Explorativ övning 3

DELBARHET OCH PRIMTAL*

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

De viktigaste begreppen är

- delbarhet och divisionsalgoritmen
- största gemensamma delaren
- minsta gemensamma multipeln
- Euklides algoritm
- primtal
- Aritmetikens fundamentalsats
- presentation av heltal i olika baser.
- 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.

De viktiga uppgifterna (eller de som rekommenderas) är **A – H, K**. Bland de övriga, välj de uppgifter som Du tycker är intressanta. Vi återkommer till talteorin senare i avsnittet om “Restaritmetiker” (som ofta kallas för “klockaritmetiker”).

* **preliminär version**

jub@math.chalmers.se (Juliusz Brzezinski)

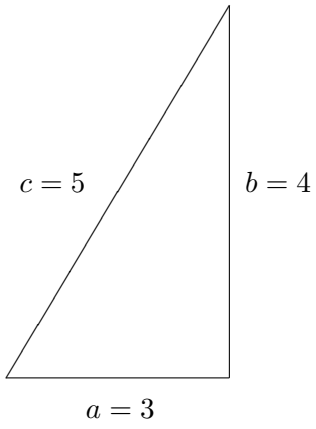
DELBARHET OCH DIVISIONSALGORITMEN

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:

(3.1) 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 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

[†] 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.

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 Övning K 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:

(3.2) 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. Se vidare Övning P. □

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:

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

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

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:

(3.4) 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 $b = \pm a$.*

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:

(3.5) 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:

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

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.

(3.7) Euklides sats. *Det finns oändligt många 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. 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 C

1. Utnyttja rutat papper för att rita alla möjliga rektanglar med 1,2,3,4,5,6,7,8,9,10,11, 12 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. Föreslå en beräkningsprocedur (en algoritm) som kan avgöra om ett givet heltal är primt. Försök avgöra om talet 143 är primt. (Läs eventuellt om primtal och "Eratosthenes såll" i "Matte med mening" på sid. 32).

4. 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?

5. 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.

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 SGD(a,b)) och den minsta gemensamma multipeln (betecknas MGM(a,b)). T ex är man intresserad av SGD(a,b) då man vill förkorta bråket $\frac{a}{b}$ (t ex $\frac{24}{40}=\frac{3}{5}$, ty 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 MGM$(12,30)=60$). Formella definitioner av dessa begrepp som är mest vanliga i matematiska sammanhang är följande:

(3.8) 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 SGD(a,b). Man brukar definiera SGD$(0,0)=0$. Man säger att a och b är **relativt prima** om 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 $d'=d$.

(3.9) 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 MGM(a,b). Som för SGD definierar man 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 SGD(a,b) ovan!).

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

(3.10) 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 $d=$ 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 SGD(a, b) utan också två heltal x, y sådana att SGD$(a, b) = ax + by$. Vi illustrerar detta med samma exempel:

(3.11) 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 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:

(3.12) 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:

(3.13) 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 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 D

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

Övning E

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 F

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 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 satsen (3.14) nedan.

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

$$\begin{aligned} 100 &= 2^2 \cdot 5^2, \\ 108 &= 2^2 \cdot 3^3, \\ 2002 &= 2 \cdot 7 \cdot 11 \cdot 13. \end{aligned}$$

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:

(3.14) 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 SGD$(p, a) = 1$ därför att p är ett primtal. Enligt (3.22) 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:

(3.15) 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. □

(3.16) Anmärkning. Ofta kallar man sats (3.14) 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 SGD(a, b) och MGM(a, b) utan Euklides algoritm. Även om denna möjlighet inte är särskilt praktisk används den flitigt i skolan.

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

(3.18) 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 G

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.

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-Kharezmi) 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

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

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 siffror" och 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.

[¶]Se t ex artikeln "Att utveckla små barns antalsuppfattning" av Elisabet Doverborg och Ingrid Pramling Samuelsson i Nämnaren Tema "Matematik från början", NCM, Göteborg 2000.

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 H

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

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

3. 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?

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

5. 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?

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

[‖] 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.

jub@math.chalmers.se (Juliusz Brzezinski)

7. 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 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.

(3.19) 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:

(3.20) 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 I

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 J

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 $(1234)_6$.

Övning K

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 $2(x - x_0) = 5(y - y_0)$. 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.

Exempel till Övning K: 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 i

[**] 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

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

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.

enlighet med (3.11), 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. □

Övning L

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.

Övning M

Aritmetiska följder av primtal. Vi repeterar att en aritmetisk följd med differansen d är en följd av talen a, $a+d$, $a+2d$, …, $a+nd,\ldots$. (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 $3+4n$.

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

Övning N

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 O

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").

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 P

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.

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

[‡]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".

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.

Övning Q

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.

Följande övningar i Vretblads bok rekommenderas:

Vretblad: 2.42 a) (227 a)), 2.43 (228), 2.47 (230), 2.48 (231), 2.49 (232), 2.50 (233), 2.55 (235).

APPENDIX: NÅGRA BEVIS

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

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

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 $b \neq 0$. □

(3.22) 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. □

NÅGRA METODISKA SYNPUNKTER

Vikten av talteorin i skolan. Talteorin som motivationskälla.

Delbarhet med 0.

Aritmetikens fundamentalsats – sammansatta tal och primtal.

Datorer i matematikundervisningen (talteorins lämplighet).

1 ej primtal.

SGD och MGM – största och minsta (i vilken mening).