Explorativ övning 6

DELBARHET OCH PRIMTAL*

Syftet med denna övning är att bekanta sig med delbarhetsegenskaper hos heltalen. Låt a, b och d beteckna heltal. De viktigaste begreppen är

- delbarhet (d delar a)
- primtal
- största gemensamma delaren ($SGD(a, b)$)
- minsta gemensamma multipeln ($MGM(a, b)$)
- Euklides algoritm
- Aritmetikens fundamentalsats

Vi sysslar också med presentation av heltal i olika baser.

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 och rolig. 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". I Vretblads bok diskteras delbarhetsbegreppet i avsnitten 2.1 – 2.4.

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;

*MAL200, ht 99

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?

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 i stencilen om “Delbarhet och primtal”.

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 $b = \pm a$.

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).

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”).

Övning D

1. Vad menas med största gemensamma delaren (SGD) till två heltal a och b? Jämför Dina funderingar med definitionen i stencilen om "Delbarhet och primtal".

2. Beräkna $SGD(a,b)$ samt två heltal x_0 och y_0 sådana att $SGD(a,b) = ax_0 + by_0$ då

   (a) $a = 78, b = 21$,

   (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?

   Ledning. Se stencilen om "Delbarhet och primtal".

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 $\mathrm{SGD}(a,b) = d$, $\mathrm{MGM}(a,b) = m$, $a = da'$, $b = db'$. 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 $\mathrm{SGD}(a,b)$ samt $\mathrm{MGM}(a,b)$.

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.

Övning H

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

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

eller alla heltalspar (x, y) som löser ekvationen

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

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

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

där $n > 2$. Det tog mer än 350 år att lösa den ekvationen. I september 1994 visade den engelske matematikern Andrew Wiles att ekvationen saknar heltaliga lösningar (x, y, z) med $xyz \neq 0$. I talteorin finns många närbesläktade problem som fortfarande väntar på sin lösning. Vi skall i denna övning syssla med mycket enkla Diofantiska ekvationer av typen $ax + by = N$.

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

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

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

   Ledning. Gör som ovan.

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

[‡]Catalans ekvation är

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

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

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

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.

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 $SGD(a, d) = 1$) 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

[¶] 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".

detta fast det är lite jobbigt). Visa att det finns oändligt många n sådana att $f(n)$ är sammansatt.

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

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

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

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.

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.

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).