(0,2)}_{p+q=2} < \underbrace{(1,1)}_{p+q=2} < \underbrace{(0,3)}_{p+q=3} < \underbrace{(1,2)}_{p+q=3} < \underbrace{(2,1)}_{p+q=3} < \underbrace{(0,4)}_{p+q=4} < \underbrace{(1,3)}_{p+q=4} < \underbrace{(2,2)}_{p+q=4} < \underbrace{(3,1)}_{p+q=4} < \dots$$

Vi definierar nu $f\colon \mathbb{N} \to \mathbb{N} \times \mathbb{Z}_+$ så att den bevarar ordningen på de båda mängderna, d.v.s. $f(0) = (0,1)$, $f(1) = (0,2)$, $f(2) = (1,1)$ o.s.v. Då är f en bijektion. Vi kan illustrera detta i en bild:

[7] X och Y är inte nödvändigtvis disjunkta. Det kan därför vara enklare att konstruera en surjektion $f\colon \mathbb{N} \to X \cup Y$ istället för en bijektion.



Figur 6: Ordningen på $\mathbb{N} \times \mathbb{Z}_+$ och konstruktionen av f.

Vi kan sedan utvidga f från de negativa heltalen $\mathbb{Z}_-$ till $\mathbb{Z}_- \times \mathbb{Z}_+$ på ett symmetriskt vis, d.v.s. $f(-1) = (-1, 1)$, $f(-2) = (-1, 2)$, $f(-3) = (-2, 1)$, $f(-4) = (-1, 3)$, o.s.v. Med detta blir f en bijektion från $\mathbb{Z}$ till $\mathbb{Z} \times \mathbb{Z}_+$. Som vi tidigare beskrev kan vi sedan sätta samman f med surjektionen $g\colon \mathbb{Z} \times \mathbb{Z}_+ \to \mathbb{Q}$ som ges av $g((p, q)) = \frac{p}{q}$ och får då en surjektion från $\mathbb{Z}$ till $\mathbb{Q}$. Därför gäller att $\mathbb{Q} \leq_c \mathbb{Z}$. Eftersom vi dessutom har att $\mathbb{Z} =_c \mathbb{N}$ från ovan så vet vi nu att $\mathbb{Q} \leq_c \mathbb{N}$ så $\mathbb{Q}$ är en uppräknelig mängd. □

Övning 5.31. Visa att om X och Y är två uppräkneliga mängder så är även deras Cartesiska produkt $X \times Y$ uppräknelig.

Övning 5.32. Låt X_n vara en uppräknelig mängd för varje $n \in \mathbb{N}$. Visa att även $\bigcup_{n=0}^{\infty} X_n$ är uppräknelig.

5.7 Överuppräkneliga mängder

Vi har fortfarande inte hittat någon överuppräknelig mängd men vi har talmängder kvar att undersöka och det visar sig att nästa mängd, de reella talen $\mathbb{R}$, faktiskt är överuppräknelig.

Sats 5.33. *Mängden av reella tal $\mathbb{R}$ är överuppräknelig.*

Bevis. Vi kommer här att använda oss av ett motsägelsebevis. Vi börjar därför med att anta att $\mathbb{R}$ faktiskt är uppräknelig och att vi har en uppräkning av $\mathbb{R}$. Vi ska nu visa att detta antagande leder till en motsägelse.

Vi börjar med att påminna oss om att varje reellt tal kan skrivas i sin decimalutveckling som $a, a_1a_2a_3\ldots$ där $a \in \mathbb{Z}$ och varje a_n är någon av siffrorna 0 till och med 9. Med en uppräkning kan vi dessutom räkna upp alla reella tal x_n på följande vis:

$$
\begin{aligned}
x_0 &= a_0, a_{01}a_{02}a_{03}\dots \\
x_1 &= a_1, a_{11}a_{12}a_{13}\dots \\
x_2 &= a_2, a_{21}a_{22}a_{23}\dots \\
&\vdots
\end{aligned}
$$

Vi ska nu konstruera ett reellt tal $y = 0, y_1y_2y_3\dots$ som omöjligt kan vara med i den här uppräkningen, vilket ger oss vår sökta motsägelse. Vi konstruerar detta tal genom att välja varje decimal y_n på följande vis:

$$
y_n = \begin{cases} 1 & \text{om } a_{nn} = 0 \\ 0 & \text{om } a_{nn} \neq 1 \end{cases}.
$$

Detta gör att y omöjligt kan vara något av talen $x_1, x_2, x_3, \dots$ eftersom det skiljer sig från x_n i den n:te decimalen för varje n. Vi har alltså hittat ett tal som inte är med i uppräkningen men detta motsäger att det faktiskt var en uppräkning. Denna motsägelse bevisar att det inte kan finnas någon uppräkning av de reella talen och därför måste denna mängd vara överuppräknelig. □

Anmärkning 5.34. Metoden som används i detta bevis kallas *Cantors diagonalmetod* efter matematikern Georg Cantor som år 1891 använde metoden för att bevisa existensen av överuppräkneliga mängder.

Anmärkning 5.35. Vi har här visat att $\mathbb{N} <_c \mathbb{R}$. Man kan då fråga sig om det finns en mängd mellan $\mathbb{N}$ och $\mathbb{R}$, d.v.s. en mängd X med egenskapen att $\mathbb{N} <_c X <_c \mathbb{R}$. Utsagan att det inte finns någon sådan mängd X kallas för *kontinuum hypotesen* och har en lång och fortfarande pågående historia inom matematiken. Matematikern Paul Cohen visade 1963 att kontinuum hypotesen är oberoende av de axiom som vanligtvis används som grund för mängdläran, de så kallade ZFC axiomen. Detta betyder att man varken kan bevisa eller motbevisa kontinuum hypotesen inom ramen för ZFC axiomen. Sedan dess har man försökt att lösa denna fråga på andra sätt, till exempel genom att utöka ZFC axiomen med ytterligare axiom som gör att man kan avgöra om kontinuum hypotesen är sann eller inte. Detta pågår än idag.

Övning 5.36. Låt X vara mängden av alla oändliga talföljder av nollor och ettor, d.v.s. alla följder $a_0, a_1, a_2, a_3, \dots$ där varje a_n är antingen 0 eller 1. Visa att X är en överuppräknelig mängd genom att använda Cantors diagonalmetod.

Från föregående sats följer också att de komplexa talen $\mathbb{C}$ är överuppräkneliga, eftersom $\mathbb{R} \subset \mathbb{C}$ och därmed $\mathbb{R} \leq_c \mathbb{C}$.

6 Polynom

Ett *polynom av grad n* är ett objekt f som består av ett ändligt antal givna komplexa tal $a_0, a_1, \dots, a_n$ med $a_n \neq 0$ som kallas *koefficienter* och en *variabel* x som tillsammans

har formen

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Två polynom f och g anses vara lika om de har samma grad och om alla deras koefficienter är lika. Polynomen av grad 0, som ges av $f(x) = a_0$, kallas *konstanta* och polynomet $f(x) = 0$ kallas *nollpolynomet*. Graden av ett polynom f anges av $\deg f$.

Anmärkning 6.1. Vi skiljer på ett polynom f och den motsvarande *polynomfunktionen* som fås då vi låter variabeln x anta värden i till exempel $\mathbb{R}$ eller $\mathbb{C}$. Man kan också tänka sig att man låter variabeln anta andra objekt än tal, till exempel kan man låta x vara en matris.

Vi kan addera och multiplicera polynom med varandra och få nya polynom. Om $f(x) = a_0 + a_1 x + \ldots a_n x^n$ och $g(x) = b_0 + b_1 x + \ldots b_m x^m$ är polynom av grad n och m respektive så definierar vi polynomet $f + g$ som det polynom vars koefficienter är $a_k + b_k$ där $a_k = 0$ för $k > n$ och $b_k = 0$ för $k > m$. På samma sätt är polynomet fg det polynom vars koefficienter c_k ges genom att utföra multiplikationen $f(x)g(x)$ och samla ihop termerna efter deras grad. Vi får då att $(fg)(x) = c_0 + c_1 x + \ldots c_{m+n} x^{m+n}$ där $c_k = \sum_{j=0}^{k} a_{k-j} b_k$. Vi har även följande sats.

Sats 6.2. *Om varken f eller g är nollpolynomet gäller att* $\deg(fg) = \deg f + \deg g$.

Bevis. Låt $\deg f = n$ och $\deg g = m$. Då vet vi att $a_n \neq 0$ och $b_m \neq 0$. Det följer då att $c_{m+n} = a_n b_m \neq 0$ och $c_k = 0$ för $k > m + n$. Alltså har vi $\deg(fg) = m + n$. □

Vårat sista mål kommer nu vara att studera ekvationen $f(x) = 0$ där f är ett polynom. En sådan ekvation kallas för en *algebraisk ekvation* eller en *polynomekvation*. En rot till den algebraiska ekvationen $f(x) = 0$ är ett tal α sådant att $f(\alpha) = 0$. Ett sådant α kallas också för ett *nollställe* till polynomet f. Vi skiljer på ekvationen som har rötter och polynomet som har nollställen.

Vi har redan sett två exempel på gemensamma egenskaper för polynom och heltal, nämligen att de kan adderas och multipliceras. Vi ska nu titta på några andra egenskaper som polynomen delar med heltalen. Vi kommer inte att utforska fullständigt hur långt dessa likheter sträcker sig och vilka skillnader som finns eftersom detta skulle ta alldeles för lång tid. Intresserade uppmuntras istället att läsa mer om abstrakt algebra, där både heltalen och polynomen kan ses som exempel på något som kallas för *ring*.

Definition 6.3. Låt f och g vara polynom. Vi säger att g *delar* f om det finns ett polynom h sådant att $f = gh$. Vi skriver då $g \mid f$.

Exempel 6.4.

1. $(2x - 1) \mid (4x^2 - 1)$ eftersom $4x^2 - 1 = (2x - 1)(2x + 1)$.
2. Låt f vara ett polynom. För alla tal $\lambda \neq 0$ gäller då att $\lambda \mid f$ eftersom $f = \lambda \frac{1}{\lambda} f$.

Precis som för heltalen har vi följande motsvarande regler för polynom.

Sats 6.5. *Låt f, g, h, φ, ψ vara polynom som uppfyller att $f \mid g$ och $f \mid h$. Då gäller att $f \mid (\varphi g + \psi h)$.*

Beviset är helt och hållet analogt med beviset för motsvarande sats för heltal, allt som behöver göras är att byta ut alla heltal mot polynom.

Precis som för heltal har alla polynom alltid vissa delare som man kallar *triviala*. Som vi såg i ett exempel så delar varje nollskild konstant alla polynom. Det gäller även att varje polynom f delas av λf där λ är en nollskild konstant. Det är dessa delare som vi nu kallar *triviala*. Vidare säger vi att om $g = \lambda f$ för någon nollskild konstant λ så är polynomen f och g *associerade*. Vi kallar då också en delare som inte är trivial för en *äkta* delare. Från sats 6.2 kan vi se att en äkta delare g till f alltid måste uppfylla att $0 < \deg g < \deg f$. Vi kallar ett polynom av grad minst 1 utan äkta delare *irreducibelt*. Det följer direkt att alla polynom av grad 1 är irreducibla eftersom en äkta delare skulle ha grad 0 men alla dessa är triviala. Ett polynom som inte är irreducibelt kallas helt enkelt för *reducibelt*.

Vi kan också tänka oss att vi begränsar oss till polynom vars koefficienter endast är reella tal, rationella tal eller heltal. Vi namnger sådana polynom efter vad de har för koefficienter, till exempel *reella polynom*. Man pratar då också om reella polynom som är *irreducibla över* $\mathbb{R}$. Till exempel kan man visa att polynomet $x^2 + 1$ är irreducibelt över $\mathbb{R}$ men inte över $\mathbb{C}$.

Följande satser för tankarna till lemma 3.16 och aritmetikens fundamentalsats.

Sats 6.6. *Om f är reducibelt så är alla äkta delare till f av lägst grad irreducibla.*

Sats 6.7. *Varje polynom av grad minst 1 kan skrivas som en produkt av irreducibla polynom.*

Även bevisen är väldigt lika deras heltalsmotsvarigheter. Vi bevisar sats 6.6 för att visa hur små skillnaderna är.

Bevis. Eftersom f är reducibelt måste det ha äkta delare och därför också en äkta delare av lägst grad. Kalla denna äkta delare av lägst grad g.[8] Antag nu att g också är reducibelt. Då kan vi skriva $g = ab$ för några polynom a, b av lägra grad än $\deg g$. Eftersom $f = cg$ får vi då $f = cab$ så att även a och b är äkta delare till f. Alltså är a och b äkta delare till f av lägre grad än g, som var en äkta delare av lägsta grad. Denna motsägelse visar att g måste vara irreducibelt. □

6.1 Nollställen och faktorer

Vi ska nu titta närmare på kopplingen mellan ett polynoms nollställen och dess delare.

Antag att polynomet $x - \alpha$ delar polynomet f så att vi kan skriva $f(x) = (x - \alpha)g(x)$. Då måste $x = \alpha$ vara ett nollställe till polynomet f eftersom $f(\alpha) = 0 \cdot g(\alpha = 0)$. Antag

[8] Denna delare är inte unik i den mening att även λg är en äkta delare av samma grad för $\lambda \neq 0$.

nu istället att $x = \alpha$ är ett nollställe till f. Vi kan alltid skriva $f(x) = (x - \alpha)g(x) + c$ för något polynom g och någon konstant c. Om vi stoppar in $x = \alpha$ får vi då

$$0 = f(\alpha) = 0 \cdot g(\alpha) + c = c$$

så vi ser att då måste $c = 0$ och därför är f delbart med $x - \alpha$. Vi sammanfattar vad vi precis har bevisat i en sats som kallas *faktorsatsen*.

Sats 6.8 (Faktorsatsen)**.** *Polynomet $x - \alpha$ är en delare i polynomet f om och endast om α är ett nollställe till f.*

Anmärkning 6.9. Vårat bevis visar också att även om α inte är ett nollställe till f så kan vi ändå skriva $f(x) = (x - \alpha)g(x) + f(\alpha)$.

Faktorsatsen säger alltså att problemet att hitta förstagradsfaktorer till ett polynom är ekvivalent med att hitta nollställen till polynomet. *Algebrans fundamentalsats* säger oss att sådana nollställen alltid existerar.

Sats 6.10 (Algebrans fundamentalsats)**.** *Varje polynom av grad minst* 1 *har minst ett komplext nollställe.*

Algebrans fundamentalsats är speciell i det avseendet att den ännu inte har något helt algebraiskt bevis. Alla kända bevis använder sig istället av andra metoder, så som till exempel teorin om analytiska funktioner, differentialtopologi, algebraisk topologi, Riemannytor, Riemanngeometri, m.m. De mest algebraiska bevisen använder sig av några grundläggande satser från envariabelanalys, till exempel satsen om mellanliggande värden.

Om vi kombinerar faktorsatsen och algebrans fundamentalsats får vi följande sats.

Sats 6.11. *Varje polynom $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ av grad n kan skrivas som en produkt av förstagradspolynom $f(x) = a_n(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$ där $\alpha_1, \alpha_2, \dots, \alpha_n$ är komplexa tal.*

Vi kan tyvärr inte säga något om denna faktorisering är entydig eller inte än. Vi återkommer till detta problem senare när vi har studerat polynomdivision närmare. Observera att en viss faktor kan dyka upp flera gånger, till exempel kan vi ha att $\alpha_1 = \alpha_2$. Till exempel händer detta för polynomet $x^2 + 2x + 1 = (x + 1)(x + 1)$ där $\alpha_1 = \alpha_2 = -1$. Antalet gånger som en viss faktor dyker upp i faktoriseringen av ett polynom kallas för nollställets *multiplicitet*.

6.2 Divisionsalgoritmen och Euklides algoritm

Vi har tidigare definierat vad delbarhet betyder för polynom. Precis som för heltal ska vi nu se att det finns en algoritm för att utföra en sådan division och att den kan användas för att hitta den största gemensamma delaren av två polynom med hjälp av Euklides algoritm.

Vi börjar med att beskriva hur en polynomdivision går till. För att göra detta går vi igenom ett exempel där vi vill dela polynomet $f(x) = 2x^3 - x^2 - 3x + 5$ med polynomet

$g(x) = x^2 - 2$. Precis som vi för heltal började med att multiplicera divisorn med en så hög tiopotens som möjligt utan att den blir större än dividenden och sedan dra bort så många multipler av detta från dividenden utan att resultatet blir negativ ska vi nu ska vi nu multiplicera divisorn g med en så hög potens av x som möjligt utan att resultatet har högre grad än f och sedan dra bort en multipel av detta från dividenden f för att få bort $2x^3$-termen i $f(x)$. Vi ställer upp det som följer:

$$\begin{array}{rl} & 2x \\ \hline 2x^3 - x^2 - 3x + 5 & \big| \; x^2 - 2 \\ -(2x^3 - 4x) & \\ \hline -x^2 + x + 5 & \end{array}$$

Vi ser här att $f(x) - 2xg(x) = 3x^2 - 3x + 5$. Eftersom graden av differensen är minst lika stor som graden av divisorn kan vi fortsätta.

$$\begin{array}{rl} & 2x - 1 \\ \hline 2x^3 - x^2 - 3x + 5 & \big| \; x^2 - 2 \\ -(2x^3 - 4x) & \\ \hline -x^2 + x + 5 & \\ -(-x^2 + 2) & \\ \hline x + 3 & \end{array}$$

Vi kan nu se att $f(x) - (2x-1)g(x) = x + 3$. Nu har differensen lägre grad än divisorn så vi kan inte fortsätta. Svaret blir alltså att $f(x) = (2x - 1)g(x) + x + 3$ där $2x - 1$ är kvoten och $x + 3$ är resten. Likt hur det är för heltal gäller att man för alla polynom f, g kan skriva $f = qg + r$ där q, r är polynom och $\deg r < \deg g$. Att $r(x) = 0$ är detsamma som att $g \mid f$.

Två polynom f, g har alltid gemensamma delare, till exempel är varje nollskild konstant en gemensam delare likt hur ± 1 är gemensamma delare till varje par av heltal. Vi kan därför också titta på två polynoms största gemensamma delare. Det uppkommer lite tvetydigheter här eftersom om vi har en gemensam delare så är alla dess associerade polynom också gemensamma delare. Detta kan dock användas till vår fördel i vissa lägen. För att vara mer precisa gör vi följande definition.

Definition 6.12. En *största gemensam delare* till två polynom f, g är ett polynom h sådant att varje gemensam delare till f och g också delar h.

Vi tänker oss nu att vi vill hitta $\mathrm{SGD}(f, g)$ där f och g är två polynom där $\deg g \leq \deg f$. Vi börjar då med att utföra en divison av f med g och får då $f = q_1 g + r_1$ där $\deg r_1 < \deg g$. Precis som för heltalen så måste då varje gemensam delare till f och g också vara en delare till r_1 och varje gemensam delare till g och r_1 måste också vara en delare till f. Vi kan då reducera problemet till att hitta $\mathrm{SGD}(g, r_1)$. Vi skriver då $g = q_2 r_1 + r_2$ där $\deg r_2 < \deg r_1$. På detta vis kan vi sedan fortsätta tills vi får en rest av

grad 0. Om denna rest är nollpolynomet är den föregående resten en största gemensam delare till f och g. Om denna sista rest inte är nollpolynomet utan en nollskild konstant λ säger vi att polynomen f och g är *relativt prima* och skriver $\mathrm{SGD}(f,g) = 1$.

Exempel 6.13. Vi vill bestämma $\mathrm{SGD}(f,g)$ där $f(x) = 2x^4 + 8x^3 - 16x + 6$ och $g(x) = x^4+2x^3+x^2+4x-2$. Vi ser att $f(x) = 2(x^4+4x^3-8x+3)$ så vi kan lika gärna arbeta med det associerade polynomet x^4+4x^3-8x+3. Vi kan se att $x^4+4x^3-8x+3 = g(x)+2x^3-x^2-12x+5$ så att $r_1(x) = 2x^3 - x^2 - 12x + 5$. Vi ska nu dela polynomet g med r_1. För att göra det lite enklare för oss använder vi $2g$ istället.

$$
\begin{array}{r|l}
 & x + \frac{5}{2} \\
\hline
2x^4 + 4x^3 + 2x^2 + 8x - 4 & 2x^3 - x^2 - 12x + 5 \\
-(2x^4 - x^3 - 12x^2 + 5x) & \\
\hline
5x^3 + 14x^2 + 3x - 4 & \\
-\left(5x^3 - \frac{5}{2}x^2 - 30x + \frac{25}{2}\right) & \\
\hline
\frac{33}{2}x^2 + 33x - \frac{33}{2} &
\end{array}
$$

Vi ser att vi får $q_1(x) = \left(x + \frac{5}{2}\right)$ och $r_2(x) = \frac{33}{2}x^2 + 33x - \frac{33}{2}$. För att göra beräkningarna enklare väljer vi istället det associerade polynomet $x^2 + 2x - 1$ och fortsätter Euklides algoritm med detta polynom.

$$
\begin{array}{r|l}
 & 2x - 5 \\
\hline
2x^3 - x^2 - 12x + 5 & x^2 + 2x - 1 \\
-(2x^3 + 4x^2 - 2x) & \\
\hline
-5x^2 - 10x + 5 & \\
-(-5x^2 - 10x + 5) & \\
\hline
0 &
\end{array}
$$

Den här divisionen gick jämnt ut. Alltså är $x^2 + 2x - 1$ en största gemensam delare till f och g.

Vi ska nu åter titta på sats 6.11. Innan vi kan bevisa att faktoriseringen som ges är unik om man bortser från faktorernas ordning behöver vi ett par lemman som motsvarar de lemman som behövdes för att bevisa aritmetikens fundamentalsats.

Lemma 6.14. *För alla polynom f, g finns det polynom p, q sådana att* $\mathrm{SGD}(f,g) = pf + qg$.

Bevis. Precis som för heltal kan vi göra Euklides algoritm baklänges för att hitta polynomen p och q. För enkelhetens skull, antag att vi har genomfört Euklides algoritm och fått $f = q_1 g + r_1$ och $g = q_2 r_1 + r_2$ med r_2 som sista rest som inte är nollpolynomet. Alltså

kan vi sätta $\mathrm{SGD}(f,g) = r_2$. Vi har också att

$$\begin{aligned} r_2 &= g - q_2 r_1 \\ &= g - q_2(f - q_1 g) \\ &= -q_2 f + (q_1 q_2 + 1)g \end{aligned}$$

och ser därför att vi i detta fall kan välja $p = -q_2$ och $q = (q_1 q_2 + 1)$. På samma sätt kan man få fram p och q oavsett hur många steg vi har i Euklides algoritm. □

Lemma 6.15. *Låt f, g vara polynom och låt h vara ett irreducibelt polynom sådant att $h \mid fg$. Då gäller att $h \mid f$ eller $h \mid g$.*

Bevis. Om $h \mid f$ är vi redan färdiga så antag att $h \nmid f$. Eftersom h är irreducibelt måste vi ha att $\mathrm{SGD}(h, f) = 1$ och från föregående lemma vet vi då att vi kan hitta polynom p, q sådana att $1 = ph + qf$. Vi får då att

$$\begin{aligned} g &= g(ph + qf) \\ &= pgh + qfg. \end{aligned}$$

Eftersom $h \mid fg$ ser vi att h delar både pgh och qfg. Alltså måste h dela deras summa, som ju är g. □

Anmärkning 6.16. Jämför dessa bevis med bevisen för motsvarande satser för heltal för att se likheterna.

Det föregående lemmat kan lätt generaliseras till följande lemma, på precis samma sätt som motsvarande lemma för heltal.

Lemma 6.17. *Låt $f_1, f_2, \ldots, f_n$ vara polynom och låt h vara ett irreducibelt polynom sådana att $h \mid f_1 f_2 \ldots f_n$. Då gäller att $h \mid f_k$ för något k.*

Vi är nu redo att bevisa att faktoriseringen som ges av sats 6.11 är unik upp till ordningen av faktorerna.

Bevis. Antag att vi har två faktoriseringar $f(x) = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) = b_m(x - \beta_1)(x - \beta_2)\ldots(x - \beta_m)$. Vi kan direkt se att $n = m$ eftersom de två uttrycken annars skulle ha olika grad och därför omöjligt kunna vara samma polynom. Vi kan också se att $a_n = b_m$ eftersom de annars skulle ha olika koefficienter framför x^n-termen.

Eftersom $(x - \alpha_1) \mid f(x)$ vet vi att $(x - \alpha_1) \mid (x - \beta_1)(x - \beta_2)\ldots(x - \beta_n)$ och därför att $(x - \alpha_1) \mid (x - \beta_k)$ för något k. Eftersom vi inte är intresserade av ordningen kan vi utan inskränkning anta att $k = 1$. Då måste polynomen $x - \alpha_1$ och $x - \beta_1$ vara associerade men eftersom båda polynomens koefficient framför x-termen är 1 måste de dessutom vara samma polynom, d.v.s. $\alpha_1 = \beta_1$. Vi kan nu betrakta $(x - \alpha_2)\ldots(x - \alpha_n) = (x - \beta_2)\ldots(x - \beta_n)$ och genomföra samma resonemang för att visa att $\alpha_2 = \beta_2$. Fortsätter vi hela vägen ser vi att $\alpha_k = \beta_k$ för alla k. □

6.3 Reella polynom

Vi ska nu ägna lite tid åt reella polynom, alltså polynom där alla koefficienter är reella. Ett exempel på ett reellt polynom är $f(x) = x^2 + 1$. Vi kan lätt se att detta polynom inte har några reella nollställen eftersom $x^2 \geq 0$ för alla $x \in \mathbb{R}$ och därför får vi $f(x) = x^2 + 1 \geq 1$ för alla $x \in \mathbb{R}$. Motsäger detta algebrans fundamentalsats? Nej, eftersom algebrans fundamentalsats tillåter komplexa nollställen och mycket riktigt kan vi se att $f(i) = i^2 + 1 = -1 + 1 = 0$. Vi kan också se att $f(-i) = (-i)^2 + 1 = i^2 + 1 = 0$. Det komplexa talet $-i$ är det komplexa konjugatet av i. För ett allmänt komplext tal $z = \alpha + i\beta$ definieras dess konjugat som det komplexa talet $\overline{z} = \alpha - i\beta$. Det är ingen slump att det komplexa nollstället i dyker upp tillsammans med dess konjugat $-i$, vilket vi nu ska bevisa. Vi kommer behöva använda oss av följande egenskaper:

- $\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}$,
- $\overline{z_1} \cdot \overline{z_2} = \overline{z_1 \cdot z_2}$,
- $\overline{z} = z \iff z \in \mathbb{R}$.

Sats 6.18. *Låt f vara ett reellt polynom. Om det har ett komplext nollställe $z = \alpha + i\beta$ så är även $\overline{z} = \alpha - i\beta$ ett nollställe.*

Bevis. Låt z vara ett nollställe för f, d.v.s. $f(z) = 0$ och låt $f(x) = a_0 + a_1 x + \dots a_n x^n$. Vi har då följande:

$$\begin{aligned} f(\overline{z}) &= a_0 + a_1\overline{z} + \dots a_n\overline{z}^n \\ &= a_0 + a_1\overline{z} + \dots a_n\overline{z^n} \\ &= \overline{a_0} + \overline{a_1 z} + \cdots + \overline{a_n z^n} \\ &= \overline{a_0 + a_1 z + \cdots + a_n z^n} \\ &= \overline{f(z)} \\ &= \overline{0} \\ &= 0. \end{aligned}$$

Alltså är även $\overline{z}$ ett nollställe till f. □

Man brukar säga att komplexa nollställen till reella polynom kommer i konjugerade par.

Anmärkning 6.19. Observera att vi har använt oss av att $\overline{a_k} = a_k$ för varje k eftersom polynomet f är reellt och därför är alla koefficienter reella. Om polynomet inte är reellt fungerar inte detta steg och faktum är att komplexa nollställen för ickereella polynom inte behöver komma i konjugerade par.

Om vi använder oss av faktorsatsen ser vi då att ett reellt polynom f med ett komplext nollställe z måste vara delbart med $(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}$. Detta är

i sin tur ett reellt polynom eftersom om vi skriver $z = \alpha + i\beta$ där $\alpha, \beta \in \mathbb{R}$ ser vi att

$$\begin{aligned} z + \overline{z} &= \alpha + i\beta + \alpha - i\beta \\ &= 2\alpha, \\ z\overline{z} &= (\alpha + i\beta)(\alpha - i\beta) \\ &= \alpha^2 - (i\beta)^2 \\ &= \alpha^2 + \beta^2. \end{aligned}$$

Vi kan också se att nollställena z och $\overline{z}$ måste ha samma multiplicitet. Som följd av detta vet vi att det alla polynom av grad minst 3 är reellt reducibla, d.v.s. vi kan faktorisera det i termer av reella polynom av grad högst 2. Vi har alltså följande sats.

Sats 6.20. *Varje reellt polynom kan skrivas som en produkt av reellt irreducibla reella polynom av grad högst 2. Faktoriseringen är unik upp till ordning på faktorerna och associationer.*

6.4 Lösningsmetoder för algebraiska ekvationer

Vi har hittills gått igenom en massa teori om polynom och algebraiska ekvationer. Det är nu dags att sätta denna teori till arbete och hitta några användsbara metoder för att lösa algebraiska ekvationer.

Till att börja med har vi den välkända $p-q$-formeln, som kan användas för att enkelt och direkt hitta alla nollställen till ett andragradspolynom, nämligen

$$x^2 + px + q = 0 \;\Leftrightarrow\; x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}\,.$$

För polynom av grad 3 och 4 finns liknande formler som är mer komplicerade och vi kommer därför inte att gå igenom dem. För polynom av grad 5 och högre är det bevisat att det inte finns några sådana formler. När vi löser en algebraisk ekvation kommer vårat mål alltså vara att försöka hitta tillräckligt många nollställen så att vi kan faktorisera ner polynomet till grad 2 och då använda exempelvis $p-q$-formeln för att avsluta lösningen.

Vi har redan sett att ett reellt polynom med ett komplext nollställe z också har $\overline{z}$ som nollställe. Om vi försöker lösa en reell algebraisk ekvation och lyckas hitta en komplex lösning får vi då också en till lösning på köpet. Detta kanske låter oss förenkla problemet till något vi kan lösa direkt.

Exempel 6.21. Betrakta polynomet $f(x) = x^4 + 2x^2 - 8$. Vi har givits informationen att $x = 2i$ är ett nollställe. Eftersom polynomet är reellt och $x = 2i$ är ett ickereellt nollställe vet vi därför att även $x = -2i$ måste vara ett nollställe. Alltså kan f delas med $(x - 2i)(x + 2i) = x^2 + 4$. Utför vi divisionen ser vi att det återstår $x^2 - 2$. Eftersom detta har grad två kan vi hitta dess nollställen direkt med $p - q$-formeln, eller i detta fall med konjugatregeln, och vi får då nollställena $x = \pm\sqrt{2}$. Därför kan vi skriva $f(x) = (x - 2i)(x + 2i)(x - \sqrt{2})(x + \sqrt{2})$.

Exempel 6.22. Vi betraktar ännu en gång polynomet $f(x) = x^4 + 2x^2 - 8$. Vi vet redan vad alla nollställena är men vi ska nu visa att denna ekvation kan lösas även utan några ledtrådar. För att göra detta utnyttjar vi att alla potenser av x är jämna. Om vi då gör variabelbytet $y = x^2$ kan vi skriva $f(x) = x^4 + 2x^2 - 8 = y^2 + 2y - 8 = g(y)$. Eftersom g är ett polynom av grad 2 kan vi hitta dess nollställen direkt med $p-q$-formeln. Vi får då

$$y^2 + 2y - 8 = 0 \;\Leftrightarrow\; x = -1 \pm \sqrt{1+8} = -1 \pm 3.$$

Nu gäller det att komma ihåg att $y = x^2$, så lösningen $y = -4$ ger oss nollställen $x = \pm 2i$ till f och nollstället $y = 2$ ger oss nollställen $x = \pm\sqrt{2}$.

Exempel 6.23. Betrakta nu istället polynomet $f(x) = x^4 - x^3 - 2x - 4$. Vi har givits informationen att detta polynom har ett rent imaginärt nollställe. Ett imaginärt nollställe måste ha formen $x = ib$ där $b \in \mathbb{R}$. Med insättning får vi då ekvationen

$$\begin{aligned} 0 &= f(ib) \\ &= b^4 + ib^3 - 2ib - 4 \end{aligned}$$

Om $b^4 + ib^3 - 2ib + 4 = 0$ måste både realdelen och imaginärdelen vara 0. Vi kan alltså dela upp denna ekvation i två ekvationer:

$$\begin{cases} b^4 - 4 &= 0 \\ b^3 - 2b &= 0 \end{cases}$$

Vi börjar med ekvationen $b^3 - 2b = 0$. Vi skriver $0 = b^3 - 2b = b(b^2 - 2)$ och ser då att $b = 0$ eller $b^2 - 2 = 0$. Ekvationen $b^2 - 2$ har lösningarna $b = \pm\sqrt{2}$. Genom insättning i ekvationen $b^4 - 4 = 0$ ser vi då att $b = 0$ är en falsk lösning men att då båda andra lösningarna stämmer. Observera att vi här direkt har hittat det konjugerade par som vi förväntade oss av det imaginära nollstället eftersom polynomet f är reellt.

Genom att dela f med polynomet $(x - i\sqrt{2})(x + i\sqrt{2}) = (x^2 + 2)$ får vi kvoten $x^2 - x - 2$ vars nollställen vi direkt bestämmer till $x = 2$ och $x = -1$ med $p-q$-formeln.

Precis som ickereella nollställen till reella polynom alltid kommer i konjugerade par så kommer även irrationella nollställen till rationella polynom i konjugerade par. Detta beskrivs av följande sats.

Sats 6.24. *Låt f vara ett rationellt polynom med ett nollställe $x_1 = \alpha + \sqrt{\beta}$ där $\alpha, \beta \in \mathbb{Q}$ och $\sqrt{\beta}$ är irrationellt. Då är även $x_2 = \alpha - \sqrt{\beta}$ ett nollställe till f.*

Beviset för denna sats är likt motsvarande sats för ickereella nollställen till reella polynom. Likheten mellan båda dessa satser tyder på att något djupare ligger till grund för detta fenomen. Det visar sig att båda dessa satser är specialfall av en mer allmän sats som tas upp i högre kurser i algebra.

Om ett polynom har ett nollställe av multiplicitet minst 2 kan man komma åt det med hjälp av följande sats.

Sats 6.25. *Låt polynomet f ha ett nollställe $x = \alpha$ av multiplicitet $m \geq 2$. Då är $x = \alpha$ ett nollställe till polynomet f' av multiplicitet $m - 1$. Vidare, om $x = \alpha$ är ett enkelt nollställe till f så är det inte ett nollställe till f'.*

Bevis. Enligt faktorsatsen kan vi skriva $f(x) = (x-\alpha)^m g(x)$ för något polynom g sådant att $g(\alpha) \neq 0$. Enligt produktregeln för derivator får vi då

$$\begin{aligned} f'(x) &= m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x) \\ &= (x-\alpha)^{m-1}(mg(x) + (x-\alpha)g'(x)) \\ &= (x-\alpha)^{m-1} h(x) \end{aligned}$$

där $h(x) = mg(x)+(x-\alpha)g'(x)$. Vidare gäller att $h(\alpha) = mg(\alpha)+(\alpha-\alpha)g'(x) = mg(\alpha) \neq 0$. Detta bevisar båda satsens påståenden. □

Vi ger ett exempel på hur detta kan användas.

Exempel 6.26. Vi har fått tipset att polynomet $f(x) = x^4-3x^3+x^2+4$ har ett nollställe av multiplicitet 2 och vi vill hitta samtliga nollställen. Vi deriverar därför polynomet och får $f'(x) = 4x^3 - 9x^2 + 2x$. Vi vill nu hitta en SGD för f och f' eftersom vi vet att de har en gemensam delare som motsvarar deras gemensamma nollställe. Vi kan direkt se att f' har ett nollställe $x = 0$ som inte f har och vi kan därför faktorisera bort det nollstället innan vi påbörjar Euklides algoritm. Vi kan också göra det lite enklare för oss och använda $4f$ istället så att vi minimerar de rationella tal som behövs.

$$\begin{array}{r|l} & x^2 - \frac{3}{4}x - \frac{19}{16} \\ \hline 4x^4 - 12x^3 + 4x^2 + 16 & 4x^2 - 9x + 2 \\ -(4x^4 - 9x^3 + 2x^2) & \\ \hline -3x^3 + 2x^2 + 16 & \\ -\left(-3x^3 + \frac{27}{4}x^2 - \frac{3}{2}x\right) & \\ \hline -\frac{19}{4}x^2 + \frac{3}{2}x + 16 & \\ -\left(-\frac{19}{4}x^2 + \frac{171}{16}x - \frac{19}{8}\right) & \\ \hline -\frac{147}{16}x + \frac{147}{8} & \end{array}$$

Vi ser att $r_1(x) = -\frac{147}{16}x + \frac{147}{8}$. Detta har grad 1 och är därför den siste icketriviala resten eftersom vi vet att f och f' har en gemensam faktor och därför är det också en största gemensam delare. Vi väljer därför det associerade polynomet $x - 2$. Det måste dessutom vara det dubbla nollstället. Vi vet alltså att f kan delas med $(x-2)^2$. Mycket riktigt, utför vi divisionen ser vi att $f(x) = (x-2)^2(x^2+x+1)$. Med $p-q$-formeln ser vi att polynomet $x^2 + x + 1$ har nollställen $x = -\frac{1}{2} \pm \sqrt{\frac{1}{4} - 1} = -\frac{1}{2} \pm \sqrt{-\frac{3}{4}} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$.

På detta vis kan vi alltså leta efter dubbla nollställen. Med hjälp av följande sats kan vi även leta efter rationella nollställen i vissa fall.

Sats 6.27. *Låt* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *där* $a_k \in \mathbb{Z}$ *för varje* k*. Antag att* f *har ett rationellt nollställe* $x = \frac{p}{q}$ *där* $\mathrm{SGD}(p,q) = 1$*. Då gäller att* $p \mid a_0$ *och* $q \mid a_n$*. Om* $a_n = 1$ *måste eventuella rationella nollställen vara heltal.*

Bevis. Eftersom vi antar att $f\left(\frac{p}{q}\right) = 0$ kan vi skriva följande:

$$\begin{aligned} 0 &= q^n f\left(\frac{p}{q}\right) \\ &= q^n\left(a_0 + a_1\frac{p}{q} + \cdots + a_n\frac{p^n}{q^n}\right) \\ &= a_0q^n + a_1pq^{n-1} + \cdots + a_np^n \\ &= a_0q^n + p\left(a_1q^{n-1} + \cdots + a_np^{n-1}\right). \end{aligned}$$

Härifrån ser vi att $p \mid -a_0q^n$ men eftersom $\mathrm{SGD}(p,q) = 1 \Rightarrow \mathrm{SGD}(p,q^n) = 1$ följer att $p \mid a_0$. Om vi istället skriver

$$a_0q^n + a_1pq^{n-1} + \cdots + a_np^n = q\left(a_0q^{n-1} + a_1pq^{n-2} + \cdots + a_{n-1}p^{n-1}\right) + a_np^n$$

ser vi att $q \mid -a_np^n$. På samma sätt måste då gälla att $q \mid a_n$. Vidare, om $a_n = 1$ måste isåfall $q = \pm 1$ vilket betyder att $\frac{p}{q} \in \mathbb{Z}$. □

Observera att satsen inte säger något om huruvida det faktiskt existerar något rationellt nollställe eller exakt vilket det är. Det finns många polynom med heltalskoefficienter som saknar rationella nollställen. Vad satsen istället säger är att om ett heltalspolynom har ett rationellt nollställe så kan det endast vara något av ändligt många rationella tal som också bestäms av satsen. Istället för att gissa på måfå kan man alltså systematiskt testa ändligt många och då vara säker på att man har hittat alla rationella nollställen. Vi visar hur detta kan gå till med ett exempel.

Exempel 6.28. Vi har fått tipset att polynomet $f(x) = x^3 - 3x^2 - 2x + 6$ har ett rationellt nollställe. Eftersom $a_n = 1$ vet vi dessutom att detta nollställe måste vara ett heltal $x = p$ och att detta heltal ska dela 6. Eftersom $6 = 2 \cdot 3$ kan vi se att de möjliga nollställena då är $p = \pm 1, \pm 2, \pm 3, \pm 6$. Vi har alltså 8 möjliga nollställen som vi helt enkelt får testa. Genom insättning ser vi då att endast $p = 3$ är ett nollställe. Vi kan då bryta ut faktorn $x - 3$ ur $f(x)$ och får då $f(x) = (x-3)(x^2-2)$. Polynomet $x^2 - 2$ har nollställena $x = \pm\sqrt{2}$. Vi har då hittat samtliga nollställen.

Som avslutning gör vi iakttagelsen att om ett andragradspolynom $x^2 + ax + b$ har nollställen $x = x_1$ och $x = x_2$ kan vi skriva $x^2 + ax + b = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$. Vi kan alltså se att $a = -(x_1 + x_2)$ och $b = x_1x_2$. Koefficienterna är alltså direkt kopplade till polynomets nollställen. Liknande relationer gäller för polynom av alla grader, till exempel kan vi för ett polynom $x^3 + ax^2 + bx + c$ av grad 3 skriva

$$\begin{aligned} x^3 + ax^2 + bx + c &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Vi ser alltså att

$$\begin{aligned} a &= -(x_1 + x_2 + x_3), \\ b &= x_1x_2 + x_1x_3 + x_2x_3, \\ c &= -x_1x_2x_3. \end{aligned}$$

För ett allmänt polynom $f(x) = a_0 + a_1x + \cdots + a_nx^n$ av grad n kan man se att koefficienten a_{n-1} alltid är lika med -1 gånger summan av alla nollställen och koefficienten a_0 alltid är lika med $(-1)^n$ gånger produkten av alla nollställen, d.v.s.

$$\begin{aligned} a_{n-1} &= -\sum_{k=1}^{n} x_k, \\ a_0 &= (-1)^n \prod_{k=1}^{n} x_k. \end{aligned}$$

Dessa samband kan också användas för att hitta eller åtminstone göra bättre gissningar på vilka nollställen ett polynom har.