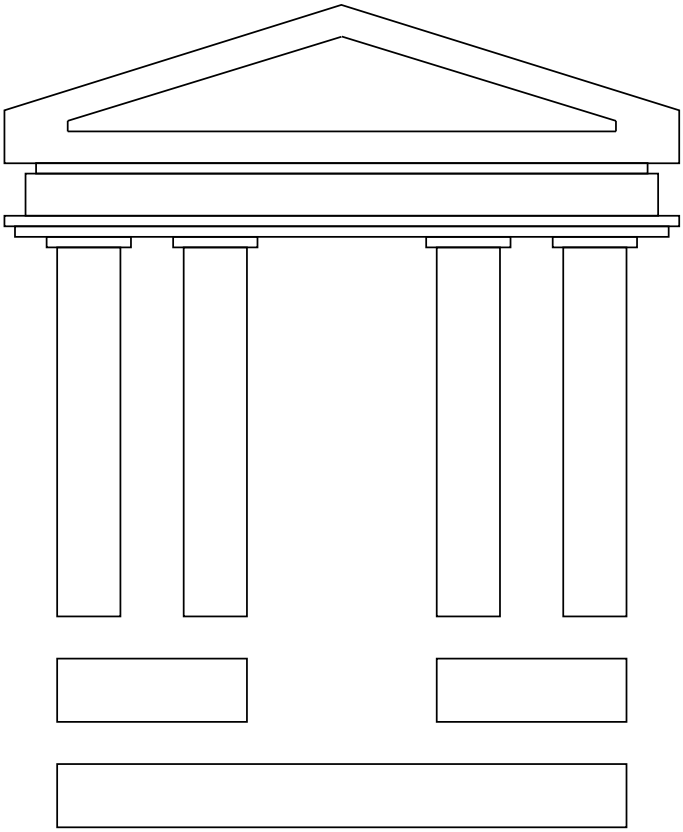


Matematikhistoria 3.1

Med talteori

Johan Wild

2019–08–07

©Johan Wild 2016

johan.wild@europaskolan.se

Får gärna användas i undervisning, kontakta i så fall författaren.

2019–08–07

Innehåll

1 Inledning

Denna lilla text har flera syften. Den skall

1. vända upp och ned på några begrepp du tror dig känna till, så att matematiken blir lite mer spännande,
2. introducera matematiken utifrån ett historiskt perspektiv,
3. introducera matematiken utifrån ett vetenskapligt perspektiv, samt
4. framställa matematiken på ett sådant sätt att den tränar läsning av svåra texter.

Framförallt punkt 2 och 3 kan inte göras samtidigt. Det finns en motsägelse i dessa mål, då människan har kunnat räkna så mycket längre än människan har haft behov av att ge beräkningarna och resonemangen sådan struktur att man kan kalla det för vetenskapen matematik. Därför får det bli lite hopp i både den historiska framställningen såväl som i den matematiska strukturen.

För att träna punkt 4 framställs ibland vissa påståenden både med så många matematiska symboler som möjligt, och på svenska.

Denna text är under ständig förbättring och har växt fram utifrån ett behov av läromedel i kurserna *Euklidisk geometri* (under läroplanen Lpf94) och *Axiomatiska system* (från och med spetsutbildningen och Gy11). Ett varmt tack till Hampus Söderström, Sci11, för korrekturläsning.

I version 3.0 av denna text infördes min alternativa definition av primtal. Ett varmt tack till Ebba Koerfer, Malin Loberg, Viktoria Sedig, Ingrid Sandberg och Evelina Evald i Sci13 för alla frågor rörande Euklides lemma, vilket var upprinnelsen till detta.

Version 3.1 har fler och bättre övningar. Dessutom är det inledande avsnittet om ekvationslösning i $\mathbb{Z}_{12}$ tillagt.

2 Symboler

I matematiken används ett flertal symboler för att korta ned vad som behöver skrivas för att uttrycka olika saker. Du har med säkerhet stött på några av dem, till exempel $+$ och $=$.

Här följer en lista över några symboler och hur de kan användas. Symbolerna $\mathbb{J}$, $\mathbb{U}$ och $\mathbb{P}$ är inte vedertagna symboler, men lämpar sig bra för denna text.

Symbol	**Betydelse**	**Exempel**
$\mathbb{N}$	De naturliga talen	$1, 2, 3, \ldots$
$\mathbb{Z}$	De hela talen	$0, 1, -1, 2, -2, \ldots$
$\mathbb{Q}$	De rationella talen	$1/2$, 0, $-8768376876/9837489$
$\mathbb{R}$	De reella talen	0,1,$1/2$, -4, π
$\mathbb{C}$	De komplexa talen	0,1,i, $3 - 4i$
$\mathbb{P}$	Primtalen	2,3,5,7,13
$\mathbb{J}$	De jämna talen	0,2,4,6
$\mathbb{U}$	De udda talen	1,3,5
$\in$	Tillhör	$3 \in \mathbb{Z}$
$\equiv$	Identiskt lika (definieras till)	$f(x) \equiv 3$
$\equiv$	Kongruent med (inom modulär aritmetik)	$4 \equiv 9 \pmod 5$
$\Rightarrow$	Implicerar	$x > 3 \Rightarrow x^2 > 9$
$\Leftrightarrow$	Ekvivalens	Se nedan
$\mid$	Delar	$3 \mid 9$
$\forall$	För alla	$n > 0 \, \forall \, n \in \mathbb{N}$
$\exists$	Det existerar	$\exists \, n : n^2 = 9$
:	Så att	$\exists \, n : n^2 = 9$
$\wedge$	Och	$x > 0 \wedge x^2 = 4 \Leftrightarrow x = 2$
$\vee$	Eller	$x < -3 \vee x > 3 \Leftrightarrow x^2 > 9$
$\aleph$	Ordning av oändligheten	$\lvert\mathbb{N}\rvert = \aleph_0$
∞	”Oändligheten”	Används i sammanhang som ”... då $x \to \infty$ ... ”
$\lvert\cdot\rvert$	Absolutbelopp	$\lvert-3\rvert = 3$ (Används även som symbol för norm i många sammanhang, till exempel kardinalitet för mängder.)
$\lVert\cdot\rVert$	Norm	$\lVert-3\rVert = 3$, $\lVert f(x)\rVert > 0$
$\varnothing$	Tomma mängden	$\lvert\varnothing\rvert = 0$
$\setminus$	Utom	$\mathbb{N} = \mathbb{Z}^+ \setminus \{0\}$
$\cap$	Snitt	$\{f(x), 0, a, 5\} \cap \{0, 1, a, b, 3\} = \{0, a\}$
$\cup$	Union	$\{f(x), 0, a, 5\} \cup \{0, 1, a, b, 3\}$ $= \{f(x), 0, 1, 3, 5, a, b\}$
$\subset$, $\subseteq$	(Äkta) delmängd, delmängd	$\mathbb{N} \subset \mathbb{Z}$
$\propto$	Proportionell mot	$y \propto x^2$

Det är vanligt att avnända det grekiska alfabetet i matematiken.

Versal	Gemen	Svenskt namn	Versal	Gemen	Svenskt namn
α	α	alfa	N	ν	ny
β	β	beta	O	o	omicron
Γ	γ	gamma	Π	π	pi
Δ	δ	delta	P	ρ	rho
E	ϵ	epsilon	Σ	σ	sigma
Z	ζ	zeta	T	τ	tau
N	η	eta	Υ	υ	upsilon
Θ	θ	theta	Φ	ϕ	phi
I	ι	iota	X	χ	chi
K	κ	kappa	Ξ	ξ	xi
L	λ	lambda	Ψ	ψ	psi
M	μ	my	Ω	ω	omega

3 Grunder

3.1 Talmängder

Först måste vi reda ut vad vi egentligen arbetar med. Det finns vissa vedertagna symboler för de olika talmängderna som kan vara bra att känna till. De naturliga talen betecknas $\mathbb{N}$.

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

Skrivsättet med tre punkter i slutet betyder att du skall tänka dig att talföljden fortsätter enligt mönstret i det oändliga.

Heltalen har fått beteckningen $\mathbb{Z}$.

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\} = \{\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Dessa två sätt att uttrycka $\mathbb{Z}$ är vanliga. I den sista varianten skall alltså följden börja med oändligt många negativa heltal före -3 och fortsätta med oändligt många heltal efter 3. Bokstaven Z för denna mängd kommer av tyskans **zahl** som betyder tal.

Skillnaden mellan $\mathbb{N}$ och $\mathbb{Z}$ är alltså att $\mathbb{N}$ inte innehåller varken talet 0 eller de negativa talen.

Symbolen $\in$ betyder "tillhör", den kan också utläsas "i" eller "som till-hör". Symbolen $\notin$ betyder "tillhör ej", jämför med symbolerna $=$ och $\neq$.

Exempelvis gäller $0 \in \mathbb{Z}$, $-2 \notin \mathbb{N}$ och $3 \in \mathbb{Z}$. Observera också att alla naturliga tal är heltal, men inte tvärt om.

Ibland har man glädje av att ange att en hel mängd element inte tillhör en mängd. Symbolen $\setminus$ används för detta och utläses "utom". Exempelvis gäller $\mathbb{N} = \mathbb{Z}^+ \setminus \{0\}$. Detta utläses "de naturliga talen är de positiva heltalen utom mängden som innehåller talet noll". Observera också skrivsättet med ett litet $+$ på $\mathbb{Z}$ för att ange de positiva heltalen. Talet 0 är alltså ett positivt tal.

Vidare finns de rationella talen. Ibland kallar man även dessa "bråk". Symbolen som används för dem är $\mathbb{Q}$, vilket kommer från engelskans ord för kvot, "quotient".

Exempelvis gäller $\frac{1}{2} \in \mathbb{Q}$, $-\frac{7}{3} \in \mathbb{Q}$, $2 \in \mathbb{Q}$ och $\frac{2}{5} \notin \mathbb{N}$. Observera att alla heltal (och därmed alla naturliga tal) också är rationella tal. Exempelvis gäller ju $2 = \frac{2}{1}$.

Det finns två talmängder till, men vi återkommer till dessa, eftersom de inte behövs i den inledande delen av denna text.

3.2 Räkneoperationer

Nu måste vi reda ut vad man får göra med tal. Det finns **två** räknesätt, addition och multiplikation. Subtraktion "finns inte"! När vi skriver $5-3$ menar vi i själva verket $5+(-3)$. Det finns alltså två betydelser av tecknen $+$ och $-$. Dels kan de användas som **indikator**, säga något om hur talen är (positiva eller negativa), dels kan de användas som **operator**, säga vad som skall göras med talen (adderas eller subtraheras). Att man använder samma tecken för dessa båda betydelser är ganska olyckligt ur pedagogiskt perspektiv, men sådant är livet.

På samma sätt "finns inte" division. När vi skriver $8/2$ menar vi i själva verket $8\cdot\frac{1}{2}$. Subtraktion och division är alltså inte egna räknesätt som du är vana att tänka på dem, utan bara kortare skrivsätt för addition och multiplikation. Av praktiska skäl använder vi naturligtvis ordet subtrahera och skriver till exempel $5-3$, poängen är att det matematiskt sett inte är en egen operation.

3.3 Inverser, enhetselement och ekvationslösning

Låt oss studera ekvationen

$$2x+3=13.$$

Du kan naturligtvis lösa ekvationen, men nu skall vi studera lösningsmetoden i ett lite mer vetenskapligt perspektiv. Har man tränat ganska mycket på att lösa denna sorts ekvation kanske man säger att man "flyttar över 3:an". Det är bra, ordet **algebra** har sin grund i det arabiska ordet *al-jabr* som betyder *omförflyttningen*. Ordet syftar på just denna operation.

Om du skulle behöva motivera närmare vaför denna förflyttning fungerar, så skulle du berätta att det man i själva verket gör är att man subtraherar talet 3 från både höger och vänster led i ekvationen och får

$$\begin{array}{lll} 2x+3-3 & = & 13-3 \\ 2x+0 & = & 10 \\ 2x & = & 10 \end{array}$$

Anledningen till att detta är bra är att $3-3=0$, vilket gör att 3:an "försvinner" ur vänsterledet. Nu var det ju så att operationen subtraktion inte finns. Skriver vi $3-3$ menar vi $3+(-3)$. Vi gör följande definition.

Definition 3.3.1. Talet a är **additativ invers** till talet b om

$$a+b=0.$$

▲

Med ett finare språkburk skulle vi säga att vi adderade den additativa inversen till 3 till båda led i ekvationen för att eleminera 3:an i vänsterledet.

För att "göra oss av med" 2:an säger vi normalt att vi delar båda led med två. Återigen finns inte division. Det vi gör är att multiplicera båda led med $\frac{1}{2}$. Vi får

$$\begin{aligned} 2x &= 10 \\ \frac{1}{2} \cdot 2x &= 10 \cdot \frac{1}{2} \\ 1 \cdot x &= 5 \\ x &= 5. \end{aligned}$$

Det här var smart eftersom produkten $2 \cdot \frac{1}{2} = 1$. Vi gör följande definition.

Definition 3.3.2. Talet a är **mulitplikativ invers** till talet b om

$$a \cdot b = 1.$$

▲

Talen 0 och 1 är lite speciella. Om man adderar 0 till något tal a förändras inte talet a. Vi har att $a + 0 = a$. Detsamma händer om man multiplicerar a med 1, $1 \cdot a = a$. Vi benämner dessa element det **additativa enhetselementet** repspektive det **multiplikativa enhetselentet**.

Vi kunde lösa vår ekvation eftersom vi kunde hitta additativ invers till 3 och multiplikativ invers till 2.

Tänk om vi däremot har att göra med en ekvation som bara rör heltal. Då saknar faktiskt ekvationen $2x+3 = 13$ lösning! Bland heltalen finns den additativa inversen till 3, men den multiplikativa inversen till 2 finns inte bland heltalen.

Vi har alltså ingen systematisk metod att finna lösningen till $2x = 10$. Vi kan gissa en lösning och pröva oss fram, men principiellt kan vi inte lösa ekvationen.

Det kan vara så att vissa tal har invers, men inte alla. Det beror på vilken mängd man studerar. I $\mathbb{Z}$ är det bara 1 och -1 som har multiplikativ invers. I $\mathbb{Q}$ har alla tal utom 0 multiplikativ invers.

3.4 Ekvationer på en klocka

Ekvationer av typen $ax + b = c$ där $a \neq 0$ och $a \neq \pm 1$ är inte så spännande i $\mathbb{Z}$, $\mathbb{Q}$ eller $\mathbb{R}$. De är lösbara i de två sista mängderna, men inte i den första.

Vi ska se att det blir roligare om vi räknar med färre tal. Om vi begränsar oss till heltal $0 \leq a < n$ för något bestämt n händer det intressanta saker. Eftersom vi är så vana att se klockor börjar vi med fallet $n = 12$. Vi kallar denna mängd $\mathbb{Z}_{12}$, vilken alltså består av talen $0, 1, 2, \ldots, 11$. Vår klocka består alltså bara av en visare, och den kan bara visa hela timmar.

Utan att vara allt för precis så håller du säkert med om att

$$\begin{aligned} 2 + 3 &= 5 \\ 10 + 6 &= 4 \\ 3 \cdot 6 &= 6 \\ 4 \cdot 4 &= 4 \end{aligned}$$

på en klocka. Vi har exempelvis att $10 + 6 = 16$ och $4 \cdot 4 = 16$, men talet 16 finns ju inte i $\mathbb{Z}_{12}$, men det motsvaras på ett naturligt sätt av talet 4.

Låt oss nu se på en ekvation i $\mathbb{Z}_{12}$, exempelvis

$$3x + 7 = 4.$$

Vi angriper detta som förut och frågar oss vilket tal som är additativ invers till 7. Ett förhastat förslag är -7, eftersom -7 inte finns i $\mathbb{Z}_{12}$. Däremot gäller $7+5=0$ i $\mathbb{Z}_{12}$. Den additativa inversen till 7 är alltså 5!

Du inser säkert att alla tal har additatvi invers i $\mathbb{Z}_{12}$. Det är ju bara att "snurra klart varvet" till 0 om man verkligen tänker sig beräkningen som förflyttningar av en visare.

Vi får

$$\begin{aligned} 3x+7+5 &= 4+5 \\ 3x &= 9. \end{aligned}$$

Nu blir det däremot intressant. Vi förstår naturligtvis att en lösning till ekvationen är $x=3$, men frågan är om vi kan hitta en algebraisk metod att lösa denna sorts ekvation. Vi vill ju gärna kunna lösa alla ekvationer av typen $ax=b$ i $\mathbb{Z}_n$ för alla n.

Talet 3 saknar multiplikativ invers i $\mathbb{Z}_{12}$, så därför kan vi inte lösa ekvationen. Däremot kan vi lösa ekvationen

$$5x = 4$$

eftersom $5 \cdot 5 = 1$ i $\mathbb{Z}_{12}$. Vi får

$$\begin{aligned} 5x &= 4 \\ 5 \cdot 5x &= 5 \cdot 4 \\ x &= 8. \end{aligned}$$

Denna ekvation gick tydligen att lösa, och den har också bara en lösning. Däremot har ekvationen $3x=9$ faktiskt flera lösningar, både $x=3$, $x=7$ och $x=11$.

Ekvationen $3x=7$ saknar lösningar. En matematiker ställer sig genast följande frågor.

> I vilka fall är ekvationen $ax=b$ lösbar i $\mathbb{Z}_n$? Om ekvationen är lösbar, när finns det bara en repspektive flera lösningar? Hur många i så fall? Finns det någon metod att lösa ekvationen.

Det råkar vara så att svaret är att alla sådana ekvationer är lösbara om n är ett primtal. I vissa fall (olika a för olika n) finns multiplikativ invers till a, och då finns exakt en lösning. Om det finns lösningar som inte går att hitta (med hjälp av en multiplikativ invers), då finns det alltid flera lösningar.

Med hjälp av teorin i denna text skall vi förstå varför det blir så.

3.5 Om matematik

Alla som tycker om att titta på fotboll är nog överens om att det inte bara är en fråga om vem som vinner en match. Det finns en skönhet i själva spelet fotboll. Man vill se snygga finter och teknisk bollkontroll. Framförallt vill man se smarta passningar så att det verkligen blir en lagsport.

Detta håller nog många med om. Även de som normalt inte tittar på fotbollsmatcher förstår att det finns en skönhet som man skulle ha behållning av om man förstod alla regler och helst kunde spela lite själv.

Om man istället tar ett spel som schack, som är mycket mer abstrakt, så går nog de flesta med på att det även här finns en skönhet i spelet. Kan man spela schack kan man följa med i en match och se hur en spelare fintar bort sin motståndare på mer eller mindre snygga sätt.

Även de som inte spelar schack eller ens kan alla regler förstår nog att man kan tillämpa spelets regler så att man skulle uppfatta vissa sätt som vackrare än andra sätt om man bara förstod dem.

Av någon anleding är människan mycket bra på denna sorts spel. Varför evolutionen har gett oss förmågan flytta runt pjäser efter vissa regler kan tyckas märklig, men så är det. Vi ägnar oss gladeligen åt schack, sudoko, bridge och andra kortspel. De flesta datorspel innebär också att man skall kombinera något på olika vis, eller följa abstrakta regler.

Även de flesta sporter, som fotboll, innebär att man bestämmer ett uppsättning regler och följer dem för att det är kul.

Vi kan koda av symboler (bokstäver) och bilda ord som vi sätter ihop till meningar. Vi klarar av att skilja på dessa i olika språk, precis som vi förstår att bollen skall behandlas på olika sätt i fotboll och basket.

Matematik är i själva verket precis ett sådant här spel. Vi har infört symboler och vi har bestämt vad man får göra med dessa. Egentligen är matematiken massor av olika spel. I det ”spel” där vi räknade med alla tal kunde vi flytta runt talen för att lösa vissa ekvationer, men i det ”spel” där vi räknade som på en klocka kunde vi inte det. Däremot uppstod i vissa fall flera lösningar.

Geometrin är på många sätt ett spel i sig själv. Genom att kombinera olika regler kan man få olika resultat. Pythagoras sats är kanske det mest kända av de mer avancerade resultaten. Att ”spela” geometri innebär att du skall kombinera olika begrepp som punkter, linjer och vinklar, till något mål som exempelvis Pythagoras sats.

Vissa spel av denna typ har ett tydligt slutmål som uppnås relativt lätt. Det finns till exempel inte så många varianter av luffarschack[1]. Andra spel, som schack, utvecklas ständigt. Folk kommer på nya strategier hela tiden, ingen blir fulllärd.

Matematiken är det största spel som människan konstruerat. Matematiken innehåller de flesta spel, bland annat schack, sudoko och alla kortspel.

Matematiken utvecklas både genom att vi upptäcker nya regelsystem att följa och genom att de kända regelsystemen leder oss till okända resultat. Det finns många olösta problem även i de fall där reglerna är kända.

Det som däremot skiljer det vi brukar kalla matematik från det vi brukar kalla spel är att vi kan använda matematiken till att lösa praktiska problem och till att förstå naturen. Det finns matematiska modeller som beskriver hur hela universum har utvecklats från Big Bang, hur stabila grundämnen bildas och hur dessa kan sättas samman till molekyler. Vi förstår genom statistiken och andra modeller hur samhällen utvecklas på olika sätt, till exempel inom ekonomin. Och så kan vi förståss lösa diverse praktiska problem i vår vardag.

Det är alltså en god idé att lära sig spela just detta spel!

[1]Det finns bara 126 sätt att placera ut fem kryss och fyra cirklar på 3×3 rutor.

3.6 Övningar

1. Bevisa att talen 4 och 5 inte är varandras additativa inverser i $\mathbb{Z}$.

Facit

1. I matematiken är det ofta så att det uppenbara kan vara svårt att formulera. I detta fall blir beviset helt enkelt att $4 + 5 = 9 \neq 0$.

4 Historia

Texter om matematikens historia brukar inledas med att studera Babylonien, Egypten, Kina och Indien. Det man brukar intressera sig för är följande frågeställningar.

- Hur skrevs tal? Vilka siffror användes och på vilket sätt kombinerades dessa till tal?
- Hur räknade man? Vilka systematiska metoder hade man för att kombinera två tal till ett nytt vid till exempel addition?
- Hade man ekvationer och (linjära) ekvationssystem? Kunde man göra abstrakta uttryck för problemställningar och kunde man kombinera dessa för att lösa avancerade problem?
- Hur behandlades irrationella tal och kvadratiska ekvationer? Hur löstes problemet med tal som inte går att uttrycka i bråkform?
- Vad kände man till om geometri?
- Vilken världsuppfattning hade man? Ofta hänger detta ihop med kännedomen om astronomi och den matematik som krävs för att göra förutsägelser om sådana spörsmål.

Efter dessa gamla kulturer brukar man ta upp den matematik som fanns i Grekland, hur araberna förvaltade och vidareutvecklade denna och vad som hände då européer äntligen hade vett att ta till sig av arabernas kunskaper.

Under Romarriket utvecklades nämligen nästan ingen matematik alls. Inte heller finns det så mycket spår av högre matematik från Syd- och mellanamerika.

Denna text tar upp de gamla kulturerna och grekerna till och med Euklides. Tyngdpunkten ligger på Pythagoras och dennes talteori.

5 De gamla

5.1 Nilen

Nilen är världens längsta flod. Den har sina källor i Victoriasjön och i de Etiopiska bergen. Människan uppstod i trakterna för Nilens källor, och det är också längs Nilen denna historia om matematiken tar sin början.

Nilen rinner idag genom mycket torra och fattiga länder. Dess vatten är livsnödvändigt för invånarna i området, både för bevattning och för transporter. Innan människan

exploaterade Nilen svämmade den årligen över då smältvattnet från bergen uppströms nådde lågländerna. Denna flodvåg förde med sig mycket näringsrikt slam. När Nilen efter hand sjönk kvarstod en bördig mylla. Detta möjliggjorde ett fruktbart jordbruk som gjorde folket, eller i alla fall den härskande eliten, rik och mäktig för ca 4000 år sedan.

Tyvärr förstördes gränsmarkeringar av vattnet. Därför var man tvungen att man mäta upp jorden på nytt varje år för att rättvist kunna fördela åkermarken. Ur detta behov sägs geometrin ha fötts. Geometri betyder nämligen jordmätning.

Eftersom mycket vatten dunstar under passagen genom Sudans och Egyptens öknar är det inte mycket av vattnet som når ut i Medelhavet. Det stora delta som finns norr om Kairo vore inte ens farbart med båt om det inte vore för byggda kanaler.

Invånarna runt Nilen har i alla tider byggt bevattningskanaler, som med tiden gjorde att allt mindre vatten nådde nedströms. Bland annat för att bli mindre beroende av sina uppströms grannar, och för att få jämnare flöde under hela året, byggde Egypten den jättelika Assuandammen som stod klar 1970. I den kan ett helt års förbrukning av vatten lagras.

5.2 Egypten

Längs Nilen har det funnits jordbruk från ca år 5000 f Kr. Den första dynastin med makt i både övre och nedre Egypten hade sin storhetstid ca 3100 f Kr. Hieroglyferna översattes år 1822 e Kr av Jean Champollion (1790 - 1832) med hjälp av den s k Rosettastenen. På den är en text nedtecknad både på grekiska och med hieroglyfer, vilket möjliggjorde översättningen.

Ca år 1650 f Kr, i det mellersta riket, nedtecknades Rhindpapyren. Dessa kallas så efter Henry Rhind som hittade dem år 1858. De innehåller ca 110 matematiska problem med lösningar. De utgör tillsammans med Moskvapapyren (vilka kallas så för att de idag förvaras i Moskva) och några andra funna texter huvudkällan för vår kunskap om den matematiska vetenskapen i Egypten.

Vid denna tid behärskade egyptierna bråkräkning, ekvationslösning och beräkningar av ytor och volymer. Lustigt nog finns inte någon metod för att beräkna volymen av en pyramid med. Däremot finns det angivet hur man beräknar volymen av en stympad pyramid, en pyramid med en mindre pyramid i toppen avlägsnad.

Bråk nedtecknades som summor av *stambråk*, bråk med ett i täljaren. Egyptierna hade alltså inget sätt att skriva $\frac{5}{6}$, utan uttryckte det som $\frac{1}{2} + \frac{1}{3}$.

De hade ingen utvecklad algebra för att lösa ekvationer, men ett exempelproblem är: Ett tal och dess fjärdedel har summan 15. Vilket är talet? Detta problem löstes genom ett resonemang: Utgå från talet 4, vars fjärdedel är 1. Summan av dessa är 5 som blott är en tredjedel av vad den skall vara. Därför måste det sökta talet vara $4 \cdot 3 = 12$.

Man kan konstatera att egyptierna var tvungna att vara ganska smarta, även för att lösa ganska enkla problem. Idag skulle vi lösa samma problem genom att nedteckna ekvationen

$$x + \frac{x}{4} = 15.$$

Genom att använda algebra systematiskt och utan att behöva tänka så mycket i varje steg kommer vi lätt fram till att lösningen är $x = 12$.

Sensmoralen är alltså att *människan har uppfunnit matematiken för att slippa tänka och vara smart*. Matematiken gör problemlösning enklare!

5.3 Babylonien

Ordet *meso* är grekiska och betyder mellan. Namnet Mesopotamien syftar på landet mellan floderna Eufrat och Tigris. Babylonien är namnet på den kultur som rådde där 2300 - 1600 f Kr.

Kungen Hammurabi härskade där omkring 1700 f Kr. Från denna tid finns lertavlor med kilskrift bevarade, varav vissa innehåller matematik. År 1838 e Kr lyckades Henry Rawlinson tolka dessa tecken. Även i detta fall lyckades man göra detta tack vare att man fann en text, Behistuinskriften, med samma text på tre språk.

Babylonierna kunde lösa ekvationssystem med upp till fem obekanta, lösa andragradsekvationer och vissa tredjegradsekvationer. De kände även till det samband vi idag kallar Pythagoras sats. Intressant är att de inte gjorde skillnad på aritmetik och geometri.

5.4 Kina

Shang-dynastin härskade i Kina från ca år 1600 f Kr. Från denna tid finns vissa inskriptioner i ben bevarade av matematisk natur. Från ca år 1000 f Kr härskade Zhou-dynastin, vilken senare bröts upp i feodala småstater. Runt år 600 f kr började man använda järn. Akademier knutna till hoven i dessa småstater växte fram. En av de mer kända akademikerna från denna tid är Konfucius.

År 221 f Kr enas återigen alla småstater under Quin Shi Huangdi. Han införde bland annat ett standardiserat måttsystem. Denna dynasti varade i ca 400 år.

Kineserna kände till ungefär samma matematik som egyptierna och babylonierna, men låg flera hundra år efter dem. Det är inte säkerställt om de hade kontakt med varandra.

5.5 Indien

Runt Indusfloden växte en kultur fram ca år 3000 f Kr. Man har inte hittat någon bevarad matematik från denna kultur. Tusen år senare växte det fram en annan kultur runt floden Ganges.

Skrifter finns från denna tid som handlar om hur man gör hållfasthetsberäkningar vid byggnationer av tempel i tegel. Dock användes inte tegel vid denna tid, vilket man gjorde under den tidigare tiden. Därför kanske man kan dra slutsatsen att matematiken härrör från den äldre kulturen.

De siffror vi använder idag härrör från Indien, men från en mycket senare tid.

5.6 Gemensamt för de gamla rikena

Följande punkter kan sammanfatta vad de gamla rikena har gemensamt vad gäller synen på matematik och sättet den behandlades på.

- Matematiken var ett redskap för handel och ingenjörskonst, matematiken hade inte mycket egenvärde i sig.
- Resultaten presenterades till exempel i skrifter om hur man bygger ett altare eller en fördämning. Det finns nästan inga fristående verk som handlar om matematiken i sig.

- De hade inga sätt att kontrollera om matematiska uttryck (formler) stämmer. Även om de kunde beräkna en vinkels storlek kvarstod fortfarande det mättekniska problemet att kontrollera resultatet. Det var svårt att tillverka mätinstrument med tillräcklig precision.

- Matematiken växte fram med starka ledare som införde gemensamma måttsystem och som hade råd att hålla matematiker vid sina hov.

6 Grekland

Tiden för det gamla Grekland brukar delas in i tre delar. Tabellen nedan anger hur detta görs samt vilka matematiker som tas upp i denna bok.

Ekpok	**Period**	**Matematiker**
Klassisk tid	500 – 338 f Kr	Thales, Pythagoras, Zenon
Hellenistisk tid	338 – 30 f Kr	(Sokrates), Platon, Aristoteles, Euklides
Romersk tid	30 f Kr – 395 e Kr	

De händelser som markerar skiften mellan epokerna är när Alexander den store invaderar Grekland år 338 f Kr, när romarna gör detsamma år 30 f Kr samt när Romarriket delas år 395 e Kr.

6.1 Thales ca 624 – 548 f Kr

Thales gjorde många resor, bland annat till Babylonien och Egypten, där han lärde sig mycket astronomi och geometri. Thales brukar tas som den förste grekiske matematikern. Han var den förste som formulerade påståenden av den typ vi kallar *satser*. Han föddes och verkade i Miletos, dagens Turkiet.

Några geometriska satser brukar tillskrivas Thales. Dessa är:

- *Thales sats* Varje vinkel, som är inskriven i en halvcirkel, är rät.

- En cirkel halveras av sin diameter.

- Basvinklarna i en likbent triangel är lika stora.

- Vertikalvinklar är lika stora.

- Om två vinklar och en sida i en triangel är lika stora som var sin av två vinklar och en lika belägen sida i en annan triangel, så är trianglarna kongruenta.

Thales bevisade inte dessa satser som Euklides senare gjorde i Elementa. Det finns två anledningar till att Thales och dessa satser tas upp i denna text. Dels brukar den första benämnas Thales sats och tas normalt upp på gymnasiet. Dels kanske det är överraskande att dessa över huvud taget är satser som går att bevisa utifrån mer grundläggande antaganden. Dessa sanningar brukar närmast betraktas som axiom på gymnasienivå.

6.2 Pythagoras ca 570 – 495 f Kr

Pythagoras växte upp på Samos, en ö i Egeiska havet. Han hade kontakt med Thales under sin studietid och ägnade därefter 20 år åt resor, bland annat till Egypten och Babylonien.

Under Pythagoras reseår hade Samos förvandlats från en tillåtande och öppen stat till en tyranni under Polykrates. Pythagoras avböjde ett erbjudande om att verka vid hans hov och bosatte sig i en grotta på en avlägsen del av ön. Pythagoras fick muta sin första elev att ta lektioner. När eleven efter en tid hellre betalade för utbildningen var han fast.

Vid denna tid hade de grekiska stadsstaterna bildat kolonier på kusterna till närliggande delar av Medelhavet. En av dessa kolonier i Magna Graecia, Stor-Grekland, var Kroton som ligger i nuvarande södra Italien. Dit begav sig Pythagoras, som nu var känd som ”den vise från Samos”. Han fick beskydd och finansiering av en rik man vid namn Milon, som hade segrat 12 gånger i de olympiska och pythiska spelen.

Här grundade Pythagoras en blandning mellan akademi och religiös sekt vars valspråk var ”Allt är tal”. Lärjungarna kallades pythagoréer. Sällskapet var hemligt och man fäste stor vikt vid att upptäckterna inte kom till allmänhetens kännedom. Det berättas att en man som avslöjade dodekaedern dränktes.

Även kvinnor fick delta.

Pythagoréerna studerade även harmoniska klanger med strängar. Detta är ett av de första exemplen på hur man kopplat ihop naturfenomen med matematik.

Pythagoras levde tyvärr under en orolig tid, och inte mycket är bekräftat om hans liv och död. En myt förtäljer att avundsjuka mot att pythagoréerna inte avslöjade sina upptäckter ledde till att en man som tidigare nekats inträde i sällskapet hetsade folket i Milons stad mot dem under en segerfest där man firade att Milon vunnit en konflikt med en grannstad. Milons hus brändes ned. Milon undkom, men inte Pythagoras.

Det som främst skiljer pythagoréerna och deras studier av matematik från tidigare kulturer är att de studerade matematiken för dess egen skull, samt att de försökte formulera matematiken *axiomatiskt-deduktivt*. Det senare betyder att de försökte bygga upp matematiken från ett litet antal grundläggande antaganden, *axiom*, och ur dessa försökte bevisa att andra påståenden var sanna.

6.3 Zenon ca 490 - 425 f Kr

Zenon kom från Elea i södra dagens södra Italien och var lärjunge till Parmenides. I sin ungdom var Zenon pythagoré. Med tiden blev han mer filosof än matematiker. Han är känd för sina paradoxer, bland annat den om Akilles och sköldpaddan som tas upp på lektionstid. Sokrates skall enligt Platon ha mött Zenon i sin ungdom.

6.4 Sokrates 469 - 399 f Kr

En av de viktigaste filosoferna för utvecklingen av den västerländska kulturen. Nämns här mest för att göra trion Sokrates - Platon - Aristoteles komplett.

6.5 Platon 427 - 347 f Kr

Grundade en akademi i Aten ca 385 f Kr där man studerade, undervisade och forskade i allt möjligt, bland annat filosofi och matematik. Ovanför porten lär det ha stått ”Låt ingen som är obevandrad i geometri komma in här”.

Platons namn återfinns inom matematiken genom att de fem regelbundna månghörningarna, polyhedrarna, som ibland kallas för de platonska kropparna. Dessa var viktiga för Platons beskrivning av naturen. Tetraedern stod för eld, kuben för jord, oktaedern för luft och ikosaedern för vatten. Dodekaedern stod för hela universum.

6.6 Aristoteles 384 - 322 f Kr

Från 18-års ålder till Platons död studerade Aristoteles vid Platons akademi. Efter detta blev han privatlärare åt Alexander den store då denne var ung. Alexanders pappa Filip II var kung i Makedonien. Grekerna tyckte att makedonierna var obildade barbarer, vilket Filip på sätt och vis höll med om eftersom han gav i uppdrag åt grekernas störste vetenskapsman att bilda hans son. Detta var ett led i att göra Makedonien mer grekiskt.

Aristoteles var verksam inom många områden. Bland annat härrör från honom uppdelningen av kunskap i *episteme*, det vi skulle kalla vetenskap idag, *fronesis*, vishet/klokhet samt *techne*, den form av tyst kunskap som exempelvis ”sitter i handen” på den som är duktig på att tälja.

Det främsta bidrag Aristoteles lämnade till matematiken var att han lade grunden till logiken och för logiska resonemang. Följande tabell beskriver fyra mycket viktiga begrepp Aristoteles införde.

Begrepp	**Förklaring**
Axiom	Grundläggande sanning som är gemensam för alla vetenskaper.
Postulat	Grundläggande sanning för en enskild vetenskap.
Påstående	Kan visas vara antingen sant eller falskt.
Sats/teorem	Ett påstående som visats vara sant.

Skillnaden mellan axiom och postulat kan exemplifieras med två citat ur Elementa. Ett postulat är *Man kan dra en rät linje från en punkt till en annan* och ett axiom är *Storheter som är lika med en och samma storhet är också inbördes lika.* Vi ser alltså hur postulatet rör endast geometrin, medan axiomet är inte är knutet till en vetenskap.

Nu för tiden gör man inte så stor skillnad på axiom och postulat. Det ord som fått ge vika är postulat.

En samling axiom, postulat och definitioner som gör det möjligt att härleda satser utgör ett *axiomatiskt system*, eller ett *formellt system*.

Senare i denna text skall vi se hur de moderna axiomen för algebran är formulerade.

6.7 Euklides 325 - 265 f Kr

Euklides var verksam i Alexandria större delen av sitt liv. Troligen studerade han under elever till Platon.

Efter Alexander den stores död 323 f Kr fick en av Alexanders generaler, Ptolemaios, makten över Egypten. Han grundade i Alexandria ett Museion, ett slags universitet, en samlingsplats för lärda, i praktiken ett statsfinansierat forskningsinstitut.

Idag återfinns ordet museion i musiskt lärande, vilket innefattar bildkonst, drama, musik etc. Härur är även ordet musik bildat. Förr räknades alltså matematik och filosofi till denna typ av konstform. Hur som helst verkade Euklides vid denna institution.

6.7.1 Elementa

Euklides största bedrift var att han skrev ned mycket av den matematik som var känd vid denna tid i en serie böcker med namnet Elementa. Denna innehåller 13 böcker, eller kapitel, som av tradition betecknas med romerska siffror. Tabellen nedan visar vad de innehåller.

Bok	**Innehåll**
Bok I-VI	Plangeometri
Bok VII-IX	Talteori och aritmetik
Bok X	Inkommensurabla storheter
Bok XI-XIII	Rymdgeometri

Innehållet framställdes axiomatiskt-deduktivt vilket var nytt, men inspirerat av Aristoteles. *Deduktiv* bevisföring betyder att resultatet är en logisk följd av givna förutsättningar. Motsatsen är *induktiv* bevisföring där slutsatser dras från enstaka (vanligtvis flera) händelser.

Elementa är så gedigen att den har använts som läromedel under mer än 2000 år. Det är bara på senare årtionden som svenska läromedel lämnat den axiomatiska framställningen av geometrin.

6.8 Geometri och talteori

För grekerna var geometri en sak och talteori och räkning en annan. Geometri var något man utförde med en ograderad linjal och passare. Med endast dessa hjälpmedel kan man bevisa satser och göra geometriska konstruktioner.

Ett bra exempel på denna skillnad är det som kallas Pythagoras sats. Den säger att för en rätvinklig triangel är summan av kvadraterna av längden av de två kortaste sidorna lika stor som kvadraten av längden av den längsta sidan. Observera att det alltså inte är meningen att man skall mäta sidorna och genomföra denna beräkning. Man kan bevisa påståendet endast med ovan nämnda hjälpmedel.

De pythagoreiska tripletterna rör heltal och hör hemma i talteorin.

7 Grundläggande talteori

I detta och hela kapitel 7 – 9 använder vi bara heltal. Mer precist håller vi oss till ringen[2] $\mathbb{Z}$.

7.1 Delare, primtal och faktorer

Vissa tal går att uttrycka som produkten av två andra tal, två **faktorer**.

Exempel 7.1.1. $33 = 3 \cdot 11$. ▲

Vi skulle också säga att talet 3 ovan **delar** 33, eller är en **delare** till 33. Vi preciserar detta.

Definition 7.1.2. Ett tal d är en **delare** till ett tal a om det finns ett heltal q så att $a = d \cdot q$. Vi säger också att talen d och q är **delare** till a, och att talet q är **kvoten** som fås då a delas med d.

Med symbolspråk: $d \mid a \Leftrightarrow \exists q \in \mathbb{Z} : a = qd$ ▲

Övning 1

Exempel 7.1.3. Talet 6 är en delare till 42. Talet 42 har delarna 1, 2, 3, 6, 7, 14, 21 och 42. ▲

Exempel 7.1.4. Då 42 delas med 14 fås kvoten 3. ▲

Exempel 7.1.5. Talet 7 är en faktor i 42. Talet 42 har faktorerna 2, 3 och 7. ▲

Övnign 2

Ofta använder man symbolen D_a för att ange **delaremängden** till talet a. Till exmepel gäller $D_{42} = \{1, 2, 3, 6, 7, 14, 21, 42\}$.

I vissa sammanhang räknas inte talet själv med i sin delaremängd, och ibland räknas även de negativa delarna med (då skulle till exempel $-14 \in D_{42}$ gälla). Sammanhanget får avgöra det om det inte preciseras.

Symbolen $\mid$ används för att uttrycka att "delar". Uttrycket $3 \mid 6$ utläses "tre delar sex". Symbolen $\nmid$ är negationen till $\mid$ och utläses "delar inte". Exempelvis gäller $5 \nmid 7$.

Observera att ett uttryck av typen $5 \mid 24$ är *sant* eller *falskt*. Exemplet är $5 \mid 24$ falskt. Ett vanligt missförstånd är att tolka det som någon slags symbol för division. Att skriva $4 \mid 24 = 6$ är alltså helt fel!

Vissa tal går inte att skriva som produkten av två andra tal som båda är större än 1. Detta brukar tas som en definition av **primtal**, men här skall vi göra en annan definition.

Definition 7.1.6. Talet p är ett **primtal** om $p \mid ab$ medför att $p \mid a$ eller $p \mid b$ för alla a, b i $\mathbb{Z}$. Talet 1 är inte ett primtal. ▲

Varför vi gör en annan definition än den gängse motiveras i appendix B. Det kan kännas tryggt att formulera och bevisa följande sats.

Sats 7.1.7. *Om p är ett primtal så har det endast delarna 1 och p.*

Bevis. Antag att p är ett primtal. Alla tal har delaren 1 och alla tal delar sig själv. Det som återstår är att bevisa att p inte kan ha någon annan delare än p.

[2] Begreppet **ring** introduceras i avsnitt 12.2.

Antag att p skulle ha någon annan delare c. Det betyder att det existerar ett q så att $p = cq$.

Men då skulle det kunna vara så att $p \mid ab$ trots att p varken delar a eller b. Det skulle kunna vara så att $c \mid a$ och $q \mid b$.

Då kan inte p vara ett primtal vilket strider mot förutsättningarna. Alltså kan det inte finnas någon annan delare c □

Exempel 7.1.8. Talen $2, 3, 5, 7, 11, 13, 17, 19$ och 23 är exempel på primtal. ▲

Notera att talet 1 inte räknas som ett primtal.

Definition 7.1.9. Med en **faktorisering** av ett tal menas att skriva talet som en produkt av primtal. ▲

Exempel 7.1.10. Att skriva 42 som $6 \cdot 7$ räknas alltså inte som en faktorisering, eftersom talet 6 kan skrivas som $2 \cdot 3$. ▲

I praktiken måste man ofta utföra faktoriseringar i flera steg.

Exempel 7.1.11. $18 = 2 \cdot 9 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$. ▲

Exempel 7.1.12. $18 = 3 \cdot 6 = 3 \cdot 2 \cdot 3 = 2 \cdot 3^2$. ▲

De två sista exemplen visar att de två olika sätten att bryta upp talet 18 slutligen ger samma uppsättning primtalsfaktorer. Detta gäller generellt. Därför formulerar vi följande mycket viktiga sats, som kallas **aritmetikens fundamentalsats**.

Sats 7.1.13. *Faktoriseringen av ett tal är entydig.*

Notera att det inte på något vis är självklart. I $\mathbb{Z}_{12}$ gäller både $4 = 2 \cdot 2$ och $4 = 4 \cdot 4$.

Bevis. Antag att det finns två olika faktoriseringar av talet z:

$$\begin{aligned} z &= p_1 \cdot p_2 \cdot \cdots \cdot p_n \\ z &= q_1 \cdot q_2 \cdot \cdots \cdot q_m \end{aligned}$$

där alla $p_1, p_2, \ldots, p_n$ och $q_1, q_2, \ldots, q_m$ är primtal. Utan inskränkning kan vi anta att $n < m$.

Uppenbarligen gäller $p_1 \mid z$. Enligt definition 7.1.6 måste därför p_1 dela något av alla $q_1, q_2, \ldots, q_m$. Det är bara möjligt om p_1 i själva verket är ett av dessa. Låt oss numrera dem så att $p_1 = q_1$. Det ger

$$p_1 \cdot p_2 \cdot \cdots \cdot p_n = p_1 \cdot q_2 \cdot \cdots \cdot q_m.$$

Kancelleringslagen[3] ger då att

$$p_2 \cdot p_3 \cdot \cdots \cdot p_n = q_2 \cdot q_3 \cdot \cdots \cdot q_m.$$

Nu måste med samma resonemang p_2 dela båda led och vi får att $p_2 = q_2$. När vi delat bort alla primtal i vänsterledet har vi kvar

$$1 = q_s \cdot \cdots \cdot q_m$$

där $s = n + 1$.

Sista likheten är bara möjlig om alla $q_s, \ldots, q_m$ är 1. Därför är alla p_k lika med var sin q_k och det kan alltså inte finnas två olika faktoriseringar. □

[3] **Kancelleringslagen** säger att om $ab = ac$ så gäller $b = c$. Denna lag gäller i $\mathbb{Z}$, se sats 8.5.2

7.2 Representation av heltal

Nu när vi vet att faktoriseringen av heltalen är entydig kan vi tänka på tal som klumpar av primtal.

Vi skriver ett tal som produkten av alla primtal det innehåller. Exempelvis gäller $12 = 2^2 \cdot 3$, $25 = 5^2$, $64 = 2^5$ och $1105 = 5 \cdot 13 \cdot 17$. Generellt skriver vi

$$a = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}$$

och definierar följande.

Definition 7.2.1. Multipliciteten för en faktor i ett tal är det antal gånger faktorn förekommer i talet. ▲

Övning 3

Exempel 7.2.2. Multipliciteten för faktor 3 i talet 18 är alltså två, och faktorn 2 har multiplicietet ett. ▲

I det generella uttrycket är alltså multipliciteten för faktorn p_k talet μ_k.

Multipliciteten för faktorer som inte ingår i ett tal kan man betrakta som noll. Det är med detta synsätt inte nödvändigt att ha en gräns för vilka primtal som används vid faktoriseringen av ett tal. Vi kan skriva

$$a = p_1^{\mu_1} p_2^{\mu_2} \cdots$$

där det är underförstått att nästan alla $\mu_k = 0$.

Exempel 7.2.3. $55 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^0 \cdot \cdots$ ▲

Multiplikation är en mycket simpel operation i denna representation. Då två tal multipliceras adderas multipliciteterna för faktorerna i respektive tal.

Exempel 7.2.4. $12 \cdot 33 = 2^2 \cdot 3^1 \ \cdot \ 3 \cdot 11 = 2^2 \cdot 3^2 \cdot 11$ ▲

Generellt får vi att om

$$a = p_1^{\mu_1} p_2^{\mu_2} \cdots \tag{7.1}$$

och

$$b = p_1^{\nu_1} p_2^{\nu_2} \cdots \tag{7.2}$$

så gäller

$$a^2 = p_1^{2\mu_1} p_2^{2\mu_2} \cdots$$

och

$$a \cdot b = p_1^{\mu_1+\nu_1} p_2^{\mu_2+\nu_2} \cdots .$$

Detta synsätt, och exemplet ovan, kan tyckas onödigt. Vad har man för nytta av att först faktorisera tal, sedan addera multipliciteterna för faktorerna?

Det kan tyckas omständigt, men detta är dels en grund för att förstå en hel del andra begrepp, dels kommer du stöta på andra mängder med samma algebraiska struktur som heltalen där det är mycket viktigt vilka faktorer olika element har.

Begreppet delare får i alla fall någon slags konkretisering med denna typ av representation.

Om $d \mid a$ ”innehåller” a alla faktorer[4] som d består av.

Hur är det med addition då? Kan man inte skriva tal som summan av andra tal också? Behövs verkligen två operationer då multiplkation kan ses som en upprepad addition?

Jo, men det är faktiskt mycket mer komplicierat. Även om vi begränsar oss till positiva heltal kan tal skrivas som summan av andra tal på väldigt många sätt. Uppdelningen i termer är alltså inte unik.

Exempelvis finns 7 sätt att skriva talet 5:

$$\begin{aligned} 5 &= 5+0 \\ &= 4+1 \\ &= 3+2 \\ &= 3+1+1 \\ &= 2+2+1 \\ &= 2+1+1+1 \\ &= 1+1+1+1+1+1. \end{aligned}$$

Dessutom är vi intresserade av en generell teori som gäller annat än heltal. Du har säkert stött på uttryck som

$$(x+3)+(2x-5) = 3x-2.$$

Uttrycken i vänster led kan adderas vilket resulterar i summan i högerledet. Om vi däremot studerar uttrycket

$$(x+3)\cdot(2x-5) = 2x^2+x-15$$

förstår vi att vi aldrig kan få termer som innehåller x^2 genom att summera ett antal termer av typen $ax+b$.

När man räknar med annat än heltal är multiplikation varkligen något annat än upprepad addition.

Det finns också fall där addition har den geometriska tolkningen *förlyttning* medan multiplikation tolkas som en *skalning*, *rotation* eller *spegling*. I dessa fall kan inte upprepade additioner bli en multiplikation.

7.3 Några satser om delare

Det är alltså ofta nödvändigt att kunna dela upp tal i delar. Vi fortsätter på det temat för olika sammansättningar av tal.

Sats 7.3.1. *Om d delar a och d delar b gäller även att d delar summan $a+b$.*

Med symbolspråk: $d \mid a \wedge d \mid b \Rightarrow d \mid a+b$

Bevis. Eftersom $d \mid a$ finns något tal q_1 så att $a = q_1 d$. Eftersom $d \mid b$ finns något tal q_2 så att $b = q_2 d$. Vi får då att $a+b = q_1 d + q_2 d = d(q_1+q_2)$ vilket visar att $d \mid a+b$. □

[4]Vi använder inte ordet *primtal* i denna typ av uttalanden. För heltal är faktorer och primtal samma sak, men i högre matematik kommer du se att man kan räkna med annat än heltal, men på samma sätt som man räknar med heltal. Då är det bättre att väja sig vid ordet faktor istället för primtal.

Intuitivt är det bra om man "ser" att om både a och b delas av d betyder det att både a och b delvis innehåller samma faktorer som d. Denna gemensamma klump faktorer kan brytas ut ur summan $a + b$.

Observera att omvändningen till satsen inte gäller. Till exempel gäller $5 \mid 8+2$, men uppenbart gäller varken $5 \mid 8$ eller $5 \mid 2$. Däremot kan man formulera följande sats, som vi kommer att ha nytta av.

Sats 7.3.2. *Om $d \mid a$ och $d \mid a + b$ gäller $d \mid b$.*

Med symbolspråk: $d \mid a \wedge d \mid a + b \Rightarrow d \mid b$

Bevis. Eftersom $d \mid a$ finns något tal q_1 så att $a = q_1 d$. Eftersom $d \mid a+b$ finns något tal q_2 så att $a + b = q_2 d$. Därför gäller

$$\begin{aligned} a + b &= q_2 d \\ b &= q_2 d - a \\ b &= q_2 d - q_1 d \\ b &= (q_2 - q_1) d \end{aligned}$$

vilket visar att $d \mid b$. □

Följande satser är på samma tema och bevisas snarlikt.

Övning 4 **Sats 7.3.3.** *Om $d \mid a$ och $d \mid b$ gäller $d \mid ab$.*

Med symbolspråk: $d \mid a \wedge d \mid b \Rightarrow d \mid ab$

Övning 5 **Sats 7.3.4.** *Om $d \mid a$ och $d \mid b$ gäller $d^2 \mid ab$.*

Med symbolspråk: $d \mid a \wedge d \mid b \Rightarrow d^2 \mid ab$

Övning 6 **Sats 7.3.5.** *Om $d \mid a$ och $c \mid b$ gäller $cd \mid ab$.*

Med symbolspråk: $d \mid a \wedge c \mid b \Rightarrow cd \mid ab$

7.4 Antalet primtal

Det finns oändligt många tal. Är det då självklart att det finns oändligt många primtal? Nej, varför skulle det inte räcka med ett ändligt antal, som kan kombineras på ett oändligt antal sätt? Det kan man kanske tycka, men så är det inte. Man kan visa att följande är sant.

Sats 7.4.1. *Det finns oändligt många primtal.*

Nedan följer beviset för denna sats. Därefter några exempel på hur beviset skall tolkas.

Bevis. Antag att det finns ändligt många primtal, n st, $p_1 = 2, p_2 = 3, p_3 = 5, \cdots, p_n$. Nu bildar vi ett tal P som är produkten av alla dessa, $P = p_1 \cdot p_2 \cdot \cdots \cdot p_n = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_n$.

Bilda nu talet $q = P + 1$. Eftersom vi har förutsatt att det finns ett ändligt antal primtal kan q inte vara ett nytt primtal. Därför finns det ett primtal p som delar q. Naturligtvis gäller $p \mid P$. Enligt sats 7.3.2 gäller därför $p \mid 1$ vilket inte kan stämma. Slutsatsen blir därför att det inte kan finnas ändligt många primtal. □

Exempel 7.4.2. Om det bara skulle ha funnits tre primtal, 2, 3 och 5 skulle vi alltså ha bildat produkten av dessa, $2 \cdot 3 \cdot 5 = 30$, och sedan adderat 1, $30 + 1 = 31$, vilket är ett primtal.

Tänk igenom att man lika gärna skulle ha kunnat subtrahera 1 och också fått ett primtal, $30 - 1 = 29$. ▲

Exempel 7.4.3. Om det bara skulle ha funnits sex primtal, 2, 3, 5, 7, 11 och 13 skulle vi ha bildat $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$ och sedan $30030 + 1 = 30031$, som inte är ett nytt primtal.

Däremot är 30031 delbart med två primtal som inte är två av de ursprungliga sex, $30031 = 59 \cdot 509$

Man får alltså inte per automatik nya (riktiga) primtal med denna metod, men man kan bilda tal som inte är delbara med de ursprungliga primtalen. ▲

7.5 Faktorisering i praktiken

Små tal kan ofta faktoriseras endast genom att man kommer ihåg multiplikationstabellen och använder den baklänges.

Det är lätt att se att $56 = 7 \cdot 8 = 2^3 \cdot 7$. Däremot är det kanske mindre uppenbart att $2993 = 41 \cdot 73$ eller att $22770 = 2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 23$. Skall sådana tal faktoriseras är det bäst att ta en dator till hjälp.

Däremot finns det vissa knep att ta till. Alla jämna tal är exempelvis delbara med 2 (detta skall utvidgas till en definition senare, se 8.4.5). Till exempel gäller $206 = 2 \cdot 103$. För andra tal kan följande satser vara till hjälp.

Sats 7.5.1. *Tal vars siffersumma har delaren* 3*, har också själv delaren* 3*.*

Vi skall bevisa denna sats, men för att det skall bli lättare att följa beviset tas först ett exempel.

Exempel 7.5.2. Vi undersöker om $3 \mid 846$. Eftersom talet 846 är skrivet i basen 10 gäller

$$\begin{aligned} 846 &= 8 \cdot 100 + 4 \cdot 10 + 6 = \\ &= 8 \cdot 10^2 + 4 \cdot 10 + 6 = \\ &= 8 \cdot (9+1)^2 + 4 \cdot (9+1) + 6 = \\ &= 8 \cdot (9^2 + 2 \cdot 9 + 1) + 4 \cdot (9+1) + 6 = \\ &= (8 \cdot 9^2 + 8 \cdot 2 \cdot 9 + 4 \cdot 9) + (8 + 4 + 6). \end{aligned}$$

Alla termer i den en första parentesen innehåller faktorn 9 och därmed faktorn 3. Om hela talet skall innehålla faktorn 3 måste alltså summan i den andra parentesen, talets siffersumma, innehålla faktorn 3. ▲

Om troliggörandet ovan skall finslipas så att det blir ett formellt bevis måste detta hantera ett godtyckligt tal.

Bevis. Låt talet uttryckas med siffrorna $s_n s_{n-1} \dots s_0$. Vi skall nu visa att talet är delbart med tre (eller nio) om $s_n + s_{n-1} + \cdots s_1 + s_0$ är delbart med tre (eller nio). Eftersom talet är skrivet i basen tio gäller

$$\begin{aligned} s_n s_{n-1} \dots s_0 &= s_n \cdot 10^n + s_{n-1} \cdot 10^{n-1} + \cdots + s_1 \cdot 10 + s_0 = \\ &= s_n \cdot (9+1)^n + s_{n-1} \cdot (9+1)^{n-1} + \cdots + s_1 \cdot (9+1) + s_0 = \\ &= (\text{Termer som innehåller faktorn } 9) + (s_n + s_{n-1} + \cdots + s_0). \end{aligned}$$

Alla termer i den första parentesen uppkommer då alla $(9+1)$ multiplicerars ihop när någon 9:a används. Jämför med uttrycket $(8 \cdot 9^2 + 8 \cdot 2 \cdot 9 + 4 \cdot 9)$ i exemplet ovan. Det är möjligt att bilda ett precist uttryck för dessa termer, men det faller lite utanför denna texts intentioner.

Den sista termen uppkommer då alla 1:or används i alla $(9+1)$. Denna term är just talets siffersumma. Vi ser alltså att en förutsättning för att ett tal skall vara delbart med tre är att dess siffersumma skall vara delbar med tre. □

Exempel 7.5.3. $12 = 2^2 \cdot 3$ 12 har siffersumman 3. ▲

Exempel 7.5.4. $2118 = 2 \cdot 3 \cdot 353$ 2118 har siffersumman 12 ▲

Övning 7

Sats 7.5.5. *Tal vars två sista siffror är delbara med* 4*, är delbara med* 4*.*

Följande exempel kan tjäna som idéskiss för beviset av satsen.

Exempel 7.5.6. $34564 = 345 \cdot 100 + 64 = 345 \cdot 25 \cdot 4 + 16 \cdot 4 = 4 \cdot (345 \cdot 25 + 16) = 4 \cdot 8641$. ▲

Följande sats är du nog bekant med. Försök bevisa den själv. Det går till som i satsen ovan.

Övning 8

Sats 7.5.7. *Tal som slutar på* 0 *eller* 5 *har delaren* 5*.*

Till sist finns ett resultat som rör tal delbara med 9.

Sats 7.5.8. *Tal vars siffersumma har delaren* 9*, har också själv delaren* 9*.*

Beviset för denna sats är samma som beviset för sats 7.5.1.

Dessa satser är de enklaste satserna om faktorisering. Det finns fler satser som är tillämpbara i olika sammanhang, men de blir allt mer jobbiga att använda och allt mer begränsade till en mindre grupp tal.

Faktum är att det inte finns något smart sätt att faktorisera stora tal. Den som kommer på det kommer antingen bli mycket rik och berömd eller mördad. Att detta är svårt är nämligen mycket viktigt vid kryptering och dekryptering.

Om någon löste detta problem skulle vi inte kunna använda dagens metod för att kryptera information vid kommunikation mellan till exempel en bankomat och banken. Hela IT-samhället bygger (i dagsläget) på att detta problem inte löses.

En organisation som lägger mycket resurser på att finna en metod för att faktorisera stora tal snabbt är NSA, National Security Agency, i USA. Vem vet, kanske har de redan lyckats!

7.6 Största gemensamma delare

Två tal kan naturligtvis ha samma delare. Ofta är det intressant att försöka hitta den största gemensamma delaren till två tal.

Exempel 7.6.1. Talen 84 och 90 har båda delarna 2, 3 och 6. Däremot har 84 bland annat delaren 12, vilket inte 90 har. ▲

Definition 7.6.2. Talet $d > 0$ är den **största gemensamma delaren** till a och b, båda inte noll, om

1. $d \mid a$ och $d \mid b$,
2. $c \mid a$ och $c \mid b \Rightarrow c \mid d$.

Vi skriver $\text{sgd}(a, b) = d$. ▲

På engelska heter detta begrepp **greatest common divisor** vilket förkortas gcd. Övning 9

En metod för att hitta den största gemensamma delaren till två tal är att studera faktoriseringen av talen.

Sats 7.6.3. *Den största gemensamma delaren till två tal är produkten av alla faktorer som finns i båda talen.*

Exempel 7.6.4. Vilken är den största gemensamma delaren till talen 12 och 18?

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ 18 &= 2 \cdot 3 \cdot 3 \\ \text{sgd}(12, 18) &= 2 \cdot 3 = 6 \end{aligned}$$

Om man skriver ut alla faktorer och ställer dem under varandra som exemplet visar, är det lätt att se vilka faktorer som är gemensamma. Talen 12 och 18 har alltså båda faktorerna 2 och 3 vilket ger att deras största gemensamma delare är 6. ▲

Exempel 7.6.5. Vilken är den största gemensamma delaren till talen 210 och 220?

$$\begin{aligned} 210 &= 2 \cdot 3 \cdot 5 \cdot 7 \\ 220 &= 2 \cdot 2 \cdot 5 \cdot 11 \\ \text{sgd}(210, 220) &= 2 \cdot 5 = 10 \end{aligned}$$

▲

Uttryckt på faktorform får vi att med a och b som i (7.1) respektive (7.2) så gäller

$$\text{sgd}(a, b) = p_1^{\min(\mu_1, \nu_1)} p_2^{\min(\mu_2, \nu_2)} \cdots .$$

7.7 Minsta gemensamma multipel

Definition 7.7.1. Ett tal a är en **multipel** av b om det finns ett tal m skiljt från noll så att $a = m \cdot b$.

Med symbolspråk: a är en multipel av $b \Leftrightarrow \exists m \neq 0 : a = bm$ ▲

Exempel 7.7.2. Talen $4, 8, 12, 16, \ldots$ är **multiplar** av talet 4. Definitionen tillåter också negativa multiplar. Exempelvis är -12312545 en multipel av 5. ▲

Ett mycket intressant problem är följande: Vilket är det minsta tal som är multipel av två givna tal? Detta är den **minsta gemensamma multipeln**, mgm, till de båda talen.

Exempel 7.7.3. Talet $216 = 12 \cdot 18$ är en multipel till både talet 12 och talet 18. Talet 216 är alltså en gemensam multipel till 12 och 18, men det är inte den minsta gemensamma multipeln. ▲

Även mgm går att bestämma genom att studera faktoriseringen.

Sats 7.7.4. *Den minsta gemensamma multipeln till två tal är produkten av de faktorer som förekommer någon gång i de båda talens faktorisering.*

Exempel 7.7.5. Vilken är den minsta gemensamma multipeln till talen 12 och 18?

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ 18 &= 2 \cdot \quad 3 \cdot 3 \\ \operatorname{mgm}(12,18) &= 2 \cdot 2 \cdot 3 \cdot 3 = 36 \end{aligned}$$

Det minsta tal som är en multipel av både 12 och 18 är $36 = 3 \cdot 12 = 2 \cdot 18$. ▲

Övning 9

Exempel 7.7.6. Vilken är den minsta gemensamma multipeln till talen 210 och 220?

$$\begin{aligned} 210 &= 2 \cdot \quad \cdot 3 \cdot 5 \cdot 7 \\ 220 &= 2 \cdot 2 \quad \cdot 5 \cdot \quad 11 \\ \operatorname{mgm}(210,220) &\quad 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4620 \end{aligned}$$

Det minsta tal som är en multipel av både 210 och 220 är $4620 = 22 \cdot 210 = 21 \cdot 220$.
▲

Uttryckt på faktorform får vi att med a och b som i (7.1) respektive (7.2) så gäller

$$\operatorname{mgm}(a,b) = p_1^{\max(\mu_1,\nu_1)} p_2^{\max(\mu_2,\nu_2)} \cdots .$$

Det finns ett samband mellan den största gemensamma delaren till två tal och talens minsta gemensamma multipel.

Övning 11

Sats 7.7.7. *För två tal a och b gäller $a \cdot b = \operatorname{sgd}(a,b) \cdot \operatorname{mgm}(a,b)$.*

Bevis. Vänsterledet ges av

$$a \cdot b = p_1^{\mu_1+\nu_1} p_2^{\mu_2+\nu_2} \cdots$$

och högerledet av

$$\operatorname{sgd}(a,b) \cdot \operatorname{mgm}(a,b) = p_1^{\min(\mu_1,\nu_1)+\max(\mu_1,\nu_1)} p_2^{\min(\mu_2,\nu_2)+\max(\mu_2,\nu_2)} \cdots .$$

För varje primtal k blir multiplicieteten i vänsterledet $\mu_k+\nu_k$, medan den i högerledet är $\min(\mu_k,\nu_k)+\max(\mu_k,\nu_k)$, men summan av det största och det minsta av μ_k och ν_k är $\mu_k+\nu_k$. Därför är vänsterledet lika med högerledet. □

Den uppmärksamme läsaren har kanske noterat att det aldrig gavs en precis definition av mgm. Den skulle till sin utformning likna definitionen av sgd, vara en uppradning av krav på mgm i stil med att det skall vara en multipel av två tal och dessutom det minsta sådana tal. Om man vill kan man ta sats 7.7.7 som definition av mgm.

7.8 Tal som är relativt prima

Definition 7.8.1. Två tal är **relativt prima** om de saknar gemensamma faktorer.
▲

Övining 13

Detta betyder att deras största gemensamma delare är 1 och deras minsta gemensamma multipel är deras produkt.

Med vår vanliga notation för multipliciteter gäller

$$\begin{aligned} \mu_k \neq 0 &\Rightarrow \nu_k = 0 \\ \nu_k \neq 0 &\Rightarrow \mu_k = 0 \end{aligned}$$

om a och b är relativt prima.

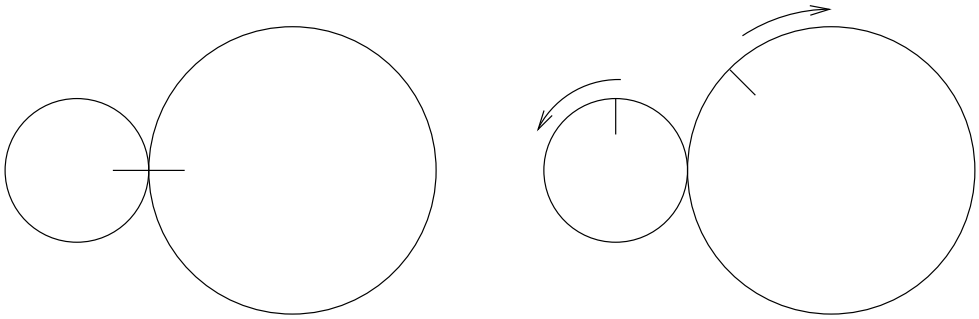
Exempel 7.8.2. Talen $33 = 3 \cdot 11$ och $35 = 5 \cdot 7$ är relativt prima. Vidare gäller $\operatorname{sgd}(33,35) = 1$ och $\operatorname{mgm}(33,35) = 33 \cdot 35 = 1155$. ▲

Två primtal är naturligtvis alltid relativt prima.

7.9 Tillämpningar

Övning 10

Ett sätt att få en bild av begreppet minsta gemensamma multipel är att tänka sig två hjul som ligger an mot varandra och där man markerat kontaktpunkten, som i den vänstra bilden nedan.



Om vi tänker oss att det mindre hjulet driver det större, kommer det större inte rotera lika fort som det mindre. Frågan är hur många varv som de båda hjulen måste rotera innan markeringarna åter igen står mitt för varandra.

Detta kommer att ske då båda markeringarna har färdats en sträcka som är den minsta gemensamma multipeln av de båda hjulens omkrets.

Om hjulens radier är r_1 respektive r_2 och antalet varv som krävs är n_1 respektive n_2 gäller

$$r_1 n_1 = r_2 n_2.$$

Om r_1 och r_2 inte innehåller speciellt många gemensamma faktorer, så måste n_1 och n_2 kompensera för detta och blir då stora. Om r_1 och r_2 är relativt prima gäller $n_1 = r_2$ och $n_2 = r_1$.

Ett mycket viktigt skäl till att öva sig till att bli duktig på att faktorisera tal och ta fram största gemensamma delaren och minsta gemensamma multipeln till par av tal, är att annan matematik blir enklare då.

Till exempel är det som brukar kallas för minsta gemensamma nämnaren till två bråk, i själva verket just den minsta gemensamma multipeln till nämnarna.

Exempel 7.9.1. Beräkna $\frac{5}{12} + \frac{7}{18}$.

$$\frac{5}{12} + \frac{7}{18} = \frac{5 \cdot 3}{12 \cdot 3} + \frac{7 \cdot 2}{18 \cdot 2} = \frac{15}{36} + \frac{14}{36} = \frac{19}{36}$$

De tal man förlänger med för att få lika nämnare är just de saknade faktorerna. ▲

När man förkortar ett bråk är det just den största gemensamma delaren till täljare och nämnare man delar med.

Exempel 7.9.2. Förkorta 48/36 så mycket som möjligt.

$$\frac{48}{36} = \frac{4 \cdot 12}{3 \cdot 12} = \frac{4}{3}$$

▲

Ett annat exempel då denna teori kommer till användning är då man skall bryta ut den största gemensamma faktorn ur ett uttryck.

Exempel 7.9.3. Bryt ut största möjliga faktor ur uttrycket $18x + 12y$.

$$18x + 12y = 6 \cdot 3x + 6 \cdot 2y = 6\,(3x + 2y)$$

▲

Naturligtvis finns fler och mer avancerade exempel. I högre kurser i matematik på gymnasiet kommer denna teori inte bara tillämpas på tal, utan även på variabler och polynom.

7.10 Övningar

1. Visa att $7 \mid 21$.
2. Bestäm alla positiva delare till 108.
3. Vilket är det minsta tal som har multipliciteten 5 för en av sina faktorer.
4. Bevisa sats 7.3.3.
5. Bevisa sats 7.3.4.
6. Bevisa sats 7.3.5.
7. Bevisa sats 7.5.5.
8. Bevisa sats 7.5.7.
9. Bestäm den största gemensamma delaren och minsta gemensamma multipeln till 2475 och 2310.
10. Två kugghjul som har 252 respektive 120 kuggar är monterade så att det ena driver det andra. Det finns markeringar på hjulen som då och då står mitt för varandra. Hur många varv måste hjulen snurra mellan två sådana tillfällen?
11. Bevisa sats 7.7.7.
12. Visa att produkten av tre på varandra följande tal är delbar med 6.
13. Är talen 13129472834700875 respektive 17081038401340 relativt prima?
14. Visa att $2 \mid n^2 + n \ \ \forall \ \ n \in \mathbb{Z}$.

    Nya övnignar som inte har införts på rätt ställe.

15. Bevisa att för $p \in \mathbb{P}$, $p \geq 5$ gäller $24 \mid p^2 - 1$
16. Gäller $n^2 + n + 41 \in \mathbb{P}$ för alla $n \in \mathbb{Z}^+$?

Facit

1. Observera att det korrekta beviset för detta är att det finns ett tal q så att $21 = 7q$, nämligen $q = 3$. Att svara ”3” eller ”21/7 = 3” är felaktiga svar på denna övning.
2. $D_{108} = \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$
3. Det är $2^5 = 32$.
4. Beviset är nästan identiskt med det för sats 7.3.1.
5. Beviset är nästan identiskt med det för sats 7.3.1.
6. Beviset är nästan identiskt med det för sats 7.3.1.

7. -

8. -

9. $\text{sgd}(2310, 2475) = 165$ och $\text{mgm}(2310, 2475) = 34650$.

10. Minsta gemensamma multipeln för kuggarna är 2520. Det betyder att det mindre hjulet måste snurra 21 varv och det större 10 varv.

11. Tips: Resonera om de ingående faktorerna i respektive led.

12. Varannat tal är delbart med två och var tredje med tre. Har man tre på varandra följande tal är minst ett därför jämnt och ett delbart med tre. Deras produkt blir därför delbar med 6 enligt sats 7.3.5.

13. Nej, båda är delbara med 5.

14. Bryt ut ett n. Då fås $n^2 + n = n(n+1)$. En av dessa faktorer är jämn eftersom n och $n+1$ är två på varandra följande tal.

    Nya övnignar som inte har införts på rätt ställe.

15. Vi har att $p^2 - 1 = (p-1)(p+1)$. Eftersom detta är två på varandra följande jämna tal (primtal är udda!) så måste ett av dem vara delbart med 4 och det andra med två. Dessutom är $p-1$, p, $p+1$ tre på varandra följande tal, så ett av dem är delbart med 3. Det kan inte vara p eftersom $p \in \mathbb{P}$. Sammantaget har vi alltså att multipliciteten för 2 minst är tre och vi har minst en faktor 3. Det betyder att $p^2 - 1$ är delbart med 24.

16. Nej, välj $n = 41$ så innehåller alla termer faktorn 41 som kan brytas ut. Uttrycket är dock intressant eftersom det ger primtal för så många n. Försök att skriva om uttrycket på något smart sätt för $n = 40$ för att se att detta värde på n inte heller ger något primtal. Undersök kvoten mellan n och antalet värden på n som ger primtal. Först vid $n = 2337$ är andelen primtal som fås med uttrycket mindre än 50%!

8 Finns division?

Ovan nämns att orden faktor och delare är synonymer om man inte menar just primtalsfaktor då man säger faktor. Exempelvis säger vi att talet 7 är en faktor i talet 42 eftersom $42 = 6 \cdot 7$. Vi säger också att talet 7 delar talet 42 med kvoten 6. Hur hade det blivit om divisionen inte hade gått jämnt upp? Kom ihåg att vi ännu så länge bara sysslar med heltal!

Det vore inte så praktiskt att ha en matematik där vissa räkneoperationer bara gäller vissa par av tal. I så fall skulle man till exempel få dela 42 med 7, men inte med 11. Så kan man inte ha det! Vi skall se hur man kan komma runt problemet och ändå prata om division av heltal trots att det egentligen inte går.

8.1 Kvot och rest

Sats 8.1.1. *För varje par av tal a och n finns ett tal q och ett tal r så att $a = qn + r$ och $0 \leq r < n$.*

Definition 8.1.2. Satsen ovan beskriver **euklidisk division**. Talet a benämns **dividend**, n benämns **divisor**, q benämns **kvot** och r benämns **rest**. Divisionen sägs gå **jämnt upp** om resten blir noll. ▲

Övning 1

Exempel 8.1.3. Om 42 delas med 11 fås kvoten 3 och resten 9 eftersom $42 = 11 \cdot 3 + 9$. Om talet 15 delas med 5 fås kvoten 3 och resten 0 eftersom $15 = 5 \cdot 3 + 0$, divisionen går jämnt upp. ▲

Följande sats är mycket naturlig. Du kanske tycker den är självklar, men den tas ändå upp här eftersom dess motsvarighet vid räkning med polynom kommer att vara mycket viktig.

Sats 8.1.4. *Talet a är en delare till n om och endast om resten blir noll då n delas med a.*

I olika sammanhang kan det vara lika rätt att säga ”talet 11 delar inte talet 42” och ”talet 11 delar talet 42 med resten 9”.

Begreppen kvot och rest dyker upp på ett naturligt sätt i algoritmen för division av tal, vilket följande exempel visar.

$$\begin{array}{r} 172 \\ \hline 1035 \;\big|\; 6 \\ -\,6 \\ \hline 43 \\ -42 \\ \hline 15 \\ -12 \\ \hline 3 \end{array}$$

Resten är det som blir kvar när siffrorna i talet som skall delas tagit slut, här fås resten 3 då 1035 delas med 6.

8.2 Diofantiska ekvationer

Nu skall vi studera ett enkelt exempel på ekvationer med flera variabler där man söker heltalslösningar. De har fått sitt namn efter Diofantos, som var verksam runt 250 e Kr i Alexandria.

I detta avsnitt begränsar vi oss till linjära diofantiska ekvationer med två obekanta.

Definition 8.2.1. En **diofantisk ekvation** är en ekvation i två variabler på formen

$$ax + by = c \tag{8.1}$$

där $a, b \neq 0$, $a, b, c \in \mathbb{Z}$ och där lösningar söks i $\mathbb{Z}$. ▲

Ekvationen $3x + 4y = 5$ är en diofantisk ekvation. Vi kan multiplicira båda led med 2 och får då ekvationen $6x + 8y = 10$, vilken naturligtvis har samma lösningsmängd som den första ekvationen. Vi gör därför följande definition.

Definition 8.2.2. En diofantisk ekvation är **primitiv** om

$$\text{sgd}(a, b, c) = 1.$$

▲

Om inget annat sägs är det underförstått att en diofantisk ekvation är primitiv i denna text.

Diofantiska ekvationer har oändligt många lösningar. Övning 2

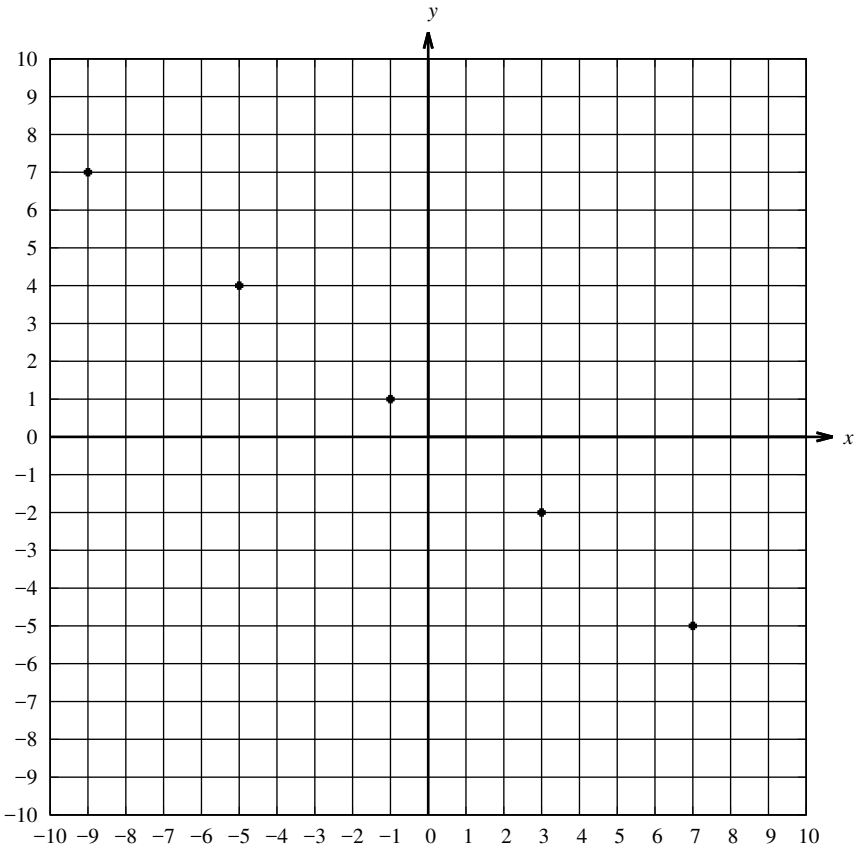
Sats 8.2.3. *Om paret* (x_0, y_0) *är en lösning till* (8.1) *så är även paret* $(x_0 + bn, y_0 - an)$ *en lösning för alla* $n \in \mathbb{Z}$.

Övning 3

Innan vi studerar hur man löser diofantiska ekvationer skall vi belysa några intressanta poänger. Vi tar ekvationen $3x + 4y = 1$ som exempel. Det är lätt att hitta en lösning, exempelvis $(x_0, y_0) = (-1, 1)$.

Sats 8.2.3 ger då att alla lösningar ges av $(x_n, y_n) = (-1 + 4n, 1 - 3n)$.

En grafisk representation av lösningarna ges nedan.



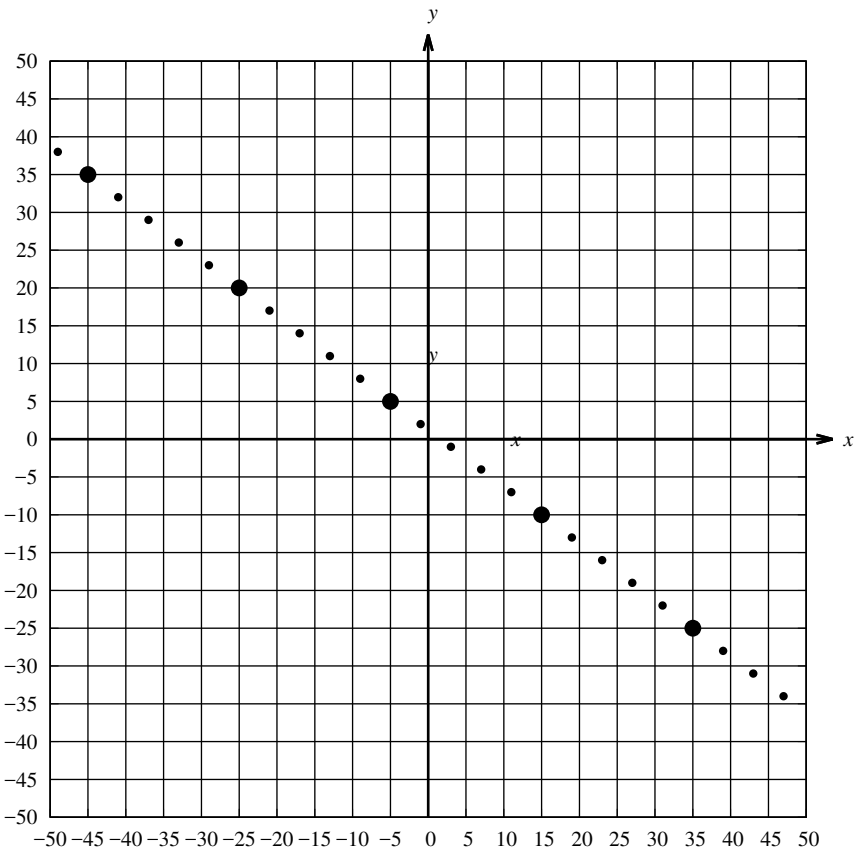
Antag nu att vi vill lösa $3x+4y = 5$. Om man multiplicerar lösningarna till $3x+4y = 1$ med 5 får vi lösningar till vår nya ekvation eftersom

$$3 \cdot 5x_n + 4 \cdot 5y_n = 5$$

då får en faktor 5 som kan strykas från både höger och vänster led.

Notera dock att mängden av alla $(5x_n, 5y_n) = (-5 + 5 \cdot 4n, 5 - 5 \cdot 3n)$ för alla $n \in \mathbb{Z}$ inte är *alla* lösningar till $3x + 4y = 5$. Till exempel är inte $(-1, 2)$ med i denna lösningsmängd.

En grafisk representation av alla lösningar ges nedan. Den delmängd som ges av $(5x_n, 5y_n)$ är markerad med fetare punkter. Observera skalan! Alla lösningar har heltalskoordinater!



Övning 5 Vi har följande sats.

Sats 8.2.4. *Om (x_0, y_0) är en lösning till $ax + by = 1$, så ges lösningarna till $ax + by = c$ av $(c\,x_0 + bn, c\,y_0 - an)$ för alla $n \in \mathbb{Z}$.*

Övning 6 Följande sats handlar om en egenskap för ekvationen om det finns lösningar.

Sats 8.2.5. *Om det finns en lösning till $ax + by = c$, så gäller*

$$\text{sgd}(a, b) = 1.$$

Bevis. Antag att $\text{sgd}(a, b) = s$. Det betyder att det existerar tal q_1 och q_2 så att $a = q_1\,s$ och $b = q_2\,s$. Vi har därför

$$s(q_1 x + q_2 y) = c.$$

Eftersom likheten skall gälla måste $s \mid c$ gälla. Det finns alltså ett q_3 så att $c = q_3\,s$. Talet s delar alltså både a, b och c, men då ekvationen är primitiv måste $s = 1$ gälla. Därmed gäller $\text{sgd}(a, b) = 1$. □

Det är viktigt att förstå att omvändningen till satsen inte är bevisad. Vi vet ännu inte att det finns lösningar om $\text{sgd}(a, b) = 1$, och ännu inte hur de hittas. Om detta handlar kommande avsnitt.

8.3 Euklides algoritm

Det finns en algoritm för att bestämma den största gemensamma delaren till två tal som heter Euklides algoritm. När man använder den får man på köpet lösningarna till diofantiska ekvationer.

Antag att vi vill lösa ekvationen $391x + 160y = 1$.

Vi bildar först kvot och rest då 391 delas av 160,

$$391 = 160 \cdot 2 + 71.$$

Vi bildar sedan en ny kvot och rest då den förra kvoten delas av förra resten. Med steget ovan utskrivet fås

$$\begin{aligned} 391 &= 160 \cdot 2 + 71 \\ 160 &= 71 \cdot 2 + 18 \\ 71 &= 18 \cdot 3 + 17 \\ 18 &= 17 \cdot 1 + 1 \\ 17 &= 1 \cdot 17 + 0. \end{aligned}$$

Eftersom en rest alltid är mindre än det man delar med måste denna process sluta förr eller senare.

Sats 8.3.1. ***Euklides algoritm*** *Den sista nollskillda resten i processen ovan är den största gemensamma delaren till de två ursprungliga talen.*

Bevis. Om $a = bq + r$ gäller $\text{sgd}(a, b) = \text{sgd}(b, r)$. Detta inses genom att skriva $r = a - bq$. Den störste delaren till både a och b måste därför dela r.

För alla steg i algoritmen

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \\ r_n &= r_{n+1}q_{n+2} + r_{n+2} \\ r_{n+1} &= r_{n+2}q_{n+3} + 0 \end{aligned}$$

där r_{n+2} antas vara den sista nollskillda resten, fås alltså

$$\text{sgd}(a, b) = \text{sgd}(b, r_1) = \text{sgd}(r_1, r_2) = \cdots = \text{sgd}(r_{n+1}, r_{n+2}).$$

I sista steget syns att $r_{n+2} \mid r_{n+1}$. Därför gäller $\text{sgd}(r_{n+1}, r_{n+2}) = r_{n+2}$ och därmed $\text{sgd}(a, b) = r_{n+2}$.

□

Vi kan nu lösa vår ekvation genom att använda oss av resultatet ovan. Vi utför på sätt och vis algoritmen baklänges och börjar med att lösa ut 1 ur den näst sista raden. Vi får

$$1 = 18 - 17.$$

Nu kan vi lösa ut 17 ur den tredje raden, $17 = 71 - 18 \cdot 3$ och sätta in i detta uttryck. Vi får

$$1 = 18 - (71 - 18 \cdot 3) = 4 \cdot 18 - 71.$$

Vi löser ut 18 ur rad två, $18 = 160 - 71 \cdot 2$, och sätter in. Vi får

$$1 = 4 \cdot 18 - 71 = 4 \cdot (160 - 71 \cdot 2) - 71 = 4 \cdot 160 - 9 \cdot 71.$$

Till sist gör vi likadant med första raden, $71 = 391 - 160 \cdot 2$, och får

$$1 = 4 \cdot 160 - 9(391 - 160 \cdot 2) = 22 \cdot 160 - 9 \cdot 391.$$

Vi identifierar ur detta steg att $x_0 = -9$ och $y_0 = 22$ löser vår ekvation. Sats 8.2.3 ger att alla lösningar ges av

$$(x_n, y_n) = (-9 + 160n, 22 - 391n) \; \forall \; n \in \mathbb{Z}.$$

Övning 7

Processen ovan är lättare att åskådliggöra om man skriver både Euklides algoritm och lösningen av ekvationen bredvid varandra, vilket visas nedan.

Rad nr	**Euklides algoritm**	**Ekvationens lösning**
1		$1 = 22 \cdot 160 - 9 \cdot 391$
2	$391 = 160 \cdot 2 + 71$	$1 = 4 \cdot 160 - 9 \cdot (391 - 160 \cdot 2)$
3		$1 = 4 \cdot 160 - 9 \cdot 71$
4	$160 = 71 \cdot 2 + 18$	$1 = 4 \cdot (160 - 71 \cdot 2) - 1 \cdot 71$
5		$1 = 4 \cdot 18 - 1 \cdot 71$
6	$71 = 18 \cdot 3 + 17$	$1 = 1 \cdot 18 - 1 \cdot (71 - 18 \cdot 3)$
7		$1 = 1 \cdot 18 - 1 \cdot 17$
8	$18 = 17 \cdot 1 + 1$	$1 = 1 \cdot 18 - 1 \cdot 17$

Börja med att tillämpa Euklides algoritm, men lämna en tom rad (nr 1) och därefter varannan rad tom. Lämna också plats till höger om resultatet, den platsen kommer användas för att lösa ekvationen.

När du kommit till den sista nollskilda resten (här på rad 8) löser du ut den och skriver den likheten till höger.

På ”vägen ned”i Euklides algoritm kan man inte på förhand veta var den skall sluta, så rad 7 i detta exempel visar sig vara onödig, men om det hade blivit en rad 9 och 10 hade nr 7 varit nödvändig.

I kolumnen till höger på rad 6 byts resten 17 ut mot det som fås då 17 löses ut ur liketen till vänster.

Rad 5 finns för att ha någonstans att förenkla likheten så att den innehåller talen 18 och 71 med sina koefficienter (4 respektive -1).

På rad 4 är det dags att lösa ut 18 ur högerkolumnen och byta ut resultatet mot 18 i vänsterkolumnen.

Återigen förenklas resultatet på rad 3 för att bevara resterna från Euklides algorimt, men nu är de 160 respektive 71.

Denna procedur upprepas ”hela vägen upp”. Detta exempel är ganska litet (få rader), så redan på rad 2 byts den första resten från Euklides algorimt (71) ut mot det önskade slutresultatet.

På rad 1 identifieras en lösning till ekvationen eftersom vi nu ser att koefficienten framför 160 är 22 och koefficienten framför 391 är -9.

Observera hur tydligt det blir om man lämnar plats för kommande utbyten på vägen upp och skriver alla multiplikationstecken, minustecken och koefficienter under (eller, efterom vi är på väg upp”, över) varandra.

Detta var bara ett exempel, men vi formulerar metoden ovan som en sats.

Sats 8.3.2. *Om $c = \text{sgd}(a, b)$ existerar det ett par (x, y) så att ekvationen $ax+by = c$ har en lösning.*

Bevis. Vi fortsätter med notationen från beviset av sats 8.3.1.

Vi uttrycker $r_{n+2} = r_n - r_{n+1}q_{n+2}$. Vi kan i detta substituera r_{n+1} med hjälp av (den icke utskrivna) tredje sista raden. På detta sätt kan man forsätta till dess till dess r_{n+2} är uttryckt på formen $ax + by$. □

8.4 Modulär aritmetik

Inom talteorin är det ofta intressant att "räkna med rester". Det man menar då är att man betraktar alla tal som ger samma rest vid division med något tal som "samma tal", eller ekvivalenta tal.

Exempel 8.4.1. Talet 18 ger resten 3 då det delas med 5. Det gör talet 23 också. Man använder då skrivsättet $23 \equiv 18 \pmod 5$. Detta utläses "23 är kongruent med 18 modulo 5". ▲

Vi preciserar detta.

Definition 8.4.2. Talen a och b är **kongruenta modulo** n om det finns ett tal q så att $a - b = qn$.

Med symbolspråk: $a \equiv b \pmod n \Leftrightarrow n \mid a - b$ ▲

Övning 8

Den här lilla texten kan inte göra rättvisa åt detta begrepp. Vi skall avnända oss av ett konkret resultat i endast ett bevis längre fram. Innan dess måste vi se hur man räknar. Övning 9

Exempel 8.4.3. Om vi vill beräkna $18+24 \pmod 5$ kan vi först beräkna $18+24 = 42$ och sedan beräkna $42 \equiv 2 \pmod 5$. Vi kan istället beräkna $18 \equiv 3 \pmod 5$ och $24 \equiv 4 \pmod 5$ och sedan $3 + 4 = 7 \equiv 2 \pmod 5$, eller kortare $18 + 24 \equiv 3 + 4 \equiv 2 \pmod 5$.

Detsamma gäller multiplikation: $18 \cdot 24 = 432 \equiv 2 \pmod 5$, eller enklare $18 \cdot 24 \equiv 3 \cdot 4 = 12 \equiv 2 \pmod 5$ ▲

Vi generaliserar detta till följande sats.

Sats 8.4.4. *Om* $a \equiv b \pmod n$ *och* $c \equiv d \pmod n$ *gäller* $a + c \equiv b + d \pmod n$ *och* $a \cdot c \equiv b \cdot d \pmod n$.

Den sats vi kommer att använda oss av i ett kommande bevis är den som snart följer. För att denna text skall vara konsistent måste vi dock först definiera vad som menas med ett jämnt tal.

Definition 8.4.5. Ett tal n är **jämnt** om det innehåller en faktor 2. Då finns ett tal m så att $n = 2m$. Talet 0 definieras som jämnt. Tal som inte är jämna är **udda** och går att skriva som $2m + 1$ för något m. ▲

Vi återkommer till jämna och udda tal senare.

Sats 8.4.6. *Om* a *är jämnt gäller* $a^2 \equiv 0 \pmod 4$ *och om* a *är udda gäller* $a^2 \equiv 1 \pmod 4$.

Bevis. Om a är jämnt gäller enligt definition 8.4.5 att a går att skriva $a = 2n$ för något n. Vi får då $a^2 = (2n)^2 = 4n^2 \equiv 0 \pmod 4$.

Om a är udda gäller enligt definition 8.4.5 att a går att skriva $a = 2n + 1$ för något n. Vi får då $a^2 = (2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4$. □

En följd av denna sats är alltså att $a^2 \equiv 2 \pmod 4$ eller $a^2 \equiv 3 \pmod 4$ *inte* kan gälla för något tal.

8.5 Ekvationer i $\mathbb{Z}_n$

Nu skall vi återkomma till talmängden $\mathbb{Z}_n$ och förklara resultaten i avsnitt 3.4.

Definition 8.5.1. Talmängden $\mathbb{Z}_n$ består av alla heltal $0, 1, \ldots n-1$ där vi definierar addition och multiplikation enligt

$$\begin{aligned} a+b &= c \\ a \cdot b &= c \end{aligned}$$

där c är resten som fås då $a+b$ och $a \cdot b$ beräknas i $\mathbb{Z}$ och delas med n. ▲

Observera att $\mathbb{Z}_n$ i någon mening är en "egen liten värld" som egentligen inte har med heltalen att göra på annat sätt att heltalen används för att definiera $\mathbb{Z}_n$. Begrepp som primtal och största gemensamma delare är definierat i $\mathbb{Z}$ och vi vet (ännu) inte om de motsvaras på ett naturligt sätt i $\mathbb{Z}_n$. Det är som att vi tagit schackpjäser och hittat på ett nytt spel med dessa.

Vi börjar med att notera att faktorisering inte är entydig i $\mathbb{Z}_n$. I $\mathbb{Z}_{12}$ gäller till exempel

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 6 &= 6 \cdot 3. \end{aligned}$$

Vi har ju bevisat att faktorisering är entydig i $\mathbb{Z}$, så nu måste vi studera vilken detalj i det beviset som inte gäller i $\mathbb{Z}_{12}$. Den operation som görs i beviset som inte gäller i $\mathbb{Z}_n$ är kancelleringslagen. Från exemplet ovan ser vi att $2 \cdot 3 = 6 \cdot 3$, men $2 \neq 6$. Generellt gäller följande sats.

Sats 8.5.2. *Om det finns två tal $a \neq 0$ och $b \neq 0$ i en ring[5] för vilka det gäller att $ab = 0$, så gäller inte kancelleringslagen i ringen.*

Eftersom till exempel $6 \cdot 2 = 0$ i $\mathbb{Z}_{12}$ så gäller alltså inte kancelleringslagen i $\mathbb{Z}_{12}$.

Nu skall vi återkomma till "ekvationerna på en klocka" vi hade i avsnitt 3.4. Alla tal har som sagt additativ invers i $\mathbb{Z}_n$, men bara vissa tal har multiplikativ invers. Vi såg att vi i $\mathbb{Z}_{12}$ inte kunde lösa ekvationen

$$3x = 6$$

då 3 saknar muliplikativ invers i $\mathbb{Z}_{12}$ medan ekvationen

$$5x = 4$$

gick att lösa då 5 har invers, nämligen 5.

Generellt gäller följande sats.

Sats 8.5.3. *Endast tal som är relativt prima med n har multiplikativ invers i $\mathbb{Z}_n$.*

Bevis. Om a är given och vi söker dess multiplikativa invers b skall alltså $ab = 1$ gälla. Det betyder att $ab \equiv 1 \pmod{n}$ i $\mathbb{Z}$. Detta betyder per definition att

$$ab = 1 + qn$$

för något tal q. De obekanta i denna diofantiska ekvation är b och q, och ekvationen har en lösning om $\text{sgd}(a, n) = 1$, vilket betyder att a och n skall vara relativt prima. □

[5]För definition av en **ring**, se 12.2.1.

En följd av denna sats är att $\mathbb{Z}_p$ är en kropp[6]. Om ett tal $a \geq 0$ är mindre än p är a och p relativt prima. Med symbolspråk kan detta skrivas

$$a \in \mathbb{Z}^+ \wedge a < p \Rightarrow \text{sgd}(a, p) = 1.$$

Detta betyder att alla element i $\mathbb{Z}_p$ har mulitplikativ invers och $\mathbb{Z}_p$ är därmed en kropp.

8.6 Mikrotillämpning

Begreppet relativt prima tal har en tillämpning i problem av följande typ. Om du har en hink som rymmer 3 liter och en som rymmer 5 liter, hur kan du då kombinera dessa så att du får en liter vatten (förutsatt att du har någonstans att hälla vattnet och att du har en kran som du kan tappa oändligt mycket vatten ur om du skulle behöva)?

Lösningen är att du mäter upp två fulla hinkar om 5 liter och från detta tar bort tre fulla hinkar om 3 liter, då får du en liter kvar: $2 \cdot 5 - 3 \cdot 3 = 1$.

Detta var möjligt endast eftersom hinkarnas volymer var relativt prima. Du skulle aldrig kunna bilda en liter genom att använda hinkar om t ex 6 och 4 liter. Däremot skulle du kunna bilda två liter vatten eftersom $\text{sgd}\,(4, 6) = 2$.

8.7 Finaltillämpning

Nu har vi all teori för att lösa den sorts problem som beskrevs i inledningen, avsnitt 3.4.

Antag att vi vill hitta den multiplikativa inversen till 17 i $\mathbb{Z}_{47}$. Det betyder att vi vill lösa ekvationen

$$17 \cdot x = 1$$

i $\mathbb{Z}_{47}$. Det betyder i sin tur att vi (per definition) vill lösa den Diofantiska ekvationen

$$17\,x = 1 + 47\,n$$

men vi är bara intresserad av x som uppfyller $0 \leq x < 47$. Vilket värde n får är ointressant.

Eftersom n är okänt och oviktigt kan vi lika gärna skriva denna ekvation

$$17\,x + 47\,n = 1.$$

En lösning är $(x_0, n_0) = (-11, 4)$, men den lösning vi är intresserade av är i detta fall $x_1 = -11 + 47 = 36$.

8.8 Övningar

1. Bestäm kvot och rest då 14 delas med 8.
2. Bevisa sats 8.2.3.
3. Lös $5x + 6y = 1$.
4. Bevisa sats 8.2.4.

[6]För definition av en **kropp**, se 12.3.1.

5. Skriv ned några lösningar till $5x + 6y = 1$ respektive $5x + 6y = 3$ för att illustrera poängen med sats 8.2.4.
6. Försök lös $2x + 4y = 3$ för att beylysa sats 8.2.5.
7. Lös ekvationen $212x + 87y = 1$.
8. Bestäm två tal som är kongruent med $18 \pmod 5$.
9. Bestäm det minsta positiva heltal a så att
$18347183740871348001 \cdot 16294617364066513486344 \equiv a \pmod 2$
10. Bevisa sats 8.4.4.
11. Lär dig beviset till sats 8.4.6 utantill.
12. Visa att $a \in \mathbb{U} \quad \Rightarrow \quad a^2 \equiv 1 \pmod 4$
13. Visa att $a \in \mathbb{U} \quad \Rightarrow \quad a^2 \equiv 1 \pmod 8$
14. Visa att $3 \mid n^3 + n$ för alla $n \in \mathbb{Z}$.
15. Visa att $n^2 \equiv 0 \pmod 3$ eller $n^2 \equiv 1 \pmod 3$ för alla $n \in \mathbb{Z}$.
16. Ange det minsta tal $z > 5$ som uppfyller $z \equiv 5 \pmod 9$.

Facit

1. Kvoten blir 1 och resten 6 eftersom $14 = 1 \cdot 8 + 6$.
2. Ledning: Sätt in de föreslagan lösningarna i ekvationen och förenkla.
3. Lösningarna ges av $(x_n, y_n) = (-1 + 6n, 1 - 5n)$.
4. Ledning: Sätt in de föreslagan lösningarna i ekvationen och förenkla.
5. -
6. Till exempel kan du begrunda att summan av jämna tal knappas kan bli talet 3.
7. Lösningarna ges av $(x_n, y_n) = -16 + 87n, 39 - 212n$.
8. 18 ger resten 3 då det delas med 5. Två andra exempel är 28 och 23.
9. Det andra talet är jämnt, så det är kongruent med noll modulo två. Produkten blir därför noll.
10. -
11. -
12. Om $a \in \mathbb{U}$ kan man skriva $a = 2m + 1 \quad \Rightarrow \quad a^2 = 4m^2 + 4m + 1$ vilket ger $a^2 \equiv 1 \pmod 4$.
13. Om $a \in \mathbb{U}$ kan man skriva $a = 2m+1 \quad \Rightarrow \quad a^2 = 4m^2+4m+1 = 4m(m+1)+1$. Antingen är m eller $m + 1$ jämn vilket ger $a^2 \equiv 1 \pmod 8$.
14. Skriv $n^3 + n = n(n^2 - 1) = n(n - 1)(n + 3)$. Av dessa faktorer är minst en delbar med 3.
15. Undersök vad som händer i de tre fallen $n \equiv 0 \pmod 3$, $n \equiv 1 \pmod 3$ respektive $n \equiv 2 \pmod 3$.
16. $5 + 9 = 13$.

9 Lite om pythagoréernas matematik

9.1 Talmystik

För pythagoréerna var allt tal. Hela deras värld kretsade kring talen som en sorts religion. Tabellen nedan visar på den religiösa innebörden för de några tal.

Tal	**Innebörd**
1	Det som skapar alla andra tal.
2	Det första talet. Representerar motsats. Det första jämna talet. Jämna tal var kvinnliga och udda tal manliga.
3	Det första udda talet. Representerade harmoni.
4	Det första kvadratiska talet. Representerade rättvisa.
5	Representerade äktenskap. Summan av mannen och kvinnan.
6	Representerade skapelse.
7	Heligt eftersom det fanns sju planeter.
10	Det heligaste talet. Universums tal eftersom $1+2+3+4=10$ och *ett* element behövs för att bestämma en punkt, *två* element behövs för att bestämma en linje, *tre* element behövs för att bestämma ett plan och *fyra* element behövs för att bestämma en tetraeder. Triangeltal.

9.2 Jämna och udda tal

Pythagoréerna representerade naturliga tal som ett antal punkter. Ett tal definierades som jämnt om det gick att dela in punktmängden i två lika stora grupper. Ur detta går det att bevisa följande satser.

1. Summan av jämna tal är ett jämnt tal.
2. Summan av ett udda tal och ett jämnt tal är ett udda tal.
3. Summan av två udda tal är ett jämnt tal.
4. (Följdsats) Summan av ett jämnt antal udda tal är ett jämnt tal.
5. Kvadraten av ett jämnt tal är ett jämnt tal och kvadraten av ett udda tal är ett udda tal.

Den moderna definitionen av ett jämnt tal gavs i 8.4.5. Pythagoréerna definierade att ett tal n är **jämnt** om n st föremål kan ordnas i två lika stora grupper. Om inte detta går är n **udda**.

Vår intuitiva uppfattning om tal säger oss naturligtvis att de båda definitionerna är ekvivalenta, de betyder samma sak. Däremot blir bevisföringen lite olika i de båda fallen.

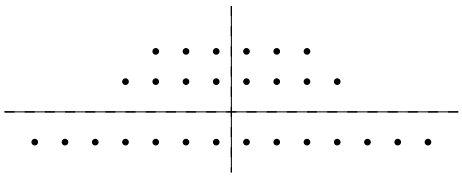
Sats 9.2.1. *Summan av två jämna tal är ett jämnt tal, summan av två udda tal är ett jämnt tal och summan av ett udda och ett jämnt tal är ett udda tal.*

Bevis. Modernt bevis Låt j_1 och j_2 vara två jämna tal och u_1 och u_2 vara två udda tal. Enligt definition 8.4.5 kan man skriva att $j_1 = 2k_1$, $j_2 = 2k_2$, $u_1 = 2v_1 + 1$ och $u_2 = 2v_2 + 1$. Summorna blir då

$$\begin{array}{rcll} j_1 + j_2 & = & 2k_1 + 2k_2 & = & 2\left(k_1 + k_2\right) \\ u_1 + u_2 & = & 2v_1 + 1 + 2v_2 + 1 & = & 2\left(v_1 + v_2 + 1\right) \\ j_1 + u_1 & = & 2k_1 + 2v_1 + 1 & = & 2\left(k_1 + v_1\right) + 1. \end{array}$$

Vi ser alltså att summan av två jämna tal blir jämnt eftersom summan innehåller faktorn 2, liksom summan av två udda tal. Däremot gäller detta inte för summan av ett udda tal och ett jämnt tal.

Pythagoreiskt bevis Följande exempel visar att summan av 6 och 8 är jämn.



Generellt gäller att två jämna tal per definition vardera kan delas upp i två lika stora delar. Talens summa kan då också delas upp i två lika stora delar, båda bildade genom att summera en del från vardera av de två ursprungliga talen.

Om ett udda tal adderas till ett jämn blir det en enhet över som måste läggas till någon av summans delar, som då inte blir lika stora.

Summan av två udda tal blir däremot jämn eftersom det blir två enheter över som kan läggas en till var och en av summans delar. □

Vi kan passa på att formulera ett par användbara satser till.

Sats 9.2.2. *Kvadraten av ett jämnt tal är jämn och kvadraten av ett udda tal är udda.*

Bevis. Vi använder oss av notationen från föregående bevis.

$$\begin{array}{ll} j_1^2 = \left(2k_1\right)^2 = 2 \cdot 2 \cdot k_1^2 & \text{Jämnt} \\ u_1^2 = \left(2v_1 + 1\right)^2 = \left(2v_1\right)^2 + 2 \cdot 2v_1 + 1 = 2\left(2v_1^2 + 2v_1\right) + 1 & \text{Udda} \end{array}$$

□

9.3 Pythagoreisk trippel

Pythagoréerna gillade att gruppera tal som med olika definitioner på något vis hör ihop.

Definition 9.3.1. Trippeln (a, b, c), utgör en **pythagoreisk trippel** om $a^2 + b^2 = c^2$. ▲

Övning 1.

Exempel 9.3.2. Talen $(3, 4, 5)$ utgör en pythagoreisk trippel eftersom $3^2 + 4^2 = 5^2$. Ett annat exempel är $(8, 15, 17)$. ▲

Det är inte så intressant att betrakta till exempel $(6, 8, 10)$ som en ny trippel eftersom denna är bildad ur $(3, 4, 5)$ genom att multiplicera talen med 2. Vi gör därför följande definition.

Definition 9.3.3. En pythagoreisk trippel är **primitiv** om talen i den är relativt prima. ▲

Observera att detta inte har någonting att göra med det som kallas Pythagoras sats. Pythagoréerna, liksom alla grekiska matematiker vid den här tiden, gjorde stor skillnad på geometri och aritmetik. Pythagoras sats var för övrigt känd i Mesopotamien 1500 år innan Pythagoras levde.

Det finns flera formler för att skapa pythagoreiska tripletter. Pythagoréerna kände till följande sats. Övning 2

Sats 9.3.4. *Låt m vara ett positivt udda heltal. Då utgör talen (a, b, c) där* Övning 3 Övning 4 Övning 5

$$\begin{aligned} a &= m \\ b &= \frac{m^2-1}{2} \\ c &= \frac{m^2+1}{2} \end{aligned}$$

en pythagoréeisk trippel.

Platon kände till att man kunde välja (a, b, c) på ytterligare ett sätt.

Sats 9.3.5. *Låt m vara ett positivt heltal. Då utgör talen (a, b, c) där*

$$\begin{aligned} a &= 4m \\ b &= 4m^2-1 \\ c &= 4m^2+1 \end{aligned}$$

en pythagoreisk trippel.

Inget av dessa båda val ger alla pythagoreiska tripletter. Den enda gemensamma de ger är $(3, 4, 5)$. Vill man få alla måste man blanda in fler variabler enligt följande sats.

Sats 9.3.6. *Låt k, m, n vara positiva heltal där $m > n$. Då utgör talen (a, b, c)*

$$\begin{aligned} a &= k\left(m^2-n^2\right) \\ b &= 2kmn \\ c &= k\left(m^2+n^2\right) \end{aligned}$$

en pythagoreisk trippel.

Pythagoréerna var inte de första att intressera sig för dessa tripletter. Babylonierna nedtecknade dem i tabeller på lertavlor som återfunnits. Övning 6

Sats 9.3.7. *I en primitiv pythagoreisk trippel (x, y, z) är precis en av x eller y jämn och z är udda.*

Bevis. Beviset bygger helt på satserna 8.4.6, 9.2.1 och 9.2.2.

Antag först att både x och y är jämna. Då gäller enligt sats 9.2.2 att x^2 och y^2 också är jämna. Enligt sats 9.2.1 blir då även $x^2 + y^2 = z^2$ också jämnt. Eftersom alla tal x, y och z är jämna innehåller alla då en faktor 2 och $\text{sgd}(x, y, z) = 2 \neq 1$. Trippeln (x, y, z) kan då inte vara primitiv.

Antag nu att både x och y är udda. Då gäller enligt sats 8.4.6 att $x^2 \equiv 1 \pmod 4$ och $y^2 \equiv 1 \pmod 4$. Vi får då $x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$. Men $z^2 \equiv 2$ kan inte gälla enligt sats 8.4.6, så detta fall utesluts också.

Kvar blir att en av x eller y är udda. Då är en av x^2 eller y^2 udda enligt sats 9.2.2 och därmed är z^2 ett udda tal enligt sats 9.2.1. Till sist, enligt sats 9.2.2 är då också z udda. □

9.4 Perfekta tal

Definition 9.4.1. Ett tal är **perfekt** om det är lika med summan av alla sina delare. ▲

För att satsen skall äga relevans är det underförstått att endast positiva delare som är mindre än talet själv avses.

Följande exempel var kända under antiken:

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \end{aligned}$$

samt 496 och 8128.

I Elementa IV finns följande sats.

Sats 9.4.2. *Om 2^n-1 är ett primtal är $m = 2^{n-1}(2^n-1)$ perfekt.*

Exempelvis är talet $2^5-1 = 31$ ett primtal. Alltså är talet $2^4(2^5-1) = 16\cdot 31 = 496$ perfekt. Det är oklart om pythagoréerna kände till denna sats, eller om den stammar från Euklides själv.

En reflektion är att alla perfekta tal på formen $2^{n-1}(2^n-1)$ är jämna. Kan möjligen alla jämna perfekta tal skrivas på denna form? Detta visades av Euler på 1700-talet.

Om det existerar udda perfekta tal är fortfarande en obesvarad fråga. Man har dock visat att det inte finns några udda perfekta tal mindre än 10^{300}. Det femte perfekta talet, $33550336 = 2^{12}(2^{13}-1)$, upptäcktes först på 1400-talet.

9.5 Mättade och vänskapliga tal

Definition 9.5.1. Ett tal benämns **mättat** (**omättat**) om summan av talets divisorer blir större (mindre) än talet. Om summan av talets divisorer är precis ett större (mindre) än talet benämns det **svagt mättat** (**svagt omättat tal**). ▲

Pythagoréerna kände till att alla tal på formen 2^n är svagt omättade. Exempelvis har $2^3 = 8$ divisorerna $1, 2$ och 4. Summan $1+2+4 = 7 = 8-1$, 8 är alltså ett svagt omättat tal.

Pythagoréerna hittade aldrig några svagt mättade tal. Det är fortfarande okänt om de existerar.

Definition 9.5.2. Två tal benämns **vänskapliga** om de är summan av varandras divisorer. ▲

Övning 7

Pythagoréerna kände till paret 220 och 284 och kanske fler exempel och tillskrev vänskapliga tal mystiska egenskaper.

En arabisk matematiker vid namn Thābit ibn Qurra (826 – 901 e Kr) formulerade följande sats.

Sats 9.5.3. *Låt $p = 3\cdot 2^{n-1}-1$, $q = 3\cdot 2^n - 1$ och $r = 9\cdot 2^{2n-1}-1$ där $n > 1$. Om p, q och r är primtal så är paret $2^n pq$ och $2^n r$ vänskapligt.*

Trots den allmänna formen kände araberna bara till tre fall, då $n = 2$, $n = 4$ och $n = 7$.

Satsen generaliserades senare av Euler som kunde hitta några par som inte ges av Thabits uttryck, och på 1700-talet kände man till 61 par. Nu känner vi till ca 12 miljoner par.

9.6 Övningar

1. Avgör om talen 45, 27 och 36 utgör en pythagoreisk trippel.
2. Bevisa satserna 9.3.4, 9.3.5 och 9.3.6.
3. Varför måste m vara ett udda positivt heltal i sats 9.3.4?
4. Byt m i sats 9.3.4 mot $2m + 1$ och förenkla uttrycket. Vad vinner man på detta?
5. Varför måste $m > n$ i sats 9.3.6?
6. Talet 89789777249 är ett primtal. Visa att talen 52325840864, 72967187668 och 89789777249 inte utgör en pythagoreisk trippel.
7. Kontrollera att 220 och 284 är vänskapliga.
8. Lär dig beviset till sats 9.2.1 utantill.
9. Lär dig beviset till sats 9.2.2 utantill.
10. Lär dig beviset till sats 9.3.7 utantill.

Facit

1. Ja.
2. Gör detta genom att bilda $a^2 + b^2$ repsektive c^2 och förenkla till dess du ser att uttrycken blir lika.
3. Om m är jämnt blir b och c inte heltal.
4. Nu måste inte m vara udda eftersom $2m + 1$ är udda för alla m.
5. Annars blir inte $a > 0$. Förvisso fås fortfarande en pythagoreisk trippel, men den är då uppenbart inte primitiv.
6. Eftersom det största talet är ett primtal är talen relativt prima. De kan dock inte utgöra en pythagoreisk trippel eftersom båda två av de mindre är jämna.
7. Bestäm mängden av alla delare till talen och kontrollera!
8. -
9. -
10. -

10 Mer om talens historia

10.1 Det onaturliga talet noll

Man vet att talet noll användes redan ca 312 f Kr vid astronomiska beräkningar av matematiker i Babylonien. Talet noll användes även av en indisk matematiker vid namn Brahmagupta (född 589 e Kr). De arabiska matematiker som axlade grekernas mantel använde i grunden indiska siffror.

Det arabiska ordet *sifr* är en översättning av *sunya* från sanskrit, vilket betyder tom eller *icke existerande*. Ordet sifr blev det latinska ordet *zephirum*, vilket blev det engelska ordet *zero*. Vi använder ordet *siffra* som ett samlingsnamn för de symboler vi uttrycker tal med.

Det svenska ordet *noll* kan spåras från latinets *nullus*. Intressant nog finns det faktiskt en slags gradskillnad mellan noll och zero, vilket kan spåras tillbaka till hur respektive kultur (den romerska respektive den indiska) såg på tomhet och frånvaro rent filosofiskt. För romarna betydde frånvaro att det frånvarande var på någon annan plats. Indierna däremot tolkade frånvaro i betydelsen att något verkligen inte existerade över huvud taget. Zero är alltså något starkare än noll.

Den som förde de arabiska siffrorna till Europa var Leonardo från Pisa (ca 1170 - 1250, även känd som Fibonacci). Vi återvänder till Leonardo senare. Varken romare eller greker använde nollan vid beräkningar. Hur som helst kom nollan sent till Europa och får därför inte vara med i de naturliga talen.

10.2 De negativa talen

De negativa talen har under mycket lång tid varit högst onaturliga i matematikhistorien. Grekerna skilde mycket starkt på talteori och geometri. Tal representerade objekt, vilka måste finnas och därmed inte kan vara negativa. I geometrin är avstånd alltid positiva.

Även araberna tänkte på avstånd som positiva. De sammanförde i viss mån det vi kallar algebra och geometri idag, även om de inte hade någon koordinatgeometri, vilket är en uppfinning från 1600-talet. För araberna var $x^2 + ax = b$ och $x^2 = b - ax$ två helt olika ekvationer.

10.3 Hur man betecknar tal

I alla tider har människan uttryckt tal med mer eller mindre komplicerade kombinationer av symboler. Vissa av dessa kombinationer är uttänkta så att de underlättar beräkningar.

Så är inte fallet med det romerska sättet att uttrycka tal. De använde ett system där vissa bokstäver betydde olika tal (I=1, V=5, X=10, C=100, D=500 och M=1000). Om ett mindre tal skrevs före ett större skulle det mindre subtraheras från det större. Om det mindre stod efter det större skulle talen adderas. Så blir till exempel 3=III, 4=IV, 6=VI, 1904=MCMIV.

I Grekland användes under olika tider flera sätt att uttrycka tal, mer eller mindre lika det sätt romarna kom att använda. Beräkningar med dessa symboler var mycket komplicerade. Man använde kulramar och räknebrickor där kulor, stenar eller dylikt flyttades runt efter avancerade system.

Under hellenistisk tid använde grekerna bokstäver för att uttrycka tal. Naturligtvis använde grekerna det grekiska alfabetet, men det är inte viktigt för poängen här. Bokstaven a fick betyda 1, b var 2, c var 3 och så vidare upp till i som var 9. Bokstäverna j till r betydde 10 till 90 och s till å betydde 100 till 900.

Talet 12 blev alltså $jb = 10 + 2$, talet 823 blev $zkc = 800 + 20 + 3$ och talet 102 blev $sb = 100 + 2$. Notera för det första att det inte behövdes en symbol för noll. Notera för det andra att dessa tre tal lika gärna skulle kunna ha skrivits exempelvis $bj = 2 + 10$, $kzc = 20 + 800 + 3$ och $bs = 2 + 100$.

Var i talet de enskilda tecknen står, tecknens position, är alltså inte viktigt för

tolkningen av talet. Grekerna använde nämligen inget positionssystem, men det gör vi!

10.3.1 Positionssystemet

När vi skriver 12 menar vi $1 \cdot 10 + 2$, och när vi skriver 21 menar vi $2 \cdot 10 + 1$. Vi använder nämligen normalt talet 10 som bas för att skriva tal.

Det spelar alltså roll vilken position siffrorna 1 respektive 2 har då vi uttrycker tal. Vi har också ord för de olika positionerna. I fallet 923 kallar vi siffran 9 för *hundratal* eftersom dess plats står för att man skall tänka på den som multiplicerad med 100. Av samma anledning benämner vi siffran 2 med *tiotal* och 3:an *ental*.

En förutsättning för detta system är att man kan ange "tomma platser" med symbolen 0, som i fallet $102 = 1 \cdot 100 + 0 \cdot 10 + 2$.

För att ha något att jämföra med senare preciserar vi nu att ett tal uttryckt med $n + 1$ siffror i basen tio är ett skrivsätt så att

$$a_n a_{n-1} \cdots a_1 a_0 \Leftrightarrow a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$$

där de n symbolerna a_{n-1} till a_0 är någon av siffrorna 0 till 9 och symbolen a_n är någon av siffrorna 1 till 9 (om a_n är 0 har talet bara n siffror).

Observera att i vänsterledet av uttrycket ovan är symbolerna a_n till a_0 just symboler, medan de i högerledet representerar tal.

Fallet 102 är alltså ett tal med tre siffror ($n = 2$) där $a_2 = 1$, $a_1 = 0$ och $a_0 = 2$.

Även decimaler har värden som beror på vilken plats de har. Vi kallar den första för tiondel ($\frac{1}{10} = 10^{-1}$) och nästa för hundradel ($\frac{1}{100} = 10^{-2}$). Talet $1,52$ tolkas därför som $1 + 5 \cdot 10^{-1} + 2 \cdot 10^{-2}$.

Detta system att beteckna tal införde alltså Leonardo från Pisa på 1200-talet. Han visade också på den stora fördelen med detta sätt att skriva tal: Det underlättar beräkningar!

Man kan använda andra baser än tio för att uttrycka tal. För att undvika missförstånd anges då basen som ett subscript till talet.

Exempel 10.3.1. Uttrycket 236_{10} och 354_8 anger samma plats på tallinjen, de är samma tal uttryckt i baserna 10 respektive 8, ty

$$236_{10} = 2 \cdot 10^2 + 3 \cdot 10 + 6 \cdot 10^0 = 3 \cdot 8^2 + 5 \cdot 8 + 4 \cdot 8^0 = 354_8.$$

▲

Exempel 10.3.2. Decimaler, det vi till exempel kallar tiondelar och hundradelar, uttrycks på samma sätt.

$$5,5_{10} = 5 \cdot 10^0 + 5 \cdot 10^{-1} = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 1 \cdot 2^{-1} = 101,1_2.$$

▲

10.3.2 Babylonierna

Detta folk använde talet 60 som bas för att uttrycka tal. Möjligen använde de denna bas för att den har så många divisorer, vilket kan ha underlättat beräkningar. De hade ett positionssystem och kunde uttrycka decimaler. En vinkel kunde till exempel vara

$$32°25'12'' = 32 \cdot 60^0 + 25 \cdot 60^{-1} + 12 \cdot 60^{-2}.$$

När de babyloniska skrifterna översattes till latin kallades talet framför 60^{-1} för pars prima minuta (första lilla delen) och talet framför 60^{-2} för pars secunda minuta (andra lilla delen). Härur kommer våra ord för minuter och sekunder. Att en timme har 60 minuter kan man alltså spåra mer än 4000 år bakåt i tiden.

10.4 Algoritmer för räkning med hela tal

Sedan tidigare vet du att det finns metoder att ställa upp beräkningar med tal så att dessa kan utföras enkelt. En väl preciserad metod att lösa ett problem i ett ändligt antal steg kallas för en **algoritm**. Vi går här inte in på hur algoritmerna för att addera, subtrahera, multiplicera och dividera två heltal går till. Jag hoppas följande exempel får dig att minnas.

$$\begin{array}{r} 96 \\ +\,32 \\ \hline 128 \end{array} \qquad \begin{array}{r} 96 \\ -\,24 \\ \hline 72 \end{array} \qquad \begin{array}{r} 42 \\ \cdot\,14 \\ \hline 168 \\ +\,42 \\ \hline 588 \end{array} \qquad \begin{array}{r|l} 1032 & 6 \\ \cline{2-2} -\,6 & 172 \\ \cline{1-1} 43 & \\ -42 & \\ \cline{1-1} 12 & \\ -12 & \\ \cline{1-1} 0 & \end{array}$$

Ordet algoritm kommer från en försvenskning (via andra språk) av namnet på en persisk matematiker, Al-Kwarizmi (ca 790 - 840), som var en viktig länk mellan de indiska och arabiska matematikerna. Även ordet algebra härrör från honom. Det arabiska ordet *al-jabr* betyder ungefär *återför*, eller *flytta tillbaka*. Det användes som benämning på den operation som omvandlar $3x + 2 = 4 - 2x$ till $5x + 2 = 4$ genom att addera $2x$ till båda sidor för att eliminera en negativ term på ena sidan.

Operationen som omvandlar $5x + 2 = 4$ till $5x = 2$ genom att subtrahera 2 från båda sidor benämndes *al-muqalaba*, vilket betyder *jämförande*.

När Al-Kwarizmis texter översattes till latin översattes aldrig al-jabr, vilket så småningom kom att bli vårt ord algebra.

10.4.1 Europas ovilja att acceptera nymodigheter

Den gamla traditionen att använda kulram (abakus) eller de romerska räknebrädorna vid beräkningar levde länge kvar i Europa, långt efter det att Leonardo från Pisa införde de arabiska siffrorna och de algoritmer för räkning som fortfarande lärs ut till barn idag.

Det var mycket komplicerat att räkna med räknebrädorna. Utbildningen för att klara detta var på universitetsnivå, och ville man vara säker på att lära sig alla räknesätt (inte bara addition och subtraktion) räckte det inte med vilket universitet som helst i Tyskland eller Frankrike. Det skulle vara ett fint universitet i Italien! Detta berättas i en anekdot från 1400-talet.

En vältränad räknemästare behövde jobba i timmar med en beräkning som ett skolbarn idag klarar på några minuter. Varför överlevde detta system? Jo, det var nästan ingen utom de utbildade räknemästarna som kunde räkna. Därför hade dessa en hög status och viss makt. En köpman eller godsägare var beroende av sin räknemästare.

De arabiska siffrorna och algoritmerna för räkning var alltså ett hot mot en hel yrkesgrupp. Räknemästarna gjorde därför sitt bästa för att baktala nymodigheterna, vilket lyckades ganska bra. Under hela medeltiden och renässansen rasade en

akademisk strid mellan abakisterna, som förespråkade de gamla kulramarna, och algoristerna, som förespråkade de nya algoritmerna.

Än in på 1800-talet var kulramar vanliga på det engelska finansdepartementet. I Frankrike förbjöds räkning med räknebrädor i skolor och i förvaltningen vid franska revolutionen. Det tog alltså mer än ett halvt millenium för Europa att ta till sig de arabiska metoderna!

10.5 Rationella och irrationella tal

För pythagoréerna var som sagt allt tal. Talen byggde upp världen och universum var alltså uppbyggt av odelbara punkter, atomer. Förhållandet mellan två sträckor måste alltså kunna uttryckas med ett **rationellt tal**. Namnet kommer av att dessa tal var tal man kunde tänka sig. Det är par av heltal som oftast utskrivs på formen

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

Ibland kallar man dessa **bråk**, vilket kommer av ”bruten”.

Denna världsbild innebär att man kan införa en ny mindre enhet att mäta längderna med så att båda sträckornas längder blir heltal.

Om två sträckor från början inte båda var en multipel av samma grundenhet, kunde man införa en ny enhet så att de blev det. Exempelvis gäller detta för två sträckor som är 1 m och 0,23 m långa. Här kan man byta enhet från meter till centimeter så att sträckorna blir 100 cm respektive 23 cm långa.

Någon gång ca 430 f Kr upptäckte dock pythagoréerna att denna process inte är tillämpbar för att jämföra en sida och diagonalen i en kvadrat. Det betyder att diagonalen i en kvadrat med ett rationellt tal som sida, inte är ett rationellt tal.

Vi formulerar detta som en sats.

Sats 10.5.1. *Det finns inget rationellt tal vars kvadrat är två.*

Bevis. Detta bevis är ett motsägelsebevis. Låt oss anta att det finns en lösning som är ett rationellt tal,

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

Låt oss också anta att detta är förkortat så långt det är möjligt. Med denna lösning fås

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2.$$

Detta ger att

$$a^2 = 2b^2. \tag{10.1}$$

Definition 8.4.5 ger oss att a^2 är ett jämnt tal. Vidare ger sats 9.2.2 att talet a därför också är jämnt. Återigen enligt definition 8.4.5 kan därför a skrivas som $a = 2c$ för något tal c.

Stegvis får vi alltså

$$\begin{aligned} a^2 &= 2b^2 \\ (2c)^2 &= 2b^2 \\ 4c^2 &= 2b^2 \\ 2c^2 &= b^2. \end{aligned}$$

Med samma argumentation som ovan får vi att b^2 är ett jämnt tal, och därmed också talet b.

Detta motsäger vårt antagande att kvoten

$$x = \frac{a}{b}$$

är förkortad så långt det är möjligt. Detta tal kan alltså inte existera. □

För pythagoréerna var dessa storheter därför ojämförbara, eller **inkommensurabla storheter**. Med detta menas alltså att det inte finns någon mindre enhet där båda storheterna kan uttryckas som heltal. Kvoten mellan två ojämförbara storheter blir alltså (enligt pythagoréerna) ett tal man inte kan tänka sig, otänkbara tal. Därav namnet irrationella tal.

Idag räknar vi naturligtvis med $\sqrt{2}$ som vilket tal som helst. Det tillhör de reella talen, vilka bland annat innehåller de rationella talen. Tal som inte är rationella benämns ibland **irrationella** tal. Det blir mer om dessa senare.

Denna upptäckt skakade om pythagoréernas världsbild. De beslöt därför att hemlighålla den. Att avslöja existensen av de irrationella talen för omvärlden bestraffades med döden, vilket också blev Hippasos öde eftersom han inte kunde hålla tyst om sin upptäckt. I vissa framställningar av historien återges istället denna upptäckt som något positivt som sporrade pythagoréerna till vidare studier.

Beviset ovan är det klassiska beviset. Redan i likheten (10.1) skulle vi dock kunnat dra slutsatsen att det finns ett jämnt antal faktorer i vänsterledet men ett udda i högerledet. Likheten kan alltså inte råda och redan här finns en motsägelse.

10.6 Övningar

1. Lär dig beviset till sats 10.5.1 utantill.

Facit

1. -

11 Vår tids matematik

Föregående avsnitt visar att frågan ”Vad är ett tal?” inte så lätt låter sig besvaras. Hippasos upptäckte i någon mening de irrationella talen, och värre skulle det bli, även om det dröjde till början av 1800-talet. Man upptäckte vid den här tiden att det fanns en rad intressanta egenskaper som de olika typerna av tal hade. Liksom på 400-talet f Kr fanns det matematiker som trodde på de nya upptäckterna och de som inte gjorde det. Vi återkommer till detta senare.

11.1 Om att konstruera talmängder

Gud skapade de naturliga talen, resten är människans verk.

Citatet är från Leopold Kronecker (1823-1891). Det han menade var att vi måste utgå ifrån något i vårt bygge av matematiken. Vi måste utgå från att det finns naturliga tal och att vi kan addera och multiplicera dem. Däremot finns det varken additativ eller multiplikativ invers till alla naturliga tal.

Från dessa grundläggande antaganden måste vi på något sätt definiera vad som egentligen menas med de hela talen, $\mathbb{Z}$. Därefter måste vi definiera vad som menas med addition och multiplikation i denna talmängd. Att göra detta ligger dock lite utanför ramarna för denna text.

Steget från de hela talen till de rationella talen, $\mathbb{Q}$, går det däremot enklare att illustrera.

Definition 11.1.1. Mängden $\mathbb{Q}$ utgörs av ordnade par av heltal där det andra talet inte är noll. Ett element i $\mathbb{Q}$ tecknas antingen (a, b) eller vanligare $\frac{a}{b}$.

Räkneoperationen addition och multiplikation definieras till

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

Heltalen utgör en delmängd till de rationella talen i den mening att heltalet n identifieras med $\frac{n}{1}$.

Den additativa inversen till $\frac{a}{b}$ är $\frac{-a}{b}$ och den multiplikativa inversen är $\frac{b}{a}$. Det additativa enhetselementet 0 saknar alltså mulitplikativ invers.

Två rationella tal $\frac{a}{b}$ och $\frac{c}{d}$ definieras till lika om $ad = bc$. ▲

Notera att alla definitioner endast bygger på egenskaper för de hela talen!

11.2 Uppräknelighet

11.2.1 Hela tal och rationella tal

Talmängden $\mathbb{Z}$ innehåller som sagt både de positiva och negativa talen. En intressant frågeställning är om det finns fler heltal än naturliga tal. En första gissning är kanske att det finns ungefär dubbelt så många, men vi måste vara noggrannare än så.

De hela talen går att räkna upp. Med det menas att man kan ordna dem efter varandra på ett sådant sätt att man är säker på att få med alla, och det skall speciellt vara möjligt att peka ut vart och ett av talen. Med ett finare språk säger man att de är **uppräkneliga**. Motsatsen är **överuppräknelig**.

Elementen i $\mathbb{Z}$ kan tecknas

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\}.$$

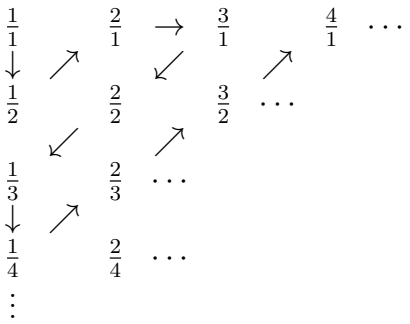
Detta är uppenbart en uppräkning av alla hela tal.

Eftersom det svarar precis ett helt tal till varje naturligt tal så måste vi dra slutsatsen att det finns lika många element i de båda mängderna. Förvisso är det oändligt många element i båda mängderna, men det är samma oändlighet. En symbol som brukar användas för denna oändlighet är $\aleph_0$. Symbolen $\aleph$ är för övrigt den första bokstaven i det hebreiska alfabetet och utläses "aleph".

Om du nu tänker på intervallet mellan 0 och 1 så inser du kanske att det där finns oändligt många rationella tal. Där finns $\frac{1}{2}$, $\frac{3}{4}$, $\frac{998}{1000}$ och alla de andra. Finns det fler rationella tal än hela tal? Om det finns oändligt många bara mellan 0 och 1 så kan man kanske tycka det, men så är icke fallet.

Den tyske matematikern Georg Cantor (1845 - 1918) visade att det finns lika många av varje. Han konstruerade nämligen en uppräkning av de rationella talen enligt

mönstret nedan.



På detta sätt går det att sätta fingret på (indexera) varje element i $\mathbb{Q}$ och räkna upp dem med elementen i $\mathbb{N}$. Det finns alltså $\aleph_0$ element i $\mathbb{Q}$ också!

11.2.2 Reella tal

De reella talen består av allt vi normalt kallar tal. Symbolen som används för att beteckna denna mängd är $\mathbb{R}$. Alla rationella tal är reella tal, precis som att alla hela tal är rationella tal. Utöver dessa utgörs de reella talen av till exempel $\sqrt{2}$, som enligt sats 10.5.1 inte är ett rationellt tal.

De reella talen uppfyller samma algebraiska struktur som de rationella talen. De utgör med andra ord en kropp även de.

Ett rationellt tal kan uttryckas exakt med två heltal, exempelvis $1/4$ och $2/3$. För vissa av dem gäller att de går att uttrycka med ett ändligt antal decimaler. Detta gäller $3/4 = 0.75$, men inte $2/3$.

Däremot gäller att alla rationella tal får en *periodisk* decimalutveckling. Det betyder att det finns en sekvens decimaler som återkommer gång på gång i all oändlighet. För att visa detta skriver man ett streck över den sekvens som skall upprepas.

$$\begin{aligned} \frac{1}{3} &= 0,333333333\ldots = 0,\overline{3} \\ \frac{56}{123} &= 0,455284552845528455284552845528\ldots = 0,\overline{45528} \end{aligned}$$

Detta gäller inte de reella tal som inte är rationella tal. De får en icke-periodisk decimalutveckling. För att särskilja de olika typerna gör vi följande definition.

Definition 11.2.1. De **irrationella talen** utgörs av alla reella tal som inte är rationella. ▲

En märklig egenskap de reella talen har är att de i någon mening är ”fler” än de naturliga talen, de är överuppräkneligt många. Detta formulerades och visades också av Cantor.

Sats 11.2.2. *De reella talen är överuppräkneliga.*

Bevis. Antag att det finns en uppräkning som innehåller alla de reella talen, exempelvis den som återges nedan.

$$\begin{aligned} &0,17897193287876764\ldots \\ &0,76575465854352343\ldots \\ &0,44231322342432438\ldots \\ &0,00000000100000100\ldots \\ &\vdots \end{aligned}$$

Alldeles oavsett hur denna uppräkning är kan nu alltid ett nytt reellt tal bildas, som skiljer sig från alla dessa tal. Låt det nya talet få en decimalutveckling som i n:te decimalen skiljer sig från det n:te talets n:te decimal.

Med uppräkningen ovan får alltså det nya talets första decimal inte vara 1, den andra decimalen får alltså inte vara 6, den tredje inte 2 och så vidare. Det tal som konstrueras på detta sätt kommer att skilja sig från alla tal i uppräkningen. Därför kan uppräkningen inte innehålla alla reella tal. □

Om vi återgår till intervallet mellan 0 och 1 på tallinjen, så finns det alltså "hål" mellan alla rationella tal, medan de reella talen "fyller ut" hela tallinjen, de bildar ett kontinuum.

Cantor forskade just om frågor kring oändlighetsbegreppet, och visade att det finns olika stora oändligheter. Den oändlighet som de reella talen tillhör tecknas $\aleph_1$ och är alltså större än den som de naturliga talen tillhör: $\aleph_0 < \aleph_1$.

En fråga som följer av detta är om det finns någon ordning av oändligheten mellan dessa två, och om man kan tänka sig högre ordningar av oändligheten än $\aleph_1$. Detta lämnas som övning.

11.2.3 Transcendenta och algebraiska tal

Även om de reella talen fyller ut hela tallinjen, finns det vissa av dem som skiljer ut sig.

Definition 11.2.3. En lösning till en polynomekvation med endast heltalskoefficienter är ett **algebraiskt tal**. Övriga reella tal kallas **transcendenta tal**. ▲

Övning 2

Exempel 11.2.4. Talet $\sqrt{2}$ är algebraiskt eftersom det är en av lösningarna till $x^2 - 2 = 0$. ▲

Det går att räkna upp alla polynomekvationer med heltalskoefficienter. Det betyder att deras lösningar också går att räkna upp. Det betyder i sin tur att de algebraiska talen är uppräkneliga.

Det ger till slut att det måste vara de transcendenta talen som är överuppräkneliga. De flesta tal är alltså inte lösningen till någon ekvation!

Några transcendenta tal är dock ändå mycket viktiga, till exempel är π ett transcendent tal. Detta visades först 1882 av Lindemann (1852 - 1939).

11.3 Övningar

1. Som bekant är bara var tredje tal delbart med 3. Varför är det ändå rätt att säga att det finns lika många tal som är delbara med 3 som det finns tal som inte är delbara med tre?
2. Visa att talet 7/3 är algebraiskt.
3. Lär dig beviset till sats 11.2.2 utantill.

Facit

1. Tal som är delbara med tre utgör en uppräknelig mängd.
2. Det är lösning till ekvationen $3x - 7 = 0$.
3. -

12 Grupper, ringar och kroppar

På 1800-talet började man också ”räkna med annat än tal”. Med detta menas att man identifierade generella strukturer på annat än tal, men som påminner om räkneregler för tal. Detta utvecklades till vad som idag benämns abstrakt algebra.

Vi skall snart se på några sådana strukturer, men först måste vi reda ut vad som menas med några ord.

Definition 12.0.1. Låt M vara en mängd och a, b och c vara godtyckliga element i M. Låt $+$ beteckna en räkneoperation i denna mängd. Operationen är **sluten** om $a+b \in M$, är **kommutativ** om $a+b = b+a$ och **associativ** om $(a+b)+c = a+(b+c)$. Det finns ett **enhetselement** $e \in M$ till operationen om $a + e = a$ gäller för alla $a \in M$. ▲

Exempel på en icke sluten operation är till exempel fallet där mängden är alla udda tal och operationen är addition. Exempelvis gäller då $3 + 5 = 8$ vilket är ett jämnt tal. Operationen ”leder ut” ur mängden, så att säga.

Ett annat exempel är räkning med addition och multiplikation i $\mathbb{Z}^-$ (de negativa heltalen). Här är addition sluten, $(-4)+(-5) = -9$, men inte multiplikation, $(-4)\cdot(-5) = 20 \notin \mathbb{Z}^-$.

Den vanliga multiplikationen är, liksom additionen, kommutativ för tal av olika sorter. Exempelvis gäller ju $2 \cdot 3 = 3 \cdot 2$.

12.1 Grupper

En grupp är ett system där man har en mängd (till exempel tal, men det måste inte vara tal) och **en** räkneoperation.

Definition 12.1.1. En **grupp** består av en mängd och en räkneoperation som uppfyller följande krav.

1. Operationen skall vara sluten och associativ.
2. Det skall finnas ett enhetselement till operationen.
3. Alla element skall ha en invers under operationen.

Om räkneoperationen dessutom är kommutativ har man en **kommutativ grupp**. ▲

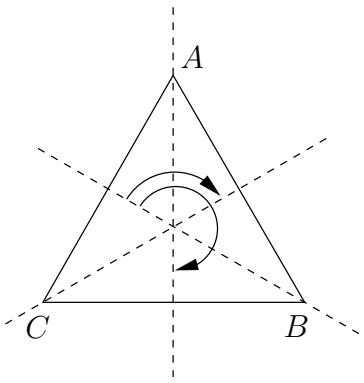
Skall man vara noga betecknas en grupp med ett par, en mängd och en operation, till exempel $(\mathbb{Z}, +)$. Om inget missförstånd kan uppstå använder man ibland bara mängdens namn som beteckning även för gruppen.

Exempel 12.1.2. $(\mathbb{Z}, +)$ är en kommutativ grupp. Addition är både sluten, kommutativ och associativ, och alla element i $\mathbb{Z}$ har en additativ invers. Enhetselementet i gruppen är talet 0. ▲

Exempel 12.1.3. $(\mathbb{Q}\backslash\{0\}, \cdot)$ är en kommutativ grupp. Multiplikation är både sluten, kommutativ och associativ, och alla element i $\mathbb{Q}$ utom 0 har en multiplikativ invers. Enhetselementet i gruppen är talet 1. ▲

För att det skall bli någon poäng med det hela måste vi också ta ett exempel som inte rör just tal.

Exempel 12.1.4. Symmetrioperationerna på en liksidig triangel utgör en icke-kommutativ grupp. Låt A, B och C vara hörnpunkterna i en liksidig triangel. En symmetrioperation på ett objekt är en operation som lämnar objektet oförändrat. Symmetrioperationerna på triangeln nedan är E, att inte göra någonting, R_1 och R_2, att vrida triangeln runt sitt centrum med 120° respektive 240°, samt R_3, R_4 och R_5, att vrida triangeln 180° runt axlarna genom A, B respektive C.

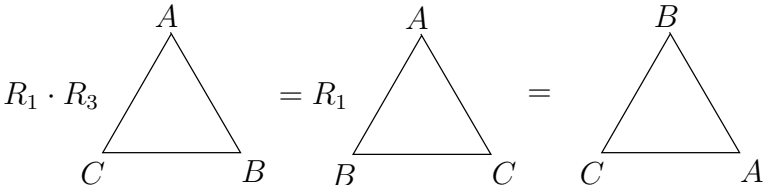


Under R_1 byter hörnen plats enligt $A \to B$, $B \to C$ och $C \to A$. Under R_3 är hörn A stilla, men hörnen B och C byter plats.

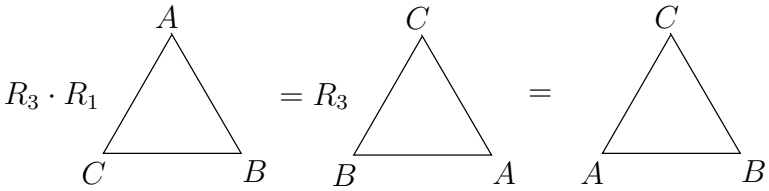
Operationerna kan nu kombineras. Låt symbolen $\cdot$ stå för detta. Till exemepel gäller här $R_1 \cdot R_1 = R_2$ och $R_1 \cdot R_2 = E$.

Mängden $\{E, R_1, R_2, R_3, R_4, R_5\}$ och operationen $\cdot$ utgör tillsammans en grupp. E är enhetselementet. Alla element har en invers. Operationerna R_1 och R_2 är varandras inverser och R_3, R_4 och R_5 är alla sina egna inverser.

Det intressanta med denna grupp är att den inte är kommutativ. Till exempel gäller $R_1 \cdot R_3 = R_5$.



Som du ser blir resultatet av att först verka med R_3 och sedan med R_1 samma sak som att verka med R_5. Om man istället byter ordning får vi $R_3 \cdot R_1 = R_4$.



Alltså gäller $R_1 \cdot R_3 \neq R_3 \cdot R_1$ i denna grupp!

▲

Det kan kanske verka konstigt, men symmetrioperationer av olika slag är extremt viktiga i fysiken. På sätt och vis verkar det faktiskt som att det är just de symmetriska egenskaperna för universum som allting annat följer ur. Till exempel kan man visa att det finns en bevarad storhet till varje symmetri. Detta visade Emmy Noether (1882 - 1935) år 1915. Man trodde från början att det fanns problem inbyggda i den allmänna relativitetsteorin, men Emmy löste problemet. När hon ändå höll på visade hon att sambandet mellan bevarad storhet och symmetri är mycket mer generellt än att bara gälla inom den allmänna relativitetsteorin.

Begreppet energi och att detta är bevarat i ett slutet system ”följer” ur att rum-

tidens struktur inte ändras med tiden (är translationsinvariant i tiden). Begreppet rörelsemängd är relaterat till att rumtiden är translationsinvariant.

Exempel 12.1.5. Mängden $\mathbb{Z}_{12}$ är en grupp under addition.

Denna grupp är kommutativ. Till exempel gäller $9 + 5 = 5 + 9$. Enhetselementet är naturligvis talet 0.

Alla element har en invers. Till exempel är inversen till 4 talet 8 eftersom $4 + 8 = 0$.

Generellt är $\mathbb{Z}_n$ en grupp under addition. ▲

12.2 Ringar

Vi är ju vana vid två räknesätt, inte bara ett som i en grupp.

Definition 12.2.1. En **ring** består av en mängd och två räkneoperationer. Båda skall vara slutna, associativa och ha ett enhetselement. En av dem skall vara kommutativ. Alla element skall ha en invers under den kommutativa operationen.

Om båda operationerna är kommutativa säger man att ringen är kommutativ. ▲

Exempel 12.2.2. De hela talen, $\mathbb{Z}$, utgör tillsammans med operationerna addition och multiplikation en ring. Alla tal har en additativ invers, men det finns ingen invers till multiplikationen. Enhetselementet till addition är talet 0 och enhetselementet till multiplikation är talet 1. ▲

Exempel 12.2.3. I högre kurser i matematik kommer du att stöta på något som kallas polynom. Dessa utgör också en ring. ▲

Exempel 12.2.4. Mängden $\mathbb{Z}_{12}$ är även en ring. Generellet är $\mathbb{Z}_n$ en ring. ▲

12.3 Kroppar

Det finaste man kan ha är en kropp! Det märker du av dess definition.

Definition 12.3.1. En **kropp** består av en mängd och två räkneoperationer som båda är slutna, associativa och har enhetselement. Båda operationerna skall vara kommutativa. Alla element utom enhetselementet till den första operationen skall ha en invers till den andra operationen. ▲

Skillnaden mellan en kropp och en ring är alltså att alla element skall ha en multiplikativ invers i kroppen.

Exempel 12.3.2. De rationella talen, $\mathbb{Q}$, utgör tillsammans med operationerna addition och multiplikation en kropp. Alla element utom 0 har en multiplikativ invers. ▲

Som vi vet från sats 8.5.3 har de tal som är relativt prima med n multiplikativ invers i $\mathbb{Z}_n$. Om n är ett primtal är alla naturliga tal mindre än n relativt prima med n. Det bevisar följande sats.

Sats 12.3.3. *$\mathbb{Z}_p$ en kropp då $p \in \mathbb{P}$.*

12.4 Övningar

1. Bilda hela multiplikationstabellen för symmetrioperationerna på en liksidig triangel. Tips: Rita trianglar på samma sätt som i exempel och/eller skapa en triangel IRL som du vänder och vrider på.12.1.4.

2. Vilka tal förutom 5 har multiplikativ invers i $\mathbb{Z}_{12}$.

3. Fyll i hela multiplikationstabellen för $\mathbb{Z}_5$ intill.

	1	2	3	4
1	1		3	
2			1	
3				
4		3		

4. Beräkna $7 + 9$ i $\mathbb{Z}_{11}$

5. Bestäm den additativa inversen till 8 i $\mathbb{Z}$.

6. Bestäm den additativa inversen till 7 i $\mathbb{Z}_9$.

7. Bestäm den multiplikativa inversen till 5 i $\mathbb{Z}_7$

Facit

1.

	E	R_1	R_2	R_3	R_4	R_5
E	E	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	E	R_4	R_5	R_3
R_2	R_2	E	R_1	R_5	R_3	R_4
R_3	R_3	R_5	R_4	E	R_2	R_1
R_4	R_4	R_3	R_5	R_1	E	R_2
R_5	R_5	R_4	R_3	R_2	R_1	E

2. Talen 1,7 och 11.

3.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

4. 5

5. -8

6. 2

7. 3

A Axiom för kroppar

En mängd där man kan ”räkna” med elementen på det sätt man kan med rationella tal benämns **kropp**. Därför används symbolen K för den aktuella mängden. De rationella talen $\mathbb{Q}$ och mängden av alla rationella funktioner är exempel på kroppar, liksom $\mathbb{Z}_p$ där p är ett primtal.

Mer precist är en kropp en mängd där det finns två räkneoperationer definierade, addition (med symbolen $+$) och multiplikation (med symbolen $\cdot$). För dessa räkneoperationer gäller följande.

A1 Slutenhet: $a + b \in K$ för alla $a, b \in K$.

A2 Addition är kommutativ: $a + b = b + a$ för alla $a, b \in K$.

A3 Addition är associativ: $(a + b) + c = a + (b + c)$ för alla $a, b, c \in K$.

A4 Det finns ett element $0 \in K$ som uppfyller att $0 + a = a$ för alla $a \in K$.

A5 Till varje $a \in K$ finns ett element $-a$ med egenskapen att $a + (-a) = 0$.

M1 Slutenhet: $a \cdot b \in K$.

M2 Multiplikation är kommutativ: $a \cdot b = b \cdot a$ för alla $a, b \in K$.

M3 Multiplikation är associativ: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ för alla $a, b, c \in K$.

M4 Det finns ett element $1 \neq 0 \in K$ som uppfyller $1 \cdot a = a$ för alla $a \in K$.

M5 Till varje $a \neq 0 \in K$ finns ett element a^{-1} med egenskapen att $a \cdot a^{-1} = 1$.

D1 Distributiva lagen: $a \cdot (b + c) = a \cdot b + a \cdot c$ för alla $a, b, c \in K$.

Det som skiljer ringar från kroppar är alltså det sista axiomet rörande multiplikation, M5. Detta axiom garanterar att det finns en multiplikativ invers till alla element i kroppen (utom elementet 0).

Det finns ingen subtraktion definierad för elementen i en kropp. Dessutom gäller att det inte finns någon division definierad. När vi skriver a/b menar vi egentligen $a \cdot b^{-1}$.

B Om definitionen av primtal

Här förklaras valet av definition av primtal. Att olika definitioner görs i olika böcker är i sig inget konstigt. Det förekommer ofta i matematiken. Som läsare måste man naturligtvis se upp med detta om man jämför hur teoirer framställs i olika böcker, och det är också en av de förmågor som tränas i och med denna text och i kurser där den används.

Jag har tre huvudsakliga skäl till min definition av primtal. Det ena är pedagogiskt sett till just denna text och de läsare den är skriven för, de två andra skälen är lite mer djupsinnigt matematiska och kräver betydligt mer matematiska kunskaper än vad som kan anses förkunskaper för denna text. Jag avslutar kort med dessa.

Detta avsnitt riktar sig alltså först och främst inte till elever i årskurs ett på gymnasiet, utan till övriga intresserade läsare som undrar varför den gängse definitionen inte används.

Först och främst är det önskvärt att denna text skall vara självkonsistent. Om sats 7.1.7 skulle användas som definition av primtal, vilket är brukligt, skulle definition 7.1.6 behöva bevisas. Som sats brukar 7.1.6 benämnas Euklides lemma.

Låt oss gå igenom den ”normala” sättet att formulera satser rörande detta och deras bevis.

Den normala definitionen av primtal.

Definition B.0.1. Ett tal a är ett **primtal** om det endast delas av 1 och a. ▲

Med denna definition måste vi formulera följande sats eftersom den behövs i beviset av satsen som säger att faktorisering är entydig i $\mathbb{Z}$, sats 7.1.13.

Sats B.0.2. ***Eulkides lemma*** *Om p är ett primtal och $p \mid ab$ så gäller $p \mid a$ eller $p \mid b$.*

Man brukar bevisa sats B.0.2 genom att hänvisa till följande sats.

Sats B.0.3. ***Bézouts identitet*** *Om u och v är relativt prima finns det tal m och n så att*

$$mu + nv = 1.$$

Bevis. Bevis av sats B.0.2

Antag att p är ett primtal och att $p \mid ab$, men att $p \nmid a$. Då skall vi visa att $p \mid b$.

Talen p och a är relativt prima, därför finns enligt Bézouts identitet m och n så att

$$mp + na = 1.$$

Vi multiplicerar med b och får

$$mpb + nab = b.$$

Talet p delar båda termerna i vänsterledet (enligt förutsättningarna skall $p \mid ab$) och måste då även dela högerledet, $p \mid b$. □

Vi måste nu bevisa sats B.0.3, Bézouts identitet, eftersom den användes i föregående bevis.

Bevis. Bevis av sats B.0.3 Givet u och v finns ett minsta posivita

$$d = mu + nv$$

bland alla tal på formen $ku + lv$. Om u delas med d fås enligt sats 8.1.1 (euklidisk division) en kvot q och en rest $0 \leq r < d$ så att $u = qd + r$ vilket ger

$$0 \leq r = u - qd = u - q(mu + nv) = (1 - qm)u + nv < d.$$

Vi noterar att r alltså också gåra att skriva på formen $ku + lv$. Eftersom d skulle vara det *minsta* positiva heltal av alla dessa måste alltså $r = 0$ gälla, och därmed gäller $d \mid u$.

På samma sätt gäller $d \mid v$. Om det finns något tal c så att $c \mid u$ och $c \mid v$ gäller $c \mid d$ enligt sats 7.3.1. Därför gäller $d = \text{sgd}(u, v)$, men eftersom u och v skulle vara relativt prima gäller $d = 1$. □

Detta bevis ger att talen m och n existerar, men inte hur de hittas. Det följer dock av Euklides algoritm, sats 8.3.1. I själva verket följer Bézouts identitet av Euklides algoritm.

Eftersom Euklides lemma används för att bevisa att faktorisering är entydig är det önskvärt att dess bevis genomförs innan satsen används. Vi har nu dock sett att det krävs en hel del för detta bevis. Alldeles för mycket för att få en pedagogiskt lämplig text.

Detta är en anleding till att jag valt att definiera primtal från Euklides lemma (7.1.6). Vi slipper några krångliga bevis och slipper använda begrepp som introduceras långt senare i texten (kvot och rest, relativt prima).

Implikationskedjorna nedan tydliggör min poäng:

$$7.1.6 \Rightarrow 7.1.13$$

$$\text{B.0.1 , 7.8.1, 8.1.1} \Rightarrow \text{B.0.3} \Rightarrow \text{B.0.2} \Rightarrow 7.1.13$$

De två lite djupsinnigare anledningarna till mitt val av defnition följer nu.

Vi har följande inkulsionskedja.

Kommutativ ring $\supset$ Integretetsområde[7] $\supset$ UFD[8] $\supset$ PID [9] $\supset$ Euklidisk område[10] $\supset$ Kropp

Talmängden $\mathbb{Z}$ är i någon mening "ur-ringen", den man av mycket naturliga skäl först studerar i sin matematiska karriär. För att visa att $\mathbb{Z}$ är en UFD med det traditionella sättet att definiera primtal, som i detta avsnitt, måste man åberopa att $\mathbb{Z}$ dessutom är en euklidisk ring.

Matematiker brukar sträva efter att använda så lite struktur som möjligt för att göra bevis så allmänna som möjligt vilket i sig motiverar min defnition.

Till sist, inom högre ringteori definierar man normalt **primelement** som jag definierat primtal i denna text. Man definierar också **irreducibla element** som något som inte går att skriva som produkten av två element som har multiplikativ invers.

Den traditionella definitionen av primtal liknar alltså mer den för irreducibla element snarare än den för primelement. Varför skall $\mathbb{Z}$ vara ett undantag, då $\mathbb{Z}$ är den mest naturliga ringen?

[7] Eng Integral domain
[8] Unique factorization domain
[9] Principal ideal domain
[10] Eng Eucledian domain