Explorativa Övningar till Aritmetik och Algebra

efter en uppgiftssamling utarbetad av Juliusz Brzezinski

5 februari 2019

Innehåll

1 FUNKTIONER OCH FUNKTIONSBEGREPPET **5**

2 TALSYSTEM – POSITIONSSYSTEM **9**

3 KOMPLEXA TAL **17**

4 MATEMATISK INDUKTION **23**

5 DELBARHET, PRIMTAL, DIVISIONSALGORITMEN **33**

5.1 Heltal och delbarhet 33

5.2 Primtal 39

5.3 Största Gemensamma Delaren och Minsta Gemensamma Multipeln 42

6 ARITMETIKENS FUNDAMENTALSATS OCH DIOFANTISKA EKVATIONER **47**

7 RESTARITMETIKER **59**

8 POLYNOM OCH POLYNOMEKVATIONER **67**

Kapitel 1

FUNKTIONER OCH FUNKTIONSBEGREPPET

Övning A Vad är en funktion?

- Nedan följer beskrivningar av vad en funktion är för något, tagna ut olika läroböcker. Diskutera vilken syn på funktioner de olika beskrivningar ger:

  - M2a, gymnasiebok: Inom ett exempel om pris för bilhyra: Om kostnaden beteckas K, gäller att "K är en funktion av x." Vi kan skriva att $K = 580 + 15x$. Eftersom K beror av x kan vi skriva $K = 580 + 15x$. $K(x)$ utläses "k av x" eller "kx". Lägg märke till att $K(8)$ är ett skrivsätt. Det är inte en multiplikation! Vanligast är att använda bokstaven f, som i ordet funktion.
  - M1b, gymnasiebok: Ordet *funktion* betyder samband. En funktion kan vara något helt vardagligt som t ex att telefonräkningen beror på hur mycket du ringer. Ofta beskrivs funktioner med hjälp av formler, tabeller och grafer.
  - M1c, gymnasiebok, **Definition**. En funktion är en regel som till varje tillåtet x-värde ger precis *ett* y-värde. Då är y en *funktion* av x.
  - Vretblad- Ekstig, s.82: Låt A och B vara två icke tomma mängder. En *funktion från A till B* är en *regel* som till varje element x i A ordnar exakt ett element i B. Detta senare element kallas *bilden* av x genom f och skrivs $f(x)$.

- Skriv ner fem exempel på funktioner, så olika som möjligt.

- Testa funktionslådorna (om kartongerna är på plats i salen): välj en funktion (en kartong), se vad det är för funktion utan att visa det för dina kamrater, låt dem testa olika värde och gissa vilken funktion de var. Hitta gärna på egna funktioner.

Övning B Olika uttrycksform för en funktion

En **funktion** uttrycker ett samband mellan olika saker. Detta kan visas upp på olika sätt

- Med en bild (Cartesisk graf eller annan typ av ritning)
- Med ord som beskriver hur funktionen verkar,
- Med tal: genom en värdetabell (som visar några eller alla möjliga värden),
- Med en algebraisk formel.

Här ger jag några exempel, i den ena eller den andra formen. Precisera rimliga definitionsmängd och värdemängd för varje exempel. Försök att beskriva samma funktion på alla de andra former som passar. Vissa sätt passar inte alla funktioner! Kan du hitta en invers till några av funktionerna? (dvs en funktion som "gör ogjort" vad funktionen har gjort, som tar utvärdet och ger invärdet)

- $x \mapsto 3x + 5$
- Arean av en kvadrat med given sidlängd
- $y = \sqrt{x}$
- Här är en värdetabell där varje tal i den översta raden avbildas till det tal som ligger under (0 eller 1)

  1 2 3 4 5 6 7 8 9 10 ...
  0 1 0 1 0 1 0 1 0 1 ...

- Välj några djur. För varje djur, ange dess läten.

Övning C

Ange namn på varje egenskap som beskrivs nedan, där f är en funktion från mängden A till mängden B: (2p)

- $\forall b \in B,\ (\exists a \in A : f(a) = b)$ f är .....
- $\forall x, y \in A,\ (x \geq y \Rightarrow f(x) \leq f(y))$ f är .....
- $\forall a, c \in A,\ (f(a) = f(c) \Rightarrow a = c)$ f är .....
- $\exists b \in B,\ (\forall a \in A, f(a) = b)$ f är .....

Övning D

Numeriska funktioner kan ha olika egenskaper. Försök formulera definitioner för följande egenskaper i logiska termer.

- växande,
- avtagande,
- jämn (grafen är symmetrisk med avseende på y-axeln),
- udda (grafen är symmetrisk med avseende på punkten i origo),
- begränsad,
- obegränsad.

Övning E

Gå tillbaka till de exempel på funktioner från övningarna ovan

- Vilka är injektiva funktioner (dvs att två olika invärde alltid leder till olika utvärde)?
- Vilka är surjektiva (dvs att alla möjliga utvärde uppnås).
- Vilka är bijektiva (dvs både injektiva och surjektiva)?
- Vilka funktioner går att sätta samman (det som kommer ut från den ena stoppas in i den andra och man betraktar det hela som en enda funktion)? Vad blir sammansättningen?
- Vilka har en invers funktion? Hur kan du formulera den inversa funktionen?

Övning F

Hitta exempel där man använder en variabel på de olika sätten som anges i 3UV-modellen (se artikel änkad från kurshemsidan, Ursini-Trigueros, A model for the uses of variable in elementary algebra).

Kapitel 2

TALSYSTEM – POSITIONSSYSTEM

Räkning är en mycket gammal mänsklig aktivitet som troligen fanns redan i början av vår civilisation*. Det är också troligt att först hade man räkneord motsvarande ett, två möjligen tre föremål och allt som överskred den gränsen uppfattades som "många". Det finns en mycket intressant forskning som visar hur små barn uppfattar t ex fyra föremål†. Man kan föreställa sig att när det gäller räkning återspeglar barnens utveckling den process som för länge sedan var en del av civilisationens framsteg. Olika kulturer utvecklades på olika sätt när det gäller förmågan att räkna och framför allt kunna uttrycka tal både skriftligt och muntligt.

Vårt sätt att skriva tal har sitt ursprung i Indien och kom till Europa i början av 1100–talet genom kontakterna med den arabiska civilisationen. Då översattes från arabiska till latin en bok av den arabiske matematikern al-Chwarizmi (eller al-Khwarezmi) som skrevs nära 300 år tidigare. Boken fick titeln "Liber Algorithmi de numeris Indorum". Denna bok beskriver just vårt nuvarande positionssystem som bygger på bas 10 och som skapades i Indien troligen mellan 400f.Kr och 600f.Kr. En mycket stor betydelse för spridningen av vårt sätt att skriva tal hade boken "Liber abaci" av en italiensk handelsman och matematiker Leonardo Fibonacci (känd som Leonardo från Pisa). I denna bok, som kom ut år 1202, skriver författaren *"Det finns nio indiska tecken:* $9, 8, 7, 6, 5, 4, 3, 2, 1$. *Med hjälp av dessa tecken och tecknet* 0*, som på arabiska kallas "sifr", kan man skriva vilket tal som helst."* Indierna kallade nolltecknet för "sunja", vilket betyder "tom"(tom plats mellan siffror). I Europa översattes termen till "nullus", vilket på latin betyder "intet".

Vad betyder ordet "positionssystem" och varför säger man att det är "decimalt"(eller att dess bas är 10)? Vi har som bekant 10 siffror, vilket antyder att 10 spelar en speciell roll för vårt talsystem. Sambandet med 10 är dock mycket djupare – varje tal kan skrivas som en summa av potenser av 10 och varje siffra säger vilken potens och hur många gånger ingår den i talet. T ex har vi

*efter en text av Juliusz Brzezinski

†Se t ex artikeln "Att utveckla små barns antalsuppfattningäv Elisabet Doverborg och Ingrid Pramling Samuelsson i Nämnaren Tema "Matematik från början", NCM, Göteborg 2000.

$$248 = 2 \cdot 100 + 4 \cdot 10 + 8$$

dvs 248 är summan av 2 stycken $10^2 = 100$, 4 stycken $10^1 = 10$ och 8 stycken $10^0 = 1$. Positionen av varje siffra säger vilken potens av 10 svarar mot denna. När man går från höger till vänster ökar tiopotensen med 1 så att längst till höger har vi enheter ($10^0 = 1$), därefter tiotal ($10^1 = 10$), hundratal ($10^2 = 100$), tusental ($10^3 = 1000$) osv. Talet 2506 kan skrivas som

$$2506 = 2 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10^1 + 6.$$

Observera att man vanligen utelämnar 10^0 och man inte behöver skriva termer som svarar mot siffran 0.

Det svåraste steget i samband med konstruktionen av vårt talsystem var just införandet av siffran 0. De äldsta dokument som innehåller taltecken är mer än 6000 år gamla. Det tog mer än 4000 år innan man kom på tanken att kunna uttrycka alla tal med hjälp av "vanliga siffroröch det som i vårt talsystem är siffran 0. Det finns onekligen en psykologisk svårighet relaterad till acceptansen av siffran och talet 0. Vi ägnar en övning nedan åt den problematiken.

Vårt talsystem är ett resultat av en mycket lång och invecklad historisk utveckling. Låt oss notera att det finns kulturer som kom fram till andra talsystem med andra baser än 10. T ex har Mayaindianerna utvecklad ett system som i princip bygger på bas 20. Det finns även idag kulturer på öar i närheten av Nya Guinea som använder talsystem uppbyggda kring bas 5. 4000 f.Kr. hade sumererna, som bodde i i delar av dagens Irak, ett talsystem som byggde på bas 10. 1500 år senare förvandlades detta talsystem inom samma geografiska område till ett system med bas 60 som är mycket bättre känt tack vare talrika utgrävningar (uppdelningen av timmar i minuter och minuter i sekunder är troligen en kvarleva av detta system). Det finns mycket intressanta teorier om orsaker till denna förvandling. Under historiens gång fanns olika idéer om att ersätta vårt decimala system med ett system med bas 12. Bland annat var Karl den XII en varm anhängare av en sådan förändring (ett system med bas 12 kan spåras i olika sammanhang – vilka?).

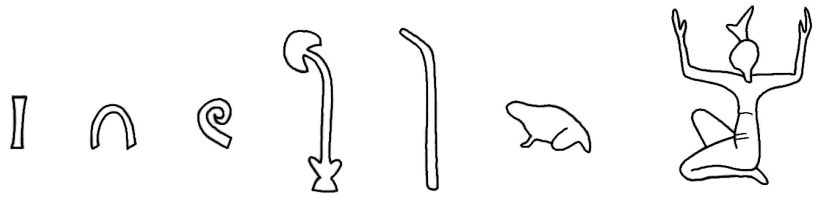
Vi ger exempel på andra positionssystem i samband med övningen nedan.

Övning A

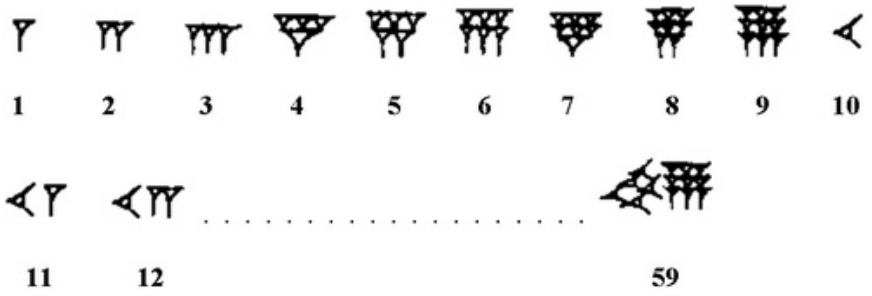
1. Skriv ditt födelseår och din ålder med hjälp av det Egyptiska talsystemet och av det Babylonska talsystemet (se bilderna nedan). Det Babylonska talsystemet har bas 60, men skrivs med hjälp av bara två symboler: ettor och tior.

2. Skriv talen 23054 och 675003 som summor av tiopotenser med motsvarande siffror som koefficienter.

Figur 2.1: Egyptiska tal: ett additivt system med bas 10



Figur 2.2: Babylonska tal: ett positionssystem med bas 60



Example:

3756 =

(3756 = 1 * 60^2 + 2 * 60 + 36)

3. Fundera över skillnaden mellan användningen av termer “siffra” och “tal". Är t ex 2 en siffra, ett tal eller bådadera (beroende på sammanhang)?

4. Varför kan talet 0 (siffran 0) skapa ett psykologiskt problem när det introduceras? Kan associationer av typen “noll är det ingenting"(citat tagen från en lärobok till första klassen) bidra till detta?

5. Romerska siffror som fortfarande används ganska ofta väcker associationer till en annan bas än 10. Vilken? Försök motivera Din bedömning!

6. Datorer använder s k binärt positionssystem. Dess bas är 2 i stället för 10. Detta system är speciellt lämpligt för datorer därför att varje tal kan skrivas med hjälp av enbart två siffror – 0 och 1[‡]. Datorer “förstår"inmatningen av ett sådant tal som en sekvens av signaler som svarar mot två olika tillstånd (impuls och avsaknad av impuls eller en svag impuls och en stark impuls). I stället för potenser av 10 används potenser av 2. T ex är i det binära systemet:

$$11101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1.$$

Vi har alltså $11101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 = 16 + 8 + 4 + 1 = 29$. Ibland skriver man $(11101)_2 = 29$ dvs man skriver basen 2 som index. Observera att vi skriver 2 i stället för 2^1 och vi utelämnar $2^0 = 1$ i notationen. Skriv talen $(11011)_2$ och $(110011)_2$ i tiosystemet.

Vad vinner man och vad förlorar man i det binära systemet i förhållande till det decimala?

7. Försök skriva talen 51 och 95 i binära systemet.

8. Talens namn i olika språk tyder på att för länge sedan använde man andra positionssystem. Ta reda på t ex räkneord för 80 i danskan (och eventuellt franskan). Vilket positionssystem kunde påverka dagens termer?

Divisionsalgoritmen för heltal kan också användas för att uttrycka tal i olika **positionssystem**. Som bekant använder vi bas 10 för att skriva tal. Detta innebär att t ex $128 = 1 \cdot 10^2 + 2 \cdot 10 + 8$, $6405 = 6 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10 + 5$ osv. Våra erfarenheter av decimalsystemet säger att varje naturligt tal N kan skrivas entydigt på formen:

$$(*) \qquad N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

där a_0, $a_1, \ldots, a_k$ är talets N siffror dvs $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Vårt positionssystem är långt ifrån unikt. Man vet t ex att i Babylonien för flera tusen år sedan använde man ett positionssystem med bas 60 (uppdelningen av timmar i 60 minuter och minuter i 60 sekunder är ett arv

[‡]Binära systemet används också av vissa stammar i Mikronesien. Om detta vittnar termer: 1 “ke-yap", 2 “pullet", 3 “ke-yap-pullet", 4 “pullet-pullet". Tyvärr kallas allt som är större än 4 “mycket". Jfr artikeln om barnens antalsuppfattning som citeras i början av denna övning.

från den tiden). Inkaindianerna använde både bas 5 och 10, mayaindianerna däremot använde "vigesimalsystemet" dvs bas 20. De franska räkneorden för också tanken till bas 20. Moderna datorer använder oftast baser 2, 8 och 16. Vad betyder dessa påståenden? De säger att i stället för 10 i likheten $(*)$ ovan kan man använda ett helt godtyckligt naturligt tal $b > 1$. Det enda som förändras är att siffrorna a_i är då $0, 1, \ldots, b-1$.

Först visar vi ett exempel som illustrerar hur man kan skriva om ett heltal från bas 10 till en annan bas. Därefter visar vi den allmänna satsen om representationer i godtyckliga baser.

(2.1) Exempel. (a) Vi skall skriva talet 97 i bas 5. Man dividerar 97 med 5 och därefter upprepar samma procedur med kvoten osv:

$$97 = 5 \cdot \underline{19} + 2,$$

$$19 = 5 \cdot \underline{3} + 4,$$

$$3 = 5 \cdot \underline{0} + 3.$$

Resterna nerifrån uppåt ger siffrorna i bas 5 dvs

$$97 = 3 \cdot 5^2 + 4 \cdot 5 + 2.$$

Alltså är 97 i bas 5 lika med 342. Man brukar skriva: $97 = (342)_5$. Hur kan man motivera denna procedur? Det räcker att göra insättningar (vi skriver den understrukna faktorn först):

$$97 = \underline{19} \cdot 5 + 2 = (\underline{3} \cdot 5 + 4) \cdot 5 + 2 = \underline{3} \cdot 5^2 + 4 \cdot 5 + 2 = 3 \cdot 5^2 + 4 \cdot 5 + 2.$$

(b) Vi skall skriva talet $N = 29$ i bas 2. Siffrorna i bas 2 är endast två: 0 och 1 (datorer bygger på den enkla formen!). Vi använder divisionsalgoritmen flera gånger:

$$29 = 2 \cdot \underline{14} + 1,$$

$$14 = 2 \cdot \underline{7} + 0,$$

$$7 = 2 \cdot \underline{3} + 1,$$

$$3 = 2 \cdot \underline{1} + 1,$$

$$1 = 2 \cdot \underline{0} + 1.$$

Tittar vi på resterna nerifrån uppåt får vi siffrorna i bas 2 dvs $29 = (11101)_2$ dvs

$$29 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1.$$

Precis som i första fallet gör vi insättningar:

$$29 = \underline{14} \cdot 2 + 1 = (\underline{7} \cdot 2) \cdot 2 + 1 = \underline{7} \cdot 2^2 + 1 =$$

$$(\underline{3} \cdot 2 + 1) \cdot 2^2 + 1 = \underline{3} \cdot 2^3 + 1 \cdot 2^2 + 1 = (\underline{1} \cdot 2 + 1) \cdot 2^3 + 1 \cdot 2^2 + 1 =$$

$$1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1.$$

□

Nu visar vi vår allmänna sats:

(2.2) Sats. *Låt $b > 1$ vara ett naturligt tal. Då kan varje naturligt tal N skrivas entydigt på formen*

$$N = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

där "siffrorna" $a_0, a_1, a_2, \ldots, a_k$ är naturliga tal och $0 \leq a_i < b$.

Bevis. Vi visar satsen med matematisk induktion med avseende på N. Om $N < b$ så är påståendet klart – vi har $N = a_0$. Låt oss anta att satsen är bevisad för alla naturliga tal mindre än $N \geq b$. Vi visar satsen för talet N. Låt b^k vara den största potensen av b som inte är större än N dvs $b^k \leq N$ och $N/b^k < b$. Enligt divisionsalgoritmen är

$$N = b^k q + r,$$

där $0 \leq r < b^k$ och $0 < q < b$. Kvoten q och resten r definieras entydigt av N. Nu betecknar vi q med a_k. Men $r < b^k \leq N$ så att enligt induktionsantagandet kan vi skriva

$$r = a_{k-1}b^{k-1} + \cdots + a_1 b + a_0,$$

där $0 \leq a_i < b$, vilket bevisar satsen. □

Övning B

Att gissa ett tal. Försök förklara hur man gissar de tre talen x, y och z i följande sifferlek:

- Tänk på ett tal mellan 0 och 9 (säg, x);
- Multiplicera talet med 2;
- Addera 1;
- Multiplicera med 5;
- Addera ett annat tal mellan 0 och 9 (säg, y);
- Multiplicera med 10;
- Addera ett annat heltal mellan 0 och 9 (säg, z);
- Vilket tal har du fått?

Låt oss anta att talet som man har fått är N. Räkna ut $N - 50$. Siffrorna i detta tal är just x, y och z (i denna ordning). Testa med Dina gruppkamrater!

Övning C

1. Skriv talen 555 i det binära systemet (dvs i bas 2) och i det hexadecimala systemet (dvs i bas 16). Kan Du förklara fördelar och nackdelar i samband med användningen av olika baser?

   Anmärkning. I det hexadecimala systemet används oftast A, B, C, D, E och F för att beteckna siffrorna $10, 11, 12, 13, 14$ och 15.

2. Skriv i vårt vanliga decimala system talen $(1234)_5$ och $(1234)_6$.

• Se även Vretblad-Ekstig, avsnitt 2.6 och tillhörande övningar.

Kapitel 3

KOMPLEXA TAL

Övningens syfte är att bekanta sig med **komplexa tal**. De komplexa talen, som är en utvidgning av de reella talen, kom till på 1400–talet då man försökte lösa kvadratiska ekvationer som t ex $x^2+1=0$, $x^2-2x+2=0$ osv. Man kände redan till existensen av en allmän formel för kvadratiska ekvationer:

$$x^2+px+q=0$$

har två reella lösningar

$$x_1=-\frac{p}{2}-\sqrt{\frac{p^2}{4}-q} \quad \text{och} \quad x_2=-\frac{p}{2}+\sqrt{\frac{p^2}{4}-q}$$

om bara **diskriminanten** $\Delta=p^2-4q\geq 0$ (om $\Delta=0$ så är uttrycket under rottecknet i lösningarna lika med 0 så att det finns en så kallad **dubbelrot** $x_1=x_2=-\frac{p}{2}$).

Om man t ex försöker lösa ekvationen $x^2-2x+2=0$ i enlighet med dessa formler så får man

$$x_1=1-\sqrt{-1}, \quad x_2=1+\sqrt{-1}.$$

Detta verkar vara meningslöst, men om man betecknar $\sqrt{-1}=i$, accepterar att $i^2=-1$ och sätter in t ex x_1 i ekvationen så får man

$$\text{V.L.}=(1-i)^2-2(1-i)+2=1-2i+i^2-2+2i+2=0=\text{H.L.},$$

dvs x_1 satisfierar ekvationen. Även x_2 är en "lösning". Observera att vi inte bara har accepterat

symbolen i och dess egenskap $i^2 = -1$, utan också de vanliga räknelagarna för "de gamla talen" i samband med t ex kvadrering. Under 1400-talet och i början av 1500-talet började man lösa kvadratiska ekvationer och även ekvationer av högre grad med dessa nya tal. Tänk Dig ett barn som endast känner till de naturliga talen och plötsligt kommer i kontakt med ett problem som leder till ekvationen $2x = 1$ (att dela något i två lika delar). Då dyker ett behov upp av ett nytt tal $\frac{1}{2}$. Det var ungefär samma situation, fast på en mer avancerad nivå, som ledde till komplexa tal.

Det tog drygt 300 år innan man kom underfund med en helt tillfredsställande definition av de komplexa talen som från början definierades som: uttryck på formen

$$a + bi, \text{ där } a, b \in \mathbb{R} \text{ och } i^2 = -1.$$

a kallas vanligen **realdelen** och b **imaginärdelen** av z. Vi bekantar oss med den formella definitionen i avsnittet om "Talsystem". I detta avsnitt kommer vi att arbeta med komplexa tal precis som man har arbetat med dessa tal under flera hundra år genom att acceptera definitionen ovan.

Observera att två komplexa tal $a+bi$ och $c+di$ betraktas som lika då och endast då $a = c$ och $b = d$. Man utför alla vanliga operationer: addition, subtraktion, multiplikation och division på precis samma sätt som för vanliga reella tal – det enda som tillkommer är villkoret $i^2 = -1$. Syftet med denna övning är att bekanta sig med de grundläggande egenskaperna hos de komplexa talen:

- de fyra räknesätten,
- konjugat och absolutbelopp,
- geometrisk tolkning av komplexa tal,
- polär framställning,
- lösning av ekvationer: kvadratiska och binomiska,
- enhetsrötter.

Vi följer Kapitel 6 i Vretblads bok.

Övning A

1. Lös följande uppgifter i Vretblads bok: 6.2, 6.4, 6.5.
2. Låt $z_1 = a_1 + b_1 i$ och $z_2 = a_2 + b_2 i$ beteckna två komplexa tal. Hur definieras summan $z_1 + z_2$, skillnaden $z_1 - z_2$, produkten $z_1 z_2$ och kvoten $\frac{z_1}{z_2}$ (här antas $z_2 \neq 0$)? Skriv ut definitionerna med ledning av avsnitt 6.2 i Vretblads bok.

Övning B

1. Låt $z = a + bi$. Vad menas med det konjugerade talet $\bar{z}$ (se avsnitt 6.2 i Vretblads bok).
2. Låt $z = 3 + 5i$. Beräkna $\bar{z}$.
3. Låt z, z_1, z_2 beteckna komplexa tal. Bevisa formlerna:
   (a) $\overline{\bar{z}} = z$,
   (b) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$,
   (c) $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$,
   (d) $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$ $(z_2 \neq 0)$,

Övning C

1. Låt $z = a + bi$. Vad menas med absolutbeloppet $|z|$?
2. Låt z, z_1, z_2 beteckna komplexa tal. Bevisa formlerna:
   (a) $|z|^2 = z\bar{z}$,
   (b) $|z| = |\bar{z}|$,
   (c) $|z_1 z_2| = |z_1||z_2|$,
   Ledning. Kvadrera likheten och använd (a)!
   (d) $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$ $(z_2 \neq 0)$.
3. Beräkna två heltal k, l så att $(23^2 + 35^2)(10^2 + 100^2) = k^2 + l^2$. Använd komplexa tal och (c). Kan Du generalisera Ditt resultat?
4. Lös följande uppgifter i Vretblads bok: 6.9 c), d), e), f).

Övning D

Man tolkar det komplexa talet $z = a + bi$ som punkten (a, b) i ett vanligt rätvinkligt koordinatsystem (se avsnitt 6.4 i Vretblads bok). Man identifierar z med punkten (a, b) – man säger ofta "punkten z" om (a, b). Ibland vill man se talet z som en vektor – oftast från $(0, 0)$ till punkten (a, b).

1. Rita ett rätvinkligt koordinatsystem och tolka geometriskt följande tal:
   (a) $z = a + bi$ och $\bar{z} = a - bi$ (försök beskriva deras läge i förhållande till varandra);
   (b) $\operatorname{Re} z = a$, $\operatorname{Im} z = b$ och $|z| = \sqrt{a^2 + b^2}$. Kan Du se ett samband mellan $|z|$ och en känd sats?
   (c) $z_1 + z_2$ då $z_1 = a + bi$ och $z_2 = c + di$. Tolka därefter $|z_1 + z_2|$, $|z_1|$ och $|z_2|$;
   Ledning. Summan $z_1 + z_2$ svarar mot diagonalen i den parallellogram som har sina hörn i (de punkter som svarar mot) $(0, 0)$, z_1, z_2 och $z_1 + z_2$.

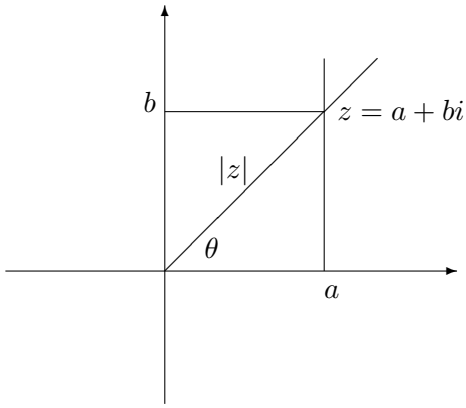
2. Kan Du förklara hur triangelolikheten $|z_1 + z_2| \leq |z_1| + |z_2|$ kan tolkas geometriskt med hjälp av förra uppgiften? (för ett algebraiskt bevis av denna olikhet se boken eller föreläsningsanteckningar).

3. Hur tolkas $z_1 - z_2$ då z_1 och z_2 uppfattas som vektorer från $(0, 0)$ till punkterna z_1 och z_2? Använd samma bild som i förra uppgiften. Hur tolkas $|z_1 - z_2|$? Låt $z_1 = a + bi$, $z_2 = c + di$ och skriv ut $|z_1 - z_2|$ – känner Du igen en känd formel?

4. Lös övningar 6.41 a), b), c), f) i Vretblads bok.

Övning E

1. Betrakta figuren



och förklara varför $a = |z| \cos\theta$ och $b = |z| \sin\theta$. Vi förutsätter att $z \neq 0$.

Anmärkning. Vinkeln θ kallas ett **argument** för z och betecknas $\theta = \arg z$. Ofta väljer man denna vinkel så att $0 \leq \theta < 2\pi$. Om θ är ett argument, så är både $\theta + 2\pi$ och $\theta - 2\pi$ argument för z. Man kan skriva

$$z = a + bi = |z|(\cos\theta + i \sin\theta).$$

Den sista framställningen kallas **polär form**.

2. Skriv på polär form

   (a) $z = 1 + i$,

   (b) $z = \sqrt{3} + i$.

3. Låt $z_1 = |z_1|(\cos\theta_1 + i \sin\theta_1)$ och $z_2 = |z_2|(\cos\theta_2 + i \sin\theta_2)$ vara komplexa tal på polär form. Beräkna produkten $z_1 z_2$ och kvoten $\frac{z_1}{z_2}$. Skriv dessa tal på polär form. Förklara vad som händer med beloppen och med argumenten då man multiplicerar eller dividerar två komplexa tal (se avsnitt 6.4 i boken).

4. Lös uppgift 6.33 i Vretblads bok.

5. Tolka geometriskt förhållandet mellan ett komplext tal $z \neq 0$ och talet iz?

6. Om $z = |z|(\cos\theta + i\sin\theta)$, så är $z^n = |z|^n(\cos n\theta + i\sin n\theta)$, vilket kallas **de Moivres formel** (se Vretblads bok avsnitt 6.4). Lös med hjälp av denna formel uppgifterna 6.73, 6.38 och 6.39 a) i boken.

Övning F

Kvadraträtter och kvadratiska ekvationer.

1. Vad menas med beteckningen $\sqrt{-1}$? Lös ekvationen $z^2 = -1$?

   Anmärkning. Med $\sqrt{a+bi}$ menas vanligen en godtycklig lösning till ekvationen $z^2 = a + bi$. Denna ekvation har två olika lösningar om $a + bi \neq 0$. Ibland fixerar man en lösning genom lämpliga villkor. Man skriver mycket ofta $\sqrt{-1}$ för att just beteckna talet i (och ej $-i$).

2. Beräkna:

   (a) $\sqrt{3+4i}$,

   (b) $\sqrt{7-24i}$ (se boken om Du vill),

   (c) $\sqrt{i}$.

3. I början av detta kapitel finns allmänna formler för lösningar av kvadratiska ekvationer. Använd dessa formler för att lösa ekvationerna 6.53 och 6.56 i Vretblads bok.

Övning G

Binomiska ekvationer. Ekvationerna av typen $z^n = A$, där A är ett komplext tal, kallas **binomiska**. Läs om dessa ekvationer i avsnitt 6.6 i boken. Om $A = |A|(\cos\alpha + i\sin\alpha)$ så ges alla lösningar på formen

$$z_k = \sqrt[n]{|A|}(\cos\frac{\alpha+2\pi k}{n} + \sin\frac{\alpha+2\pi k}{n}),$$

där $k = 0, 1, \ldots, n-1$.

1. Lös ekvationen $z^4 = -16$. Se exempel 1 i avsnitt 6.6. Läs noga. Använd formeln ovan för att lösa denna ekvation.

2. Lös ekvationen $z^3 = 2i - 2$.

Övning H

Enhetsrötter. Lösningarna till ekvationerna $z^n = 1$ kallas **enhetsrötter**. Dessa komplexa tal har många anmärkningsvärda egenskaper och spelar en stor roll i matematiken.

1. Beräkna enhetsrötterna för $n = 2, 3, 4, 5, 6$ och tolka dessa komplexa tal geometriskt (en bild för varje n).

2. Beräkna summan av alla fjärde enhetsrötter dvs alla lösningar till ekvationen $z^4 = 1$. Visa att Ditt resultat kan generaliseras (studera enhetsrötterna i uppgiften ovan).

3. Rita enhetscirkeln i det komplexa planet och välj en godtycklig punkt a på denna cirkel. Låt $z_1,\ z_2, z_3, z_4$ beteckna lösningarna till ekvationen $z^4 = 1$. Beräkna summan av kvadraterna av avstånden mellan a och z_k dvs summan

$$|z_1 - a|^2 + |z_2 - a|^2 + |z_3 - a|^2 + |z_4 - a|^2.$$

Försök generalisera Ditt resultat till enhetsrötterna $z^n = 1$ för godtyckliga n.

Följande övningar i Vretblads bok rekommenderas:

Vretblad: 6.9, 6.17, 6.57, 6.63, 6.65, 6.78, 6.81, 6.82, 6.83.

Kapitel 4

MATEMATISK INDUKTION

Syftet med denna övning är att introducera en av de viktigaste bevismetoderna i matematiken – **matematisk induktion**. Termen "induktion" är lite olycklig därför att matematisk induktion är en i högsta grad deduktiv metod. Men faktum är att ett bevis med hjälp av matematisk induktion mycket ofta baseras på vanlig induktion dvs en serie av matematiska experiment som leder till en generalisering – man formulerar en förmodan (en hypotes) och därefter ger man ett strängt bevis med hjälp av matematisk induktion. Vi skall exemplifiera bevis med matematisk induktion nedan. Du kan också läsa avsnitt 4.2 i Vretblads bok.

Vi börjar med ett exempel för att därefter formulera induktionsprincipen.

Exempel. Undersök vilka belopp som kan betalas med tvåkronors– och femkronorsmynt (t ex i Danmark finns det sådana). Formulera en förmodan och ge ett bevis.

Lösning*. Vi har redan sysslat med den uppgiften i Övning 3. Det är klart att beloppen 1 krona och 3 kronor inte kan betalas. Men det verkar som att varje belopp större än 3 kronor kan betalas med givna mynt ($4 = 2 \cdot 2$, $5 = 5 \cdot 1$, $6 = 2 \cdot 3$, $7 = 2 \cdot 1 + 5 \cdot 1$ osv.). Vi formulerar detta som vår förmodan och försöker ge ett bevis. Vi antar att ett belopp på k kronor, där $k \geq 4$ kan betalas dvs

$$k = 2x + 5y$$

dvs k kronor betalas med x tvåkronorsmynt och y femkronorsmynt. Nu vill vi visa att även beloppet på $k + 1$ kronor kan betalas med dessa mynt.

Vi resonerar så här. Om antalet av femkronorsmynt är minst 1 dvs $y \geq 1$ så ersätter vi ett sådant mynt med 3 stycken tvåkronorsmynt (i stället får vi 6 kronor). I matematiska termer betyder det att

*Uppgiften kan lösas på flera andra sätt.

$$k + 1 = 2(x + 3) + 5(y - 1).$$

Om däremot $y = 0$ dvs man betalar $k = 2x$ kronor med enbart tvåkronorsmynt, så måste $x \geq 2$ (ty $k \geq 4$). I sådant fall ersätter vi två stycken tvåkronorsmynt med en "femma". I matematiska termer:

$$k + 1 = 2(x - 2) + 5$$

Alltså gäller implikationen:

Om ett belopp k kronor kan betalas och $k \geq 4$, så kan beloppet $k + 1$ kronor betalas.

Nu drar vi slutsatsen att varje belopp på minst 4 kronor kan betalas med två– och femkronorsmynt. Vi vet nämligen att 4 kronor kan betalas och möjligheten att kunna betala k kronor med $k \geq 4$ implicerar möjligheten att kunna betala nästa belopp på $k + 1$ kronor. □

Resonemanget ovan är just ett exempel på **matematisk induktion**. Induktionsprincipen fungerar på följande sätt. Man har en följd av påståenden P_1, P_2, P_3, ..., P_n, ... (i vårt exempel ovan är påståendena: P_1 = "4 *kronor kan betalas med givna mynt*", P_2 = "5 *kronor kan betalas med givna mynt*", P_3 = "6 *kronor kan betalas med givna mynt*" osv.). **Induktionsprincipen** säger följande:

Låt $P_1, P_2, \ldots, P_n, \ldots$ vara en följd av påståenden sådan att
1. *det första påståendet P_1 är sant*
och
2. *för varje $k \geq 1$ gäller implikationen: om påståendet P_k är sant så är påståendet P_{k+1} också sant.*
Då är alla påståenden P_n för $n = 1, 2, 3, \ldots$ sanna.

Slutsatsen bygger på följande resonemang: P_1 är sant. Att P_1 är sant medför att P_2 är sant. Alltså är P_2 sant. Att P_2 är sant medför att P_3 är sant. Alltså är P_3 sant. Att P_3 är sant medför att P_4 är sant. Alltså är P_4 sant osv. Vi sluter oss till att P_n är sant för alla $n = 1, 2, 3, \ldots$.

Denna motivering är inte ett bevis av induktionsprincipen som är en mycket viktig egenskap hos de naturliga talen. Diskussion om denna princip kan du läsa mer om i Vretblads Appendix 1 om de naturliga talens egenskaper. Innan vi övergår till övningar låt oss notera att ett bevis av implikationen "*om P_k gäller så gäller P_{k+1}*" kallar man för **induktionssteget**. Förutsättningen att P_k gäller kallas vanligen **induktionsantagandet**.

Det finns flera enkla modifikationer av induktionsprincipen. Vi möter dessa modifikationer i olika bevis. Vi ger exempel på ett antal mycket vanliga tillämpningar av induktionsmetoden i samband med övningar nedan. Vi diskuterar också andra exempel på föreläsningen.

I första hand försök lösa uppgifterna **A** – **G, I**. Du kan hoppa över **H**.

Övning A

1. Man berättar ofta följande händelse ur C.F Gauss † liv. Gauss matematiklärare ville sysselsätta sina elever under en längre stund. Han beordrade dem då att beräkna summan av alla naturliga tal från 1 till 100 dvs summan:

$$\sum_{i=1}^{100} i = 1 + 2 + 3 + \cdots + 100.$$

Gauss, som då var 8 år gammal, kom med sin lösning efter en kort stund – summan är lika med 5050. Gauss tänkte så här. Betrakta i stället två summor:

$$S(100) = 1 + 2 + 3 + \cdots + 99 + 100$$

och

$$S(100) = 100 + 99 + 98 + \cdots + 2 + 1.$$

När man parar ihop motsvarande termer (första med första, andra med andra, osv) så får man 100 par och summan i varje par är 101. Alltså är

$$2S(100) = 100 \cdot 101.$$

Detta ger

$$S(100) = \frac{1}{2}10100 = 5050.$$

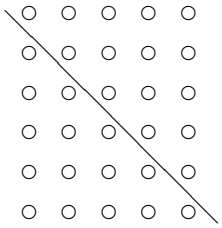
2. Försök generalisera Gauss metod och skriv ut formeln för summan

$$S(n) = \sum_{i=1}^{n} i = 1 + 2 + \cdots + n$$

av n efterföljande heltal.

†Carl Friedrich Gauss (30/4 1777 – 23/2 1855) var en av de mest framstående matematikerna genom tiderna. I sin doktorsavhandling (1799) sysslade han med polynomekvationer och visade en mycket viktig sats som ibland kallas "algebrans fundamentalsats" (idag snarare polynomalgebrans fundamentalsats"). Hans mest kända verk heter "Disquisitiones Arithmeticae" (1801) och handlar mest om talteori. 17 år gammal visade Gauss hur man kan konstruera en regelbunden 17-hörning med passare och linjal. Detta avgjorde hans val mellan matematik och lingvistik som var ett annat av hans stora intressen. Gauss sysslade också med fysik och astronomi.

3. Betrakta följande bild och använd den för att bevisa formeln för $S(n)$ i enlighet med Gauss idé (bilden svarar mot $n = 5$):



4. Ge ett bevis av formeln för $S(n)$ med hjälp av matematisk induktion.

Övning B

1. Betrakta följande bilder och räkna ettorna i varje tabell på två olika sätt: dels i hela kvadraten och dels som summor av ettorna i varje "L-formad vinkel" som du kan dela uppp kvadraten i.

$$1 \qquad \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{matrix}$$

   Vilka formler för antalet ettor i varje kvadrat får man? Kan Du generalisera resultaten till en formel giltig för varje $n \times n$ – kvadrat?

2. Försök nu ge ett induktivt bevis (dvs ett bevis med hjälp av matematisk induktion) för Din formel.

   Ledning. Detta bevis finner Du som exempel i slutet av detta kapitel eftersom det är vårt första exempel på ett bevis av en likhet mellan två uttryck. Men försök först att skriva ett bevis på egen hand. Liknande exempel följer nedan.

Övning C

1. Studera summor

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)}$$

för $n = 2, 3, 4, 5$. Ställ upp en förmodan och bevisa Ditt påstående med matematisk induktion.

2. Observera att

$$\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1}$$

och utnyttja likheten till att bestämma en formel för summan ovan.

Övning D

1. Bevisa med matematisk induktion att

$$\sum_{i=1}^{n} i(i+1) = 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}.$$

2. Man definierar $n! = 1 \cdot 2 \cdots n$ (man utläser symbolen $n!$ som "n fakultet"). Visa att

$$\sum_{i=1}^{n} i \cdot i! = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1.$$

Övning E

Matematisk induktion används mycket ofta för att bevisa olikheter. Vi ägnar denna övning åt olikheter.

1. Studera beviset av olikheten $3^n > n^3$ då $n \geq 4$ i Vretblads bok på sid. 106.

2. Bevisa på liknande sätt olikheten $2^n > n^2$ då $n \geq 5$.

Övning F

1. Betrakta talföljden $1, 3, 6, 10, 15, \ldots$. Kan Du skriva ut några efterföljande tal?

2. Låt a_k beteckna $k-$te talet i följden dvs $a_1 = 1$, $a_2 = 3$, $a_3 = 6$ osv. Ange sambandet mellan a_{k+1} och a_k då $k \geq 1$.

   Anmärkning. Låt $a_1, a_2, \ldots, a_k, a_{k+1} \ldots$ vara en talföljd. En formel som uttrycker a_{k+1} med hjälp av a_k (ibland även tidigare termer som t ex a_{k-1}) kallas en **rekursionsformel** (se exempel i Vretblads bok, avsnitt 4.3.

3. Kan Du uttrycka a_n med hjälp av n? Försök! Svaret finns på slutet av detta kapitell. Bevisa Din formel med matematisk induktion.

4. Lös uppgift 4.47 i Vretblads bok. Observera att man här måste använda en modifikation av induktionsprincipen: Man kontrollerar att *de två första påståendena P_1 och P_2 gäller.* Därefter visar man implikationen: *för varje $k \geq 1$, om P_k och P_{k+1} gäller så gäller också P_{k+2}.*

Övning G

1. Låt $T_n = 6^n - 1$ då $n = 1, 2, 3, \ldots$, dvs $T_1 = 6^1 - 1 = 5$, $T_2 = 6^2 - 1 = 35$, $T_3 = 6^3 - 1 = 215$ osv. Man observerar lätt att alla dessa tal är delbara med 5. Är det sant för varje n? Visa Ditt påstående med matematisk induktion.

   Ledning. Eftersom detta är vår första uppgift som handlar om tillämpning av induktion på delbarhetsegenskaper visar vi en lösning i slutet av denna stencil. Men försök lösa uppgiften själv innan Du tittar på lösningen.

2. För varje $n = 0, 1, 2, 3, \ldots$ är talet $T_n = 7^n - 1$ delbart med 6.

   Anmärkning. Observera att vi numrerar talen från 0 (i Exempel 1 började vi med 1). Notera att en sådan modifikation inverkar inte på induktionsprincipen. Varför?

3. Studera talen $T_n = 2 \cdot 4^n + 1$ för $n = 0, 1, 2, 3, \ldots$. Dessa tal har en gemensam faktor. Vilken? Bevisa Ditt påstående.

4. Studera talen $T_n = 2^{2n-1} + 1$ för $n = 1, 2, 3, \ldots$. Dessa tal har en gemensam faktor. Vilken? Bevisa Ditt påstående.

5. Studera talen $T_n = 2^{4n-2} + 1$ för $n = 1, 2, 3, \ldots$. Dessa tal har en gemensam faktor. Vilken? Bevisa Ditt påstående.

   Anmärkning. Alla uppgifter i denna övning kan lösas (mycket enklare) med hjälp av restaritmetik.

Övning H

Vi skall fortsätta tankegången från Övning B och summera både de naturliga talen och deras kvadrater (om Du tycker att det är roligt så kan Du med samma metoder gå vidare och summera t ex tredje eller fjärde potenser av de naturliga talen osv).

1. Vi börjar med summan

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2.$$

   Studera följande tabeller och summera talen på två olika sätt som i Övning B:

$$
\begin{array}{c}1\end{array}
\qquad
\begin{array}{cc}1&2\\1&2\end{array}
\qquad
\begin{array}{ccc}1&2&3\\1&2&3\\1&2&3\end{array}
\qquad
\begin{array}{cccc}1&2&3&4\\1&2&3&4\\1&2&3&4\\1&2&3&4\end{array}
\qquad
\begin{array}{ccccc}1&2&3&4&5\\1&2&3&4&5\\1&2&3&4&5\\1&2&3&4&5\\1&2&3&4&5\end{array}
\qquad
\begin{array}{ccccc}1&2&3&k&n\\1&2&3&k&n\\1&2&3&k&n\\&&&&\\1&2&3&k&n\\&&&&\\1&2&3&k&n\end{array}
$$

Utnyttja formeln för summation av de naturliga talen som vi fick i uppgiften om summan $1 + 2 + \cdots + n$. Det behövs några omskrivningar innan man kommer åt den sökta summan av kvadraterna. När Du får en formel kontrollera först att den är riktig för, säg, $n = 1, 2, 3, 4$.

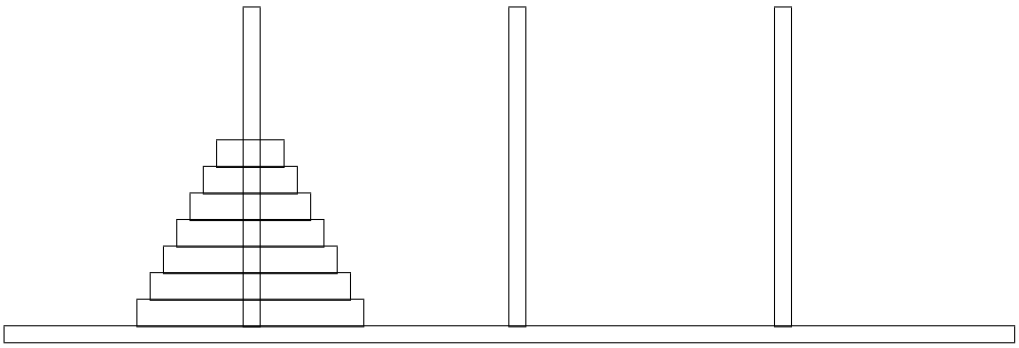
2. Utnyttja de två olika sätten att summera ettorna i Övning B för att få formeln för $S_1(n) = 1 + 2 + \cdots + n$. Den uppgiften är något enklare än förra, men det krävs också en enkel omskrivning.

3. Försök ge en formel för $S_3(n) = \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3$ genom att placera $1^2, 2^2, 3^2, \ldots, n^2$ i stället för $1, 2, 3, \ldots, n$ i tabellerna ovan. Bevisa formeln med matematisk induktion. (Du behöver inte göra den uppgiften om Du inte har tid. För den sökta formeln se eventuellt svar på slutet av denna stencil.)

Övning I

"Tornen i Hanoi". Problemet formulerades år 1883 av den franske matematikern Édouard Lucas under pseudonym M. Claus[‡]. På en platta med 3 pinnar sitter n stycken skivor med olika diameter på en av pinnarna (bilden visar $n = 7$ skivor – detta är antalet skivor på en IKEA–model som kan köpas för 35 kronor).

[‡]Detta enligt Ian Stewarts bok "The Magical Maze" med undertiteln "Seeing the world through mathematical eyes". Boken kom ut 1997 i London. I boken citeras en saga som berättar om bakgrunden till problemet med "Tornen i Hanoi" eller snarare tornen i världens medelpunkt vid Benares templet. I Ian Stewarts bok finns flera mycket intressanta matematiska problem som inte förutsätter några förkunskaper i ämnet.



Dessa skivor skall flyttas till en annan pinne med hänsyn till följande regler:

R1. Endast en skiva kan flyttas vid varje drag och sättas på en annan pinne.

R2. En större skiva får inte placeras på en mindre.

1. Lös uppgiften för $n = 2, 3, 4, 5, 6, 7$ skivor (Du kan "konstruera" Ditt eget spel genom att välja 7 föremål av olika storlek som kan läggas på varandra).

2. Antag att Du har löst problemet för t ex 6 skivor. Hur kan Du beskriva Din strategi för att lösa problemet för 7 skivor?

3. Kan Du bevisa att det alltid går att lösa problemet för varje n? Hur kan man utnyttja matematisk induktion?

4. Hur många drag behövs det för att lösa problemet för n skivor?

Övning J

1. Försök hitta ett fel i följande "bevis" med matematisk induktion. Vi påstår att *alla människor har samma ögonfärg*. Satsen är självklart sann om antalet människor n är lika med 1. Antag att satsen är sann för antalet människor lika med k dvs antag att i varje population med k individer har alla samma ögonfärg. Ta nu $k + 1$ människor. Utelämna en människa i gruppen. De återstående k har samma ögonfärg enligt induktionsantagandet. Ta nu den människa som vi har utelämnat och jämför hennes ögonfärg med en av dem som ingår i gruppen på k människor. De har samma ögonfärg enligt induktionsantagandet. Alltså har alla $k + 1$ samma ögonfärg. Nu gäller påståendet för $n = 1$ och om det gäller för k så gäller det för $k + 1$. Enligt induktionsprincipen gäller påståendet för varje $n = 1, 2, 3, 4, \ldots$ dvs alla människor har samma ögonfärg.

Följande övningar i Vretblads bok rekommenderas:

Vretblad: 4.15 (OBS! summan skall vara $1+2+4+8+\cdot 2^n$, med 4 och inte 3), 4.17, 4.24, 4.33, 4.35, 4.42, 4.46, 4.50.

Några lösningar och svar:

Övning B:

Vi vill visa att för varje $n \geq 1$ gäller likheten

$$1 + 3 + \cdots + (2n-1) = n^2.$$

Först kontrollerar vi att likheten gäller då $n = 1$ ("påståendet P_1"):

$$\text{V.L.} = 1 \quad \text{och} \quad \text{H.L.} = 1^2$$

så att V.L = H.L.

Nu antar vi att likheten gäller för ett naturligt tal $k \geq 1$ ("påståendet P_k") dvs

$$1 + 3 + \cdots + (2k-1) = k^2.$$

Vi vill visa att likheten då måste gälla för nästa tal $k+1$ ("påståendet P_{k+1}") dvs

$$1 + 3 + \cdots + (2k-1) + (2k+1) = (k+1)^2.$$

(Vi vill visa att påståendet P_k medför påståendet P_{k+1}).

Vi startar med vänsterledet i sista likheten och utnyttjar förutsättningen att näst sista likhet gäller:

$$[1 + 3 + \cdots + (2k-1)] + (2k+1) = k^2 + (2k+1) = (k+1)^2.$$

Vi har bevisat påståendet för $k+1$ under förutsättningen att påståendet gäller för k. Därmed kan vi konstatera att likheten enligt induktionsprincipen gäller för varje naturligt tal $n \geq 1$.

Övning F:

Svar: $a_n = \frac{n(n+1)}{2}$.

Övning H 3:

Svar: $S_3(n) = \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2 = \left(\frac{n(n+1)}{2}\right)^2$

Övning G 1:

Vi har $T_1 = 6^1 - 1 = 5$, vilket är ett tal delbart med 5. Nu resonerar vi på följande sätt. Låt oss anta att vi redan vet att talet T_k är delbart med 5 dvs $T_k = 5q_k$, där q_k är ett heltal. Vad kan man säga om nästa tal T_{k+1}? Vi har

$$T_{k+1} - T_k = (6^{k+1} + 1) - (6^k + 1) = 6^{k+1} - 6^k = 6^k(6 - 1) = 5 \cdot 6^k.$$

Därför

$$T_{k+1} = T_k + 5 \cdot 6^k = 5q_k + 5 \cdot 6^k = 5(q_k + 6^k).$$

Den sista likheten visar att även T_{k+1} är en multipel av 5: $T_{k+1} = 5q_{k+1}$ med $q_{k+1} = q_k + 6^k$. Alltså har vi visat implikationen:

För varje k gäller att 5 delar T_k implicerar att 5 delar T_{k+1}.

Enligt induktionsprincipen är alla tal $T_n = 6^n - 1$ delbara med 5.

Kapitel 5

DELBARHET, PRIMTAL, DIVISIONSALGORITMEN

Syftet med detta avsnitt* är att titta närmare på heltalens multiplikativa struktur.

De viktigaste begreppen är

- delbarhet och divisionsalgoritmen
- primtal
- största gemensamma delaren
- minsta gemensamma multipeln
- Euklides algoritm

5.1 Heltal och delbarhet

Detta och nästa avsnitt kan betraktas som en kort inledning till talteorin. Eftersom talteorin ger en möjlighet till flera mycket intressanta problem, som ofta kan formuleras enkelt och elementärt, är antalet övningar ganska stort. Flera av dessa övningar finns som illustration för att visa att talteorin verkligen är en källa till roliga problem och kan med fördel redan mycket tidigt utnyttjas i skolarbete.

Vi återkommer till talteorin senare i avsnittet om "Restaritmetiker" (som ofta kallas för "klockaritmetiker") och senare i utbildningen med kursen "Algebra och Talteori".

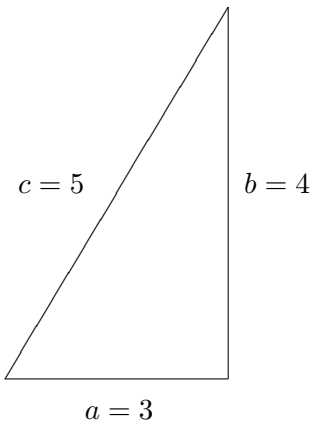
*efter en text av Juliusz Brzezinski

Med de naturliga talen menar man vanligen

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}^{\dagger}.$$

Ordet “naturligt"är helt förklarligt eftersom dessa tal är direkt relaterade till en av de mest naturliga mänskliga aktiviteter – behovet att räkna. De naturliga talen har fascinerat människor i flera tusen år. Ibland har denna fascination en karaktär av magi eller rentav vidskepelse. Man tror på olika mystiska egenskaper hos speciella tal som t ex 7 (“lyckligt"), 13 (“olyckligt"). Pythagoras och hans elever relaterade allt till talen och försökte förklara omvärlden med deras hjälp. Talet 1 var grunden för världen själv – alla andra tal har sitt ursprung i talet 1 ($1 + 1 = 2$, $1 + 1 + 1 = 3$ osv). Det var symbolen för gudarnas fader Zeus (möjligen Zeus själv?). Talet 2 och alla jämna tal symboliserade kvinnlighet, medan talet 3 och alla udda tal större än 3 var symbolen för manlighet. Dessa “egenskaper"har naturligtvis ingenting med matematik att göra. Det fanns dock alltid ett rent matematiskt intresse för de naturliga talen – under flera tusen år har man observerat och studerat olika samband mellan dessa tal. Sådana observationer ledde ofta till både matematikens utveckling och till mycket intressanta tillämpningar. Låt oss nämna några exempel:

(5.1) Exempel. (a) Den rätvinkliga triangeln med sidorna 3, 4, 5



har alltid fascinerat människor. Likheten

$$3^2 + 4^2 = 5^2$$

som i detta fall avspeglar den allmänna egenskapen hos rätvinkliga trianglar, som är bäst känd som Pythagoras sats, gav upphov till många matematiska frågor. Finns det andra rätvinkliga trianglar med heltaliga sidor? Finns det rätvinkliga trianglar med heltaliga sidor sådana att

[†]Ibland kallar man inte 0 som ett naturligt tal – det tog flera tusen år innan talet 0 fick sin naturliga plats bland talen. 0 är ett av heltalen.

en katet är 1 större än den andra? (Det finns oändligt många sådana trianglar t ex en triangel med sidorna 20, 21, 29). Det finns faktiskt böcker som beskriver olika typer av Pythagoreiska trianglar (dvs rätvinkliga trianglar med heltaliga sidor). Triangeln med sidorna 3,4,5 användes av antika geodeter för att mäta rätta vinklar – man använde en lina med 12 knuttar som spändes så att man fick triangel med sidorna 3, 4 och 5. Då fick man rät vinkel mellan sidorna av längderna 3 och 4.

(b) Som ett annat exempel låt oss nämna magiska kvadrater. En av de mest berömda finns på Albrecht Dürers kopparstick "Melankolien 1":

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Summan av alla tal i denna kvadrat längs varje rad, varje kolonn och varje diagonal är 34. Det finns många andra intressanta samband mellan talen i de mindre kvadraterna (begrunda själv!). Magiska kvadrater har intresserat människor för deras egen skull, men de har också mycket intressanta tillämpningar i samband med experimentplaneringen t ex när man vill testa hur olika sorters växter odlas under varierande förhållanden (t ex konstgödsel, temperatur, fuktighet osv). Försök konstruera en magisk kvadrat med 3 rader och 3 kolonner uppbyggd av talen 1,2,...,9!

(c) Det finns många märkliga samband mellan de naturliga talen. Titta t ex på följande likheter:

$$\begin{aligned} 10^2 + 11^2 + 12^2 &= 13^2 + 14^2 \\ 59^4 + 158^4 &= 133^4 + 134^4 \\ 3^3 + 4^3 + 5^3 &= 6^3 \end{aligned}$$

Den sista likheten säger att summan av tre kuber till höger är en kub. Pierre de Fermat påstod i mitten av 1600-talet att summa av två kuber av naturliga tal (större än 0) aldrig är en kub. Detta visades av Leonard Euler 100 år senare (se vidare i avnittet om Diofantiska ekvationer). Inte heller summa av två fjärde potenser av naturliga tal (större än 0) kan vara en fjärde potens, vilket visades av Fermat. Den näst sista likheten hittades av Euler. Han var intresserad av möjligheten att summan av två kvadrater är lika med summan av två andra kvadrater, eller summan av två kuber är lika med summan av två andra kuber osv. Kan Du

ge ett exempel på en summa av två kvadrater av naturliga tal som är lika med summan av två andra kvadrater? □

De negativa talen $-1, -2, -3, \ldots$ trädde in i matematiken relativt sent – i praktiken under 1400-talet då den italienske munken och matematikern Luca Pacioli publicerade år 1494 sin bok "Summa de Arithmetica". I denna bok sammanfattade Pacioli dåtidens vetande om aritmetik och ekvationslösning. Egentligen kan vissa idéer om negativa heltal spåras till Indien, men enligt flera historiker var dessa kunskaper ytliga och hade inte någon inverkan på senare utveckling av talbegreppet. Det är mycket troligt att både den kinesiska och arabiska vetenskapen kom fram till de negativa talen helt oberoende av den europeiska. Talet 0 introducerades i Indien för circa 1500 år sedan.

Med heltalen menas talen $0, \pm 1, \pm 2, \pm 3, \ldots$ dvs alla naturliga tal och deras motsatta tal. Sålunda är heltalen en utvidgning av de naturliga talen. Heltalsmängden betecknas oftast med $\mathbb{Z}$ dvs

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

I en senare del av kursen kommer vi att bekanta oss närmare med heltalens historia, deras ursprung och definition. I detta avsnitt sysslar vi med ett av de viktigaste begreppen som gäller heltalen – delbarhet. T ex delar 5 talet 15 och kvoten är 3. Man säger att 5 är en delare till 15. Rent allmänt har vi följande definition:

(5.2) Definition. Man säger att ett heltal d **delar** ett heltal a om det finns ett heltal q sådant att $a = dq$. Man skriver då $d|a$, vilket utläses "d delar (eller dividerar) a"(man säger också "a är **delbart** med d"eller "a är en **multipel** av d"). Om d inte delar a så skriver man $d \nmid a$. Om d delar a så säger man att d är en **delare** till a. En delare d till a kallas **äkta** (eller **icke–trivial**) om $1 < |d| < |a|$. □

T ex har man $5|15$ eller $4|36$, men $5 \nmid 13$. Talet 12 har följande delare: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. Talen ± 1 och ± 12 är inte äkta delare till 12, medan alla övriga är äkta.

Exempel. Man kontrollerar mycket lätt med hjälp av en miniräknare med minst 10 siffror att $641|2^{32} + 1$ (senare visar vi påståendet i ett avsnitt om restaritmetiker). P. Fermat trodde på 1600-talet att talet $2^{32} + 1$ saknar äkta delare. Det var först L. Euler som 100 år efter Fermat hittade den äkta delaren 641. □

Med all säkerhet känner Du till den mycket vanliga metoden (algoritmen) som man använder för att dela ett heltal med ett heltal skilt från 0. Man får då **kvoten** och **resten**. T ex ger den vanliga divisionsalgoritmen att 134 delat med 26 ger kvoten 5 och resten 4. Man antecknar detta samband så att $134 = 26 \cdot 5 + 4$. Rent allmänt formuleras denna egenskap på följande sätt:

(5.3) Divisionsalgoritmen. *Om a och b är heltal och $b \neq 0$ så är*

$$a = bq + r, \quad \text{där} \;\; 0 \leq r < |b|.$$

Både q (kallad **kvoten***) och r (kallad* **resten***) är entydigt definierade av a och b.*

För bevis av Divisionsalgoritmen se Appendix på slutet av detta avsnitt.

Övning A

1. Bestäm alla delare till talet 24.
2. Motivera att varje heltal n kan skrivas antingen på formen $n = 2k$ om det är jämnt eller på formen $n = 2k + 1$ om det är udda, där k är ett heltal;
3. Motivera att varje heltal n kan skrivas på exakt en av formerna $n = 3k$ eller $n = 3k + 1$ eller $n = 3k + 2$, där k är ett heltal.
4. Hur lyder en liknande egenskap hos heltalen då man ersätter 2 eller 3 ovan med t ex 5?
5. Man vet att ett naturligt tal d delar ett naturligt tal a. Hur skall Du uttrycka det med symboler? Om du skulle välja mellan $d|a$ och $\frac{a}{d}$, vilket är den rätta? Bägge?

Delbarhetsrelationen har flera viktiga egenskaper som man ofta utnyttjar i olika sammanhang. Vi börjar med en övning som leder oss till dessa egenskaper.

Övning B

Låt a, b, c, d beteckna heltal.

1. Vad betyder det att d är en delare till a? Tänk på svaret och jämför med definitionen ovan.
2. Visa att om 5 delar a och b så delar 5 både $a + b$ och $a - b$. Formulera denna egenskap för en godtycklig delare d till a och b i stället för 5. Bevisa Ditt påstående!
3. Visa att delbarhetsrelationen är transitiv dvs om $a|b$ och $b|c$ så $a|c$.
4. Visa att om två av talen a, b, c i likheten $a + b = c$ är delbara med d så är också det tredje talet delbart med d.
5. Visa att om $a|b$ och $b|a$ så är $b = \pm a$.

Nu sammanfattar vi slutsatserna från övningen:

(5.4) Proposition. *Låt a, b, c, d beteckna heltal. Då gäller:*

(a) *om $d|a$ och $d|b$ så $d|a \pm b$,*

(b) *om $a|b$ och $b|c$ så $a|c$,*

(c) *om två av talen a, b, c i likheten $a + b = c$ är delbara med d så är också det tredje talet delbart med d,*

(d) *om $a|b$ och $b|a$ så är $b = \pm a$.*

• **Se även Vretblad-Ekstig, avsnitt 2.1 och tillhörande övningar.**

5.2 Primtal

Bland de naturliga talen har **primtalen** en särställning. De första 20 primtalen är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.$$

Primtalen definieras som de naturliga tal som endast har två olika naturliga delare: 1 och sig självt. Talet 1 är inte ett primtal eftersom det har bara en naturlig delare[‡]. Ett tal större än 1 som inte är ett primtal kallas **sammansatt**.

Primtalen har en mycket viktig egenskap som byggstenar för alla naturliga tal. Vi kommer nämligen bevisa att *varje naturligt tal större än* 1 *kan skrivas som produkt av primtal och dessutom på exakt ett sätt om man bara bortser från primtalens ordningsföljd.* T ex har vi

$$30 = 2 \cdot 3 \cdot 5$$

och även $30 = 3 \cdot 5 \cdot 2 = 2 \cdot 5 \cdot 3$, men det är bara ordningsföljden som kan ändras. Människors intresse för primtalen är flera tusen år gammalt och redan för drygt 2000 år sedan visade den grekiske matematikern Euklides att **det finns oändligt många primtal** (se ett bevis nedan). Först noterar vi den formella definitionen:

(5.5) Definition. Man säger att ett positivt heltal p är ett **primtal** om $p > 1$ och p saknar äkta delare (dvs p har exakt två olika positiva delare: 1 och sig självt). Ett positivt heltal större än 1 som inte är ett primtal kallas **sammansatt**. □

Observera att om ett naturligt tal n är sammansatt så kan man dela n i faktorer: $n = n_1 n_2$ så att n_1 och n_2 är naturliga tal som är äkta delare till n dvs $1 < n_1 < n$ och $1 < n_2 < n$.

Euklides[§] visade sin sats om att att det finns oändligt många primtal i nionde boken av sitt stora verk "Elementa" genom att använda följande sats från sjunde boken:

(5.6) Sats. *Om n är ett heltal större än* 1 *så är n delbart med ett primtal.*

[‡]Det finns en mycket viktig förklaring varför 1 inte accepteras som primtal – se vidare Aritmetikens fundamentalsats.

[§]Euklides levde i Grekland c:a 300 f.Kr.. Hans mest berömda verk är "Elementa" – en bokserie bestående av 13 delar som handlar om dåtidens matematik. "Elementa" känns bäst för ett försök att presentera det som idag kallas för Euklidisk geometri. Denna teori är modellen av geometriska relationer i våra närmaste omgivningar. Men tre volymer av Euklides verk handlar om talteorin – huvudsakligen om delbarhet och primtal. Delar av Euklides "Elementa" hade använts i skolan under 2000 år fram till början av 1900–talet.

Bevis. Låt p beteckna den minsta av alla delare till n som är större än 1. Då saknar p äkta delare eftersom en äkta delare till p skulle vara en delare till n, vilket är omöjligt eftersom p var den minsta delaren till n som är större än 1. Detta innebär att p är ett primtal eftersom $p > 1$ och p saknar äkta delare. □

Nu kan vi bevisa att det finns oändligt många primtal.

(5.7) Euklides sats. *Det finns oändligt många primtal.*

Bevis. Antag att $2, 3, 5, \ldots, p$ betecknar alla primtal (så att p betecknar det sista). Vi bildar ett nytt tal som vi betecknar med N:

$$N = 2 \cdot 3 \cdot 5 \cdots p + 1,$$

dvs talet N är produkten av alla primtal plus 1. Talet N är större än 1 och har en primtalsdelare, säg, q enligt vår förra sats. Detta primtal q kan inte vara lika med något av talen $2, 3, 5, \ldots, p$ eftersom dessa tal inte är delare till N (N delat med något av dessa tal lämnar resten 1). Alltså har vi visat att det måste finnas ytterligare ett primtal q som inte fanns bland $2, 3, 5, \ldots, p$ trots att vi tog alla. Detta innebär att det inte går att skriva en ändlig lista som omfattar alla primtal dvs det måste finnas oändligt många primtal. □

Övning A

1. Utnyttja rutat papper för att rita alla möjliga rektanglar med 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ..., 24 hela rutor. Kan Du dra några slutsatser om skillnader mellan olika tal? Beter sig primtalen på ett speciellt sätt?

2. Vilka av följande tal är primtal (stryk under primtalen): 1,2,3,4,5, 101, 103, 105, 1001, 10101?

3. Du vill göra en lista över alla primtal upp till 120. Använd följande metod som heter *Eratosthenes såll*: Skriv alla tal upp till 120 (gärna i en tabell med 6 eller 10 spalter). Ringa in talet 2 med en färg och stryk bort vartannat tal därefter (med samma färg). Ringa in 3:an i en ny färg och stryk bort vart tredje tal därefter i den färgen. Ringa in 5:an i en tredje färg och stryk bort vart femte tal därefter. Sedan gör du likande med 7:an och var 7:e tal, med 11 och vart 11:e tal, med 13, osv. (dvs. ringa in det första tal som inte är stryket, och dess multipler, till dess att du inte hittar nå gra nya tal att stryka). Skriv ner alla tal som är inrigade eller inte markerade alls. Dessa är alla primtal upp till 120 (du kan förstås ta en större tabell och utnyttja samma system för att utvidga listan). Observera att de tal som är strukna i vissa färger följer enkla visuella mönster. Kan du förklara dessa?

4. Föreslå en beräkningsprocedur (en algoritm) som kan avgöra om ett givet heltal är primt. Avgör om talet 143 är primt. (Läs gärna mer om primtal och "Eratosthenes såll" i boken "Matte med mening" av Kristin Dahl).

5. Låt $N = ab$ vara ett naturligt tal uppdelat i produkt av två heltaliga faktorer. Visa att minst en av dessa faktorer är $\leq \sqrt{N}$. Hur kan man använda denna egenskap för att skriva 143 som produkt av primtal?

6. Skriv följande tal som produkt av primtal:

   (a) 2704, (b) 392688, (c) 749088,

   (talen har "snälla" primfaktorer!).

   Anmärkning. Det är inte så enkelt att avgöra om ett givet naturligt tal är ett primtal. Det finns speciella algoritmer och datorprogram som delvis löser detta problem. De bästa algoritmerna bygger på mycket avancerade delar av algebraisk talteori. De utnyttjas i olika säkerhetssystem t ex i samband med olika banktjänster. Det tar några sekunder att testa om ett tal med, säg, 100 siffror är ett primtal. Men det tar en mycket lång tid att faktoruppdela ett sådant tal i produkt av primtal om talet är sammansatt.

• **Se även Vretblad-Ekstig, avsnitt 2.2 och 2.5 med tillhörande övningar.**

5.3 Största Gemensamma Delaren och Minsta Gemensamma Multipeln

Det är ofta mycket viktigt att kunna beräkna det största heltal som dividerar två givna heltal a och b, och det minsta heltal som två givna heltal a och b delar samtidigt. De kallas största gemensamma delaren (betecknas $\mathrm{SGD}(a,b)$) och den minsta gemensamma multipeln (betecknas $\mathrm{MGM}(a,b)$). T ex är man intresserad av $\mathrm{SGD}(a,b)$ då man vill förkorta bråket $\frac{a}{b}$ (t ex $\frac{24}{40}=\frac{3}{5}$, ty $\mathrm{SGD}(24,40)=8$). Minsta gemensamma multipeln är intressant då man adderar bråk (t ex $\frac{1}{12}+\frac{1}{30}=\frac{7}{60}$, ty $\mathrm{MGM}(12,30)=60$). Formella definitioner av dessa begrepp som är mest vanliga i matematiska sammanhang är följande:

(5.8) Definition. Med **största gemensamma delaren** till a och b menar man ett positivt heltal d som delar a och b och är delbart med varje gemensam delare till a och b dvs

(a) $d|a$ och $d|b$,

(b) om $d'|a$ och $d'|b$, så $d'|d$.

Största gemensamma delaren till a och b betecknas med $\mathrm{SGD}(a,b)$. Man brukar definiera $\mathrm{SGD}(0,0)=0$. Man säger att a och b är **relativt prima** om $\mathrm{SGD}(a,b)=1$. I detta fall säger man ofta att a och b saknar gemensamma delare (även om ±1 delar dessa tal). □

Den största gemensamma delaren till a och b är definierad entydigt därför att om både d och d' är sådana delare så gäller $d|d'$ och $d'|d$, vilket innebär att $d'=\pm d$. Men både d och d' är positiva så att $d'=d$.

(5.9) Definition. Med **minsta gemensamma multipeln** till a och b menar man ett positivt heltal m som är delbart med a och b och som delar varje gemensam multipel av a och b dvs

(a) $a|m$ och $b|m$,

(b) om $a|m'$ och $b|m'$, så $m|m'$.

Minsta gemensamma multipeln av a och b betecknas med $\mathrm{MGM}(a,b)$. Som för SGD definierar man $\mathrm{MGM}(0,0)=0$. □

Även minsta gemensamma multipeln av a och b definieras entydigt av dessa tal (motivera detta påstående med liknande argument som för $\mathrm{SGD}(a,b)$ ovan!).

Exempel. $\mathrm{SGD}(24,40)=8$, $\mathrm{MGM}(12,30)=60$. □

(5.10) Anmärkning. Det är klart att SGD(a, b) är störst bland alla delare till a och b, medan MGM(a, b) är minst bland alla gemensamma multipler av dessa tal. T ex kunde vi i definitionen av $d = \text{SGD}(a, b)$ kräva att d delar både a och b samt att d är det största heltalet med den egenskapen. Det är dock mycket bättre att i stället fokusera på en annan egenskap: varje delare till a och b måste dela d (som är därmed den största delaren). Denna egenskap är mycket användbar i olika bevis. Dessutom möter vi senare precis samma definition då vi sysslar med delbarheten av polynom. Vi kommemterar också denna definition nedan i samband med metodiska synpunkter. □

Hur kan man beräkna SGD och MGM i praktiken? En mycket viktig metod är **Euklides algoritm**. Euklides algoritm säger hur man kan beräkna SGD(a, b). Låt $a = 444$ och $b = 210$. Man bildar en divisionskedja:

$$\begin{aligned} 444 &= 210 \cdot 2 + 24 \\ 210 &= 24 \cdot 8 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 \end{aligned}$$

dvs man dividerar $a = 444$ med $b = 210$ och man får den första kvoten (här 2) och den första resten (här 24). Därefter dividerar man talet $b = 210$ med den första resten (här 24) och man får den andra kvoten (här 8) och den andra resten (här 18). Man fortsätter tills man får resten noll. Eftersom resterna är mindre och mindre så måste man avsluta processen med resten 0 (varför?). Den sista nollskilda resten (här 6) är just största gemensamma delaren till a och b dvs SGD$(444, 210) = 6$.

Vi skall både anteckna Euklides algoritm och motivera att den verkligen ger största gemensamma delaren för helt godtyckliga heltal a och $b \neq 0$. Vi har följande divisionskedja:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < |b|, \\ b &= r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 \leq r_3 < r_2, \\ &\vdots & \vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2}, \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Varje kedja av den här typen måste vara ändlig därför att en avtagande kedja av resterna $r_1 > r_2 > r_3 > \ldots \geq 0$ måste vara ändlig. Vi påstår att den sista icke-försvinnande resten i denna kedja, som här betecknas med r_n, är den största gemensamma delaren till a och b. Att det verkligen är sant kontrollerar man mycket enkelt med hjälp av definitionen av SGD(a, b). Den sista likheten i kedjan säger att r_n är delaren till r_{n-1}. Alltså visar den näst sista likheten

att r_n är delaren till r_{n-2}. Nu vet vi att r_n delar r_{n-1} och r_{n-2}. Alltså visar likheten för r_{n-3} att även denna rest är delbar med r_n. Vi fortsätter vår vandring uppåt och steg för steg visar vi att alla tal r_{n-1}, r_{n-2}, r_{n-3}, ..., r_1, b, a är delbara med r_n. Alltså är r_n en gemensam delare till a och b.

Om nu d är en godtycklig gemensam delare till a och b så visar den första likheten att d delar r_1. Alltså ger den andra likheten att d delar r_2. Då vi vet att d delar r_1 och r_2 så får vi ur den tredje likheten att d också delar r_3. På det sättet får vi att d är en delare till alla tal i sekvensen $a, b, r_1, r_2, r_3, \ldots, r_{n-2}, r_{n-1}, r_n$. Detta visar att r_n är den största gemensamma delaren till a och b. Det är klart att man kan formalisera vårt resonemang genom att använda matematiskt induktion.

Med hjälp av Euklides algoritm kan man inte bara beräkna $\mathrm{SGD}(a, b)$ utan också två heltal x, y sådana att $\mathrm{SGD}(a, b) = ax + by$. Vi illustrerar detta med samma exempel:

(5.11) Exempel. Låt $a = 444$ och $b = 210$. Euklides algoritm ger

$$\begin{aligned} 444 &= 210 \cdot 2 + 24 \\ 210 &= 24 \cdot 8 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 \end{aligned}$$

Nu har vi

$$\begin{aligned} 6 &= \underline{24} - \underline{18} \cdot 1 = \underline{24} - (\underline{210} - \underline{24} \cdot 8) \cdot 1 = \\ &= \underline{24} \cdot 9 - \underline{210} = (\underline{444} - \underline{210} \cdot 2) \cdot 9 - \underline{210} = \\ &= \underline{444} \cdot 9 - \underline{210} \cdot 19 = \underline{444} \cdot 9 + \underline{210} \cdot (-19). \end{aligned}$$

□

Möjligheten att lösa ekvationen $\mathrm{SGD}(a, b) = ax + by$ i heltal x och y kommer att spela en mycket viktig roll och kommer att användas flera gånger under kursens gång. Därför noterar vi den egenskapen som en sats och ger ett bevis i Appendix på slutet av denna stencil. Beviset ger inte någon möjlighet att hitta x och y (ofta vill man veta att x och y finns utan att behöva räkna ut dessa tal). Om man vill beräkna x och y så kan man använda Euklides algoritm som i exemplet ovan. Vi noterar satsen redan nu:

(5.12) Sats. *Om a och b är heltal och $d = SGD(a, b)$ så existerar två heltal x_0 och y_0 sådana att*

$$d = ax_0 + by_0.$$

Vi visar ett exempel på en tillämpning av den sista satsen. Om 2 och 3 är delare till ett heltal N så är också $2 \cdot 3 = 6$ en delare till N. Detta följer från följande påstående:

(5.13) Proposition. *Om a och b är två relativt prima delare till ett heltal N så är också ab en delare till N.*

Bevis. Låt $N = aq_1$ och $N = bq_2$ med hela q_1 och q_2. Eftersom a och b är relativt prima dvs $\mathrm{SGD}(a, b) = 1$ så är $ax + by = 1$ för lämpliga heltal x och y (enligt den sista satsen). Alltså är

$$N = N(ax + by) = Nax + Nby = bq_2ax + aq_2by = ab(q_2x + q_1y),$$

vilket visar att N är delbart med ab. □

Övning A

1. Vad menas med största gemensamma delaren (SGD) till två heltal a och b? Jämför Dina funderingar med definitionen.
2. Beräkna $\mathrm{SGD}(a, b)$ samt två heltal x_0 och y_0 sådana att $\mathrm{SGD}(a, b) = ax_0 + by_0$ då
   (a) $a = 165, b = 102$,
   (b) $a = 624, b = 570$.

Övning B

1. Är det sant eller falskt:
   (a) Om ett heltal N är delbart med 2 och 3, så är det delbart med $2 \cdot 3 = 6$?
   (b) Om ett heltal N är delbart med 4 och 6, så är det delbart med $4 \cdot 6 = 24$?
2. Varför gäller enbart ett av dessa påståenden?

Övning C

1. Är det sant eller falskt:
   (a) om 6 delar ab och 6 inte delar a så måste 6 dela b;
   (b) om 6 delar ab och 6 saknar gemensamma delare med a så måste 6 dela b;
   (c) om 5 delar ab och 5 inte delar a så måste 5 dela b.

2. Varför gäller inte alla påståenden ovan?

3. Visa att om d är en delare till produkten ab och d saknar gemensamma delare med a, dvs $\mathrm{SGD}(d, a) = 1$, så är d en delare till b.

   Ledning. Det finns heltal x och y sådana att $ax + dy = 1$ – utnyttja denna likhet. Du kan också läsa beviset av Bezouts sats i stencilen om primtalen, multiplikation och diofantiska ekvationer.

• **Se även Vretblad-Ekstig, avsnitt 2.3 och tillhörande övningar.**

Kapitel 6

ARITMETIKENS FUNDAMENTALSATS OCH DIOFANTISKA EKVATIONER

Syftet med detta avsnitt är att bekanta sig med delbarhetsegenskaper hos heltalen.

De viktigaste begreppen är

- Aritmetikens fundamentalsats
- Diofantiska ekvationer

Detta avsnitt kan betraktas som en kort inledning till talteorin. Eftersom talteorin ger en möjlighet till flera mycket intressanta problem, som ofta kan formuleras enkelt och elementärt, är antalet övningar ganska stort. Flera av dessa övningar finns som illustration för att visa att talteorin verkligen är en källa till roliga problem och kan med fördel redan mycket tidigt utnyttjas i skolarbete.

Vi återkommer till talteorin senare i avsnittet om "Restaritmetiker" (som ofta kallas för "klockaritmetiker").

ARITMETIKENS FUNDAMENTALSATS

Nu kan vi förklara primtalens viktiga roll som byggstenar för alla heltal – varje heltal större än 1 är en entydig produkt av primtal. T ex

$$100 \quad = \quad 2^2 \cdot 5^2,$$

$$\begin{aligned} 108 &= 2^2 \cdot 3^3, \\ 2002 &= 2 \cdot 7 \cdot 11 \cdot 13. \end{aligned}$$

Ett primtal t ex 5 betraktas också som produkt av primtal – produkt med endast en faktor 5 (dvs $5 = 5$). En sådan överenskommelse har stora fördelar – den förenklar många formuleringar (t ex kan vi säga att varje naturligt tal större än 1 är en produkt av primtal).

Först visar vi en mycket viktig egenskap hos primtalen som egentligen är nyckeln till aritmetikens fundamentalsats:

(6.1) Sats. *En primdelare till en produkt av två heltal är en delare till (minst) en av faktorerna dvs om $p|ab$ så $p|a$ eller $p|b$, då p är ett primtal och a, b är heltal.*

Bevis. Antag att $p \nmid a$. Då är $\mathrm{SGD}(p, a) = 1$ därför att p är ett primtal. Enligt (6.7) existerar två heltal x, y sådana att $px + ay = 1$. Om man multiplicerar den likheten med b får man $b = pbx + aby$. Men enligt förutsättningen är $ab = pq$ för ett heltal q. Alltså är $b = p(bx + qy)$ dvs $p|b$. □

Observera att det inte har någon betydelse att den sista satsen handlar av ett primtal som delar en produkt av två faktorer – ett primtal som delar en produkt av ett godtyckligt antal faktorer måste dela någon av dessa. Vi utnyttjar denna egenskap av primtal i beviset av aritmetikens fundamentalsats:

(6.2) Aritmetikens fundamentalsats. *Varje heltal större än 1 är en entydig produkt av primtal dvs om*

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

där p_i och q_j är primtal så är $r = s$ och vid en lämplig numrering av faktorerna är $p_i = q_i$.

Bevis. Först visar vi att varje naturligt tal $n > 1$ är en produkt av primtal. Låt oss anta att det finns naturliga tal som inte kan skrivas som en sådan produkt. Låt oss välja bland dessa naturliga tal det minsta. Vi betecknar detta tal med n. Detta innebär att $n > 1$ är det minsta naturliga tal som inte är en produkt av primtal. Talet n är inte ett primtal (ett primtal är en produkt av primtal med bara en faktor). Alltså är n ett sammansatt tal dvs $n = n_1 n_2$, där både n_1 och n_2 är äkta delare till n dvs $1 < n_1 < n$ och $1 < n_2 < n$. Eftersom både $n_1 > 1$ och $n_2 > 1$ är mindre än n så måste dessa tal kunna skrivas som produkt av primtal (ty n är det minsta som inte kan skrivas). Men detta betyder att också n kan skrivas som produkt av primtal. På det sättet får vi att det inte finns något naturligt tal som inte kan skrivas som produkt av primtal.

Nu visar vi att varje naturligt tal $n > 1$ kan skrivas som produkt av primtal bara på ett sätt om man bortser från faktorernas ordningsföljd. På samma sätt som tidigare låt oss anta att det finns ett naturligt tal större än 1 som kan skrivas på olika sätt som en sådan produkt och låt $n > 1$ beteckna det minsta av alla naturliga tal som har olika framställningar:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

där $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ är primtal. Observera att n inte är ett primtal (ett primtal har endast en framställning). Eftersom p_1 är ett primtal och p_1 delar produkten $q_1 q_2 \cdots q_s$ så måste p_1 dela en av dess faktorer t ex p_1 delar q_1. Men q_1 är också ett primtal så att $p_1 = q_1$ (om ett primtal delar ett primtal så måste det vara samma primtal). Nu får vi:

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$$

så att talet $1 < \frac{n}{p_1} < n$ har två olika framställningar som produkt av olika primtal. Detta är dock omöjligt eftersom n var det minsta naturliga talet med olika framställningar. Slutsatsen är att det inte finns något minsta naturliga tal $n > 1$ med två olika framställningar som produkt av primtal. □

(6.3) Anmärkning. Ofta kallar man sats (6.1) för aritmetikens fundamentalsats. Även om formuleringen ovan handlar om positiva heltal så kan vi säga rent allmänt att varje heltal $N \neq 0, \pm 1$ är en produkt

$$N = \varepsilon p_1 p_2 \cdots p_n,$$

där p_i är primtal och $\varepsilon = \pm 1$. Enligt aritmetikens fundamentalsats är en sådan framställning entydig så när som på faktorernas ordningsföljd. Faktoruppdelningar av liknande typ är kända t ex för polynom. Vi diskuterar både faktoruppdelningar för heltalen och för polynom i ett senare avsnitt. □

Primfaktoruppdelningar av heltal ger en möjlighet att beräkna $\mathrm{SGD}(a, b)$ och $\mathrm{MGM}(a, b)$ utan Euklides algoritm. Även om denna möjlighet inte är särskilt praktisk används den flitigt i skolan.

(6.4) Exempel. Vi vill bestämma $\mathrm{SGD}(a, b)$ och $\mathrm{MGM}(a, b)$ då $a = 90$ och $b = 150$. Eftersom $a = 90 = 2 \cdot 3 \cdot 3 \cdot 5$ och $b = 2 \cdot 3 \cdot 5 \cdot 5$, så är $\mathrm{SGD}(90, 150) = 2 \cdot 3 \cdot 5 = 30$. samt $\mathrm{MGM}(90, 150) = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 450$. En primfaktor p ingår i $\mathrm{SGD}(a, b)$ om den ingår i både a och b. Dess exponent är minimum av exponenterna i a och b. En primfaktor p ingår i $\mathrm{MGM}(a, b)$ om den ingår i minst ett av talen a eller b. Dess exponent är maximum av exponenterna i a och b. □

(6.5) Anmärkning. Vi avslutar detta avsnitt med några kommentarer om primfaktoruppdelningar av heltal. Det är inte lätt att faktoruppdela ett helt godtyckligt heltal N i primfaktorer. Om N är ett relativt litet så kan man testa små primtal och kontrollera om de dividerar N. T ex om $N = 420$ så dividerar man först med 2, därefter med 2 igen, med 3, 5 och 7. Man brukar ibland skriva resultaten på följande sätt

420	2
210	2
105	3
35	5
7	7
1	

dvs $420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7$.

Den metoden förutsätter att vi känner till en lista över de små primtalen. Det är också viktigt att relativt snabbt kunna bedömma om talet är delbart med t ex 2, 3, 5, 7 osv. Sådana "delbarhetskriterier" diskuterar vi i ett senare avsnitt om restaritmetiker. Tyvärr fungerar sådana metoder endast då talen är små. För faktoruppdelningar av stora heltal krävs mycket avancerade metoder. De bästa kända algoritmerna för primtalsfaktorisering kräver c:a $N^{1/5}$ räkneoperationer för att hitta en primfaktor till N (om N är sammansatt och "slumpmässigt"valt). Om en räkneoperation tar $1\mu s$ och talet har 200 siffror, så krävs det $10^{40}\mu s \approx 3 \cdot 10^{26}$ år för att genomföra beräkningarna för N (10^6 datorer var och en kapabel att utföra en operation på $1\mu s$ skulle behöva $3 \cdot 10^{20}$ år för att klara dessa beräkningar!). Dessa omständigheter gör att tal $N = pq$, där p och q är stora primtal (med, säg, 100 siffror) används för säkerhetskryptering av känsliga uppgifter som t ex bankkoder. Vi diskuterar ett sådant system i samband med ett senare avsnitt om restaritmetiker. □

Övning A MGM och SGD

1. Låt $a = 45$ och $b = 50$. Bestäm minsta gemensamma multipeln till dessa tal.

2. Låt a och b vara två heltal. Försök beskriva en procedur som ger MGM(a, b).

3. Visa att SGD(a, b) MGM$(a, b) = ab$ och förklara hur denna formel kan användas till beräkningar av MGM(a, b). Använd formeln i den första uppgiften ovan.

   Ledning. Låt $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ och $b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ vara faktoruppdelningar av a och b i produkt av olika primtal $p_1, p_2, \ldots, p_r$ (några av exponenterna $k_1, k_2, \ldots, k_r$ och $l_1, l_2, \ldots, l_r$ kan vara lika med 0). Med vilken exponent ingår t ex p_1 i SGD(a, b), MGM(a, b) och ab? Jämför exponenterna för p_1 i SGD(a, b) MGM(a, b) och i ab.

• **Se även Vretblad-Ekstig, avsnitt 2.4 och tillhörande övningar.**

Övning B Diofantos

Diofantiska* ekvationer. Termen "Diofantisk ekvation" gäller ekvationer vars heltaliga eller rationella lösningar man vill bestämma. T ex att bestämma alla heltaliga lösningar (x, y, z) till ekvationen

$$x^2 + y^2 = z^2$$

eller alla heltalspar (x, y) som löser ekvationen

$$3^x - 2^y = 1.$$

Den första ekvationen ovan kallas Pythagoras ekvation och har oändligt många lösningar (t ex alla $(n^2-1, 2n, n^2+1)$, där n är ett heltal – $n = 2$ ger $(3, 4, 5)$). Den andra ekvationen (ett specialfall av Catalans† ekvation) har en lösning $(2, 3)$. Den mest berömda av alla Diofantiska ekvationer är Fermats ekvation:

$$x^n + y^n = z^n,$$

där $n > 2$. Det tog mer än 350 år att lösa den ekvationen. I september 1994 visade den engelske matematikern Andrew Wiles att ekvationen saknar heltaliga lösningar (x, y, z) med $xyz \neq 0$‡

I talteorin finns många närbesläktade problem som fortfarande väntar på sin lösning. Vi skall i denna övning syssla med mycket enkla Diofantiska ekvationer av typen $ax + by = N$.

1. Bestäm ett heltalspar (x_0, y_0) sådant att $2x + 5y = 1$ (Du kan försöka gissa en lösning!). Bestäm därefter alla heltalspar (x, y) sådana att $2x + 5y = 1$.

   Ledning. Observera att om $2x + 5y = 2x_0 + 5y_0$ så är $2(x - x_0) = 5(y_0 - y)$. Detta ger att $y - y_0 = 2k$ för ett heltal k. Uttryck y med hjälp av y_0 och därefter x med hjälp av x_0.

2. Låt (x_0, y_0) vara en lösning till ekvationen $ax + by = N$, där a och b saknar gemensamma delare (dvs a och b är relativt prima). Bestäm alla lösningar till denna ekvation dvs alla heltalspar (x, y) sådana att $ax + by = N$.

   Ledning. Gör som ovan.

*Diofantos (eller Diophantus) var en grekisk matematiker som levde i Alexandria omkring 250 e.Kr.. Troligen skrev han 13 volymer av ett verk under namnet "Arithmetica". 6 av dessa volymer finns bevarade.

†Catalans ekvation är

$$x^y - z^t = 1$$

med $y, t > 1$. Det är inte känt om denna ekvation har en lösning i naturliga tal skild från $x = 3$, $y = 2$, $z = 2$, $t = 3$.

‡Det finns en mycket intressant bok av Simon Singh "Fermats gåta" som berättar om olika turer kring Fermats problem och dess lösning. Filmen som Simon Singh gjorde för BBC Discovery: Fermat's Enigma finns tillgänglig på http://topdocumentaryfilms.com/fermats-last-theorem/).

Exempel : Linjära Diofantiska ekvationer.

Vi skall bestämma alla heltaliga lösningar (x, y) till ekvationen $12x+28y = 20$. Först dividerar vi alla koefficienter med 4 och får den ekvivalenta ekvationen $3x + 7y = 5$. Nu behöver vi en *partikulär* lösning till denna ekvation. En sådan lösning kan vi rent allmänt beräkna med Euklides algoritm, men vi kan också gissa en lösning utan större problem. Först tar vi ekvationen $3x+7y = 1$ och ser direkt att $x = -2$, $y = 1$ är en lösning. För att få en lösning till vår ekvation måste vi multiplicera denna med 5 dvs $x_0 = -10$, $y_0 = 5$ är en partikulär lösning till ekvationen $3x + 7y = 5$ (kontrollera!). Låt (x, y) beteckna en godtycklig heltalig lösning. Då är $3x + 7y = 3x_0 + 7y_0$. Alltså är $3(x - x_0) = 7(y_0 - y)$. Likheten visar att 3 dividerar högerled och eftersom 3 saknar gemensamma delare med 7 måste $3 \mid y_0 - y$ dvs $y_0 - y = 3k$, där k är ett heltal. Vi får $y = y_0 - 3k$ och insättning ger $3(x - x_0) = 7 \cdot 3k$ dvs $x - x_0 = 7k$. Alltså är $x = x_0 + 7k = -10 + 7k$, $y = y_0 - 3k = 5 - 3k$ med ett godtyckligt heltal k den allmänna lösningen till den givna ekvationen. □

• **Se även Vretblad-Ekstig, avsnitt 2.7 och tillhörande övningar, speciellt 2.88, 2.89, 2.95. och blandade övningar till kap 2 speciellt: 2.105, 2.106, 2.107, 2.112.**

• **Välj ut någon eller några av övningarna nedan att lösa och fundera på! De anknyter till forskningsfrågor i talteori**. För mer om primtal rekommenderas websajten "The Prime Pages" vid primes.utm.edu som innehåller mycket intressant om primtal.

Övning C

Primtalstvillingar. Man säger att två primtal p och q är **tvillingar** om $q - p = 2$.

1. Skriv ut alla primtalstvillingar < 100.

2. 3, 5 och 7 är "primtalstrillingar". Motivera att det inte finns några andra primtal p, q, r sådana att $r - q = q - p = 2$.

   Anmärkning. Primtalstvillingar intresserade människor redan under antiken. De nämns i Euklides böcker. Man vet inte om det finns oändligt många sådana primtalspar, men stora framsteg i denna fråga publicerades år 2013. Sök på "Yiting Zhang bounded gaps between primes" för artiklar om nya rön.

Övning D Dirichlet och primtal

Aritmetiska följder av primtal. Vi repeterar att en aritmetisk följd med differansen d är en följd av talen a, $a + d$, $a + 2d$, ..., $a + nd$, ... (detta betyder att om $a_i = a + id$ och $a_{i+1} = a + (i + 1)d$, så är $a_{i+1} - a_i = d$ dvs differensen av två efterföljande tal i följden är lika med d). T ex är 11, 17, 23 en aritmetisk följd med differansen 6.

1. Skriv ut alla aritmetiska följder av primtal som är < 50 och som består av minst tre stycken primtal.

2. Försök skriva ut en aritmetisk följd bestående av 4 primtal.

   Anmärkning. Man vet att det finns godtyckligt långa aritmetiska följder av primtal. Men det finns godtyckligt långa avsnitt av de naturliga talen som saknar primtal t ex är $11!+2$, $11!+3, \ldots, 11!+11$ tio efterföljande sammansatta tal (varför?). Vi har $11! = 1 \cdot 2 \cdots 11$ och rent allmänt $n! = 1 \cdot 2 \cdots n$ dvs $n!$ är produkten av alla naturliga tal från 1 till n.

3. Skriv ut en följd av 100 efterföljande sammansatta tal och generalisera Din konstruktion till en följd av n efterföljande sammansatta tal.

   Anmärkning. Dirichlet* visade 1828 att varje aritmetisk följd $a + nd$, där a och d är relativt prima (dvs $\mathrm{SGD}(a,d) = 1$) och $n = 1, 2, 3, \ldots$ innehåller oändligt många primtal. T ex finns det enligt Dirichlets sats oändligt många primtal på formen $1 + 4n$ och oändligt många på formen $3 + 4n$.

Övning E Goldbachs förmodan

Goldbachs† förmodan. År 1742 formulerade Goldbach påståendet att varje jämnt heltal större än 2 är en summa av två primtal. T ex $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$ osv. Ännu har man inte lyckats bevisa detta påstående.

1. Kontrollera Goldbachs förmodan för alla jämna heltal < 50.

2. Visa att Goldbachs förmodan implicerar att varje udda heltal större än 5 är en summa av tre primtal.

   Anmärkning. En rysk matematiker I.M. Vinogradov visade 1937 att varje udda heltal som är större än $3^{3^{15}}$ verkligen är en summa av tre primtal. Vingradovs konstant är så stor (mer än 7 miljoner siffror!) att det inte finns en chans att kontrollera hans sats för heltal mindre än $3^{3^{15}}$ med hjälp av datorer. Nyligen reducerades storleken av den konstanten betydligt, men gränsen är fortfarande utom räckhåll för datorberäkningar. Det finns en Internet–sida där man kan skriva in ett godtyckligt jämnt heltal som därefter testas och presenteras som summa av två primtal – om detta är möjligt (talet kan inte vara för stort).

Övning F Mersenne–primtal

De största kända primtalen hittar man bland så kallade Mersenne–tal $M_n = 2^n - 1$. Marin Mersenne började studera dessa tal år 1644. Talen M_n då $n = 2, 3, 5, 7, 13, 17, 19$ är primtal. T ex är $M_{19} = 2^{19} - 1 = 524287$ ett primtal. Man känner 35 Mersenne–primtal – det sista $2^{1398269} - 1$ upptäcktes i november 1996. Senaste nytt om Mersenne–talen kan fås på Internet (sök "Mersenne Prime").

*Peter Gustav Lejeune Dirichlet (13/2 1805 – 5/5 1859) var en mycket framstående tysk matematiker som bidrog med resultat till flera matematikgrenar.

†Christian Goldbach (18/3 1690 – 20/11 1764) var en tysk matematiker. Läs om Goldbachs förmodan i "Matte med mening" på sid. 36.

1. Visa att talet M_{23} inte är ett primtal – kontrollera att $47|2^{23}-1$.

2. Motivera att Mersenne–talen M_n inte är primtal då n är sammansatt.

   Ledning. Börja med jämna n.

Övning G Fermattal

Formler för primtal. Man har studerat olika "formler" $f(n)$ som för varje n ger ett primtal (och helst alla).

1. L. Euler[‡] fann att $f(n) = n^2+n+41$ ger primtal då $n = 0, 1, 2, \ldots, 40$ (Du kan kontrollera detta fast det är lite jobbigt). Visa att det finns oändligt många n sådana att $f(n)$ är sammansatt.

   Anmärkning. Både C. Goldbach och L. Euler visade att varje polynom $f(n)$ med heltaliga koefficienter ger ett sammansatt tal för något n. Vi visar den satsen som en enkel övning i avsnittet om polynom.

2. Fermat trodde att hans tal $F_n = 2^{2^n}+1$ är primtal för varje $n = 0, 1, 2, 3, \ldots$. Vi vet redan (se stencilen "Induktion och deduktion") att hans förmodan var falsk. Kontrollera med miniräknare att $641|F_5$.

   Anmärkning. Man har studerat andra "formler" för primtal. T ex vet man att det finns ett positivt reellt tal a sådant att heltalsdelen av talet a^{3^n} (dvs det största heltalet mindre än detta tal) är ett primtal för varje n. Men man känner tyvärr inte talet a. Det finns ett polynom i 26 variabler (av grad 25) som alltid ger primtal då variablerna antar icke–negativa heltaliga värden och polynomets värde är större än 0. Man får alla primtal, men de kommer inte i någon naturlig ordning. Man lyckades minska antalet variabler i liknande polynom, men man var tvungen att öka dess grad (se en mycket intressant bok av Paulo Ribenboim, "The Little Book of Big Primes", Springer–Verlag, 1991.

[‡]Leonhard Euler (15/4 1707 – 18/9 1783) var en schweizisk matematiker. Men han var verksam under många år i St Petersburg och Berlin. Eulers sysslade mest med matematik, men han gjorde också viktiga insatser i andra vetenskaper. Han var en av de mest produktiva vetenskapsmänen i historien och skrev hundratals artiklar och böcker. Under de sista åren av sitt liv var han blind, men han publicerade lika mycket som tidigare – han dikterade sina artiklar och böcker som skrevs av en betjänt. Euler hade 13 barn. Läs om Euler i "Matte med mening".

Övning H

Primtal i intressanta former.

1. Man visar att det finns oändligt många primtal p som är summor av två heltaliga kvadrater dvs $p = a^2 + b^2$, för två heltal a och b. Varje primtal p som lämnar resten 1 vid division med 4 kan skrivas på detta sätt (se vidare avsnittet om restaritmetiker). Visa att varje primtal som lämnar resten 3 vid division med 4 inte är en summa av två heltaliga kvadrater.

   Ledning. Både a och b i $p = a^2 + b^2$ måste vara udda.

   Anmärkning. Ganska nyligen visade två matematiker – J. Friedlander (University of Toronto) och H. Iwaniec (Rutgers University) – att det finns oändligt många primtal p som kan skrivas på formen $p = a^2 + b^4$ med heltal a och b. Detta resultat betraktas som en stor matematisk sensation.

2. Försök hitta 5 primtal p som kan skrivas på formen $p = a^2 + b^4$, där a och b är heltal.

3. Det är inte känt om $n^2 + 1$ är ett primtal för oändligt många n (men man tror att det är så). Visa att $n^2 + 1$ är sammansatt för oändligt många n.

   Anmärkning. Det finns många obesvarade frågor av liknande karaktär. Är t ex $n^2 + 2$ ett primtal för oändligt många n? Man vet inte om talet $n! + 1$ är ett primtal för oändligt många n. Vi nämnde Fermat–talen $F_n = 2^{2^n} + 1$ – man vet inte heller om det finns oändligt många primtal bland dessa.

APPENDIX: Två bevis

(6.6) Divisionsalgoritmen. *Om a och b är heltal och $b \neq 0$ så är*

$$a = bq + r, \quad \text{där} \;\; 0 \leq r < |b|.$$

Både q (kallad **kvoten**) *och r (kallad* **resten**) *är entydigt definierade av a och b.*

Bevis. Först noterar vi att det räcker om vi bevisar satsen då $b > 0$ eftersom $b < 0$ innebär att $|b| = -b > 0$. Om satsen gäller då delaren är positiv, så är $a = (-b)q + r$, med $0 \leq r < |b|$. Denna likhet kan skrivas om till $a = b(-q) + r$. Alltså förutsätter vi vidare att $b > 0$.

Låt oss nu välja det största möjliga heltalet k sådant att $q \leq \frac{a}{b}$. Alltså är $q + 1 > \frac{a}{b}$. Dessa olikheter säger att $a - bq \geq 0$ och $a - bq < b$. Om vi betecknar $a - bq$ med r så får vi $a = bq + r$ och $0 \leq r < b$.

Slutligen visar vi att kvoten q och resten r definieras entydigt av a och b. Antag att:

$$a = bq + r = bq' + r,'$$

där $0 \leq r < |b|$ och $0 \leq r' < |b|$ dvs både q och q' är kvoter samt r och r' är rester. Då är $b(q - q') = r' - r$, så att b delar $r' - r$. Men både r och r' är mindre än $|b|$, vilket innebär att deras skillnad är delbar med b endast om de är lika dvs $r = r'$. Alltså är $bq = bq'$, så att $q = q'$ eftersom $b \neq 0$. □

(6.7) Sats. *Om a och b är heltal och $d = SGD(a, b)$ så existerar två heltal x_0 och y_0 sådana att*

$$d = ax_0 + by_0.$$

Bevis. Om $a = b = 0$ så är påståendet klart (som x och y kan man välja helt godtyckliga heltal). Anta att a eller b inte är 0. Det är klart att det finns positiva heltal som kan skrivas på formen $ax + by$ t ex om $a \neq 0$ så är $\pm a = a \cdot (\pm 1) + b \cdot 0$ och antingen a eller $-a$ är ett positivt heltal. Även $b = a \cdot 0 + b \cdot 1$ kan skrivas på formen $ax + by$. Låt d_0 vara det minsta positiva heltal som kan skrivas på den önskade formen dvs

$$(*) \qquad d_0 = ax_0 + by_0.$$

Vi påstår att $d_0 = d$. Först observerar vi att varje heltal $ax + by$ är delbart med d_0. För att bevisa detta delar vi $ax + by$ med d_0. Då är

$$ax + by = qd_0 + r,$$

där resten r är mindre än delaren d_0. Men

$$r = ax + by - qd_0 = ax + by - q(ax_0 + by_0) = a(x - qx_0) + b(y - qy_0)$$

så att r måste vara 0 ty annars får man ett tal som är mindre än d_0 och som kan skrivas på den önskade formen. Alltså dividerar d_0 både a och b ty bägge kan skrivas på formen $ax + by$. Ekvationen $(*)$ visar att om d' är en delare till a och b, så är d' en delare till d_0. Alltså är d_0 den största gemensamma delaren till a och b. □

Kapitel 7

RESTARITMETIKER

Restaritmetiker påminner om heltalsaritmetiken, men i stället för att addera eller multiplicera vanliga heltal adderar man och multiplicerar rester vid division med ett fixt heltal n. Rester adderas och multipliceras så att summan och produkten också är rester. Dessa operationer kallas addition och multiplikation "modulo n". Detta är ett exempel på nya "talsystem" som lyder samma räknelagar som de vanliga heltalen (kommutativa, associativa, distributiva lagen, identitetselement 0 och 1, additiv invers mm) men är ganska annorlunda. Restaritmetiker förekommer mycket ofta i vardagliga situationer även om man inte alltid är medveten om deras närvaro – veckodagar återkommer modulo 7, och tiden räknas ofta modulo 24 (eller 12). Ett grafiskt sätt att representera restaritmetik är som en (analog!) klocka, med n "timmar", numrerade $0, \ldots, n-1$. Restaritmetiker ger en möjlighet att lösa många relativt enkla och intressanta problem som gäller delbarhetsegenskaper hos heltalen.

Läs avsnitt 3.4 i Vretblads bok. Lös i första hand övningar **A, B, C E1, G, H**. Observera att avsnitt 3.3 i boken, där restklasser introduceras, utgår från ekvivalensrelationer. Vi tar inte upp ekvivalensrelationer i denna kurs, så det kan vara mer naturligt att använda den introduktion till restklasser som ges i denna stencil.

Övning A

Denna övning handlar om aritmetiker modulo 7, modulo 12 och modulo 31.

1. Den 1 mars är en fredag. Med ledning av detta, beräkna vilken veckodag den 24 mars är. Förklara hur Du resonerar.
2. Mars har 31 dagar. Beräkna vilken veckodag den 8 april är (den 1 mars är en fredag).
3. Låt oss numrera veckodagarna så att söndag har nummer 0, måndag nummer 1, tisdag nummer 2 osv. Om den 1 i månaden infaller på en måndag så kan man bestämma veckodagen i denna månad genom att dela datumet med 7 – resten säger vilken veckodag

man har (t ex infaller den 24 på en onsdag ty 24 lämnar resten 3 vid division med 7). Föreslå en metod för att bestämma veckodagen i en månad som börjar på en torsdag dvs vad skall man göra med dagens datum för att resten vid division med 7 skall ge veckodagen.

4. Konstruera en "kalender" för hela året genom att för varje månad ange ett tal som skall adderas till dagens datum så att resten av datumet vid division med 7 ger veckodagen.

5. Rita en 12-klocka och en 7-klocka (som en vanlig analog klocka med 7 markeringar bara, numrerade 0, 1, 2, 3, 4, 5, 6). På varje klocka, öva på att addera tal (även över 0-märket). De enda talen du har är talen $0, 1, n-1$ med t.ex $8+6 \equiv 2 \bmod 12$.

6. Skriv en additionstabell för räkning på en 12-klocka (dvs modulo 12) och en additionstabell för räkning på en 7-klocka (dvs modulo 7). Tabellerna är kvadratiska, med n rader och n spalter (n är här 12 eller 7).

7. Öva på att multiplicera (med upprepad addition) på klockorna, och skriv en multiplikationstabell modulo 12 och en multiplikationstabell modulo 7. Ser du några intressanta skillnader mellan dina två multiplikationstabeller? Kan du förklara dem i så fall?

Definition Låt n vara ett heltal större än 1. Då gäller $a \equiv b(\bmod n)$ om $a-b$ är delbart med n.

Vi utläser $a \equiv b(\mathrm{mod}n)$ som "a och b är kongruenta modulo n". Ett annat sätt att uttrycka att $a \equiv b(\mathrm{mod}n)$ är att det finns något heltal s sådant att $a = b + s \cdot n$. Man kan också säga att a och b har samma rest vid division med n. Denna beskrivning gör tydligt att kongruens modulo n är en ekvivalensrelation, dvs. den uppfyller

- Reflexivitet: $a \equiv a(\mathrm{mod}n)$
- Symmetri: Om $a \equiv b(\mathrm{mod}n)$ så $b \equiv a(\mathrm{mod}n)$
- Transitivitet: Om $a \equiv b(\mathrm{mod}n)$ och $b \equiv c(\mathrm{mod}n)$ så $a \equiv c(\mathrm{mod}n)$.

Heltalen indelas då i restklasser efter vilken rest de ger vid division med n.

Exempel. Modulo 3 har vi restklasserna

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

Det gäller $[-6] = [-3] = [0] = [3] = [6]; [-5] = [-2] = [1] = [4] = [7]$ osv.

Exempel. Modulo 5 har vi restklasserna

$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$

$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$

$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

$$[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$$

$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

Där gäller $[-10] = [-5] = [0] = [5] = [10]$ och $[-14] = [-9] = [-4] = [1] = [6] = [11]$ osv.

Observera att varje n ger upphov till ett eget system av talrester modulo n, som betecknas $\mathbb{Z}_n$. Restklasser modulo n har olika egenskaper för olika n.

Att ett tal a är **delbart** med n betyder att $a \equiv 0(\mathrm{mod} n)$. Detta är ett kraftfullt sätt att visa att ett tal är delbart med n. Mer om detta om en stund.

Vi tittar igen på exemplen ovan.

- $24 \equiv 3(\mathrm{mod}7)$ eftersom $24 - 3 = 21$ är jämnt delbart med 7. Så 24 mars är samma veckodag som 3 mars, en söndag.
- 8 april ligger 38 dagar efter 1 mars. $38 \equiv 3(\mathrm{mod}7)$ eftersom 35 är jämnt delbart med 7.

Räkneregler

Låt n vara ett positivt heltal, k ett godtyckligt heltal, och antag att $a \equiv b(\mathrm{mod} n)$ och $c \equiv d(\mathrm{mod} n)$. Då gäller

$$k \cdot a \equiv k \cdot b \ (\mathrm{mod} n) \quad (1)$$

$$a + c \equiv b + d \ (\mathrm{mod} n) \quad (2)$$

$$a \cdot c \equiv b \cdot d \ (mod n) \quad (3)$$

Bevis

(2): Vi har att $a = b + s \cdot n$ och $c = d + t \cdot n$ för vissa heltal s och t, så $a + c = b + d + (s + t)n$.

(3): Vi har som ovan att $a = b + s \cdot n$ och $c = d + t \cdot n$ för vissa heltal s och t, så $ac = (b + sn)(d + tn) = bd + btn + snd + stn2 = bd + (bt + sd + stn) \cdot n$, så $ac \equiv bd(\mathrm{mod} n)$ eftersom $bt + sd + stn$ är ett heltal.

(1) är ett specialfall av (3).

Upprepad användning av (3) ger att om $a \equiv b(\mathrm{mod}n)$ så $a^k \equiv b^k(\mathrm{mod}n)$ för varje positivt heltal k.

Subtraktion fungerar också "modulo n". Om $a \equiv b$ och $c \equiv d$ så gäller $a - c \equiv b - d$. (Här har vi underförstått Â´Â´mod n", det kan man göra när den s.k. modulen n framgår av sammanhanget.) Däremot går det i allmänhet inte att dividera kongruenser. T.ex. gäller $9 \equiv 3(mod6)$, men $3 \not\equiv 1(mod6)$, så det går alltså inte att dividera med 3 (om man inte dividerar även modulen med 3). Ett annat exempel på att kongruensräkning skiljer sig från heltalsaritmetik att produkten av två tal som inte är noll kan bli noll. Ett sådant exempel är att trots att $2 \not\equiv 0(\mathrm{mod}6)$ och $3 \not\equiv 0(\mathrm{mod}6)$ så är $2 \cdot 3 = 6 \equiv 0(\mathrm{mod}6)$.

Återgå nu till de inledande exemplen med veckodagar och se hur du kan använda det nya sätt att räkna.

Ett annat exempel är att om vi vill beräkna sista siffran i ett tal, t.ex 37^{23}, så observerar vi att sista siffran fås som resten vid division med 10. Nu gäller modulo 10 att $37^{23} \equiv (-3)^2 3 = (-3)^{2\cdot 11+1} = (-3) \cdot ((-3)^2)^{11} = -3 \cdot (9)^{11} \equiv -3 \cdot (-1)^{11} = -3 \cdot (-1) = 3$

För att se hur kraftfull kongruensräkning är kan du fundera på hur man skulle beräkna sista siffran i 37^{23} med "vanlig" aritmetik. En annan metod är dock att observera att vid upprepad multiplikation av ett tal som slutar på 7 med sig självt så får man successivt tal med slutsiffra $7, 9, 3, 1, 7, 9, 3, 1, \cdots$, alltså ett periodiskt förlopp med period 4, så det gäller att finna var 23 passar in, m.a.o. vad 23 är modulo 4.

Våra delbarhetsregler kan lätt verifieras med kongruensräkning. Vi har t.ex.: ett heltal är delbart med 11 precis då dess alternerande siffersumma är delbar med 11. Låt nämligen talet vara $a = a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0$, där $a_n, a_{n-1}, \ldots, a_0$ är siffrorna då a skrivs i bas 10 som vanligt, så (modulo 11)

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_{n-2} \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$$

$$\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \ldots + a_{n-2} \cdot (-1)^{n-2} + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n \pmod{11}$$

$$\equiv a_0 - a_1 + a_2 - \ldots + a_{n-2} \cdot (-1)^{n-2} + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n \pmod{11}.$$

Talet ger alltså samma rest vid division med 11 som sin alternerande siffersumma.

Övning B

Delbarhetskriterier: Använd kongruensräkning för att bevisa delbarhetstester nedan:

1. Ett tal är delbart med 2 omm (om och endast om) entalssiffran är delbar med 2.
2. Ett tal är delbart med 5 omm entalssiffran är 0 eller 5.
3. Ett tal är delbart med 9 omm siffersumman är delbar med 9.

4. Ett tal är delbart med 3 omm siffersumman är delbar med 3.
5. Ett tal är delbart med 4 omm talet bildat av de två sista siffrorna är delbart med 4.
6. Ett tal är delbart med 8 omm talet bildat av de tre sista siffrorna är delbart med 8.
7. Ett tal är delbart med 11 omm den alternerande siffersumman är delbar med 11. (Se ovan.)

Övning C

1. Bestäm sista siffran i talen

   (a) 2^{2002}, (b) 13^{20}, (c) $7^{7^{7^7}}$.

2. Bestäm resten vid division av

   (a) 3^{100} med 7, (b) 2^{1000} med 3,5,11,13, (c) 99^{99} med 13.

   Ledning. Visa först att $99^2 \equiv -1 \pmod{13}$. Se lösningar på slutet av stencilen och exempel 3.12, 3.13 i Vretblads bok.

Övning D

1. (a) P. Fermat påstod att talen $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, ...$ är primtal. Det är verkligen sant då $n = 0, 1, 2, 3, 4$. Visa det! (en miniräknare kan vara till hjälp).

   (b) Hundra år senare visade L. Euler att $641 | F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$. Visa det genom att räkna i $\mathbb{Z}_{641}$ och utnyttja följande likheter: $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$.

2. (a) För 2500 år sedan påstod kinesiska matematiker att om ett heltal $n > 1$ är en delare till $2^n - 2$ så måste n vara ett primtal. Detta påstående är sant då $n < 341$ men $341 | 2^{341} - 2$ trots att 341 inte är ett primtal. Visa det!

   Ledning. $341 = 11 \cdot 31$ och $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$.

   Anmärkning. P. Fermat kände till den kinesiska hypotesen och han visste att hans tal $F_n = 2^{2^n} + 1$ hade egenskapen

   $$F_n | 2^{F_n} - 2.$$

   Det var grunden för hans påstående att F_n var primtal.

   (b) Visa att $F_n | 2^{F_n} - 2$.

Övning E

1. (a) Beräkna summorna

   $1^3 + 2^3$ modulo 3,

$1^3 + 2^3 + 3^3 + 4^3$ modulo 5,

$1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3$ modulo 7.

Ser Du ett mönster? Vad kan man säga om summan

$1^3 + 2^3 + ... + 100^3$ modulo 101?

Ledning. Räkna i $\mathbb{Z}_{101}$.

(b) Kan Du ställa upp en förmodan angående summan

$1^3 + 2^3 + ... + (n-1)^3$

modulo n? Bevisa Ditt påstående!

2. Visa att $m|1^k + 2^k + ... + (m-1)^k$ då k och m är positiva udda heltal.

Övning F

1. Beräkna inverser a^{-1} till alla $a \in \mathbb{Z}_7$, $a \neq 0$. Beräkna också $\sum a^{-1}$, $a \in \mathbb{Z}_7$, $a \neq 0$.

2. Låt p vara ett udda primtal. Visa att om

$$1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b},$$

där a, b är heltal så gäller $p|a$.

Ledning. Utnyttja att $\mathbb{Z}_p$ är en kropp dvs varje nollskild rest har invers .

Övning G

1. Låta x vara ett udda heltal. Visa att $x^2 \equiv 1 \pmod 8$. Vilka rester ger kvadrater av heltalen modulo 8?

2. Visa att om $x^3 + y^3 = z^3$, där x, y, z är heltal så är minst ett av dessa tal delbart med 7.

Ledning. Arbeta med rester modulo 7. Visa att $x^3 \equiv \pm 1 \pmod 7$ om $7 \nmid x$.

3. Visa att om $x^2 + y^2 = z^2$, där x, y, z är heltal så finns det bland dessa tal ett som är delbart med 3 och ett delbart och ett delbart med 5 ($3^2 + 4^2 = 5^2$ är "den minsta" Pythagoreiska triangeln).

4. Visa att om $x^2 + y^2 = z^2$, där x, y, z är heltal så är x eller y delbart med 4.

Ledning. Man kan förutsätta att x, y, z är relativt prima (har största gemensamma delaren lika med 1). Betrakta rester av talen modulo 8. Motivera att ett av talen x, y är jämnt och ett udda.

Övning H

1. Visa att $6|n^3 - n$ då n är ett heltal.
2. Fermats lilla sats säger att att $p|a^p - a$ då p är ett primtal och a är ett godtyckligt heltal. Utnyttja denna sats i följande uppgifter:
3. Visa att $30|n^5 - n$ då n är ett heltal.
4. Visa att $42|n^7 - n$ då n är ett heltal.

Övning I

1. Bestäm det minsta positiva heltalet n som lämnar resterna 1,2,3,4,5 vid division med respektive 2,3,4,5,6.
2. Bestäm alla n sådana att $4|n$, $9|n+1$, $25|n+2$.

Följande övningar i Vretblads bok rekommenderas:

Vretblad: 3.21, 3.22, 3.26, 3.27, 3.30 – 3.34.

Några exempel på lösningar:

Lösning till C2 (b): Vi skall beräkna resten vid division av 2^{1000} med 11. Först noterar vi att $2^5 \equiv -1 \pmod{11}$ ty $2^5 + 1 = 33 \equiv 0 \pmod{11}$. Nu har vi $2^{1000} = (2^5)^{200} \equiv (-1)^{200} \pmod{11}$. Men $(-1)^{200} = 1$ så att $2^{1000} \equiv 1 \pmod{11}$ dvs 2^{1000} lämnar resten 1 vid division med 11.

Lösning till G3: Vi skall visa att om x, y, z är tre heltal sådana att $x^2 + y^2 = z^2$ så är ett av talen delbart med 5. Den sista likheten implicerar likheten av rester vid division med 5: $[x^2 + y^2]_5 = [z^2]_5$ dvs $[x^2]_5 + [y^2]_5 = [z^2]_5$. Om $r = 0, 1, 2, 3, 4$ är en rest vid division med 5 så är $r^2 = 0, 1, 4, 4, 1$ dvs kvadrater av resterna modulo 5 är lika med 0 eller 1 eller 4. Alltså är alla $[x^2]$, $[y^2]$, $[z^2]$ lika med 0 eller 1 eller 4. Om ingen av dessa tre är lika med 0 så är alla lika med 1 eller 4. Detta ger $[z^2]_4 = [x^2]_5 + [y^2]_5 = 2$ eller 3, vilket är omöjligt. Alltså måste minst en av dessa tre kvadrater vara lika med 0 dvs ett av talen x, y, z lämnar resten 0 vid division med 5.

Lösning till H2: Vi visar att $30|n^5 - n$ för alla heltal n. Vi har $30 = 2 \cdot 3 \cdot 5$. Det är klart att $2|n^5 - n$ (kontrollera fallen n jämnt, n udda). Om $3|n$ så är det klart att $3|n^5 - n$. Om $3 \nmid n$ så har vi $n^5 - n = n(n^4 - 1) = n[(n^2)^2 - 1]$, vilket är delbart med 3 enligt Fermats lilla sats (den säger att $3|a^2 - 1$ om $3 \nmid a$ – här är $a = n^2$). I varje fall $3|n^5 - n$. Det återstår att visa $5|n^5 - n$, men detta är precis vad Fermats lilla sats säger för primtalet 5.

Kapitel 8

POLYNOM OCH POLYNOMEKVATIONER

Syftet med denna övning är att repetera gymnasiekunskaper om polynom och polynomekvationer samt att bekanta sig med en del nya egenskaper hos polynom. Vi kommer att undersöka hur olika egenskaper hos polynom beror på deras koefficienter. Därför betraktar vi polynom med koefficienter i olika talområden: $\mathbb{Z}$ (heltaliga koefficienter), $\mathbb{Q}$ (rationella koefficienter), $\mathbb{R}$ (reella koefficienter), $\mathbb{C}$ (komplexa koefficienter). Vi betecknar med $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ alla polynom med koefficienter i respektive $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$. Om R betecknar ett av dessa talområden så skriver vi $R[X]$ för alla polynom med koefficienter i R. $R[X]$ kallas **polynomringen över** R. De viktigaste begreppen i detta avsnitt är

- Delbarhet av polynom
- Divisionsalgoritmen
- Största gemensamma delaren
- Reducibla och irreducibla polynom
- Nollställen till polynom (dubbla rötter, multipla rötter)
- Faktoruppdelningar av polynom i olika polynomringar

Vi följer kapitel 7 i Vretblads bok.

Övning A

Den första övningen ägnas åt divisionsalgoritmen. Om $f(X)$ och $g(X) \neq 0$ är två polynom så betecknar vi med $q(X)$ och $r(X)$ kvoten och resten vid division av $f(X)$ med $g(X)$. Man har $f(X) = g(X)q(X) + r(X)$, där $\operatorname{grad} r(X) < \operatorname{grad} g(X)$ eller $r(X) = 0$.

1. Bestäm kvoten och resten vid division av följande polynom:
   (a) $f(X) = X^4 + 5X^3 - 3X + 2,\ \ g(X) = X^2 - 1$
   (b) $f(X) = 5X^3 - 2X + 1,\ \ g(X) = X^2 + X$
   (c) $f(X) = X^4 + 2X^3 + 4X^2 + 2X + 3,\ \ g(X) = X^2 + 2X + 3$
2. Vad kan man säga om resten vid division av ett polynom $f(X)$ med ett polynom $X - a$? Vilken grad har resten? Bevisa att resten av $f(X)$ vid division med $X - a$ är lika med $f(a)$.
   Ledning. Enligt divisionsalgoritmen är $f(X) = (X-a)q(X)+r(X)$. Vad kan man säga om $r(X)$? Beräkna resten genom insättning av $X = a$.
3. Beräkna resten vid division av $f(X)$ med $X - a$ då
   (a) $f(X) = X^3 - 2X^2 + 8X + 5,\ \ a = 3$
   (b) $f(X) = 3X^4 + 5X^2 - 4X - 11,\ \ a = -1$
   Du behöver inte utföra divisionen!

Övning B

1. Vad säger faktorsatsen? Försök förklara hur man utnyttjar faktorsatsen för att lösa polynomekvationer.
2. Lös ekvationen $X^3 - 6X^2 + 11X - 6 = 0$ som har en rot $X = 1$.
3. Lös uppgift 7.24 i Vretblads bok.

Övning C

Låt $K[X]$ vara en av polynomringarna $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$.

1. Vad menas med ett reducibelt, respektive irreducibelt, polynom i $K[X]$?
2. Om möjligt, uppdela följande polynom i produkt av minst två polynom av lägre grad i $\mathbb{Q}[X]$, $\mathbb{R}[X]$ och $\mathbb{C}[X]$:
   (a) $f(X) = X^2 + 1$
   (b) $f(X) = X^4 - 1$
   (c) $f(X) = X^4 + 4$
   (d) $f(X) = X^4 + 2X^2 + 9$
   Vilka av polynomen är irreducibla i respektive polynomring?

3. Visa att följande polynom är irreducibla i givna polynomringar (dvs inte kan faktoruppdelas i produkt av två polynom av lägre grad):

   (a) $X^3 - 2$ i $\mathbb{Q}[X]$

   (b) $X^2 + 2X + 2$ i $\mathbb{R}[X]$

   (c) $X^4 + 1$ i $\mathbb{Q}[X]$

   Ledning. Nästa uppgift kan underlätta denna. Om ett polynom har heltaliga koefficienter och kan uppdelas i produkt av två polynom av lägre grad med rationella koefficienter så kan det också uppdelas i en produkt av två polynom med heltaliga koefficienter och samma grad. Detta påstående kallas ”Gauss lemma” och visas t ex i kursen ”Algebraisk talteori”. Du får använda detta (ganska självklara) resultat i (c).

4. Låt $f \in K[X]$. Visa att

   (a) Om $\operatorname{grad} f \geq 2$ och f har ett nollställe i K så är f reducibelt i $K[X]$.

   (b) Om $\operatorname{grad} f = 2$ eller 3 så är f reducibelt i $K[X]$ då och endast då f har nollställen i K.

   (c) Konstruera ett exempel som visar att (b) inte gäller då $\operatorname{grad} f = 4$.

5. Faktoruppdela de givna polynomen i produkt av irreducibla i $\mathbb{Q}[X]$, $\mathbb{R}[X]$ och $\mathbb{C}[X]$:

   (a) $X^4 - 1$

   (b) $X^4 + X^2 - 6$

   (c) $X^6 + 1$

Övning D

1. Vad menas med att ett polynom $d(X) \in K[X]$ delar ett polynom $f(X) \in K[X]$?

2. Vad menas med största gemensamma delaren till två polynom $f(X)$ och $g(X)$? Beräkna $\mathrm{SGD}(f, g)$ med hjälp av Euklides algoritm då

   (a) $f(X) = X^5 - 14X - 4,\ \ g(X) = X^3 - 3X - 2$

   (b) $f(X) = X^4 - 1,\ \ g(X) = 2X^3 - X^2 + 2X - 1$

   Anmärkning. På samma sätt som för heltal visar man att $\mathrm{SGD}(f, g) = fp + gq$, där p och q är lämpliga polynom. Polynomen p och q kan beräknas med hjälp av Euklides algoritm.

3. Bevisa att om två polynom f och g är relativt prima dvs $\mathrm{SGD}(f, g) = 1$ och $f|h$ samt $g|h$ så $fg|h$. Kan Du se en likhet med en sats om heltal? Vilken?

4. Bevisa att om ett polynom d delar produkten fg av två polynom och d är relativt primt med f (dvs $\mathrm{SGD}(d, f) = 1$) så d delar g. Vad säger motsvarande sats om heltalen?

Övning E

Lösning av ekvationer. En polynomekvation är en ekvation av typen $f(X) = 0$, där $f(X)$ är ett polynom. Svårigheterna med att lösa sådana ekvationer växer med graden. Helt banalt löser man förstagradsekvationer: $ax + b = 0$, $a \neq 0$ ger $x = -\frac{b}{a}$. För andragradsekvationer $ax^2 + bx + c = 0$, $a \neq 0$, har man den välkända formeln

$$x_{1,2} = -\frac{b}{2a} \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}$$

som kan härledas med kvadratkomplettering. För ekvationer av grad 3 och 4 existerar mycket mer komplicerade formler som man lyckades härleda under 1500–talet. Man vet att för helt godtyckliga ekvationer av grad ≥ 5 är det inte möjligt att uttrycka rötterna med hjälp av de fyra räknesätten och rotutragningar som tillämpas på ekvationens koefficienter. Detta visades av den store norske matematikern N.H. Abel* och den lika berömde franske matematikern É. Galois† Rent praktiskt löser man ofta polynomekvationer med numeriska metoder som ger helt tillfredsställande närmevärden till lösningarna. Ibland utnyttjas enkla satser vars tillämpningsmöjligheter är ganska begränsade när det gäller att lösa ekvationer, men är helt tillräckliga i undervisningssammanhang. Vi har två sådana satser i kursboken:

Om ett rationellt tal $\frac{p}{q}$, där $p, q \in \mathbb{Z}$, $SGD(p, q) = 1$, är ett nollställe till polynomet $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ med heltaliga koefficienter a_i, så är p en delare till den lägsta koefficienten a_0, och q är en delare till den högsta koefficienten a_n.

Om α är ett (komplext) nollställe till ett polynom $f(X)$ med reella koefficienter, dvs $f(\alpha) = 0$, så är också $\bar{\alpha}$ ett nollställe till $f(X)$, dvs $f(\bar{\alpha}) = 0$.

1. Lös följande ekvationer:
   (a) $X^3 - 6X^2 + 11X - 6 = 0$
   (b) $2X^3 - X^2 + 2X - 1 = 0$
   (c) Övning 7.65 eller 7.66 i Vretblads bok.
2. Lös uppgifterna 7.45 och 7.52 i Vretblads bok.
3. Man vet att polynomet $X^4 - 2X^3 + 3X^2 - 2X + 2$ har ett nollställe $1 + i$. Bestäm alla andra nollställen till polynomet.

*Nils Henrik Abel (5/8 1802 – 6/4 1829). Abel visade sina resultat om ekvationer av grad ≥ 5 när han var 19 år gammal. Han löste många viktiga matematiska problem inom flera olika områden. I Oslo finns hans monument i den Kungliga Parken.

†Évariste Galois (25/10 1811 – 30/5 1832). Under sitt mycket korta liv skapade Galois en mycket viktig teori idag kallad ”Galoisteori” som sysslar med polynomekvationer. Han visade hur abstrakta matematiska teorier kan bidra till att lösa komplicerade matematiska problem. På det sättet bidrog han till utvecklingen av den moderna matematiken. Galois lade grunden för gruppteorin och teorin för ändliga kroppar. Dessa teorier har stor betydelse för hela matematiken och dess tillämpningar inom fysik, kemi, kodningsteori och radarkommunikation.

Övning F

1. Låt $N = a_n a_{n-1} \dots a_1 a_0$ beteckna ett naturligt tal med siffrorna a_i (t ex $N = 452 = a_2 a_1 a_0$ med $a_0 = 2$, $a_1 = 5$, $a_2 = 4$). Betrakta polynomet

$$(*) \qquad f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

(a) **Delbarhetskriterium vid division med 3 och 9.** Visa att N är delbart med 3 (respektive 9) då och endast då siffersumman i N är delbar med 3 (respektive 9).

Ledning. Dividera $f(X)$ med $X - 1$. Observera att $N = f(10)$ och att siffersumman i N är lika med $f(1)$. Sätt in $X = 10$ och drag slutsatsen att N och dess siffersumma ger samma rest vid division med 3 (respektive 9).

(b) **Delbarhetskriterium vid division med 11.** Visa att N ger samma rest vid division med 11 som sin *alternerande siffersumma* $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ (exempel: 1936 är delbart med 11 ty $6 - 3 + 9 - 1 = 11$ är delbart med 11).

Ledning. Gör som i (a), men ersätt $X - 1$ med $X + 1$.

Övning G

Derivatan av ett polynom. Låt $f(X) = a_0 + a_1 X + \ldots + a_n X^n \in K[X]$. Derivatan av $f(X)$ definieras helt formellt som

$$f'(X) = a_1 + 2a_2 X + \ldots + n a_n X^{n-1}.$$

Man kan utan svårigheter kontrollera de vanliga deriveringsreglerna

$$(f + g)' = f' + g' \quad \text{och} \quad (fg)' = f'g + fg'.$$

1. Visa att $a \in K$ är ett multipelt nollställe till $f \in K[X]$ (dvs a har multipliciteten > 1) då och endast då $f(a) = f'(a) = 0$.

Lösning. "⇒" Låt $f(X) = (X - a)^2 q(X)$ (multipliciteten av a är minst 2). Då är $f'(X) = 2(X - a)q(X) + (X - a)^2 q'(X)$ så att $f(a) = f'(a) = 0$.

"⇐" Antag att $f(a) = f'(a) = 0$ och att multipliciteten av a är 1 dvs $f(X) = (X-a)q(X)$ och $q(a) \neq 0$. Då är $f'(X) = q(X)+(X-a)q'(X)$ så att $f'(a) = q(a) \neq 0$ – en motsägelse.

2. Bestäm reella tal a och b så att polynomet $f(X) = aX^{2000} + bX^{1999} + 1$ är delbart med $(X - 1)^2$.

3. Lös uppgift 7.113 i Vretblads bok.

Övning H

1. Lös följande kvadratiska ekvationer genom att utnyttja sambandet mellan rötter och koefficienter, Vretblad sid. 172-173 (utan formler eller kvadratkomplettering):
   (a) $X^2 - 6X + 8 = 0$
   (b) $X^2 + 5X + 6 = 0$
   (c) $X^2 - X - 2 = 0$

2. Låt x_1, x_2, x_3 beteckna rötterna till ekvationen $aX^3 + bX^2 + cX + d = 0$, $a \neq 0$. Skriv ut sambanden mellan ekvationens rötter och koefficienter. Ange en ekvation av grad 3 med rötterna 1,2,3.

3. Låt x_1, x_2 och x_3 vara rötterna till ekvationen $X^3 - 5X^2 + 6X + 7 = 0$. Beräkna $x_1^2 + x_2^2 + x_3^2$ och $x_1^3 + x_2^3 + x_3^3$.