Explorativ övning 6

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 mycket enkelt och elementärt, är antalet övningar ganska stort. Men flera av dem finns för att visa att talteorin är mycket intressant, rolig och kan med fördel redan mycket tidigt utnyttjas i skolarbete.

De viktiga uppgifterna (eller de som rekommenderas) är **A – H, J, 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").

DELBARHET OCH DIVISIONSALGORITMEN

Vi börjar med en kort repetition av några viktiga egenskaper hos **heltalen**:

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

*MAL200/220, ht 00 – en preliminär version

(6.1) Definition. Om a och d är två heltal så säger man att d **delar** a om $a = dq$, där q är ett heltal. Man säger också att a är **delbart** med d eller att a är en **multipel** av d. Man skriver då $d|a$. Om d inte delar a så skriver man $d \nmid a$. En delare d till a kallas **äkta** (eller **icke–trivial**) om $1 < |d| < |a|$. □

Exempel. $3|6$, men $5 \nmid 8$. 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). Varje heltal a är alltid delbart med ± 1 och $\pm a$. Dessa delare kallas ofta "triviala". □

Du vet mycket väl hur man kan dela ett heltal med ett heltal skilt från 0 för att få **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:

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

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

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 $b \neq 0$. □

Övning A

1. 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;

2. 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.

3. Hur lyder en liknande egenskap hos heltalen då man ersätter 2 eller 3 ovan med t ex 5?

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:

(6.3) 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

De positiva heltalen större än 1 delas i primtal och sammansatta tal. Primtalen spelar en mycket viktig roll eftersom de är "byggstenar" för alla andra heltal – varje sammansatt heltal större än 1 är deras produkt.

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

Primtalen mindre än 100 är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Följden av primtalen är oändlig. Detta påstående visades för mer än 2000 år sedan av Euklides[†]. Euklides visade sin sats i nioende boken av sitt stora verk "Elementa" genom att använda följande sats från sjunde boken:

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

Bevis. Satsen visas med hjälp av matematisk induktion. Om $n = 2$ så är satsen klar ty 2 är ett primtal. Antag att satsen gäller för alla heltal $2, 3, \ldots, k$. Vi visar att satsen gäller för nästa tal $n = k+1$. Om $k+1$ är ett primtal så är påståendet klart ty $k+1|k+1$. Om $k+1$ är sammansatt så har $k+1$ en äkta delare $1 < d < k+1$. Enligt vårt induktiva antagande gäller satsen för d dvs det finns ett primtal p som delar d. Detta primtal är i sin tur en delare till $k+1$. Enligt induktionsprincipen gäller satsen för varje heltal $n > 1$ dvs varje n är delbart med ett primtal. □

Nu kan vi bevisa att det finns oändligt många primtal.

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

Bevis. Antag att $p_1, p_2, \ldots, p_n$ är alla primtal. Bilda talet

$$N = p_1 p_2 \cdots p_n + 1.$$

Talet N är större än 1 så det måste vara delbart med ett primtal p (se sats (6.5)). Primtalet p är ett av primtalen $p_1, p_2, \ldots, p_n$. Alltså delar p både N och $N - 1 = p_1 p_2 \cdots p_n$. Men detta innebär att p också delar $N - (N - 1) = 1$, vilket är orimligt. Vårt antagande att det endast finns ändligt många primtal har lett oss till en motsägelse. Alltså måste antagandet vara falskt dvs det finns oändligt många primtal. □

Övning C

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

[†]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.

3. 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?

4. 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 avsnittet om "Delbarhet och primtal").

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:

(6.7) 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 $d' = d$.

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

(6.9) Anmärkning. Det är klart att $\mathrm{SGD}(a,b)$ är störst bland alla delare till a och b, medan $\mathrm{MGM}(a,b)$ är minst bland alla gemensamma multipler av dessa tal. T ex kunde vi i definitionen av $d=\mathrm{SGD}(a,b)$ 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 dessa SGD och MGM i praktiken? En mycket viktig metod är **Euklides algoritm**. Euklides algoritm säger hur man kan beräkna $\mathrm{SGD}(a,b)$. Man bildar en divisionskedja:

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

Varje kedja av den här typen måste vara ändlig därför att en avtagande kedja av resterna $r_1 > r_2 > r_3 > \ldots \ge 0$ 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 $\mathrm{SGD}(a,b)$. 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 ett exempel:

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

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

så att $\mathrm{SGD}(444, 210) = 6$ (den sista nollskilda resten). 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 enkelt bevis. 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.

(6.11) 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. □

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:

(6.12) 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 D

1. Vad menas med största gemensamma delaren (SGD) till två heltal a och b? Jämför Dina funderingar med definitionen som följer.

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) $a = 102, b = 165$,

   (b) $a = 1133, b = 1111$.

   Utnyttja Euklides algoritm i enlighet med exempel i avsnittet om "Delbarhet och primtal".

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. 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 SGD$(a, b) = d$, MGM$(a, b) = m$, $a = da'$, $b = db'$. Motivera först att $m = d_0a'b'$ för ett heltal d_0 (observera att a' och b' delar m och är relativt prima). Visa att $d|d_0$ genom att utnyttja $a = da'|m$ och $b = db'|m$. Man får $d|d_0b'$ och $d|d_0a'$. Men $1 = a'x + b'y$ för lämpliga x och y så att $d_0 = d_0a'x + d_0b'y$ är delbart med d. En annan möjlighet är att studera primfaktoruppdelningar av a, b och SGD(a, b) samt MGM(a, b).

Övning G

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.

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. Vi skall visa detta påstående om en liten stund. Först behöver vi en mycket viktig egenskap hos primtalen:

(6.13) 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 (6.11) 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 $p|b$. □

Nu kan vi visa satsen om faktoruppdelningar av heltal i produkter av primtal:

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

$$n = p_1 p_2 \cdots p_m = p_1' p_2' \cdots p_n',$$

där p_i *och* p_j' *är primtal så är* $m = n$ *och vid en lämplig numrering av faktorerna är* $p_i = p_i'$.

Bevis. Först visar vi med induktion att varje heltal $N > 1$ är en produkt av primtal. Vi börjar med $N = 2$ då vårt påstående gäller. Låt $N > 2$ och antag att varje positivt heltal större än 1 och mindre än N är en produkt av primtal. Som vi vet från sats (6.5) finns det ett primtal p som delar N. Låt $N = pq$. Om $q = 1$ så är $N = p$ ett primtal (en produkt med endast en faktor!). Om $q \neq 1$ så är $1 < q < N$. Alltså är q en produkt av primtal och därmed är också N en sådan produkt.

Entydigheten visar vi med induktion med avseende på summan $s = m + n$. Om $s = 2$ så har vi $m = n = 1$ och $p_1 = p_1'$. Antag att vårt påstående gäller då antalet faktorer är mindre än s och låt

$$p_1 p_2 \cdots p_m = p_1' p_2' \cdots p_n',$$

där $m + n = s$. Primtalet p_m är en delare till produkten till höger så att enligt (6.13) är p_m en delare till en av faktorerna. Genom att eventuellt numrera om dessa faktorer kan vi anta att $p_m | p_n'$. Men båda dessa tal är primtal så att $p_m = p_n'$. Alltså gäller

$$p_1 p_2 \cdots p_{m-1} = p_1' p_2' \cdots p_{n-1}',$$

och i denna likhet är antalet primfaktorer lika med $s - 2 < s$. Enligt induktionsantagandet är antalet faktorer till vänster lika med antalet faktorer till höger dvs $m - 1 = n - 1$. Alltså är $m = n$. Dessutom kan man numrera faktorerna så att $p_i = p_i'$ då $i = 1, \ldots, n - 1$. □

(6.15) Anmärkning. Ofta kallar man sats (6.13) 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.

(6.16) 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. □

(6.17) 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. □

POSITIONSSYSTEM

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.

(6.18) 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:

(6.19) 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 H

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 I

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 J

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 J: 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

[‡]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 $x = 3$, $y = 2$, $z = 2$, $t = 3$.

Euklides algoritm i enlighet med (6.10), 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 K

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.

Lösning till Övning K 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.

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).

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 $3 + 4n$.

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.

[¶] 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.

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.

   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 $641 | F_5$.

**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. 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).