

Kompletterande material till kursen i
Diskret matematik



Jonathan Nilsson

Senast uppdaterad den 12 oktober 2020

Kapitel 1

Talteori

1.1 Kinesiska restsatsen

1.1.1 Introduktion

Vi ska nu titta på system av kongruenser. Ett sådant kan exempelvis se ut så här:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Vi letar alltså efter ett heltal x som uppfyller båda kongruenserna samtidigt. Man verifierar lätt att $x = 8$ är en lösning till ovanstående system, och man kan också se att faktiskt alla heltal på formen $x = 8 + 15k$ där $k \in \mathbb{Z}$ löser systemet. Vi kan alltså säga att lösningen till systemet är $x \equiv 8 \pmod{15}$.

Det var låga tal i detta exempel, så man kunde nästan gissa lösningen. Men hur löser man denna typ av system i allmänhet?

1.1.2 Metod 1: Substitution i diofantiska ekvationer

Vi demonstrerar en lösningsmetod på systemet ovan.

Den övre ekvationen kan skrivas om till en linjär diofantisk ekvation i två variabler som

$$x \cdot 1 + y \cdot 3 = 2.$$

Denna har vi en standardmetod för att lösa genom att använda Euklides algoritm. Resultatet blir att mängden lösningar (x, y) blir

$$\{(2 + 3k, -k) \mid k \in \mathbb{Z}\}.$$

I detta exempel struntar vi dock i vilket värde y har, det viktiga är att $x = 2 + 3k$ löser ekvationen för varje $k \in \mathbb{Z}$. Detta kan vi också se direkt i vårt fall då talen är så små.

Härnäst stoppar vi in $x = 2 + 3k$ i den nedre ekvationen och skriver om till en diofantisk ekvation:

$$x \equiv 3 \pmod{5} \Leftrightarrow x + z \cdot 5 = 3 \Leftrightarrow 2 + k \cdot 3 + z \cdot 5 = 3 \Leftrightarrow k \cdot 3 + z \cdot 5 = 1.$$

Detta är nu en diofantisk ekvation i variablerna k och z . Nu kan vi lösa denna med Euklides algoritm. Resultatet blir att alla lösningar ges av

$$(k, z) = (2 + 5n, -1 - 3n) \text{ där } n \in \mathbb{Z}.$$

Vi struntar i vad z är, men vi kan nu hitta alla lösningar x till systemet:

$$x = 2 + 3k = 2 + 3(2 + 5n) = 8 + 15n \Leftrightarrow x \equiv 8 \pmod{15}.$$

Sats 1.1

Kinesiska restsatsen

Antag att n_1 och n_2 är relativt prima. Då har följande system en unik lösning modulo $n_1 n_2$.

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Bevis

Varje lösning till översta ekvationen har form $x = a_1 + kn_1$ för något $k \in \mathbb{Z}$. Detta ger i andra ekvationen $a_1 + kn_1 + zn_2 = a_2 \Leftrightarrow kn_1 + zn_2 = a_2 - a_1$. Eftersom $\gcd(n_1, n_2) = 1$ så har enligt Euklides algoritm ekvationen en lösning där $k = k_0 + wn_2$ där k_0 är en lösning, och $w \in \mathbb{Z}$. Återsubstitution ger

$$x = a_1 + (k_0 + wn_2)n_1 = a_1 + k_0 n_1 + w(n_1 n_2) \quad w \in \mathbb{Z} \Leftrightarrow x \equiv a_1 + k_0 n_1 \pmod{n_1 n_2}.$$

Det finns alltså en unik lösning modulo produkten $n_1 n_2$ vilket vad var som skulle bevisas.

Satsen kan också användas iterativt för system av fler än två ekvationer. Låt n_1, n_2, n_3 vara parvis relativt prima och betrakta systemet

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3}. \end{cases}$$

Enligt kinesiska restsatsen kan vi lösa de översta två ekvationerna - lösningen får formen $x \equiv b \pmod{n_1 n_2}$. Vi får nu systemet

$$\begin{cases} x \equiv b \pmod{n_1 n_2} \\ x \equiv a_3 \pmod{n_3}. \end{cases}$$

Eftersom n_3 saknar gemensam delare med både n_1 och n_2 så är även $\gcd(n_1, n_2 n_3) = 1$. Därför kan vi tillämpa Kinesiska restsatsen en gång till, och får en unik lösning modulo produkten $n_1 n_2 n_3$. Samma idé kan upprepas godtyckligt många gånger. Vi har nu bevisat följande följsats:

Sats 1.2

Följsats

Antag att $n_1, n_2, \dots, n_t$ är parvis relativt prima. Då har systemet

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_t \pmod{n_t} \end{cases}$$

en unik lösning modulo produkten $n_1 n_2 \cdots n_t$.

Samma lösningsmetod som ovan fungerar också, fast man får upprepa den en extra gång för varje ny rad i systemet.

1.1.3 Metod 2: Formel via inverser i $\mathbb{Z}_{n_i}$

Det finns en annan metod att lösa system av kongruenser som kan vara snabbare, men svårare att memorera. Vi vill åter lösa systemet

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_t \pmod{n_t} \end{cases}$$

Vi definierar $N = n_1 \cdot n_2 \cdots n_t$ och för varje index i inför vi $N_i := N/n_i$. Då är N_i produkten av alla $n_1, \dots, n_t$ utom n_i . Eftersom n_i och N_i är relativt prima så är N_i inverterbart i $\mathbb{Z}_{n_i}$, vi kan alltså hitta tal b_i som uppfyller

$$b_i \cdot N_i \equiv 1 \pmod{n_i} \quad \forall i.$$

Nu kan vi direkt skriva ned lösningen till ekvationen:

$$x \equiv a_1 b_1 N_1 + a_2 b_2 N_2 + \cdots + a_t b_t N_t \pmod{n_1 n_2 \cdots n_t}.$$

Vi ser att detta är en lösning eftersom modulo n_1 blir

$$x \equiv a_1 (N_1^{-1} N_1) + n_1 (\text{termer}) \equiv a_1 \cdot 1 \equiv a_1 \pmod{n_1},$$

där vi använde att $b_1 = N_1^{-1}$ och att n_1 delar var och en av $N_2, N_3, \dots, N_t$. Samma räkning fungerar för varje kongruens. Enligt Kinesiska restsatsen blir denna lösning unik modulo N .

Vi formulerar detta som en sats:

Sats 1.3

När $n_1, \dots, n_t$ är parvis relativt prima har systemet

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_t \pmod{n_t} \end{cases}$$

den unika lösningen

$$x \equiv a_1 b_1 N_1 + a_2 b_2 N_2 + \cdots + a_t b_t N_t \pmod{N},$$

där $N = n_1 \cdot n_2 \cdots n_t$ och $N_i = N/n_i$ och talen b_i uppfyller $b_i N_i \equiv 1 \pmod{n_i}$.

Satsen ger en algoritm för att lösa kongruenssystemet:

1. Beräkna talen N och $N_1, N_2, \dots, N_t$
2. För varje i : Hitta b_i så att $b_i N_i \equiv 1 \pmod{n_i}$. Detta kan göras genom att gissa eller med Euklides algoritm.

3. Skriv ned lösningen $x \equiv a_1 b_1 N_1 + a_2 b_2 N_2 + \dots + a_t b_t N_t \pmod{N}$
4. Reducera uttrycket för x så att $0 \leq x < n_1 n_2 \dots n_t$
5. Testa din lösning!

Exempel 1.1

Lös kongruenssystemet

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases}$$

Lösning:

3, 4, 5 är parvis relativt prima, så systemet har en unik lösning modulo $N = 3 \cdot 4 \cdot 5 = 60$. Vi har $(n_1, n_2, n_3) = (3, 4, 5)$ så $(N_1, N_2, N_3) = (20, 15, 12)$. Vi hittar nu inverser, eftersom talen är små är det lätt att gissa inverserna.

$$b_1 \cdot 20 \equiv 1 \Leftrightarrow b_1 \cdot 2 \equiv 1 \pmod{3} \text{ så vi väljer lösningen } b_1 = 2.$$

$$b_2 \cdot 15 \equiv 1 \Leftrightarrow b_2 \cdot 3 \equiv 1 \pmod{4} \text{ så vi väljer lösningen } b_2 = 3.$$

$$b_3 \cdot 12 \equiv 1 \Leftrightarrow b_3 \cdot 2 \equiv 1 \pmod{5} \text{ så vi väljer lösningen } b_3 = 3.$$

Enligt satsen ges en lösning till systemet av

$$x = a_1 b_1 N_1 + a_2 b_2 N_2 + a_3 b_3 N_3 = 2 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 3 \cdot 3 \cdot 12 = 80 + 45 + 108 = 233.$$

Och alla lösningar ges av $x \equiv 233 \pmod{60}$. Vi kan dock reducera modulo 60 och svara:

Svar: Systemets lösning är $x \equiv 53 \pmod{60}$.

Systemet hade också kunnat lösas med den gamla metoden - lös varje rad och substituera i nästa. Notera att det är enkelt att testa sin lösning!

1.2 Eulers φ -funktion

Eulers φ -funktion ("fi-funktion") är användbar för att beräkna kongruenser av höga potenser, och även inom RSA-algoritmen.

Den grekiska bokstaven "fi" kan också skrivas ϕ .

Definition 1.1

Funktionen $\varphi : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ definieras för varje positivt heltal n av

$$\varphi(n) = \left| \{a \mid 1 \leq a \leq n \text{ och } \gcd(a, n) = 1\} \right|.$$

Med andra ord är $\varphi(n)$ antalet tal mellan 1 och n som saknar gemensamma primfaktorer med n .

(Här är $\mathbb{Z}_+ = \{1, 2, 3, \dots\}$ de positiva heltalen).

Exempel 1.2

Vi har

$$\varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6$$

$$\varphi(10) = |\{1, 3, 7, 9\}| = 4$$

$$\varphi(11) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}| = 10$$

$$\varphi(12) = |\{1, 5, 7, 11\}| = 4$$

Vi ser att om p är ett primtal så får vi $\varphi(p) = p - 1$. Man kan också resonera sig fram till att $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$. Det gäller också att $\varphi(ab) = \varphi(a)\varphi(b)$ när $\gcd(a, b) = 1$.

Eftersom varje tal n kan primtalsfaktoriseras som $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ så får vi enligt ovanstående regler

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdots \varphi(p_t^{k_t}) = p_1^{k_1-1}(p_1 - 1) \cdot p_2^{k_2-1}(p_2 - 1) \cdots p_t^{k_t-1}(p_t - 1).$$

Sats 1.4

Om $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ är primtalsfaktoriseringen av talet n så gäller

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot p_2^{k_2-1}(p_2 - 1) \cdots p_t^{k_t-1}(p_t - 1).$$

Exempel 1.3

Vi har

$$\varphi(27) = \varphi(3^3) = 3^2(3 - 1) = 8 \cdot 2 = 16$$

$$\varphi(100) = \varphi(2^2 5^2) = 2^1(2 - 1) \cdot 5^1(5 - 1) = 2 \cdot 20 = 40$$

$$\varphi(221) = \varphi(13 \cdot 17) = 13^0(13 - 1) \cdot 17^0(17 - 1) = 12 \cdot 16 = 192$$

Det är alltså lätt att räkna ut $\varphi(n)$ så länge vi vet primtalsfaktoriseringen av n . Anledningen till att man vill kunna beräkna $\varphi(n)$ är kanske främst för att beräkna potenser i kongruensräkning. Detta bygger på följande kända sats:

Sats 1.5

Eulers sats:

Antag att a och n är relativt prima. Då har vi

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

Bevis

Låt $x_1, x_2, \dots, x_{\varphi(n)}$ vara de tal mellan 1 och n som är relativt prima med n . Låt a vara ett tal med $\gcd(a, n) = 1$. Då är

$$\{x_1, x_2, \dots, x_{\varphi(n)}\} = \{ax_1, ax_2, \dots, ax_{\varphi(n)}\} \quad (\text{som delmängder av } \mathbb{Z}_n).$$

Multiplikation med a permuterar (flyttar runt) alltså bara talen x_i , mängderna är samma. Men då är också produkten över de två mängderna samma i $\mathbb{Z}_n$:

$$\prod_{i=1}^{\varphi(n)} x_i = \prod_{i=1}^{\varphi(n)} ax_i = a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i.$$

Eftersom varje x_i är inverterbart i $\mathbb{Z}_n$ kan vi cancellera de två lika produkterna och vi får $a^{\varphi(n)} = 1$ i $\mathbb{Z}_n$, vilket är ekvivalent med vad vi skulle bevisa.

Innan vi börjar använda detta för att räkna ser vi att vi nu kan bevisa en ännu mer känd sats som en enkel följsats.

Sats 1.6**Fermats lilla sats:**

När p är ett primtal så gäller

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

för alla heltal a .

Alternativt kan vi skriva $a^{p-1} \equiv 1 \pmod{p}$ som gäller så fort $p \nmid a$.

Bevis

Efter reduktion modulo p kan vi anta $0 \leq a < p$. Om $a = 0$ är satsen trivialt sann. Annars är $\gcd(a, p) = 1$ och enligt Eulers sats har vi

$$1 \equiv a^{\varphi(p)} \equiv a^{p-1} \pmod{p}.$$

Efter multiplikation i båda led med a är satsen bevisad.

Vi kan nu tack vare Fermat enkelt räkna ut höga potenser modulo primtal. Modulo tal som inte är primtal kan vi använda Eulers sats istället som följande exempel visar:

Exempel 1.4

1. Beräkna 2^{123} modulo 5.
2. Beräkna 89^{212} i $\mathbb{Z}_7$.
3. Beräkna 7^{100} modulo 15.
4. Beräkna de två sista siffrorna i 3^{250}

Lösning:

1. Enligt Fermat är $2^4 \equiv 1 \pmod{5}$. Eftersom vi kan skriva $123 = 4 \cdot 30 + 3$ får vi därför

$$2^{123} \equiv 2^{4 \cdot 30 + 3} \equiv (2^4)^{30} \cdot 2^3 \equiv 1^{30} \cdot 8 \equiv 3 \pmod{5}.$$

2. I $\mathbb{Z}_7$ ha vi $89 \equiv 5$. Så vi gör som på förra uppgiften:

$$89^{212} \equiv 5^{212} \equiv 5^{6 \cdot 35 + 2} \equiv (5^6)^{35} \cdot 5^2 \equiv 1^{35} \cdot 25 \equiv 4 \pmod{7}.$$

3. Vi har $\varphi(15) = (5-1)(3-1) = 8$. Så eftersom 7 och 15 är relativt prima får vi enligt Euler $7^8 \equiv 1 \pmod{15}$, och därför har vi

$$7^{100} \equiv 7^{8 \cdot 12 + 4} \equiv (7^8)^{12} \cdot 7^4 \equiv 1^{12} \cdot 7^4 \equiv 7^2 \cdot 7^2 \equiv 4 \cdot 4 \equiv 1 \pmod{15}$$

4. De två sista siffrorna är talets rest modulo 100, så svaret fås genom att beräkna 3^{250} i $\mathbb{Z}_{100}$. Vi har $\varphi(100) = 40$ enligt exemplet ovan, så

$$3^{250} \equiv 3^{40 \cdot 6 + 10} \equiv 1 \cdot 3^{10} \equiv (3^5)^2 \equiv 243^2 \equiv 43^2 \equiv (40 + 3)^2 \equiv 1600 + 240 + 9 \equiv 49.$$

Slutsiffrorna blev alltså 49.

Som man såg i exemplet är det ibland fortfarande svårt att räkna ut potenser när man tittar modulo höga tal.

I sådana fall kan man använda sig av metoden med **successiv kvadrering**. Vi visar med ett exempel (som liknar det ovan).

Exempel 1.5

Vi ska beräkna 3^{37} modulo 100.

Vi börjar med att i $\mathbb{Z}_{100}$ beräkna $3^2, 3^4, 3^8, 3^{16}$ och så vidare. Varje potens fås enkelt genom att kvadrera föregående och reducera modulo 100. Vi beräknar potenser tills potensen skulle överstiga 37:

$$3^2 = 9 \quad 3^4 = 81 \quad 3^8 = 61 \quad 3^{16} = 21 \quad 3^{32} = 41.$$

Skriv nu 37 binärt: Vi har $37 = (100101)_2 = 32 + 4 + 1$. Därför har vi i $\mathbb{Z}_{100}$

$$3^{37} \equiv 3^{32+4+1} \equiv 3^{32} \cdot 3^4 \cdot 3^1 \equiv 41 \cdot 81 \cdot 3 \equiv 81 \cdot 23 \equiv 63,$$

där vi återanvände våra tidigare potensberäkningar. Slutsats: $3^{37} \equiv 63 \pmod{100}$.

Samma metod fungerar modulo andra tal än 100, men det blir lite krångligare att beräkna resterna.

Fermats lilla sats kan också användas till ett enkelt primtalstest.

Sats 1.7

Fermats primtalstest

Låt p vara ett heltal. Om det finns ett tal a så att $a^p \not\equiv a \pmod{p}$ så är p inte ett primtal.

Bevis

Satsen är precis det kontrapositiva påståendet till Fermats lilla sats!

Notera dock att bara för att det gäller att $a^p \equiv a \pmod{p}$ för alla a så behöver inte p vara ett primtal! Det finns sammansatta tal som uppfyller $a^p \equiv a \pmod{p}$ för alla a - sådana kallas Carmichael-tal. Det minsta Carmichael-talet är 561.

Exempel 1.6

Är $p = 48189803$ ett primtal? Är 4793317 ett primtal? Vi testar med en dator att $2^p \equiv 35066457 \pmod{p}$. Därför är p inte ett primtal.

Vi testar också att $2^q \equiv 2 \pmod{q}$ - men vi kan inte dra någon slutsats. Vi testar också att $3^q \equiv 3 \pmod{q}$, men hur många test vi än gör så kan vi inte dra slutsatsen att q är ett primtal.

Observera att trots att vi lyckades visa att p inte är ett primtal så ger testet ingen information av vilka faktorerna kan vara!

1.3 RSA-algoritmen

1.3.1 Introduktion

Det är viktigt att kunna kommunicera på ett krypterat sätt, så att även om någon avlyssnar meddelandet så är informationen otydbar.

För att åstadkomma detta i modern tid publicerade Rivest–Shamir–Adleman sin RSA-algoritm. Den bygger på att alla har en hemlig och en offentlig ”nyckel” (som egentligen bara är stora tal).

Alla känner varandras offentliga nycklar, men ingen känner till någon annans hemliga nyckel. Om Bob vill skicka ett hemligt meddelande till Alice så kan han använda Alices offentliga nyckel för att designa ett krypterat meddelande. Meddelandet kan sedan skickas på öppna kanaler, och endast Alice kan med sin hemliga nyckel avkoda meddelandet.

Algoritmen bygger på det faktum att det är praktiskt sett omöjligt att givet en produkt $n = pq$ av två stora primtal kunna hitta de två faktorerna p och q .

1.3.2 Från text till heltal och tillbaka

Algoritmen jobbar endast med tal, så för att skicka ett textmeddelande behöver man först komma överens om ett sätt att översätta mellan text och heltal. Detta kan man komma

överens om offentligt - man kan ju exempelvis para ihop tecken med tvåsiffriga heltal enligt

$$(A, B, C, \dots) \leftrightarrow (10, 11, 12, \dots)$$

och sedan andra tecken med

$$(\text{mellanrum}, \text{punk}, \text{komma}, \text{streck}, \text{kolon}, \text{frågetecken}, \text{utropstecken}, \dots) \leftrightarrow (40, 41, \dots).$$

Sedan slår man bara ihop meddelandet till ett enda stort heltal, exempelvis får vi

$$\text{"hej!"} \longleftrightarrow 17141946$$

Om meddelandet blir för långt delar man upp det i bitar av förutbestämd storlek, och krypterar t.ex. 20 tecken åt gången. Detta steg är inte så intressant från en matematisk synvinkel.

1.3.3 Nyckelgenerering

Om man vill delta i RSA-samhället behöver man skapa sin offentliga och hemliga nyckel. Detta gör man såhär:

1. Välj två stora primtal p och q .
2. Beräkna heltalen $n = pq$ och $\varphi(n) = (p-1)(q-1)$.
3. Välj ett heltal e så att $1 < e < (p-1)(q-1)$ och så att $\gcd(e, (p-1)(q-1)) = 1$. Din offentliga nyckel är heltalsparet (n, e) - publicera dessa tal öppet.
4. Hitta det minsta positiva talet d så att $d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$. Din hemliga nyckel består av detta tal d - håll talet för dig själv. Talen $p, q, (p-1)(q-1)$ behövs inte i avkodningen men måste också hemlighållas eftersom de kan användas för att beräkna d .

Nu har du alltså skapat en offentlig nyckel (n, e) och en hemlig nyckel d . På webbplatser som använder RSA-kryptering används idag tal n i storleksordningen 2048 bits. Detta gör det praktiskt omöjligt att hitta dess faktorer p och q .

1.3.4 Kryptering

Säg nu att man vill skicka mig ett hemligt meddelande. Man hämtar då min offentliga nyckel (n, e) . Man skriver sedan om meddelandet som ett heltal M . Här måste $M < n$, annars får man bryta upp meddelandet i stycken.

Sedan beräknar man $C = M^e \pmod{n}$, detta går snabbt för en dator. Då blir M alltså ett heltal $< n$, vårt krypterade meddelande. Detta kan man skicka till mig över en öppen kanal.

1.3.5 Avkryptering

Jag mottar meddelandet C . Jag använder sedan min hemliga nyckel d för att beräkna $C^d \pmod{n}$. Resultatet blir det ursprungliga meddelandet M .

1.3.6 Bevis för att det fungerar

Det enda som ska bevisas är att verkligen $C^d \equiv M \pmod{n}$.

Att $ed \equiv 1 \pmod{\varphi(n)}$ innebär att $ed - 1 = k \cdot \varphi(n)$. Därför blir

$$C^d \equiv (M^e)^d \equiv M^{ed} = M^{ed-1} \cdot M \equiv M^{\varphi(n) \cdot k} \cdot M \equiv (M^{\varphi(n)})^k \cdot M \equiv 1^k \cdot M \equiv M \pmod{n}.$$

(Här antog vi i implicit i räkningen att M inte var delbart med p eller q , men man kan verifiera att resultatet också gäller i dessa specialfall)

Övningsuppgifter

Problem märkta ★ är lite svårare, hoppa över dem om du fastnar.

Problem märkta (T) är tagna från gamla tentor (ej nödvändigtvis från denna kurs).

1.1 Lös vart och ett av följande kongruenssystem genom att gissa en lösning.

$$(a) \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 4 \pmod{5} \end{cases} \quad (b) \begin{cases} x \equiv 7 \pmod{101} \\ x \equiv 2 \pmod{5} \end{cases} \quad (c) \begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

1.2 (T) Lös kongruenssystemet

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{9} \end{cases}$$

Genom

(a) Successiv substitution.

(b) Formeln i Sats 1.3

1.3 Lös följande ekvationssystem

$$(a) \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 10 \pmod{26} \end{cases} \quad (b) \begin{cases} x \equiv 8 \pmod{20} \\ x \equiv 5 \pmod{49} \end{cases}$$

1.4 (T) Lös kongruenssystemet

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{9} \\ x \equiv 3 \pmod{25} \end{cases}$$

1.5 ★ Lös vart och ett av följande kongruenssystem.

$$(a) \begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 1 \pmod{15} \end{cases} \quad (b) \begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{15} \end{cases}$$

1.6 Sun-Tzu som ursprungligen formulerade satsen hade som exempel följande problem (fritt översatt):

Det finns ett par saker av okänt antal.

Om vi grupperar dem i högar om tre så blir två över.

Om vi grupperar dem i högar om 5 så blir tre över.

Om vi grupperar dem i högar om 7 så blir två över.

Hur många saker har vi?

Lös Sun-Tzus problem!

1.7 Hitta alla lösningar till följande ekvationssystem

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 8 \pmod{11} \end{cases}$$

1.8 Beräkna $\varphi(30)$ genom att skriva ned alla element i mängden

$$\{a \mid 1 \leq a \leq 30 \text{ och } \gcd(a, 30) = 1\}.$$

1.9 Beräkna

- (a) $\varphi(13 \cdot 11)$
- (b) $\varphi(3^5)$
- (c) $\varphi(99)$
- (d) $\varphi(5^3 \cdot 31^2)$

1.10 Det finns en alternativ formel för att beräkna $\varphi(n)$: om $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ så har vi

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

- (a) Beräkna $\varphi(11 \cdot 13)$ med formeln
- (b) Beräkna $\varphi(18)$ och $\varphi(36)$ och $\varphi(72)$ med formeln
- (c) Bevisa att formeln är sann!

1.11 ★ Hitta alla tal n som uppfyller $\varphi(n) = \frac{n}{2}$

1.12 Använd Fermats lilla sats för att beräkna 29^{437} modulo 13. Ditt svar skall ligga mellan 0 och 13.

1.13 Använd Eulers sats för att beräkna 22^{239} modulo 15. Ditt svar skall ligga mellan 0 och 15.

1.14 Använd Eulers sats för att beräkna 41^{437} modulo 12. Ditt svar skall ligga mellan 0 och 12.

1.15 ★ Lös ekvationen $x^{103} \equiv 4 \pmod{11}$.

Tips: Använd först Fermats lilla sats för att förenkla ekvationen

1.16 Med en dator har vi beräknat att ett par kongruenser håller:

- (a) $541^{2899590618} \equiv 2265131892 \pmod{2899590619}$ kan vi dra någon slutsats om huruvida talet 2899590619 är ett primtal eller sammansatt?
- (b) $7784325556 \equiv 1 \pmod{784325557}$ kan vi dra någon slutsats om huruvida talet 784325557 är ett primtal eller sammansatt?
- (c) $31^{512461} \equiv 31 \pmod{512461}$ kan vi dra någon slutsats om huruvida talet 512461 är ett primtal eller sammansatt?

1.17 Beräkna 17^{131} modulo 241 med successiv kvadrering. Ditt svar skall ligga mellan 0 och 240. Använd en enkel miniräknare till denna uppgift!

1.18 Bestäm de två sista siffrorna i talet 43^{451}

1.19 En student ska beräkna 13^{25} i $\mathbb{Z}_{11}$. Studenten skriver:

Eftersom $13 = 2$ och $25 = 3$ i $\mathbb{Z}_{11}$ får vi $13^{25} = 2^3 = 8$ i $\mathbb{Z}_{11}$

Förklara vad som är fel i studentens argument.

1.20 I den här uppgiften ska du gå igenom RSA-algoritmen för små primtal, notation är som i texten ovan. Du ska först generera ditt nyckelpar. Du har valt de två primtalen $p = 11$ och $q = 3$.

- (a) Beräkna n och $\varphi(n)$.
- (b) Du väljer $e = 3$. Verifiera att e och $\varphi(n)$ är relativt prima.
- (c) Beräkna d , alltså det minsta positiva tal som uppfyller $ed \equiv 1 \pmod{\varphi(n)}$.
- (d) Skriv ned din offentliga och hemliga nyckel.
- (e) Någon vill skicka meddelandet $M = 7$ till dig. Vad blir det krypterade meddelandet?
- (f) Du tar emot det krypterade meddelandet C från förra deluppgiften. Använd din hemliga nyckel för att avkryptera meddelandet och verifiera att det blir korrekt.

1.21 Gå igenom samma steg som i föregående uppgift fast med talen

$$(p, q, e, M) = (13, 7, 5, 50)$$

- 1.22 I nyckelgenereringen vid RSA väljer man $p = 67$ och $q = 71$. Vilket är det minsta talet e som man kan välja som del av sin offentliga nyckel?
- 1.23 ★ Alices offentliga RSA nyckel är $(n, e) = (6588529, 23)$. Alice hemlighåller faktorerna för n , men Eva har lyckats få reda på att $\varphi(n) = 6583284$. Hjälp Eva att faktorisera n ! Skriv sedan ned en allmän algoritm för hur man givet n och $\varphi(n)$ kan hitta p och q .

Kortfattade svar till övningsuppgifterna

1.1

$$(a) x \equiv 9 \pmod{10} \quad (b) x \equiv 7 \pmod{505} \quad (c) x \equiv 16 \pmod{30}$$

1.2 $x \equiv 67 \pmod{180}$

1.3

$$(a) x \equiv 62 \pmod{286} \quad (b) x \equiv 348 \pmod{980}$$

1.4 $x \equiv 353 \pmod{900}$

1.5 Observera att $\gcd(15, 6) \neq 1$, Kinesiska restsatsen håller inte!

$$(a) x \equiv 1 \pmod{30} \quad (b) \text{Lösning saknas.}$$

1.6 $23 + 105k$ saker för något $k \in \mathbb{N}$.

1.7 $x \equiv 206 \pmod{1155}$

1.8 $\varphi(30) = |\{1, 7, 11, 13, 17, 19, 23, 29\}| = 8$

1.9 (a) 120

(b) 162

(c) 60

(d) 93000

1.10 (a) 120

(b) 6 och 12 och 24

(c) Tips: Tänk först vad formeln säger när n är en primpotens: $n = p^k$

1.11 $n \in \{2^k | k > 0\}$

1.12 9

1.13 13

1.14 5

1.15 $x \equiv 5 \pmod{11}$

1.16 (a) 2899590619 är sammansatt enligt Fermats primtalstest.

(b) Vi kan inte dra någon slutsats av testet. (784325557 är faktiskt ett primtal)

(c) Vi kan inte dra någon slutsats av testet. (512461 är faktiskt sammansatt)

1.17 28

1.18 07

1.19 Man kan inte reducera exponenterna på det viset vid modulatoräkning.

1.20 (a) $n = 33$ och $\varphi(n) = 20$.(b) $20 = 2 \cdot 2 \cdot 5$, så $\gcd(3, 20) = 1$.(c) $d = 7$

(d) Offentlig nyckel: $(33, 3)$. Hemlig nyckel: 7

(e) $7^3 \equiv 13 \pmod{33}$. $C = 13$.

(f) $C^d \equiv 13^7 \equiv 7 \pmod{33}$, stämmer.

1.21 Gå igenom samma steg som i föregående uppgift fast med talen

$$(p, q, e, M) = (13, 7, 5, 50)$$

(a) $n = 91$ och $\varphi(n) = 72$.

(b) $\gcd(72, 5) = 1$.

(c) $d = 29$

(d) Offentlig nyckel: $(91, 5)$. Hemlig nyckel: 29

(e) $50^5 \equiv 85 \pmod{91}$. $C = 85$.

(f) $C^d \equiv 85^{29} \equiv 50 \pmod{91}$, stämmer.

1.22 $e = 13$

1.23 $6588529 = 2083 \cdot 3163$

Kapitel 2

Binära operationer

2.1 Introduktion

De reella talen är bra till mycket. Med deras hjälp kan man mäta avstånd, hastigheter, beräkna räntekostnader, förändringshastigheter och så vidare. I vissa sammanhang behöver man dock räkna på andra sätt.

Vad är klockan 75893498 timmar till exempel? Adderar vi 24 timmar visar ju klockan samma sak, så i denna situation hade det varit bättre att ha ett talsystem där $24 = 0$. Här kan man utföra beräkningarna i gruppen $(\mathbb{Z}_{24}, +)$.

De komplexa talen är ett välbekant talsystem som har många tillämpningar, de är exempelvis speciellt användbara inom signalbehandling, kontrollteori, elektromagnetism, kvantmekanik, och fluidmekanik.

Inom en del av kemin räknar man med en typ av *symmetrigrupper* för att analysera kristaller. Här består varje "tal" av en symmetri, och två sådana symmetrier kan kombineras för att forma nya symmetrier.

Kvaternioner är ett talsystem som påminner om de komplexa talen, fast istället för en imaginär enhet i så har man tre olika, i, j, k . Kvaternionerna kan användas för att beskriva rotationer i rummet och har därför tillämpats för beräkningar inom bland annat aerodynamik, navigation, datorgrafik, och molekylärdynamik.

För att förstå dessa typer av talsystem, eller *algebraiska strukturer* måste man glömma mycket som man tar för givet vid räkning med reella tal.

2.2 Binära operationer

Definition 2.1

En **binär operation** på en mängd M är en funktion $f : M \times M \rightarrow M$.

En binär operationen tar alltså två stycken element i M och producerar ett tredje element i M . Man brukar införa en symbol som t.ex. $\star$ för den binära operationen och sedan skriva $a \star b$ istället för $f(a, b)$.

Vanlig addition, subtraktion, och multiplikation är exempel på binära operationer på $\mathbb{R}$. Här kan man också ersätta $\mathbb{R}$ med $\mathbb{Z}$, $\mathbb{Q}$, eller $\mathbb{C}$. Notera dock att vi inte kan definiera operationen "subtraktion" på de naturliga talen $\mathbb{N}$ - en binär operation på $\mathbb{N}$ ska ju för varje par av element i $\mathbb{N}$ ge ett nytt element i $\mathbb{N}$, men vi har t.ex. $3 - 5 \notin \mathbb{N}$.

En mängd M tillsammans med en binär operation $\star$ kallas ibland för en **magma**, och vi skriver $(M, \star)$ för magman för att poängtera att den består *både* av en mängd och en binär operation på mängden. Det händer också att man har två olika binära operationer på samma mängd: t.ex. är "heltalen med addition" $(\mathbb{Z}, +)$ en annan algebraisk struktur än "heltalen med multiplikation" $(\mathbb{Z}, \cdot)$. Man kallar ofta binära operationer för "multiplikation" även om den inte behöver ha något med vanlig multiplikation att göra.

Ett enkelt exempel är "sten-sax-påse magman" nedan. Vår mängd består här av tre element:

$$M = \left\{ \text{sten}, \text{sax}, \text{påse} \right\}.$$

Vi definierar en binär operationen $\star$ på M genom att bestämma att produkten av två element är vinnaren i sten-sax-påse, t.ex. $\text{sten} \star \text{sax} = \text{sten}$. Det kan ju också bli oavgjort, så

vi definierar även $\text{sax} \star \text{sax} = \text{sax}$ och så vidare.

Om mängden M är ändlig kan man precis som med vanlig multiplikation beskriva operationen $\star$ med hjälp av en "multiplikationstabell" här skriver vi elementet $a \star b$ i a 's rad och b 's kolonn. Så här ser multiplikationstabellen ut för sten-sax-påse-magman:

$\star$	sten	sax	påse
sten	sten	sten	påse
sax	sten	sax	sax
påse	påse	sax	påse

2.3 Binära operationers egenskaper

Lägg märke till att ett uttryck av formen $a \star b \star c$ saknar entydig betydelse: en binär operation tar ju två element i mängden och producerar ett tredje, så vi kan antingen beräkna $a \star (b \star c)$ eller $(a \star b) \star c$ - det kan hända att dessa faktiskt ger olika resultat. Notera t.ex. att i sten-sax-påse magman så har vi

$$\text{sten} \star (\text{sax} \star \text{påse}) \neq (\text{sten} \star \text{sax}) \star \text{påse},$$

här blir ju vänsterledet sten medan högerledet blir påse . Detta är en ganska ovanlig egenskap bland matematiska objekt.

Definition 2.2

En binär operation på M kallas **associativ** om

$$(a \star b) \star c = a \star (b \star c) \text{ för alla } a, b, c \in M.$$

Man säger då också att magman är associativ. I en associativ magma kan man alltså skriva $a \star b \star c$ utan att det blir otydligt eftersom det då inte spelar någon roll var man sätter parenteserna.

Magman $(\mathbb{Z}, +)$ är associativ och vi kan skriva ett uttryck som $1 + 5 + 7$ utan parenteser eftersom $(1 + 5) + 7 = 1 + (5 + 7)$.

Å andra sidan är magman $(\mathbb{Z}, -)$ inte associativ. Ett uttryck av formen $8 - 3 - 2$ saknar entydig betydelse¹ eftersom $3 = (8 - 3) - 2 \neq 8 - (3 - 2) = 7$.

Definition 2.3

En binär operation på M kallas **kommutativ** eller **abelsk**² om

$$a \star b = b \star a \text{ för alla } a, b \in M.$$

Sten-sax-påse magman ovan är faktiskt kommutativ. Vi är mest vana att räkna med kommutativa operationer: t.ex. är $(\mathbb{R}, +)$ och $(\mathbb{R}, \cdot)$ kommutativa. Men vi känner också till flera exempel på icke-kommutativa operationer. Subtraktion och division är t.ex. inte kommutativa, och matrismultiplikation från linjär algebra är inte heller kommutativ.

Definition 2.4

Antag att $\star$ är en binär operation på M . Om det finns ett element e i M som uppfyller $e \star x = x = x \star e$ för alla $x \in M$ så kallas e för ett **identitetselement** i $(M, \star)$.

När vi betraktar heltalen med multiplikation $(\mathbb{Z}, \cdot)$ så är heltalet 1 ett identitetselement eftersom $1 \cdot x = x = x \cdot 1$ för alla heltal x .

Om vi istället betraktar heltalen med addition $(\mathbb{Z}, +)$ så är heltalet 0 ett identitetselement eftersom $0 + x = x = x + 0$ för alla heltal x .

Exempel 2.1

Låt $M_{2 \times 2}$ vara mängden av 2×2 -matriser med koefficienter som är reella tal. På denna mängd definierar man en binär operation som kallas **matrismultiplikation** enligt följande:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{bmatrix}$$

Med denna binära operation blir $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ett identitetselement.

Nu tittar vi på en rent abstrakt struktur $(\{\text{🍏}, \text{🍉}, \text{🍊}\}, \star)$ där $\star$ beskrivs av multiplikationstabellen nedan

$\star$	🍏	🍉	🍊
🍏	🍊	🍏	🍉
🍉	🍏	🍉	🍊
🍊	🍉	🍊	🍏

¹Det är dock vanligt att man ändå inför *konventioner* för hur uttryck av formen $8 - 3 - 2$ ska beräknas. En dator beräknar exempelvis sådana uttryck från vänster till höger, alltså $(8 - 3) - 2$.

²Efter den norska matematikern Niels Henrik Abel (1802-1829) som bland annat studerade denna typ av algebraiska strukturer.

Här kan vi utläsa från tabellen att 🍉 är ett identitets-element: att multiplicera ett element x med 🍉 ger alltid resultat x .

Sten-sax-påse magman är ett exempel på en algebraisk struktur som inte har något identitets-element.

Sats 2.1

Det kan aldrig finnas mer än ett identitets-element i en för en binär operation.

Bevis

Vi gör ett motsägelsebevis. Antag att e och f är olika identitets-element i $(M, \star)$. Då gäller

$$e = f \star e = f,$$

i första likheten använde vi att f är ett identitets-element, och i andra likheten att använde vi att e är ett identitets-element. Alltså är $e = f$ vilket är en motsägelse. Alltså kan det inte finnas mer än ett identitets-element.

Definition 2.5

Antag att e är ett identitets-element i $(M, \star)$, och låt $a \in M$. En **invers** till a är ett element $b \in M$ så att $a \star b = e = b \star a$.

Om b är en invers till a så blir ju automatiskt också a en invers till b enligt definitionen, vi säger att a och b är *varandras inverser*. Oftast använder man notationen a^{-1} för inversen till a , om den binära operationen är relaterad till vanlig addition så skriver man ibland istället $-a$ för inversen till a .

Här följer ett antal exempel.

Exempel 2.2

- $I(\mathbb{Z}, +)$ är 0 identitets-element. Inversen av ett heltal a är $-a$ eftersom $a + (-a) = 0$. Varje heltal har alltså en invers under operationen $+$.
- $I(\mathbb{Z}, \cdot)$ är 1 identitets-element. Här gäller $1^{-1} = 1$ och $(-1)^{-1} = -1$, men alla andra heltal saknar inverser under $\cdot$.
- $I(\mathbb{Q}, \cdot)$ är 1 identitets-element. Här gäller $(\frac{a}{b})^{-1} = \frac{b}{a}$ när $a, b \neq 0$ eftersom $\frac{a}{b} \cdot \frac{b}{a} = 1$. Detta innebär att alla element utom 0 har en invers i $(\mathbb{Q}, \cdot)$.

Precis som man kan prata om identitets-element för en binär operation kan man också prata om *noll-element*. Vi säger att n är ett *noll-element* för en binär operation $*$ på M om $x * n = n$ och $n * x = n$ för alla $x \in M$.

Exempelvis ser vi att 0 är ett noll-element i $(\mathbb{Z}, \cdot)$, och noll-matrisen är noll-element i $(\text{Mat}_{2 \times 2}(\mathbb{R}), \cdot)$. Å andra sidan är $(\mathbb{Z}, +)$ och sten-sax-påse-magman exempel där noll-element inte existerar.

2.4 Grupper

Definition 2.6

En **grupp** $(G, \star)$ är en mängd G tillsammans med en binär operation $\star$ på G som uppfyller följande tre villkor:

- Operationen $\star$ är associativ, d.v.s. $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in G$.
- Det existerar ett identitetslement för $\star$ d.v.s. det existerar ett $e \in G$ så att $e \star a = a = a \star e$ för alla $a \in G$.
- Varje element i G har en invers d.v.s. för alla $a \in G$ så existerar $a^{-1} \in G$ med $a \star a^{-1} = e = a^{-1} \star a$.

Ibland inkluderar man också villkoret att $(G, \star)$ ska vara **sluten**, alltså att $g \star h \in G$ för alla $g, h \in G$, men egentligen följer det av det faktum att $\star$ är en binär operation på G . Om det är underförstått vilken binär operation $\star$ man pratar om säger man också att G är en grupp när man menar $(G, \star)$.

Som exempel noterar vi att $(\mathbb{Z}, +)$ och $(\mathbb{R}, +)$ och $(\mathbb{Q}, +)$ alla är grupper. Addition är associativ i samtliga fall, identitetslementet är 0 i samtliga fall, och inversen av ett element a är $-a$.

$(\mathbb{R}, \cdot)$ är *inte* en grupp: associativitet gäller och identitetslement finns, men 0 saknar invers: inget element multiplicerat med 0 kan bli 1.

Tar vi bort nollan får vi dock en grupp, det vill säga $(\mathbb{R} \setminus \{0\}, \cdot)$ är en grupp.

Vårt frukt-exempel från tidigare utgör också en grupp:

$\star$			
			
			
			

Här ser vi direkt från tabellen att  är ett identitetslement och att

$$\begin{array}{ccc} \text{apple}^{-1} = \text{orange} & \text{orange}^{-1} = \text{apple} & \text{watermelon slice}^{-1} = \text{watermelon slice} \end{array}$$

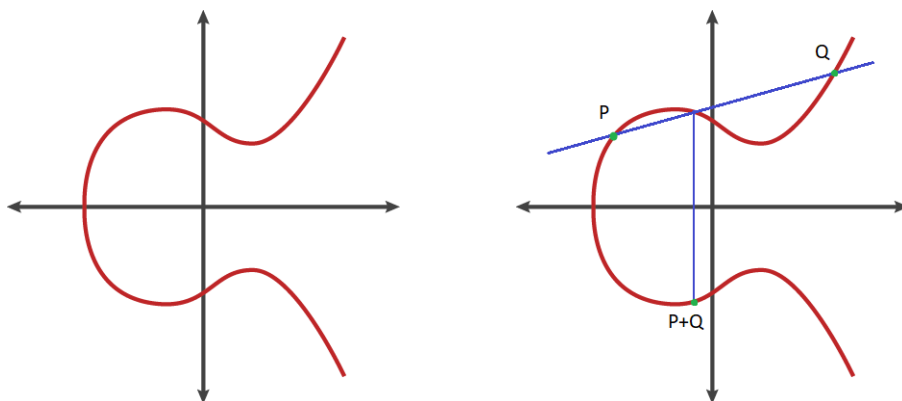
så alla element har inverser. Associativitet gäller också, men det är svårare att se direkt ur tabellen.

En annan grupp med många praktiska³ och teoretiska⁴ tillämpningar är *gruppen associerad med en elliptisk kurva*. Grafen till kurvan $y^2 = x^3 - x + 1$ visas nedan. Man kan definiera summan av två punkter P och Q på kurvan enligt följande: dra en linje mellan P och Q , den skär kurvan i en tredje punkt - spegla denna punkt i x -axeln för att få $P + Q$. Denna

³Elliptiska kurvor över ändliga kroppar används för bland annat kryptering och heltalsfaktorisering.

⁴Teorin för elliptiska kurvor utgjorde ett viktigt steg i beviset av Fermats stora sats.

struktur utgör en grupp⁵!



2.4.1 Exempel: Symmetrigruppen för en triangel

Låt $S_3 = \{f : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \mid f \text{ är bijektiv}\}$. Då blir S_3 en grupp under operationen funktionssammansättning.

Vi kan skriva ett element i S_3 som $f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$.

Med denna notation blir elementen i S_3 :

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Räknar vi ut alla produkter av dessa 6 element får vi följande multiplikationstabell för gruppen S_3 :

$\circ$	e	r_1	r_2	σ_1	σ_2	σ_3
e	e	r_1	r_2	σ_1	σ_2	σ_3
r_1	r_1	r_2	e	σ_3	σ_1	σ_2
r_2	r_2	e	r_1	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	e	r_1	r_2
σ_2	σ_2	σ_3	σ_1	r_2	e	r_1
σ_3	σ_3	σ_1	σ_2	r_1	r_2	e

S_3 kallas den *symmetriska gruppen* på mängden $\{1, 2, 3\}$. Ordet kommer från det faktum att man kan se varje element i S_n som en symmetri - ett sätt att avbilda någonting på sig självt (i vårt fall mängden $\{1, 2, \dots, n\}$).

Man kan tolka detta geometriskt: Om vi tar en liksidig triangel och döper hörnen till 1, 2, 3 så kan varje element i S_3 ses om ett sätt att *flytta triangeln till sig själv*. Titta exempelvis på r_1 ovan. Den flyttar hörn $1 \mapsto 2 \mapsto 3 \mapsto 1$, och motsvarar alltså en *rotation* av triangeln. r_2 roterar åt motsatt håll. σ_1 skiftar hörn 2 med hörn 3, så σ_1 *speglar* triangeln i linjen som går från hörn 1 till mitten på sidan mellan 2 och 3. σ_2 och σ_3 är två andra speglingar, och identitetelementet e är operationen som inte flyttar något alls. Gruppoperationen motsvarar här att utföra flyttningarna efter varandra. Vi ser t.ex. från tabellen att $r_1 \circ (r_1 \circ r_1) = e$ och detta stämmer ju - roterar vi triangeln tre gånger kommer vi tillbaka till utgångsläget!

⁵Egentligen måste vi också introducera en oändlighetspunkt som blir vårt identitets-element på kurvan.

Övningsuppgifter

2.1 I den här övningen ska vi träna på att räkna med abstrakta binära operationer. Betrakta därför sten-sax-påse magman från kapitlets början.

(a) Beräkna $\text{✂} \star ((\text{✂} \star \text{👜}) \star \text{👤})$.

(b) Lös ekvationen $(\text{✂} \star X) \star \text{👜} = \text{✂}$ i sten-sax-påse magman.

(c) Visa att man genom att sätta ut parenteser på olika vis i uttrycket



kan få resultatet att bli både 👤 , ✂ , och 👜 .

(d) Finns det några identitetslement eller nollelement i denna magma?

2.2 De utvidgade reella talen $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$ kan vara användbara när man exempelvis räknar på gränsvärden.

(a) Hur bör man definiera addition $+$ på $\overline{\mathbb{R}}$? Vi vill att operationen ska överensstämma med vanlig addition för reella tal, och att identitetslement och inverser fortfarande ska finnas. Blir den resulterande operationen kommutativ? Associativ? Finns nollelement? Blir strukturen en grupp?

(b) Samma fråga fast för multiplikation på $\overline{\mathbb{R}}$.

(c) Utifrån de binära operationerna du valt i de föregående deluppgifterna, gäller då den "distributiva lagen" $a \cdot (b + c) = a \cdot b + a \cdot c$ i $\overline{\mathbb{R}}$?

2.3 För varje deluppgift nedan, ange om den givna magman är associativ, kommutativ, har identitetslement, ett nollelement, och vilka element som har inverser.

(a) $(\mathbb{R}, \star)$ där $a \star b = ab + 1$.

(b) $(\mathbb{R}, \bullet)$ där $a \bullet b = a^b$.

(c) $(\mathbb{R}, \square)$ där $a \square b = \frac{a+b}{2}$, alltså medelvärde av a och b .

(d) $(\mathbb{R} \cup \{-\infty, \infty\}, \uparrow)$ där $a \uparrow b = \max(a, b)$, produkten av två tal är alltså det största av talen.

2.4 Vilka av följande binära operationer är kommutativa?

(a) $(\mathbb{R}^+, /)$ alltså positiva reella tal med division.

(b) Sten-sax-påse magman.

(c) Den binära operationen $\star$ med följande tabell:

$\star$			

- (d) $(\{f : \mathbb{R} \rightarrow \mathbb{R}\}, \cdot)$ alltså mängden funktioner $\mathbb{R} \rightarrow \mathbb{R}$ med punktvis multiplikation: $(f \cdot g)(x) := f(x)g(x)$.
- (e) $(\{f : \mathbb{R} \rightarrow \mathbb{R}\}, \circ)$ alltså mängden funktioner $\mathbb{R} \rightarrow \mathbb{R}$ med sammansättning: $(f \circ g)(x) := f(g(x))$.

2.5 Ingen av följande exempel på binära operationer utgör grupper. Förklara vad som saknas i vart fall!

- (a) $(\mathbb{N}, +)$, alltså de naturliga talen med addition.
- (b) $(\mathbb{Z}, -)$, alltså de naturliga talen med subtraktion.
- (c) $(\mathbb{Z}, \cdot)$, alltså heltalen med multiplikation.
- (d) Mängden av 2×2 -matriser med matrismultiplikation.
- (e) $(\mathbb{N}_0, \#)$ där $a \# b = |a - b|$.
- (f) Operationen $*$ på $\{a, b\}$ med följande multiplikationstabell

$*$	a	b
a	a	a
b	a	b

2.6 Skriv ned en multiplikationstabellen för en grupp med två element på så vis att de tre villkoren i definitionen av en grupp är uppfyllda. Det finns väsentligen en enda grupp med två element, fundera på vad detta påstående betyder mer precist.

2.7 Låt $(G, \star)$ vara en grupp.

- (a) Bevisa att det bara finns en enda invers till varje $g \in G$.
- (b) Bevisa att om $(G, \star)$ är en grupp och $g, h \in G$ så har vi $(g \star h)^{-1} = h^{-1} \star g^{-1}$.

2.8 I kapitlet visade vi hur gruppen associerad med en elliptisk kurva fungerade.

- (a) Är gruppen associerad med en elliptisk kurva kommutativ?
- (b) Är gruppen verkligen associativ? Prova att välja tre punkter P, Q, R i bilden i detta kapitel och beräkna $(P + Q) + R$ respektive $P + (Q + R)$.

2.9 En **kropp** är en mängd med två binära operationer som uppfyller vissa villkor. Exempel på kroppar är $(\mathbb{R}, +, \cdot)$ och $(\mathbb{Z}_5, +, \cdot)$. I den här uppgiften ska vi räkna i kroppen $(K, +, \cdot)$ där $K = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$. De två binära operationerna ges i följande tabeller:

$+$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\heartsuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
$\spadesuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

$\cdot$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$
$\heartsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\spadesuit$	$\clubsuit$	$\spadesuit$	$\diamondsuit$	$\heartsuit$
$\diamondsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$

- (a) Beräkna $\diamondsuit \cdot (\heartsuit + ((\heartsuit + \clubsuit) \cdot \spadesuit))$.
- (b) Har $(K, +)$ ett identitetselement? Ett nollelement?
- (c) Har $(K, \cdot)$ ett identitetselement? Ett nollelement?
- (d) Hitta de additiva inverserna $-\clubsuit$, $-\heartsuit$, $-\spadesuit$, och $-\diamondsuit$ i $(K, +)$.
- (e) Hitta de multiplikativa inverserna $\heartsuit^{-1}$, $\spadesuit^{-1}$, och $\diamondsuit^{-1}$ i $(K, \cdot)$.
- (f) Lös ekvationen $\spadesuit(x + \heartsuit) = \diamondsuit$. Beskriv hur du hittar lösningen!

(g) "Roten ur" är något vi bara definierat för reella tal. Hur skulle du välja att definiera "roten ur" på K ? Vad blir då $\sqrt{\clubsuit}$, $\sqrt{\heartsuit}$, $\sqrt{\spadesuit}$, och $\sqrt{\diamondsuit}$?

(h) Se om förra deluppgiften kan användas för att lösa ekvationen $x^2 + \heartsuit = \spadesuit$.

2.10 Låt M vara mängden av 2×2 -matriser där summan i varje rad och kolonn är 1. Med andra ord har vi

$$M = \left\{ \begin{bmatrix} a & 1-a \\ 1-a & a \end{bmatrix} \mid a \in \mathbb{R} \right\}$$

(a) Visa att matrismultiplikation (se Exempel 2.3) är en binär operation på M . Kontrollera alltså att om $A, B \in M$ så har vi också $A \cdot B \in M$.

(b) Är $(M, \cdot)$ associativ?

(c) Har $(M, \cdot)$ ett identitetselement?

(d) Finns det ett noll-element i $(M, \cdot)$?

2.11 I kapitlet tittade vi på symmetrier för en triangel - sätt att avbilda triangeln på sig själv genom rotationer och speglingar. Nu tittar vi på en kvadrat med hörn 1, 2, 3, 4 ritade medsols istället. Varje symmetri för kvadraten motsvaras av en bijektion $f : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$. T.ex. motsvaras en medsols rotation 90° av bijektionen $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Bijektionen $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ motsvarar en spegling av kvadraten. Hur många symmetrier har kvadraten? Finns det bijektioner som inte motsvarar symmetrier? Bildar symmetrierna en grupp?

Kortfattade svar till övningsuppgifterna

2.1 (a) 

(b) $X =$  eller $X =$ 

(c) $(\text{bag} \star \text{rock}) \star (\text{rock} \star \text{rock}) = \text{rock}$
 $(\text{bag} \star (\text{rock} \star \text{rock})) \star \text{rock} = \text{rock}$
 $\text{bag} \star (\text{rock} \star (\text{rock} \star \text{rock})) = \text{bag}$

(d) Nej och nej

2.2 (a) För att ∞ ska bete sig som man förväntar sig bör vi för alla $x \in \mathbb{R}$ definiera $x + \infty = \infty = \infty + x$ och $x + (-\infty) = -\infty = (-\infty) + x$. Vi bör också definiera $\infty + \infty = \infty$ och $(-\infty) + (-\infty) = -\infty$. Problemet blir att definiera $\infty + (-\infty)$. För att alla element ska ha inverser måste vi definiera $\infty + (-\infty) = 0 = (-\infty) + \infty$. Den resulterande operationen blir kommutativ, men vi tappar associativitet för operationen:

$5 = 5 + 0 = 5 + ((-\infty) + \infty) \neq (5 + (-\infty)) + \infty = (-\infty) + \infty = 0$. Strukturen blir därför inte en grupp. Operationen har identitetslement 0 men inget nollelement (∞ blir dock *nästan* ett nollelement!).

(b) Det går inte heller att få denna operation associativ.

(c) Nej, $-\infty = \infty \cdot (1 + (-2)) = \infty - \infty = 0$.

2.3 (a) Ej associativ, kommutativ, identitetslement saknas och därmed också inverser, nollelement saknas.

(b) Ej associativ, ej kommutativ, saknar både identitetslement, nollelement och inverser.

(c) Ej associativ, kommutativ, saknar både identitetslement, nollelement, och inverser.

(d) Associativ, kommutativ, identitetslement: $-\infty$, nollelement: ∞ .

2.4 (a) Ej kommutativ.

(b) Kommutativ.

(c) Kommutativ (multiplikationstabellen är symmetrisk).

(d) Kommutativ.

(e) Ej kommutativ.

2.5 (a) Inverser saknas (till alla tal utom 0)

(b) Ej associativ

(c) Inverser saknas (till alla tal utom 1 och -1).

(d) Inverser saknas (noll-matrisen har t.ex. ingen invers).

(e) Icke associativ (men har id.elt och inverser)

(f) a saknar invers (b är identitetslement)

2.6

*	a	b
a	a	b
b	b	a

. Alla 2-elementsgrupper har denna struktur, fast kanske andra namn på a och b . Ett exempel är $(\mathbb{Z}_2, +)$ där a, b kallas 0, 1.

- 2.7 (a) Antag att både a och b är inverser till g . Då gäller
 $a = a \star e = a \star (g \star b) = (a \star g) \star b = e \star b = b$, så $a = b$.
- (b) Vi har $(g \star h) \star (h^{-1} \star g^{-1}) = g \star (h \star (h^{-1}) \star g^{-1}) = g \star e \star g^{-1} = g \star g^{-1} = e$. I omvänd ordning blir produkten också e . Därför är $h^{-1} \star g^{-1}$ inversen till $g \star h$.
- 2.8 (a) Ja! Följer av hur addition definieras.
- (b) Ja! Svårt att visa, men man ser det om man testar med ett par punkter.
- 2.9 (a) ♥
- (b) Identitetselement: ♣. Nollelement saknas.
- (c) Identitetselement: ♥. Nollelement ♣.
- (d) $-\clubsuit = \clubsuit, -\heartsuit = \heartsuit, -\spadesuit = \spadesuit, -\diamondsuit = \diamondsuit$
- (e) Hitta de multiplikativa inverserna $\heartsuit^{-1} = \heartsuit, \spadesuit^{-1} = \diamondsuit, \diamondsuit^{-1} = \spadesuit$
- (f) Multiplicerar vi båda led med $\spadesuit^{-1} = \diamondsuit$ så får vi $x + \heartsuit = \diamondsuit \star \spadesuit$. Om vi adderar $-\heartsuit = \heartsuit$ till båda sidor får vi $x = \spadesuit + \heartsuit = \diamondsuit$. Så lösningen är $x = \diamondsuit$
- (g) Vi kan definiera $\sqrt{a}$ som det x som uppfyller $x \cdot x = a$. Detta ger $\sqrt{\clubsuit} = \clubsuit, \sqrt{\heartsuit} = \heartsuit, \sqrt{\spadesuit} = \diamondsuit$, och $\sqrt{\diamondsuit} = \spadesuit$.
- (h) $x^2 + \heartsuit = \spadesuit \Leftrightarrow x^2 = \spadesuit + (-\heartsuit) = \spadesuit + \heartsuit = \diamondsuit \Leftrightarrow x = \sqrt{\diamondsuit} = \spadesuit$ så $x = \spadesuit$.

2.10 Vi inför notationen $M_a = \begin{bmatrix} a & 1-a \\ 1-a & a \end{bmatrix}$.

- (a) Genom att använda definitionen från kapitlet av matrismultiplikation ser vi att vi får $M_a \cdot M_b = M_{1-a-b+2ab} \in M$.
- (b) Ja: $(M_a \cdot M_b) \cdot M_c = M_{a+b+c-2ab-2ac-2bc+4abc} = M_a \cdot (M_b \cdot M_c)$
- (c) Ja, $M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ är identitetselement.
- (d) Ja, $M_{\frac{1}{2}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ är nollelement. Observera att matrisen med fyra nollor inte är ett nollelement - den ligger inte i magman!

2.11 Kvadraten har åtta symmetrier: 4 rotationer (inklusive identitets-funktionen):

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

och fyra speglingar (en horisontell, en vertikal, två diagonala):

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Det finns dock $4! = 24$ bijektioner på mängden $\{1, 2, 3, 4\}$ - alla motsvarar ej symmetrier, en symmetri måste t.ex. skicka diagonalt motstående hörn till diagonalt motstående hörn, exempelvis är inte $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ en symmetri. Symmetrierna bildar en grupp som heter D_4 - den dihedrala gruppen av ordning 8.