Elementär talteori

Lars-Åke Lindahl

2012

Förord

Detta kompendium innehåller material för en fempoängskurs i elementär talteori och har sammanställts av föreläsningsanteckningarna till en kurs i ämnet som jag höll vårterminen 2002 och har tidigare förelegat i en engelskspråklig version.

Innehållet är elementärt i den meningen att de enda förkunskaper och färdigheter som krävs för att ta sig igenom materialet, utöver grundläggande gymnasiekunskaper, är förtrogenhet med induktionsbevis och indirekta bevis samt kännedom om gränsvärdesbegreppet för talföljder. Närmare bestämt behöver man veta att begränsade monotona följder har ett gränsvärde. (Diskussionen om antalet primtal i avsnitt 2 fordrar visserligen mer analyskunskaper, men den delen kan hoppas över utan att sammanhanget går förlorat.) Speciellt behöver man alltså inte ha läst någon kurs i algebra även om kunskaper i abstrakt algebra naturligtvis är en fördel och ökar förståelsen.

Samtliga avsnitt avslutas med övningsuppgifter, som i stor utsträckning hämtats från ett kompendium av Stig Christofferson. Jag är tacksam för att jag fått hans tillstånd till detta. Svar till övningarna finns i slutet av kompendiet, och flertalet teoriuppgifter har också försetts med ledningar eller lösningar.

En preliminär version av kompendiet blev omsorgsfullt läst och kommenterad av Joakim Elgh, en av studenterna på kursen, och jag vill tacka honom för några mycket användbara förslag till förbättringar och förenklingar.

Uppsala, 2012
Lars-Åke Lindahl

Innehåll

1 Delbarhet

Definition 1.1 Ett heltal b är *delbart* med heltalet a, vilket skrivs $a \mid b$, om det finns ett heltal x sådant att $b = ax$. Man säger i så fall också att b är en *multipel* av a och att a är en *delare* till b.

Att a inte är en delare till b skrivs $a \nmid b$.

Varje heltal a är uppenbarligen delbart med talen ± 1 och $\pm a$. Dessa delare kallas *triviala*.

Bevisen för följande enkla egenskaper lämnas som övning till läsaren.

Sats 1.2 *Låt a, b och c vara heltal*

(i) *Om $a \mid b$ och $b \neq 0$, så gäller att $|a| \leq |b|$.*
(ii) *Om $a \mid b$, så gäller att $a \mid bc$.*
(iii) *Om $a \mid b$ och $b \mid c$, så gäller att $a \mid c$.*
(iv) *Om $c \mid a$ och $c \mid b$, så gäller att $c \mid (ax + by)$ för alla heltal x och y.*
(v) *Om $a \mid b$ och $b \mid a$, så är $a = \pm b$.*
(vi) *Antag att $c \neq 0$. Då gäller att $a \mid b$ om och endast om $ac \mid bc$.*

Varje nollskilt heltal har på grund av sats 1.2 (i) bara ändligt många delare. Två tal, som inte båda är 0, kan därför bara ha ändligt många gemensamma delare, och eftersom talet 1 är en gemensam delare finns det åtminstone en gemensam delare och därmed också en *största gemensam delare* till de båda talen.

Definition 1.3 Den största gemensamma delaren till två tal a och b, som inte båda är lika med noll, betecknas $\text{sgd}(a, b)$. För att begreppet ska bli definierat även i fallet $a = b = 0$ sätter vi vidare $\text{sgd}(0, 0) = 0$.

Om $\text{sgd}(a, b) = 1$ säger man att talen a och b är *relativt prima*.

Anmärkning. Lämpligheten av den speciella definitionen $\text{sgd}(0, 0) = 0$ kommer att framgå av sats 1.9.

Om åtminstone ett av talen a och b är skilt från noll, så gäller per definition ekvivalensen

$$d = \text{sgd}(a, b) \Leftrightarrow d \mid a \wedge d \mid b \wedge (x \mid a \wedge x \mid b \Rightarrow x \leq d).$$

Uppenbarligen är vidare

$$\text{sgd}(b, a) = \text{sgd}(a, b) = \text{sgd}(-a, b) = \text{sgd}(a, -b) = \text{sgd}(-a, -b),$$

så när man ska beräkna den största gemensamma delaren till två tal kan man ersätta dem med deras absolutbelopp.

Exempel 1 Talet 102 har de positiva delarna 1, 2, 3, 6, 17, 34, 51 och 102, och talet -170 har de positiva delarna 1, 2, 5, 10, 17, 34, 85 och 170. De gemensamma positiva delarna är 1, 2, 17 och 34. Följaktligen är $\text{sgd}(102, -170) = 34$. □

Att som i exemplet ovan bestämma den största gemensamma delaren till två tal genom att först bestämma alla delarna till de båda talen verkar inte vara någon praktiskt genomförbar metod om de båda givna talen är mycket stora. Vi ska därför beskriva en effektiv alternativ metod som bygger på följande sats.

Sats 1.4 *För alla heltal n är* $\text{sgd}(a, b) = \text{sgd}(a - nb, b)$.

Bevis. Sätt $r = a - nb$; då är $a = r + nb$. Om $c \mid b$, så följer det därför av sats 1.2 (iv) att $c \mid a$ om och endast om $c \mid r$. Paret a, b och paret a, r har följaktligen samma gemensamma delare. Speciellt har de samma största gemensamma delare. □

Vi kan på ett naturligt sätt utvidga definitionen av största gemensamma delare till att gälla fler än två tal − givet n heltal $a_1, a_2, \ldots, a_n$ som inte alla är lika med noll definierar vi deras *största gemensamma delare* $\text{sgd}(a_1, a_2, \ldots, a_n)$ som det största heltal som delar alla de givna talen. Slutligen utvidgar vi definitionen så att begreppet blir definierat för alla n-tiplar av heltal genom att sätta $\text{sgd}(0, 0, \ldots, 0) = 0$.

Talen $a_1, a_2, \ldots, a_n$ kallas *relativt prima* om $\text{sgd}(a_1, a_2, \ldots, a_n) = 1$, och de kallas *parvis relativt prima* om varje par av talen är relativt prima.

Exempel 2 Talen 4, 6, and 9 är relativt prima men inte parvis relativt prima. □

Sats 1.5 (Divisionsalgoritmen) *Givet heltal a och b med $a > 0$ finns det två entydigt bestämda heltal q och r sådana att $b = aq + r$ och $0 \leq r < a$.*

Talet q kallas *kvoten* och r kallas *(huvud)resten* vid division av b med a. Uppenbarligen är $q = \lfloor b/a \rfloor$, där $\lfloor x \rfloor$ betecknar det största heltalet som är mindre än eller lika med det reella talet x.

Bevis. Betrakta den aritmetiska följden

$$\ldots,\ b - 3a,\ b - 2a,\ b - a,\ b,\ b + a,\ b + 2a,\ b + 3a,\ \ldots.$$

Låt r beteckna det minsta icke-negativa heltalet i följden; då är per definition $r = b - qa$ för något heltal q och $0 \leq r < a$. Detta bevisar existensen av en kvot q och en rest r med de angivna egenskaperna.

För att bevisa entydigheten antar vi att vi också har två heltal q' och r' som uppfyller likheten $b = aq' + r'$ och olikheten $0 \leq r' < a$. Då följer genom subtraktion att

$$r - r' = a(q' - q) \quad \text{och} \quad -a < r - r' < a,$$

vilket ger oss olikheten

$$-a < a(q' - q) < a,$$

och efter division med det positiva talet a olikheten

$$-1 < q' - q < 1.$$

Eftersom $q' - q$ är ett heltal återstår endast möjligheten att $q' - q = 0$, dvs. $q' = q$, och detta medför förstås att $r = b - aq = b - aq' = r'$. Därmed är entydigheten bevisad. □

Rent allmänt kallas ett heltal r en *rest* till b vid division med a om det finns ett heltal q sådant att $b = aq + r$ (alltså utan ytterligare storleksrestriktioner på r). Om r och r' är två godtyckliga rester till b vid division med a, så är

uppenbarligen $r' - r = na$ för något heltal n, och omvänt är $r + na$ en rest för varje rest r och varje heltal n.

För huvudresten r är antingen $0 \leq r \leq a/2$ eller $a/2 < r < a$, och i det sistnämnda fallet satisfierar resten $r' = r - a$ olikheten $-a/2 < r' < 0$.

Vid division med a finns det med andra ord alltid en unik rest r som uppfyller olikheten $-a/2 < r \leq a/2$. Denna rest kallas *resten med minst belopp*. Vi har därför följande variant av divisionsalgoritm som för vissa ändamål är mer effektiv än den vanliga.

Sats 1.5' (Variant av divisionsalgoritmen) *Givet heltal a och b med $a > 0$ finns det två entydigt bestämda heltal q och r sådana att $b = aq + r$ och $-a/2 < r \leq a/2$.*

EXEMPEL 3 Eftersom $37 = 2 \cdot 13 + 11 = 3 \cdot 13 - 2$ är 11 är huvudresten och -2 resten med minst belopp då 37 divideras med 13. □

Vi ska nu diskutera en viktig klass av delmängder till mängden $\mathbf{Z}$ av alla heltal.

Definition 1.6 En icke-tom delmängd A av heltal kallas ett *ideal* om den är sluten under subtraktion och under multiplikation med godtyckliga heltal, dvs. om den har följande två egenskaper:

(i) $x, y \in A \Rightarrow x - y \in A$,
(ii) $x \in A$, $n \in \mathbf{Z} \Rightarrow nx \in A$.

EXEMPEL 4 Mängderna $\{0\}$, $\mathbf{Z}$ och $\{0, \pm 3, \pm 6, \pm 9, \dots\}$ är ideal, och allmänt är mängden $A = \{ng \mid n \in \mathbf{Z}\}$ av alla multipler av ett givet heltal g ett ideal. Det sistnämnda idealet säges vara *genererat* av talet g och betecknas $g\mathbf{Z}$.

Beteckningen $g\mathbf{Z}$ innebär att exempelvis $\{0, \pm 3, \pm 6, \pm 9, \dots\} = 3\mathbf{Z}$, $\{0\} = 0\mathbf{Z}$ och $\mathbf{Z} = 1\mathbf{Z}$. De tre nämnda idealen genereras med andra ord av talen 3, 0 respektive 1. □

För att visa att en delmängd A till $\mathbf{Z}$ är ett ideal räcker det att verifiera att villkoret (i) i definition 1.6 är uppfyllt, ty vi har följande resultat.

Sats 1.7 *En icke-tom delmängd A till $\mathbf{Z}$ är ett ideal om differensen $x - y$ av två godtyckliga tal x och y i A också ligger i A.*

Bevis. Antag att A är en icke-tom delmängd med egenskapen (i), och låt x_0 vara ett godtyckligt element i A. Eftersom $0 = x_0 - x_0$ noterar vi först att $0 \in A$. Det följer därför sedan att $x \in A \Rightarrow -x = 0 - x \in A$ och att

$$x, y \in A \Rightarrow x, -y \in A \Rightarrow x + y = x - (-y) \in A,$$

dvs. mängden A är sluten under addition.

Antag nu att implikationen $x \in A \Rightarrow nx \in A$ gäller för något icke-negativt heltal n (något som säkert gäller för $n = 0$). Då gäller också att

$$x \in A \Rightarrow (n+1)x = nx + x \in A.$$

Det följer därför med induktion att implikationen $x \in A \Rightarrow nx \in A$ gäller för alla icke-negativa heltal n. Om slutligen $x \in A$ och n är ett negativt heltal, så är talet $-n$ positivt, och det följer först att $(-n)x \in A$ och sedan att $nx = -(-n)x \in A$.

Detta visar att mängden A också har egenskapen (ii) i definition 1.6, och den är därför ett ideal. □

Anmärkning. Begreppet ideal är ett ringbegrepp. En *ring* är en mängd med två operationer, addition och multiplikation, som uppfyller vissa naturliga axiom. Heltalen $\mathbf{Z}$ bildar en ring och ett annat viktigt exempel ges av mängden av alla polynom med vanlig polynomaddition och polynommultiplikation som operationer. För ideal i godtyckliga ringar är emellertid egenskapen (ii) inte en konsekvens av egenskapen (i). Ringen $\mathbf{Z}$ är således speciell i detta avseende.

Idealen i exempel 4 genereras alla av ett enda tal g. Detta är ingen tillfällighet, ty alla ideal i $\mathbf{Z}$ har som vi nu ska visa denna egenskap.

Sats 1.8 *Varje ideal A i $\mathbf{Z}$ genereras av ett unikt icke-negativt tal g, dvs.*

$$A = g\mathbf{Z} = \{ng \mid n \in \mathbf{Z}\}.$$

Om A är skilt från nollidealet $\{0\}$, så är vidare generatorn g det minsta positiva talet i A.

Bevis. Nollidealet genereras av 0, så antag att A innehåller något nollskilt tal x_0. Eftersom A på grund av villkoret (ii) i idealdefinitionen också innehåller talet $-x_0$ $(= (-1)x_0)$, innehåller A säkert positiva tal. Låt g vara det minsta positiva talet i A.

Vi ska visa att idealet A genereras av talet g. Att ng tillhör A för alla heltal n följer omedelbart av villkoret (ii), så vi behöver bara visa att det inte finns några andra tal i A än multipler av g. Antag därför att $b \in A$ och dividera b med g. Enligt divisionsalgoritmen finns det tal q och r med $0 \leq r < g$ så att $b - qg = r$. Eftersom $qg \in A$ följer det av idealegenskapen (i) att $r \in A$, och eftersom g är det minsta positiva talet i A, drar vi slutsatsen att $r = 0$. Följaktligen är $b = qg$, dvs. b är en multipel av g. □

Vi ska nu använda sats 1.8 för att karakterisera största gemensamma delaren till två tal a och b. Betrakta för den skull mängden

$$A = \{ax + by \mid x, y \in \mathbf{Z}\}.$$

Denna mängd är uppenbarligen sluten under subtraktion, dvs. ett ideal, och enligt föregående sats genereras A av ett unikt icke-negativt tal g. Detta tal har per definition följande två egenskaper:

(i) Det finns två heltal x_0, y_0 sådana att $ax_0 + by_0 = g$.

(ii) För alla heltal x och y finns det ett heltal n så att $ax + by = ng$.

Genom att välja $x = 1$ och $y = 0$ i (ii) ser vi att $a = ng$ för något heltal n, vilket betyder att $g \mid a$. Av motsvarande skäl gäller också att $g \mid b$, så g är en gemensam delare till a och b.

Genom att använda (i) ser vi vidare att varje gemensam delare till a och b också är en delare till of g. Speciellt är därför den största gemensamma delaren $d = \text{sgd}(a, b)$ en delare till g, vilket medför att $d \leq g$. Det följer att g är den största gemensamma delaren, dvs. $g = \text{sgd}(a, b)$.

Likheten gäller också i det triviala fallet $a = b = 0$, ty då är A lika med idealet $\{0\}$ som genereras av talet 0, och vi har ju definierat $\text{sgd}(0, 0)$ som 0.

Sammanfattningsvis har vi därmed bevisat följande sats:

Sats 1.9 *Idealet* $\{ax + by \mid x, y \in \mathbf{Z}\}$ *genereras av den största gemensamma delaren* $\text{sgd}(a, b)$*, dvs.*

(i) Det finns heltal x_0 *och* y_0 *sådana att* $ax_0 + by_0 = \text{sgd}(a, b)$*.*

(ii) För alla heltal x *och* y *är* $ax + by$ *en multipel av* $\text{sgd}(a, b)$*.*

Beviset för sats 1.9 generaliseras enkelt så att det fungerar för n heltal $a_1, a_2, \ldots, a_n$ istället för två heltal a och b. Det generella resultatet lyder som följer.

Sats 1.9' *Låt* $a_1, a_2, \ldots, a_n$ *vara godtyckliga heltal. Då genereras idealet*

$$\{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_1, x_2, \ldots, x_n \in \mathbf{Z}\}$$

av den största gemensamma delaren $d = \text{sgd}(a_1, a_2, \ldots, a_n)$*, dvs.*

(i) Det finns heltal $y_1, y_2, \ldots, y_n$ *sådana att* $a_1y_1 + a_2y_2 + \cdots + a_ny_n = d$*.*

(ii) För alla heltal $x_1, x_2, \ldots, x_n$ *är talet* $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ *en multipel av den största gemensamma delaren* d*.*

Vi ska nu angripa problemet att på ett effektivt sätt beräkna största gemensamma delaren till två heltal a och b. Vi kan förstås antaga att båda talen är icke-negativa och att $a \geq b$.

Om $b = 0$ så är $\text{sgd}(a, b) = \text{sgd}(a, 0) = a$, och saken är klar. I motsatt fall utnyttjar vi sats 1.4 enligt vilken $\text{sgd}(a, b) = \text{sgd}(a - nb, b)$ för alla heltal n. Genom att speciellt använda divisionsalgoritmen $a = qb + r$ med $0 \leq r < b$ erhåller vi därför likheten

$$\text{sgd}(a, b) = \text{sgd}(a - qb, b) = \text{sgd}(r, b) = \text{sgd}(b, r). \tag{1}$$

Om $r = 0$, så är vi klara eftersom i så fall $\text{sgd}(a, b) = \text{sgd}(b, 0) = b$. Annars ersätter vi med hjälp av ekvation (1) paret (a, b) med det mindre paret (b, r), där $b \leq a$ och $r < b$, och vi kan nu upprepa hela proceduren. Eftersom vi i varje steg får ett nytt par med mindre heltal måste vi slutligen komma till en punkt där ett av talen är lika med 0.

Hela proceduren kan sammanfattas på följande vis:

Euklides algoritm

Låt a *and* b *vara heltal med* $a \geq b \geq 0$*. Sätt* $a_0 = a$ *och* $b_0 = b$*.*

(i) Om $b_0 = 0$*, så är* $\text{sgd}(a, b) = a_0$*.*

(ii) Använd i annat fall divisionsalgoritmen för att beräkna huvudresten r *då* a_0 *divideras med* b_0*, dvs.* $a_0 = qb_0 + r$ *med* $0 \leq r < b_0$*.*

(iii) Sätt $a_0 = b_0$ *och* $b_0 = r$ *och gå till (i).*

Algoritmen måste stoppa eftersom de successivt erhållna talen b_0 bildar en avtagande följd av icke-negativa heltal.

Istället för att använda huvudresten kan man också i varje steg använda resten med minst absolutbelopp. Detta leder i allmänhet till färre iterationer. Denna variant av algoritmen lyder som följer:

Euklides algoritm med rest med minst belopp

Låt a *och* b *vara heltal med* $a \geq b \geq 0$*. Sätt* $a_0 = a$ *och* $b_0 = b$*.*

(i) Om $b_0 = 0$*, så är* $\text{sgd}(a, b) = a_0$*.*

(ii) Använd i annat fall divisionsalgoritmen för att beräkna resten r *med minst absolutbelopp då* a_0 *divideras med* b_0*, dvs.* $a_0 = qb_0 + r$ *med* $|r| \leq b_0/2$*.*

(iii) Sätt $a_0 = b_0$ och $b_0 = |r|$ och gå till (i).

I steg (iii) utnyttjar vi att $\text{sgd}(a_0, b_0) = \text{sgd}(a_0, -b_0)$, så det spelar ingen roll att vi använder beloppet $|r|$ av resten för att erhålla ett icke-negativt tal b_0. I varje iteration är det nya talet b_0 högst lika med hälften av det gamla, så algoritmen måste stoppa efter ändligt många steg.

EXEMPEL 5 Låt oss beräkna $\text{sgd}(247, 91)$. Den vanliga divisionsalgoritmen ger oss

$$\begin{aligned} 247 &= 2 \cdot 91 + 65 \\ 91 &= 1 \cdot 65 + 26 \\ 65 &= 2 \cdot 26 + 13 \\ 26 &= 2 \cdot 13. \end{aligned}$$

Följaktligen är

$$\text{sgd}(247, 91) = \text{sgd}(91, 65) = \text{sgd}(65, 26) = \text{sgd}(26, 13) = \text{sgd}(13, 0) = 13.$$

Genom att istället använda divisionsalgoritmen med rest med minst absolutbelopp erhålls

$$\begin{aligned} 247 &= 3 \cdot 91 - 26 \\ 91 &= 3 \cdot 26 + 13 \\ 26 &= 2 \cdot 13. \end{aligned}$$

Följaktligen är $\text{sgd}(247, 91) = \text{sgd}(91, 26) = \text{sgd}(26, 13) = \text{sgd}(13, 0) = 13$. □

På grund av sats 1.9 vet vi att den linjära ekvationen

$$ax + by = \text{sgd}(a, b)$$

har minst en heltalslösning x_0 och y_0. (Vi kommer längre fram att se att det faktiskt finns oändligt många heltalslösningar.) Som biprodukt till Euklides algoritm har vi också en algoritm för att hitta en sådan lösning. Låt (a_0, b_0), (a_1, b_1), (a_2, b_2), …, (a_n, b_n) med $a_0 = a$, $b_0 = b$ och $b_n = 0$ beteckna de successiva talpar som erhålls i algoritmen. Om $q_1, q_2, \ldots, q_n$ betecknar de vid divisionerna erhållna kvoterna, så är

$$\begin{aligned} &a_0 = a, \quad b_0 = b \\ &a_i = b_{i-1}, \quad b_i = a_{i-1} - q_i b_{i-1} \quad \text{för } i = 1, 2, \ldots, n \\ &a_n = \text{sgd}(a, b). \end{aligned}$$

Vart och ett av talen a_i och b_i är en linjärkombination av de föregående talen a_{i-1} och b_{i-1} med heltalskoefficienter och följaktligen slutligen en linjärkombination av a och b med heltalskoefficienter, dvs. $a_i = x_i a + y_i b$ för lämpliga heltal x_i, y_i som kan bestämmas genom att räkna ”baklänges”, och motsvarande gäller för b_i. Speciellt gäller då detta för $a_n = \text{sgd}(a, b)$.

EXEMPEL 6 Genom att redovisa beräkningarna i exempel 5 nedifrån och upp och använda varianten med rest med minst belopp ser vi att

$$13 = 91 - 3 \cdot 26 = 91 - 3 \cdot (3 \cdot 91 - 247) = 3 \cdot 247 - 8 \cdot 91.$$

Ekvationen $247x + 91y = 13$ har således heltalslösningen $x = 3$, $y = -8$. □

Vi fortsätter nu med ett antal delbarhetsresultat som följer som konsekvenser av sats 1.9.

Sats 1.10 *Om $c \mid a$ och $c \mid b$, så gäller att $c \mid \mathrm{sgd}(a,b)$, dvs. varje gemensam delare till a och b är också en delare till den största gemensamma delaren* $\mathrm{sgd}(a,b)$.

Bevis. Enligt sats 1.9 finns det heltal x_0, y_0 sådana att $ax_0 + by_0 = \mathrm{sgd}(a,b)$, och slutsatsen i sats 1.10 följer nu av sats 1.2 (iv). □

Sats 1.11 *Låt a och b vara godtyckliga heltal.*
(i) För alla icke-negativa heltal c är $\mathrm{sgd}(ca,cb) = c \cdot \mathrm{sgd}(a,b)$.
(ii) Om $d = \mathrm{sgd}(a,b) \neq 0$, så är $\mathrm{sgd}(a/d, b/d) = 1$.

Bevis. (i) Sätt $d = \mathrm{sgd}(a,b)$. Idealet $\{ax + by \mid x, y \in \mathbf{Z}\}$ genereras av talet d. Eftersom $cax + cby = c(ax + by)$ genereras därför idealet $\{cax + cby \mid x, y \in \mathbf{Z}\}$ av talet cd. Men det sistnämnda idealet genereras också av talet $\mathrm{sgd}(ca,cb)$, och eftersom generatorn är entydigt bestämd drar vi slutsatsen att $\mathrm{sgd}(ca,cb) = cd$.

(ii) Enligt (i) är $d \cdot \mathrm{sgd}(a/d, b/d) = \mathrm{sgd}(a,b) = d$, och påstående (ii) följer nu genom division med d. □

Sats 1.12 *Om* $\mathrm{sgd}(a,b) = 1$ *och $a \mid bc$, så gäller att $a \mid c$.*

Bevis. Antag att $\mathrm{sgd}(a,b) = 1$. Om $a \mid bc$, så är a är en gemensam delare till ac och bc. Men enligt sats 1.11 är $\mathrm{sgd}(ac,bc) = c \cdot \mathrm{sgd}(a,b) = c$, så det följer därför av sats 1.10 att $a \mid c$. □

Sats 1.13 *Om $a \mid c$, $b \mid c$ och* $\mathrm{sgd}(a,b) = 1$*, så gäller att $ab \mid c$.*

Bevis. Antag att $a \mid c$, $b \mid c$ och $\mathrm{sgd}(a,b) = 1$. Då är $c = am$ för något heltal m, och $b \mid am$. Antagandet $\mathrm{sgd}(a,b) = 1$ medför nu på grund av sats 1.12 att $b \mid m$, dvs. $m = bn$ för något heltal n. Följaktligen är $c = abn$, vilket visar att $ab \mid c$. □

Sats 1.14 *Om* $\mathrm{sgd}(a,b) = \mathrm{sgd}(a,c) = 1$*, så är* $\mathrm{sgd}(a,bc) = 1$.

Bevis. Antag att $\mathrm{sgd}(a,b) = \mathrm{sgd}(a,c) = 1$; då finns det på grund av sats 1.9 heltal x, y och z, w sådana att $ax + by = 1$ och $az + cw = 1$. Detta medför att

$$by \cdot cw = (1 - ax)(1 - az) = 1 - ax - az + a^2xz = 1 - an,$$

där $n = x + z - axz$ är ett heltal. Vi har nu likheten $an + bcyw = 1$ med heltal n och yw och som medför att $\mathrm{sgd}(a,bc) = 1$. □

Unionen $I \cup J$ av två ideal $I = a\mathbf{Z}$ och $J = b\mathbf{Z}$ i $\mathbf{Z}$ behöver inte vara ett ideal. Unionen är i själva verket ett ideal om och endast om det ena av de två idealen I och J är en delmängd av det andra, dvs. om och endast om en av de två generatorerna a och b är delbar med den andra. Det finns emellertid alltid ett *minsta ideal* som innehåller unionen $I \cup J$, nämligen idealet

$$\mathrm{sgd}(a,b)\,\mathbf{Z} = \{ax + by \mid x, y \in \mathbf{Z}\}.$$

Det minsta idealet som innehåller de båda idealen $a\mathbf{Z}$ och $b\mathbf{Z}$ genereras med andra ord av den största gemensamma delaren $\mathrm{sgd}(a,b)$.

Å andra sidan följer det direkt ur idealdefinitionen att *snittet* $I \cap J$ av två ideal $I = a\mathbf{Z}$ och $J = b\mathbf{Z}$ är ett ideal. Per definition tillhör vidare ett tal x snittet $I \cap J$ om och endast om x tillhör både I och J, dvs. om och endast om x är en multipel av både talet a och talet b.

Idealet $a\mathbf{Z} \cap b\mathbf{Z}$ är således lika med mängden av alla gemensamma multipler till talen a och b. Denna observation leder oss till följande begrepp som är dualt till begreppet största gemensammma delare.

Definition 1.15 Låt a och b vara två heltal. Den icke-negativa generatorn till idealet $a\mathbf{Z} \cap b\mathbf{Z}$ kallas den *minsta gemensamma multipeln* till de två talen och betecknas $\mathrm{mgm}(a, b)$.

Den minsta gemensamma multipeln $\mathrm{mgm}(a_1, a_2, \ldots, a_n)$ till en godtycklig uppsättning $a_1, a_2, \ldots, a_n$ av heltal definieras på ett analogt sätt som den entydigt bestämda icke-negativa generatorn till idealet $a_1\mathbf{Z} \cap a_2\mathbf{Z} \cap \cdots \cap a_n\mathbf{Z}$.

Notera att $\mathrm{mgm}(a, b) = 0$ om och endast om minst ett av de båda talen a och b är lika med 0, ty snittet $a\mathbf{Z} \cap b\mathbf{Z}$ är lika med det triviala idealet $\{0\}$ endast i detta fall. Om talen a och b båda är skilda från 0 så är $a\mathbf{Z} \cap b\mathbf{Z}$ ett icke-trivialt ideal eftersom det säkert innehåller talet ab. I detta fall finns det således icke-triviala gemensamma multipler och den minsta gemensamma multipeln $\mathrm{mgm}(a, b)$ är ett positivt heltal.

Exempel 7 $\mathrm{mgm}(30, 42)$=210, ty i följden 30, 60, 90, 120, 150, 180, 210, ... av positiva multipler till 30 är talet 210 det första tal som också är en multipel av 42. □

Sats 1.16 *För alla heltal a och b och alla icke-negativa heltal c är*

$$\mathrm{mgm}(ca, cb) = c \cdot \mathrm{mgm}(a, b).$$

Bevis. Likheten är trivialt uppfylld om något av talen a, b och c är lika med noll, ty då är båda sidorna av den lika med noll, så antag att samtliga tre tal är nollskilda. Varje gemensam positiv multipel till talen ca och cb har då formen cm, där m är en gemensam positiv multipel till talen a och b, och den minsta gemensamma multipeln $\mathrm{mgm}(ca, cb)$ till ca och cb fås uppenbarligen genom att välja m som $\mathrm{mgm}(a, b)$, den minsta positiva multipeln till a och b. Detta betyder att $\mathrm{mgm}(ca, cb) = c \cdot \mathrm{mgm}(a, b)$. □

Sats 1.17 *Låt a och b vara icke-negativa heltal. Då är*

$$\mathrm{mgm}(a, b) \cdot \mathrm{sgd}(a, b) = ab.$$

Bevis. Om ett av de två talen är lika med noll, så är $\mathrm{mgm}(a, b) = ab = 0$, så vi kan antaga att a och b båda är positiva. Sätt $d = \mathrm{sgd}(a, b)$. Om $d = 1$, så måste på grund av sats 1.13 varje gemensam multipel till a och b också vara en multipel till ab, och det följer härav att ab är den minsta gemensamma multipeln till a och b, dvs.

$$ab = \mathrm{mgm}(a, b) = \mathrm{mgm}(a, b) \cdot \mathrm{sgd}(a, b).$$

Om $d > 1$, så är $\mathrm{sgd}(a/d, b/d) = 1$, och enligt det just bevisade specialfallet är

$$\mathrm{mgm}(a/d, b/d) = a/d \cdot b/d.$$

Multiplicera nu denna likhet med d^2 och använd sats 1.16; detta resulterar i likheten

$$ab = d^2 \cdot \operatorname{mgm}(a/d, b/d) = d \cdot \operatorname{mgm}(a, b) = \operatorname{sgd}(a, b) \cdot \operatorname{mgm}(a, b). \qquad \square$$

Övningar

1.1 Skriv för talet 10 upp samtliga
a) delare, b) positiva delare, c) icke-triviala delare.

1.2 Bestäm det största icke-negativa heltalet n för vilket
a) $2^n \mid 360$, b) $3^n \mid 360$, c) $5^n \mid 360$, d) $7^n \mid 360$.

1.3 Hur många tal mellan 100 och 1000 är delbara med 6?

1.4 Bestäm a) $\operatorname{sgd}(10, 14)$, b) $\operatorname{sgd}(-10, 14)$, c) $\operatorname{sgd}(-10, -14)$.

1.5 Är talen 10, 14 och 35 a) relativt prima, b) parvis relativt prima?

1.6 Skriv upp divisionsalgoritmen (med huvudrest) för division av
a) 25 med 7, b) -25 med 7.

1.7 Skriv upp divisionsalgoritmen med till beloppet minsta rest för division av a) 25 med 7, b) 28 med 8.

1.8 Bestäm med hjälp av Euklides algoritm största gemensamma delaren till
a) 512 och 299, b) 1079 och 611, c) 5041 och 2769.

1.9 Bestäm a) $\operatorname{mgm}(84, 360)$, b) $\operatorname{mgm}(10, 12, 15)$, c) $\operatorname{mgm}(n, n+1)$, $n \geq 1$, d) $\operatorname{mgm}(2^n + 1, 2^n - 1)$, $n \geq 1$.

1.10 För vilka positiva heltal a och b med $a \geq b$ är $\operatorname{mgm}(a, b) = 10$?

1.11 Visa att för varje udda tal n är $n^2 - 1$ delbart med 8.

1.12 Visa att inget kvadrattal är av formen $4n + 2$ eller $4n + 3$.

1.13 Visa att produkten av
a) två konsekutiva heltal är delbar med 2,
b) tre konsekutiva heltal är delbar med 6,
c) fyra konsekutiva heltal är delbar med 24,
d) k konsekutiva heltal är delbar med $k!$.

1.14 Visa att för alla heltal $n \geq 2$ och $k \geq 1$ gäller att
a) $(n-1) \mid (n^k - 1)$, b) $(n-1)^2 \mid (n^k - 1)$ om och endast om $(n-1) \mid k$.

1.15 Visa att om $ad - bc = \pm 1$, så är $\operatorname{sgd}(a+b, c+d) = 1$. Gäller omvändningen?

1.16 Visa att för alla positiva heltal a, m och n med $m \neq n$ är

$$\operatorname{sgd}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{om } a \text{ är jämnt,} \\ 2 & \text{om } a \text{ är udda.} \end{cases}$$

1.17 Visa att om $a \geq 2$ och m, $n \geq 1$, så är $\operatorname{sgd}(a^m - 1, a^n - 1) = a^{\operatorname{sgd}(m,n)} - 1$.

1.18 Låt c vara ett heltal ≥ 2. Visa att varje heltal $n \geq 1$ entydigt kan skrivas

$$n = a_r c^r + a_{r-1} c^{r-1} + \cdots + a_1 c + a_0,$$

där $r \geq 0$, $a_r > 0$ och $0 \leq a_i \leq c - 1$ för $i = 0, 1, \ldots, r$.

2 Primtal

Definition 2.1 Ett heltal > 1 kallas *primtal* om det bara har triviala delare. Ett heltal $p > 1$ är med andra ord ett primtal om och endast om

$$1 < x < p \Rightarrow x \nmid p.$$

Ett heltal > 1 som inte är ett primtal kallas *sammansatt*.

Sats 2.2 *Låt b och c vara heltal och låt p vara ett primtal. Om p är en delare till bc, så är p en delare till b eller till c.*

Bevis. Antag att $p \mid bc$. Om $p \nmid b$, så är $\text{sgd}(p, b) = 1$ beroende på att p bara har triviala delare, och sats 1.12 medför därför att $p \mid c$. □

Sats 2.2 har följande generalisering till fler än två faktorer:

Sats 2.2' *Låt p vara ett primtal. Om $p \mid b_1 b_2 \cdots b_n$, så gäller att $p \mid b_i$ för något index i.*

Bevis. Sats 2.2 tillämpad på talen $b = b_1$ och $c = b_2 \cdots b_n$ ger oss implikationen $p \mid b_1 b_2 \cdots b_n \Rightarrow p \mid b_1 \vee p \mid b_2 \ldots b_n$. Satsens påstående följer därför med induktion. □

Sats 2.3 (Aritmetikens fundamentalsats) *Varje heltal $n > 1$ kan skrivas som en produkt av primtal på ett entydigt sätt bortsett från primfaktorernas ordning.*

Bevis. Existensen av en sådan faktorisering visas med induktion. Antag att $n > 1$ och att varje tal mindre än n kan skrivas som en produkt av primtal. Om n är ett primtal, så har vi en faktorisering av n bestående av en primtalsfaktor. Om n istället är ett sammansatt tal, så är $n = n_1 n_2$ med $1 < n_1 < n$ and $1 < n_2 < n$, och det följer av induktionsantagandet att vart och ett av talen n_1 och n_2 är en produkt av primtal. Därför är också n en produkt av primtal.

Antag nu att det finns ett heltal > 1 med två olika faktoriseringar. Då finns det ett minsta sådant tal n. Låt $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ vara två olika faktoriseringar i primtal p_i och q_j. Eftersom p_1 är en delare till n, är p_1 en delare till produkten $q_1 q_2 \cdots q_s$, och det följer därför av sats 2.2′ att p_1 delar något av primtalen $q_1, \ldots, q_s$. Genom att numrera om dessa tal kan vi antaga att $p_1 \mid q_1$, vilket naturligtvis innebär att $p_1 = q_1$. Genom att dividera n med p_1 får vi nu ett mindre tal

$$\frac{n}{p_1} = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

än n med två olika primtalsfaktoriseringar, något som strider mot antagandet att n är det minsta talet med olika primtalsfaktoriseringar. Denna motsägelse visar att primtalsfaktoriseringen är unik. □

Om två givna tals primtalsfaktoriseringar är kända, så kan vi lätt bestämma talens största gemensamma delare och minsta gemensamma multipel.

Sats 2.4 *Låt a och b vara två positiva heltal och antag att*

$$a = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \quad \textit{och} \quad b = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$

där $p_1, p_2, \ldots, p_k$ är olika primtal samt m_1, m_2, …, m_k och $n_1, n_2, \ldots, n_k$ är icke-negativa heltal. Sätt $d_j = \min(m_j, n_j)$ och $D_j = \max(m_j, n_j)$; då är

$$\operatorname{sgd}(a,b) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \quad \textit{och} \quad \operatorname{mgm}(a,b) = p_1^{D_1} p_2^{D_2} \cdots p_k^{D_k}.$$

Bevis. Uppenbart. □

Med satserna 2.3 och 2.4 i ryggen är det lätt att ge nya enkla bevis för satserna 1.10–1.17 i förra avsnittet om delbarhet, största gemensamma delare och minsta gemensamma multipel, och läsaren uppmanas att göra detta som övning.

Sats 2.5 *Det finns oändligt många primtal*

Bevis. Vi ska visa att det för varje given uppsättning $p_1, p_2, \ldots, p_n$ av primtal finns ett primtal q som inte tillhör uppsättningen; detta innebär förstås att antalet primtal inte kan vara ändligt. Sätt för den skull

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

Enligt sats 2.3 har N en primfaktor q (som skulle kunna vara talet N självt). Eftersom $\operatorname{sgd}(N, p_j) = \operatorname{sgd}(1, p_j) = 1$ för $j = 1, 2, \ldots, n$, medan $\operatorname{sgd}(N, q) = q$, följer det att $q \neq p_j$ för alla j. □

Å andra sidan innehåller, som följande sats visar, följden av primtal godtyckligt stora luckor.

Sats 2.6 *För varje heltal k finns det k stycken sammansatta tal i följd.*

Bevis. Betrakta talen $(k+1)! + 2$, $(k+1)! + 3$, …, $(k+1)! + (k+1)$; de är samtliga sammansatta eftersom de är delbara med respektive $2, 3, \ldots, k+1$. □

Vi ska nu ge en grov uppskattning av antalet primtal i ett godtyckligt intervall $[0, N]$. Låt för den skull $\pi(x)$ beteckna antalet primtal som är mindre än eller lika med det reella talet x så att

$$\pi(x) = \begin{cases} 0 & \text{om } x < 2, \\ 1 & \text{om } 2 \le x < 3, \\ 2 & \text{om } 3 \le x < 5, \\ \vdots & \\ n & \text{om } p_n \le x < p_{n+1}, \\ \text{osv.} & \end{cases}$$

där p_n betecknar det n:te primtalet i följd.

Vi behöver följande olikhet.

Lemma 2.7 *Låt x vara ett reellt tal > 2. Då är*

$$\sum_{p \le x} \frac{1}{p} > \ln \ln x - 1.$$

Här ska summeringen ske över alla primtal p som är $\le x$.

Anmärkning. Eftersom $\ln\ln x$ går mot ∞ med x, följer det av olikheten i lemmat att summan $\sum 1/p$ över alla primtal är oändlig, och detta medför förstås att antalet primtal är oändligt. Beviset för lemma 2.7 ger oss med andra ord ett alternativt bevis för sats 2.5.

Bevis. Låt $p_1, p_2, \ldots, p_n$ beteckna alla primtal som är $\leq x$, och sätt

$$\mathcal{N} = \{p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \mid k_1 \geq 0, k_2 \geq 0, \ldots, k_n \geq 0\}.$$

Detta innebär att mängden $\mathcal{N}$ består av talet 1 och alla positiva tal som har en primtalsfaktorisering som inte innehåller några andra primtal än de n första primtalen $p_1, p_2, \ldots, p_n$.

Eftersom faktoriseringen av varje positivt heltal som är mindre än eller lika med x bara använder primtal som är $\leq x$, innehåller mängden $\mathcal{N}$ vart och ett av talen 1, 2, 3, ..., $\lfloor x \rfloor$ (= heltalsdelen av x). Följaktligen är

$$\sum_{n\in\mathcal{N}} \frac{1}{n} \geq \sum_{n=1}^{\lfloor x\rfloor} \frac{1}{n} \geq \int_1^{\lfloor x\rfloor+1} \frac{dt}{t} = \ln(\lfloor x\rfloor + 1) > \ln x.$$

Observera nu att

$$\prod_{p\leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p\leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^k} + \cdots\right) = \sum_{n\in\mathcal{N}} \frac{1}{n}.$$

Genom att kombinera denna identitet med föregående olikhet erhåller vi den nya olikheten

$$\prod_{p\leq x} \left(1 - \frac{1}{p}\right)^{-1} > \ln x,$$

och genom att logaritmera båda leden också olikheten

$$\sum_{p\leq x} \ln\left(1 - \frac{1}{p}\right)^{-1} > \ln\ln x. \tag{1}$$

Nu använder vi Maclaurinutvecklingen av $\ln(1+x)$ för att för $0 \leq x < 1$ erhålla olikheten

$$-\ln(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \leq x + \frac{x^2}{2}(1 + x + x^2 + \ldots) = x + \frac{x^2}{2} \cdot \frac{1}{1-x}.$$

Eftersom $1/(1-x) \leq 2$ då $x \leq \frac{1}{2}$, drar vi slutsatsen att olikheten

$$\ln(1-x)^{-1} = -\ln(1-x) \leq x + x^2$$

gäller för $0 \leq x \leq \frac{1}{2}$.

Om p är ett primtal, så är förstås $0 \leq \frac{1}{p} \leq \frac{1}{2}$, och därför är följaktligen

$$\ln(1 - \frac{1}{p})^{-1} \leq \frac{1}{p} + \frac{1}{p^2}.$$

Genom att summera dessa olikheter för alla primtal $p \leq x$ och jämföra med olikheten (1), erhåller vi olikheten

$$\sum_{p\leq x} \frac{1}{p} + \sum_{p\leq x} \frac{1}{p^2} > \ln\ln x. \tag{2}$$

Här kan summan $\sum 1/p^2$ över alla primtal $\leq x$ uppskattas på följande vis:

$$\sum_{p\leq x}\frac{1}{p^2}\leq\sum_{n=2}^{\infty}\frac{1}{n^2}\leq\sum_{n=2}^{\infty}\frac{1}{n(n-1)}=\sum_{n=2}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)=1,$$

och genom att kombinera denna olikhet med olikheten (2) erhåller vi slutligen det eftersökta resultatet

$$\sum_{p\leq x}\frac{1}{p}>\ln\ln x-1.$$

□

Lemma 2.8 *För alla reella tal x gäller likheten*

$$\sum_{p\leq x}\frac{1}{p}=\frac{\pi(x)}{x}+\int_2^x\frac{\pi(u)}{u^2}\,du.$$

Bevis. Likheten är trivialt sann för $x<2$, så antag att $x\geq 2$ och låt $p_1<p_2<\cdots<p_n$ beteckna primtalen $\leq x$. Då är

$$\begin{aligned}\int_2^x\frac{\pi(u)}{u^2}\,du&=\sum_{k=1}^{n-1}\int_{p_k}^{p_{k+1}}\frac{\pi(u)}{u^2}\,du+\int_{p_n}^{x}\frac{\pi(u)}{u^2}\,du\\&=\sum_{k=1}^{n-1}\int_{p_k}^{p_{k+1}}\frac{k}{u^2}\,du+\int_{p_n}^{x}\frac{n}{u^2}\,du\\&=\sum_{k=1}^{n-1}k\left(\frac{1}{p_k}-\frac{1}{p_{k+1}}\right)+n\left(\frac{1}{p_n}-\frac{1}{x}\right)\\&=\sum_{k=1}^{n-1}\frac{k}{p_k}-\sum_{k=2}^{n}\frac{k-1}{p_k}+\frac{n}{p_n}-\frac{n}{x}\\&=\sum_{k=1}^{n}\frac{1}{p_k}-\frac{\pi(x)}{x}.\end{aligned}$$

□

Sats 2.9 *För varje $\epsilon>0$ och varje reellt tal ω finns det ett reellt tal $x>\omega$ sådant att*

$$\pi(x)>(1-\epsilon)\frac{x}{\ln x}.$$

Anmärkning. För den som är bekant med begreppet övre limes kan vi formulera påståendet i satsen på följande enkla vis: $\limsup_{x\to\infty}\frac{\pi(x)}{x/\ln x}\geq 1$.

Bevis. Antag att satsen är falsk. Då finns det ett $\epsilon>0$ och ett ω så att olikheten $\pi(x)\leq(1-\epsilon)x/\ln x$ gäller för alla $x>\omega$. Men för $x>\omega$ är i så fall

$$\begin{aligned}\int_2^x\frac{\pi(u)}{u^2}\,du&=\int_2^{\omega}\frac{\pi(u)}{u^2}\,du+\int_{\omega}^{x}\frac{\pi(u)}{u^2}\,du\leq C+(1-\epsilon)\int_{\omega}^{x}\frac{1}{u\ln u}\,du\\&=C+(1-\epsilon)(\ln\ln x-\ln\ln\omega)=D+(1-\epsilon)\ln\ln x,\end{aligned}$$

där C och D är konstanter (som beror av ω). Eftersom $\pi(x)<x$, följer det nu av lemma 2.8 att

$$\sum_{p\leq x}\frac{1}{p}\leq(1-\epsilon)\ln\ln x+\text{Konstant}.$$

Detta strider mot lemma 2.7. □

Sats 2.9 kan skärpas avsevärt. Följande resultat, först formulerat som en förmodan av Gauss, bevisades 1896 av J. Hadamard och Ch. de la Vallée Poussin med hjälp av avancerade funktionsteoretiska metoder.

Sats 2.10 (Primtalssatsen)

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Beviset för primtalssatsen är alltför komplicerat för att ges här.

Det följer förstås av primtalssatsen att $\pi(x)/x < C/\ln x$ för alla x och någon konstant C. Kvoten $\pi(x)/x$ går således mot 0 och kvoten $(x-\pi(x))/x$ går mot 1 då x går mot oändligheten. För positiva heltal n är $n-\pi(n)$ lika med antalet icke-primtal i intervallet $[1,n]$, och kvoten $(n-\pi(n))/n$ representerar följaktligen andelen icke-primtal bland de n första postiva heltalen. Att denna kvot går mot 1 betyder att i viss mening är "nästan alla" positiva heltal sammansatta.

Å andra sidan är primtalen inte särskilt sällsynta, ty logaritmfunktionen växer mycket långsamt. Enligt primtalssatsen kan vi använda $x/\ln x$ som en approximation till $\pi(x)$. Om x är ett stort tal och y är litet jämfört med x, så är $\ln(x+y) \approx \ln x$ och följaktligen

$$\pi(x+y) - \pi(x) \approx \frac{x+y}{\ln(x+y)} - \frac{x}{\ln x} \approx \frac{y}{\ln x}.$$

Detta betyder att det mellan x och $x+y$ finns approximativt $y/\ln x$ stycken primtal. Vi kan således förvänta oss att hitta ett primtal i intervallet om intervallets längd är $\ln x$. Om primtalen vore helt slumpmässigt fördelade skulle sannolikheten för ett tal i intervallet att vara primtal således vara ungefär $1/\ln x$. För exempelvis $x = 10^{100}$ är $\ln x \approx 230$, så om vi väljer ett heltal N "slumpmässigt" i en omgivning av 10^{100} är sannolikheten att talet N är ett primtal i runda slängar $1/230$. Vi kan förstås öka denna sannolikhet till det dubbla genom att undvika de jämna heltalen, och om vi ser till att talet N inte är delbart med 2, 3 eller 5, ökar sannolikheten att N är primtal till cirka $1/60$. Förutsatt att vi har tillgång till någon effektiv metod för att avgöra huruvida ett tal är primtal eller sammansatt (och sådana metoder finns!) kan vi således producera ett mycket stort primtal genom att först välja talet N på måfå men inte delbart med by 2, 3 eller 5 (och några andra små primtal) och sedan utföra ett primtalstest på N. Om testet visar att N är primtal, så är vi glada, annars betraktar vi nästa tal i följden $N+2$, $N+4$, $N+6$, ... som inte är delbart med 3 och 5 (och de andra valda små primtalen) och testar om detta är ett primtal. På grund av primtalssatsen kan vi känna oss tämligen säkra på att hitta ett primtal efter inte alltför många försök.

Övningar

2.1 Bestäm primtalsfaktoriseringen av talen
a) 360, b) 271, c) 2981, d) 10^{20}, e) 10!.

2.2 Visa att n är en heltalskvadrat om och endast om varje exponent a_i är jämn i den kanoniska primtalsfaktoriseringen $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$.

2.3 a och b är relativt prima positiva heltal. Visa att om ab är en heltalskvadrat så är a och b också det.

2.4 Visa att varje heltal $n \geq 2$ har en minsta delare $d \geq 2$. Visa att d är ett primtal, och att $d \leq \sqrt{n}$ såvida inte n självt är ett primtal.

2.5 Visa att inte för något $n \geq 2$ är $n^4 + 4$ ett primtal.

2.6 Ett primtal (skrivet som decimaltal) har alla siffror lika med 1. Visa att antalet ettor är ett primtal.

2.7 Visa att talet $1 + 1/2 + 1/3 + \cdots + 1/n$ inte är ett heltal för något $n \geq 1$.

2.8 Låt $\lfloor x \rfloor$ beteckna heltalsdelen av det reella talet x, dvs. det unika heltal som uppfyller olikheten $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Visa att
a) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$,
b) $\lfloor \lfloor x \rfloor / m \rfloor = \lfloor x/m \rfloor$, om m är ett positivt heltal.

2.9 Låt p vara ett primtal. Visa att den största potens p^k som delar $n!$ fås för $k = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$.

2.10 Bestäm den största potensen av 15 som delar 60!.

2.11 Hur många nollor slutar talet 169! på när det skrivs ut på decimalform?

2.12 Visa att binomialkoefficienterna $\dfrac{n!}{k!(n-k)!}$ är heltal genom att visa att varje primtalsfaktor i nämnaren förekommer som faktor i täljaren minst lika många gånger som i nämnaren.

2.13 Visa att varje positivt heltal på formen $4k + 3$ har en primtalsfaktor av samma form.

2.14 Visa att det finns oändligt många primtal som har formen $4k + 3$.

3 Den linjära diofantiska ekvationen ax+by=c

Låt a, b och c vara heltal och betrakta ekvationen

$$ax + by = c. \tag{1}$$

Vi är enbart intresserade av heltalslösningar x och y.

Från avsnitt 1 vet vi redan en hel del om ekvationen. Enligt sats 1.9 består mängden $\{ax + by \mid x, y \in \mathbf{Z}\}$ av alla multiplar $n \cdot \text{sgd}(a, b)$ av den största gemensamma delaren till talen a och b. Detta innebär att ekvation (1) har heltalslösningar om och endast om $\text{sgd}(a, b) \mid c$. Euklides algoritm ger oss vidare en metod att hitta en heltalslösning x_0, y_0 till ekvationen $ax + by = \text{sgd}(a, b)$, och genom att multiplicera denna lösning med $c/\text{sgd}(a, b)$ erhåller vi en lösning till ekvation (1). Det återstår således endast att hitta den allmänna lösningen när man känner en speciell lösning, och nästa sats visar hur det går till.

Sats 3.1 *(i) Ekvationen $ax+by = c$ har heltalslösningar om och endast om c är en multipel av den största gemensamma delaren $d = \text{sgd}(a, b)$ till koefficienterna a och b.*

(ii) Om ekvationen har en heltalslösning x_0, y_0, så har den oändligt många heltalslösningar, och alla andra heltalslösningar formen

$$x = x_0 + \frac{b}{d}\,n, \quad y = y_0 - \frac{a}{d}\,n, \quad n \in \mathbf{Z}.$$

Bevis. Påstående (i) har vi redan visat, och man verifierar lätt att heltalen x och y i påstående (ii) satisfierar ekvationen $ax + by = c$ för alla heltal n om x_0, y_0 är en heltalslösning. För att visa att de är de enda lösningarna antar vi att x, y är en godtycklig heltalslösning. Då är $ax + by = ax_0 + by_0$, varav följer att $a(x - x_0) = b(y_0 - y)$ och att

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{2}$$

Eftersom $\text{sgd}(a/d, b/d) = 1$, följer det nu av ekvation (2) och sats 1.12 att b/d är en delare till $x - x_0$, dvs. det finns ett heltal n så att $x - x_0 = bn/d$. Genom att sätta in detta i ekvation (2) och förenkla får vi också likheten $y - y_0 = -an/d$. Detta visar att den allmänna lösningen har den angivna formen. □

Fallet $\text{sgd}(a, b) = 1$ är så viktigt att det är värt en separat formulering

Korollarium 3.2 *Antag att talen a och b är relativt prima. Då har den linjära ekvationen*

$$ax + by = c$$

heltalslösningar för alla heltal c. Om x_0, y_0 är en lösning, så ges alla lösningar av att

$$x = x_0 + bn, \quad y = y_0 - an, \quad n \in \mathbf{Z}.$$

Det följer av sats 3.1 att avståndet mellan två konsekutiva x-lösningar till en lösbar ekvation $ax + by = c$ är lika med b/d och att avståndet mellan två konsekutiva y-lösningar är lika med a/d, där $d = \text{sgd}(a, b)$. Om ekvationen är lösbar, så finns det därför en lösning (x, y) med $0 \leq x \leq b/d - 1$. Vi kan hitta denna lösning genom att lösa ekvationen med avseende på y för $x = 0$, $x = 1$, $x = 2$, osv. till dess att vi träffar på ett y med heltalsvärde. Naturligtvis kan vi också lösa ekvationen genom att söka efter en heltalslösning med y i intervallet $0 \leq y \leq a/d - 1$. Om åtminstone ett av de båda talen a/d och b/d är litet, så kan vi således enkelt lösa ekvationen $ax + by = c$ genom trial-and-error-metoden.

Exempel 1 Lös ekvationen

$$247x + 91y = 39.$$

Lösning 1: Ekvationen är lösbar eftersom $\text{sgd}(247, 91) = 13$ och $13 \mid 39$. Eftersom $91/13 = 7$ har ekvationen en heltalslösning (x, y) med $0 \leq x \leq 6$. Genom att i tur och ordning pröva $x = 0$, 1, 2, finner vi att $x = 2$ ger ett heltalsvärde $y = -5$. Den allmänna lösningen till ekvationen är således $x = 2 + 7n$, $y = -5 - 19n$.

Lösning 2: I exempel 6 i avsnitt 1 fann vi att $x = 3$, $y = -8$ löser ekvationen $247x + 91y = 13$, och genom att multiplicera denna lösning med 3 erhåller vi partikulärlösningen $x_0 = 9$, $y_0 = -24$ till vår givna ekvation. Den allmänna lösningen är därför $x = 9 + 7n$, $y = -24 - 19n$. Denna parametrisering av lösningarna skiljer sig från den i lösning nr 1, men de båda lösningsmängderna är förstås lika.

Lösning 3: Lösning nr 2 använder Euklides algoritm, och den metod som vi nu ska presentera är ekvivalent med Euklides algoritm, men själva framställningen är lite annorlunda. För att lösa ekvationen

$$247x + 91y = 39 \tag{3}$$

börjar vi med att dividera 247 med 91 med $247 = 2 \cdot 91 + 65$ som resultat. Följaktligen är $247x = 91 \cdot 2x + 65x$ och $247x + 91y = 65x + 91(2x + y)$. Genom att introducera de nya heltalsvariablerna $x_1 = x$, $y_1 = 2x + y$ kan vi därför skriva om ekvation (3) på formen

$$65x_1 + 91y_1 = 39, \tag{4}$$

och denna ekvation har mindre koefficienter än den ursprungliga. Notera vidare att om x_1 och y_1 är heltal, så är också $x = x_1$ och $y = y_1 - 2x$ heltal. Att bestämma heltalslösningarna till ekvation (4) är därför ekvivalent med att bestämma heltalslösningarna till ekvation (3)

Vi kan nu upprepa samma manöver. Vi dividerar 91 med 65 med $91 = 65+26$ som resultat och skriver sedan $65x_1 + 91y_1 = 65(x_1 + y_1) + 26y_1$ för att kunna ersätta ekvation (4) med den ekvivalenta ekvationen

$$65x_2 + 26y_2 = 39, \qquad \text{där } x_2 = x_1 + y_1,\ y_2 = y_1. \tag{5}$$

Vi fortsätter på den inslagna vägen genom att notera att $65 = 2 \cdot 26 + 13$ och erhåller ekvationen

$$13x_3 + 26y_3 = 39, \qquad \text{där } x_3 = x_2,\ y_3 = 2x_2 + y_2. \tag{6}$$

Nu är $26 = 2 \cdot 13$ varför

$$13x_4 + 0y_4 = 39, \qquad \text{där } x_4 = x_3 + 2y_3,\ y_4 = y_3. \tag{7}$$

Från ekvation (7) drar vi slutsatsen att $x_4 = 39/13 = 3$ medan y_4 får vara ett godtyckligt heltal som vi kallar n. Genom att sedan arbeta oss bakåt får vi i tur och ordning

$$\begin{aligned}
&y_3 = y_4 = n, \quad x_3 = x_4 - 2y_3 = 3 - 2n \\
&x_2 = x_3 = 3 - 2n, \quad y_2 = y_3 - 2x_2 = n - 2(3 - 2n) = -6 + 5n \\
&y_1 = y_2 = -6 + 5n, \quad x_1 = x_2 - y_1 = 3 - 2n + 6 - 5n = 9 - 7n \\
&x = x_1 = 9 - 7n, \quad y = y_1 - 2x = -6 + 5n - 2(9 - 7n) = -24 + 19n. \qquad \square
\end{aligned}$$

För linjära ekvationer med fler än två variabler har vi följande resultat som följer omedelbart av sats 1.9′.

Sats 3.3 *Den linjära ekvationen $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ med heltalskoefficienter har heltalslösningar om och endast om* $\operatorname{sgd}(a_1, a_2, \ldots, a_n) \mid c$.

Det är lätt att anpassa den tredje lösningsmetoden i exempel 1 så att den tar hand om ekvationer med fler än två variabler.

Exempel 2 Bestäm heltalslösningarna till ekvationen

$$6x + 10y + 15z = 5.$$

Lösning: Ekvationen har heltalslösningar eftersom $\operatorname{sgd}(6, 10, 15) = 1$. Vi utgår från den minsta koefficienten 6 i vänsterledet och skriver de övriga två koefficienterna på formen $10 = 6+4$ och $15 = 2 \cdot 6+3$. Med nya variabler $x_1 = x+y+2z$, $y_1 = y$ och $z_1 = z$ kan vi nu skriva om vår linjära ekvation så att den får formen

$$6x_1 + 4y_1 + 3z_1 = 5.$$

Eftersom $6 = 2 \cdot 3$ och $4 = 3 + 1$, sätter vi nu $x_2 = x_1$, $y_2 = y_1$ och $z_2 = 2x_1 + y_1 + z_1$. Detta variabelbyte transformerar ekvationen till

$$0x_2 + y_2 + 3z_2 = 5.$$

Nu är 1 den minsta nollskilda koefficienten och vi sätter $x_3 = x_2$, $y_3 = y_2 + 3z_2$ och $z_3 = z_2$. Ekvationen får nu formen

$$0x_3 + y_3 + 0z_3 = 5$$

och har heltalslösningarna $x_3 = m$, $y_3 = 5$ och $z_3 = n$, där m och n är godtyckliga heltal. Genom att arbeta oss bakåt får vi sedan efter några enkla räkningar:

$$x = 5 + 5m - 5n, \quad y = 5 - 3n, \quad z = -5 - 2m + 4n, \quad m, n \in \mathbf{Z}. \qquad \square$$

Övningar

3.1 Bestäm samtliga heltalslösningar till följande ekvationer:
a) $3x + 2y = 1$, b) $3x - 2y = 1$, c) $6x + 4y = 2$, d) $3x + 2y = 2$,
e) $3x + 2y = 101$.

3.2 Bestäm samtliga heltalslösningar till ekvationerna
a) $17x - 43y = 100$, b) $12x + 34y = 1234$, c) $101x + 102y = 103$,
d) $110x - 174y = 18$.

3.3 Hur många lösningar har ekvationen $51x + 21y = 5121$ med positiva heltal x, y?

3.4 Bestäm heltalslösningarna till ekvationerna
a) $x + 2y + 3z = 4$, b) $2x + 3y + 4z = 5$, c) $7x - 11y + 23z = 100$,
d) $5x + 7y + 10z + 13w = 1$.

3.5 Bestäm alla heltalslösningar till systemet

$$\begin{cases} 7x + 3y + 19z = 1500 \\ 8x + 6y + 33z = 2000. \end{cases}$$

3.6 I den här övningen beskrivs hur man bestämmer heltalslösningar till ekvationen

$$ax + by = \text{sgd}(a, b)$$

med hjälp av Euklides algoritm och rekursionsformler.
Sätt $r_{-1} = a$, $r_0 = b$, och låt $q_1, q_2, \ldots, q_k$ och $r_1, r_2, \ldots, r_k = \text{sgd}(a, b)$ vara de successiva kvoter och rester som erhålles i Euklides algoritm, dvs.

$$r_{i-2} = q_i r_{i-1} + r_i, \qquad \text{för } i = 1, 2, \ldots, k.$$

Definiera följderna x_{-1}, x_0, x_1, x_2, $\ldots$, x_k och y_{-1}, y_0, y_1, y_2, $\ldots$, y_k rekursivt genom att sätta $x_{-1} = 1$, $x_0 = 0$, $y_{-1} = 0$, $y_0 = 1$ samt

$$x_{i+1} = x_{i-1} - x_i q_{i+1} \quad \text{och} \quad y_{i+1} = y_{i-1} - y_i q_{i+1} \quad \text{för } 0 \le i \le k - 1.$$

Visa att

$$ax_i + by_i = r_i \qquad \text{för } -1 \le i \le k.$$

3.7 Låt a, b och c vara positiva heltal och antag att $\text{sgd}(a,b) = 1$. Visa att den diofantiska ekvationen $ax + by = c$
a) har en lösning i positiva heltal om $ab < c$,
b) saknar lösning i positiva heltal om $a + b > c$.

3.8 Låt a, b och c vara positiva heltal och antag att $\text{sgd}(a,b) = 1$. Vi söker icke-negativa heltalslösningar, dvs. lösningar i heltal $x \geq 0$, $y \geq 0$, till ekvationen $ax + by = c$.
a) Visa att det alltid finns en icke-negativ lösning om $c \geq (a-1)(b-1)$.
b) Visa att det inte finns någon icke-negativ lösning om $c = ab - a - b$.

4 Kongruenser

Definition 4.1 Låt m vara ett positivt heltal. Om $m \mid (a-b)$ säger vi att talet a är *kongruent* med talet b *modulo* m och skriver $a \equiv b \pmod{m}$. Om $m \nmid (a-b)$ är a inte kongruent med b modulo m, och vi skriver $a \not\equiv b \pmod{m}$.

Uppenbarligen är påståendet $a \equiv b \pmod{m}$ ekvivalent med att $a = qm + b$ för något heltal q. Mängden av alla med a kongruenta tal b modulo m är därför identisk med mängden av alla rester som kan fås genom att dividera a med modulen m.

Vi listar nu några användbara egenskaper som följer direkt ur definitionen av kongruens.

Sats 4.2 *Kongruens modulo m är en ekvivalensrelation, dvs.*
(i) $a \equiv a \pmod{m}$ *för alla heltal* a.
(ii) Om $a \equiv b \pmod{m}$, *så är* $b \equiv a \pmod{m}$.
(iii) Om $a \equiv b \pmod{m}$ *och* $b \equiv c \pmod{m}$, *så är* $a \equiv c \pmod{m}$.

Bevis. Beviset för satsen lämnas åt läsaren. □

Nästa sats visar att kongruenser kan adderas, multipliceras och höjas till potenser.

Sats 4.3 *Låt a, b, c och d vara heltal.*
(i) Om $a \equiv b \pmod{m}$ *och* $c \equiv d \pmod{m}$, *så är* $a + c \equiv b + d \pmod{m}$.
(ii) Om $a \equiv b \pmod{m}$ *och* $c \equiv d \pmod{m}$, *så är* $ac \equiv bd \pmod{m}$.
(iii) Om $a \equiv b \pmod{m}$, *så är* $a^k \equiv b^k \pmod{m}$ *för alla icke-negativa heltal* k.
(iv) Låt $f(x)$ *vara ett polynom i variabeln* x *med heltalskoefficienter och antag att* $a \equiv b \pmod{m}$. *Då är* $f(a) \equiv f(b) \pmod{m}$.

Bevis. (i) lämnas åt läsaren.

(ii) Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $a = b + mq$ och $c = d + mr$ för lämpliga heltal q och r. Det följer att $ac = bd + m(br + dq + mqr)$, vilket visar att $ac \equiv bd \pmod{m}$.

(iii) Genom att välja $c = a$ och $d = b$ i (ii) ser vi att antagandet $a \equiv b \pmod{m}$ medför att $a^2 \equiv b^2 \pmod{m}$. Genom att använda egenskapen (ii) ytterligare en gång får vi kongruensen $a^3 \equiv b^3 \pmod{m}$, och det allmänna fallet följer med induktion.

(iv) Antag att $f(x) = \sum_{j=0}^{n} c_j x^j$. Genom att använda egenskapen (iii) ser vi först att $a^j \equiv b^j \pmod{m}$ för alla j, och sedan följer det från (ii) att $c_j a^j \equiv c_j b^j \pmod{m}$. Upprepad användning av (i) leder slutligen till slutsatsen $f(a) = \sum_{j=0}^{n} c_j a^j \equiv \sum_{j=0}^{n} c_j b^j = f(b) \pmod{m}$. □

Anmärkning om beräkning av potenser. I många tillämpningar behöver man kunna beräkna potenser a^k modulo m snabbt och effektivt. Den naiva metoden att använda sig av $k-1$ stycken multiplikationer fungerar för små värden på k, men för stora tal k, som dem som används i exempelvis RSA-algoritmen som vi kommer att diskutera i avsnitt 8, tar detta alldeles för lång tid. Istället bör man beräkna a^k rekursivt med hjälp av formlerna

$$a^k = \begin{cases} (a^{k/2})^2 = (a^{\lfloor k/2 \rfloor})^2 & \text{om } k \text{ är jämnt,} \\ a \cdot (a^{(k-1)/2})^2 = a \cdot (a^{\lfloor k/2 \rfloor})^2 & \text{om } k \text{ är udda.} \end{cases}$$

På detta sätt erhåller man a^k från $a^{\lfloor k/2 \rfloor}$ med hjälp av en multiplikation (kvadrering) om exponenten k är jämn, och med två multiplikationer (kvadrering följt av multiplikation med a) om exponenten k är udda. Beroende på värdet på k kommer den allra första beräkningen i rekursionen att vara a^2 eller $a^3 = a \cdot a^2$.

Totala antalet multiplikationer för att beräkna a^k från a med rekursion är av storleksordningen $\log k$, vilket är litet jämfört med k. Om k har den binära utvecklingen $k = \alpha_r \alpha_{r-1} \dots \alpha_1 \alpha_0 = \sum_{j=0}^{r} \alpha_j 2^j$, (där $\alpha_r = 1$), så är $\lfloor k/2 \rfloor = \alpha_r \alpha_{r-1} \dots \alpha_1$, och k är udda om $\alpha_0 = 1$ och jämnt om $\alpha_0 = 0$. Härav följer lätt att antalet kvadreringar som behövs för att beräkna a^k är lika med r och att antalet extra multiplikationer med a är lika med antalet nollskilda siffror α_j minus 1. Detta innebär att det krävs högst $2r$ multiplicationer för att beräkna potensen a^k.

Exempel 1 Den rekursiva beräkningen av $3^{1304} \pmod{121}$ sammanfattas av följande tabell:

k	1304	652	326	163	162	81	80	40	20	10	5	4	2	1
$3^k \pmod{121}$	81	9	3	27	9	3	1	1	1	1	1	81	9	3

Talen i den översta raden beräknas från vänster till höger; om ett tal är jämnt erhålls nästa tal genom division med 2, och om det är udda erhålls nästa tal genom subtraktion med 1. Talen i den nedersta raden beräknas från höger till vänster. Exempelvis är $3^4 = (3^2)^2 \equiv 9^2 \equiv 81$, $3^5 = 3 \cdot 3^4 \equiv 3 \cdot 81 \equiv 243 \equiv 1$ och $3^{326} = (3^{163})^2 \equiv 27^2 \equiv 3$. □

Vi undersöker härnäst vad som händer när modulen multipliceras eller divideras med ett tal. Beviset för följande sats lämnas åt läsaren.

Sats 4.4 *Låt c vara ett godtycklig positivt heltal, och låt d vara en positiv delare till m.*

(i) Om $a \equiv b \pmod{m}$, så är $ac \equiv bc \pmod{mc}$.

(ii) Om $a \equiv b \pmod{m}$, så är $a \equiv b \pmod{d}$.

Man kan i allmänhet inte dividera en kongruens utan att samtidigt ändra modulen. Vi har följande resultat.

Sats 4.5 *Låt c vara ett nollskilt heltal och sätt $d = \text{sgd}(c, m)$.*
(i) Om $ca \equiv cb \pmod{m}$, så är $a \equiv b \pmod{m/d}$
(ii) Om $ca \equiv cb \pmod{m}$ och $\text{sgd}(c, m) = 1$, så är $a \equiv b \pmod{m}$.

Bevis. (i) Om $ca \equiv cb \pmod{m}$, så gäller per definition att $m \mid c(a-b)$ och detta medför att $\frac{m}{d} \Big| \frac{c}{d}(a-b)$. Eftersom $\text{sgd}\Big(\frac{m}{d}, \frac{c}{d}\Big) = 1$, följer härav att $\frac{m}{d} \Big| (a-b)$, dvs. $a \equiv b \pmod{m/d}$.

(ii) är ett specialfall av (i). □

Ett system av kongruenser kan ersättas av en enda kongruens på följande sätt:

Sats 4.6 *Låt $m_1, m_2, \ldots, m_r$ vara positiva heltal och sätt*

$$m = \text{mgm}(m_1, m_2, \ldots, m_r).$$

Följande två påståenden är då ekvivalenta:
(i) $a \equiv b \pmod{m_i}$ för $i = 1, 2, \ldots, r$.
(ii) $a \equiv b \pmod{m}$.

Bevis. Antag att $a \equiv b \pmod{m_i}$ för alla i. Då är $a - b$ en gemensam multipel till alla talen m_i, och därför är talet $a - b$ också delbart med den minsta gemensamma multipeln m. Detta betyder att $a \equiv b \pmod{m}$.

Om det omvänt gäller att $a \equiv b \pmod{m}$, så gäller det också att $a \equiv b \pmod{m_i}$ för varje i eftersom $m_i \mid m$. □

I återstoden av det här avsnittet betecknar m ett fixt positivt tal, som vi använder som modul.

Definition 4.7 Låt a vara ett heltal. Mängden $\overline{a} = \{x \in \mathbf{Z} \mid x \equiv a \pmod{m}\}$ av alla tal som är kongruenta modulo m med a kallas en *restklass*, eller *kongruensklass*, modulo m.

Eftersom kongruensrelationen är en ekvivalensrelation följer det att
- alla tal som tillhör samma restklass är ömsesidigt kongruenta modulo m,
- tal som tillhör olika restklasser är inkongruenta,
- för varje givet par av heltal a och b är antingen $\overline{a} = \overline{b}$ eller $\overline{a} \cap \overline{b} = \emptyset$,
- $\overline{a} = \overline{b}$ om och endast om $a \equiv b \pmod{m}$.

Sats 4.8 *Det finns exakt m olika restklasser modulo m, nämligen $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$.*

Bevis. Enligt divisionsalgoritmen finns det för varje heltal a ett unikt heltal r i intervallet $[0, m-1]$ sådant att $a \equiv r \pmod{m}$. Varje restklass $\overline{a}$ är därför identisk med en av restklasserna $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$, och dessa är olika eftersom $i \not\equiv j \pmod{m}$ om $0 \le i < j \le m-1$. □

Definition 4.9 Med ett *fullständigt restsystem* modulo m menas en uppsättning $x_1, x_2, \ldots, x_m$ av m stycken heltal tillhörande olika restklasser modulo m.

Mängden $\{0, 1, 2, \ldots, m-1\}$ är ett exempel på ett fullständigt restsystem modulo m.

EXEMPEL 2 $\{4, -7, 14, 7\}$ är ett fullständigt restsystem modulo 4. □

Lemma 4.10 *Om x och y tillhör samma restklass modulo m så är* $\text{sgd}(x, m) = \text{sgd}(y, m)$.

Bevis. Om $x \equiv y \pmod{m}$ så är $x = y + qm$ för något heltal q, och det följer av sats 1.4 att $\text{sgd}(x, m) = \text{sgd}(y, m)$. □

Två tal a och b ger upphov till samma restklass modulo m, dvs. $\overline{a} = \overline{b}$, om och endast om $a \equiv b \pmod{m}$. På grund av lemma 4.10 är därför följande definition konsistent.

Definition 4.11 En restklass $\overline{a}$ sägs vara *relativt prima* mot sin modul m om
$$\text{sgd}(a, m) = 1.$$

Definition 4.12 Antalet restklasser som är relativt prima mot modulen m betecknas $\phi(m)$, och funktionen $\phi\colon \mathbf{Z}_+ \to \mathbf{Z}_+$ kallas *Eulers ϕ-funktion.*

En mängd $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ bestående av ett tal från varje restklass som är relativt prima mot modulen m kallas ett *reducerat restsystem* modulo m.

Följande två observationer följer omedelbart ur definitionerna:

- $\phi(m)$ är lika med antalet tal i intervallet $[0, m-1]$ som är relativt prima mot talet m.
- $\{y_1, y_2, \ldots, y_{\phi(m)}\}$ är ett reducerat restsystem modulo m om och endast om talen är parvis inkongruenta modulo m och $\text{sgd}(y_i, m) = 1$ för alla i.

EXEMPEL 3 Talen i intervallet $[0, 7]$ som är relativt prima mot talet 8 är 1, 3, 5 och 7. Följaktligen är $\phi(8) = 4$, och $\{1, 3, 5, 7\}$ är ett reducerat restsystem modulo 8. □

EXEMPEL 4 Om p är ett primtal så är talen 1, 2, …, $p-1$ samtliga relativt prima mot p. Det följer att $\phi(p) = p-1$ och att $\{1, 2, \ldots, p-1\}$ är ett reducerat restsystem modulo p. □

EXEMPEL 5 Låt p^k vara en primtalspotens. Ett heltal är då relativt prima mot talet p^k om och endast om det inte är delbart med p. Intervallet $[0, p^k - 1]$ innehåller därför p^{k-1} tal som inte är relativt prima mot p^k, nämligen talen np, där $n = 0, 1, 2, \ldots, p^{k-1} - 1$, medan de återstående $p^k - p^{k-1}$ talen i intervallet är relativt prima mot p^k. Följaktligen är

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

I avsnitt 7 kommer vi att ge en formel för $\phi(m)$ för allmänt m (se korollarium 7.3). □

Sats 4.13 *Antag att* $\text{sgd}(a, m) = 1$*, att $\{r_1, r_2, \ldots, r_m\}$ är ett fullständigt restsystem samt att $\{s_1, s_2, \ldots, s_{\phi(m)}\}$ är ett reducerat restsystem modulo m. Då är också $\{ar_1, ar_2, \ldots, ar_m\}$ ett fullständigt restsystem och $\{as_1, as_2, \ldots, as_{\phi(m)}\}$ ett reducerat restsystem modulo m,*

Bevis. För att visa att mängden $\{ar_1, ar_2, \ldots, ar_m\}$ är ett fullständigt restsystem behöver vi bara kontrollera att elementen är valda från olika restklas-

ser, dvs. att de är parvis inkongruenta modulo m. Men enligt sats 4.5 medför $ar_i \equiv ar_j \pmod{m}$ att $r_i \equiv r_j \pmod{m}$, dvs. att $i = j$, och detta visar att elementen är parvis inkongruenta.

Eftersom $\text{sgd}(s_i, m) = 1$ och $\text{sgd}(a, m) = 1$ är vidare $\text{sgd}(as_i, m) = 1$ för $i = 1, 2, \ldots, \phi(m)$ på grund av sats 1.14. Talen $as_1, as_2, \ldots, as_{\phi(m)}$ tillhör därför restklasser som är relativt prima mot modulen m, och av samma skäl som ovan tillhör de olika restklasser. Då de dessutom är $\phi(m)$ till antalet bildar de ett reducerat restsystem. □

Sats 4.14 (Eulers sats) *Om* $\text{sgd}(a, m) = 1$ *så är*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Bevis. Låt $\{s_1, s_2, \ldots, s_{\phi(m)}\}$ vara ett reducerat restsystem modulo m. Enligt sats 4.13 är då också mängden $\{as_1, as_2, \ldots, as_{\phi(m)}\}$ ett reducerat restsystem, och följaktligen motsvaras varje element s_i i det förstnämnda systemet av exakt ett element as_j i det sistnämnda så att $s_i \equiv as_j \pmod{m}$. Genom att multiplicera ihop talen och använda oss av sats 4.3 (ii) drar vi därför slutsatsen att

$$\prod_{j=1}^{\phi(m)} (as_j) \equiv \prod_{i=1}^{\phi(m)} s_i \pmod{m},$$

och att följaktligen

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} s_j \equiv \prod_{i=1}^{\phi(m)} s_i \pmod{m}.$$

Eftersom $\text{sgd}(s_i, m) = 1$ kan vi använda sats 4.5 (ii) upprepade gånger för att dividera bort talen s_i. Efter $\phi(m)$ divisioner erhålles $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Nästa sats följer som omedelbart korollarium.

Sats 4.15 (Fermats lilla sats) *Om* p *är ett primtal och* $p \nmid a$, *så är*

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

För varje heltal a *är därför* $a^p \equiv a \pmod{p}$.

Bevis. Om $p \nmid a$, så är $\text{sgd}(a, p) = 1$, och eftersom $\phi(p) = p - 1$ enligt exempel 4 följer nu den första delen omedelbart av Eulers sats. Genom att multiplicera kongruensen med a noterar vi att $a^p \equiv a \pmod{p}$, och detta gäller uppenbarligen också i fallet $a \equiv 0 \pmod{p}$. □

EXEMPEL 6 Modulo 7 är $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$ och slutligen $3^6 \equiv 1$, helt i överensstämmelse med Fermats sats. På motsvarande sätt är $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$ och följaktligen $2^6 \equiv 1$. □

Övningar

4.1 Vilka tal n i intervallet $[1, 20]$ är kongruenta med 45 modulo
a) 9, b) 10, c) 11, d) 30, e) 40, f) 50?

4.2 För vilka tal $m \geq 2$ gäller
a) $20 \equiv 13 \pmod{m}$, b) $20 \equiv -13 \pmod{m}$, c) $25 \equiv 13 \pmod{m}$?

4.3 Visa att kongruensen $x^2 \equiv x \pmod{m}$ endast har lösningarna $x \equiv 0$ och $x \equiv 1 \pmod{m}$, om m är a) ett primtal och b) en primtalspotens.

4.4 Visa att för varje $x \geq 1$ har x och x^5 samma slutsiffra (i decimalsystemet).

4.5 Visa att talet $a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ är delbart med
a) 11 om och endast om talet
$$a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$$
är delbart med 11,
b) 7 om och endast om talet
$$(a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \cdots$$
är delbart med 7,
c) 13 om och endast om talet
$$(a_0 - 3a_1 - 4a_2) - (a_3 - 3a_4 - 4a_5) + (a_6 - 3a_7 - 4a_8) - \cdots$$
är delbart med 13.

4.6 Använd resultaten i föregående övning för att undersöka delbarhet med 11, 7 och 13 för talen a) 123444321 och b) 1171311713.

4.7 Lös övningarna 1.11, 1.12, 1.13 och 1.14 med hjälp av kongruensräkning.

4.8 Sätt $S_n = 1 + 2 + 3 + \cdots + (n-1)$ för $n \geq 2$.
a) Visa att $S_n \equiv 0 \pmod{n}$, om n är udda.
b) Bestäm huvudresten då S_n divideras med n om talet n är jämnt.

4.9 a) $\{a_1, a_2, \ldots, a_n\}$ är ett fullständigt restsystem modulo n. Bestäm huvudresten då $a_1 + a_2 + \cdots + a_n$ divideras med n.
b) $\{a_1, a_2, \ldots, a_{\phi(n)}\}$ är ett reducerat restsystem modulo n. Bestäm huvudresten då $a_1 + a_2 + \cdots + a_{\phi(n)}$ divideras med n.

4.10 För vilka $n \geq 2$ gäller att
a) $1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}$,
b) $1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}$?

4.11 Bestäm $\phi(n)$ för $n = 1, 2, \ldots, 10$.

4.12 Skriv upp ett a) fullständigt och b) reducerat restsystem modulo 20. Använd till beloppet minsta rester.

4.13 Visa att talen a, $2a$, $3a$, $\ldots$, na bildar ett fullständigt restsystem modulo n om $\text{sgd}(a, n) = 1$.

4.14 Låt m och n vara relativt prima positiva heltal. Kan man välja fullständiga restsystem $a_1, a_2, \ldots, a_m$ och $b_1, b_2, \ldots, b_n$ modulo m respektive n, så att talen $a_i + b_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, bildar ett fullständigt restsystem modulo mn?

4.15 Låt m och n vara relativt prima positiva heltal. Huvudresterna modulo mn utgörs av talen $j + mk$, där $0 \leq j \leq m-1$ och $0 \leq k \leq n-1$.
a) Visa att om $\text{sgd}(j, m) > 1$, så är $\text{sgd}(j + mk, mn) > 1$ för alla k.
b) Visa att om $\text{sgd}(j, m) = 1$, så är (för fixt j) exakt $\phi(n)$ stycken av talen $j + mk$, $0 \leq k \leq n-1$, relativt prima mot mn.
[Ledning: Visa att de n talen är inkongruenta modulo n.]
c) Använd a) och b) för att visa att $\phi(mn) = \phi(m)\phi(n)$.

4.16 Bestäm slutsiffran i a) 3^{60}, b) 2^{60}, c) 57^{75}.

4.17 Bestäm de två sista siffrorna i a) 3^{60}, b) 2^{60}, c) 57^{75}.

4.18 Visa att varje primtal utom 2 och 5 delar oändligt många av talen
a) 1, 11, 111, 1111, ..., b) 9, 99, 999, 9999, ...

4.19 Visa att om primtalen p och q är skilda, så gäller att $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

4.20 Låt p vara ett primtal.
a) Visa med hjälp av Fermats lilla sats att $(a+b)^p \equiv a^p + b^p \pmod{p}$.
b) Visa att $(a+b)^p \equiv a^p + b^p \pmod{p}$ utan att använda Fermats sats.
c) Visa att $a^p \equiv a \pmod{p}$, dvs. Fermats sats, med hjälp av b).

4.21 Låt p vara ett primtal. Visa att om $a^p \equiv b^p \pmod{p}$, så är $a^p \equiv b^p \pmod{p^2}$.

5 Pseudoprimtal

Om ett tal n är sammansatt, så har det en primfaktor p som är mindre än eller lika med $\sqrt{n}$. Om talet n inte är delbart med något primtal mindre än eller lika med $\sqrt{n}$, är följaktligen n ett primtal. Detta betyder att vi i värsta fall måste genomföra cirka $\sqrt{n}$ divisioner för att avgöra om talet n är sammansatt.

I de allra flesta fallen kan vi emellertid använda Fermats sats 4.15 för att visa att att givet tal n är sammansatt utan att behöva hitta några faktorer, ty om $\text{sgd}(a, n) = 1$ och $a^{n-1} \not\equiv 1 \pmod{n}$, så är nödvändigtvis talet n sammansatt. Vår förmåga att beräkna potenser $a^k \pmod{n}$ snabbt gör detta till en mycket effektiv metod. (Antalet multiplikationer och divisioner som behövs är proportionellt mot $\log n$ som är betydligt mindre än $\sqrt{n}$.)

Exempel 7 För att visa att talet 221 är sammansatt utan att behöva faktorisera det beräknar vi $2^{220} \pmod{221}$. De nödvändiga beräkningarna ges av följande tabell:

k	220	110	55	54	27	26	13	12	6	3	2	1
$2^k \pmod{221}$	16	30	128	64	8	4	15	118	64	8	4	2

Beräkningarna visar att $2^{220} \equiv 16 \pmod{221}$, och det följer att talet 221 måste vara sammansatt. I själva verket är $221 = 13 \cdot 17$. □

Omvändningen till Fermats sats gäller inte, dvs. $a^{m-1} \equiv 1 \pmod{m}$ medför inte att m är ett primtal. I vissa fall kan man därför inte avgöra huruvida ett tal är sammansatt eller ej med hjälp av ovanstående procedur.

Exempel 8 Talet 341 är sammansatt ($= 11 \cdot 31$), men ändå är $2^{340} \equiv 1 \pmod{341}$ vilket följer av beräkningarna i tabellen nedan.

k	340	170	85	84	42	21	20	10	5	4	2	1
$2^k \pmod{341}$	1	1	32	16	4	2	1	1	32	16	4	2

Testet upptäcker således inte att 341 är sammansatt. Men vi kan förstås pröva med en annan bas än 2, och om vi använder oss av 3 får vi följande tabell:

k	340	170	85	84	42	21	20	10	5	4	2	1
$3^k \pmod{341}$	56	67	254	312	163	201	67	56	243	81	9	3

Eftersom $3^{340} \equiv 56 \not\equiv 1 \pmod{341}$, drar vi nu slutsatsen att talet 341 är sammansatt. □

Det finns faktiskt ett annat och lättare sätt att se att 341 är sammansatt som bygger på följande lemma.

Lemma 5.1 *Låt p vara ett primtal. Då är $x^2 \equiv 1 \pmod{p}$ om och endast om $x \equiv \pm 1 \pmod{p}$.*

Bevis. Kongruensen $x^2 \equiv 1 \pmod{p}$ kan förstås skrivas som $(x-1)(x+1) \equiv 0 \pmod{p}$, dvs. $p \mid (x-1)(x+1)$. Eftersom p är ett primtal är detta ekvivalent med att $p \mid (x-1)$ eller $p \mid (x+1)$, och vi drar slutsatsen att $x \equiv \pm 1 \pmod{p}$. □

Exempel 2 (fortsättning) Om vi återvänder till beräkningarna i exempel 2 ser vi att $(2^{85})^2 = 2^{170} \equiv 1 \pmod{341}$, och eftersom $2^{85} \equiv 32 \not\equiv \pm 1 \pmod{341}$ drar vi nu med hjälp av lemma 5.1 slutsatsen att 341 måste vara ett sammansatt tal. □

Definition 5.2 Låt a och n vara positiva heltal. Om $\text{sgd}(a, n) = 1$ och $a^{n-1} \equiv 1 \pmod{n}$, så kallas n ett *sannolikt primtal i basen a*. Ett sammansatt sannolikt primtal kallas ett *pseudoprimtal*.

Varje primtal är naturligtvis ett sannolikt primtal i varje bas, men det finns sannolika primtal som är sammansatta tal, dvs. det finns pseudoprimtal. Exempel 2 visar att talet 341 är ett pseudoprimtal i basen 2 men att det inte är ett sannolikt primtal i basen 3. Då uppstår följande naturliga fråga: Finns det något heltal n som är ett pseudoprimtal i varje bas a som är relativt prima mot n? Eller med andra ord: Finns det något sammansatt tal n sådant att $a^{n-1} \equiv 1 \pmod{n}$ gäller för alla tal a som är relativt prima mot n? Svaret är ja, och sådana tal kallas *Carmichaeltal*, och man vet numera att det finns oändligt många Carmichaeltal. Talet 561 är det minsta Carmichaeltalet.

Exempel 3 Talet 561 är sammansatt, ty $561 = 3 \cdot 11 \cdot 17$. Genom att använda Fermats sats på primtalen 3, 11 och 17 inser vi att kongruenserna $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ och $a^{16} \equiv 1 \pmod{17}$ gäller för alla tal a som är relativt prima mot 561. Vi noterar nu att $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$, så genom att upphöja den första kongruensen med 280, den andra med 56 och den tredje med 35 erhåller vi som resultat att $a^{560} \equiv 1 \pmod{m}$ för $m = 3$, 11 och 17. Följaktligen är också $a^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$, och detta visar att 561 är ett sannolikt primtal för alla baser a som är relativt prima mot 561. Talet 561 är således ett Carmichaeltal. □

Fortsättningen på exempel 2 antyder att det finns ett starkare sätt att testa huruvida ett tal är sammansatt än att bara försöka visa att det i någon bas inte är ett sannolikt primtal. Detta är det så kallade *starka pseudoprimtaltestet*, som vi nu ska beskriva.

Antag att vi vill visa att ett udda tal n är sammasatt. Vi startar då med att dela det jämna talet $n-1$ med 2 upprepade gånger till dess att vi får $n-1 = 2^k d$,

där d är ett udda tal. Därefter bildar vi talen

$$a^d, a^{2d}, a^{4d}, \ldots, a^{2^k d} \pmod{n}$$

genom upprepad kvadrering och reducering modulo m.

Om det sista talet i denna sekvens, dvs. $a^{2^k d}$, inte är kongruent med 1 modulo n, så är talet n sammansatt.

Om däremot $a^{2^k d} \equiv 1 \pmod{n}$, så är n ett sannolikt primtal i basen a. Antag att så är fallet och låt $a^{2^j d}$ vara det första talet i ovanstående sekvens som är kongruent med 1 modulo n. Om då $j \geq 1$ och det för det omedelbart föregående talet $a^{2^{j-1} d}$ i följden gäller att $a^{2^{j-1} d} \not\equiv -1 \pmod{n}$, så är talet n sammansatt (på grund av lemma 5.1).

I de fall då detta test inte leder till någon bestämd slutsats, dvs. då $a^d \equiv 1 \pmod{n}$ eller då $0 \leq j < k$ och $a^{2^j d} \equiv -1 \pmod{n}$, kallas talet n ett *starkt sannolikt primtal i basen a*. Ett udda, sammansatt, starkt sannolikt primtal kallas ett *starkt pseudoprimtal*.

Man kan visa att det inte finns några tal som är starka pseudoprimtal i varje bas.

De starka pseudoprimtalen är sällsynta. I intervallet $1 \leq n \leq 25 \cdot 10^9$ finns det 1 091 987 405 primtal, 2 163 Carmichaeltal, 4 842 starka pseudoprimtal i basen 2, 184 tal som är starka pseudoprimtal i såväl basen 2 som basen 3, 13 tal som är starka pseudoprimtal i baserna 2, 3 och 5, och endast ett tal som är ett starkt pseudoprimtal i baserna 2, 3, 5 och 7.

Det minsta starka pseudoprimtalet i basen 2 är talet 2047.

Exempel 4 För att visa att 2047 är ett starkt pseudoprimtal i basen 2 skriver vi först $2046 = 2 \cdot 1023$. Eftersom $1023 = 2^{10} - 1 = \sum_{j=0}^{9} 2^j$ består den binära utvecklingen av 1023 av tio stycken 1-or. Genom upprepad kvadrering och reducering modulo 2047 beräknar vi sedan potenserna 2^{2^j} modulo 2047 för $0 \leq j \leq 9$, och genom att sedan multiplicera ihop dem finner vi att $2^{1023} \equiv 1 \pmod{2047}$. Detta betyder att 2047 är ett starkt sannolikt primtal, och eftersom $2047 = 23 \cdot 89$ är det ett starkt pseudoprimtal.

Istället för att faktorisera talet kan vi naturligtvis också pröva en annan bas. I basen 3 får vi $3^{1023} \equiv 1565 \pmod{2047}$ och $3^{2046} \equiv 1013 \pmod{2047}$, vilket visar att 2047 inte är ett sannolikt primtal i basen 3 utan sammansatt. □

Övningar

5.1 Visa att talet 143 är sammansatt utan att faktorisera det.

5.2 Visa att 121 är ett starkt pseudoprimtal i basen 3.

6 Linjära kongruenser

Kongruensen

$$ax \equiv b \pmod{m} \tag{1}$$

är ekvivalent med ekvationen

$$ax - my = b \tag{2}$$

där vi naturligtvis bara betraktar heltalslösningar x och y. Vi vet från sats 3.1 att ekvationen är lösbar om och endast om $d = \text{sgd}(a, m)$ är en delare till b. Om x_0, y_0 är en lösning så har vidare varje annan heltalslösning formen

$$x = x_0 + \frac{m}{d}\,n, \quad y = y_0 + \frac{a}{d}\,n.$$

Vi får därför d stycken parvis inkongruenta x-värden modulo m till kongruensen (1) genom att välja $n = 0,\ 1,\ \ldots,\ d-1$, och varje lösning x är kongruent med en av dessa. Detta bevisar följande sats:

Sats 6.1 *Kongruensen*

$$ax \equiv b \pmod{m}$$

är lösbar om och endast om $\text{sgd}(a, m) \mid b$. *Om kongruensen är lösbar, så har den exakt* $\text{sgd}(a, m)$ *parvis inkongruenta lösningar modulo* m.

Vi får följande specialfall som omedelbara korollarier till satsen.

Korollarium 6.2 *Kongruensen* $ax \equiv 1 \pmod{m}$ *är lösbar om och endast om* $\text{sgd}(a, m) = 1$, *och i det fallet har kongruensen en unik lösning modulo* m.

Korollarium 6.3 *Om* $\text{sgd}(a, m) = 1$, *så har kongruensen* $ax \equiv b \pmod{m}$ *en unik lösning modulo* m *för varje högerled* b.

Existensen av en lösning i korollarierna 6.2 och 6.3 följer också av Eulers sats. För $x_0 = a^{\phi(m)-1}$ och $x_1 = bx_0$ blir nämligen $ax_0 = a^{\phi(m)} \equiv 1 \pmod{m}$ och $ax_1 = bax_0 \equiv b \pmod{m}$.

Det är emellertid i allmänhet effektivare att lösa kongruensen (1) genom att lösa den ekvivalenta diofantiska ekvationen (2) med hjälp av metoderna i avsnitt 3 än att utnyttja Eulers sats. En annan möjlig lösningsmetod går ut på att ersätta kongruensen (1) med en kongruens med mindre modul på följande vis:

I kongruensen (1) ersätter vi först talen a och b med kongruenta tal i intervallet $[0, m-1]$, eller ännu bättre i intervallet $[-m/2, m/2]$. Om vi utgår ifrån att detta redan gjorts kan vi nu uttrycka ekvation (2) som en kongruens på formen

$$my \equiv -b \pmod{a} \tag{3}$$

med en modul a som är mindre än modulen m i (1). Om $y = y_0$ löser kongruensen (3), så är vidare

$$x = \frac{my_0 + b}{a}$$

en lösning till kongruensen (1). Hela proceduren kan sedan naturligtvis upprepas till dess att vi slutligen erhåller en kongruens på formen $z \equiv c \pmod{n}$.

Exempel 1 Lös kongruensen

$$296x \equiv 176 \pmod{114}. \tag{4}$$

Lösning: Eftersom 2 är en delare till talen 296, 176 och 114, börjar vi med att ersätta (4) med följande ekvivalenta kongruens:

$$148x \equiv 88 \pmod{57}. \tag{5}$$

Sedan reducerar vi 148 och 88 modulo 57; eftersom $148 \equiv -23$ och $88 \equiv -26$ kan vi ersätta (5) med kongruensen

$$23x \equiv 26 \pmod{57}. \tag{6}$$

Nu övergår vi istället till kongruensen

$$57y \equiv -26 \pmod{23},$$

som, eftersom 57 är kongruent med 11 och -26 är kongruent med -3 modulo 23, är ekvivalent med kongruensen

$$11y \equiv -3 \pmod{23}. \tag{7}$$

Denna kongruens ersätter vi nu med kongruensen

$$23z \equiv 3 \pmod{11}$$

som vi genast reducerar till

$$z \equiv 3 \pmod{11}.$$

Genom att använda lösningen $z = 3$ ser vi att

$$y = \frac{23 \cdot 3 - 3}{11} = 6$$

är en lösning till kongruensen (7) och att alla lösningar har formen $y \equiv 6 \pmod{23}$. Det följer därefter att

$$x = \frac{57 \cdot 6 + 26}{23} = 16$$

löser (6) och den därmed ekvivalenta kongruensen (4), samt att alla lösningar har formen $x \equiv 16 \pmod{57}$, vilket naturligtvis också kan skrivas som att $x \equiv 16$ eller $x \equiv 73 \pmod{114}$. □

Avslutande anmärkningar. Dessa anmärkningar riktar sig till läsare som är bekanta med elementär gruppteori.

Låt $\mathbf{Z}_m^*$ beteckna mängden av alla restklasser modulo m som är relativt prima mot modulen, Vi kan förse $\mathbf{Z}_m^*$ med en multiplikation genom att definiera produkten av två restklasser på följande sätt

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

För att definitionen ska vara välartad krävs det förstås att restklasen $\overline{ab}$ bara beror av *restklasserna* $\overline{a}$ och $\overline{b}$ och inte av de speciella tal a och b som utvalts för att representera dem, samt att $\overline{ab}$ tillhör $\mathbf{Z}_m^*$. Allt detta följer emellertid av satserna 4.3 (ii) och 1.14.

Den införda multiplikationen på $\mathbf{Z}_m^*$ är uppenbarligen associativ och kommutativ, och det finns ett enhetselement, nämligen restklassen $\overline{1}$. Vidare följer det av korollarium 6.2 att ekvationen $\overline{a} \cdot \overline{x} = \overline{1}$ har en unik lösning $\overline{x} \in \mathbf{Z}_m^*$ för varje $\overline{a} \in \mathbf{Z}_m^*$. Varje element i $\mathbf{Z}_m^*$ har med andra ord en unik multiplikativ invers.

Detta visar att $\mathbf{Z}_m^*$ är en ändlig abelsk (kommutativ) grupp. Gruppens ordning (dvs. antalet element i gruppen) är lika med $\phi(m)$ enligt definitionen av Eulers ϕ-funktion.

En av de första satser som man stöter på när man studerar gruppteori lyder: Om n är en ändlig grupps ordning och e är gruppens enhetselement, så är $a^n = e$ för varje

gruppelement a. Genom att använda detta resultat på gruppen $\mathbf{Z}_m^*$ erhåller vi Eulers sats, eftersom påståendet

$$\overline{a}^{\,\phi(m)} = \overline{1}$$

bara är ett annat uttryck för att kongruensen

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

är uppfylld för alla tal a som är relativt prima mot modulen m.

Övningar

6.1 Avgör vilka av följande kongruenser som är lösbara, och bestäm i förekommande fall lösningarna:
a) $11x \equiv 12 \pmod{15}$, b) $12x \equiv 11 \pmod{15}$, c) $12x \equiv 9 \pmod{15}$,
d) $123x \equiv 456 \pmod{789}$, e) $987x \equiv 654 \pmod{321}$.

6.2 Hur många inkongruenta lösningar har
a) $30x \equiv 1089 \pmod{2175}$, b) $30x \equiv 1089 \pmod{2173}$,
c) $30x \equiv 1089 \pmod{2169}$, d) $30x \equiv 1065 \pmod{2175}$?

6.3 Lös kongruensen $7x \equiv 11 \pmod{20}$ med hjälp av Eulers sats.

6.4 Lös kongruensen $ax \equiv 1 \pmod{m}$ om
a) $a = 44$, $m = 15$, b) $a = 7$, $m = 23$, c) $a = 24$, $m = 33$.

7 Kinesiska restsatsen

Låt oss börja med att betrakta ett system bestående av två kongruenser:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

där $\text{sgd}(m_1, m_2) = 1$. Den första kongruensen har lösningarna $x = a_1 + m_1 y$, $y \in \mathbf{Z}$, och genom att sätta in detta i den andra kongruensen erhåller vi kongruensen $a_1 + m_1 y \equiv a_2 \pmod{m_2}$, dvs. $m_1 y \equiv a_2 - a_1 \pmod{m_2}$. Eftersom $\text{sgd}(m_1, m_2) = 1$ har denna kongruens lösningar på formen $y = y_0 + m_2 n$, och följaktligen är $x = a_1 + m_1 y_0 + m_1 m_2 n$. Detta visar att systemet har en unik lösning $x \equiv x_0 \pmod{m_1 m_2}$.

Vi övergår nu till att studera ett system bestående av tre kongruenser:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases} \tag{1}$$

där modulerna m_1, m_2 and m_3 är parvis relativt prima. Som vi visade ovan kan vi ersätta de två första kongruenserna i systemet med en enda kongruens på formen $x \equiv x_0 \pmod{m_1 m_2}$, och följaktligen är hela systemet (1) ekvivalent med ett system på formen

$$\begin{cases} x \equiv x_0 \pmod{m_1 m_2} \\ x \equiv a_3 \pmod{m_3}. \end{cases} \tag{2}$$

På grund av vårt antagande om modulerna är $\text{sgd}(m_1m_2, m_3) = 1$, och systemet (2) har följaktligen en entydig lösning $x \equiv x_1 \pmod{m_1m_2m_3}$.

Med induktion är det nu lätt att bevisa följande allmänna resultat.

Sats 7.1 (Kinesiska restsatsen) *Systemet*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases} \tag{3}$$

där modulerna $m_1, m_2, \ldots, m_r$ är parvis relativt prima, har en entydig lösning modulo $m_1m_2 \cdots m_r$.

Bevis. Vi ska ge ett andra alternativt bevis för satsen och samtidigt också härleda en lösningsformel.

Antag att vi för $j = 1, 2, \ldots, r$ har konstruerat heltal δ_j som uppfyller kongruenserna

$$\delta_j \equiv \begin{cases} 1 \pmod{m_j} \\ 0 \pmod{m_i} \quad \text{om } i \neq j. \end{cases}$$

Då satisfierar uppenbarligen talet

$$x = \sum_{j=1}^{r} \delta_j a_j \tag{4}$$

kongruenssystemet (3).

Det återstår därför bara att visa att talen δ_j finns. Sätt för den skull $m = m_1m_2 \cdots m_r$. Då är $\text{sgd}\Big(\dfrac{m}{m_j}, m_j\Big) = 1$, så det följer därför av korollarium 6.2 att det finns ett heltal b_j sådant att

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}.$$

Talen $\delta_j = \dfrac{m}{m_j} b_j$ har nu uppenbarligen de önskvärda egenskaperna.

Detta bevisar existensen av en lösning x till systemet (3). För att också bevisa att lösningen är unik modulo m antar vi att x' är en annan lösning. Då gäller det att $x \equiv x' \pmod{m_j}$ för $j = 1, 2, \ldots, r$, och det följer därför av sats 4.6 att $x \equiv x' \pmod{m_1m_2 \cdots m_r}$, vilket visar entydigheten. □

Formeln (4) är speciellt användbar om vi behöver lösa flera system av typen (3) med samma moduler men med olika högerled $a_1, a_2, \ldots, a_r$.

Exempel 1 Låt oss lösa systemet

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

Lösning 1: Med hjälp av metoden i vårt första bevis för den kinesiska restsatsen ersätter vi den första kongruensen med likheten $x = 1 + 3y$. Genom insättning i den andra kongruensen erhåller vi sedan $3y + 1 \equiv 2 \pmod 4$, dvs. $3y \equiv 1 \pmod 4$. Denna kongruens har lösningarna $y \equiv -1 \pmod 4$, vilket betyder att $y = -1+4z$ och att följaktligen $x = -2+12z$. Insättning i den sista kongruensen leder till kongruensen $12z - 2 \equiv 3 \pmod 5$, dvs. $12z \equiv 5 \equiv 0 \pmod 5$. Denna kongruens har den unika lösningen $z \equiv 0 \pmod 5$, vilket betyder att $z = 5t$ och att $x = -2 + 60t$. Vårt system har således den unika lösningen $x \equiv -2 \pmod{60}$.

Lösning 2: Med metoden i vårt andra bevis måste vi först bestämma tal b_1, b_2 och b_3 sådana att

$$20b_1 \equiv 1 \pmod 3, \qquad 15b_2 \equiv 1 \pmod 4, \qquad 12b_3 \equiv 1 \pmod 5.$$

Man finner lätt att $b_1 = 2$, $b_2 = 3$ och $b_3 = 3$ duger. Därefter beräknar vi $\delta_1 = 20b_1 = 40$, $\delta_2 = 15b_2 = 45$ och $\delta_3 = 12b_3 = 36$, vilket ger oss lösningen

$$x = \delta_1 + 2\delta_2 + 3\delta_3 = 40 + 90 + 108 = 238 \equiv 58 \pmod{60}. \qquad \square$$

Villkoret att modulerna $m_1, m_2, \ldots, m_r$ ska vara parvis relativt prima är absolut väsentligt för att slutsatsen i sats 7.1 ska gälla. Utan detta villkor är systemet (3) antingen olösbart eller också har det fler än en inkongruent lösning modulo $m_1 m_2 \cdots m_r$. För att systemet ska vara lösbart är det nödvändigt och tillräckligt att $\text{sgd}(m_i, m_j) \mid (a_i - a_j)$ för alla $i \neq j$. Man kan lösa ett godtyckligt system eller bevisa dess olösbarhet genom att resonera som i den första lösningen av exempel 1.

Vi ska nu härleda några viktiga konsekvenser av sats 7.1. Fixera för varje givet positivt heltal n ett fullständigt restsystem $\mathcal{C}(n)$ modulo n. Delmängden av alla tal i $\mathcal{C}(n)$ som är relativt prima mot n bildar ett reducerat restsystem som vi betecknar $\mathcal{R}(n)$. Mängden $\mathcal{R}(n)$ innehåller $\phi(n)$ stycken tal. Om vi vill vara konkreta kan vi förstås välja $\mathcal{C}(n) = \{0, 1, 2, \ldots, n-1\}$, och då blir $\mathcal{R}(n) = \{j \mid 0 \leq j \leq n-1 \text{ och } \text{sgd}(j, n) = 1\}$.

Låt nu m_1 och m_2 vara två relativt prima tal och sätt $m = m_1 m_2$. Då innehåller $\mathcal{C}(m)$ och den kartesianska produkten $\mathcal{C}(m_1) \times \mathcal{C}(m_2)$ lika många element, nämligen m stycken. Vi ska nu konstruera en explicit bijektion τ mellan dessa två mängder.

Givet $x \in \mathcal{C}(m)$ och $j = 1$ eller 2 betecknar vi med x_j det unika tal i $\mathcal{C}(m_j)$ som har egenskapen att $x_j \equiv x \pmod{m_j}$. Vi definierar sedan funktionen $\tau \colon \mathcal{C}(m) \to \mathcal{C}(m_1) \times \mathcal{C}(m_2)$ genom att sätta $\tau(x) = (x_1, x_2)$.

En avbildning mellan två mängder med lika många element är en bijektion om (och endast om) den är surjektiv. Surjektiviteten hos avbildningen τ följer omedelbart av den kinesiska restsatsen, ty givet $(x_1, x_2) \in \mathcal{C}(m_1) \times \mathcal{C}(m_2)$ finns det enligt denna sats ett (unikt) $x \in \mathcal{C}(m)$ så att $x \equiv x_1 \pmod{m_1}$ och $x \equiv x_2 \pmod{m_2}$, vilket är detsamma som att säga att $\tau(x) = (x_1, x_2)$. Avbildningen τ är därför bijektiv.

Härnäst ska vi identifiera bilden $\tau(\mathcal{R}(m))$ under avbildningen τ av det reducerade restsystemet $\mathcal{R}(m)$. Eftersom

$$\text{sgd}(x, m) = 1 \Leftrightarrow \text{sgd}(x, m_1) = \text{sgd}(x, m_2) = 1$$

och

$$x \equiv x_j \pmod{m_j} \Rightarrow (\text{sgd}(x, m_j) = 1 \Leftrightarrow \text{sgd}(x_j, m_j) = 1)$$

har vi ekvivalensen $x \in \mathcal{R}(m) \Leftrightarrow \tau(x) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$, som visar att τ avbildar mängden $\mathcal{R}(m)$ bijektivt på den kartesianska produkten $\mathcal{R}(m_1) \times \mathcal{R}(m_2)$. Den förra mängden har $\phi(m)$ element och den senare mängden har $\phi(m_1)\phi(m_2)$ element. Eftersom de två mängderna måste ha samma antal element, har vi bevisat följande viktiga sats om Eulers ϕ-funktion.

Sats 7.2 *Om $m = m_1 m_2$, där talen m_1 och m_2 är relativt prima, så är*

$$\phi(m) = \phi(m_1)\phi(m_2).$$

Korollarium 7.3 *Om $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, där $p_1, p_2, \ldots, p_r$ är olika primtal, så är*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Bevis. Genom upprepad användning av sats 7.2 erhålls

$$\phi(m_1 m_2 \cdots m_r) = \phi(m_1)\phi(m_2)\cdots\phi(m_r)$$

förutsatt att talen $m_1, m_2, \ldots, m_r$ är parvis relativt prima, och detta gäller förstås speciellt om talen m_i är potenser till olika primtal. Enligt exempel 5 i avsnitt 4 är vidare $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - 1/p)$ om p är ett primtal. □

Ett polynom $f(x) = \sum_{i=0}^{n} a_i x^i$ med koefficienter $a_i \in \mathbf{Z}$ kallas ett *heltalspolynom*, och kongruensen

$$f(x) \equiv 0 \pmod{m},$$

kallas en *polynomkongruens*. Ett heltal a kallas en lösning eller en *rot* till polynomkongruensen om $f(a) \equiv 0 \pmod{m}$.

Om a är en rot till en polynomkongruens med modulen m och om $b \equiv a \pmod{m}$, så är också b en rot. För att lösa en polynomkongruens med modulen m räcker det därför att hitta alla rötter som tillhör ett givet fullständigt restsystem $\mathcal{C}(m)$ modulo m, t.ex. att hitta alla lösningar bland talen 0, 1, 2, …, $m - 1$. Med *antalet rötter* till en polynomkongruens menar vi antalet sådana inkongruenta rötter.

Betrakta ett system

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \qquad \vdots \\ f_r(x) \equiv 0 \pmod{m_r} \end{cases}$$

av polynomkongruenser, där modulerna $m_1, m_2, \ldots, m_r$ antas vara parvis relativt prima. Med en lösning till ett sådant system menar vi förstås ett tal som samtidigt löser alla kongruenserna i systemet. Om a är en lösning till systemet och om $b \equiv a \pmod{m_1 m_2 \cdots m_r}$, så är b också en lösning till systemet eftersom det i så fall speciellt gäller att $b \equiv a \pmod{m_j}$ för varje j. För att hitta alla lösningarna till systemet räcker det därför att betrakta lösningar som tillhör ett fullständigt restsystem modulo $m_1 m_2 \cdots m_r$, och med antalet lösningar till systemet menas antalet sådana inkongruenta lösningar.

Sats 7.4 *Låt*

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \qquad \vdots \\ f_r(x) \equiv 0 \pmod{m_r} \end{cases} \tag{5}$$

vara ett system av polynomkongruenser och antag att modulerna m_1, m_2, ..., m_r är parvis relativt prima. Låt X_j vara ett fullständigt system av inkongruenta lösningar modulo m_j till den j:te kongruensen och låt n_j beteckna antalet lösningar. Antalet lösningar till hela systemet är då lika med $n_1 n_2 \cdots n_r$, och varje lösning till systemet erhålls som lösning till systemen

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

där $(a_1, a_2, \ldots, a_r)$ varierar över mängden $X_1 \times X_2 \times \cdots \times X_r$.

Naturligtvis kan en mängd X_j vara tom och då är $n_j = 0$.

Bevis. Sätt $m = m_1 m_2 \cdots m_r$, låt $\mathcal{C}(m_j)$ vara ett fullständigt restsystem modulo m_j som innehåller lösningsmängden X_j ($j = 1, 2, \ldots, r$), och låt $\mathcal{C}(m)$ vara ett fullständigt restsystem modulo m som innehåller lösningsmängden X till systemet (5) av kongruenser. På grund av den kinesiska restsatsen får vi en bijektion

$$\tau : \mathcal{C}(m) \to \mathcal{C}(m_1) \times \mathcal{C}(m_2) \times \cdots \times \mathcal{C}(m_r)$$

genom att definiera

$$\tau(x) = (x_1, x_2, \ldots, x_r),$$

där varje $x_j \in \mathcal{C}(m_j)$ är ett tal som satisfierar kongruensen $x_j \equiv x \pmod{m_j}$.

Om $a \in X$, så är a en lösning till varje individuell kongruens i systemet (5). Om $a_j \in \mathcal{C}(m_j)$ och $a_j \equiv a \pmod{m_j}$, så är följaktligen a_j en lösning till den j:te kongruensen i systemet, dvs. a_j tillhör lösningsmängden X_j. Det följer att $\tau(a) = (a_1, a_2, \ldots, a_r)$ tillhör mängden $X_1 \times X_2 \times \cdots \times X_r$ för varje $a \in X$, och bildmängden $\tau(X)$ till X under τ är följaktligen en delmängd av produktmängden $X_1 \times X_2 \times \cdots \times X_r$.

Om omvänt $\tau(a) = (a_1, a_2, \ldots, a_r) \in X_1 \times X_2 \times \cdots \times X_r$, så löser a varje individuell kongruens och tillhör således X. Detta följer av sats 4.3, ty för varje index j är $a \equiv a_j \pmod{m_j}$ och $f_j(a_j) \equiv 0 \pmod{m_j}$. Bijektionen τ avbildar därför delmängden X på delmängden $X_1 \times X_2 \times \cdots \times X_r$, varav följer att antalet element i X är lika med $n_1 n_2 \cdots n_r$. □

Exempel 2 Betrakta systemet

$$\begin{cases} x^2 + x + 1 \equiv 0 \pmod{7} \\ \quad 2x - 4 \equiv 0 \pmod{6}. \end{cases}$$

Genom att pröva med $x = 0, \pm 1, \pm 2, \pm 3$, ser vi att $x \equiv 2 \pmod 7$ och $x \equiv -3 \pmod 7$ är lösningarna till den första kongruensen i systemet. Den andra kongruensen löses av $x \equiv -1 \pmod 6$ och $x \equiv 2 \pmod 6$. Vi drar därför slutsatsen att systemet har 4 inkongruenta lösningar modulo 42, och för att hitta dem ska vi lösa vart och ett av följande fyra system:

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv -1 \pmod 6 \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 2 \pmod 6 \end{cases}$$

$$\begin{cases} x \equiv -3 \pmod 7 \\ x \equiv -1 \pmod 6 \end{cases} \qquad \begin{cases} x \equiv -3 \pmod 7 \\ x \equiv 2 \pmod 6. \end{cases}$$

Vi använder lösningsformeln (4) i beviset för den kinesiska restsatsen, och bestämmer därför talen b_1 och b_2 så att

$$\frac{42}{7} b_1 \equiv 1 \pmod 7 \quad \text{och} \quad \frac{42}{6} b_2 \equiv 1 \pmod 6.$$

Man ser lätt att $b_1 = -1$ och $b_2 = 1$ löser dessa kongruenser, och vi kan följaktligen sätta $\delta_1 = -6$ och $\delta_2 = 7$. De fyra olika lösningarna modulo 42 till vårt ursprungliga kongruenssystem är därför

$$\begin{aligned} x_1 &= -6 \cdot 2 + 7 \cdot (-1) = -19 \equiv 23 \\ x_2 &= -6 \cdot 2 + 7 \cdot 2 = 2 \\ x_3 &= -6 \cdot (-3) + 7 \cdot (-1) = 11 \\ x_4 &= -6 \cdot (-3) + 7 \cdot 2 = 32. \end{aligned}$$

□

Vår nästa sats, som följer som specialfall av sats 7.4, visar att man kan reducera problemet att lösa polynomkongruenser med godtycklig modul till problemet att lösa polynomkongruenser med moduler som är primtalspotenser.

Sats 7.5 *Låt $f(x)$ vara ett heltalspolynom. För varje positivt heltal m låter vi $X(m)$ beteckna en fullständig mängd av rötter modulo m till polynomkongruensen*

$$f(x) \equiv 0 \pmod m,$$

och $N(m)$ är antalet rötter.

Antag att $m = m_1 m_2 \cdots m_r$, där talen $m_1, m_2, \ldots, m_r$ är parvis relativt prima. Då är

$$N(m) = N(m_1) N(m_2) \cdots N(m_r).$$

För varje r-tipel $(a_1, a_2, \ldots, a_r) \in X(m_1) \times X(m_2) \times \cdots \times X(m_r)$ finns det vidare en unik motsvarande rot $a \in X(m)$ sådan att $a \equiv a_j \pmod{m_j}$ för $j = 1, 2, \ldots, r$.

Bevis. Enligt sats 4.6 är kongruensen $f(x) \equiv 0 \pmod m$ ekvivalent med systemet

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \qquad \vdots \\ f(x) \equiv 0 \pmod{m_r}. \end{cases}$$

Påståendena i satsen är därför specialfall av sats 7.4. □

EXEMPEL 3 Låt $f(x) = x^2 + x + 1$. Visa att kongruensen $f(x) \equiv 0 \pmod{15}$ saknar lösning.

Lösning: Genom att pröva $x = 0, \pm 1, \pm 2$ upptäcker vi att kongruensen $f(x) \equiv 0 \pmod 5$ saknar lösning. Därför har inte heller den givna kongruensen modulo $15 (= 5 \cdot 3)$ någon lösning. □

EXEMPEL 4 Låt $f(x) = x^2 + x + 9$. Bestäm rötterna till kongruensen

$$f(x) \equiv 0 \pmod{63}.$$

Lösning: Eftersom $63 = 3^2 \cdot 7$, börjar vi med att lösa de två kongruenserna

$$f(x) \equiv 0 \pmod 7 \quad \text{och} \quad f(x) \equiv 0 \pmod 9.$$

Den första kongruensen har bara en rot, nämligen 3 (mod 7), medan den andra kongruensen har rötterna 0 och -1 (mod 9). Den givna kongruensen har följaktligen två rötter modulo 63, och de erhålls som lösningar till kongruenserna

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 0 \pmod 9 \end{cases} \quad \text{och} \quad \begin{cases} x \equiv \ \ 3 \pmod 7 \\ x \equiv -1 \pmod 9. \end{cases}$$

Med hjälp av den kinesiska restsatsen får vi rötterna are 45 och 17 modulo 63. □

Övningar

7.1 Bestäm lösningarna till följande system av kongruenser:

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{12} \end{cases}$, b) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$, c) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{15} \end{cases}$,

d) $\begin{cases} 2x \equiv 3 \pmod 9 \\ 4x \equiv 6 \pmod{10} \\ 6x \equiv 9 \pmod{11} \end{cases}$.

7.2 Sätt upp en formel för lösningarna till systemet

$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod{11} \\ x \equiv c \pmod{14} \end{cases}.$$

7.3 En pojke har ett antal kulor som är mindre än 100. När han delar dem i tre högar med lika många kulor i varje blir det en kula över, när han delar dem i fyra högar blir det två kulor över, och när han delar dem i fem högar blir det tre kulor över. Hur många kulor har han?

7.4 Visa att det för varje $k \geq 1$ finns k konsekutiva heltal, som vart och ett är delbart med en heltalskvadrat > 1.

7.5 Beräkna a) $\phi(100)$, b) $\phi(10!)$.

7.6 Hur många av talen a, $1 \leq a \leq 100$, satisfierar villkoret
a) $\text{sgd}(a, 100) = 1$, b) $\text{sgd}(a, 100) > 1$, c) $\text{sgd}(a, 100) = 2$?

7.7 Hur många av talen a, $1 \leq a \leq n$, satisfierar $\text{sgd}(a, n) = d$, där d är en positiv delare till n?

7.8 För vilka n är $\phi(n)$ udda?

7.9 Vilka positiva heltal n satisfierar ekvationen $\phi(2n) = \phi(n)$?

7.10 Visa att för $n > 1$ är $\sum a = \frac{1}{2}n\phi(n)$, där summationen utsträcks över alla a sådana att $1 \leq a \leq n$ och $\text{sgd}(a, n) = 1$.

7.11 Vilka positiva tal n satisfierar ekvationen a) $\phi(n) = \frac{1}{3}n$, b) $\phi(n) = \frac{2}{7}n$?

7.12 Vilket är det minsta positiva tal n respektive minsta positiva jämna tal n för vilket ekvationen $\phi(x) = n$ saknar lösning x?

7.13 Bestäm alla naturliga tal n för vilka $\phi(n) = 24$.

7.14 Visa att för givet n har ekvationen $\phi(x) = n$ endast ändligt många lösningar.

8 RSA-algoritmen

År 1977 uppfann R.L. Rivest, A. Shamir och L.M. Adleman en asymmetrisk krypteringsmetod som använder kongruensräkning och som har kommit att kallas *RSA-algoritmem*. Metoden använder två nycklar, en *publik krypteringsnyckel* och en *hemlig privat dekrypteringsnyckel*. Säkerheten hos krypteringsalgoritmen beror på svårigheten att faktorisera stora sammansatta tal och att för ett givet heltal k beräkna k:te roten modulo ett sammansatt tal.

RSA-algoritmen bygger på följande sats.

Sats 8.1 *Antag att talet m är ett positivt kvadratfritt tal, dvs. att talets kanoniska primtalsfaktorisering $m = p_1 p_2 \cdots p_r$ består av olika primtal. Låt e och d vara positiva tal sådana att $ed \equiv 1 \pmod{\phi(m)}$. För varje heltal a gäller då att $a^{ed} \equiv a \pmod{m}$.*

Bevis. Enligt sats 4.6 räcker det att visa att kongruensen $a^{ed} \equiv a \pmod{p}$ gäller för varje primtal $p = p_i$ som delar modulen m. Detta är trivialt uppfyllt om $a \equiv 0 \pmod{p}$, eftersom i så fall $a^{ed} \equiv a \equiv 0 \pmod{p}$. Vi kan därför antaga att $a \not\equiv 0 \pmod{p}$.

Enligt förutsättningarna är $ed = 1 + n\phi(m)$ för något icke-negativt heltal n, och

$$\phi(m) = \phi(p \cdot m/p) = \phi(p)\phi(m/p) = (p-1)\phi(m/p).$$

Följaktligen är $ed = 1 + n(p-1)\phi(m/p) = 1 + (p-1)N$, där N är något icke-negativt heltal. På grund av Fermats sats är därför

$$a^{ed} = a^{1+(p-1)N} = a \cdot (a^{p-1})^N \equiv a \cdot 1^N = a \pmod{p}. \qquad \square$$

Den publika RSA-nyckeln består av ett par (m, e) av heltal. Talet m används som modul och talet e är den publika exponenten. Modulen m är produkten av två olika, stora primtal p och q. (Varje primtal rekommenderas ha en storlek som är minst 2^{512}). Exponenten e måste var relativt prima mot $\phi(m)$, dvs. mot såväl $p-1$ som $q-1$, och väljs normalt som ett litet primtal såsom 3 $(= 2+1)$, 17 $(= 2^4 + 1)$ eller 65537 $(= 2^{16} + 1)$, beroende på att potenserna $a^e \pmod{m}$ går snabbt att beräkna för dessa speciella val av e.

I faktiska implementeringar av RSA-algoritmen fixeras först exponenten e. Sedan genereras slumpmässigt primtal p och q som uppfyller $\text{sgd}(p-1,e) = \text{sgd}(q-1,e) = 1$ på ett sådant sätt att varje primtal av den önskade storleken (säg 2^{512}) har samma sannolikhet att väljas. Slutligen sätts $m = pq$.

Den privata nyckeln består av paret (m,d), där d är det unika positiva tal mindre än $\phi(m)$ som uppfyller kongruensen $ed \equiv 1 \pmod{\phi(m)}$. Talet d, primtalen p och q samt talet $\phi(m)$ hålls hemliga av ägaren till den privata nyckeln.

Antag att någon, säg Alice, önskar skicka ett hemligt meddelande till Bob, innehavaren av den privata nyckel. Först måste då meddelandet konverteras till ett heltal a i intervallet $[0, m-1]$ på något standardsätt. (Man kan exempelvis använda ASCII-koden. Eftersom denna kodar "H" som 072, "e" som 101, "l" som 108, "o" som 111 och "!" som 033, skulle meddelandet "Hello!" genom sammansättning bli talet $a = 072101108108111033$.) Om meddelandet är alltför långt kommer koden för det att hamna utanför det tillåtna intervallet, men det kan då delas upp i ett antal block som kodas separat.

Sändaren Alice använder nu den publika krypteringsnyckeln för att beräkna det unika tal b i intervallet $[0, m-1]$ som uppfyller kongruensen $b \equiv a^e \pmod{m}$. Detta tal b skickas sedan till Bob.

När Bob tagit emot chiffermeddelandet b använder han sin privata exponent d för att bestämma det unika tal c som uppfyller $0 \leq c < m$ och $c \equiv b^d \pmod{m}$. Enligt sats 8.1 är $c = a$, och Bob har alltså återfunnit det hemliga talet a.

Antag att någon tredje part får tillgång till talet b. För att finna talet a måste han då dra e:te roten ur b, dvs. lösa kongruensen $x^e \equiv b \pmod{m}$. Det finns emellertid inte någon (känd) användbar metod för detta annat än att hitta talet d, och för att göra detta behöver han veta $\phi(m)$, och för detta behöver han kunna faktorisera talet m. Men att faktorisera heltal med 1000 binära siffror ligger utanför vad som är möjligt med dagens algoritmer och allra snabbaste datorer. RSA-algoritmen anses därför vara mycket säker.

Det är viktigt att meddelandetalet a inte är alltför litet relativt m, ty om $a^e < m$ kan vi förstås beräkna a från chiffertextmeddelandet $b = a^e$ genom att beräkna den vanliga e:te roten ur b. Därför är det nödvändigt att använda olika tekniker för att utvidga tal med få nollskilda siffror för att få en säker algoritm.

Övningar

8.1 Välj i detta lilla testexempel för RSA-algoritmen $p = 11$ och $q = 13$ så att $m = pq = 143$. Välj vidare krypteringsnyckeln $e = 77$.
a) Beräkna dekryperingsnyckeln d.
b) Kryptera talet $a = 50$ och verifiera att det återfås vid dekryptering.

9 Polynomkongruenser med primtalsmodul

Sats 7.5 reducerar studiet av polynomkongruenser $f(x) \equiv 0 \pmod{m}$ med en allmän modul m till fallet att m är en primtalspotens p^k. I det här avsnittet ska vi behandla fallet $k = 1$, dvs. kongruenser med primtalsmoduler, medan kongruenser med högre primtalspotenser som moduler kommer att diskuteras i nästa avsnitt.

Vi startar med att påminna om några allmänna begrepp för polynom och om divisionsalgoritmen.

Låt $f(x) = \sum_{i=0}^{n} a_i x^i$ vara ett heltalspolynom i variabeln x och antag att $a_n \neq 0$. Koefficienten a_n kallas då polynomets *ledande koefficient*, och talet n är polynomets *grad* och betecknas $\deg f(x)$. För att gradtalet ska bli definierat även för nollpolynomet, dvs. det polynom vars alla koefficienter är lika med noll, definierar vi nollpolynomets gradtal som symbolen $-\infty$, som vi betraktar som mindre än alla heltal.

Frasen "$f(x)$ är ett polynom av grad $< n$" betyder med andra ord att $f(x)$ antingen är ett polynom som har minst en nollskild koefficient och (vanlig) grad strikt mindre än n, eller nollpolynomet.

Om $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \equiv b_i \pmod{m}$ och $g(x) = \sum_{i=0}^{n} b_i x^i$, så är uppenbarligen $f(c) \equiv g(c) \pmod{m}$ för alla heltal c. I en polynomkongruens $f(x) \equiv 0 \pmod{m}$ kan vi således reducera koefficienterna modulo m, och speciellt kan vi utesluta alla termer $a_i x^i$ med $a_i \equiv 0 \pmod{m}$ utan att ändra lösningsmängden.

Exempel 1 Kongruensen

$$20x^5 + 17x^4 + 12x^2 + 11 \equiv 0 \pmod{4}$$

är ekvivalent med kongruensen

$$x^4 + 3 \equiv 0 \pmod{4},$$

och genom att pröva med -1, 0, 1, 2 hittar vi lösningarna $x \equiv \pm 1 \pmod{4}$. □

Anmärkning. Eftersom koefficienter som är delbara med modulen m kan ersättas med noll, förenklas en del resultat om man använder sig av begreppet *grad modulo m* eller *m-grad*. Med m-graden hos polynomet $f(x) = \sum_{i=0}^{n} a_i x^i$ menas då det största talet i med egenskapen att $m \nmid a_i$. (Om alla koefficienterna är delbara med m, är m-graden lika med $-\infty$.) Polynomet i exempel 1 har således 4-grad lika med 4. Vi kommer dock inte att använda oss av begreppet m-grad, så med ett polynoms grad menar vi fortsättningsvis alltid det vanliga gradtalet.

När ett heltalspolynom $f(x)$ divideras med ett heltalspolynom $g(x)$ behöver kvoten och resten inte vara heltalspolynom. Om den ledande koefficienten i $g(x)$ är 1, så är emellertid såväl kvot som rest heltalspolynom.

Sats 9.1 (Divisionsalgoritmen för heltalspolynom) *Låt $f(x)$ och $g(x)$ vara två heltalspolynom och antag att den ledande koefficienten hos $g(x)$ är lika med 1. Då finns det två entydigt bestämda heltalspolynom $q(x)$ och $r(x)$ sådana att $f(x) = q(x)g(x) + r(x)$ och $\deg r(x) < \deg g(x)$.*

Bevis. Vi visar existensen av polynomen $q(x)$ och $r(x)$ med hjälp av induktion, och lämnar beviset för entydigheten åt läsaren.

Sätt $n = \deg f(x)$ och $k = \deg g(x)$. Om $n < k$ låter vi $q(x)$ vara nollpolynomet och sätter $r(x) = f(x)$. Antag därför att $n \geq k$, att ax^n är den ledande termen i polynomet $f(x)$ samt att vi har bevisat existensen av polynomen $q(x)$ och $r(x)$ för alla polynom $f(x)$ med lägre gradtal än n. Betrakta polynomet $f(x) - ax^{n-k}g(x)$; det är ett polynom av grad $n_1 < n$ eftersom de två polynomen $f(x)$ och $ax^{n-k}g(x)$ har samma ledande koefficient a. Enligt induktionsantagandet finns det därför polynom $q_1(x)$ och $r(x)$ så att $f(x) - ax^{n-k}g(x) = q_1(x)g(x) + r(x)$ och $\deg r(x) < k$. De båda polynomen

$q(x) = ax^{n-k} + q_1(x)$ och $r(x)$ uppfyller nu villkoren i satsen, och därmed är induktionssteget klart, och existensen bevisad. □

Följande modulversion av den vanliga faktorsatsen för polynom följer nu omedelbart ur divisionsalgoritmen.

Sats 9.2 *Antag att $f(x)$ är ett heltalspolynom. Då är heltalet a en rot till kongruensen $f(x) \equiv 0 \pmod{m}$ om och endast om det finns ett heltalspolynom $q(x)$ och ett heltal b så att*

$$f(x) = (x-a)q(x) + mb.$$

Bevis. Vi använder divisionsalgoritmen och får $f(x) = (x-a)q(x) + c$, där kvoten $q(x)$ är ett heltalspolynom och resten c är ett konstant polynom, dvs. ett heltal. Eftersom $f(a) = c$, blir talet a en rot till kongruensen $f(x) \equiv 0 \pmod{m}$ om och endast om $c \equiv 0 \pmod{m}$, dvs. om och endast om $c = mb$ för något heltal b. □

Vi övergår nu till att studera polynomkongruenser av typen

$$f(x) \equiv 0 \pmod{p}$$

där modulen p är ett primtal. Om gradtalet hos $f(x)$ är större än eller lika med p kan vi reducera gradtalet på följande sätt: Dividera polynomet $f(x)$ med $x^p - x$; enligt divisionsalgoritmen finns det då två heltalspolynom $q(x)$ och $r(x)$ så att $f(x) = (x^p - x)q(x) + r(x)$ och $\deg r(x) < p$. Enligt Fermats sats är vidare $a^p - a \equiv 0 \pmod{p}$ och följaktligen $f(a) \equiv r(a) \pmod{p}$ för alla heltal a. Detta bevisar följande sats.

Sats 9.3 *Om p är ett primtal, så är varje polynomkongruens $f(x) \equiv 0 \pmod{p}$ ekvivalent med en polynomkongruens $r(x) \equiv 0 \pmod{p}$, där $r(x)$ är ett polynom med mindre grad än p.*

Ett annat sätt att beräkna polynomet $r(x)$ i sats 9.3 är att utnyttja följande lemma.

Lemma 9.4 *Antag att $n \geq p$ och att $n \equiv r \pmod{p-1}$, där $1 \leq r \leq p-1$. Då är $x^n \equiv x^r \pmod{p}$ för alla x.*

Bevis. Enligt förutsättningarna är $n = q(p-1) + r$ för något heltal q, och enligt Fermats sats är $x^{p-1} \equiv 1 \pmod{p}$ om $x \not\equiv 0 \pmod{p}$. För $x \not\equiv 0 \pmod{p}$ har vi därför kongruensen $x^n = (x^{p-1})^q \cdot x^r \equiv 1^q \cdot x^r = x^r \pmod{p}$, och i fallet $x \equiv 0 \pmod{p}$ är kongruensen trivialt sann. □

Genom att använda oss av lemma 9.4 kan vi ersätta alla termer med gradtal större än eller lika med p i ett heltalspolynom $f(x)$ med ekvivalenta termer av grad mindre än p, och detta leder till ett heltalspolynom $r(x)$ av grad mindre än p och med samma rötter modulo p som $f(x)$.

Exempel 2 Betrakta kongruensen $x^{11} + 2x^8 + x^5 + 3x^4 + 4x^3 + 1 \equiv 0 \pmod{5}$. Division med $x^5 - x$ ger

$$x^{11} + 2x^8 + x^5 + 3x^4 + 4x^3 + 1 = (x^6 + 2x^3 + x^2 + 1)(x^5 - x) + 5x^4 + 5x^3 + x + 1.$$

Den givna kongruensen är således ekvivalent med kongruensen

$$5x^4 + 5x^3 + x + 1 \equiv 0 \pmod 5,$$

som förenklas till $x + 1 \equiv 0 \pmod 5$ och har lösningen $x \equiv 4 \pmod 5$.

Istället kunde vi ha använt lemma 9.4. Eftersom $11 \equiv 3$, $8 \equiv 4$ och $5 \equiv 1$ modulo 4, ersätter vi termerna x^{11}, $2x^8$ och x^5 med x^3, $2x^4$ respektive x. Detta resulterar i polynomet

$$x^3 + 2x^4 + x + 3x^4 + 4x^3 + 1 = 5x^4 + 5x^3 + x + 1 \equiv x + 1 \pmod 5. \quad \square$$

Sats 9.5 *Låt p vara ett primtal. De icke-kongruenta talen $a_1, a_2, \ldots, a_k$ är rötter till polynomkongruensen $f(x) \equiv 0 \pmod p$ om och endast om det finns två heltalspolynom $q(x)$ och $r(x)$ sådana att*

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_k)q(x) + pr(x)$$

och $\deg r(x) < k$.

Bevis. Om det finns sådana polynom, så är $f(a_j) = pr(a_j) \equiv 0 \pmod p$. Omvändningen visas med hjälp av induktion över antalet rötter k. För $k = 1$ bevisades existensen av $q(x)$ och $r(x)$ i sats 9.2. Antag att satsen är sann för $k - 1$ rötter. Då finns det två polynom $q_1(x)$ och $r_1(x)$ med $\deg r_1(x) < k - 1$ och sådana att

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_{k-1})q_1(x) + pr_1(x). \tag{1}$$

Detta ger, eftersom $f(a_k) \equiv 0 \pmod p$, att

$$(a_k - a_1)(a_k - a_2) \cdots (a_k - a_{k-1})q_1(a_k) \equiv 0 \pmod p.$$

Eftersom $\operatorname{sgd}(a_k - a_j, p) = 1$ för $j = 1, 2, \ldots, k - 1$, kan vi dividera bort faktorerna $(a_k - a_j)$ i ovanstående kongruens med $q_1(a_k) \equiv 0 \pmod p$ som resultat. Enligt sats 9.2 finns det därför ett polynom $q(x)$ och ett heltal b så att

$$q_1(x) = (x - a_k)q(x) + pb,$$

och genom att sätta in detta i ekvation (1) ser vi att polynomen $q(x)$ och $r(x) = b(x - a_1)(x - a_2) \cdots (x - a_{k-1}) + r_1(x)$ uppfyller alla krav. $\square$

Som korollarium till ovanstående sats får vi följande resultat.

Sats 9.6 (Wilsons sats) *Om p är ett primtal, så är $(p - 1)! \equiv -1 \pmod p$.*

Bevis. Enligt Fermats sats har polynomet $x^{p-1} - 1$ rötterna 1,2, …, $p - 1$ modulo p. Följaktligen finns det polynom $q(x)$ och $r(x)$ sådana att

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1))q(x) + pr(x)$$

och $\deg r(x) < p - 1$. Genom att jämföra gradtal och ledande koefficienter ser vi att $q(x) = 1$. Genom att sätta $x = 0$ erhåller vi nu kongruensen

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

Om p är ett udda primtal, så drar vi slutsatsen att $(p - 1)! \equiv -1 \pmod p$, och för $p = 2$ får vi samma resultat eftersom $1 \equiv -1 \pmod 2$. $\square$

En polynomkongruens med allmän modul kan ha fler rötter än polynomets grad. Exempelvis har kongruensen $x^2 - 1 \equiv 0 \pmod 8$ fyra rötter: 1, 3, 5 och 7. Om modulen är ett primtal, så kan emellertid inte antalet rötter överstiga gradtalet, såvida inte alla polynomets koefficienter är delbara med primtalet. Detta följer som korollarium till sats 9.5.

Sats 9.7 *Låt p vara ett primtal och låt $f(x)$ vara ett heltalspolynom av grad n och med minst en koefficient som inte är delbar med p. Då har kongruensen $f(x) \equiv 0 \pmod p$ högst n rötter.*

Bevis. Antag att kongruensen har k rötter $a_1, a_2, \ldots, a_k$, och skriv med hjälp av sats 9.5 polynomet på formen $f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)q_1(x)+pr_1(x)$. Här måste kvoten $q_1(x)$ vara skild från nollpolynomet eftersom vi har antagit att inte alla koefficienterna i $f(x)$ är delbara med p. Följaktligen är $n = \deg f(x) = k + \deg q_1(x) \geq k$. □

En polynomkongruens kan å andra sidan sakna rötter. Kongruensen $x^2-2 \equiv 0 \pmod 3$ har inga rötter, och kongruensen $x^p-x+1 \equiv 0 \pmod p$ saknar rötter om p är ett primtal på grund av Fermats sats.

Här följer ett kriterium som garanterar att antalet rötter är lika med polynomets gradtal.

Sats 9.8 *Låt p vara ett primtal och antag att polynomet $f(x)$ har grad $n \leq p$ och ledande koefficient 1. Vi dividerar polynomet $x^p - x$ med $f(x)$ och får med hjälp av divisionsalgoritmen framställningen $x^p - x = q(x)f(x) + r(x)$, där $\deg r(x) < \deg f(x)$. Kongruensen $f(x) \equiv 0 \pmod p$ har då exakt n rötter om och endast om varje koefficient i $r(x)$ är delbar med p.*

Anmärkning. Antagandet att den ledande koefficienten hos polynomet $f(x)$ är 1 är i själva verket inte någon större inskränkning. Om den ledande koefficienten är a, kan vi förstås antaga att $\text{sgd}(a, p) = 1$. Genom att välja talet a' så att $a'a \equiv 1 \pmod p$ och ersätta polynomet $f(x)$ med polynometl $a'f(x) - (a'a - 1)x^n$ erhåller vi ett nytt polynom med ledande koefficient 1 och med samma rötter modulo p som $f(x)$.

Bevis. Låt m vara gradtalet hos polynomet $q(x)$; då är $m + n = p$ och den ledande koefficienten hos $q(x)$ är också 1. Om varje koefficient i $r(x)$ är delbar med p, så gäller på grund av Fermats sats att $q(a)f(a) \equiv a^p - a \equiv 0 \pmod p$ för varje heltal a. Eftersom p är ett primtal följer det av detta att $q(a) \equiv 0 \pmod p$ eller $f(a) \equiv 0 \pmod p$, dvs. varje heltal är rot till antingen $q(x) \equiv 0 \pmod p$ eller $f(x) \equiv 0 \pmod p$. Enligt sats 9.7 har den första kongruensen högst m rötter och den andra högst n rötter, så tillsammans finns det högst $m + n = p$ rötter. Men antalet rötter är p stycken, så därför drar vi slutsatsen att kongruensen $f(x) \equiv 0 \pmod p$ måste ha precis n rötter.

För att visa omvändningen utgår vi från likheten $r(x) = x^p - x - q(x)f(x)$ och noterar att det följder av Fermats sats att varje rot till $f(x)$ modulo p också är en rot till $r(x)$ modulo p. Om $f(x)$ har n rötter, så har följaktligen $r(x)$ minst n rötter. Eftersom graden hos $r(x)$ är mindre än n är detta emellertid möjligt endast om varje koefficient hos $r(x)$ är delbar med p. □

Korollarium 9.9 *Antag att p är ett primtal och att $d \mid (p-1)$. Då har kongruensen $x^d - 1 \equiv 0 \pmod p$ exakt d rötter.*

Bevis. Sätt $p-1=nd$. Genom att använda identiteten

$$y^n-1=(y-1)(y^{n-1}+y^{n-2}+\cdots+y+1)$$

och ersätta y med x^d, erhåller vi likheten $x^p-x=(x^{p-1}-1)x=(x^d-1)q(x)$, där $q(x)=x\sum_{j=0}^{n-1}x^{jd}$. Sats 9.8 är nu direkt tillämpbar. □

Övningar

9.1 Skriv upp en med $20x^3+15x^2+12x+4\equiv 0 \pmod m$ ekvivalent polynomkongruens genom att reducera koefficienterna, om m är lika med a) 2, b) 3, c) 4, d) 5, e) 11.

9.2 Skriv upp en med $x^9+2x^7+3x^4+4x^2+5x+6\equiv 0 \pmod p$ ekvivalent polynomkongruens genom att reducera graden och även koefficienterna, om p är lika med a) 2, b) 3, c) 5.

9.3 Visa att alla heltal x satisfierar $x^{42}+40x^2\equiv 0 \pmod{41}$.

9.4 Kongruensen $x^2+10x+6\equiv 0 \pmod{17}$ har en rot $x=1$. Bestäm en ekvivalent kongruens av formen $(x-1)g(x)\equiv 0 \pmod{17}$, och bestäm samtliga rötter.

9.5 Kongruensen $x^2+12x+12\equiv 0 \pmod{25}$ har uppenbarligen en rot $x=1$. Bestäm samtliga rötter.

9.6 Bestäm lösningarna till kongruensen $x^3+2x+2\equiv 0 \pmod m$, om m är lika med a) 2, b) 3, c) 5, d) 6, e) 7, f) 10, g) 35.

9.7 Lös kongruensen $20x^3+15x^2+12x+4\equiv 0 \pmod m$ (jämför övning 1), om m är lika med a) 2, b) 3, c) 4, d) 5, e) 20.

9.8 Hur många lösningar kan kongruensen $x^2+ax+b\equiv 0 \pmod m$ högst ha, om m är lika med a) 5, b) 41, c) 205, d) 210?
Ge exempel på värden på a och b, som ger maximalt många lösningar.

10 Polynomkongruenser med primtalspotensmodul

Det generella tillvägagångssättet för att lösa polynomkongruensen $f(x)\equiv 0 \pmod m$ då m är en primtalspotens p^k, är att starta med en rot till $f(x)$ modulo p och använda denna för att generera en rot (eller i vissa fall flera rötter) modulo p^2. Samma teknik används sedan för att producera rötter modulo p^3, p^4 och så vidare till dess att vi slutligen erhåller rötterna med avseende på den ursprungliga modulen p^k. Detaljerna kommer att beskrivas nedan

Låt oss börja med observationen att om $f(x)$ är ett heltalspolynom och a är ett heltal så finns det ett heltalspolynom $g(t)$ sådant att

$$f(a+t)=f(a)+f'(a)t+t^2g(t). \tag{1}$$

Detta är ett specialfall av Taylors formel, och för att bevisa det noterar vi att $f(a+t)$ är ett polynom i variabeln t med heltalskoefficienter, och att följaktligen $f(a+t)=A+Bt+t^2g(t)$, där $g(t)$ är ett heltalspolynom. Koefficienten A fås

genom att sätta $t = 0$, och för att bestämma B deriverar vi först och sätter sedan $t = 0$.

Låt oss nu betrakta kongruensen

$$f(x) \equiv 0 \pmod{p^2}, \tag{2}$$

där p är ett primtal. Varje lösning a till denna kongruens måste också vara en lösning till kongruensen

$$f(x) \equiv 0 \pmod{p}. \tag{3}$$

Låt oss omvänt antaga att a är en lösning till (3) och låt oss leta efter lösningar b till (2) sådana att $b \equiv a \pmod{p}$, dvs. sådana att $b = a + pt$ för något heltal t. Enligt ekvation (1) är

$$f(a+pt) = f(a) + f'(a)pt + p^2t^2g(pt) \equiv f(a) + pf'(a)t \pmod{p^2},$$

så talet $a + pt$ löser kongruensen (2) om och endast om $f(a) + pf'(a)t \equiv 0 \pmod{p^2}$, dvs. om och endast om

$$f'(a)t \equiv -\frac{f(a)}{p} \pmod{p}. \tag{4}$$

Om $\operatorname{sgd}(f'(a), p) = 1$, så har (4) en entydig lösning $t \equiv t_0 \pmod{p}$, och det följer att $x \equiv a + pt_0 \pmod{p^2}$ löser kongruensen (2) och att det också är den enda lösningen som också uppfyller $x \equiv a \pmod{p}$.

Om $p \mid f'(a)$, så är kongruensen (4) lösbar om och endast om $p^2 \mid f(a)$, och i så fall är varje tal t en lösning till (4), vilket innebär att $x \equiv a + pj \pmod{p^2}$ löser (2) för $j = 0, 1, \ldots, p-1$. I det fallet har kongruensen p rötter som är kongruenta med a modulo p.

Om $p \mid f'(a)$ och $p^2 \nmid f(a)$, så saknar slutligen (2) lösningar som är kongruenta med a.

Steget som leder från p^k till p^{k+1} är helt analogt. Detta betyder att vi har följande sats.

Sats 10.1 *Låt p vara ett primtal och låt k vara ett godtyckligt positivt tal, och antag att a är en lösning till kongruensen $f(x) \equiv 0 \pmod{p^k}$.*

(i) Om $p \nmid f'(a)$, så finns det exakt en lösning b till kongruensen $f(x) \equiv 0 \pmod{p^{k+1}}$ sådan att $b \equiv a \pmod{p^k}$. Lösningen ges av att $b = a + p^kt$, där t är den unika lösningen till kongruensen $f'(a)t \equiv -f(a)/p^k \pmod{p}$.

(ii) Om $p \mid f'(a)$ och $p^{k+1} \mid f(a)$, så finns det p stycken lösningar till $f(x) \equiv 0 \pmod{p^{k+1}}$ som är kongruenta med a modulo p^k; dessa lösningar är $a+p^kj$ för $j = 0, 1, \ldots, p-1$.

(iii) Om $p \mid f'(a)$ och $p^{k+1} \nmid f(a)$, så finns det inga lösningar till kongruensen $f(x) \equiv 0 \pmod{p^{k+1}}$ som är kongruenta med a modulo p^k.

Bevis. Låt b vara en lösning till $f(x) \equiv 0 \pmod{p^{k+1}}$ som är kongruent med a modulo p^k. Då är $b = a + p^kt$ för något heltal t. Det följer av (1) att

$$0 \equiv f(b) = f(a) + f'(a)p^kt + p^{2k}t^2g(p^kt) \equiv f(a) + f'(a)p^kt \pmod{p^{k+1}},$$

ty $2k \geq k+1$. Eftersom $f(a) \equiv 0 \pmod{p^k}$, är talet $f(a)/p^k$ ett heltal, och vi kan följaktligen dividera kongruensen ovan med p^k och erhåller då

$$f'(a)t \equiv -f(a)/p^k \pmod{p}.$$

Den sistnämnda kongruensen har en entydig lösning om $\text{sgd}(f'(a), p) = 1$, dvs. om $p \nmid f'(a)$. Om $p \mid f'(a)$, så krävs det för lösning att $f(a)/p^k \equiv 0 \pmod{p}$, dvs. att $p^{k+1} \mid f(a)$, och i det fallet får vi en lösning för varje värde på t. Om slutligen $p \mid f'(a)$ och $p^{k+1} \nmid f(a)$, så löser inget värde på t kongruensen. □

Korollarium 10.2 *Låt p vara ett primtal och k ett godtyckligt positivt heltal. Om a löser kongruensen $f(x) \equiv 0 \pmod{p}$ och $p \nmid f'(a)$, så har kongruensen $f(x) \equiv 0 \pmod{p^k}$ exakt en lösning b sådan att $b \equiv a \pmod{p}$.*

Bevis. Enligt sats 10.1 (i) finns det en unik lösning b_2 till kongruensen $f(x) \equiv 0 \pmod{p^2}$ som är kongruent med a modulo p. Det följer att $f'(b_2) \equiv f'(a) \pmod{p}$, och följaktligen att $p \nmid f'(b_2)$. Enligt samma sats finns det därför en unik lösning b_3 till kongruensen $f(x) \equiv 0 \pmod{p^3}$ sådan att $b_3 \equiv b_2 \equiv a \pmod{p}$. Genom att fortsätta i samma stil erhåller vi slutligen en unik lösning $b = b_k$ till kongruensen $f(x) \equiv 0 \pmod{p^k}$ som är kongruent med a modulo p. □

Sammanfattning. Det allmänna tillvägagångssättet för att bestämma alla rötter till kongruensen $f(x) \equiv 0 \pmod{p^k}$ kan sammanfattas på följande vis.

1. Bestäm först alla lösningar till kongruensen $f(x) \equiv 0 \pmod{p}$.
2. Välj en av dessa, säg a_1; då finns det antingen 0, 1 eller p lösningar till kongruensen $f(x) \equiv 0 \pmod{p^2}$ som är kongruenta med a_1 modulo p. Om det finns lösningar, så hittar vi dem genom att lösa den linjära kongruensen $f'(a_1)t \equiv -f(a_1)/p \pmod{p}$. Om det inte finns några lösningar, så börjar vi om med ett annat a_1.
3. Om kongruensen $f(x) \equiv 0 \pmod{p^2}$ har lösningar, så väljer vi en, säg a_2, och bestämmer sedan motsvarande rötter till $f(x) \equiv 0 \pmod{p^3}$ genom att lösa kongruensen $f'(a_2)t \equiv -f(a_2)/p^2 \pmod{p}$. Gör så för varje rot till kongruensen $f(x) \equiv 0 \pmod{p^2}$.
   Observera att om $a_2 \equiv a_1 \pmod{p}$, så är $f'(a_2) \equiv f'(a_1) \pmod{p}$, så vi behöver inte göra några nya beräkningar för att erhålla de nödvändiga derivatorna $f'(a_2)$.
4. Genom att fortsätta på den inslagna vägen kommer vi slutligen att hitta alla lösningarna till $f(x) \equiv 0 \pmod{p^k}$.

Det är värt att betona att om vi i något steg erhåller multipla lösningar, så måste vi fortsätta ovanstående process på varje lösning

Tyvärr finns det ingen allmän metod för att starta algoritmen, dvs. för att hitta samtliga lösningar till kongruensen $f(x) \equiv 0 \pmod{p}$ (annan än att pröva alla tal i något fullständigt restsystem). I nästa avsnitt ska vi diskutera vad som kan sägas om antalet lösningar, och i efterföljande avsnitt ska vi behandla några specialfall.

EXEMPEL 1 Lös kongruensen $7x^6 + 4x + 12 \equiv 0 \pmod{135}$.

Lösning: Eftersom $135 = 3^3 \cdot 5$, är kongruensen ekvivalent med systemet

$$\begin{cases} 7x^6 + 4x + 12 \equiv 0 \pmod{5} \\ 7x^6 + 4x + 12 \equiv 0 \pmod{3^3}. \end{cases} \tag{5}$$

Sätt $f(x) = 7x^6 + 4x + 12$. Vi kan med hjälp av Fermats sats ersätta den första kongruensen i systemet med kongruensen $2x^2 + 4x + 2 \equiv 0 \pmod{5}$, som förenklas till $(x + 1)^2 \equiv 0 \pmod{5}$ och har den enda roten -1.

För att lösa den andra kongruensen i systemet börjar vi med kongruensen $f(x) \equiv 0 \pmod 3$, som är ekvivalent med kongruensen $x^2 + x \equiv 0 \pmod 3$, eftersom $x^6 \equiv x^2 \pmod 3$. Dess lösningar är $x \equiv 0 \pmod 3$ och $x \equiv -1 \pmod 3$. Derivering ger $f'(x) = 42x^5 + 4$, och eftersom $f'(0) = 4 \equiv 1 \pmod 3$ och $f'(-1) = -38 \equiv 1 \pmod 3$, följer det av korollarium 10.2 att kongruensen $f(x) \equiv 0 \pmod{3^3}$ har två lösningar.

För att hitta dessa börjar vi med $x_1 = 0$ och löser den linjära kongruensen $f'(0)t \equiv -f(0)/3 \pmod 3$, dvs. $t \equiv -4 \equiv 2 \pmod 3$. Vi drar slutsatsen att $x_2 = 0 + 2 \cdot 3 = 6$ löser $f(x) \equiv 0 \pmod{3^2}$. Härnäst löses kongruensen $f'(0)t \equiv f'(6)t \equiv -f(6)/9 \pmod 3$, som ger att $t \equiv 2 \pmod 3$. Det följer att $x_3 = 6 + 2 \cdot 9 = 24$ löser $f(x) \equiv 0 \pmod{3^3}$.

Genom att istället utgå från $y_1 = -1$ löser vi först kongruensen $f'(-1)t \equiv -f(-1)/3 \pmod 3$, som ger att $t \equiv -5 \equiv 1 \pmod 3$. Följaktligen löser $y_2 = -1 + 1 \cdot 3 = 2$ kongruensen $f(x) \equiv 0 \pmod{3^2}$. Därefter löser vi kongruensen $f'(-1)t \equiv f'(2)t \equiv -f(2)/9 \pmod 3$. Lösningen är $t \equiv 2 \pmod 3$, varav följer att $y_3 = 2 + 2 \cdot 9 = 20$ löser kongruensen $f(x) \equiv 0 \pmod{3^3}$.

För att hitta de två lösningarna till vår ursprungliga kongruens använder vi nu den kinesiska restsatsen och löser med hjälp av den de båda systemen

$$\begin{cases} x \equiv -1 \pmod 5 \\ x \equiv 24 \pmod{3^3} \end{cases} \quad \text{and} \quad \begin{cases} x \equiv -1 \pmod 5 \\ x \equiv 20 \pmod{3^3}. \end{cases}$$

Lösningarna är $x \equiv 24 \pmod{135}$ and $x \equiv 74 \pmod{135}$. □

EXEMPEL 2 Bestäm samtliga lösningar till kongruensen $x^{10} \equiv 24 \pmod{125}$.

Lösning: Eftersom $125 = 5^3$ börjar vi med att lösa kongruensen $f(x) \equiv 0 \pmod 5$, där $f(x) = x^{10} - 24$. Enligt Fermats sats är $x^5 \equiv x \pmod 5$, och det följer att $f(x) \equiv x^2 - 24 \equiv x^2 - 4 \equiv (x-2)(x+2) \pmod 5$. Vi drar därför slutsatsen att kongruensen $f(x) \equiv 0 \pmod 5$ har två lösningar, $x \equiv \pm 2 \pmod 5$.

Härnäst noterar vi att $f'(x) = 10x^9$ är delbart med 5 för alla x och speciellt då för $x = \pm 2$. Var och en av lösningarna ± 2 ger därför upphov till 5 eller 0 lösningar modulo 25 till kongruensen $f(x) \equiv 0 \pmod{25}$ beroende på om $25 \mid f(\pm 2)$ eller ej. Nu är $f(\pm 2) = 1000$ delbart med 25, och därför får vi tio inkongruenta lösningar på formen $\pm 2 + 5j$ modulo 25, $j = 0, 1, 2, 3, 4$. Vi kan förstås också skriva dem som ± 2, ± 7, ± 12, ± 17, and ± 22.

Låt a_2 vara en av dessa lösningar; eftersom $f'(a_2) \equiv f'(\pm 2) \equiv 0 \pmod 5$ kommer a_2 att ge upphov till 5 eller 0 lösningar till kongruensen $f(x) \equiv 0 \pmod{125}$ beroende på om $125 \mid f(a_2)$ eller ej. Låt oss därför beräkna $f(x)$ modulo 125 för var och en av ovanstående lösningar till kongruensen $f(x) \equiv 0 \pmod{25}$. Efter lite räkning erhåller vi $f(\pm 2) \equiv 0$, $f(\pm 7) \equiv 100$, $f(\pm 12) \equiv 75$, $f(\pm 17) \equiv 50$ och $f(\pm 22) \equiv 25$. Vi får följaktligen fem lösningar från var och en av rötterna 2 och -2 och inga lösningar från de andra rötterna till kongruensen $f(x) \equiv 0 \pmod{25}$. De erhållna lösningarna är $\pm 2 + 25j$ modulo 125, $j = 0, 1, 2, 3, 4$, dvs. 2, 23, 27, 48, 52, 73, 77, 98, 102 and 123. □

Övningar

10.1 Lös kongruenserna a) $x^2 - x + 2 \equiv 0 \pmod{121}$, b) $x^3 \equiv 11 \pmod{625}$, c) $x^3 + 2x + 2 \equiv 0 \pmod{250}$.

10.2 Bestäm för varje $k \geq 1$ antalet lösningar till kongruenserna
a) $x^3 + 3x + 9 \equiv 0 \pmod{5^k}$, b) $x^2 + x + 7 \equiv 0 \pmod{3^k}$.

10.3 Hur många lösningar har $x^3 + 19x + 5 \equiv 0 \pmod{p^k}$, $k \geq 1$, om p är lika med a) 2, b) 3, c) 5?

10.4 Lös kongruensen $x^2 \equiv x \pmod{375}$.

10.5 Visa att för varje udda heltal a och varje positivt n har kongruensen $x^3 \equiv a \pmod{2^n}$ exakt en lösning modulo 2^n.

11 Kongruensen $x^2 \equiv a \pmod{m}$

I det här avsnittet ska vi studera kongruensen

$$x^2 \equiv a \pmod{m} \tag{1}$$

och vi ska behandla följande tre frågor:

- När är kongruensen lösbar?
- Hur många lösningar har en lösbar kongruens?
- Hur hittar man lösningarna?

Vi ska först visa att man alltid kan reducera en kongruens på formen (1) till en kongruens av samma form och med $\text{sgd}(a, m) = 1$.

Antag för den skull att $\text{sgd}(a, m) > 1$ och låt p vara ett primtal som delar $\text{sgd}(a, m)$, dvs. $p \mid a$ och $p \mid m$. Antag att x är en lösning till (1). Då gäller att $p \mid x^2$ och följaktligen att $p \mid x$. Sätt $x = py$; då är kongruensen (1) ekvivalent med kongruensen $p^2y^2 \equiv a \pmod{m}$, och genom att dividera med p erhåller vi

$$py^2 \equiv a/p \pmod{m/p}. \tag{2}$$

Vi har nu tre olika fall:

(i) Om $p^2 \mid m$ och $p^2 \mid a$, så är (2) ekvivalent med kongruensen $y^2 \equiv a/p^2 \pmod{m/p^2}$, och för varje lösning y_0 till denna kongruens (om det finns någon) finns det p inkongruenta lösningar modulo m till den ursprungliga kongruensen (1). Dessa är $x \equiv py_0 \pmod{m/p}$.
Om $\text{sgd}(a/p^2, m/p^2) > 1$, så upprepar vi hela proceduren.

(ii) Om $p^2 \mid m$ men $p^2 \nmid a$, så är (2) en motsägelse. Kongruensen (1) har således inga lösningar i det fallet.

(iii) Om $p^2 \nmid m$, så är $\text{sgd}(p, m/p) = 1$, och det finns följaktligen ett tal c sådant att $cp \equiv 1 \pmod{m/p}$. Det följer att (2) är ekvivalent med kongruensen $y^2 \equiv ca/p \pmod{m/p}$. Varje lösning y_0 till denna kongruens ger upphov till en unik lösning $x \equiv py_0 \pmod{m}$ till (1).
Om $\text{sgd}(ca/p, m/p) > 1$ upprepar vi hela proceduren.
Observera att om $p^2 \mid a$, så är $ca/p = cp \cdot a/p^2 \equiv 1 \cdot a/p^2 \equiv a/p^2 \pmod{m/p}$, dvs. (2) är i detta fall ekvivalent med kongruensen $y^2 \equiv a/p^2 \pmod{m/p}$.

Exempel 1 Lös följande fyra kongruenser:

$$\text{(i) } x^2 \equiv 36 \pmod{45}, \quad \text{(ii) } x^2 \equiv 15 \pmod{45},$$
$$\text{(iii) } x^2 \equiv 18 \pmod{21}, \quad \text{(iv) } x^2 \equiv 15 \pmod{21}.$$

Lösning: (i) Här är $\text{sgd}(36, 45) = 9$ och genom att sätta $x = 3y$ erhåller vi den ekvivalenta kongruensen $y^2 \equiv 4 \pmod 5$ med lösningarna $y \equiv \pm 2 \pmod 5$. Följaktligen är $x \equiv \pm 6 \pmod{15}$, dvs. 6, 9, 21, 24, 36 och 39 är lösningarna till kongruensen (i).

(ii) Eftersom $9 \mid 45$ men $9 \nmid 15$ finns det inga lösningar till (ii).

(iii) Eftersom $\text{sgd}(18, 21) = 3$, skriver vi $x = 3y$ och erhåller följande följd av ekvivalenta kongruenser: $9y^2 \equiv 18 \pmod{21}$, $3y^2 \equiv 6 \pmod 7$, $y^2 \equiv 2 \pmod 7$ med lösningarna $y \equiv \pm 3 \pmod 7$. Följaktligen har (iii) lösningarna $x \equiv \pm 9 \pmod{21}$.

(iv) Eftersom $\text{sgd}(15, 21) = 3$, sätter vi $x = 3y$ och får $9y^2 \equiv 15 \pmod{21}$, dvs. $3y^2 \equiv 5 \pmod 7$. Eftersom $5 \cdot 3 \equiv 1 \pmod 7$, multiplicerar vi den sista kongruensen med 5, vilket ger $y^2 \equiv 4 \pmod 7$ med lösningarna $y \equiv \pm 2 \pmod 7$. Således är $x \equiv \pm 6 \pmod{21}$ lösningarna till (iv). □

Definition 11.1 Antag att $\text{sgd}(a, m) = 1$. Om kongruensen $x^2 \equiv a \pmod m$ har en lösning kallas a en *kvadratisk rest till* m, och om lösning saknas kallas a en *kvadratisk ickerest till* m.

Genom att skriva modulen m som en produkt av primtal och utnyttja sats 7.5 reducerar vi studiet av kongruensen (1) till ett studium av kongruenser på formen

$$x^2 \equiv a \pmod{p^k}$$

där modulen är en primtalspotens. Nu kan vi använda tekniken i avsnitt 10. Eftersom x^2 har derivatan $2x$ och $2x \equiv 0 \pmod 2$ måste vi skilja på fallen $p = 2$ och p udda primtal.

Lemma 11.2 *Om p är ett udda primtal,* $\text{sgd}(a, p) = 1$ *och a är en kvadratisk rest till p, så har kongruensen $x^2 \equiv a \pmod p$ exakt två rötter.*

Bevis. Enligt antagandet finns det minst en rot b. Uppenbarligen är $-b$ också en rot och $-b \not\equiv b \pmod p$, eftersom $b \not\equiv 0$. Enligt sats 9.7 kan kongruensen inte ha fler än två rötter. □

Sats 11.3 *Om p är ett udda primtal och* $\text{sgd}(a, p) = 1$*, så har kongruensen $x^2 \equiv a \pmod{p^k}$ exakt två lösningar om a är en kvadratisk rest till p, och inga lösningar om a är en kvadratisk ickerest till p.*

Bevis. Sätt $f(x) = x^2 - a$; då är $f'(x) = 2x$ inte delbart med p för något $x \not\equiv 0 \pmod p$. Det följer därför av korollarium 10.2 och lemma 11.2 att kongruensen $x^2 \equiv a \pmod{p^k}$ har exakt två lösningar för varje k om a är en kvadratisk rest. Eftersom varje lösning till den senare kongruensen också löser kongruensen $x^2 \equiv a \pmod p$ kan det inte finnas några lösningar om a är en kvadratisk ickerest till p. □

Fallet $p = 2$ är annorlunda, och den fullständiga bilden ges av följande sats.

Sats 11.4 *Antag att talet a är udda. Då gäller att*

(i) kongruensen $x^2 \equiv a \pmod 2$ alltid är lösbar och har exakt en lösning;

(ii) kongruensen $x^2 \equiv a \pmod 4$ är lösbar om och endast om $a \equiv 1 \pmod 4$, i vilket fall det finns precis två lösningar;

(iii) kongruensen $x^2 \equiv a \pmod{2^k}$, med $k \geq 3$, är lösbar om och endast om $a \equiv 1 \pmod 8$, i vilket fall det finns exakt fyra lösningar. Om x_0 är en lösning, så ges alla lösningar av $\pm x_0$ och $\pm x_0 + 2^{k-1}$.

Bevis. (i) och (ii) är uppenbara.

(iii) Antag att $x^2 \equiv a \pmod{2^k}$ har en lösning x_0. Då gäller uppenbarligen att $x_0^2 \equiv a \pmod 8$, och talet x_0 är udda eftersom a är udda. Men kvadraten på ett udda tal är kongruent med 1 modulo 8, och följaktligen är $a \equiv 1 \pmod 8$. Detta visar att villkoret $a \equiv 1 \pmod 8$ är nödvändigt för att det ska finnas någon lösning. Vidare är $(-x_0)^2 = x_0^2 \equiv a \pmod{2^k}$ och $(\pm x_0 + 2^{k-1})^2 = x_0^2 \pm 2^k x_0 + 2^{2k-2} \equiv x_0^2 \equiv a \pmod{2^k}$, eftersom $2k - 2 \geq k$. Man verifierar lätt att de fyra talen $\pm x_0$ och $\pm x_0 + 2^{k-1}$ är inkongruenta modulo 2^k. Kongruensen har således minst fyra lösningar om den har en.

Det återstår att verifiera att villkoret på a är tillräckligt för att det ska finnas en lösning samt att det finns högst fyra lösningar. Vi visar tillräckligheten genom induktion över k. Fallet $k = 3$ är klart, eftersom kongruensen $x^2 \equiv 1 \pmod 8$ har lösningen $x \equiv 1$. Antag nu att kongruensen $x^2 \equiv a \pmod{2^k}$ är lösbar och att x_0 är en lösning. Då vet vi att också $\pm x_0$ och $\pm x_0 + 2^{k-1}$ löser kongruensen, och vi ska visa att ett av dessa tal också löser kongruensen

$$x^2 \equiv a \pmod{2^{k+1}}. \tag{3}$$

Vi vet att $x_0^2 = a + 2^k n$ för något heltal n. Om n är jämnt, så är uppenbarligen x_0 en lösning till (3). Om n är udda, så är

$$(x_0 + 2^{k-1})^2 = x_0^2 + 2^k x_0 + 2^{2k-2} = a + 2^k(n + x_0) + 2^{2k-2} \equiv a \pmod{2^{k+1}},$$

beroende på att talet $n + x_0$ är jämnt (eftersom n och x_0 båda är udda tal) och $2k - 2 \geq k + 1$ (eftersom $k \geq 3$). Detta avslutar induktionssteget.

I intervallet $[1, 2^k]$ finns det slutligen 2^{k-3} tal a som är kongruenta med 1 modulo 8. För varje sådant tal a har vi redan hittat 4 olika lösningar till kongruensen $x^2 \equiv a \pmod{2^k}$ i samma intervall, och alla dessa är udda. Sammanlagt har vi alltså $4 \cdot 2^{k-3} = 2^{k-1}$ stycken lösningar. Men det finns exakt 2^{k-1} udda tal i intervallet, så det finns inte utrymme för några fler lösningar. Varje kongruens har följaktligen exakt fyra lösningar. □

Genom att kombinera de två ovanstående satserna med sats 7.5 får vi följande fullständiga svar på frågan om antalet lösningar till kongruensen $x^2 \equiv a \pmod m$.

Sats 11.5 *Låt $m = 2^k p_1^{k_1} \cdots p_r^{k_r}$, där talen p_i är skilda udda primtal, och låt a vara ett tal som är relativt prima mot m. Då är kongruensen $x^2 \equiv a \pmod m$ lösbar om och endast om a är en kvadratisk rest till p_i för varje i samt $a \equiv 1 \pmod 4$ i fallet $k = 2$ och $a \equiv 1 \pmod 8$ i fallen $k \geq 3$.*

Om kongruensen är lösbar, så finns det 2^r lösningar om $k = 0$ eller $k = 1$, 2^{r+1} lösningar om $k = 2$, och 2^{r+2} lösningar om $k \geq 3$.

För att kunna använda sats 11.5 behöver ni något kriterium för när ett tal är en kvadratisk rest till ett givet primtal p. Först noterar vi att det finns lika många kvadratiska rester som kvadratiska ickerester till ett udda primtal.

Sats 11.6 *Låt p vara ett udda primtal. Då finns det exakt $(p-1)/2$ inkongruenta kvadratiska rester till p och lika många kvadratiska ickerester till p.*

Bevis. Alla kvadratiska rester fås genom kvadrering av talen i ett reducerat restsystem. Eftersom varje lösbar kongruens $x^2 \equiv a \pmod{p}$ har exakt två lösningar om $\text{sgd}(a, p) = 1$, följer det att antalet kvadratiska rester är lika med halva antalet element i det reducerad restsystemet, dvs. $(p-1)/2$ stycken. För att erhålla alla kvadratiska rester kan man exempelvis ta $1^2, 2^2, \ldots, [(p-1)/2]^2$. □

Lemma 11.7 *Låt p vara ett udda primtal och antag att $a \not\equiv 0 \pmod{p}$. Då gäller modulo p att*

$$(p-1)! \equiv \begin{cases} a^{(p-1)/2} & \text{om } a \text{ är en kvadratisk ickerest till } p, \\ -a^{(p-1)/2} & \text{om } a \text{ är en kvadratisk rest till } p. \end{cases}$$

Bevis. Kongruensen $mx \equiv a \pmod{p}$ är lösbar för varje heltal m i intervallet $1 \leq m \leq p-1$, dvs. för varje m finns det ett heltal n, sådant att $1 \leq n \leq p-1$ och $mn \equiv a \pmod{p}$. Om kongruensen $x^2 \equiv a \pmod{p}$ saknar lösning, så är $n \neq m$. Om den däremot är lösbar, så har den exakt två lösningar och dessa har formen $x \equiv m_0 \pmod{p}$ och $x \equiv p - m_0 \pmod{p}$, vilket betyder att $n \neq m$ för alla utom två värden på m.

Betrakta nu produkten $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$. Om kongruensen $x^2 \equiv a \pmod{p}$ saknar lösning, så kan vi para ihop de $p-1$ stycken fakroterna i $(p-1)/2$ par så att produkten av de två talen i varje par är kongruent med $a \pmod{p}$, och detta medför att $(p-1)!$ är kongruent med $a^{(p-1)/2}$.

Om å andra sidan kongruensen har två lösningar, m_0 och $p - m_0$, så tar vi undan dessa två tal och parar ihop de återstående $p-3$ talen i $(p-3)/2$ stycken par så att produkten av de två talen i varje par är kongruent med $a \pmod{p}$. Eftersom $m_0(p - m_0) \equiv -m_0^2 \equiv -a \pmod{p}$, följer det att $(p-1)! \equiv -a \cdot a^{(p-3)/2} \equiv -a^{(p-1)/2} \pmod{p}$. □

Nu erinrar vi oss Wilsons sats som vi bevisade tidigare som sats 9.6:

Wilsons sats *Om p är ett primtal så gäller att $(p-1)! \equiv -1 \pmod{p}$.*

Låt oss först notera att vi för $p > 2$ får Wilsons sats som specialfall av lemma 11.7 genom att välja $a = 1$, som uppenbarligen är en kvadratisk rest till varje primtal p. För det andra, och viktigare, får vi genom att kombinera Wilsons sats med lemma 11.7 följande lösbarhetskriterium av Euler.

Sats 11.8 (Eulers kriterium) *Låt p vara ett udda primtal och antag att $p \nmid a$. Då är a en kvadratisk rest till p om $a^{(p-1)/2} \equiv 1 \pmod{p}$ och en kvadratisk ickerest om $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Följande viktiga resultat följer omedelbart av Eulers kriterium.

Sats 11.9 *Låt p vara ett primtal. Då är -1 en kvadratisk rest till p om och endast om $p = 2$ eller $p \equiv 1 \pmod{4}$.*

Bevis. -1 är en kvadratisk rest till 2 eftersom $1^2 = 1 \equiv -1 \pmod{2}$. För udda primtal använder vi Eulers kriterium och noterar att $(-1)^{(p-1)/2} = 1$ om och endast om talet $(p-1)/2$ är jämnt, dvs. om och endast om p är ett primtal på formen $4k + 1$. □

Vi noterar också att Fermats sats är en omedelbar konsekvens av Eulers kriterium, ty genom kvadrering får vi

$$a^{p-1} = \left(a^{(p-1)/2}\right)^2 \equiv (\pm 1)^2 = 1 \pmod{p}.$$

Låt oss slutligen behandla problemet att hitta en lösning till kongruensen $x^2 \equiv a \pmod{p}$ under förutsättning att a är en kvadratisk rest till p. I fallet $p \equiv 3 \pmod{4}$ har vi följande resultat:

Sats 11.10 *Låt p vara ett primtal och antag att $p \equiv 3 \pmod{4}$. Om a är en kvadratisk rest till p, så har kongruensen $x^2 \equiv a \pmod{p}$ de två lösningarna $\pm a^{(p+1)/4}$.*

Bevis. Eftersom a är en kvadratisk rest är $a^{(p-1)/2} \equiv 1 \pmod{p}$, och det följer att

$$\left(\pm a^{(p+1)/4}\right)^2 = a^{(p+1)/2} = a \cdot a^{(p-1)/2} \equiv a \pmod{p}. \qquad \square$$

Observera att det inte är nödvändigt att i förväg verifiera att a är en kvadratisk rest genom att visa att $a^{(p-1)/2} \equiv 1 \pmod{p}$, utan det räcker att beräkna $x \equiv a^{(p+1)/4} \pmod{p}$. Om $x^2 \equiv a \pmod{p}$, så är $\pm x$ de två lösningarna, annars är $x^2 \equiv -a \pmod{p}$, och vi kan sluta oss till att det inte finns några lösningar.

Övningar

11.1 Visa att för varje udda primtal p är
a) $(p-2)! \equiv 1 \pmod{p}$, b) $2 \cdot (p-3)! \equiv -1 \pmod{p}$.

11.2 Visa att för udda primtal p är $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$. Vad har $2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2$ för till beloppet minsta rest modulo p?

11.3 Visa att för varje primtal p är $(k-1)!(p-k)! \equiv (-1)^k \pmod{p}$ för $k = 1, 2, \ldots, p-1$.

11.4 Bestäm en lösning till $x^2 \equiv -1 \pmod{13}$ med hjälp av Wilsons sats.

11.5 Visa att för $k \geq 3$ har kongruensen $x^2 \equiv 1 \pmod{2^k}$ exakt fyra lösningar, nämligen $x \equiv \pm 1, \pm 1 + 2^{k-1} \pmod{2^k}$.

11.6 Vilka är de kvadratiska resterna modulo 23?

11.7 Undersök med hjälp av Eulers kriterium om a) 2 och b) 5 är en kvadratisk rest modulo 17.

11.8 Hur många inkongruenta lösningar har kongruensen a) $x^2 \equiv 2 \pmod{17}$, b) $x^2 \equiv 2 \pmod{17^2}$, c) $x^2 \equiv 2 \pmod{17^{100}}$, d) $x^2 \equiv 2 \pmod{10}$?

11.9 Hur många inkongruenta lösningar har kongruensen $x^2 \equiv 17 \pmod{2^k}$, om k är lika med a) 1, b) 2, c) 3, d) 4, e) 100?

11.10 Hur många inkongruenta lösningar har kongruensen $x^2 \equiv 21 \pmod{m}$, om m är lika med a) 2, b) 4, c) 8, d) 5, e) 20, f) 40, g) 100, h) 500, i) 1000?

11.11 Visa att det finns oändligt många primtal av formen $4k+1$.
[Ledning: Visa att varje primfaktor till $(2n)^2 + 1$ är av formen $4k+1$. Låt sedan $p_1, p_2, \ldots, p_r$ vara primtal av formen $4k+1$ och betrakta talet $N = (2p_1p_2 \cdots p_r)^2 + 1$.]

12 Allmänna kvadratiska kongruenser

En allmän kvadratisk kongruens

$$ax^2 + bx + c \equiv 0 \pmod{m}, \tag{1}$$

kan genom kvadratkomplettering reduceras till ett system bestående av en kongruens på formen $y^2 \equiv d \pmod{m'}$ och en linjär kongruens.

Det enklaste fallet inträffar när $\text{sgd}(4a, m) = 1$, ty då kan vi multiplicera kongruensen (1) med $4a$ utan att behöva ändra modulen m för att få följande ekvivalenta kongruens

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{m},$$

dvs.

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}.$$

Genom att sätta $y = 2ax + b$ erhåller vi följande resultat:

Sats 12.1 *Låt m vara ett udda positivt tal som är relativt prima mot talet a. Då fås alla lösningar till kongruensen*

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

som lösningar till följande system av kongruenser:

$$\begin{cases} y^2 \equiv b^2 - 4ac & \pmod{m} \\ 2ax \equiv y - b & \pmod{m}. \end{cases}$$

Eftersom $\text{sgd}(2a, m) = 1$ har den linjära kongruensen en unik lösning modulo m för varje rot y till den kvadratiska kongruensen.

Exempel 1 Låt oss lösa kongruensen $8x^2 + 5x + 1 \equiv 0 \pmod{23}$. Vi kompletterar först kvadraten genom att multiplicera med 32 och får då $(16x + 5)^2 \equiv 5^2 - 32 = -7 \equiv 16 \pmod{23}$, vilket medför att $16x + 5 \equiv \pm 4$. Lösningen till kongruensen $16x \equiv -1 \pmod{23}$ är $x \equiv 10$, och kongruensen $16x \equiv -9 \pmod{23}$ ger att $x \equiv 21$. Detta innebär att 10 och 21 är de enda lösningarna till den ursprungliga kongruensen. □

När $\text{sgd}(4a, m) > 1$ börjar vi med att faktorisera talet $4a$ som $4a = a_1a_2$ på ett sådant sätt att a_2 och m är relativt prima. Vi kan nu multiplicera kongruensen (1) med a_2 utan att ändra modulen, men när vi sedan multiplicerar med a_1 måste vi ändra modulen till a_1m för att erhålla en ekvivalent kongruens på formen $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{a_1m}$, och den kongruensen kan nu i sin tur skrivas som $(2ax + b)^2 \equiv b^2 - 4ac \pmod{a_1m}$. Detta leder till följande generalisering av sats 12.1.

Sats 12.2 *Skriv talet $4a$ på formen $4a = a_1a_2$, där faktorn a_2 är relativt prima mot m. Då fås alla lösningar till kongruensen*

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

som lösningar till följande system av kongruenser:

$$\begin{cases} y^2 \equiv b^2 - 4ac & \pmod{a_1m} \\ 2ax \equiv y - b & \pmod{a_1m}. \end{cases}$$

EXEMPEL 2 Vi löser kongruensen $3x^2+3x+2 \equiv 0 \pmod{10}$ med hjälp av sats 12.2. Eftersom $4a = 12 = 4 \cdot 3$ och $\text{sgd}(3, 10) = 1$, är den givna kongruensen ekvivalent med kongruensen

$$(6x+3)^2 \equiv 3^2 - 4 \cdot 3 \cdot 2 = -15 \equiv 25 \pmod{40}.$$

Kongruensen $y^2 \equiv 25 \pmod{40}$ har fyra rötter, nämligen 5, 15, 25 och 35. För varje rot y löser vi sedan den linjära kongruensen $6x \equiv y - 3 \pmod{40}$. Lösningarna är i tur och ordning 7, 2, 17 och 12 (mod 20). Den ursprungliga kongruensen har således lösningarna $x \equiv 2$ och $x \equiv 7 \pmod{10}$. □

Övningar

12.1 Skriv följande kongruenser som $y^2 \equiv a \pmod{m}$ och en linjär kongruens:
a) $x^2+4x+5 \equiv 0 \pmod{10}$, b) $x^2+3x+5 \equiv 0 \pmod{10}$,
c) $x^2+3x+5 \equiv 0 \pmod{9}$, d) $3x^2+x+5 \equiv 0 \pmod{9}$.

13 Legendresymbolen och Gauss lemma

Med hjälp av den s.k. Legendresymbolen kan vi på ett enkelt och bekvämt sätt uttrycka att ett heltal är en kvadratisk rest eller kvadratisk ickerest med avseende på ett givet udda primtal. Symbolen definieras på följande vis.

Definition 13.1 Låt p vara ett udda primtal och sätt om a är ett godtyckligt heltal

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{om } a \text{ är en kvadratisk rest till } p, \\ -1 & \text{om } a \text{ är en kvadratisk ickerest till } p, \\ 0 & \text{om } p \mid a. \end{cases}$$

$\left(\frac{a}{p}\right)$ kallas *Legendresymbolen.*

Sats 13.2 *Låt p vara ett udda primtal. Då gäller:*

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(ii) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(iv) *om* $\text{sgd}(a, p) = 1$, *så är* $\left(\frac{a^2}{p}\right) = 1$ *och* $\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right)$,

(v) $\left(\frac{1}{p}\right) = 1$,

(vi) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{om } p \equiv 1 \pmod{4}, \\ -1 & \text{om } p \equiv 3 \pmod{4}. \end{cases}$

Bevis. Kongruensen (i) är självklar om $p \mid a$, och om $\text{sgd}(p, a) = 1$ så är (i) bara en omformulering av Eulers kriterium (sats 11.8). Återstående egenskaper (ii)–(vi) är samtliga enkla konsekvenser av (i). □

Legendresymbolen $\left(\frac{a}{p}\right)$ kan beräknas för godtyckliga heltal a med hjälp av egenskaperna (iii), (iv) och (vi) i sats 13.2 genom faktorisering, om vi känner värdet av $\left(\frac{q}{p}\right)$ för primtal q. För $q = 2$ kommer vi att beräkna symbolen nedan, och för udda primtal q beräknas den enklast med hjälp av Gauss reciprocitetslag som vi ska diskutera i nästa avsnitt. Bevisen för dess dessa resultat bygger på följande hjälpsats.

Lemma 13.3 (Gauss lemma) *Låt p vara ett udda primtal och antag att talet a är relativt prima mot p. Betrakta de minsta positiva resterna modulo p till talen a, $2a$, $3a$, …, $\frac{p-1}{2}a$, och låt N vara antalet sådana rester som är större än $p/2$. Då är $\left(\frac{a}{p}\right) = (-1)^N$.*

Bevis. Talen $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ är relativt prima mot p och parvis inkongruenta modulo p. Låt $r_1, r_2, \ldots, r_N$ representera de minsta positiva resterna som är större än $p/2$, och låt $s_1, s_2, \ldots, s_M$ beteckna de återstående resterna, dvs. de som är mindre än $p/2$. Då är förstås $N + M = (p-1)/2$.

Kvoten q när ja divideras med p är lika med $\lfloor ja/p \rfloor$, dvs. heltalsdelen av ja/p. Det följer att

$$ja = \lfloor ja/p \rfloor\, p + \text{något } r_i \text{ eller något } s_k. \tag{1}$$

Talen $p - r_1$, $p - r_2$, …, $p - r_N$ är positiva och mindre än $p/2$, relativt prima mot p och parvis inkongruenta modulo p. Vidare är inget tal $p - r_i$ lika med något tal s_k. Ty antag att $p - r_i = s_k$, och låt $r_i \equiv ma \pmod p$ och $s_k \equiv na \pmod p$, där m och n är olika tal mellan 1 och $p/2$. Då är $p = r_i + s_k \equiv (m+n)a \pmod p$, och eftersom $\text{sgd}(a, p) = 1$ måste $p \mid (m+n)$, vilket är en motsägelse eftersom $0 < m + n < p$.

Således är $p - r_1$, $p - r_2$, …, $p - r_N$, $s_1, s_2, \ldots, s_M$ olika heltal i intervallet $[1, (p-1)/2]$, och eftersom deras antal är $M + N = (p-1)/2$, är de lika med talen 1, 2, …, $(p-1)/2$ i någon ordning. Därför gäller att

$$(p - r_1)(p - r_2) \cdots (p - r_N) s_1 s_2 \cdots s_M = ((p-1)/2)!,$$

dvs.

$$(-1)^N r_1 r_2 \cdots r_N s_1 s_2 \cdots s_M \equiv ((p-1)/2)! \pmod p.$$

Men talen $r_1, r_2, \ldots, r_N, s_1, s_2, \ldots, s_M$ är också i någon ordning kongruenta med talen a, $2a$, …, $\frac{p-1}{2}a$, och följaktligen är

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^N a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a = (-1)^N a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p.$$

Eftersom varje faktor i $((p-1)/2)!$ är relativt prima mot p, kan vi dividera båda sidorna i den sista kongruensen med $((p-1)/2)!$ med $a^{(p-1)/2} \equiv (-1)^N \pmod p$ som resultat. Slutsatsen i lemmat följer nu av del (i) i sats 13.2. □

Som enkel tillämpning av Gauss lemma ska vi nu beräkna $\left(\frac{2}{p}\right)$.

Sats 13.4 *Låt p vara ett udda primtal. Då är 2 en kvadratisk rest till p om $p \equiv \pm 1 \pmod 8$, och en kvadratisk ickerest till p om $p \equiv \pm 3 \pmod 8$. Detta innebär att*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{om } p \equiv \pm 1 \pmod 8, \\ -1, & \text{om } p \equiv \pm 3 \pmod 8. \end{cases}$$

Bevis. Välj $a = 2$ i Gauss lemma; då är N antalet tal i följden 2, 4, ..., $p-1$ som är större än $p/2$, dvs. N är antalet heltal k sådana att $p/2 < 2k < p$, eller ekvivalent $p/4 < k < p/2$. Följaktligen är $N = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor$. För $p = 4n+1$ blir $N = 2n - n = n$, och för $p = 4n-1$ blir också $N = (2n-1) - (n-1) = n$. Följaktligen är talet N jämnt om n är jämnt, dvs. om if $p = 8m \pm 1$, och N är udda om n är udda, dvs. om $p = 8m \pm 3$. □

Exempel 1 Kongruensen $x^2 \equiv 2 \pmod{17}$ är lösbar eftersom $17 \equiv 1 \pmod 8$. I själva verket löser $x \equiv \pm 6 \pmod{17}$ kongruensen. □

Sats 13.5 *Om p är ett udda primtal och a är ett udda heltal som inte är delbart med p, så är*

$$\left(\frac{a}{p}\right) = (-1)^n, \qquad \text{där } n = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Bevis. Vi ska visa att n har samma paritet som talet N i Gauss lemma, dvs. att $n \equiv N \pmod 2$. Vi använder därvid samma notation som i beviset för lemmat. Genom att summera över j i likheten (1) får vi

$$\sum_{j=1}^{(p-1)/2} ja = p \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{N} r_i + \sum_{k=1}^{M} s_k = pn + \sum_{i=1}^{N} r_i + \sum_{k=1}^{M} s_k. \tag{2}$$

Eftersom talen $(p-r_1)$, $(p-r_2)$, ..., $(p-r_N)$, $s_1, s_2, \ldots, s_M$ är talen 1, 2, ..., $(p-1)/2$ i någon ordning, är

$$\sum_{j=1}^{(p-1)/2} j = \sum_{i=1}^{N} (p - r_i) + \sum_{k=1}^{M} s_k = pN - \sum_{i=1}^{N} r_i + \sum_{k=1}^{M} s_k,$$

och genom att subtrahera detta från ekvation (2) får vi

$$(a-1) \sum_{j=1}^{(p-1)/2} j = p(n-N) + 2 \sum_{i=1}^{N} r_j.$$

Eftersom $a-1$ är ett jämnt tal, är talet $p(n-N)$ jämnt, och det medför att $n - N$ är jämnt. □

Exempel 2 Låt oss använda sats 13.5 för att beräkna $\left(\frac{3}{p}\right)$ för primtal $p \geq 5$. Eftersom

$$\left\lfloor \frac{3j}{p} \right\rfloor = \begin{cases} 0 & \text{om } 1 \leq j \leq \lfloor p/3 \rfloor, \\ 1 & \text{om } \lfloor p/3 \rfloor + 1 \leq j \leq (p-1)/2. \end{cases}$$

följer det att $\left(\frac{3}{p}\right) = (-1)^n$, där $n = (p-1)/2 - \lfloor p/3 \rfloor$. Genom att betrakta fallen $p = 12k \pm 1$ och $p = 12k \pm 5$ var för sig ser vi att n är jämnt om och endast om $p \equiv \pm 1 \pmod{12}$. Följaktligen är $\left(\frac{3}{p}\right) = 1$ om och endast om $p \equiv \pm 1 \pmod{12}$. □

Gauss lemma och sats 13.5 är alltför ohanterliga för numeriska beräkningar av Legendresymbolen $\left(\frac{a}{p}\right)$. Istället använder man Gauss reciprocitetslag som kommer att vara temat i nästa avsnitt.

Övningar

13.1 Är kongruensen $x^2 \equiv 2 \pmod{p}$ lösbar om p är lika med
a) 29, b) 31, c) 97, d) 101 e) 111?

13.2 Beräkna a) $\left(\frac{61}{31}\right)$, b) $\left(\frac{33}{31}\right)$, c) $\left(\frac{29}{31}\right)$, d) $\left(\frac{8}{31}\right)$, e) $\left(\frac{128}{821}\right)$.

13.3 Bestäm $\left(\frac{3}{17}\right)$ med hjälp av a) Gauss lemma, b) sats 13.5, c) Eulers kriterium.

13.4 Låt p vara ett udda primtal och antag att $ab \equiv 1 \pmod{p}$. Visa att om kongruensen $x^2 \equiv a \pmod{p}$ är lösbar, så är också kongruensen $x^2 \equiv b \pmod{p}$ lösbar.

13.5 Låt p vara ett udda primtal och antag att $\text{sgd}(a, p) = \text{sgd}(b, p) = 1$. Visa att om kongruenserna $x^2 \equiv a \pmod{p}$ och $x^2 \equiv b \pmod{p}$ båda saknar lösning, så är kongruensen $x^2 \equiv ab \pmod{p}$ lösbar.

13.6 Visa att för udda primtal p gäller

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{om } p \equiv 1, 3 \pmod{8}, \\ -1 & \text{om } p \equiv 5, 7 \pmod{8}. \end{cases}$$

13.7 Visa att om p är ett udda primtal, så är $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

13.8 Låt a vara en kvadratisk rest till det udda primtalet p. Visa att lösningarna till kongruensen $x^2 \equiv a \pmod{p}$ är
a) $x \equiv \pm a^{n+1} \pmod{p}$, om $p = 4n + 3$,
b) $x \equiv \pm 2^{2n+1} a^{n+1} \pmod{p}$ eller $x \equiv \pm a^{n+1} \pmod{p}$, om $p = 8n + 5$.
Bestäm med hjälp härav lösningarna till
c) $x^2 \equiv -2 \pmod{19}$, d) $x^2 \equiv -1 \pmod{29}$.

14 Kvadratisk reciprocitet

Gauss reciprocitetslag relaterar lösbarheten hos kongruensen $x^2 \equiv p \pmod{q}$, där p och q är skilda udda primtal, till lösbarheten hos $x^2 \equiv q \pmod{p}$. I termer av Legendresymbolen får reciprocitetslagen följande formulering:

Sats 14.1 (Gauss reciprocitetslag) *Låt p och q vara två skilda udda primtal. Då är*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

dvs.

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{om } p \equiv 1 \pmod 4 \text{ eller } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right) & \text{om } p \equiv 3 \pmod 4 \text{ och } q \equiv 3 \pmod 4. \end{cases}$$

Bevis. På grund av sats 13.5 är $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^M(-1)^N = (-1)^{M+N}$, där

$$M = \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] \qquad \text{and} \qquad N = \sum_{j=1}^{(p-1)/2} \left[\frac{jq}{p}\right].$$

Vi skall visa att $M + N = (p-1)(q-1)/4$.

Betrakta för den skull mängden

$$A = \{(j,k) \mid j = 1, 2, \ldots, (p-1)/2 \text{ och } k = 1, 2, \ldots, (q-1)/2\}.$$

Vi kan representera A som en rektangulär mängd av gitterpunkter med heltalskoordinater i ett rätvinkligt koordinatsystem. Eftersom $\text{sgd}(p,q) = 1$ är inget av talen jq/p ett heltal då $j = 1, 2, \ldots, p-1$. Följaktligen ligger ingen punkt i A på linjen $y = \frac{q}{p}x$. Låt B vara mängden av alla punkter i A som ligger under denna linje, dvs. (j,k) ligger i B om och endast om $k < jq/p$. För ett givet j satisfieras detta villkor av $k = 1, 2, \ldots, \lfloor jq/p \rfloor$. Det finns således exakt $\lfloor jq/p \rfloor$ punkter i B med första koordinat j. Eftersom detta gäller för $j = 1, 2, \ldots, (p-1)/2$ är antalet punkter i B lika med N.

Analogt är M lika med antalet punkter i mängden

$$C = \{(j,k) \in A \mid j < kp/q\} = \{(j,k) \in A \mid k > jq/p\}$$

som består av alla punkter i A ovanför linjen $y = \frac{q}{p}x$. Eftersom A är den disjunkta unionen av mängderna B och C, är $M + N$ lika med antalet punkter i A, som är $(p-1)(q-1)/4$.

Detta tal är udda om och endast om talen $(p-1)/2$ och $(q-1)/2$ båda är udda, dvs. om och endast om $p \equiv q \equiv 3 \pmod 4$. De båda Legendresymbolerna $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$ har således motsatta tecken om och endast om $p \equiv q \equiv 3 \pmod 4$. □

EXEMPEL 1 Talet 991 är ett primtal. Beräkna Legendresymbolen $\left(\frac{402}{991}\right)$.

Lösning: Eftersom $402 = 2 \cdot 3 \cdot 67$ behöver vi beräkna följande symboler:

$$\left(\frac{2}{991}\right) = 1. \qquad [991 \equiv -1 \pmod 8]$$

$$\left(\frac{3}{991}\right) = -\left(\frac{991}{3}\right) = -\left(\frac{1}{3}\right) = -1. \qquad [991 \equiv 3 \pmod 4,\ 991 \equiv 1 \pmod 3]$$

$$\begin{aligned}
\left(\frac{67}{991}\right) &= -\left(\frac{991}{67}\right) && [991 \equiv 67 \equiv 3 \pmod 4] \\
&= -\left(\frac{-14}{67}\right) && [991 \equiv -14 \pmod{67}] \\
&= -\left(\frac{-1}{67}\right)\left(\frac{2}{67}\right)\left(\frac{7}{67}\right) && [-14 = (-1)\cdot 2 \cdot 7] \\
&= -(-1)\cdot(-1)\cdot\left(-\left(\frac{67}{7}\right)\right) && [67 \equiv 3 \pmod 8, \quad 7 \equiv 3 \pmod 4] \\
&= \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1. && [67 \equiv 4 \pmod 7]
\end{aligned}$$

Det följer nu att $\left(\frac{402}{991}\right) = \left(\frac{2}{991}\right)\left(\frac{3}{991}\right)\left(\frac{67}{991}\right) = 1 \cdot (-1) \cdot 1 = -1.$ □

EXEMPEL 2 Talet 2137 är ett primtal som är kongruent med 1 modulo 8 och $666 = 2 \cdot 3^2 \cdot 37$. Det följer därför att

$$\left(\frac{666}{2137}\right) = \left(\frac{2}{2137}\right)\left(\frac{37}{2137}\right) = 1 \cdot \left(\frac{2137}{37}\right).$$

Eftersom $2137 \equiv -9 \pmod{37}$ och $37 \equiv 1 \pmod 4$, är vidare

$$\left(\frac{2137}{37}\right) = \left(\frac{-9}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{3^2}{37}\right) = 1.$$

Alltså är $\left(\frac{666}{2137}\right) = 1.$ □

Övningar

14.1 Beräkna a) $\left(\frac{3}{97}\right)$, b) $\left(\frac{123}{97}\right)$, c) $\left(\frac{328}{823}\right)$, d) $\left(\frac{360}{991}\right)$, e) $\left(\frac{1327}{2137}\right)$.

14.2 Vilka av följande kongruenser är lösbara?
a) $x^2 \equiv 7 \pmod{101}$, b) $x^2 \equiv -7 \pmod{101}$,
c) $x^2 \equiv 7 \pmod{303}$, d) $x^2 \equiv 21 \pmod{101}$,
e) $x^2 \equiv 21 \pmod{7171}$, f) $x^2 \equiv 711 \pmod{7171}$.

14.3 Visa att för alla udda primtal p, $p \neq 5$, gäller

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{om } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{om } p \equiv \pm 3 \pmod{10}. \end{cases}$$

14.4 För vilka primtal p är kongruensen $x^2 \equiv -3 \pmod{3p}$ lösbar?

14.5 Bestäm det största primtalet p som är mindre än 100 och för vilket kongruensen $x^2 + 4x + 75 \equiv 0 \pmod p$ är lösbar.

15 Primitiva rötter

Vi börjar med att beräkna potenserna 3^i modulo 7 för $0 \leq i < \phi(7) = 6$ och får då $3^0 = 1$, $3^1 = 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$. Mängden

$$\{3^i \mid 0 \leq i < \phi(7)\}$$

är tydligen ett reducerat restsystem modulo 7, dvs. varje heltal a som inte är delbart med 7 är kongruent modulo 7 med 3^i för ett unikt heltal i modulo $\phi(7)$. Detta förhållande tillåter oss att ersätta beräkningar som enbart använder multiplikation och exponentiering modulo 7 med beräkningar som istället använder addition modulo $\phi(7)$.

EXEMPEL 1 Lös kongruensen $x^5 \equiv 6 \pmod 7$.

Lösning: Sätt $x \equiv 3^y \pmod 7$. Eftersom $6 \equiv 3^3 \pmod 7$ kan den givna kongruensen nu skrivas $3^{5y} \equiv 3^3 \pmod 7$, vilket betyder att $5y \equiv 3 \pmod 6$. Den sistnämnda kongruensen har entydig lösning $y \equiv 3 \pmod 6$, och den ursprungliga kongruensen har således den entydiga lösningen $x \equiv 6 \pmod 7$. □

Motiverade av exempel 1 ska vi nu utforska för vilka tal m som det finns ett tal g sådant att mängden $\{g^i \mid 0 \leq i < \phi(m)\}$ är ett reducerat restsystem modulo m. Att inte alla heltal m har den egenskapen visar följande enkla exempel.

EXEMPEL 2 Eftersom $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$ och $\phi(8) = 4$, är inte $\{a^i \mid 0 \leq i < 4\}$ ett reducerat restsystem modulo 8 för något tal a. □

Sats 15.1 *Låt m vara ett positivt heltal, låt a vara ett tal som är relativt prima mot m och definiera*

$$A = \{k \in \mathbf{Z} \mid a^{|k|} \equiv 1 \pmod m\}.$$

Då är A ett ideal i $\mathbf{Z}$.

Bevis. Vi måste visa att mängden A är sluten under subtraktion, dvs. att

$$j, k \in A \Rightarrow j - k \in A,$$

och vi kan då förstås antaga att $j \geq k$, eftersom $j - k$ tillhör A om och endast om $k - j$ tillhör A.

Så antag att $j, k \in A$. Om $j \geq k \geq 0$, så är $a^j \equiv a^k \equiv 1 \pmod m$, och följaktligen $a^{j-k} \equiv a^{j-k}a^k = a^j \equiv 1 \pmod m$. Om $j \geq 0 > k$, så är $a^j \equiv a^{-k} \equiv 1 \pmod m$, och vi drar slutsatsen att $a^{j-k} = a^j a^{-k} \equiv 1 \cdot 1 = 1 \pmod m$. Om slutligen $0 > j \geq k$, så är $a^{-j} \equiv a^{-k} \equiv 1 \pmod m$, och det följer att $a^{j-k} \equiv a^{-j}a^{j-k} = a^{-k} \equiv 1 \pmod m$. I samtliga fall gäller att $j - k \in A$. □

Observera att mängden A innehåller nollskilda tal eftersom $\phi(m)$ tillhör A enligt Eulers sats. Enligt sats 1.8 genereras idealet A av ett unikt positivt tal h, det minsta positiva heltalet i A. Detta innebär att $a^h \equiv 1 \pmod m$ medan $a^j \not\equiv 1 \pmod m$ för $1 \leq j < h$.

Definition 15.2 Den positiva generatorn till A, dvs. det minsta positiva heltalet h sådant att $a^h \equiv 1 \pmod m$, kallas *ordningen hos a modulo m* och betecknas $\operatorname{ord} a$.

Ordningen $\operatorname{ord} a$ beror naturligtvis av modulen m, men eftersom modulen alltid kommer att vara fixerad under en beräkning kommer denna mångtydighet hos beteckningen inte att förorsaka oss några svårigheter.

För samtliga moduler m är $\operatorname{ord} 1 = 1$.

EXEMPEL 3 Modulo 8 gäller att $\operatorname{ord} 3 = \operatorname{ord} 5 = \operatorname{ord} 7 = 2$. □

EXEMPEL 4 Låt oss beräkna ordningen hos talen 2, 3 and 6 modulo 7. Beräkningarna före exempel 1 visar att $\operatorname{ord} 3 = 6$. Eftersom $2^2 \equiv 4 \pmod 7$ och $2^3 \equiv 1 \pmod 7$, är $\operatorname{ord} 2 = 3$, och eftersom $6^2 \equiv 1 \pmod 7$ är $\operatorname{ord} 6 = 2$. □

Nästa sats är en omedelbar följd av att idealet A genereras av $h = \operatorname{ord} a$.

Sats 15.3 *Antag att* $\operatorname{sgd}(a, m) = 1$ *och sätt* $h = \operatorname{ord} a$ *modulo* m. *Då gällller att*

(i) $a^n \equiv 1 \pmod m$ *om och endast om* $h \mid n$;
(ii) $h \mid \phi(m)$;
(iii) $a^j \equiv a^k \pmod m$ *om och endast om* $j \equiv k \pmod h$;
(iv) talen 1, a, a^2, $\ldots$, a^{h-1} *är inkongruenta modulo* m, *och varje potens* a^n *är kongruent med ett av dessa tal modulo* m;
(v) $\operatorname{ord} a^k = h/\operatorname{sgd}(h, k)$.

Bevis. (i) följer av definitionen av generator till ett ideal.

(ii) följer av (i) och Eulers sats.

(iii) Antag att $k \geq j \geq 0$; då gäller att $a^k \equiv a^j \pmod m$ om och endast om $a^{k-j} \equiv 1 \pmod m$, ty vi kan dividera den förstnämnda kongruensen med a^j eftersom $\operatorname{sgd}(a, m) = 1$. Slutsatsen följer nu av påstående (i).

(iv) är förstås en konsekvens till (iii).

(v) Enligt (i) gäller ekvivalensen $(a^k)^n \equiv 1 \pmod m \Leftrightarrow kn \equiv 0 \pmod h$. Vi kan dividera den högra kongruensen med k förutsatt att vi ändrar modulen till $h/\operatorname{sgd}(h, k)$. Detta innebär att

$$(a^k)^n \equiv 1 \pmod m \Leftrightarrow n \equiv 0 \pmod{h/\operatorname{sgd}(h, k)}.$$

Det minsta positiva heltalet n som uppfyller den sista kongruensen är talet $n = h/\operatorname{sgd}(h, k)$; och detta är per definition ordningen hos talet a^k modulo m. □

Sats 15.3 (ii) medför att $\operatorname{ord} a \leq \phi(m)$ för varje tal a som är relativt prima mot m. Detta leder till följande uppenbara fråga: För vilka tal m finns det ett tal vars ordning är den största möjliga, dvs. $\phi(m)$? Följande definition är motiverad av denna fråga.

Definition 15.4 Antag att $\operatorname{sgd}(g, m) = 1$. Om ordningen hos g modulo m är lika med $\phi(m)$ så kallas g en *primitiv rot modulo* m, eller en *primitiv rot till* m.

EXEMPEL 5 I exempel 4 beräknade vi ordningen hos 3 modulo 7 och fann att $\operatorname{ord} 3 = 6 = \phi(7)$. Alltså är 3 en primitiv rot modulo 7. □

EXEMPEL 6 Inte alla tal har en primitiv rot. Om $m = 8$, så är $a^2 \equiv 1$ för varje udda heltal och således är $\operatorname{ord} a \leq 2 < 4 = \phi(8)$ för varje tal a som är relativt prima mot 8. Detta betyder att 8 saknar primitiva rötter. □

Sats 15.5 *Antag att g är en primitiv rot modulo m. Då gäller att*
(i) $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ *är ett reducerat restsystem modulo m;*
(ii) $g^j \equiv g^k \pmod{m}$ *om och endast om* $j \equiv k \pmod{\phi(m)}$*;*
(iii) g^k *är en primitiv rot modulo m om och endast om* $\operatorname{sgd}(k, \phi(m)) = 1$*. Om det finns en primitiv rot modulo m så finns det således exakt $\phi(\phi(m))$ stycken primitiva rötter.*

Bevis. Sats 15.5 är ett specialfall av sats 15.3. □

EXEMPEL 7 Vi har funnit att 3 är en primitiv rot modulo 7. Eftersom $\phi(\phi(7)) = \phi(6) = 2$, finns det 2 stycken primitva rötter. Den andra är 3^5, dvs. $5 \pmod{7}$. □

Vi ska visa att de enda heltalen med primitiva rötter är 1, 2, 4, p^k och $2p^k$, där p är ett udda primtal och exponenten k är ett godtyckligt positivt heltal. Vi börjar med att visa att varje primtal har primitiva rötter, och för detta behöver vi följande två lemman.

Lemma 15.6 *Om a har ordning h och b har ordning k modulo m, och om* $\operatorname{sgd}(h, k) = 1$*, så har ab ordning hk modulo m.*

Bevis. Låt r vara ordningen hos ab. Eftersom $(ab)^{hk} = (a^h)^k (b^k)^h \equiv 1^k \cdot 1^h = 1 \pmod{m}$, drar vi slutsatsen att $r \mid hk$. Att ordningen hos ab är lika med hk följer därför om vi visar att $hk \mid r$. Vi noterar då först att $b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv 1 \pmod{m}$, och att följaktligen $k \mid rh$. Eftersom talen h och k är relativt prima, medför detta att $k \mid r$, och på analogt sätt fås att $h \mid r$. Slutsatsen $hk \mid r$ följer nu av att $\operatorname{sgd}(h, k) = 1$. □

EXEMPEL 8 Modulo 7 är $\operatorname{ord} 2 = 3$ och $\operatorname{ord} 6 = 2$. Eftersom $2 \cdot 6 \equiv 5 \pmod{7}$ följer det därför av lemma 15.6 att $\operatorname{ord} 5 = \operatorname{ord}(2 \cdot 6) = 3 \cdot 2 = 6$. □

Lemma 15.7 *Låt p och q vara primtal och antag att $q^k \mid (p-1)$. Då existerar det ett tal a med ordning q^k modulo p.*

Bevis. Enligt korollarium 9.9 har kongruensen $x^{q^k} \equiv 1 \pmod{p}$ exakt q^k rötter. Enligt sats 15.3 (i) är en sådan rots ordning en delare till q^k. Om a är en rot med lägre ordning än q^k, så är a rot till kongruensen $x^{q^{k-1}} \equiv 1 \pmod{p}$, men denna kongruens har exakt q^{k-1} rötter. Följaktligen finns det exakt $q^k - q^{k-1}$ inkongruenta tal av ordning q^k.

□

Sats 15.8 *Om p är ett primtal, så finns det exakt $\phi(p-1)$ stycken primitiva rötter modulo p.*

Bevis. På grund av det sista påståendet i sats 15.5, räcker det att visa att det finns minst en primitiv rot modulo p. Låt för den skull $p - 1 = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}$ vara faktoriseringen av $p-1$ i primtalspotensfaktorer. Enligt lemma 15.7 finns det för varje $i = 1, 2, \ldots, r$ ett heltal a_i av ordning $q_i^{k_i}$. Talen $q_i^{k_i}$ är parvis relativt prima, så genom upprepad användning av lemma 15.6 drar vi slutsatsen att $g = a_1 a_2 \cdots a_r$ har ordning $p-1$, dvs. att g är en primitiv rot modulo p. □

Antag att g är en primitiv rot modulo m. Om $\operatorname{sgd}(a, m) = 1$, så följer det

av sats 15.5 att det finns ett unikt tal i sådant att $0 \leq i \leq \phi(m) - 1$ och $g^i \equiv a \pmod{m}$. Detta faktum tillåter oss att göra följande definition.

Definition 15.9 Låt g vara en primitiv rot till m och antag att $\text{sgd}(a, m) = 1$. Det minsta icke-negativa heltalet i sådant att $g^i \equiv a \pmod{m}$ kallas *index av a (i basen g)* och betecknas $\text{ind}\, a$.

Index beror både av modulen m och roten g, men eftersom m och g vanligtvis är givna bör beteckningssättet inte förorsaka några missförstånd.

Läsaren kan naturligtvis inte undgå att se likheterna mellan logaritmer och index. Nästa sats ger de allra viktigaste egenskaperna. Bevisen är enkla och lämnas åt läsaren.

Sats 15.10 *Antag att g är en primitiv rot modulo m, och låt* $\text{ind}\, a$ *beteckna index av a i basen g. Då gäller:*

(i) $\text{ind}\, 1 = 0$ *och* $\text{ind}\, g = 1$*;*

(ii) $a \equiv b \pmod{m}$ *om och endast om* $\text{ind}\, a = \text{ind}\, b$*;*

(iii) $\text{ind}\, ab \equiv \text{ind}\, a + \text{ind}\, b \pmod{\phi(m)}$*;*

(iv) $\text{ind}\, a^k \equiv k\, \text{ind}\, a \pmod{\phi(m)}$ *för alla icke-negativa heltal k.*

Sats 15.11 *Låt m vara ett positivt heltal med primitiv rot och antag att talen a och m är relativt prima. Då har kongruensen $x^n \equiv a \pmod{m}$ en lösning om och endast om*

$$a^{\phi(m)/\text{sgd}(n,\phi(m))} \equiv 1 \pmod{m}. \tag{1}$$

Antalet inkongruenta lösningar är i så fall lika med $\text{sgd}(n, \phi(m))$.

Bevis. Låt g vara en primitiv rot modulo m och sätt $d = \text{sgd}(n, \phi(m))$. Genom att övergå till index ser vi att kongruensen $x^n \equiv a \pmod{m}$ gäller om och endast om $n\, \text{ind}\, x \equiv \text{ind}\, a \pmod{\phi(m)}$. Enligt sats 6.1 är den sistnämnda kongruensen lösbar om och endast om $d \mid \text{ind}\, a$, och om det finns lösningar så finns det exakt d stycken inkongruenta lösningar.

Det återstår att visa att kongruensen (1) gäller om och endast om $d \mid \text{ind}\, a$. Genom att övergå till index ser vi att kongruensen (1) är ekvivalent med kongruensen $(\phi(m)/d)\, \text{ind}\, a \equiv 0 \pmod{\phi(m)}$, vilken gäller om och endast om d delar $\text{ind}\, a$. □

Om modulen har en primitiv rot, så kan vi bestämma lösningarna till en lösbar kongruens $x^n \equiv a \pmod{m}$ genom att använda index, förutsatt att vi beräknar (eller har tillgång till) en tabell över index för den givna modulen m. Jmf. exempel 1

Eftersom varje primtal har en primitiv rot, får vi följande korollarium till sats 15.11 som generaliserar Eulers kriterium (sats 11.8).

Korollarium 15.12 *Antag att p är ett primtal och att* $\text{sgd}(a, p) = 1$. *Då är kongruensen $x^n \equiv a \pmod{p}$ lösbar om och endast om*

$$a^{(p-1)/\text{sgd}(n,p-1)} \equiv 1 \pmod{p}.$$

Anmärkning. Korollariet ger oss en effektiv metod för att avgöra huruvida kongruensen $x^n \equiv a \pmod{p}$ är lösbar men att faktiskt hitta en lösning är

svårare. Detta är emellertid relativt lätt i fallet $\text{sgd}(n, p-1) = 1$: Utnytta Euklides algoritm för att hitta positiva tal s och t sådana att $sn = t(p-1)+1$; för dem är $a^{sn} = a^{t(p-1)}a \equiv a \pmod{p}$, vilket betyder att a^s är en lösning till kongruensen $x^n \equiv a \pmod{p}$.

Följande korollarium generaliserar korollarium 9.9.

Korollarium 15.13 *Antag att m har en primitiv rot och att $n \mid \phi(m)$. Då har kongruensen $x^n - 1 \equiv 0 \pmod{m}$ exakt n rötter.*

Bevis. Kongruensen $x^n \equiv 1 \pmod{m}$ är uppenbarligen lösbar, så det följer av sats 15.11 att den har $\text{sgd}(n, \phi(m))$ inkongruenta lösningar, dvs. n stycken. □

Vi visar härnäst att alla potenser av ett udda primtal har primitiva rötter.

Sats 15.14 *Antag att p är ett udda primtal.*

(i) Om g är en primitiv rot modulo p, så är $g + np$ en primitiv rot modulo p^2 för exakt $p-1$ värden på n modulo p.

(ii) Om g är en primitiv rot modulo p^2, så är g också en primitiv rot modulo p^k för alla $k \geq 2$.

Bevis. Låt h beteckna ordningen hos $g + np$ modulo p^2. (h kan bero av n.) Då gäller att $h \mid \phi(p^2)$, dvs. $h \mid p(p-1)$.

Men $(g+np)^h \equiv 1 \pmod{p^2}$ medför att $(g+np)^h \equiv 1 \pmod{p}$, och enligt binomialsatsen är $(g+np)^h = g^h + \sum_{j=1}^{h} \binom{h}{j}(np)^j g^{h-j} \equiv g^h \pmod{p}$, och följaktligen gäller att $g^h \equiv 1 \pmod{p}$. Eftersom g har ordning $p-1$, följer det att $(p-1) \mid h$.

Alltså är antingen $h = p-1$ eller $h = p(p-1)$. I det sistnämnda fallet är $g + np$ en primitiv rot till p^2, och i det förstnämnda fallet inte. Vi ska visa att det förstnämnda fallet bara inträffar för ett av de p möjliga värdena hos n.

Låt $f(x) = x^{p-1} - 1$; då är g en rot till kongruensen $f(x) \equiv 0 \pmod{p}$ och $f'(g) = (p-1)g^{p-2} \not\equiv 0 \pmod{p}$, eftersom $\text{sgd}(g^{p-2}, p) = 1$. Enligt sats 10.1 har därför kongruensen $f(x) \equiv 0 \pmod{p^2}$ en unik rot på formen $g + np$. Detta bevisar vårt påstående.

(ii) Det räcker att visa att om g är en primitiv rot modulo p^k, $k \geq 2$, så är g också en primitiv rot modulo p^{k+1}. Låt h vara ordningen hos g modulo p^{k+1}; då gäller att $h \mid \phi(p^{k+1})$, dvs. $h \mid p^k(p-1)$. Eftersom $g^h \equiv 1 \pmod{p^{k+1}}$ medför att $g^h \equiv 1 \pmod{p^k}$ och g är en primitiv rot modulo p^k, måste $\phi(p^k)$ vara en delare till h, dvs. $p^{k-1}(p-1) \mid h$.

Därför är antingen $h = p^{k-1}(p-1)$ eller $h = p^k(p-1) = \phi(p^{k+1})$. I det senare fallet är g en primitiv rot modulo p^{k+1} som hävdat. Vi måste visa att det förstnämnda fallet är omöjligt.

Låt $t = \phi(p^{k-1})$; då är $g^t \equiv 1 \pmod{p^{k-1}}$ enligt Eulers sats, och följaktligen $g^t = 1 + np^{k-1}$ för något heltal n. Talet n måste vara relativt prima mot p, ty antagandet $p \mid n$ medför att $g^t \equiv 1 \pmod{p^k}$, vilket strider mot att g är en primitiv rot modulo p^k.

Enligt binomialsatsen är

$$\begin{aligned} g^{pt} = (g^t)^p = (1 + np^{k-1})^p &= 1 + np^k + \frac{p(p-1)}{2}n^2p^{2k-2} + \dots \\ &\equiv 1 + np^k \pmod{p^{k+1}}. \end{aligned}$$

Här har vi använt det faktum att heltalet $\frac{p(p-1)}{2}n^2p^{2k-2} = \frac{p-1}{2}n^2p^{2k-1}$ är delbart med p^{k+1} eftersom $2k-1 \geq k+1$ när $k \geq 2$, och de återstående utelämnade termerna i utvecklingen innehåller högre potenser av p.

Eftersom $p \nmid n$ drar vi nu slutsatsen att

$$g^{pt} \not\equiv 1 \pmod{p^{k+1}}.$$

Därför är $h \neq pt = p\phi(p^{k-1}) = p^{k-1}(p-1)$, och beviset är därmed klart. □

EXEMPEL 9 Eftersom $2^2 \equiv -1 \not\equiv 1 \pmod 5$ drar vi slutsatsen att ordningen hos 2 modulo 5 måste vara 4, så 2 är en primitiv rot till 5. Enligt sats 15.14 är därför $2+5n$ en primitiv rot till 25 för exakt fyra värden på n, $0 \leq n \leq 4$. Eftersom $\phi(25) = 20$ har de primitiva rötterna till 25 ordning 20. Ordningen h modulo 25 av ett godtyckligt tal a är en delare till 20. Om $h < 20$, så gäller antingen att $h \mid 4$ eller att $h \mid 10$, så det följer att $a^4 \equiv 1 \pmod{25}$ eller $a^{10} \equiv 1 \pmod{25}$. För att avgöra om ett tal a har ordning 20 räcker det därför att beräkna a^4 och a^{10} modulo 25; ordningen är 20 om och endast om inga av dessa två potenser är kongruenta med 1. För $a = 2$ får vi $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 6$ och $2^{10} \equiv 24$. Alltså är ordningen hos 2 lika med 20, dvs. 2 är en primitiv rot till 25

För $a = 7$ får vi $7^2 \equiv -1$ och $7^4 \equiv 1 \pmod{25}$, så ordningen hos 7 är 4, och 7 är därför inte en primitiv rot till 25. Det följer nu att 12, 17 och 22 är primitiva rötter till 25.

Enligt sats 15.14 (ii) är 2 en primitiv rot till 5^k för alla k. □

Sats 15.15 *Antag att p är ett udda primtal, och låt g vara en primitiv rot modulo p^k. Om g är udda, så är g också en primitiv rot modulo $2p^k$, och om g är jämnt så är $g+p^k$ en primitiv rot modulo $2p^k$.*

Bevis. Om g är udda, så är $g^j \equiv 1 \pmod 2$ för varje $j \geq 1$. Följaktligen är $g^j \equiv 1 \pmod{2p^k}$ om och endast om $g^j \equiv 1 \pmod{p^k}$, och följaktligen är ordningen hos g modulo $2p^k$ lika med ordningen hos g modulo p^k, nämligen $\phi(p^k)$. Eftersom $\phi(2p^k) = \phi(p^k)$ är g en primitiv rot till $2p^k$.

Om g är jämnt så kan g inte vara en primitiv rot till $2p^k$, ty en primitiv rot är alltid relativt prima mot modulen. Men talet $g+p^k$ är udda och eftersom det är kongruent med g modulo p^k, är det också en primitv rot modulo p^k. Alltså är $g+p^k$ en primitiv rot till $2p^k$ enligt resonemanget i ovanstående stycke. □

EXEMPEL 10 Enligt exempel 9 är 2 en primitiv rot till 5^k för varje k. Följaktligen är $2+5^k$ en primitiv rot till $2 \cdot 5^k$ för varje k. Speciellt är alltså 7 en primitiv rot till 10 och 27 en primitiv rot till 50. Enligt samma exempel är också 17 en primitiv rot till 5^k för varje k, och eftersom 17 är udda följer det att 17 är en primitiv rot till $2 \cdot 5^k$ för varje k. □

Sats 15.16 *De enda talen med primitiva rötter är talen 1, 2, 4, p^k och $2p^k$, där p är ett godtyckligt udda primtal och k är ett godtyckligt positivt heltal.*

Bevis. Vi noterar först att 1, 2 och 4 har primitiva rötter (1, 1 respektive 3), och satserna 15.8, 15.14 och 15.15 medför att p^k och $2p^k$ har primitiva rötter för alla primtal p och alla positiva heltal k.

För att omvänt bevisa att detta är de enda talen med primitiva rötter antar vi att $m > 2$ har en primitiv rot. Enligt korollarium 15.13 har kongruensen

$x^2 \equiv 1 \pmod{m}$ exakt två inkongruenta rötter (eftersom $2 \mid \phi(m)$ för alla $m \geq 3$). Det följer därför av sats 11.5 att m måste vara antingen 4, p^k eller $2p^k$ för något udda primtal p. □

Avslutande anmärkningar. Läsare med grundkunskaper i gruppteori har förmodligen lagt märke till att de flesta begreppen i det här avsnittet är specialfall av allmänna gruppbegrepp.

Om G är en ändlig grupp med enhetselement e, så definieras ordningen $\operatorname{ord} a$ hos ett gruppelement a som det minsta positiva heltalet n som uppfyller likheten $a^n = e$, medan ordningen $\operatorname{ord} G$ hos gruppen definieras som antalet element i G. För $h = \operatorname{ord} a$ gäller att $h \mid \operatorname{ord} G$ och att $\{e, a, a^2, \ldots, a^{h-1}\}$ är en delgrupp till G. Denna delgrupp sammanfaller med G om $\operatorname{ord} a = \operatorname{ord} G$, och gruppen G kallas då *cyklisk* med a som *generator*.

Om vi tillämpar dessa allmänna begrepp på det specialla fallet då G är gruppen $\mathbf{Z}_m^*$ av alla restklasser modulo m som är relativt prima mot m, ser vi att

- ordningen h hos ett tal a modulo m sammanfaller med ordningen hos restklassen $\overline{a}$ i $\mathbf{Z}_m^*$,
- $h \mid \phi(m)$,
- ett tal g är en primitiv rot modulo m om och endast om restklassen $\overline{g}$ genererar gruppen $\mathbf{Z}_m^*$,
- det finns en primitiv rot modulo m om och endast om gruppen $\mathbf{Z}_m^*$ är cyklisk.

Med gruppteorins språk kan vi nu formulera sats 15.16 som följer: Gruppen $\mathbf{Z}_m^*$ är cyklisk om och endast om $m = 1$, 2, 4, p^k eller $2p^k$, där p är ett udda primtal och k är ett godtyckligt positivt heltal.

Övningar

15.1 Vilken ordning modulo 20 har talen a) 3, b) 7, c) 11?

15.2 Bestäm en primitiv rot modulo 14.

15.3 Visa att om $ab \equiv 1 \pmod{m}$, så har a och b samma ordning modulo m.

15.4 2 är en primitiv rot till 101. Vilken ordning modulo 101 har 2^{32}?

15.5 2 är en primitiv rot modulo 19. Hur många primitiva rötter har 19? Bestäm alla primitiva rötter modulo 19.

15.6 a har ordningen h modulo m och ordningen k modulo n, och $\operatorname{sgd}(m, n) = 1$. Vad har a för ordning modulo mn?

15.7 Låt m vara ett tal med primitiva rötter, och antag att a är ett tal som är relativt prima mot m. Visa att a är en primitiv rot till m om och endast om $a^{\phi(m)/p} \not\equiv 1 \pmod{m}$ för varje primfaktor p till $\phi(m)$.

15.8 Konstruera en indextabell för modulen 13.

15.9 Avgör vilka av följande kongruenser som är lösbara:
a) $x^4 \equiv 17 \pmod{67}$, b) $x^4 \equiv 18 \pmod{67}$, c) $x^5 \equiv 17 \pmod{67}$.
Bestäm sedan eventuella lösningar genom att exempelvis utnyttja att 2 är en primitiv rot till 67.

15.10 För vilka primtal p är kongruensen $x^3 \equiv a \pmod{p}$ lösbar för varje a som är relativt prima mot p?

15.11 Bestäm en primitiv rot (för varje $k \geq 1$) till
a) 5^k, b) $2 \cdot 5^k$, c) 7^k, d) $2 \cdot 7^k$.

15.12 Kan 4 vara en primitiv rot modulo ett primtal?

15.13 Bevisa att $\phi(2^n - 1) \equiv 0 \pmod{n}$ för varje $n \geq 2$.
[Ledning: Vad har 2 för ordning modulo $2^n - 1$?]

15.14 Visa att om p är ett udda primtal med primitiv rot g, så är $g^{(p-1)/2} \equiv -1 \pmod{p}$.

15.15 Bevisa Wilsons sats med hjälp av primitiva rötter.

15.16 a) Visa att om p och q är udda primtal och $q \mid (a^p - 1)$, så gäller antingen att $q \mid (a - 1)$ eller att $q = 2kp + 1$ för något k.
b) Visa att primfaktorerna till *Mersennetalen* $M_p = 2^p - 1$, där p är ett primtal, är av formen $2kp + 1$.
c) Visa att $2^{13} - 1$ är ett primtal.

15.17 Låt p vara ett udda primtal.
a) Visa att varje primitiv rot till p är en kvadratisk ickerest till p.
b) Visa att varje kvadratisk ickerest till p är en primitiv rot till p, om och endast om $p = 2^{2^n} + 1$, $n \geq 0$, (dvs. ett s.k. *Fermatprimtal*).
[Ledning: Hur många kvadratiska ickerester finns det och hur många primitiva rötter? Sedan man fått $p = 2^m + 1$, visar man att $m = 2^n$, då p är ett primtal.]

15.18 Visa att om a är udda och $n \geq 3$, så är
a) $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, b) $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$.

15.19 *Carmichaels funktion* λ definieras med hjälp av Eulers ϕ-funktion på följande sätt för talet 1 och för primtalspotenser:

$$\lambda(n) = \begin{cases} \phi(n) & \text{om } n = 1,\ 2,\ \text{eller } 4, \\ \phi(n)/2 & \text{om } n = 2^k \text{ och } k \geq 3, \\ \phi(n) & \text{om } n = p^k \text{ är en potens av ett udda primtal } p. \end{cases}$$

Om slutligen $n = P_1 P_2 \cdots P_k$ är en produkt av olika primtalspotenser P_j, så definieras

$$\lambda(n) = \operatorname{mgm}(\lambda(P_1), \lambda(P_2), \ldots, \lambda(P_k)).$$

a) Visa att $\lambda(n)$ är ett jämnt tal för alla $n \geq 3$.
b) Visa att om $\operatorname{sgd}(a, n) = 1$, så är $a^{\lambda(n)} \equiv 1 \pmod{n}$.
c) Visa att för varje $n \geq 1$ finns det ett tal a vars ordning modulo n är lika med $\lambda(n)$.
d) Beräkna $\lambda(360)$ och $\phi(360)$.
e) Bestäm ett tal av ordning 12 modulo 360.

15.20 Ett *Carmichaeltal* är ett sammansatt tal n med egenskapen att $a^{n-1} \equiv 1 \pmod{n}$ för alla a med $\operatorname{sgd}(a, n) = 1$.
a) Visa att om n är ett Carmichaeltal, så är $n - 1$ en multipel av $\lambda(n)$.
b) Visa att alla Carmichaeltal är udda.
c) Visa att inget Carmichaeltal är delbart med någon primtalskvadrat.
d) Visa att en produkt $n = p_1 p_2 \cdots p_k$ av skilda udda primtal är ett Carmichaeltal om och endast om $(p_i - 1) \mid (n - 1)$ för $i = 1, 2, \ldots, k$.
e) Visa att ett Carmichaeltal måste vara en produkt av minst tre udda primtal.

16 Aritmetiska funktioner

Funktioner med de positiva heltalen som definitionsmängd och de reella talen (eller mer allmänt de komplexa talen) som målmängd kallas *aritmetiska funktioner*.

Vi har redan stött på en mycket viktig aritmetisk funktion – *Eulers ϕ-funktion*. Andra viktiga aritmetiska funktioner som kommer att studeras i det här avsnittet är

- $\tau(n)$, antalet positiva delare till n;
- $\sigma(n)$, summan av de positiva delarna till n;
- $\sigma_k(n)$, summan av k:te potenserna av de positiva delarna till n.

Vi kommer att använda följande konventioner för summor och produkter: $\sum_{d|n} f(d)$ och $\prod_{d|n} f(d)$ betecknar summan respektive produkten av $f(d)$ över alla positiva delare d till n. Exempelvis är $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$.

Med denna notation är

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d, \qquad \sigma_k(n) = \sum_{d|n} d^k.$$

Delarfunktionerna τ och σ kan förstås ses som specialfall av σ_k, eftersom $\tau = \sigma_0$ och $\sigma = \sigma_1$.

Definition 16.1 En aritmetisk funktion f kallas *multiplikativ* om den inte är identiskt noll och uppfyller likheten $f(mn) = f(m)f(n)$ för alla par av relativt prima positiva tal m och n. Om $f(mn) = f(m)f(n)$ för alla par m och n, relativt prima eller ej, sägs f vara *fullständigt multiplikativ*.

Om f är multiplikativ, så är $f(n) = f(n)f(1)$ för varje positivt heltal n, och eftersom det finns något tal n för vilket $f(n) \neq 0$, följer det att $f(1) = 1$. Med hjälp av induktion följer det vidare lätt att om $m_1, m_2, \ldots, m_r$ är parvis relativt prima positiva tal, så är

$$f(m_1 m_2 \cdots m_r) = f(m_1)f(m_2)\cdots f(m_r).$$

Detta gäller speciellt när talen $m_1, m_2, \ldots, m_r$ är potenser av olika primtal. Om $n > 1$ har faktoriseringen $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ som produkt av potenser av olika primtal, så är följaktligen $f(n) = f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_r^{k_r})$. Funktionen f är således fullständigt bestämt av värdena $f(p^k)$ för alla primtalspotenser.

Vi vet redan att Eulers ϕ-funktion är multiplikativ (sats 7.2), och vi har använt denna omständighet för att erhålla en formel för $\phi(n)$.

Vår nästa sats ger en allmän metod för att konstruera multiplikativa funktioner.

Sats 16.2 *Låt f vara en multiplikativ funktion och definiera en ny aritmetisk funktion F genom att sätta*

$$F(n) = \sum_{d|n} f(d).$$

Då är F multiplikativ.

Bevis. Låt m och n vara två relativt prima tal. Om $d \mid mn$, så är $d = d_1 d_2$, där $d_1 \mid m$ och $d_2 \mid n$. Vidare är $d_1 = \text{sgd}(m, d)$, $d_2 = \text{sgd}(n, d)$ och $\text{sgd}(d_1, d_2) = 1$, och faktoriseringen är unik. Följaktligen är

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) f(d_2) \\ &= \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = F(m) F(n). \end{aligned}$$

□

Korollarium 16.3 *(i) Funktionerna τ, σ och σ_k är multiplikativa.*

(ii) Om $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ är den kanoniska primtalsfaktoriseringen av n, så är

$$\tau(n) = \prod_{j=1}^{r} (k_j + 1) \qquad \textit{och} \qquad \sigma(n) = \prod_{j=1}^{r} \left(\frac{{p_j}^{k_j+1} - 1}{p_j - 1} \right).$$

Bevis. (i) Eftersom $\sigma_k(n) = \sum_{d \mid n} d^k$ och funktionen $f(n) = n^k$ är (fullständigt) multiplikativ, följer det av föregående sats att funktionen σ_k är multiplikativ. Funktionerna τ och σ är specialfall av σ_k.

(ii) De positiva delarna till p^k är $1, p, p^2, \ldots, p^k$. Följaktligen är $\tau(p^k) = k+1$ och $\sigma(p^k) = \sum_{j=0}^{k} p^j = (p^{k+1} - 1)/(p - 1)$. Formlerna för $\tau(n)$ och $\sigma(n)$ följer av detta. □

Sats 16.4 *För varje positivt heltal n är $\sum_{d \mid n} \phi(d) = n$.*

Bevis. Sätt $F(n) = \sum_{d \mid n} \phi(d)$; då är funktionen F multiplikativ enligt sats 16.2. Eftersom funktionen $G(n) = n$ också är multiplikativ, räcker det att verifiera att $F(p^k) = p^k$ för alla primtalspotenser p^k för att bevisa att $F(n) = n$ för alla n. Men $\phi(p^j) = p^j - p^{j-1}$ för $j \geq 1$, och alltså är

$$F(p^k) = \sum_{d \mid p^k} \phi(d) = \sum_{j=0}^{k} \phi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k.$$

□

Låt f vara en aritmetisk funktion och sätt $F(n) = \sum_{d \mid n} f(n)$. Är funktionen f entydigt bestämd av funktionen F? Vi har

$$\begin{cases} F(1) = f(1) \\ F(2) = f(1) + f(2) \\ F(3) = f(1) \qquad + f(3) \\ F(4) = f(1) + f(2) \qquad + f(4) \\ F(5) = f(1) \qquad\qquad + f(5) \\ \quad \vdots \\ F(n) = f(1) + \qquad \ldots \qquad + f(n) \end{cases}$$

Detta kan uppfattas som ett triangulärt linjärt ekvationssystem med $f(1)$, $f(2)$, …, $f(n)$ som okända. Det är nu uppenbart att $f(n)$ är en linjärkombination av $F(1)$, $F(2)$, …, $F(n)$ med heltalskoefficienter. Speciellt är alltså funktionen f entydigt bestämd av funktionen F. Vi ska härleda en formel för $f(n)$, och för det ändamålet behöver vi följande funktion:

Definition 16.5 Sätt

$$\mu(n) = \begin{cases} 1 & \text{om } n = 1, \\ 0 & \text{om } n \text{ är delbart med } p^2 \text{ för något primtal } p \\ (-1)^r & \text{om } n = p_1 p_2 \cdots p_r, \text{ där } p_1, p_2, \ldots, p_r \text{ är skilda primtal.} \end{cases}$$

Funktionen μ kallas *Möbius μ-funktion.*

Sats 16.6 *Funktionen μ är multiplikativ och*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{om } n = 1 \\ 0 & \textit{om } n > 1. \end{cases}$$

Bevis. Multiplikativiteten är självklar. Definiera funktionen F genom att sätta $F(n) = \sum_{d|n} \mu(d)$; då är F multiplikativ enligt sats 16.2. Eftersom $\mu(p) = -1$ och $\mu(p^j) = 0$ för $j \geq 2$, är $F(p^k) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0$, för alla primtal p och alla $k \geq 1$. Alltså är $F(n) = 0$ för alla $n > 1$, och $F(1) = \mu(1) = 1$. □

Sats 16.7 (Möbius inversionsformel) *Låt f vara en godtycklig aritmetisk funktion. Om $F(n) = \sum_{d|n} f(d)$ för varje positivt tal n, så är*

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Bevis. Genom att använda definitionen av F och byta summationsordning får vi

$$\begin{aligned} \sum_{d|n} \mu(d) F(n/d) &= \sum_{d|n} \mu(d) \sum_{k|(n/d)} f(k) = \sum_{\text{alla } d,\, k \text{ med } dk \mid n} \mu(d) f(k) \\ &= \sum_{k|n} f(k) \sum_{d|(n/k)} \mu(d). \end{aligned}$$

Enligt sats 16.6 är $\sum_{d|(n/k)} \mu(d) = 0$ utom för $k = n$, när värdet är 1. Följaktligen är $\sum_{d|n} \mu(d) F(n/d) = \sum_{k|n} f(k) \sum_{d|(n/k)} \mu(d) = f(n)$. □

Följande omvändning gäller också.

Sats 16.8 *Om $f(n) = \sum_{d|n} \mu(d) F(n/d)$ för varje positivt heltal n, så är*

$$F(n) = \sum_{d|n} f(d).$$

Bevis. Sätt $G(n) = \sum_{d|n} f(d)$; då är $f(n) = \sum_{d|n} \mu(d) G(n/d)$ enligt sats 16.7. Följaktligen är

$$\sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) G(n/d) \tag{1}$$

för alla n. Vi ska nu använda induktion för att visa att detta medför att $F(n) = G(n)$ för alla positiva heltal n.

Genom att välja $n = 1$ i ekvation (1) får vi först $\mu(1)F(1/1) = \mu(1)G(1/1)$, dvs. $F(1) = G(1)$. Antag sedan att $F(m) = G(m)$ för alla $m < n$. Eftersom $n/d < n$ för alla positiva delare d till n förutom $d = 1$, förenklas nu (1) till $\mu(1)F(n/1) = \mu(1)G(n/1)$, och vi drar slutsatsen att $F(n) = G(n)$. Induktionen är därmed genomförd. □

Övningar

16.1 Bestäm a) $\tau(60)$, b) $\sigma(60)$, c) $\sigma_2(60)$.

16.2 För vilka tal n är
a) $\tau(n) = 4$, b) $\tau(n) = 6$, c) $\sigma(n) = 8$, d) $\sigma(n) = 10$?

16.3 a) Visa att $\tau(n)$ är udda om och endast om $n = m^2$ för något heltal m.
b) Visa att $\sigma(n)$ är udda om och endast om $n = m^2$ eller $n = 2m^2$.

16.4 a) Visa att $\sigma(p^k) = \sigma(p^{k-1}) + p^k$ för alla primtal p och $k \geq 1$.
b) Visa att om f är multiplikativ och uppfyller $f(p^k) = f(p^{k-1}) + p^k$ för alla primtal p och $k \geq 1$, så är $f = \sigma$.

16.5 Visa att $\prod_{d|n} d = n^{\tau(n)/2}$.

16.6 Låt $F(n) = \sum_{d|n} f(d)$. Visa att $\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\lfloor N/k \rfloor$.
Tillämpa speciellt formeln för $f(n) = 1$ och för $f(n) = n$.

16.7 Bestäm $\mu(n)$ för n lika med a) 10, b) 20, c) 30.

16.8 Låt f vara en multiplikativ aritmetisk funktion, och låt n ha den kanoniska primtalsfaktoriseringen $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Visa att

$$\sum_{d|n} \mu(d)f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r)).$$

16.9 Bestäm (t.ex. med hjälp av föregående uppgift)
a) $\sum_{d|n} \mu(d)\tau(d)$, b) $\sum_{d|n} \mu(d)\sigma(d)$, c) $\sum_{d|n} \mu(d)\phi(d)$, d) $\sum_{d|n} |\mu(d)|$.

16.10 Visa att $\sum_{k=1}^{n} \mu(k)\lfloor n/k \rfloor = 1$.

16.11 Visa att om f är en positiv aritmetisk funktion och $F(n) = \prod_{d|n} f(d)$, så är $f(n) = \prod_{d|n} F(d)^{\mu(n/d)}$.

16.12 Låt $F(n) = \sum_{d|n} f(d)$. Visa att om F är multiplikativ, så är f också det.

16.13 Ett *perfekt tal* är ett positivt heltal n sådant att $\sigma(n) = 2n$, t.ex. $n = 6$.
a) Visa att om $2^m - 1$ är ett primtal, så är $n = 2^{m-1}(2^m - 1)$ ett perfekt tal. (Visa också att m måste vara ett primtal för att $2^m - 1$ skall vara ett primtal, ett s.k. Mersenneprimtal.)
b) Visa att varje jämnt perfekt tal n har den i a) angivna formen.

Anm. Det är inte känt om det finns några udda perfekta tal.

17 Summor av kvadrater

I det här avsnittet ska vi behandla problemet att representera positiva heltal som summor av kvadrater. Speciellt kommer vi att avgöra vilka tal som kan skrivas som en summa av två kvadrater, och vi kommer att visa att varje positivt tal kan skrivas som en summa av fyra kvadrater.

Per definition är ett positivt heltal n en summa av två kvadrater om ekvationen $x^2 + y^2 = n$ har en heltalslösning x, y. Eftersom $x^2 \equiv 0$ eller $1 \pmod 4$ för alla heltal x, är det klart att summan $x^2 + y^2$ av två kvadrater aldrig är kongruent med 3 modulo 4. Följaktligen kan inget tal på formen $4m + 3$ vara summan av två kvadrater. För primtal har vi följande nödvändiga och tillräckliga villkor.

Sats 17.1 *Låt p vara ett primtal. Då är p summan av två kvadrater om och endast om $p = 2$ eller $p \equiv 1 \pmod 4$.*

Bevis. Enligt kommentarerna före satsen är inget primtal $\equiv 3 \pmod 4$ summan av två kvadrater, och $2 = 1^2 + 1^2$. Det återstår att visa att varje primtal kongruent med 1 modulo 4 är en summa av två kvadrater.

Så antag att $p \equiv 1 \pmod 4$ och sätt $N = \lfloor \sqrt{p} \rfloor$; då är $N < \sqrt{p} < N + 1$. Talet -1 är en kvadratisk rest till p enligt sats 11.9, och följaktligen finns det ett heltal i sådant att $i^2 \equiv -1 \pmod p$.

Låt A vara mängden av alla par (j, k) där j och k är heltal i intervallet $[0, N]$, låt B beteckna mängden av alla restklasser modulo p, dvs. $B = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$, och definiera slutligen funktionen $f\colon A \to B$ genom att sätta $f(x, y) = \overline{x + iy}$. Eftersom B har p element och A har $(N + 1)^2 > p$ element kan funktionen f inte vara injektiv, utan det måste finnas två skilda par (x_1, y_1) och (x_2, y_2) i A som avbildas på samma restklass, dvs. $x_1 + iy_1 \equiv x_2 + iy_2 \pmod p$.

Sätt $a = x_1 - x_2$ och $b = y_1 - y_2$; då är inte a och b båda lika med noll och $a \equiv -ib \pmod p$, och genom kvadrering fås $a^2 \equiv i^2 b^2 \equiv -b^2 \pmod p$, vilket innebär att $a^2 + b^2$ är en multipel av p. Men $|a| \leq N$ och $|b| \leq N$, och därför är $0 < a^2 + b^2 \leq 2N^2 < 2p$. Det följer att $a^2 + b^2 = p$. □

Lemma 17.2 *Antag att $n = a^2 + b^2$ och att primtalsfaktoriseringen av av talet n innehåller primtalsfaktorn q, där $q \equiv 3 \pmod 4$. Då gäller att*

(i) $q \mid a$ och $q \mid b$;

(ii) q måste förekomma som en jämn potens i primtalsfaktoriseringen av n.

Bevis. (i) Antag att $q \nmid a$. Då finns det ett heltal s sådant att $sa \equiv 1 \pmod q$, och genom att multiplicera kongruensen $a^2 + b^2 \equiv 0 \pmod q$ med s^2 fås

$$(sb)^2 = s^2 b^2 \equiv -s^2 a^2 \equiv -1 \pmod q,$$

dvs. -1 är en kvadratisk rest modulo q. Detta strider enligt sats 11.9 mot antagandet att $q \equiv 3 \pmod 4$. Följaktligen är delar q talet a, och av symmetriskäl delar q också b.

(ii) Eftersom $q \mid a$, $q \mid b$ och $n = a^2 + b^2$, följer det att $q^2 \mid n$. Vi kan således dividera ekvationen $n = a^2 + b^2$ med q^2 och får på så sätt ekvationen $n/q^2 = (a/q)^2 + (b/q)^2$ som visar att talet $n_1 = n/q^2$ är en summa av kvadrater. Om $q \mid n_1$, så visar ovanstående argument att $q^2 \mid n_1$. Genom att fortsätta på detta sätt ser vi att n måste vara delbart med en jämn potens av q. □

Lemma 17.3 *Om m och n båda är summor av två kvadrater, så är deras produkt mn också en summa av två kvadrater.*

Bevis. Om $m = a^2 + b^2$ och $n = c^2 + d^2$, så är

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \qquad \square$$

Sats 17.4 *Låt det positiva heltalet n ha faktoriseringen*

$$n = 2^\alpha \prod_{j=1}^{r} p_j^{\alpha_j} \prod_{j=1}^{s} q_j^{\beta_j},$$

där p_j:na och q_j:na är olika primtal, $p_j \equiv 1 \pmod 4$ och $q_j \equiv 3 \pmod 4$, samt exponenterna α, α_j och β_j är icke-negativa tal. Då kan n skrivas som en summa av två kvadrater om och endast om samtliga exponenter β_j är jämna.

Bevis. Att villkoret är tillräckligt följer genom upprepad användning av föregående lemma, ty 2 och primtalen p_j kan skrivas som summor av två kvadrater enligt sats 17.1, och kvadraten q^2 (på ett godtycklig tal q) är uppenbarligen en summa av två kvadrater ($= q^2 + 0^2$). Nödvändigheten följer omedelbart av lemma 17.2. $\square$

När vi nu har avgjort vilka tal som är summor av två kvadrater, så blir nästa naturliga uppgift att bestämma vilka tal som kan representeras som summor av tre kvadrater. Eftersom de kvadratiska resterna till 8 är 0, 1 och 4, kan summan $a^2 + b^2 + c^2$ av tre kvadrater aldrig vara kongruent med 7 modulo 8. Följaktligen är inget heltal på formen $8m + 7$ representerbart som en summa av tre kvadrater. Det är inte svårt att utvidga argumentet och visa att inget tal på formen $4^k(8m + 7)$ är en summa av tre kvadrater. Omvänt kan varje annat tal skrivas som summan av tre kvadrater. Beviset för detta, som gavs av Gauss, är komplicerat och ges inte här. Den fullständiga karakterisering ser alltså ut så här:

Sats 17.5 *Ett positivt tal kan skrivas som summan av tre kvadrater om och endast om det inte har formen $4^k(8m + 7)$.*

När vi så kommer till frågan att representera ett tal som en summa av fyra kvadrater har vi följande enkla svar.

Sats 17.6 *Varje positivt heltal är en summa av fyra kvadrater.*

Det första fullständiga beviset för detta resultat gavs av Lagrange 1770. Beviset här baseras på följande två lemman.

Lemma 17.7 *Antag att $3m$ är en summa av fyra kvadrater. Då är också m en summa av fyra kvadrater.*

Bevis. Låt $3m = a^2 + b^2 + c^2 + d^2$. Eftersom varje kvadrat är kongruent med 0 eller 1 modulo 3, finns det bara två möjligheter: antingen är alla fyra kvadraterna a^2, b^2, c^2 och d^2 kongruenta med 0 modulo 3, eller också är en av dem, säg a^2, kongruent med 0 medan övriga tre är kongruenta med 1. I det förstnämnda fallet

är $a \equiv b \equiv c \equiv d \equiv 0 \pmod 3$, och i det andra fallet är $a \equiv 0$, $b \equiv \pm 1$, $c \equiv \pm 1$ och $d \equiv \pm 1 \pmod 3$. I båda fallen kan vi därför, genom att vid behov byta tecken på något eller några av talen b, c och d, antaga att $b \equiv c \equiv d \pmod 3$. Det följer att de fyra talen $b+c+d$, $a+b-c$, $a+c-d$ och $a-b+d$ samtliga är delbara med 3, och genom att utveckla kvadraterna nedan och förenkla, finner vi att

$$\left(\frac{b+c+d}{3}\right)^2 + \left(\frac{a+b-c}{3}\right)^2 + \left(\frac{a+c-d}{3}\right)^2 + \left(\frac{a-b+d}{3}\right)^2$$
$$= \frac{3a^2+3b^2+3c^2+3d^2}{9} = \frac{9m}{9} = m,$$

vilket visar att m är en summa av fyra kvadrater. □

Lemma 17.8 *Låt n vara ett kvadratfritt heltal, dvs. n är inte delbart med p^2 för något primtal p. Då finns det heltal a och b sådana att $a^2 + b^2 \equiv -1 \pmod n$.*

Bevis. Vi visar först att resultatet gäller när n är ett primtal p. For $p = 2$ och $p \equiv 1 \pmod 4$ följer det av sats 11.9 att det finns ett tal a sådant att $a^2 \equiv -1 \pmod p$, och vi kan följaktligen komplettera med $b = 0$. Fallet $p \equiv 3 \pmod 4$ återstår, och vi ska ge ett bevis för detta fall som fungerar för alla udda primtal.

Sätt $m = (p-1)/2$ och definiera

$$A = \{0^2, 1^2, 2^2, \ldots, m^2\} \quad \text{och} \quad B = \{-1-0^2, -1-1^2, -1-2^2, \ldots, -1-m^2\}.$$

Elementen i A är inbördes inkongruenta modulo p, ty om $0 \le i \le m$ så har kongruensen $x^2 \equiv i^2 \pmod p$ exakt två rötter $\pm i$ modulo p, och det enda talet x i intervallet $[0, m]$ som är kongruent med $\pm i$ är $x = i$, eftersom $p - i > m$.

På motsvarande sätt fås att elementen i B är inbördes inkongruenta modulo p. Båda mängderna A och B innehåller således $m+1 = (p+1)/2$ inkongruenta tal. Eftersom deras union innehåller $p+1$ tal, följer det att det finns ett element a^2 i A och ett element $-1-b^2$ i B så att $a^2 \equiv -1-b^2 \pmod p$, dvs. $a^2+b^2 \equiv -1 \pmod p$.

Antag nu att $n = p_1 p_2 \cdots p_r$ är en produkt av skilda primtal. För varje primtal p_j väljer vi tal a_j, b_j så att $a_j^2 + b_j^2 \equiv -1 \pmod{p_j}$. Enligt den kinesiska restsatsen finns det tal a och b sådana att $a \equiv a_j \pmod{p_j}$ and $b \equiv b_j \pmod{p_j}$ för alla j. Det följer att $a^2+b^2 \equiv -1 \pmod{p_j}$ gäller för alla j, och detta medför att $a^2 + b^2 \equiv -1 \pmod n$. □

Bevis för sats 17.6. Låt n vara ett positivt tal och skriv talet på formen $n = k^2 m$, där m är kvadratfritt. Om m är en summa av fyra kvadrater, säg $m = a^2 + b^2 + c^2 + d^2$, så är också $n = (ak)^2 + (bk)^2 + (ck)^2 + (dk)^2$ en summa av fyra kvadrater.

Vi kan därför lika gärna från början antaga att talet n är kvadratfritt. Enligt lemma 17.8 finns det då två heltal a och b sådana att $a^2 + b^2 \equiv -1 \pmod n$.

Betrakta alla ordnade par $(ax + by - z, bx - ay - w)$, där x, y, z och w varierar över alla heltal från 0 till $\lfloor\sqrt{n}\rfloor$. Det finns $(1 + \lfloor\sqrt{n}\rfloor)^4 > n^2$ val av kvadrupler (x, y, z, w) men endast n^2 olika ordnade par modulo n. Följaktligen finns det två skilda ordnade kvadrupler (x_1, y_1, z_1, w_1) och (x_2, y_2, z_2, w_2) med alla koordinater liggande i intervallet från 0 till $\lfloor\sqrt{n}\rfloor$, och sådana att

$$ax_1 + by_1 - z_1 \equiv ax_2 + by_2 - z_2 \pmod n \quad \text{och}$$
$$bx_1 - ay_1 - w_1 \equiv bx_2 - ay_2 - w_2 \pmod n.$$

Sätt $x = x_1 - x_2$, $y = y_1 - y_2$, $z = z_1 - z_2$ och $w = w_1 - w_2$. Då gäller att $ax + by \equiv z \pmod{n}$ och $bx - ay \equiv w \pmod{n}$. Därför är

$$(ax + by)^2 + (bx - ay)^2 \equiv z^2 + w^2 \pmod{n}.$$

Men

$$(ax + by)^2 + (bx - ay)^2 = (a^2 + b^2)(x^2 + y^2) \equiv -(x^2 + y^2) \pmod{n}.$$

Det följer att $x^2+y^2+z^2+w^2 \equiv 0 \pmod{n}$, dvs. $x^2+y^2+z^2+w^2 = kn$ för något heltal k. Uppenbarligen är $|x|$, $|y|$, $|z|$ och $|w|$ alla mindre än eller lika med $\lfloor\sqrt{n}\rfloor$, och de är inte alla lika med 0, eftersom de ordnade kvadruplerna (x_1, y_1, z_1, w_1) och (x_2, y_2, z_2, w_2) är olika. Det följer att $0 < x^2 + y^2 + z^2 + w^2 \leq 4[\sqrt{n}]^2 < 4n$, och följaktligen att $k = 1$, 2 eller 3.

Om $k = 1$, så är vi klara, och om $k = 3$, så är $3n$ en summa av fyra kvadrater och talet n självt en summa av fyra kvadrater på grund av lemma 17.7. Antag nu att $k = 2$; eftersom $2n$ är jämnt är antingen inget, två eller fyra av talen x, y, z och w jämna. Om exakt två av talen är jämna, så kan vi antaga att de är x and y. I samtliga fall är då talen $x \pm y$ och $z \pm w$ jämna, och talen $(x \pm y)/2$ och $(z \pm w)/2$ är följaktligen heltal. Men

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = \frac{2x^2 + 2y^2 + 2z^2 + 2w^2}{4}$$
$$= \frac{4n}{4} = n,$$

och talet n är således en summa av fyra kvadrater. Beviset är därmed komplett. □

Samma år som Lagrange bevisade satsen om fyra kvadrater formulerade Waring följande förmoden: Varje tal är summan av 4 kvadrater, 9 kuber, 19 fjärdepotenser, och allmänt en summa av ett bestämt antal k:te potenser. Warings förmodan fick ett positivt svar 1909, då Hilbert bevisade följande sats.

Sats 17.9 *För varje heltal $k \geq 2$ finns det ett minsta heltal $s(k)$ med egenskapen att varje positivt heltal kan skrivas som en summa av $s(k)$ icke-negativa k:te potenser.*

Hilberts bevis är ett rent existensbevis och ger ingen metod för att bestämma $s(k)$. Lagranges sats och det faktum att 7 inte är någon summa av tre kvadrater visar att $s(2) = 4$.

Det är vidare ganska lätt att visa att talet $n = 2^k\lfloor(3/2)^k\rfloor - 1$ inte kan skrivas som en summa med färre än $2^k + \lfloor(3/2)^k\rfloor - 2$ stycken k:te potenser, så därför är $s(k) \geq 2^k + \lfloor(3/2)^k\rfloor - 2$ för alla $k \geq 2$. En förmodan, som med stor sannolikhet är sann, är att i själva verket $s(k) = 2^k + \lfloor(3/2)^k\rfloor - 2$, ty man vet nu att detta gäller för alla utan högst ändligt många k och för alla $k \leq 471\,600\,000$.

Exempelvis är $s(3) = 9$, $s(4) = 19$, $s(5) = 37$ och $s(6) = 73$.

Övningar

17.1 Vilka av talen 98, 343, 735, 1428 och 4680 kan skrivas som en summa av två kvadrater?

17.2 Låt q vara ett primtal på formen $4k+3$. Visa att q^2 inte är summan av två nollskilda kvadrater.

17.3 Visa att 21 inte kan skrivas som summan av kvadraterna på två rationella tal.

17.4 Låt p vara ett primtal. Visa att $p \equiv 1 \pmod 4$ om och endast om p är en delare till $n^2 + (n+1)^2$ för något $n \geq 1$.

17.5 På vilka sätt kan 1547 skrivas som en skillnad mellan två kvadrater av positiva heltal.

17.6 a) Visa att varje udda tal n kan skrivas på formen $n = x^2 - y^2$, där x och y är heltal.
b) Visa att varje heltal n kan skrivas på formen $n = x^2 - y^2 + z^2$, där x, y och z är heltal.

17.7 Visa att om n har formen $4^k(8m+7)$, så är n inte en summa av tre kvadrater.

17.8 Visa att det för att representera talet $n = 2^k\lfloor(3/2)^k\rfloor - 1$ som en summa av k-potenser behövs minst $2^k + \lfloor(3/2)^k\rfloor - 2$ stycken k-potenser.

18 Pythagoreiska tripplar

I det här avsnittet ska vi behandla problemet att bestämma alla rätvinkliga trianglar med sidor av heltalslängd, dvs. bestämma alla heltalslösningar till ekvationen

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

Problemet studerades i Egypten långt före Pythagoras, men han anses ha hittat en formel för att generera oändligt många lösningar.

Definition 18.1 Om x, y och z är positiva heltal och $x^2 + y^2 = z^2$, så kallas (x, y, z) en *pythagoreisk trippel*. Om de tre talen dessutom är parvis relativt prima, så kallas (x, y, z) en *primitiv trippel*.

Sats 18.2 *Om (x, y, z) är en pythagoreisk trippel, så är* $\text{sgd}(x, y) = \text{sgd}(x, z) = \text{sgd}(y, z)$.

Bevis. Antag att $d \mid x$. Om $d \mid y$, så gäller att $d^2 \mid (x^2 + y^2)$, varav följer att $d \mid z$. Och om $d \mid z$, så gäller att $d^2 \mid (z^2 - x^2)$, varför $d \mid y$. Det följer att x och y har samma gemensamma delare som x och z, och speciellt har de två paren samma största gemensamma delare, dvs. $\text{sgd}(x, y) = \text{sgd}(x, z)$. På motsvarande sätt fås $\text{sgd}(x, y) = \text{sgd}(y, z)$. □

Om (x, y, z) är en pythagoreisk trippel och två av de tre talen är relativt prima, så är följaktligen alla tre talen parvis relativt prima, dvs. trippeln är primitiv.

Sats 18.3 *Varje pythagoreisk trippel är en multipel av en primitiv pythagoreisk trippel. Omvänt är varje multipel av en pythagoreisk trippel en pythagoreisk trippel.*

Bevis. Om (x, y, z) är en pythagoreisk trippel och $d = \text{sgd}(x, y)$ är den största gemensamma delaren till x och y, så är uppenbarligen trippeln $(x/d, y/d, z/d)$ en primitiv pythagoreisk trippel enligt sats 18.2, och (x, y, z) är följaktligen en multipel av en primitiv trippel. Omvändningen är uppenbar. □

Sats 18.4 *Antag att (x, y, z) är en primitiv pythagoreisk trippel. Då har talen x och y motsatt paritet, dvs. ett av talen är udda och det andra är jämnt.*

Bevis. Eftersom $\text{sgd}(x, y) = 1$ kan inte båda talen vara jämna. Antag att x och y är udda. Då är $x^2 \equiv y^2 \equiv 1 \pmod 4$ och följaktligen $z^2 \equiv 2 \pmod 4$, vilket är omöjligt. Därför har x och y motsatt paritet. □

För att bestämma alla pythagoreiska tripplar räcker det på grund av sats 18.3 att bestämma alla primitiva tripplar, och då är det ingen inskränkning att antaga att x är udda och y är jämnt, eftersom (x, y, z) är en pythagoreisk trippel om och endast om (y, x, z) är det.

De primitiva pythagoreiska tripplarna (x, y, z) med jämnt y genereras av följande sats.

Sats 18.5 *En trippel (x, y, z) med jämnt y är en primitiv pythagoreisk trippel om och endast om den har formen*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

där a och b är relativt prima positiva heltal av motsatt paritet och $a > b$.

Bevis. Om x, y och z definieras på detta sätt, så är

$$x^2 + y^2 = (a^2 - b^2)^2 + 4(ab)^2 = (a^2 + b^2)^2 = z^2,$$

dvs. (x, y, z) är en pythagoreisk trippel. För att visa att trippeln är primitiv antar vi att $\text{sgd}(x, z) > 1$. Då har x och z en gemensam primtalsdelare p, som måste vara udda eftersom både x och z är udda. Notera att $z + x = 2a^2$ och $z - x = 2b^2$ och att således $p \mid 2a^2$ och $p \mid 2b^2$. Eftersom p är udda följer det nu att $p \mid a$ och $p \mid b$, vilket strider mot antagandet $\text{sgd}(a, b) = 1$. Därför är $\text{sgd}(x, z) = 1$, och det följer nu av sats 18.2 att trippeln (x, y, z) är primitiv.

Antag omvänt att (x, y, z) är en primitiv pythagoreisk trippel med jämnt y. Då måste x och z vara udda. Följaktligen är $z + x$ och $z - x$ jämna tal. Sätt $r = (z + x)/2$ och $s = (z - x)/2$; då är $r > s$, $z = r + s$ och $x = r - s$, så varje gemensam delare till r och s är en gemensam delare till x och z. Eftersom $\text{sgd}(x, z) = 1$ följer det att $\text{sgd}(r, s) = 1$.

Vi noterar nu att $y^2 = z^2 - x^2 = (z + x)(z - x) = 4rs$, så $rs = (y/2)^2$. Talet rs är således en jämn kvadrat, och eftersom r och s är relativt prima, måste r och s också vara jämna kvadrater. Sätt $r = a^2$ och $s = b^2$, där a och b är positiva heltal; då är $a > b$, $x = r - s = a^2 - b^2$, $z = r + s = a^2 + b^2$ och $y = 2\sqrt{rs} = 2ab$. Det är vidare klart att a och b har motsatt paritet, ty annars skulle talet x vara jämnt. Slutligen är $\text{sgd}(a, b) = 1$, eftersom varje gemensam delare till a och b delar både r och s och $\text{sgd}(r, s) = 1$. □

Övningar

18.1 Bestäm alla primitiva pythagoreiska tripplar (x, y, z) med $1 \leq z \leq 30$.

18.2 Bestäm samtliga positiva heltalslösningar x och y till den diofantiska ekvationen $x^2 + y^2 = 130^2$.

18.3 a) Bestäm alla primitiva pythagoreiska tripplar (x, y, z) med $y = 40$.
b) Bestäm alla pythagoreiska tripplar (x, y, z) med $y = 40$.

18.4 Visa att i varje pythagoreisk trippel är
a) minst ett tal delbart med 3,
b) minst ett tal delbart med 4,
c) minst ett tal delbart med 5.

18.5 Visa att för varje heltal $n \geq 3$ finns det en pythagoreisk triangel med en sida av längd n.

18.6 Bestäm alla pythagoreiska trianglar som har en sida av längd
a) 12, b) 13.

18.7 Visa att det finns oändligt många pythagoreiska tripplar (x, y, z) med $z = y + 1$.

19 Fermats sista sats

”Jag har ett i sanning underbart bevis för detta påstående, men marginalen är alltför trång för att rymma detsamma.” Denna berömda kommentar krafsade Fermat ner 1637 i marginalen på sitt exemplar av Diofantos bok *Arithmetica* som tillägg till en annan marginalanteckning som med modern terminologi lyder som följer:

Sats 19.1 (Fermats sista sats) *Ekvationen $x^n + y^n = z^n$ har ingen lösning i nollskilda heltal om $n \geq 3$.*

Det är troligt att Fermat hade ett bevis för fallet $n = 4$ och att han felaktigt trodde att hans argument kunde generaliseras till att täcka det allmänna fallet. I mer än tre och ett halvt sekel försökte ett stort antal matematiker förgäves att bevisa Fermats förmodan, och under detta sökande efter ett bevis utvecklades många nya fruktbara matematiska begrepp och teorier. I början av 1990-talet var det känt att Fermats förmodan var sann för alla exponenter n med en udda primtalsfaktor mindre än 10^6.

I juni 1993 meddelade så Andrew Wiles att han hade ett bevis för Fermats sats, men det ursprungliga beviset visade sig innehålla några luckor. Dessa täpptes till ett år senare av Wiles och Richard Taylor. Fermats *förmodan* hade därigenom slutligen upphöjts till *sats*. Beviset är mycket långt och använder många djupa resultat från algebraisk geometri.[1]

Vi ska visa Fermats sista sats i fallet $n = 4$. Detta följer av följande något starkare resultat.

Sats 19.2 *Ekvationen $x^4 + y^4 = z^2$ har ingen lösning i nollskilda heltal.*

Bevis. Antag motsatsen; då finns det en lösning med positiva heltal x, y och z, eftersom trippeln $(|x|, |y|, |z|)$ löser ekvationen om (x, y, z) gör det.

[1] En populär beskrivning av den fascinerande jakten på en lösning till Fermats förmodan finns i boken *Fermats gåta* av Simon Singh, MånPocket, 1999.

Låt därför x, y och z vara en positiv lösning, där z är så litet som möjligt. Vi ska härleda en motsägelse genom att visa att det finns en annan positiv lösning (x_1, y_1, z_1) med $z_1 < z$.

Antag att $\text{sgd}(x, y) > 1$; då finns det ett primtal p som delar både x och y. Det följer att $p^4 \mid (x^4 + y^4)$ och att följaktligen $p^4 \mid z^2$ och $p^2 \mid z$. Alltså är $(x/p)^4 + (y/p)^4 = (z/p^2)^2$, och vi har därmed hittat en positiv lösning med ett mindre z-värde, vilket strider mot vårt ursprungsval (x, y, z).

Vi drar slutsatsen att $\text{sgd}(x, y) = 1$. Det följer att $\text{sgd}(x^2, y^2) = 1$, och trippeln (x^2, y^2, z) är följaktligen en primitiv pythagoreisk trippel. Vi kan förstås antaga att x^2 är udda och y^2 är jämnt, och enligt sats 18.5 betyder detta att det finns relativt prima tal u och v sådana att

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad z = u^2 + v^2.$$

Speciellt är alltså (x, v, u) en primitiv pythagoreisk trippel med udda tal x. Därför finns det relativt prima heltal s och t sådana att

$$x = s^2 - t^2, \quad v = 2st, \quad u = s^2 + t^2.$$

Eftersom $\text{sgd}(s, t) = 1$, följer det av den sista likheten att u, s och t är parvis relativt prima. Men $(y/2)^2 = uv/2 = ust$, så produkten ust är en jämn kvadrat, och detta medför att u, s och t alla tre är jämna kvadrater. Det finns således positiva heltal a, b och c sådana att $s = a^2$, $t = b^2$ och $u = c^2$. Eftersom $u = s^2 + t^2$, följer det att $a^4 + b^4 = c^2$, dvs. (a, b, c) är en positiv lösning till vår ursprungliga ekvation. Men detta strider mot att (x, y, z) är en lösning med minimalt z, ty $c = \sqrt{u} \leq u^2 < u^2 + v^2 = z$, och därmed är motsägelsebeviset klart. □

Korollarium 19.3 *Ekvationen $x^4 + y^4 = z^4$ har ingen lösning i nollskilda heltal.*

Bevis. Om (x, y, z) är en sådan lösning, så är (x, y, z^2) en lösning till ekvationen i sats 19.2. Detta är en motsägelse. □

Övningar

19.1 Bestäm alla positiva heltalslösningar till ekvationen $x! + y! = z!$.

19.2 Bestäm alla positiva heltalslösningar till ekvationen $xy = 2(x + y)$.

19.3 Visa att för att bevisa Fermats stora sats räcker det att bevisa den i det fall då exponenten är ett udda primtal.

19.4 Visa att ekvationen $x^4 + y^2 = z^4$ saknar positiva heltalslösningar.

19.5 Visa att det inte finns några positiva heltal x, y sådana att både $x^2 + y^2$ och $x^2 - y^2$ är kvadrattal.

19.6 Visa att i en pythagoreisk trippel kan högst ett tal vara ett kvadrattal.

19.7 Visa att $x^4 + 4y^4 = z^2$ saknar positiva heltalslösningar.

19.8 Visa att ingen pythagoreisk triangel har en area som är ett kvadrattal.

20 Kedjebråk

I det här avsnittet ska vi beskriva en teknik för att skriva reella tal som upprepade följder av bråk. Exempelvis kan det rationella talet 157/30 utvecklas på följande sätt:

$$\frac{157}{30} = 5 + \frac{7}{30} = 5 + \frac{1}{\frac{30}{7}} = 5 + \frac{1}{4 + \frac{2}{7}} = 5 + \frac{1}{4 + \frac{1}{\frac{7}{2}}} = 5 + \frac{1}{4 + \frac{1}{3 + \frac{1}{2}}}$$

och det sista uttrycket kallas ett kedjebråk. Kedjebråket ovan är ändligt, men för att utveckla irrationella tal behövs det oändliga kedjebråk − till exempel är

$$\begin{aligned}\sqrt{2} + 1 &= 2 + (\sqrt{2} - 1) = 2 + \frac{1}{\sqrt{2} + 1} = 2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} \\ &= 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}}\end{aligned}$$

Vi börjar med att ge en formell definition av ändliga kedjebråk. Trots att vi primärt är intresserade av kedjebråk med heltalstermer är det lämpligt med en mer generell definition.

Definition 20.1 Låt $a_0, a_1, \ldots, a_n$ vara reella tal som samtliga är positiva utom möjligtvis a_0. Uttrycket

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

kallas ett *ändligt kedjebråk* och betecknas $\langle a_0, a_1, \ldots, a_n \rangle$. Talen a_k kallas kedjebråkets *termer* eller *delkvoter*.

För den som inte är nöjd med prickarna i definitionen följer här en rekursiv definition:

$$\begin{aligned}\langle a_0 \rangle &= a_0, \\ \langle a_0, a_1, \ldots, a_n \rangle &= a_0 + \frac{1}{\langle a_1, a_2, \ldots, a_n \rangle} \quad \text{om } n \geq 1.\end{aligned}$$

Antagandet att samtliga termer utom eventuellt a_0 är positiva garanterar att kedjebråken $\langle a_k, a_{k+1}, \ldots, a_n \rangle$ är positiva för $k \geq 1$, och att det därför aldrig kan bli fråga om någon division med noll i ovanstående definition.

Följande sätt att komprimera ett kedjebråk genom att uppfatta det som sammansatt av två kortare kedjebråk är användbart i induktiva resonemang.

Sats 20.2 *(i) För $0 \le k \le n$ är*

$$\langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, a_1, \ldots, a_{k-1}, \langle a_k, a_{k+1}, \ldots, a_n\rangle\rangle.$$

(ii) För $n \ge 1$ är

$$\langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, a_1, \ldots, a_{n-2}, a_{n-1} + 1/a_n\rangle.$$

Bevis. (i) Fallet $k = 0$ följer direkt av den rekursiva definitionen. För $k = n = 1$ är vidare $\langle b_0, b_1\rangle = b_0 + 1/\langle b_1\rangle = b_0 + 1/b_1$, varav följer att

$$\langle a_0, a_1, \ldots, a_n\rangle = a_0 + 1/\langle a_1, \ldots, a_n\rangle = \langle a_0, \langle a_1, a_2, \ldots, a_n\rangle\rangle$$

för alla $n \ge 1$.

Likheten i (i) gäller följaktligen för $k = 1$. Antag nu induktivt att den gäller för alla kedjebråk då $k = p < n$. Genom att använda induktionsantagandet en gång och fallet $k = 1$ två gånger får vi

$$\begin{aligned}\langle a_0, a_1, \ldots, a_n\rangle &= \langle a_0, \langle a_1, a_2, \ldots, a_n\rangle\rangle \\ &= \langle a_0, \langle a_1, a_2, \ldots, a_p, \langle a_{p+1}, \ldots, a_n\rangle\rangle\rangle \\ &= \langle a_0, a_1, a_2, \ldots, a_p, \langle a_{p+1}, \ldots, a_n\rangle\rangle,\end{aligned}$$

vilket visar att likheten också gäller för $k = p+1$. Därmed är induktionsbeviset klart.

(ii) är det specialfall av (i) som fås genom att välja $k = n - 2$. □

Oändliga kedjebråk definieras som gränsvärden av ändliga kedjebråk på ett uppenbart sätt.

Definition 20.3 Låt $(a_n)_{n=0}^{\infty}$ vara en följd av reella tal, alla positiva utom eventuellt a_0. Följden $(\langle a_0, a_1, \ldots, a_n\rangle)_{n=0}^{\infty}$ kallas ett *oändligt kedjebråk* och betecknas $\langle a_0, a_1, a_2, \ldots\rangle$. Det oändliga kedjebråket sägs *konvergera* om gränsvärdet

$$\lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n\rangle$$

existerar, och i detta fall betecknas också gränsvärdet $\langle a_0, a_1, a_2, \ldots\rangle$.

För att avgöra om ett givet oändligt kedjebråk är konvergent behöver vi studera de ändliga kedjebråken $\langle a_0, a_1, \ldots, a_n\rangle$ för växande värden på n. Antag nu att vi har beräknat värdet på $\langle a_0, a_1, \ldots, a_n\rangle$ och vill beräkna värdet på nästa kedjebråk $\langle a_0, a_1, \ldots, a_n, a_{n+1}\rangle$ utan att behöva göra om alla räkningar från början. Rekursionsformeln i definitionen är då inte till någon nytta eftersom den definierar $\langle a_0, a_1, \ldots, a_n, a_{n+1}\rangle$ i termer av a_0 och $\langle a_1, \ldots, a_n, a_{n+1}\rangle$ och inte i termer av $\langle a_0, a_1, \ldots, a_n\rangle$ och a_{n+1}. Lyckligtvis finns det ett enkelt sätt, som vi nu ska beskriva, att beräkna kedjebråken $\langle a_0, a_1, \ldots, a_n\rangle$ i följd.

Definition 20.4 Låt $(a_n)_{n=0}^{N}$ vara en ändlig ($N \in \mathbf{N}$) eller oändlig ($N = \infty$) följd av reella tal som alla är positiva utom möjligtvis a_0, och definiera två följder $(p_n)_{n=-2}^{N}$ och $(q_n)_{n=-2}^{N}$ rekursivt på följande vis:

$$\begin{aligned} &p_{-2} = 0,\ \ p_{-1} = 1,\ \ p_n = a_n p_{n-1} + p_{n-2} \quad \text{om } n \ge 0, \\ &q_{-2} = 1,\ \ q_{-1} = 0,\ \ q_n = a_n q_{n-1} + q_{n-2} \quad \text{om } n \ge 0. \end{aligned}$$

Paret (p_n, q_n), och kvoten p_n/q_n (där $n \ge 0$), kallas den *n:te konvergenten* till den givna följden $(a_n)_{n=0}^{N}$ och till motsvarande kedjebråk.

Uppenbarligen är $q_0 = 1$ och $q_n > 0$ för alla $n \geq 0$. Följden $(q_n)_{n=0}^N$ är således en positiv följd.

Sambandet mellan kedjebråk och konvergenter ges av nästa sats, som också innehåller några betydelsefulla identiteter.

Sats 20.5 *Låt $(a_n)_{n=0}^N$ vara en följd av reella tal, alla positiva utom möjligtvis a_0, och låt (p_n, q_n) vara motsvarande konvergenter. Sätt $c_n = p_n/q_n$; då är*

(i)	$\langle a_0, a_1, \ldots, a_n\rangle = c_n$	*för alla $n \geq 0$;*
(ii)	$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$	*om $n \geq -1$;*
(iii)	$c_n - c_{n-1} = (-1)^{n-1}/q_{n-1}q_n$	*om $n \geq 1$;*
(iv)	$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$	*om $n \geq 0$;*
(v)	$c_n - c_{n-2} = (-1)^n a_n/q_{n-2}q_n$	*om $n \geq 2$.*

Bevis. (i): Fallet $n = 0$ är trivialt eftersom $c_0 = p_0/q_0 = a_0/1 = a_0$.

Antag induktivt att (i) gäller för alla kedjebråk med n termer, och låt $\langle a_0, a_1, \ldots, a_n\rangle$ vara ett kedjebråk med $n+1$ termer. Eftersom

$$\langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, a_1, \ldots, a_{n-2}, a_{n-1} + 1/a_n\rangle$$

och kedjebråket i högerledet har n termer och dess $(n-1)$:a konvergent är $((a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}), (a_{n-1} + 1/a_n)q_{n-2} + q_{n-3})$, drar vi slutsatsen att

$$\begin{aligned}\langle a_0, a_1, \ldots, a_n\rangle &= \frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} = \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} \\ &= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.\end{aligned}$$

Därmed är induktionssteget klart.

(ii) Sätt $z_n = p_n q_{n-1} - p_{n-1} q_n$. Genom att utnyttja de rekursiva definitionerna får vi

$$\begin{aligned}z_n &= p_n q_{n-1} - p_{n-1} q_n = (a_n p_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= p_{n-2}q_{n-1} - p_{n-1}q_{n-2} = -z_{n-1},\end{aligned}$$

för $n \geq 0$, varav följer att $z_n = (-1)^{n-1} z_{-1}$. Men $z_{-1} = 1$ beroende på att $p_{-1} = q_{-2} = 1$ och $p_{-2} = q_{-1} = 0$. Följaktligen är $z_n = (-1)^{n-1}$, vilket är vad som skulle visas.

(iii) följer av (ii) genom division med $q_{n-1}q_n$, som är ett nollskilt tal för $n \geq 1$.

(iv) Med hjälp av de rekursiva definitionerna av p_n och q_n samt likheten (ii) får vi

$$\begin{aligned}p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2})q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = a_n(-1)^{n-2} = (-1)^n a_n.\end{aligned}$$

(v) följer av (iv) genom division med $q_{n-2}q_n$. □

Exempel 1 För att med hjälp av sats 20.5 beräkna värdet av kedjebråket $\langle -2, 5, 4, 3, 2, 1\rangle$ behöver vi konvergenterna (p_5, q_5). Dessa beräknas rekursivt med hjälp av formlerna i definition 20.4. Resultaten av beräkningarna har sammanfattats i följande tabell:

n	-2	-1	0	1	2	3	4	5
a_n			-2	5	4	3	2	1
p_n	0	1	-2	-9	-38	-123	-284	-407
q_n	1	0	1	5	21	68	157	225

För att exempelvis beräkna $p_4 = a_4p_3 + p_2$ multiplicerar vi $a_4 = 2$ med det sist beräknade p-värdet p_3 ($= -123$) och adderar den föregående termen p_2 ($= -38$) med $p_4 = 2(-123) + (-38) = -284$ som resultat. Slutligen noterar vi att $\langle -2, 5, 4, 3, 2, 1\rangle = p_5/q_5 = -407/225$. De successiva konvergenterna är -2, $-9/5$, $-38/21$, $-123/68$, $-284/157$ och $-407/225$. □

Korollarium 20.6 *Låt $(a_n)_{n=0}^N$ vara en ändlig eller oändlig följd av reella tal, alla positiva utom möjligtvis a_0, med konvergenter $c_n = p_n/q_n$. Konvergenterna c_{2i} med jämna index bildar en strikt växande följd, konvergenterna c_{2j+1} med udda index bildar en strikt avtagande följd, och för alla i och j är $c_{2i} < c_{2j+1}$, dvs.*

$$c_0 < c_2 < \cdots < c_{2i} < \cdots < c_{2j+1} < \cdots < c_3 < c_1.$$

Bevis. Enligt sats 20.5 (v) är $c_n - c_{n-2} = (-1)^n a_n/q_nq_{n-2}$. Om $n \geq 2$ är jämnt är följaktligen $c_n - c_{n-2} > 0$, och om $n \geq 3$ är udda så är $c_n - c_{n-2} < 0$.

Enligt sats 20.5 (iii) är vidare $c_{2k+1} - c_{2k} = 1/q_{2k}q_{2k+1} > 0$. För $j \geq i$ får vi därför olikheten $c_{2j+1} > c_{2j} \geq c_{2i}$, och för $j < i$ olikheten $c_{2j+1} > c_{2i+1} > c_{2i}$. I båda fallen är $c_{2j+1} > c_{2i}$. □

Exempel 2 I exempel 1 beräknade vi kedjebråket $\langle -2, 5, 4, 3, 2, 1\rangle$ och dess successiva konvergenter, och helt i enlighet med korollarium 20.6 gäller det för dessa konvergenter att

$$-2 < -\frac{38}{21} < -\frac{284}{157} < -\frac{407}{225} < -\frac{123}{68} < -\frac{9}{5}.$$ □

Låt $(a_n)_{n=0}^\infty$ vara en följd av reella tal, samtliga positiva utom eventuellt a_0, och med konvergenter $c_n = p_n/q_n$. Enligt sats 20.5 är $c_n = \langle a_0, a_1, \ldots, a_n\rangle$, och korollarium 20.6 medför att följden $(c_{2k})_{k=0}^\infty$ av konvergenter med jämna index är strängt växande och uppåt begränsad av c_1. Gränsvärdet $c' = \lim_{k\to\infty} c_{2k}$ existerar följaktligen. Analogt är följden $(c_{2k+1})_{k=0}^\infty$ strängt avtagande och nedåt begränsad av c_0, så gränsvärdet $c'' = \lim_{k\to\infty} c_{2k+1}$ existerar också. Uppenbarligen är vidare $c_{2k} < c' \leq c'' < c_{2k+1}$ för alla k.

Gränsvärdet

$$c = \lim_{n\to\infty} c_n = \lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n\rangle,$$

som existerar om och endast om $c' = c''$, existerar följaktligen om och endast om $c_{2k+1} - c_{2k} \to 0$ då $k \to \infty$. Enligt sats 20.5 är $0 < c_{2k+1} - c_{2k} < 1/q_{2k}q_{2k+1}$. Ett tillräckligt villkor för att gränsvärdet c ska existera, dvs. för att det oändliga kedjebråket $\langle a_0, a_1, a_2, \ldots\rangle$ ska vara konvergent, är därför att $\lim_{n\to\infty} q_n = \infty$, och vår nästa sats ger ett villkor på följden $(a_n)_{n=0}^\infty$ som garanterar just detta.

Sats 20.7 *Låt $(a_n)_{n=0}^\infty$ vara en följd med konvergenter (p_n, q_n) och antag att det finns en konstant $\alpha > 0$ sådan att $a_n \geq \alpha$ för alla $n \geq 1$. Då finns det två konstanter $r > 1$ och $C > 0$ sådana att $q_n \geq Cr^n$ för alla $n \geq 0$, och speciellt är därför $\lim_{n\to\infty} q_n = \infty$.*

Om $a_n \geq 1$ för alla $n \geq 1$, så är följden $(q_n)_{n=1}^\infty$ vidare strängt växande.

Bevis. Antagandena medför att $q_n = a_n q_{n-1} + q_{n-2} \geq \alpha q_{n-1} + q_{n-2}$ för $n \geq 1$. Låt r beteckna den positiva roten till andragradsekvationen $x^2 = \alpha x + 1$, dvs. $r = \alpha/2 + \sqrt{1 + \alpha^2/4}$, och låt C beteckna det minsta av de två talen 1 och a_1/r. Då är $q_0 = 1 \geq Cr^0$ och $q_1 = a_1 \geq Cr^1$, och vi påstår att $q_n \geq Cr^n$ för alla $n \geq 0$. Påståendet följer genom induktion, ty om $q_k \geq Cr^k$ för $0 \leq k \leq n-1$, så är $q_n \geq \alpha Cr^{n-1} + Cr^{n-2} = Cr^{n-2}(\alpha r + 1) = Cr^{n-2} \cdot r^2 = Cr^n$. Uppenbarligen är $r > 1$, och det följer därför att $q_n \to \infty$ då $n \to \infty$.

Om $a_n \geq 1$ för alla $n \geq 1$, så är $q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} > q_{n-1}$ för $n \geq 2$, vilket betyder att följden $(q_n)_{n=1}^{\infty}$ är strängt växande. □

Definition 20.8 En följd $(a_n)_{n=0}^{\infty}$ av reella tal kommer att kallas *trevlig* om det för någon positiv konstant α gäller att $a_n \geq \alpha$ för alla $n \geq 1$.

En följd $(a_n)_{n=0}^{\infty}$ av heltal, som samtliga är positiva utom eventuellt a_0, är uppenbarligen en trevlig följd med $\alpha = 1$, och för sådana följder är motsvarande följd $(q_n)_{n=1}^{\infty}$ strängt växande och obegränsad.

Diskussionen som föregick sats 20.7 kan nu sammanfattas på följande vis.

Sats 20.9 *Låt $(a_n)_{n=0}^{\infty}$ vara en trevlig följd med konvergenter $c_n = p_n/q_n$. Det oändliga kedjebråket $\xi = \langle a_0, a_1, a_2, \dots \rangle$ är då konvergent och uppfyller för alla $n \geq 0$ olikheterna*

$$c_{2n} < \xi < c_{2n+1} \qquad \textit{och} \tag{1}$$

$$\frac{a_{n+2}}{q_n q_{n+2}} < |\xi - c_n| < \frac{1}{q_n q_{n+1}}. \tag{2}$$

Bevis. Det återstår bara att bevisa olikheten (2). Enligt (1) tillhör talet ξ intervallet med c_n och c_{n+1} som ändpunkter för varje $n \geq 0$. Följaktligen är

$$|\xi - c_n| < |c_{n+1} - c_n| = \frac{1}{q_n q_{n+1}},$$

där den sista likheten följer av sats 20.5 (iii).

Vidare ligger talet c_{n+2} strikt mellan talen c_n och ξ. Följaktligen är

$$|\xi - c_n| > |c_{n+2} - c_n| = \frac{a_{n+2}}{q_n q_{n+2}},$$

där den sista likheten följer av sats 20.5 (v). Därmed är beviset för satsen klart. □

Det är ofta fruktbart att uppfatta ett oändligt kedjebråk som ett ändligt kedjebråk med ett oändligt kedjebråk som sin sista term (jämför med sats 20.2).

Sats 20.10 *Låt $(a_n)_{n=0}^{\infty}$ vara en trevlig följd av reella tal, låt k vara ett positivt heltal och sätt $\xi_k = \langle a_k, a_{k+1}, a_{k+2}, \dots \rangle$. Då är*

$$\langle a_0, a_1, a_2, \dots \rangle = \langle a_0, a_1, \dots, a_{k-1}, \xi_k \rangle.$$

Bevis. Ett ändligt kedjebråk $\langle a_0, a_1, \dots, a_{k-1}, x \rangle$ är uppenbarligen kontinuerligt som funktion av variabeln $x > 0$. Vi erhåller därför likheten i satsen genom att låta n gå mot oändligheten i likheten

$$\langle a_0, a_1, \dots, a_n \rangle = \langle a_0, a_1, \dots, a_{k-1}, \langle a_k, a_{k+1}, \dots, a_n \rangle \rangle,$$

ty $\langle a_k, a_{k+1}, \dots, a_n \rangle \to \xi_k$ då $n \to \infty$. □

EXEMPEL 3 Låt oss använda sats 20.10 för att beräkna det oändliga periodiska kedjebråket $\xi = \langle 1, 2, 3, 1, 2, 3, \dots \rangle = \langle \overline{1, 2, 3} \rangle$, där strecket över 1, 2, 3 antyder att detta block av tal upprepas i all oändlighet. På grund av periodiciteten är $\xi = \langle 1, 2, 3, \xi_3 \rangle$ där $\xi_3 = \xi$, dvs. $\xi = \langle 1, 2, 3, \xi \rangle$. För att bestämma värdet av detta ändliga kedjebråk använder vi konvergenterna, som beräknats i följande tabell:

n	-2	-1	0	1	2	3
a_n			1	2	3	ξ
p_n	0	1	1	3	10	$10\xi + 3$
q_n	1	0	1	2	7	$7\xi + 2$

Det följer att

$$\xi = \langle 1, 2, 3, \xi \rangle = \frac{p_3}{q_3} = \frac{10\xi + 3}{7\xi + 2}.$$

Efter förenkling erhålls andragradsekvationen $7\xi^2 - 8\xi - 3 = 0$ som har rötterna $(4 \pm \sqrt{37})/7$. Eftersom $\xi > 0$, drar vi slutsatsen att $\xi = (4 + \sqrt{37})/7$. □

EXEMPEL 4 För att beräkna värdet av det oändliga periodiska kedjebråket

$$\eta = \langle 0, 1, \overline{1, 2, 3} \rangle$$

börjar vi med att sätta $\xi = \langle \overline{1, 2, 3} \rangle$. Då är $\eta = \langle 0, 1, \xi \rangle = 0 + 1/(1 + 1/\xi) = \xi/(\xi + 1)$. Värdet av ξ beräknades i föregående exempel, och genom att sätta in $\xi = (4 + \sqrt{37})/7$ i uttrycket för η får vi $\eta = (1 + \sqrt{37})/12$. □

EXEMPEL 5 $\xi = \langle 1, 1, 1, \dots \rangle = \langle \overline{1} \rangle$ är det allra enklaste oändliga kedjebråket. Eftersom $\xi = \langle 1, \xi \rangle$, satisfierar ξ ekvationen $\xi = 1 + 1/\xi$, dvs. $\xi^2 = \xi + 1$. Denna andragradsekvation har rötterna $(1 \pm \sqrt{5})/2$, och eftersom ξ är positivt är $\langle 1, 1, 1, \dots \rangle = (1 + \sqrt{5})/2$. □

Övningar

20.1 Kedjebråksutveckla a) $\frac{19}{86}$, b) $\frac{22}{7}$.

20.2 Bestäm värdet av kedjebråket
a) $\langle 1, 1, 1, 1 \rangle$, b) $\langle 1, 9, 8, 6 \rangle$, c) $\langle 6, 8, 9, 1 \rangle$, d) $\langle 5, 4, 3, 2, 1 \rangle$.

20.3 Om $a/b = \langle a_0, a_1, \dots, a_n \rangle$, där $a > b \geq 1$, vilken kedjebråksutveckling har då a) b/a, b) $(a + b)/b$?

20.4 Bestäm konvergenterna till kedjebråket $\langle 1, 2, 3, 4, 5 \rangle$.

20.5 Lös ekvationen $295x + 327y = 1$ genom att kedjebråksutveckla $327/295$ och använda sats 20.5.

20.6 Beräkna kedjebråken
a) $\langle 1, \overline{2} \rangle$, b) $\langle \overline{1, 2} \rangle$, c) $\langle 1, 2, \overline{3} \rangle$, d) $\langle 1, \overline{2, 3} \rangle$, e) $\langle \overline{3, 2, 1} \rangle$.

20.7 Låt $\langle a_0, a_1, \dots, a_n \rangle$ vara ett kedjebråk med konvergenter p_k/q_k, $k = 0, 1, \dots, n$. Visa att
a) $q_n/q_{n-1} = \langle a_n, a_{n-1}, \dots, a_1 \rangle$.
b) $p_n/p_{n-1} = \langle a_n, a_{n-1}, \dots, a_0 \rangle$ om $a_0 > 0$. Vad har p_n/p_{n-1} för kedjebråksutveckling i fallet $a_0 = 0$?

21 Enkla kedjebråk

Definition 21.1 Ett ändligt eller oändligt kedjebråk kallas *enkelt* om alla dess termer är heltal.

Vi påminner om att alla termerna i ett kedjebråk utom möjligen den första a_0 måste vara positiva. Speciellt är alltså alla termerna i ett enkelt kedjebråk utom den första positiva heltal. Detta betyder att termerna i ett enkelt oändligt kedjebråk bildar en trevlig följd (med $\alpha = 1$), så det föreligger inga konvergensproblem. De enkla oändliga kedjebråken är automatiskt konvergenta.

Enkla ändliga kedjebråk har rationella värden. Detta följer förstås omedelbart av den rekursiva definitionen av ändliga kedjebråk, men är också en konsekvens av att konvergenterna är heltal.

Sats 21.2 *För konvergenterna (p_n, q_n) till ett ett ändligt eller oändligt enkelt kedjebråk gäller att talen p_n och q_n är relativt prima heltal. Kvoterna $c_n = p_n/q_n$ är följaktligen för $n \geq 0$ rationella tal skrivna på förkortad form.*

Bevis. Att p_n och q_n är heltal när kedjebråkets termer a_n är heltal följer omedelbart av den rekursiva definitionen. Att de är relativt prima är en konsekvens av identiteten $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$. □

Korollarium 21.3 *Varje enkelt ändligt kedjebråk $\langle a_0, a_1, \ldots, a_n \rangle$ har ett rationellt värde.*

Bevis. $\langle a_0, a_1, \ldots, a_n \rangle = p_n/q_n$. □

Sats 21.4 *Varje enkelt oändligt kedjebråk har ett irrationellt värde.*

Bevis. Antag motsatsen, dvs. att det finns ett oändligt enkelt kedjebråk med rationellt värde ξ och sätt $\xi = a/b$, där a och b är heltal. Om kedjebråkets konvergenter betecknas p_n/q_n, så gäller på grund av sats 20.9 att

$$0 < |a/b - p_n/q_n| < 1/q_n q_{n+1},$$

och genom att multiplicera denna olikhet med bq_n får vi olikheten

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}.$$

Genom att välja n så stort att $b/q_{n+1} < 1$, vilket är möjligt eftersom $q_{n+1} \to \infty$, erhåller vi olikheten $0 < |aq_n - bp_n| < 1$. Men detta är en motsägelse eftersom $aq_n - bp_n$ är ett heltal. □

Sats 21.5 *Varje reellt tal kan skrivas som ett enkelt kedjebråk. Kedjebråket är ändligt om och endast om det reella talet är rationellt.*

Bevis. Låt ξ vara ett reellt tal och sätt $a_0 = \lfloor \xi \rfloor$. Vi använder följande rekursiva algoritm för att definiera en (eventuellt tom) ändlig eller oändlig följd a_1, a_2, ... av positiva heltal.

Steg 0: Om $\xi = a_0$, så är $\xi = \langle a_0 \rangle$, och algoritmen stoppar. I motsatt fall är $0 < \xi - a_0 < 1$, och vi definierar då $\xi_1 = 1/(\xi - a_0)$, noterar att $\xi_1 > 1$ och att $\xi = \langle a_0, \xi_1 \rangle$, samt fortsätter till steg 1.

Steg k för $k = 1, 2, \ldots$: Antag att det reella talet $\xi_k > 1$ och att heltalen $a_0, a_1, \ldots, a_{k-1}$ redan är definierade med $a_j > 0$ för $j \geq 1$, samt att $\xi = \langle a_0, a_1, \ldots, a_{k-1}, \xi_k \rangle$, och sätt $a_k = \lfloor \xi_k \rfloor$.

Om $\xi_k = a_k$, så är $\xi = \langle a_0, a_1, \ldots, a_k \rangle$ och algoritmen stoppar. I motsatt fall definierar vi $\xi_{k+1} = 1/(\xi_k - a_k)$, som då är ett reellt tal > 1, noterar att $\xi_k = \langle a_k, \xi_{k+1} \rangle$ och att följaktligen $\xi = \langle a_0, a_1, \ldots, a_k, \xi_{k+1} \rangle$, samt fortsätter till steg $k + 1$.

Om algoritmen stoppar, så är ξ ett enkelt ändligt kedjebråk. Om algoritmen inte stoppar, så definierar den en oändlig följd $(a_n)_{n=0}^{\infty}$. Sätt $\eta = \langle a_0, a_1, a_2, \ldots \rangle$, och låt $c_n = p_n/q_n$ beteckna den n:te konvergenten till det oändliga kedjebråket η. Eftersom $\xi = \langle a_0, a_1, \ldots, a_n, \xi_{n+1} \rangle$, är talen c_{n-1} och c_n också konvergenter till ξ. Det följer därför av sats 20.9 och korollarium 20.6 att ξ och η båda ligger mellan talen c_{n-1} och c_n. Följaktligen är

$$|\xi - \eta| < |c_n - c_{n-1}| = \frac{1}{q_{n-1} q_n}.$$

Eftersom $q_n \to \infty$ då $n \to \infty$, drar vi slutsatsen att $\xi = \eta = \langle a_0, a_1, a_2, \ldots \rangle$. □

EXEMPEL 1 Med hjälp av algoritmen i sats 21.5 beräknar vi kedjebråksutvecklingen av $\sqrt{2}$ som följer:

$$\begin{aligned} a_0 &= \lfloor \sqrt{2} \rfloor = 1, & \xi_1 &= 1/(\xi - a_0) \;\; = 1/(\sqrt{2} - 1) = \sqrt{2} + 1; \\ a_1 &= \lfloor \xi_1 \rfloor = 2, & \xi_2 &= 1/(\xi_1 - a_1) = 1/(\sqrt{2} - 1) = \sqrt{2} + 1 = \xi_1. \end{aligned}$$

Eftersom $\xi_2 = \xi_1$, drar vi slutsatsen att $a_2 = a_1$ och $\xi_3 = \xi_2$, etc. Följaktligen är $a_n = a_1 = 2$ för alla $n \geq 1$, och detta innebär att

$$\sqrt{2} = \langle 1, 2, 2, 2, \ldots \rangle = \langle 1, \overline{2} \rangle.$$ □

Eftersom $k = k - 1 + 1/1$, kan varje heltal k skrivas på två olika sätt som enkelt kedjebråk, nämligen $k = \langle k \rangle = \langle k - 1, 1 \rangle$. Härav följer att varje rationellt tal har åtminstone två olika representationer som ändliga enkla kedjebråk, ty om $\langle a_0, a_1, \ldots, a_n \rangle$ är en representation med $a_n > 1$, så är

$$\langle a_0, a_1, \ldots, a_n - 1, 1 \rangle$$

en annorlunda representation som slutar på 1. Och omvänt, om $\langle a_0, a_1, \ldots, a_n, 1 \rangle$ är ett kedjebråk som slutar på 1, så är $\langle a_0, a_1, \ldots, a_n, 1 \rangle = \langle a_0, a_1, \ldots, a_n + 1 \rangle$. Några andra sätt att skriva rationella tal på som enkla kedjebråk finns det emellertid inte. För att bevisa detta behöver vi följande lemma.

Lemma 21.6 *Låt a_0, b_0 vara heltal, låt $a_1, a_2, \ldots, a_n$ vara positiva heltal, och låt x och y vara två reella tal ≥ 1. Då gäller*

(1) $\quad b_0 = \langle a_0, x \rangle \Rightarrow x = 1 \;\; \textit{och} \;\; a_0 = b_0 - 1$

(2) $\quad a_0 \neq b_0 \Rightarrow \langle a_0, x \rangle \neq \langle b_0, y \rangle$

(3) $\quad \langle a_0, a_1, \ldots, a_n, x \rangle = \langle a_0, a_1, \ldots, a_n, y \rangle \Rightarrow x = y$

Bevis. (1): Antag att $b_0 = \langle a_0, x \rangle$ och $x > 1$. Då är

$$a_0 < \langle a_0, x \rangle = b_0 = a_0 + 1/x < a_0 + 1,$$

vilket är motsägelsefullt eftersom b_0 är ett heltal. Följaktligen är $x = 1$ och $b_0 = a_0 + 1$.

(2): Antag att $a_0 < b_0$; då är $\langle a_0, x\rangle = a_0 + 1/x \leq a_0 + 1 \leq b_0 < \langle b_0, y\rangle$.

(3): Om $\langle a_0, x\rangle = \langle a_0, y\rangle$, så är uppenbarligen $x = y$. Påstående (3) gäller därför för $n = 0$. Antag nu att implikationen gäller med n ersatt av $n-1$, och antag att $\langle a_0, a_1, \ldots, a_n, x\rangle = \langle a_0, a_1, \ldots, a_n, y\rangle$. Eftersom

$$\langle a_0, a_1, \ldots, a_n, x\rangle = \langle a_0, a_1, \ldots, a_{n-1}, \langle a_n, x\rangle\rangle,$$

och det andra kedjebråket kan avkortas på motsvarande sätt, följer det av induktionsantagandet att först $\langle a_n, x\rangle = \langle a_n, y\rangle$ och sedan $x = y$. □

Sats 21.7 *Varje heltal k har exakt två representationer som enkla kedjebråk, nämligen $\langle k\rangle$ och $\langle k-1, 1\rangle$. Varje rationellt tal som inte är ett heltal har exakt två representationer som enkla kedjebråk och dessa har formen $\langle a_0, a_1, \ldots, a_n\rangle$ och $\langle a_0, a_1, \ldots, a_n - 1, 1\rangle$, där $n \geq 1$ och $a_n > 1$. Varje irrationellt tal har en unik representation som oändligt enkelt kedjebråk.*

Bevis. Vi har redan noterat att varje rationellt tal har två olika representationer som ändligt enkelt kedjebråk och att varje irrationellt tal kan skrivas som ett oändligt enkelt kedjebråk, så det räcker att visa att dessa representationer är de enda.

Antag först att k är ett heltal och att

$$k = \langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, \langle a_1, \ldots, a_n\rangle\rangle,$$

med $n \geq 1$. Det följer då av lemma 21.6 att $a_0 = k-1$ och $x = \langle a_1, \ldots, a_n\rangle = 1$. Om $n \geq 2$, så är $x > a_1 \geq 1$, vilket är motsägelsefullt. Alltså är $n = 1$ och $a_1 = 1$, dvs. $\langle k\rangle$ och $\langle k-1, 1\rangle$ är de enda representationerna av talet k som enkelt kedjebråk.

Låt nu $\langle a_0, a_1, \ldots, a_n\rangle = \langle b_0, b_1, \ldots, b_m\rangle$ vara två representationer av ett rationellt tal som inte är heltal, och antag att $m \geq n$. Antag att det finns ett index $k < n$ sådant att $a_k \neq b_k$, och låt k vara det minsta indexet med denna egenskap. Genom att skriva kedjebråket $\langle a_0, a_1, \ldots, a_n\rangle$ på formen

$$\langle a_0, \ldots, a_{k-1}, \langle a_k, \ldots, a_n\rangle\rangle$$

och göra motsvarande sak för $\langle b_0, b_1, \ldots, b_m\rangle$, drar vi med hjälp av lemma 21.6 slutsatsen att $\langle a_k, \ldots, a_n\rangle = \langle b_k, \ldots, b_m\rangle$, vilket är ekvivalent med att

$$\langle a_k, \langle a_{k+1}, \ldots, a_n\rangle\rangle = \langle b_k, \langle b_{k+1}, \ldots, b_m\rangle\rangle.$$

Detta är emellertid omöjligt på grund av (2) i lemma 21.6. Följaktligen är $a_k = b_k$ för alla $k < n$, och vi drar nu med hjälp av (3) slutsatsen att $a_n = \langle b_n, \ldots, b_m\rangle$. Men a_n är ett heltal, och vi vet redan att det bara finns två möjligheter att skriva ett heltal som enkelt kedjebråk; antingen är $m = n$ och $a_n = b_n$, eller $m = n+1$, $b_n = a_n - 1$ och $b_{n+1} = 1$.

Låt slutligen ξ vara ett irrationellt tal och antag att

$$\xi = \langle a_0, a_1, a_2, \ldots\rangle = \langle b_0, b_1, b_2, \ldots\rangle$$

är två skilda representationer av ξ. Då finns det ett första index k så att $a_k \neq b_k$, och vi drar med hjälp av (3) i lemmat slutsatsen att $\langle a_k, a_{k+1}, a_{k+2}, \ldots\rangle = \langle b_k, b_{k+1}, b_{k+2}, \ldots\rangle$. Detta strider emellertid mot (2) i samma lemma. □

Övningar

21.1 Kedjebråksutveckla talen

a) 19,86, b) 3,1416, c) $\sqrt{5}$, d) $\dfrac{1+\sqrt{5}}{2}$, e) $\sqrt{11}$, f) $\sqrt{14}$.

21.2 a) Bestäm början av kedjebråksutvecklingen för talet e med närmevärdet 2,71828. (Om man utvecklar 2,718275 och 2,718285 ser man hur många säkra termer man kan få.)
b) Bestäm början av kedjebråksutvecklingen för talet π med närmevärdet 3,14159.
c) Bestäm början av kedjebråksutvecklingen av $\sqrt[3]{2}$ med närmevärdet 1,2599.

21.3 Låt ξ vara ett irrationellt tal med enkel kedjebråksutveckling $\langle a_0, a_1, \dots \rangle$, och låt b_1, b_2, ... vara en (eventuellt ändlig) följd av positiva heltal. Visa att

$$\lim_{n\to\infty} \langle a_0, a_1, \dots, a_n, b_1, b_2, \dots \rangle = \xi.$$

21.4 De s.k. *Fibonaccitalen* F_n definieras av att

$$F_0 = F_1 = 1, \qquad F_n = F_{n-1} + F_{n-2} \quad \text{för } n \geq 2.$$

Visa att om $(p_n/q_n)_{n=0}^{N}$ är konvergenterna till ett (ändligt eller oändligt) enkelt kedjebråk, så är $q_n \geq F_n$ för alla n.

21.5 Låt $\langle a_0, a_1, \dots, a_n \rangle$ vara ett enkelt kedjebråk med konvergenter p_k/q_k, $k = 0, 1, \dots, n$. Visa följande påståenden:
a) Om $a_0 > 0$, så är $0 < p_0 < p_1 < \cdots < p_n$.
b) Om $a_0 < 0$, så är $p_0 < 0$ och $0 \geq p_1 > p_2 \geq p_3 > p_4 > \cdots > p_n$.
(När är $p_1 = 0$?)

21.6 Låt ξ vara ett irrationellt tal med enkelt kedjebråk $\langle a_0, a_1, a_2, \dots \rangle$. Visa att $-\xi$ har kedjebråksutvecklingen
a) $\langle -a_0 - 1, 1, a_1 - 1, a_2, a_3, \dots \rangle$ om $a_1 \geq 2$,
b) $\langle -a_0 - 1, a_2 + 1, a_3, a_4, \dots \rangle$ om $a_1 = 1$.

21.7 Låt a och b vara två positiva relativt prima heltal och antag att $a > b$. Visa att a/b har ett symmetriskt enkelt kedjebråk $\langle a_0, a_1, \dots, a_n \rangle$, dvs. att $a_k = a_{n-k}$ för $k = 0, 1, \dots, n$, om och endast om $b^2 \equiv (-1)^n \pmod{a}$.

22 Rationella approximationer till irrationella tal

Irrationella tal kan approximeras godtyckligt bra med rationella tal, vilket man uttrycker genom att säga att mängden $\mathbf{Q}$ av rationella tal är tät i mängden $\mathbf{R}$ av alla reella tal, men hur bra kan man approximera ett godtyckligt irrationellt tal ξ med rationella tal a/b om man satt en gräns för hur stor nämnaren b får vara? Den frågan ska vi behandla i det här avsnittet.

Om b är ett godtyckligt positivt heltal och a är det heltal som ligger närmast talet $b\xi$, så är $|b\xi - a| < 1/2$, och genom att dividera med b erhåller vi olikheten

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b}$$

som ger oss en uppskattning av approximationsfelet $|\xi - a/b|$ uttryckt i termer av det approximerande rationella talets nämnare b.

Detta är den bästa uppskattning som står till buds för godtyckliga nämnare b, men om $c_n = p_n/q_n$, den n:te konvergenten i utvecklingen av ξ som enkelt kedjebråk, så följer det av sats 20.9 att

$$\big|\xi - \frac{p_n}{q_n}\big| < \frac{1}{q_n^2}.$$

Approximationsfelet för konvergenterna p_n/q_n är således avsevärt mindre än vad man kan förvänta sig generellt.

Vi ska visa att man kan åstadkomma ännu bättre approximationer – det finns oändligt många rationella tal a/b sådana att $|\xi - a/b| < 1/\sqrt{5}\,b^2$ (sats 22.8). Detta resultat är skarpt i den meningen att det inte går att ersätta konstanten $\sqrt{5}$ med något större tal (sats 22.9). Rationella tal a/b som uppfyller olikheten måste vidare vara konvergenter; vi ska nämligen visa att om $|\xi - a/b| < 1/2b^2$, så är nödvändigtvis a/b en konvergent (sats 22.5). Kedjebråk och konvergenter spelar således en mycket viktig roll i teorin för rationell approximation.

I fortsättningen kommer vi att använda både $|\xi - a/b|$ och $|b\xi - a|$ som mått på hur väl a/b approximerar ξ.

Sats 22.1 *Låt ξ vara ett irrationellt tal och låt (p_n, q_n) vara den n:te konvergenten i talets enkla kedjebråksutveckling. Då är*

$$\big|\xi - \frac{p_n}{q_n}\big| < \big|\xi - \frac{p_{n-1}}{q_{n-1}}\big| \qquad \textit{och} \tag{1}$$

$$|q_n\xi - p_n| < |q_{n-1}\xi - p_{n-1}| \tag{2}$$

för alla $n \geq 1$.

Bevis. Vi börjar med att bevisa den andra olikheten, som är starkare än den första. Antag att

$$\xi = \langle a_0, a_1, a_2, \dots \rangle.$$

Genom att multiplicera olikheten (2) i sats 20.9 med q_n erhåller vi olikheten

$$\frac{a_{n+2}}{q_{n+2}} < |q_n\xi - p_n| < \frac{1}{q_{n+1}},$$

och genom att använda denna olikhet två gånger får vi olikheten

$$|q_{n-1}\xi - p_{n-1}| > a_{n+1}/q_{n+1} \geq 1/q_{n+1} > |q_n\xi - p_n|,$$

som bevisar (2).

Olikheten (1) följer nu av (2) och av att $q_n \geq q_{n-1}$ för $n \geq 1$:

$$\big|\xi - \frac{p_n}{q_n}\big| = \frac{1}{q_n}\big|q_n\xi - p_n\big| < \frac{1}{q_n}\big|q_{n-1}\xi - p_{n-1}\big| \leq \frac{1}{q_{n-1}}\big|q_{n-1}\xi - p_{n-1}\big| = \big|\xi - \frac{p_{n-1}}{q_{n-1}}\big|.$$

□

Konvergenter har ett antal intressanta extremalegenskaper som vi nu ska studera. Bevisen för dessa utnyttjar följande enkla lemma.

Lemma 22.2 *Om $r_1 = a_1/b_1$ och $r_2 = a_2/b_2$ är två rationella tal med positiva nämnare och $r_1 \neq r_2$, så är*

$$|r_1 - r_2| \geq \frac{1}{b_1 b_2}.$$

Bevis. $r_1 - r_2 = (a_1 b_2 - a_2 b_1)/b_1 b_2$ och täljaren $a_1 b_2 - a_2 b_1$ är ett nollskilt heltal vars absolutbelopp följaktligen är minst ett. □

Notera vidare att olikheten i lemmat gäller med likhet om de båda rationella talen är två konsekutiva konvergenter $c_n = p_n/q_n$ och $c_{n+1} = p_{n+1}/q_{n+1}$ till ett kedjebråk, ty på grund av sats 20.5 är $|c_{n+1} - c_n| = 1/q_{n+1}q_n$.

Sats 22.3 *Låt ξ vara ett irrationellt tal, låt B vara ett positivt heltal och betrakta värdet av $|t\xi - s|$ för alla heltal t i intervallet $[1, B]$ och alla heltal s. Antag att ett minimum antas för $s = a$ och $t = b$, dvs. att*

$$|b\xi - a| = \min\{|t\xi - s| \mid s, t \in \mathbf{Z},\ 1 \leq t \leq B\}.$$

Då är talen a och b relativt prima, och (a, b) är en konvergent i den enkla kedjebråksutvecklingen av ξ.

Bevis. Låt d vara en gemensam delare till a och b, och antag att $d > 1$. Sätt $a' = a/d$ och $b' = b/d$; då är $1 \leq b' \leq B$ och $|b'\xi - a'| = |b\xi - a|/d < |b\xi - a|$, vilket strider mot definitionen av talen a och b som minimipunkter. Alltså är $d = 1$, och talen a och b är således relativt prima.

Låt nu $c_n = p_n/q_n$ beteckna den n:te konvergenten till ξ och sätt $r = a/b$. Vi ska visa att $r = c_n$ för något n, och eftersom bråken a/b och p_n/q_n båda är skrivna på förkortad form, följer det då att $a = p_n$ och $b = q_n$.

Antag först att $r < c_0$. Eftersom $c_0 < \xi$, är $|\xi - r| > |c_0 - r| \geq 1/bq_0$ på grund av lemma 22.2. Genom att multiplicera olikheten med b erhåller vi olikheten

$$|b\xi - a| = b|\xi - r| > 1/q_0 \geq 1/q_1 > |q_0\xi - p_0|,$$

och eftersom $q_0 = 1 \leq b$, strider denna olikhet mot minimalitetsantagandena beträffande a och b. Följaktligen är $r \geq c_0$.

Antag härnäst att $r > c_1$. Eftersom $c_1 > \xi$, är nu $|\xi - r| > |c_1 - r| \geq 1/bq_1$, och genom att multiplicera med b erhåller vi på nytt olikheten

$$|b\xi - a| > 1/q_1 > |q_0\xi - p_0|,$$

som är omöjlig.

Följaktligen är $c_0 \leq r \leq c_1$. Eftersom (c_{2k}) är en växande följd och (c_{2k+1}) är en avtagande följd, båda med samma gränsvärde ξ, ligger det rationella talet r mellan c_{n-1} och c_{n+1} för något heltal n. Om r är antingen c_{n-1} eller c_{n+1}, så är beviset klart. Om så inte är fallet, så ligger dessa två konvergenter på samma sida om ξ medan konvergenten c_n ligger på den motsatta sidan. Därav följer att

$$|r - c_{n-1}| < |c_n - c_{n-1}|.$$

Eftersom den vänstra sidan av denna olikhet enligt lemma 22.2 är $\geq 1/bq_{n-1}$ och den högra sidan är lika med $1/q_n q_{n-1}$, är $1/bq_{n-1} < 1/q_n q_{n-1}$, varav följer att $q_n < b$.

Vi har också olikheten $|\xi - r| > |c_{n+1} - r| \geq 1/bq_{n+1}$, och genom att multiplicera båda sidorna med b erhåller vi olikheten $|b\xi - a| > 1/q_{n+1} > |q_n\xi - p_n|$. Eftersom $q_n < b$, strider detta mot antagandet att $|t\xi - s|$ minimeras av $t = b$ och $s = a$. Beviset är nu klart. □

Om a/b är den "bästa" approximationen till ξ i den bemärkelsen att uttrycket $|b\xi - a|$ inte kan göras mindre genom att a/b ersätts med något annat rationellt tal s/t med $1 \leq t \leq b$, så är enligt sats 22.3 a/b nödvändigtvis en konvergent till ξ. Genom att kombinera detta resultat med sats 22.1 får vi följande mer precisa information:

Sats 22.4 *Låt ξ vara ett irrationellt tal vars enkla kedjebråksutveckling har konvergenterna (p_n, q_n). Då är*

$$|q_n\xi - p_n| = \min\{|t\xi - s| \mid s, t \in \mathbf{Z},\ 1 \leq t < q_{n+1}\}, \tag{3}$$

$$\big|\xi - \frac{p_n}{q_n}\big| = \min\{\big|\xi - \frac{s}{t}\big| \mid s, t \in \mathbf{Z},\ 1 \leq t \leq q_n\}. \tag{4}$$

Bevis. Enligt sats 22.3 finns det en konvergent (p_m, q_m) sådan att

$$|q_m\xi - p_m| = \min\{|t\xi - s| \mid s, t \in \mathbf{Z},\ 1 \leq t < q_{n+1}\}.$$

Eftersom $q_k \geq q_{n+1}$ för alla $k \geq n+1$ och eftersom $|q_k\xi - p_k|$ avtar när k växer, följer det att $m = n$. Detta bevisar (3).

För att visa (4) antar vi att $1 \leq t \leq q_n$ och låter s vara ett godtyckligt heltal. Genom att utnyttja (3) erhåller vi olikheten

$$\big|\xi - \frac{p_n}{q_n}\big| = \frac{1}{q_n}\big|q_n\xi - p_n\big| \leq \frac{1}{q_n}\big|t\xi - s\big| = \frac{t}{q_n}\big|\xi - \frac{s}{t}\big| \leq \frac{q_n}{q_n}\big|\xi - \frac{s}{t}\big| = \big|\xi - \frac{s}{t}\big|.$$

Följaktligen är

$$\big|\xi - \frac{p_n}{q_n}\big| = \min_{1 \leq t \leq q_n} \big|\xi - \frac{s}{t}\big|. \qquad \square$$

Anmärkning. Om $q_{n+1} > 2q_n$, så gäller följande starkare resultat:

$$\big|\xi - \frac{p_n}{q_n}\big| = \min\{\big|\xi - \frac{s}{t}\big| \mid s, t \in \mathbf{Z},\ 1 \leq t \leq q_{n+1}/2\}.$$

Bevis. Antag att $|\xi - s/t| < |\xi - p_n/q_n|$. Med hjälp av triangelolikheten och sats 20.9 får vi då olikheten

$$1/tq_n \leq |s/t - p_n/q_n| \leq |s/t - \xi| + |\xi - p_n/q_n| < 2|\xi - p_n/q_n| < 2/q_nq_{n+1},$$

som medför att $t > q_{n+1}/2$. □

Exempel 1 Genom att använda algoritmen i sats 21.5 och decimalutvecklingen av π erhåller man kedjebråksutvecklingen $\pi = \langle 3, 7, 15, 1, 292, 1, 1, 1, 2, \dots \rangle$. De fem första konvergenterna har beräknats i följande tabell:

n	-2	-1	0	1	2	3	4
a_n		3	7	15	1	292	1
p_n	0	1	3	22	333	355	$103\,993$
q_n	1	0	1	7	106	113	$33\,102$

Konvergenten p_1/q_1 är den välkända approximationen $22/7$ som först angavs av Arkimedes, och det är den bästa approximationen bland alla rationella tal med en nämnare som inte överstiger 7. Approximationen $355/113$ är anmärkningsvärt bra; enligt sats 20.9 är

$$\left|\pi - \frac{355}{113}\right| < \frac{1}{113 \cdot 33102} < 3 \cdot 10^{-7}.$$

För att erhålla en ännu bättre rationell approximation behöver man enligt anmärkningen efter sats 22.4 ett tal a/b med $b > 33102/2 = 16\,551$, och talet $355/113$ är faktiskt den bästa rationella approximationen till π bland alla rationella tal med en nämnare som inte överstiger 16 603. □

I satserna 22.3 och 22.4 dyker konvergenter upp som lösningar till vissa minimeringsproblem. Det bör därför inte komma som någon överraskning att de ”bästa” rationella approximationerna till irrationella tal måste vara konvergenter. Följande sats preciserar detta påstående.

Sats 22.5 *Låt ξ vara ett irrationellt tal och antag att*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

där a och b är heltal och b är positivt. Då är a/b en av konvergenterna i utvecklingen av ξ som enkelt kedjebråk.

Anmärkning. Bråket a/b är inte nödvändigtvis förkortat.

Bevis. Om bråket a/b inte är förkortat, så uppfyller uppenbarligen det förkortade bråket a'/b' samma olikhet. Vi kan därför redan från början antaga att bråket a/b är förkortat, dvs. att talen a och b är relativt prima, och vi ska under detta antagande bevisa att olikheten

$$|b\xi - a| \le |t\xi - s| \tag{5}$$

gäller för alla heltal s och t med $1 \le t \le b$. Detta medför nämligen på grund av sats 22.3 att a/b är en konvergent.

Antag därför att det finns ett heltal s och ett heltal t som uppfyller $1 \le t \le b$ så att olikheten (5) inte gäller. Då är

$$|t\xi - s| < |b\xi - a|, \tag{6}$$

och det följer att

$$\left|\xi - \frac{s}{t}\right| < \frac{1}{t}\,|b\xi - a| = \frac{b}{t}\left|\xi - \frac{a}{b}\right| < \frac{b}{t} \cdot \frac{1}{2b^2} = \frac{1}{2bt}.$$

Triangelolikheten ger nu att

$$\left|\frac{a}{b} - \frac{s}{t}\right| \le \left|\frac{a}{b} - \xi\right| + \left|\xi - \frac{s}{t}\right| < \frac{1}{2b^2} + \frac{1}{2bt} = \frac{1}{2bt}\left(1 + \frac{t}{b}\right) \le \frac{1}{bt}.$$

Multiplikation med bt resulterar i olikheten $|at - bs| < 1$, och eftersom $at - bs$ är ett heltal, drar vi slutsatsen att $at - bs = 0$, dvs. $a/b = s/t$. Eftersom bråket a/b är förkortat är $t \ge b$. Men $t \le b$, så det följer att $t = b$ och $s = a$. Detta är en motsägelse på grund av olikheten (6). □

Det återstår att visa att det finns bråk a/b som uppfyller olikheten i sats 22.5. Det följer av sats 20.9 att konvergenterna p/q till ett irrationellt tal ξ uppfyller olikheten $|\xi - p/q| < 1/q^2$. Följande sats visar att av två successiva konvergenter satisfierar åtminstone alltid den ena den starkare olikheten i sats 22.5.

Sats 22.6 *Av två successiva konvergenter till utvecklingen av ett irrationellt tal ξ i enkelt kedjebråk uppfyller åtminstone den ena konvergenten p/q olikheten*

$$\Big|\xi - \frac{p}{q}\Big| < \frac{1}{2q^2}\,.$$

Bevis. Antag att satsen är falsk. Då finns det två konvergenter i följd, $c_n = p_n/q_n$ och $c_{n+1} = p_{n+1}/q_{n+1}$, så att $|\xi - c_n| > 1/2q_n^2$ och $|\xi - c_{n+1}| > 1/2q_{n+1}^2$. (Olikheterna är strikta eftersom talet ξ är irrationellt.) Eftersom de två konvergenterna ligger på motsatta sidor om ξ, följer det att

$$\frac{1}{q_n q_{n+1}} = |c_{n+1} - c_n| = |c_{n+1} - \xi| + |\xi - c_n| > \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2}.$$

Multiplikation med $q_{n+1}q_n$ ger oss olikheten

$$1 > \frac{1}{2}\Big(\frac{q_n}{q_{n+1}} + \frac{q_{n+1}}{q_n}\Big). \tag{7}$$

För att fullborda beviset noterar vi att $x + 1/x = 2 + (\sqrt{x} - 1/\sqrt{x})^2 \geq 2$ för alla positiva tal x. Den högra sidan av olikheten (7) är därför säkert ≥ 1, och detta är en motsägelse. Därmed är satsen bevisad. □

Resultatet i sats 22.6 kan förbättras som sats 22.8 kommer att visa. Vi behöver följande enkla lemma.

Lemma 22.7 *Låt x vara ett positivt reelt tal och antag att $x + \dfrac{1}{x} < \sqrt{5}$. Då är*

$$x < \frac{\sqrt{5}+1}{2} \qquad \textit{och} \qquad \frac{1}{x} > \frac{\sqrt{5}-1}{2}.$$

Bevis.
$$\begin{aligned} x + 1/x < \sqrt{5} &\Leftrightarrow x^2 - \sqrt{5}x + 1 < 0 \\ &\Leftrightarrow \big(x - (\sqrt{5}+1)/2\big)\big(x - (\sqrt{5}-1)/2\big) < 0 \\ &\Leftrightarrow (\sqrt{5}-1)/2 < x < (\sqrt{5}+1)/2, \end{aligned}$$

och om $x < (\sqrt{5}+1)/2$, så är $1/x > (\sqrt{5}-1)/2$. □

Sats 22.8 *Om ξ är irrationellt, så finns det oändligt många rationella tal a/b sådana att*

$$\Big|\xi - \frac{a}{b}\Big| < \frac{1}{\sqrt{5}\,b^2}.$$

Av tre successiva konvergenter till ξ uppfyller nämligen minst en olikheten.

Bevis. Antag att ingen av konvergenterna $c_k = p_k/q_k$, $k = n-1, n, n+1$, satisfierar olikheten. Då är $|\xi - c_k| \geq 1/\sqrt{5}\,q_k^2$ för $k = n-1$, n och $n+1$. De successiva konvergenterna c_{n-1} och c_n ligger på motsatta sidor om ξ. Följaktligen är

$$\frac{1}{q_n q_{n-1}} = |c_n - c_{n-1}| = |c_n - \xi| + |\xi - c_{n-1}| \geq \frac{1}{\sqrt{5}}\Big(\frac{1}{q_n^2} + \frac{1}{q_{n-1}^2}\Big).$$

Efter multiplikation med $q_n q_{n-1}$ erhålls olikheten $q_n/q_{n-1} + q_{n-1}/q_n < \sqrt{5}$ (som är strikt eftersom talet i olikhetens vänsterled är rationellt), och med hjälp av lemma 22.7 drar vi slutsatsen att $q_n/q_{n-1} < (\sqrt{5}+1)/2$ och att $q_{n-1}/q_n > (\sqrt{5}-1)/2$.

Analogt fås $q_{n+1}/q_n < (\sqrt{5}+1)/2$, och följaktligen är

$$\begin{aligned}\frac{\sqrt{5}+1}{2} &> \frac{q_{n+1}}{q_n} = \frac{a_n q_n + q_{n-1}}{q_n} \geq \frac{q_n + q_{n-1}}{q_n} = 1 + \frac{q_{n-1}}{q_n} \\ &> 1 + \frac{\sqrt{5}-1}{2} = \frac{\sqrt{5}+1}{2}.\end{aligned}$$

Denna motsägelse bevisar satsen. □

Sats 22.9 *Konstanten $\sqrt{5}$ i föregående sats är den bästa möjliga, ty om $C > \sqrt{5}$ och $\xi = \langle 1, 1, 1, \dots \rangle = (\sqrt{5}+1)/2$, så gäller olikheten*

$$\Big|\xi - \frac{a}{b}\Big| < \frac{1}{Cb^2}$$

bara för ändligt många heltal a och b.

Bevis. Enligt sats 22.5 måste varje rationellt tal a/b som uppfyller olikheten vara en konvergent, så det räcker att visa att det bara är ändligt många konvergenter p_n/q_n till ξ som uppfyller olikheten.

Notera först att $\xi^{-1} = (\sqrt{5}-1)/2$, att $\xi + \xi^{-1} = \sqrt{5}$ och att $\xi - \xi^{-1} = 1$.

Eftersom $p_n = p_{n-1} + p_{n-2}$ och $q_n = q_{n-1} + q_{n-2}$, där $p_{-2} = 0$ och $p_{-1} = 1$, medan $q_{-1} = 0$ och $q_0 = 1$, följer det att $q_n = p_{n-1}$ för alla $n \geq -1$ och att $(q_n)_0^\infty$ är den vanliga Fibonacciföljden. Med induktion är det lätt att visa att

$$p_n = A\xi^n + B(-\xi)^{-n},$$

där konstanterna A och B är bestämda av villkoret

$$\begin{cases} p_{-1} = A\xi^{-1} - B\xi = 1 \\ p_0 = A + B = 1 \end{cases}$$

Genom att lösa systemet får vi

$$A = \frac{1+\xi}{\xi + \xi^{-1}}, \quad B = \frac{\xi^{-1} - 1}{\xi + \xi^{-1}} \quad \text{och} \quad AB(\xi + \xi^{-1}) = \frac{\xi^{-1} - \xi}{\xi + \xi^{-1}} = -\frac{1}{\sqrt{5}}.$$

Alltså är

$$\begin{aligned}|q_n\xi - p_n| = |p_{n-1}\xi - p_n| &= |A\xi^n - B(-\xi)^{2-n} - A\xi^n - B(-\xi)^{-n}| \\ &= |B(\xi^2+1)\xi^{-n}| = -B(\xi^2+1)\xi^{-n}.\end{aligned}$$

Det följer att

$$\begin{aligned} q_n^2\left|\xi - \frac{p_n}{q_n}\right| &= |q_n\xi - p_n|\, q_n = -B(\xi^2+1)\xi^{-n}(A\xi^{n-1} + B(-\xi)^{1-n}) \\ &= -AB(\xi + \xi^{-1}) + (-1)^n B^2(\xi^2+1)\xi^{1-2n} \\ &= \frac{1}{\sqrt{5}} + B^2(-1)^n(\xi^2+1)\xi^{1-2n}. \end{aligned}$$

Då n går mot ∞ går ξ^{1-2n} mot 0, eftersom $\xi > 1$. Följaktligen är

$$\lim_{n\to\infty} q_n^2\left|\xi - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}},$$

och eftersom $1/\sqrt{5} > 1/C$, är därför

$$q_n^2\left|\xi - \frac{p_n}{q_n}\right| > \frac{1}{C}$$

för alla utom ändligt många n. Olikheten i sats 22.9 gäller således bara för ändligt många konvergenter p_n/q_n. □

Övningar

22.1 $\sqrt{2}$ har kedjebråksutvecklingen $\langle 1, \overline{2}\rangle$. Beräkna konvergenterna p_5/q_5 och p_6/q_6 och uppskatta med hjälp av dem $\sqrt{2}$.

22.2 Bestäm positiva heltal a och b, $b < 100$, sådana att $|b\xi - a|$ blir så litet som möjligt då ξ är talet a) $\sqrt{2}$, b) $\sqrt{3}$, c) π, d) e, e) 1043/471.

Bestäm också i varje fall det minsta tal b (≥ 100) som ger ett mindre värde på $|b\xi - a|$.

22.3 Bestäm tre rationella tal a/b som satisfierar olikheten $|\sqrt{3} - a/b| < 1/2b^2$.

22.4 Antag att $a/b < x/y < c/d$, där täljarna och nämnarna är heltal och nämnarna b, y och d är positiva. Visa att om $ad - bc = -1$, så är $y > b$ och $y > d$.

22.5 Låt ξ vara ett irrationellt tal med kedjebråksutveckling $\langle a_0, a_1, a_2, \dots\rangle$ och konvergenter p_n/q_n, och sätt för $n \geq 0$ och $t \geq 0$

$$c_{n,t} = \frac{tp_n + p_{n-1}}{tq_n + q_{n-1}}.$$

För $t = 0$ och $t = a_{n+1}$ får vi konvergenterna $c_{n-1} = p_{n-1}/q_{n-1}$ och $c_{n+1} = p_{n+1}/q_{n+1}$ (utom i fallet $n = 0$, då $c_{0,0}$ är odefinierat). Om t är ett heltal som ligger strikt mellan 0 och a_{n+1}, så kallas talet $c_{n,t}$ en *mellankonvergent* eller en *sekundär konvergent* till det givna kedjebråket.

a) Visa att $c_{n,t}$ är en strängt växande funktion av t om n är udda och en strängt avtagande funktion om n är jämnt.
b) Visa att om a/b är den bästa rationella approximationen till ξ med nämnare $\leq b$, dvs. om olikheten

$$\left|\xi - \frac{a}{b}\right| \leq \left|\xi - \frac{x}{y}\right|$$

gäller för alla heltal x och alla heltal y som uppfyller $1 \leq y \leq b$, så är a/b en konvergent eller en mellankonvergent till ξ.

c) För $n \geq 1$ har konvergenterna p_n/q_n den i b) angivna minimalegenskapen. Visa att däremot inte varje mellankonvergent har denna egenskap genom att t.ex. betrakta en lämplig mellankonvergent till $\sqrt{2}$.

22.6 Bestäm med hjälp av föregående övning den bästa rationella approximationen a/b med $0 < b < 100$ till ξ, dvs. den approximation som gör $|\xi - a/b|$ så litet som möjligt, då ξ är lika med
a) $\sqrt{2}$, b) $\sqrt{3}$, c) π, d) e, e) 1043/471.

22.7 Bestäm tre rationella tal a/b sådana att $|\sqrt{3} - a/b| < 1/\sqrt{5}\,b^2$.

23 Periodiska kedjebråk

I avsnitt 20 beräknade vi några periodiska enkla kedjebråk och fann att de var rötter till andragradsekvationer med heltalskoefficienter. Syftet med det här avsnittet är att visa att denna egenskap karakteriserar periodiska enkla kedjebråk. Ett irrationellt tal har med andra ord en peridisk enkel kedjebråksutveckling om och endast om talet är rot till en kvadratisk ekvation med heltalskoefficienter.

Definition 23.1 En oändlig följd $(a_n)_{n=0}^{\infty}$ kallas *periodisk* om det finns ett nollskilt heltal p och ett heltal m så att

$$a_n = a_{n+p} \quad \text{för alla } n \geq m.$$

Talet p kallas en *period* till följden.

Om p och q är två olka perioder till följden, så är också $p - q$ en period eftersom $a_{n+p-q} = a_{n+p-q+q} = a_{n+p} = a_n$ för alla tillräckligt stora tal n. Mängden av perioder tillsammans med talet 0 är således ett ideal i $\mathbf{Z}$. Det finns därför ett minsta positivt tal r sådant att alla perioder till följden är multipler av r. Detta entydigt bestämda tal kallas följdens *period* (i bestämd form) eller *periodlängd*.

En periodisk följd med period $p > 0$ kan skrivas på formen

$$\begin{aligned} &b_0, b_1, \ldots, b_{m-1}, c_0, c_1, \ldots, c_{p-1}, c_0, c_1, \ldots, c_{p-1}, \ldots \\ &\quad = b_0, b_1, \ldots, b_{m-1}, \overline{c_0, c_1, \ldots, c_{p-1}} \end{aligned}$$

där strecket över c_0, c_1, …, c_{p-1} betyder att blocket upprepas i all oändlighet.

En periodisk följd $(a_n)_{n=0}^{\infty}$ med period $p > 0$ kallas *rent periodisk* om likheten $a_n = a_{n+p}$ gäller för alla $n \geq 0$. Rent periodiska följder har formen $\overline{a_0, a_1, \ldots, a_{p-1}}$.

Definition 23.2 Ett oändligt kedjebråk $\langle a_0, a_1, a_2, \ldots \rangle$ kallas *(rent) periodiskt* om motsvarande följd $(a_n)_{n=0}^{\infty}$ av termer är (rent) periodisk. Med kedjebråkets period menas förstås perioden hos följden av termer.

Låt $\xi = \langle a_0, a_1, a_2, \ldots \rangle$ vara ett kedjebråk och sätt

$$\xi_k = \langle a_k, a_{k+1}, a_{k+2}, \ldots \rangle.$$

Om kedjebråket ξ är periodiskt med period p, så finns det per definition ett heltal m sådant att $\xi_n = \xi_{n+p}$ för alla $n \geq m$. Och omvänt, om likheten $\xi_{n+p} = \xi_n$ gäller för något n, så är ξ ett periodiskt kedjebråk med p som en period (och perioden i bestämd form är en divisor till p).

Definition 23.3 Ett irrationellt tal ξ kallas *kvadratiskt* (eller *algebraiskt av grad två*) om det är rot till någon kvadratisk ekvation med heltalskoefficienter, dvs. om $a\xi^2 + b\xi + c = 0$ för lämpliga heltalskoefficienter a, b och c med $a \neq 0$.

Sats 23.4 *Ett reellt tal ξ är ett kvadratiskt irrationellt tal om och endast om det har formen $\xi = r + s\sqrt{d}$, där d är ett positivt heltal som inte är en jämn kvadrat, r och s är rationella tal och $s \neq 0$.*

Bevis. Varje reell irrationell lösning till en kvadratisk ekvation $ax^2 + bx + c = 0$ har uppenbarligen denna form. Omvänt är varje reellt tal med denna form irrationellt och satisfierar andragradsekvationen $(x - r)^2 = s^2 d$, som efter multiplikation med kvadraterna på nämnarna hos r och s blir en andragradsekvation med heltalskoefficienter. □

Definition 23.5 Låt d vara ett positivt heltal som inte är en jämn kvadrat. Med $\mathbf{Q}[\sqrt{d}\,]$ menas mängden av alla reella tal ξ på formen $\xi = r + s\sqrt{d}$, där r och s är rationella tal. Talet $\xi' = r - s\sqrt{d}$ sägs vara *konjugerat* till ξ.

De enkla bevisen för följande två satser lämnas åt läsaren.

Sats 23.6 *$\mathbf{Q}[\sqrt{d}\,]$ är en talkropp, dvs. om ξ och η är tal i $\mathbf{Q}[\sqrt{d}\,]$, så ligger deras summa $\xi + \eta$, differens $\xi - \eta$, produkt $\xi\eta$ och kvot ξ/η också i $\mathbf{Q}[\sqrt{d}\,]$, kvoten förstås förutsatt att $\eta \neq 0$.*

Sats 23.7 *Antag att $\xi, \eta \in \mathbf{Q}[\sqrt{d}\,]$. Då är $(\xi + \eta)' = \xi' + \eta'$, $(\xi - \eta)' = \xi' - \eta'$, $(\xi\eta)' = \xi'\eta'$ och $(\xi/\eta)' = \xi'/\eta'$.*

Sats 23.8 *Om det reella talet ξ har en periodisk enkel kedjebråksutveckling, så är ξ ett kvadratiskt irrationellt tal.*

Bevis. Eftersom kedjebråket är oändligt är talet ξ irrationellt. Vi ska visa att $\xi \in \mathbf{Q}[\sqrt{d}\,]$ för något lämpligt positivt heltal d som inte är en jämn kvadrat.

Antag

$$\xi = \langle b_0, b_1, \ldots, b_{m-1}, \overline{c_0, c_1, \ldots, c_{r-1}}\,\rangle,$$

och sätt $\eta = \langle \overline{c_0, c_1, \ldots, c_{r-1}}\,\rangle$. Då är $\eta = \langle c_0, c_1, \ldots, c_{r-1}, \eta\rangle$.

Låt (p_k, q_k) vara konvergenterna till kedjebråket $\langle c_0, c_1, \ldots, c_{r-1}\rangle$. Då är

$$\eta = \langle c_0, c_1, \ldots, c_{r-1}, \eta\rangle = \frac{\eta p_{r-1} + p_{r-2}}{\eta q_{r-1} + q_{r-2}},$$

och genom att lösa denna ekvation med avseende på η ser vi att η satisfierar en andragradsekvation med heltalskoefficienter. Alltså är η ett kvadratiskt irrationellt tal, dvs. $\eta \in \mathbf{Q}[\sqrt{d}\,]$ för något lämpligt positivt heltal d som inte är en jämn kvadrat.

På motsvarande sätt får vi i termer av konvergenterna (P_k, Q_k) till kedjebråket $\langle b_0, b_1, \ldots, b_{m-1}\rangle$ att

$$\xi = \langle b_0, b_1, \ldots, b_{m-1}, \eta\rangle = \frac{\eta P_{m-1} + P_{m-2}}{\eta Q_{m-1} + Q_{m-2}},$$

så det följer av sats 23.6 att ξ tillhör $\mathbf{Q}[\sqrt{d}\,]$. □

Omvändningen till sats 23.8 gäller också, dvs. varje kvadratiskt irrationellt tal har en periodisk enkel kedjebråksutveckling. För att bevisa detta krävs det lite förberedande arbete.

Lemma 23.9 *Om ξ är ett kvadratiskt irrationellt tal, så kan ξ skrivas på formen*

$$\xi = \frac{u + \sqrt{d}}{v},$$

där d är ett heltal som inte är en jämn kvadrat, u och v är heltal och $v|(d-u^2)$.

Bevis. Enligt sats 23.4 är $\xi = r + s\sqrt{D}$, där D är ett heltal som inte är en jämn kvadrat, r och s är rationella tal och $s \neq 0$. Vi kan uppenbarligen skriva $r = a/c$ och $s = b/c$, där a, b och c är heltal och $b > 0$. Då blir

$$\xi = \frac{a + b\sqrt{D}}{c} = \frac{a|c| + \sqrt{b^2c^2D}}{c|c|} = \frac{u + \sqrt{d}}{v},$$

och heltalen $u = a|c|$, $v = c|c|$ och $d = b^2c^2D$ uppfyller nu kravet $v|(d-u^2)$. □

Antag att ξ_0 är ett kvadratiskt irrationellt tal. Med hjälp av lemma 23.9 skriver vi först

$$\xi_0 = (u_0 + \sqrt{d})/v_0,$$

där heltalet d inte är en jämn kvadrat, u_0 och v_0 är heltal och $v_0|(d - u_0^2)$.

Vi erinrar sedan om den rekursiva algoritmen i sats 21.5 för kedjebråksutvecklingen $\langle a_0, a_1, a_2, \dots \rangle$ av ξ_0. Termerna a_n ges av att

$$a_0 = \lfloor \xi_0 \rfloor, \quad \xi_{n+1} = \frac{1}{\xi_n - a_n} \quad \text{och} \quad a_{n+1} = \lfloor \xi_{n+1} \rfloor \quad \text{för } n = 0,\, 1,\, 2,\, \dots,$$

och $\xi_0 = \langle a_0, a_1, \dots, a_n, \xi_{n+1} \rangle$ för alla n.

Antag nu induktivt att $\xi_n = (u_n + \sqrt{d})/v_n$, med heltal u_n och v_n sådana att $v_n|(d - u_n^2)$. Då är

$$\xi_{n+1} = \frac{1}{\xi_n - a_n} = \frac{1}{\dfrac{\sqrt{d} - (a_n v_n - u_n)}{v_n}} = \frac{\sqrt{d} + (a_n v_n - u_n)}{\dfrac{d - (a_n v_n - u_n)^2}{v_n}} = \frac{u_{n+1} + \sqrt{d}}{v_{n+1}},$$

där $u_{n+1} = a_n v_n - u_n$ och $v_{n+1} = (d - u_{n+1}^2)/v_n$.

Talet u_{n+1} är uppenbarligen ett heltal och $u_{n+1} \equiv -u_n \pmod{v_n}$. Enligt induktionsantagandet är därför $d - u_{n+1}^2 \equiv d - u_n^2 \equiv 0 \pmod{v_n}$, dvs. v_n delar $d - u_{n+1}^2$. Därför är också v_{n+1} ett heltal, och $v_{n+1}|(d - u_{n+1}^2)$, eftersom $v_n v_{n+1} = d - u_{n+1}^2$.

Genom induktion har vi således bevisat giltigheten av följande algoritm:

Sats 23.10 *Antag att $\xi_0 = (u_0 + \sqrt{d})/v_0$, där d är ett positivt heltal som inte är en jämn kvadrat, u_0 och v_0 är heltal och $v_0|(d - u_0^2)$. Definiera följderna $(u_n)_0^\infty$, $(v_n)_0^\infty$, $(a_n)_0^\infty$ och $(\xi_n)_0^\infty$ rekursivt för $n \geq 0$ på följande sätt:*

$$\xi_n = \frac{u_n + \sqrt{d}}{v_n}, \qquad a_n = \lfloor \xi_n \rfloor$$

$$u_{n+1} = a_n v_n - u_n, \qquad v_{n+1} = \frac{d - u_{n+1}^2}{v_n}.$$

Då är u_n och v_n heltal, $v_n|(d-u_n^2)$ och $\xi_0 = \langle a_0, a_1, \ldots, a_n, \xi_{n+1}\rangle$ för alla n, och

$$\xi_0 = \langle a_0, a_1, a_2, \ldots\rangle.$$

EXEMPEL 1 Vi beräknar kedjebråksutvecklingen av talet $(1-\sqrt{5})/3$ med hjälp av algoritmen i sats 23.10. Eftersom $3 \nmid (5-1^2)$ behöver vi först skriva om talet så att det får den form som beskrivs i lemma 23.9. Genom att multiplicera täljare och nämnare med -3 fås

$$\xi_0 = \frac{-3+\sqrt{45}}{-9}, \quad \text{dvs.} \quad u_0 = -3, \quad v_0 = -9 \quad \text{och} \quad d = 45.$$

Nu gäller att $v_0|(d-u_0^2)$ och vi kan starta algoritmen. Resultatet av beräkningarna visas i följande tabell:

n	0	1	2	3	4	5	6	7	8	9
u_n	-3	12	-1	5	5	3	6	6	3	5
v_n	-9	11	4	5	4	9	1	9	4	5
a_n	-1	1	1	2	2	1	12	1	2	2

Eftersom $(u_9, v_9) = (u_3, v_3)$ drar vi slutsatsen att $\xi_9 = \xi_3$, varav följer att

$$\frac{1-\sqrt{5}}{3} = \langle -1, 1, 1, \overline{2, 2, 1, 12, 1, 2}\rangle. \qquad \square$$

Lemma 23.11 *Låt $\xi = \langle a_0, a_1, a_2, \ldots\rangle$ vara ett kvadratiskt irrationellt tal och sätt $\xi_n = \langle a_n, a_{n+1}, a_{n+2}, \ldots\rangle$. Om det för något index k gäller att konjugatet $\xi_k' < 0$, så är $-1 < \xi_n' < 0$ för alla $n > k$.*

Bevis. Det räcker på grund av induktion att visa implikationen

$$\xi_n' < 0 \Rightarrow -1 < \xi_{n+1}' < 0.$$

Så antag att $\xi_n' < 0$. Genom att använda sambandet $\xi_{n+1} = 1/(\xi_n - a_n)$ och konjugera erhåller vi likheten $\xi_{n+1}' = 1/(\xi_n' - a_n)$. Eftersom $a_n \geq 1$ är nämnaren $\xi_n' - a_n$ strikt mindre än -1, Följaktligen är $-1 < \xi_{n+1}' < 0$. $\square$

Lemma 23.12 *Låt $\xi = \langle a_0, a_1, a_2, \ldots\rangle$ vara ett kvadratiskt irrationellt tal och definiera ξ_n som i föregående lemma. Om $-1 < \xi_n' < 0$, så är $a_n = \lfloor -1/\xi_{n+1}'\rfloor$.*

Bevis. Likheten $\xi_{n+1}' = 1/(\xi_n' - a_n)$ medför att $-1/\xi_{n+1}' = a_n - \xi_n'$, och eftersom $0 < -\xi_n' < 1$ är $\lfloor -1/\xi_{n+1}'\rfloor = \lfloor a_n - \xi_n'\rfloor = a_n$. $\square$

Lemma 23.13 *Om ξ är ett kvadratiskt irrationellt tal, så finns det ett index k sådant att $\xi_k' < 0$.*

Bevis. Låt (p_k, q_k) beteckna den k:te konvergenten till ξ. Eftersom

$$\xi = \langle a_0, a_1, \ldots, a_{n-1}, \xi_n\rangle,$$

är

$$\xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}},$$

och genom att lösa ut ξ_n får vi sambandet

$$\xi_n = \frac{q_{n-2}\xi - p_{n-2}}{p_{n-1} - q_{n-1}\xi} = -\frac{q_{n-2}}{q_{n-1}}\Big(\frac{\xi - p_{n-2}/q_{n-2}}{\xi - p_{n-1}/q_{n-1}}\Big).$$

Konjugering ger

$$\xi_n' = -\frac{q_{n-2}}{q_{n-1}}\Big(\frac{\xi' - p_{n-2}/q_{n-2}}{\xi' - p_{n-1}/q_{n-1}}\Big).$$

Vi använder nu det faktum att konvergenterna p_n/q_n konvergerar mot ξ då n går mot oändligheten och att $\xi' \neq \xi$. Av detta följer att uttrycket inom parentes konvergerar mot $(\xi'-\xi)/(\xi'-\xi)$, dvs. mot 1, då n går mot oändligheten. Följaktligen är uttrycket inom parentes säkerligen positivt för tillräckligt stora n. Konjugatet ξ_n' har därför samma tecken som kvoten $-q_{n-2}/q_{n-1}$, som är negativ eftersom q_n är positivt för alla $n \geq 0$. □

Sats 23.14 *Ett reellt tal ξ har en periodisk enkel kedjebråksutveckling om och endast om det är ett kvadratiskt irrationellt tal.*

Bevis. Vi har redan bevisat att periodiska kedjebråk är kvadratiskt irrationella (sats 23.8). För att visa omvändningen låter vi $\xi = \xi_0$ vara ett kvadratiskt irrationellt tal och sätter

$$\xi_n = \frac{u_n + \sqrt{d}}{v_n}$$

som i sats 23.10. Enligt lemma 23.13 finns det ett index k sådant att $\xi_k' < 0$, och enligt lemma 23.11 är $-1 < \xi_n' < 0$ för alla $n > k$. Eftersom $\xi_n > 1$ för alla $n \geq 1$, drar vi slutsatsen att

$$1 < \xi_n - \xi_n' = \frac{2\sqrt{d}}{v_n} \quad \text{och} \quad 0 < \xi_n + \xi_n' = \frac{2u_n}{v_n}$$

för alla $n > k$. Alltså är $0 < v_n < 2\sqrt{d}$ och $u_n > 0$ om $n > k$. Genom att utnyttja sambandet $d - u_{n+1}^2 = v_n v_{n+1} > 0$ får vi vidare att $u_{n+1}^2 < d$, dvs. $u_{n+1} < \sqrt{d}$ för $n > k$. Om $n > k+1$, så är följaktligen $0 < u_n < \sqrt{d}$ och $0 < v_n < 2\sqrt{d}$. De ordnade paren (u_n, v_n) kan således bara anta ett ändligt antal möjliga värden, och därför finns det olika tal i och j med $j > i$ sådana att $u_j = u_i$ och $v_j = v_i$. Detta medför att $\xi_i = \xi_j = \xi_{i+(j-i)}$, och ξ har följaktligen en periodisk kedjebråksutveckling. □

Vi ska härnäst karakterisera de rent periodiska kedjebråken.

Definition 23.15 Ett kvadratiskt irrationellt tal $\xi = r + s\sqrt{d}$ kallas *reducerat* om $\xi > 1$ och det för konjugatet $\xi' = r - s\sqrt{d}$ gäller att $-1 < \xi' < 0$.

Sats 23.16 *Ett reellt tal ξ har en rent periodisk enkel kedjebråksutveckling om och endast om det är ett reducerat kvadratiskt irrationellt tal.*

Om $\xi = \langle\overline{a_0, a_1, \ldots, a_{r-1}}\rangle$, så är vidare $-1/\xi' = \langle\overline{a_{r-1}, a_{r-2}, \ldots, a_1, a_0}\rangle$.

Bevis. Antag att $\xi = \xi_0$ är ett reducerat kvadratiskt irrationellt tal så att speciellt $-1 < \xi_0' < 0$. Med beteckningar enligt sats 23.10 gäller då för $\xi_n = (u_n + \sqrt{d})/v_n$ att $-1 < \xi_n' < 0$ och $a_n = \lfloor -1/\xi_{n+1}' \rfloor$ för alla $n \geq 0$ på grund av lemma 23.11 och lemma 23.12.

Vi vet från sats 23.14 att ξ har en periodisk kedjebråksutveckling. Låt r vara periodlängden; då finns det ett minsta tal $m \geq 0$ sådant att

$$\xi_{n+r} = \xi_n \quad \text{för alla } n \geq m.$$

Vi ska visa att $m = 0$.

Antag därför att $m \geq 1$. Genom att utgår från likheten $\xi_m = \xi_{m+r}$ får vi först genom konjugering att $\xi'_m = \xi'_{m+r}$ och sedan att

$$a_{m-1} = \lfloor -1/\xi'_m \rfloor = \lfloor -1/\xi'_{m+r} \rfloor = a_{m+r-1}.$$

Eftersom

$$\frac{1}{\xi_{m-1} - a_{m-1}} = \xi_m = \xi_{m+r} = \frac{1}{\xi_{m+r-1} - a_{m+r-1}},$$

drar vi slutsatsen att $\xi_{m-1+r} = \xi_{m-1}$, vilket motsäger definitionen av talet m. Alltså är $m = 0$, och kedjebråksutvecklingen av ξ är således rent periodiskt.

Antag omvänt att ξ har en rent periodisk kedjebråksutveckling

$$\xi = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle,$$

där $a_0, a_1, \ldots, a_{r-1}$ är positiva heltal. Då är $\xi > a_0 \geq 1$. Om (p_n, q_n) betecknar den n:te konvergenten till ξ, så är

$$\xi = \langle a_0, a_1, \ldots, a_{r-1}, \xi \rangle = \frac{p_{r-1}\xi + p_{r-2}}{q_{r-1}\xi + q_{r-2}}.$$

Talet ξ satisfierar således andragradsekvationen

$$f(x) = q_{r-1}x^2 + (q_{r-2} - p_{r-1})x - p_{r-2} = 0.$$

Denna ekvation har två rötter, ξ och dess konjugat ξ'. Eftersom $\xi > 1$, behöver vi bara visa att $f(x)$ har en rot mellan -1 och 0 för att visa att $-1 < \xi' < 0$. Vi ska göra så genom att visa att $f(0) < 0$ och $f(-1) > 0$.

Observera att talen p_n är positiva för alla $n \geq -1$ (eftersom $a_0 > 0$). Följaktligen är $f(0) = -p_{r-2} < 0$. Vidare ser vi att

$$\begin{aligned} f(-1) &= q_{r-1} - q_{r-2} + p_{r-1} - p_{r-2} = (a_{r-1} - 1)(q_{r-2} + p_{r-2}) + q_{r-3} + p_{r-3} \\ &\geq q_{r-3} + p_{r-3} > 0. \end{aligned}$$

Talet ξ är således reducerat.

För att slutligen bevisa att $-1/\xi'$ har den angivna kedjebråksutvecklingen antar vi att $\xi = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle$. Genom att konjugera sambandet $\xi_n = 1/(\xi_{n-1} - a_{n-1})$ får vi $\xi'_n = 1/(\xi'_{n-1} - a_{n-1})$, som kan skrivas om som

$$-1/\xi'_n = a_{n-1} + \frac{1}{-1/\xi'_{n-1}} \quad \text{för alla } n \geq 1.$$

Eftersom $-1/\xi'_n > 1$ för alla n, kan ovanstående likhet uttryckas som kedjebråksutvecklingen

$$-1/\xi'_n = \langle a_{n-1}, -1/\xi'_{n-1} \rangle.$$

Genom att starta med $-1/\xi'_r$, upprepa och använda det faktum att $\xi = \xi_0 = \xi_r$ får vi alltså

$$\begin{aligned} -1/\xi' &= -1/\xi'_0 = -1/\xi'_r = \langle a_{r-1}, -1/\xi'_{r-1} \rangle = \langle a_{r-1}, a_{r-2}, -1/\xi'_{r-2} \rangle = \ldots \\ &= \langle a_{r-1}, a_{r-2}, \ldots, a_1, a_0, -1/\xi'_0 \rangle, \end{aligned}$$

vilket innebär att $-1/\xi' = \langle \overline{a_{r-1}, a_{r-2}, \ldots, a_1, a_0} \rangle$. □

EXEMPEL 2 Det kvadratiskt irrationella talet $(2+\sqrt{10})/3$ är reducerat. Vi beräknar talets kedjebråksutveckling med hjälp av sats 23.10.

Eftersom $3|(10-2^2)$ kan vi starta med $u_0=2$, $v_0=3$ och $d=10$, och de följande beräkningarna är sammanfattade i följande tabell:

n	0	1	2	3
u_n	2	1	2	2
v_n	3	3	2	3
a_n	1	1	2	1

Eftersom $(u_3,v_3)=(u_0,v_0)$ är periodlängden 3 och $(2+\sqrt{10})/3=\langle\overline{1,1,2}\,\rangle$. □

Övningar

23.1 Visa att följden $(v_n)_0^\infty$ i sats 23.10 uppfyller det rekursiva sambandet

$$v_{n+1}=v_{n-1}+a_n(u_n-u_{n+1}).$$

24 Kedjebråksutvecklingen av $\sqrt{d}$

Sats 24.1 *Låt d vara ett positivt tal som inte är en jämn kvadrat. Den enkla kedjebråksutvecklingen av $\sqrt{d}$ har formen*

$$\langle a_0,\overline{a_1,a_2,\ldots,a_{r-1},2a_0}\,\rangle,$$

där $a_0=\lfloor\sqrt{d}\,\rfloor$ och $a_j=a_{r-j}$ for $j=1,\ 2,\ \ldots,\ r-1$.

Bevis. Låt $a_0=\lfloor\sqrt{d}\,\rfloor$ och $\xi=a_0+\sqrt{d}$. Då är talet ξ reducerat eftersom $\xi>1$ och $\xi'=a_0-\sqrt{d}$ uppfyller $-1<\xi'<0$. Enligt sats 23.16 har ξ därför en rent periodisk kedjebråksutveckling som börjar med $\lfloor\xi\rfloor=2a_0$, vilket betyder att vi kan skriva ξ på formen

$$(1)\qquad \xi=a_0+\sqrt{d}=\langle\overline{2a_0,a_1,a_2,\ldots,a_{r-1}}\,\rangle=\langle 2a_0,\overline{a_1,a_2,\ldots,a_{r-1},2a_0}\,\rangle.$$

Om vi subtraherar a_0 från båda sidorna får vi

$$\sqrt{d}=\langle a_0,\overline{a_1,a_2,\ldots,a_{r-1},2a_0}\,\rangle.$$

För att visa att följden $a_1,\ a_2,\ \ldots,\ a_{r-1}$ är "symmetrisk" noterar vi att

$$\xi=a_0+\sqrt{d}=2a_0+\sqrt{d}-a_0=2a_0-\xi'=2a_0+\frac{1}{-1/\xi'}=\langle 2a_0,-1/\xi'\rangle.$$

Enligt sats 23.16 är

$$-1/\xi'=\langle\overline{a_{r-1},a_{r-2},\ldots,a_1,2a_0}\,\rangle$$

och följaktligen

$$\xi=\langle 2a_0,\overline{a_{r-1},a_{r-2},\ldots,a_1,2a_0}\,\rangle.$$

En jämförelse med (1) ger nu att $a_j=a_{r-j}$ for $1\le j\le r-1$. □

EXEMPEL 1 För att beräkna kedjebråksutvecklingen av $\sqrt{19}$ används sats 23.10 med $u_0 = 0$, $v_0 = 1$ och $d = 19$. Detta resulterar i följande tabell:

n	0	1	2	3	4	5	6	7
u_n	0	4	2	3	3	2	4	4
v_n	1	3	5	2	5	3	1	3
a_n	4	2	1	3	1	2	8	2

Det följer att kedjebråket har periodlängd 6 och att

$$\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle. \qquad \square$$

Sats 24.2 *Låt (p_n, q_n) beteckna den n:te konvergenten till $\sqrt{d}$, låt talen u_n och v_n vara definierade för talet $\xi = \sqrt{d}$ som i sats 23.10, dvs. $\xi_n = (u_n + \sqrt{d})/v_n$ med $v_n | (d - u_n^2)$, och låt r vara periodlängden hos kedjebråksutvecklingen av $\sqrt{d}$. Då gäller:*

(i) $p_n^2 - dq_n^2 = (-1)^{n-1} v_{n+1}$ *för* $n \geq -1$;

(ii) $v_n > 0$ *för* $n \geq 0$;

(iii) $v_n = 1$ *om och endast om* $r | n$.

Bevis. Sätt $\sqrt{d} = \langle a_0, a_1, a_2, \dots \rangle = \langle a_0, a_1, \dots, a_n, \xi_{n+1} \rangle$.

(i) Det gäller att

$$\sqrt{d} = \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}} = \frac{(u_{n+1} + \sqrt{d}) p_n + v_{n+1} p_{n-1}}{(u_{n+1} + \sqrt{d}) q_n + v_{n+1} q_{n-1}},$$

vilket också kan skrivas som

$$u_{n+1} p_n + v_{n+1} p_{n-1} - d q_n - (u_{n+1} q_n + v_{n+1} q_{n-1} - p_n)\sqrt{d} = 0.$$

Eftersom talet $\sqrt{d}$ är irrationellt, följer det att

$$\begin{cases} u_{n+1} p_n + v_{n+1} p_{n-1} - d q_n = 0 \\ u_{n+1} q_n + v_{n+1} q_{n-1} - p_n = 0. \end{cases}$$

Genom att eliminera u_{n+1} från ekvationssystemet får vi

$$p_n^2 - d q_n^2 = v_{n+1}(p_n q_{n-1} - q_n p_{n-1}) = (-1)^{n-1} v_{n+1},$$

där vi har använt sats 20.5 för att få den sista likheten.

(ii) Konvergenterna p_n/q_n är $> \sqrt{d}$ om n är udda och $< \sqrt{d}$ om n är jämnt. Därför har $p_n^2 - d q_n^2$ samma tecken som $(-1)^{n-1}$, så det följer av (i) att v_{n+1} är positivt för $n \geq -1$.

(iii) Eftersom $\xi = \sqrt{d}$ har periodlängd r är $\xi_{kr+1} = \xi_1$ för alla positiva tal k. Det följer

$$\xi_{kr} - a_{kr} = \frac{1}{\xi_{kr+1}} = \frac{1}{\xi_1} = \xi_0 - a_0 = -a_0 + \sqrt{d},$$

dvs. $\xi_{kr} = a_{kr} - a_0 + \sqrt{d}$. Följaktligen är $v_{kr} = 1$ (och $u_{kr} = a_{kr} - a_0$).

Antag omvänt att $v_n = 1$; då är $\xi_n = u_n + \sqrt{d}$, så $a_n = \lfloor \xi_n \rfloor = u_n + \lfloor \sqrt{d} \rfloor = u_n + a_0$ och $\xi_n - a_n = \sqrt{d} - a_0 = \xi_0 - a_0$, dvs. $\xi_{n+1} = 1/(\xi_n - a_n) = 1/(\xi_0 - a_0) = \xi_1$. Härav följer att n är en multipel av periodlängden r. $\square$

I kedjebråksutvecklingen av talet $\sqrt{19}$ i exempel 1 är alla talen i perioden utom det sista $\leq a_0$ medan den sista är lika med $2a_0$. Motsvarande gäller generellt; vi har nämligen följande resultat.

Sats 24.3 *Låt* $\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0} \rangle$. *Då är* $a_n \leq a_0$ *för* $1 \leq n \leq r-1$.

Bevis. Sätt $\xi = \xi_0 = \sqrt{d}$, låt $\xi_n = (u_n + \sqrt{d})/v_n$ vara som i sats 23.10 och antag att $1 \leq n \leq r-1$. Då är $v_n \geq 2$ enligt föregående sats, och genom att använda lemma 23.11 drar vi slutsatsen att $\xi_n' = (u_n - \sqrt{d})/v_n < 0$, ty $\xi_0' = -\sqrt{d} < 0$. Det följer att $u_n - \sqrt{d} < 0$, dvs. $u_n < \sqrt{d}$ och $\xi_n < 2\sqrt{d}/v_n \leq \sqrt{d}$. Alltså är $a_n = \lfloor \xi_n \rfloor \leq \lfloor \sqrt{d} \rfloor = a_0$. □

Övningar

24.1 Visa att kedjebråksutvecklingen av $\sqrt{d}$ har periodlängd 1 om och endast om $d = n^2 + 1$ för något heltal $n \geq 1$.

25 Pells ekvation

Ekvationen $x^2 - dy^2 = N$, med givna nollskilda heltal d och N, kallas *Pells ekvation*. Om d är negativt, så kan Pells ekvation bara ha ett ändligt antal heltalslösningar eftersom $x^2 \leq N$ och $y^2 \leq -N/d$.

Om $d = a^2$ är en jämn kvadrat, så är $(x + ay)(x - ay) = N$, och det finns åter bara ett ändligt antal heltalslösningar till Pells ekvation eftersom det bara finns ändligt många sätt att faktorisera talet N.

Vi kommer därför fortsättningsvis att antaga att *d är ett positivt heltal som inte är en jämn kvadrat.* Vi ska visa att i det fallet finns det antingen ingen heltalslösning alls eller oändligt många heltalslösningar. För $N = \pm 1$ kommer vi att ge en fullständig beskrivning av lösningsmängden.

Om (u, v) är en heltalslösning till Pells ekvation $x^2 - dy^2 = N$, så är $(\pm u, \pm v)$ också en lösning för varje teckenkombination. För att hitta alla heltalslösningar räcker det således att hitta alla *positiva* lösningar, dvs. alla heltalslösningar (u, v) med $u > 0$ och $v > 0$. Om N är en jämn kvadrat, så finns det förstås ytterligare två triviala lösningar $(\pm\sqrt{N}, 0)$, och om $-N/d$ råkar vara ett heltal som är en jämn kvadrat, så är $(0, \pm\sqrt{-N/d})$ två triviala lösningar till Pells ekvation.

Om (x_1, y_1) och (x_2, y_2) är två positiva lösningar till ekvationen $x^2 - dy^2 = N$, så är $x_1^2 - x_2^2 = d(y_1^2 - y_2^2)$, varav följer att $x_1 < x_2$ om och endast om $y_1 < y_2$. Om vi ordnar de positiva lösningarna efter växande x-värden eller efter växande y-värden, så erhåller vi således samma resultat.

Om det finns en positiv heltalslösning till Pells ekvation, så finns det uppenbarligen en positiv lösning (x_1, y_1) med minsta möjliga x-värde. Denna lösning har också minsta möjliga y-värde av alla positiva lösningar. Eftersom den spelar en speciell roll inför vi följande definition.

Definition 25.1 Antag att Pells ekvation $x^2 - dy^2 = N$ har positiva heltalslösningar. Med ekvationens *fundamentallösning*, eller *minsta positiva lösning*, menas den positiva lösning (x_1, y_1) som uppfyller villkoret att $x_1 < u$ och $y_1 < v$ för varje annan positiv lösning (u, v).

Följande sats ger ett samband mellan Pells ekvation och kedjebråk.

Sats 25.2 *Låt d vara ett positivt heltal som inte är en jämn kvadrat och antag att $|N| < \sqrt{d}$. Om (u, v) är en positiv heltalslösning till ekvationen $x^2 - dy^2 = N$, så är $u/v = p_n/q_n$ för någon konvergent (p_n, q_n) till utvecklingen av $\sqrt{d}$ i enkelt kedjebråk.*

Anmärkning. Talen u och v behöver inte vara relativt prima, men om c är deras största gemensamma delare, så gäller uppenbarligen att $c^2|N$. Om talet N är kvadratfritt, dvs. inte är delbart med någon primtalskvadrat, och speciellt om $N = \pm 1$, så är följaktligen u och v relativt prima, och detta innebär att $u = p_n$ och $v = q_n$ för något index n.

Bevis. Vi ska behandla en mer generell situation. Låt d och N vara positiva reella tal, inte nödvändigtvis heltal, sådana att $\sqrt{d}$ är irrationellt och $N < \sqrt{d}$, och antag att u och v är positiva heltal och $u^2 - dv^2 = N$.

Eftersom

$$\big(\frac{u}{v} - \sqrt{d}\big)\big(\frac{u}{v} + \sqrt{d}\big) = \frac{u^2 - dv^2}{v^2} = \frac{N}{v^2}$$

och den andra faktorn i vänsterledet är positiv, drar vi först slutsatsen att $u/v - \sqrt{d} > 0$. Det följer att $u/v + \sqrt{d} > 2\sqrt{d}$ och att

$$0 < \frac{u}{v} - \sqrt{d} = \frac{N}{v^2(u/v + \sqrt{d})} < \frac{\sqrt{d}}{2v^2\sqrt{d}} = \frac{1}{2v^2}.$$

Enligt sats 22.5 är u/v en konvergent till $\sqrt{d}$.

Låt nu d och N vara som i formuleringen av satsen. Fallet $N > 0$ är ett specialfall av det fall som vi just har bevisat.

Om $N < 0$, skriver vi om ekvationen som $y^2 - (1/d)x^2 = -N/d$. Eftersom $0 < -N/d < \sqrt{d}/d = \sqrt{1/d}$ kan vi tillämpa ovanstående generella fall med slutsatsen att v/u är en konvergent till $1/\sqrt{d}$. Antag att $\sqrt{d}$ har kedjebråksutvecklingen $\langle a_0, a_1, a_2, \dots \rangle$. Då är $1/\sqrt{d} = \langle 0, \sqrt{d} \rangle = \langle 0, a_0, a_1, a_2, \dots \rangle$, och följaktligen är

$$\frac{v}{u} = \langle 0, a_0, a_1, \dots, a_n \rangle = \frac{1}{\langle a_0, a_1, \dots, a_n \rangle}$$

för något n. Men då är $u/v = \langle a_0, a_1, \dots, a_n \rangle$ en konvergent till $\sqrt{d}$. □

Genom att kombinera satsen ovan med sats 24.2 får vi en fullständig beskrivning av lösningsmängden till Pells ekvation i fallet $N = \pm 1$.

Sats 25.3 *Antag att d är ett positivt heltal som inte är en jämn kvadrat och låt r vara periodlängden i den enkla kedjebråksutvecklingen av $\sqrt{d}$. Låt slutligen (p_n, q_n) beteckna den n:te konvergenten i kedjebråksutvecklingen.*

(i) Om periodlängden r är jämn, så

- *(a) har ekvationen $x^2 - dy^2 = -1$ inga heltalslösningar;*
- *(b) ges alla positiva heltalslösningar till $x^2 - dy^2 = 1$ av $x = p_{kr-1}$, $y = q_{kr-1}$ för $k = 1, 2, 3, \dots$, med $x = p_{r-1}$ och $y = q_{r-1}$ som fundamentallösningen.*

(ii) Om r är udda, så

(a) ges alla positiva heltalslösningar till $x^2 - dy^2 = -1$ av $x = p_{kr-1}$, $y = q_{kr-1}$ för $k = 1, 3, 5, \ldots$, med $x = p_{r-1}$ och $y = q_{r-1}$ som fundamentallösning;

(b) ges alla positiva heltalslösningar till $x^2 - dy^2 = 1$ av $x = p_{kr-1}$, $y = q_{kr-1}$ för $k = 2, 4, 6, \ldots$, med $x = p_{2r-1}$ och $y = q_{2r-1}$ som fundamentallösning.

Bevis. Enligt föregående sats finns de positiva heltalslösningarna till ekvationen $x^2 - dy^2 = \pm 1$ bland konvergenterna (p_n, q_n). Vidare är $a_0 = \lfloor \sqrt{d} \rfloor \geq 1$, så följden $(p_n)_{n=0}^{\infty}$ är strängt växande. Fundamentallösningen är därför den första lösningen som uppträder i följden (p_n, q_n).

Enligt sats 24.2 är $p_n^2 - dq_n^2 = (-1)^{n-1} v_{n+1}$, där $v_n \geq 1$ för alla n och $v_n = 1$ om och endast om $r|n$. Följaktligen är $|p_n^2 - dq_n^2| \geq 2$ utom när $n = kr - 1$ för något icke-negativt heltal k, då istället

$$p_n^2 - dq_n^2 = (-1)^{kr}.$$

Om r är jämnt, så är $(-1)^{kr} = 1$ för alla k, och (p_{kr-1}, q_{kr-1}) är följaktligen en lösning till $x^2 - dy^2 = 1$ för alla k, medan ekvationen $x^2 - dy^2 = -1$ saknar positiv lösning och naturligtvis då också saknar heltalslösning. Detta visar (i).

Om periodlängen r är udda, så är $(-1)^{kr} = 1$ för jämna k, och $= -1$ för udda k, och detta bevisar (ii). □

EXEMPEL 1 Vi ska använda sats 25.3 för att bestämma fundamentallösningen till ekvationen $x^2 - 19y^2 = 1$. Kedjebråksutvecklingen $\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle$ beräknades i föregående avsnitt. Eftersom periodlängden är 6, är fundamentallösningen $(x, y) = (p_5, q_5)$. Konvergenterna har beräknats i följande tabell:

n	-2	-1	0	1	2	3	4	5
a_n			4	2	1	3	1	2
p_n	0	1	4	9	13	48	61	170
q_n	1	0	1	2	3	11	14	39

Fundamentallösningen är således $(x, y) = (170, 39)$. □

Sats 25.3 ger en metod för att beräkna de successiva lösningarna till Pells ekvation, men det är tidsödande att beräkna konvergenterna (p_n, q_n). När man funnit fundamentallösningen kan man bestämma de återstående positiva lösningarna på ett enklare sätt, som kommer att beskrivas i sats 25.6 nedan.

Lemma 25.4 *Låt (x_1, y_1) vara en godtycklig heltalslösning till $x^2 - dy^2 = M$, låt (x_2, y_2) vara en godtycklig heltalslösning till $x^2 - dy^2 = N$, och definiera heltalen u och v genom ekvationen*

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = u + v\sqrt{d},$$

dvs. $u = x_1x_2 + y_1y_2d$ och $v = x_1y_2 + x_2y_1$.

Då är (u, v) en lösning till $x^2 - dy^2 = MN$. Om (x_1, y_1) och (x_2, y_2) är positiva lösningar, så är också (u, v) positiv.

Bevis. Konjugering ger att $(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = u - v\sqrt{d}$, och följaktligen är

$$\begin{aligned} u^2 - dv^2 &= (u + v\sqrt{d})(u - v\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) \\ &= (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = MN. \end{aligned}$$

Lösningen (u, v) är uppenbarligen positiv om de ursprungliga lösningarna är positiva. □

Korollarium 25.5 *Om ekvationen $x^2 - dy^2 = N$ har en heltalslösning, så har den oändligt många heltalslösningar.*

Bevis. Antag att ekvationen $x^2 - dy^2 = N$ har åtminstone en heltalslösning. Denna lösning, multiplicerad som i lemmat med en godtycklig heltalslösning till $x^2 - dy^2 = 1$, resulterar i en ny lösning till $x^2 - dy^2 = N$, och eftersom ekvationen $x^2 - dy^2 = 1$ har oändligt många heltalslösningar, får vi oändligt många heltalslösningar till ekvationen $x^2 - dy^2 = N$. □

Sats 25.6 *Låt (x_1, y_1) vara fundamentallösningen till ekvationen $x^2 - dy^2 = 1$. Då ges alla positiva heltalslösningar som (x_n, y_n), $n \geq 1$, där heltalen x_n och y_n definieras rekursivt av sambanden*

$$x_{n+1} = x_1x_n + y_1y_nd, \quad y_{n+1} = x_1y_n + y_1x_n.$$

Bevis. Notera att $x_{n+1} + y_{n+1}\sqrt{d} = (x_1 + y_1\sqrt{d})(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^{n+1}$. Om (x_n, y_n) är en positiv heltalslösning till Pells ekvation $x^2 - dy^2 = 1$, så är därför (x_{n+1}, y_{n+1}) också en positiv heltalslösning enligt lemma 25.4 med $M = N = 1$. Det följer därför med induktion att (x_n, y_n) är en lösning för alla n.

Det återstår att visa att varje positiv heltalslösning fås på detta sätt. Antag därför att det finns en positiv heltalslösning (u, v) som inte har formen (x_n, y_n). Eftersom x_n bildar en växande följd, måste det finnas ett heltal m sådant att $x_m \leq u < x_{m+1}$. Det följer att $y_m \leq v < y_{m+1}$, ty vi får samma resultat om de positiva lösningarna ordnas efter sina x-värden som efter sina y-värden. Det kan inte råda likhet eftersom $u = x_m$ skulle medföra att $v = y_m$.

Nu är förstås $(x_m, -y_m)$ också en (icke-positiv) heltalslösning till ekvationen $x^2 - dy^2 = 1$, så enligt lemma 25.4 får vi en lösning (s, t) genom att definiera

$$s + t\sqrt{d} = (u + v\sqrt{d})(x_m - y_m\sqrt{d}) = \frac{u + v\sqrt{d}}{x_m + y_m\sqrt{d}}\,.$$

Eftersom $x_m + y_m\sqrt{d} < u + v\sqrt{d} < x_{m+1} + y_{m+1}\sqrt{d}$, är

$$1 < s + t\sqrt{d} < \frac{x_{m+1} + y_{m+1}\sqrt{d}}{x_m + y_m\sqrt{d}} = x_1 + y_1\sqrt{d}.$$

Men $s - t\sqrt{d} = 1/(s + t\sqrt{d})$, så $0 < s - t\sqrt{d} < 1$, och det följer att

$$\begin{aligned} s &= \tfrac{1}{2}(s + t\sqrt{d}) + \tfrac{1}{2}(s - t\sqrt{d}) > \tfrac{1}{2} + 0 > 0 \\ t\sqrt{d} &= \tfrac{1}{2}(s + t\sqrt{d}) - \tfrac{1}{2}(s - t\sqrt{d}) > \tfrac{1}{2} - \tfrac{1}{2} = 0. \end{aligned}$$

Lösningen (s,t) är med andra ord positiv, och därför gäller att $s > x_1$ och $t > y_1$, men detta strider mot att $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Denna motsägelse visar att varje positiv heltalslösning (u,v) måste ha formen (x_n, y_n). □

EXEMPEL 2 I exempel 1 visade vi att fundamentallösningen till ekvationen

$$x^2 - 19y^2 = 1$$

är $(x_1, y_1) = (170, 39)$. Med hjälp av rekursionsformlerna

$$x_n = x_1x_n + 19y_1y_n, \;\; y_n = x_1y_n + y_1x_n,$$

kan vi beräkna nästkommande positiva lösningar som är

$$\begin{aligned}(x_2, y_2) &= (57\,799, 13\,260)\\ (x_3, y_3) &= (19\,651\,490, 4\,508\,361)\\ (x_4, y_4) &= (6\,681\,448\,801, 1\,532\,829\,480).\end{aligned}$$ □

Precis som i fallet $x^2 - dy^2 = 1$ kan man bestämma ytterligare lösningar till ekvationen $x^2 - dy^2 = -1$ med utgångspunkt från ekvationens fundamentallösning. Beviset för följande sats lämnas åt läsaren.

Sats 25.7 *Antag att ekvationen $x^2 - dy^2 = -1$ har en heltalslösning och låt (x_1, y_1) vara dess fundamentallösning. Definiera talen x_n och y_n rekursivt för $n \geq 1$ som i sats 25.6, dvs. $(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^n$. Då fås alla positiva heltalslösningar till $x^2 - dy^2 = -1$ som (x_n, y_n) med udda index n, och alla positiva heltalslösningar till $x^2 - dy^2 = 1$ som (x_n, y_n) med jämnt index n. Speciellt är alltså (x_2, y_2) fundamentallösningen till ekvationen $x^2 - dy^2 = 1$.*

Övningar

25.1 Bestäm fundamentallösningen till ekvationerna
a) $x^2 - 5y^2 = 1$, b) $x^2 - 7y^2 = 1$.

25.2 Bestäm fundamentallösningen till ekvationerna
a) $x^2 - 41y^2 = 1$, b) $x^2 - 41y^2 = -1$.

25.3 Bestäm alla positiva lösningar till $x^2 - 3y^2 = 1$ med $y < 100$.

25.4 Låt k vara ett positivt heltal och låt d vara ett positivt heltal som inte är ett kvadrattal. Visa att det finns oändligt många lösningar till $x^2 - dy^2 = 1$ för vilka y är en multipel av k.

Svar till övningarna

1.1 a) ±1, ±2, ±5, ±10 b) 1, 2, 5, 10 c) ±2, ±5

1.2 a) 3 b) 2 c) 1 d) 0

1.3 150

1.4 a) b) c) 2

1.5 a) Ja b) Nej

1.6 a) $25 = 3 \cdot 7 + 4$ b) $-25 = (-4) \cdot 7 + 3$

1.7 a) $25 = 4 \cdot 7 - 3$ b) $28 = 3 \cdot 8 + 4$

1.8 a) 1 b) 13 c) 71

1.9 a) 2520 b) 60 c) $n(n+1)$ d) $4^n - 1$

1.10 $(a, b) = (10, 1)$, $(10, 2)$, $(10, 5)$, $(10, 10)$, $(5, 2)$

1.13 d) Utnyttja att $n(n-1)\cdots(n-k+1) = \binom{n}{k} \cdot k!$. Detta löser problemet om alla talen är positiva. Om ett av de k talen är noll är förstås produkten noll, och om alla talen är negativa återför vi problemet på fallet att alla är positiva genom att bryta ut $(-1)^k$.

1.14 a) $n^k - 1 = (n-1)(n^{k-1} + n^{k-2} + \cdots + n + 1)$
b) Utnyttja att
$n^k - 1 = (n-1+1)^k - 1 = (n-1)^k + \binom{k}{1}(n-1)^{k-1} + \cdots + \binom{k}{2}(n-1)^2 + k(n-1)$

1.15 Utnyttja att $(a+b)d - (c+d)b = ad - bc = \pm1$. Omvändningen gäller ej; ett motexempel är $a = 5$, $b = 2$, $c = d = 1$.

1.16 Antag $n > m$ och sätt $b = a^{2^m}$ och $k = 2^{n-m}$; då är $a^{2^n} = b^k$. Eftersom $b^k + 1 = (b+1)(b^{k-1} - b^{k-2} + \cdots + b - 1) + 2$, är $\operatorname{sgd}(a^{2^m} + 1, a^{2^n} + 1) = \operatorname{sgd}(b+1, b^k + 1) = \operatorname{sgd}(b+1, 2)$. Eftersom b är jämnt om och endast om a är jämnt, följer nu påståendet.

2.1 a) $2^3 \cdot 3^2 \cdot 5$ b) 271 c) $11 \cdot 271$ d) $2^{20} \cdot 5^{20}$ e) $2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

2.5 $n^4+4 = n^4+4n^2+4-4n^2 = (n^2+2)^2-(2n)^2 = (n^2+2+2n)(n^2+2-2n) = ((n+1)^2+1)((n-1)^2+1)$, vilket är en icke-trivial faktorisering om $n \geq 2$.

2.6 Ett tal som skrivet som decimaltal har $k \cdot m$ stycken ettor är jämnt delbart med talet $n = 11\ldots1$ bestående av exakt k stycken ettor och kan således inte vara ett primtal om $k \geq 2$ och $m \geq 2$.

2.7 Låt $S = 1 + 1/2 + 1/3 + \cdots + 1/n$, låt m vara det största heltalet med egenskapen att $2^m \leq n$, och låt P vara produkten av alla udda tal som är mindre än eller lika med n. Då är varje term i summan $2^{m-1}PS$ ett heltal förutom termen $2^{m-1}P/2^m$. Följaktligen kan inte S vara ett heltal.

2.8 b) Skriv $\lfloor x \rfloor = qm + r$ med $0 \leq r \leq m-1$; då är både $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$ och $\left\lfloor \dfrac{x}{m} \right\rfloor$ lika med q.

2.9 Låt $f(n)$ vara det största k för vilket $p^k \mid n!$. Eftersom primfaktorn p enbart förekommer i talen p, $2p$, $\ldots$, $\lfloor n/p \rfloor p$, förekommer p lika många gånger i $n!$ som i produkten $p \cdot 2p \cdot \cdots \cdot \lfloor n/p \rfloor p = p^{\lfloor n/p \rfloor} \lfloor n/p \rfloor !$. Vi har därför rekursionsformeln $f(n) = \lfloor n/p \rfloor + f(\lfloor n/p \rfloor)$, som implicerar att $f(n) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots$.

2.10 15^{14}

2.11 40

2.12 Utnyttja övningarna 2.8a) och 2.9.

2.13 Utnyttja att produkten av två tal på formen $4k+1$ är ett nytt tal av samma form.

2.14 Antag att det bara finns ändligt många primtal $p_1, p_2, \ldots, p_n$ på formen $4k+3$ och betrakta talet $N = 4p_1p_2 \cdots p_n - 1$ som har formen $4k+3$. Utnyttja föregående övning för att visa att N måste ha en primfaktor på formen $4k+3$ och som då inte kan vara något av primtalen p_i.

3.1 a) $x = 1+2n,\ y = -1-3n$ b) $x = 1+2n,\ y = 1+3n$
c) $x = 1+2n,\ y = -1-3n$ d) $x = 2+2n,\ y = -2-3n$
e) $x = 1+2n,\ y = 49-3n$

3.2 a) $x = 16+43n,\ y = 4+17n$ b) $x = 15-17n,\ y = 31+6n$
c) $x = -1+102n,\ y = 2-101n$ d) $x = -3+87n,\ y = -2+55n$

3.3 15

3.4 a) $x = 3m+2n,\ y = 2-3m-n,\ z = m$
b) $x = 1+4m+3n,\ y = 1-4m-2n,\ z = m$
c) $x = 19+69m+11n,\ y = 3+46m+7n,\ z = m$
d) $x = 3-30m-39n+7k,\ y = -2+20m+26n-5k,\ z = m,\ w = n$

3.5 $x = 160-15n,\ y = 76-79n,\ z = 8+18n$

3.8 a) Om $c \geq (a-1)(b-1) = ab-a-b+1$, så är $c+a+b > ab$. Ekvationen

$$ax + by = c + a + b$$

har därför enligt föregående övning en positiv heltalslösning (x_0, y_0). Men då är $(x_0 - 1, y_0 - 1)$ en icke-negativ heltalslösning till $ax + by = c$.
b) Följer av att ekvationen $ax + by = ab$ saknar positiv heltalslösning.

4.1 a) 9, 18 b) 5, 15 c) 1, 12 d) 15 e) 5 f) inget

4.2 a) 7 b) 3, 11, 33 c) 2, 3, 4, 6, 12

4.4 Visa att $x^5 \equiv x \pmod{10}$ antingen genom prövning för $x = 0, \pm1, \pm2, \pm3, \pm4, 5$, eller alternativt genom att först visa (med hjälp av Fermats sats) att $x^5 \equiv x \pmod 5$ och $x^5 \equiv x \pmod 2$.

4.6 a) Delbart med 7, 11 och 13 b) Delbart med 11 och 13

4.8 b) $n/2$

4.9 a) 0 om n är udda, $n/2$ om n är jämnt.
b) 0 om $n \neq 2$, 1 om $n = 2$. (Utnyttja för $n > 2$ att det reducerade restsystem som fås genom att välja rester med minst absolutbelopp har formen $\pm b_1, \pm b_2, \ldots, \pm b_m$.)

4.10 a) $n \equiv \pm 1 \pmod 6$ b) $n \equiv 0, 1, 3 \pmod 4$

4.11 Respektive 1, 1, 2, 2, 4, 2, 6, 4, 6, 4

4.12 a) $0, \pm 1, \pm 2, \ldots, \pm 9, 10$ b) $\pm 1, \pm 3, \pm 7, \pm 9$

4.14 Ja, t.ex. $\{0, 1, 2, \ldots, m-1\}$ och $\{0, m, 2m, 3m, \ldots, (n-1)m\}$.

4.16 a) 1 b) 6 c) 3

4.17 a) 01 b) 76 c) 93

4.18 a), b) Låt p vara ett primtal $\neq 2, 5$, och låt k vara ett positivt heltal. Fermats sats ger att $10^{k(p-1)} \equiv 1 \pmod p$, dvs. talet $N = 10^{k(p-1)} - 1 = 9999\ldots9$ är delbart med p. Talet $N/9 = 1111\ldots1$ är naturligtvis också delbart med p om $p \neq 3$, och i fallet $p = 3$ är talet $1111\ldots1$ delbart med p om antalet ettor är delbart med 3.

4.20 b) Utnyttja binomialsatsen samt att $p \mid \binom{p}{k}$ för $1 \leq k \leq p-1$.
c) Induktion, där induktionssteget följer av att $(a+1)^p \equiv a^p + 1 \pmod p$.

4.21 Fermats sats ger $a \equiv b \pmod p$, dvs. $a = b + kp$. Av binomialsatsen följer sedan att $a^p = (b+kp)^p = b^p + mp^2$.

6.1 a) $x \equiv 12 \pmod{15}$ b) Lösning saknas c) $x \equiv 2, 7, 12 \pmod{15}$
d) $x \equiv 132, 395, 658 \pmod{789}$ e) $x \equiv 54, 161, 268 \pmod{321}$

6.2 a) 0 b) 1 c) 3 d) 15

6.3 Enligt Eulers sats är $7^8 \equiv 1 \pmod{20}$. Om $7x \equiv 11 \pmod{20}$, så är därför $x \equiv 7^8 x \equiv 7^7 \cdot 11 \equiv 13 \pmod{20}$.

6.4 a) $x \equiv 14 \pmod{15}$ b) $x \equiv 10 \pmod{23}$ c) Lösning saknas

7.1 a) $x \equiv 187 \pmod{420}$ b) Lösning saknas c) $x \equiv 68 \pmod{210}$
d) $x \equiv 249 \pmod{495}$

7.2 $154a + 210b + 99c \pmod{462}$

7.3 58

7.4 Låt $p_1, p_2, \ldots, p_k$ vara olika primtal; enligt kinesiska restsatsen finns det ett heltal x så att $x + j \equiv 0 \pmod{p_j^2}$ för $1 \leq j \leq k$.

7.5 a) 40 b) $2^{11} \cdot 3^4 \cdot 5 = 829\,440$

7.6 a) 40 b) 60 c) $\phi(50) = 20$

7.7 $\phi(n/d)$

7.8 $n = 1$ och $n = 2$.

7.9 Alla udda tal n.

7.10 Eftersom $\operatorname{sgd}(a, n) = 1 \Leftrightarrow \operatorname{sgd}(n-a, n) = 1$ och $1 \leq a \leq n-1 \Leftrightarrow 1 \leq n-a \leq n-1$, är $\sum a = \sum (n-a) = \sum n - \sum a$, där summan tas över alla a sådana att $\operatorname{sgd}(a, n) = 1$ och $1 \leq a \leq n-1$. Det följer att $2\sum a = \sum n = n \sum 1 = n\phi(n)$.

7.11 a) $n = 2^{m_1} 3^{m_2}$, där $m_1, m_2 \geq 1$.
b) $n = 2^{m_1} 3^{m_2} 7^{m_3}$, där $m_1, m_2, m_3 \geq 1$.

7.12 a) 3 b) 14.

7.13 35, 39, 45, 52, 56, 70, 72, 78, 84, 90

8.1 a) $d = 53$ b) Det krypterade talet är $b = 85$.

9.1 a) $x^2 \equiv 0 \pmod 2$ b) $-x^3 + 1 \equiv 0 \pmod 3$ c) $-x^2 \equiv 0 \pmod 4$
d) $2x - 1 \equiv 0 \pmod 5$ e) $-2x^3 + 4x^2 + x + 4 \equiv 0 \pmod{11}$

9.2 a) $x \equiv 0 \pmod 2$ b) $x^2 - x \equiv 0 \pmod 3$
c) $3x^4 + 2x^3 + 4x^2 + x + 1 \equiv 0 \pmod 5$

9.4 $(x-1)(x+11) \equiv 0 \pmod{17}$; rötter $x \equiv 1,\ 6 \pmod{17}$.

9.5 $x \equiv 1,\ 12 \pmod{25}$

9.6 a) $x \equiv 0 \pmod 2$ b) Lösning saknas c) $x \equiv 1,\ 3 \pmod 5$
d) Lösning saknas e) $x \equiv 2,\ 3 \pmod 7$ f) $x \equiv 6,\ 8 \pmod{10}$
g) $x \equiv 3,\ 16,\ 23,\ 31 \pmod{35}$

9.7 a) $x \equiv 0 \pmod 2$ b) $x \equiv 1 \pmod 3$ c) $x \equiv 0,\ 2 \pmod 4$
d) $x \equiv 3 \pmod 5$ e) $x \equiv 8,\ 18 \pmod{20}$.

9.8 a) 2 b) 2 c) 4 d) 16. Exempelvis $a = 1$, $b = 0$.

10.1 a) $x \equiv 16,\ 106 \pmod{121}$ b) $x \equiv 271 \pmod{625}$
c) $x \equiv -12 \pmod{250}$

10.2 a) $k = 1$: 2 lösningar, $k \geq 2$: 1 lösning
b) $k = 1$: 1 lösning, $k = 2,\ 3$: 3 lösningar, $k \geq 4$: ingen lösning.

10.3 a) 0 b) 1 c) 3 för alla värden på k.

10.4 $x \equiv 0,\ 1,\ 126,\ 250 \pmod{375}$

11.2 $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv 1 \cdot 3 \cdots (p-2) \cdot (-2) \cdot (-4) \cdots (-(p-1))$
$\equiv (-1)^{(p-1)/2}(p-1)! \pmod p$.
Den till beloppet minsta resten är $(-1)^{(p+1)/2}$.

11.4 $x \equiv 6! \equiv 5 \pmod{13}$

11.6 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18

11.7 a) Rest b) Ickerest

11.8 a) 2 b) 2 c) 2 d) 0

11.9 a) 1 b) 2 c) 4 d) 4 e) 4

11.10 a) 1 b) 2 c) 0 d) 2 e) 4 f) 0 g) 4 h) 4 i) 0

12.1 a) $y^2 \equiv 9 \pmod{10}$, $y = x + 2$ b) $y^2 \equiv 29 \pmod{40}$, $y = 2x + 3$
c) $y^2 \equiv 7 \pmod 9$, $y = 2x + 3$ d) $y^2 \equiv 22 \pmod{27}$, $y = 6x + 1$

13.1 a) nej b) ja c) ja d) nej e) ja

13.2 a) -1 b) 1 c) -1 d) 1 e) -1

13.3 -1

13.7 Utnyttja att exakt hälften av talen a i intervallet $1 \leq a \leq p-1$ är kvadratiska rester.

13.8 b) Utnyttja att 2 är en kvadratisk ickerest modulo p, dvs. $2^{(p-1)/2} \equiv -1 \pmod p$.
c) $x \equiv \pm 6 \pmod{19}$ d) $x \equiv \pm 12 \pmod{29}$

14.1 a) 1 b) -1 c) -1 d) 1 e) -1

14.2 a), b) c) ej lösbara d) lösbar e) ej lösbar f) lösbar

14.4 För $p = 2$ och för $p = 6n + 1$.

14.5 89

15.1 a) 4 b) 4 c) 2

15.2 3 eller 5

15.3 Utnyttja att $b^n \equiv 1 \pmod{m} \Rightarrow a^n \equiv a^n b^n \equiv (ab)^n \equiv 1 \pmod{m}$.

15.4 25

15.5 6 primitiva rötter; dessa är 2, 3, 10, 13, 14, 15.

15.6 $\operatorname{mgm}(h, k)$

15.8 Med 2 som primitiv rot får vi tabellen

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} a$	12	1	4	2	9	5	11	3	8	10	7	6

15.9 a) $x \equiv \pm 10 \pmod{67}$ b) lösning saknas c) $x \equiv -11 \pmod{67}$

15.10 $p = 2$, $p = 3$ och $p = 6n + 5$

15.11 a) 2 b) 27 c) 3 d) 3

15.12 Nej, ty för udda primtal p är $4^{(p-1)/2} = 2^{p-1} \equiv 1 \pmod{p}$, vilket medför att $\operatorname{ord} 4 < \phi(p)$.

15.14 Kongruensen $x^2 \equiv 1 \pmod{p}$ har rötterna ± 1. Eftersom $(g^{(p-1)/2})^2 \equiv 1 \pmod{p}$ och g:s ordning är $p - 1$ är därför $g^{(p-1)/2} \equiv -1 \pmod{p}$.

15.17 a) Följer av Eulers kriterium och övning 15.14.

15.18 a) Eftersom 2^n inte har någon primitiv rot är $\operatorname{ord} a < \phi(2^n) = 2^{n-1}$, och det följer att $\operatorname{ord} a \mid 2^{n-2}$.
b) Visa med induktion att $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$.

15.19 b) Det räcker att visa påståendet då $n = p^k$ är en primtalspotens. Använd Eulers sats för udda p och övning 15.18 a) för $p = 2$ och $k \geq 3$.
c) Skriv $n = P_1 P_2 \cdots P_k$ som en produkt av olika primtalspotenser och börja med att bevisa att det för varje i finns ett tal a_i som har ordning $\lambda(P_i)$ modulo P_i. Fallen $P_i = 2$ och $P_i = 4$ är uppenbara, om $P_i = 2^m$ med $m \geq 3$ kan vi använda övning 15.18, och om P_i är en potens av ett udda primtal låter vi a_i vara en primitiv rot till P_i. Enligt den kinesiska restsatsen finns det ett tal a som är kongruent med a_i modulo n för varje i. Avsluta beviset genom att visa att $\operatorname{ord} a = \lambda(n)$.
d) $\lambda(360) = 12$, $\phi(360) = 96$.
e) T.ex. 7.

15.20 a) Enligt föregående övning finns det ett tal a av ordning $\lambda(n)$. Eftersom $a^{n-1} \equiv 1 \pmod{n}$, gäller därför att $\lambda(n) \mid (n - 1)$.
b) Eftersom $\lambda(n)$ är ett jämnt tal för $n \geq 3$, följer det av a) att n är udda.
c) För udda primtal p följer implikationen $p^2 \mid n \Rightarrow p \mid \lambda(n)$ av Carmichaelfunktionens definition. Om p^2 delar n så delar därför p talet $n - 1$ på grund av a), och detta är förstås en motsägelse.

15.20 d) Följer av a) eftersom $(p_i - 1) \mid \lambda(n)$.
e) Antag $n = pq$ är ett Carmichaeltal, där $q < p$ är udda primtal. Eftersom $(p-1) \mid (pq-1)$ är $pq - 1 = x(p-1)$ för något heltal x. Olikheten $pq - q < pq - 1 = x(p-1)$ ger att $x > q$, så $x \geq q + 1$. Men detta leder till motsägelsen $pq - 1 \geq (q+1)(p-1) = pq + p - q - 1 \geq pq$.

16.1 a) 12 b) 168 c) 5460

16.2 a) $n = p^3$ eller $n = pq$
b) $n = p^5$ eller $n = p^2q$ (där p och q är olika primtal)
c) $n = 7$ d) inget n.

16.5 $\left(\prod_{d|n} d\right)^2 = \left(\prod_{d|n} d\right)\left(\prod_{d|n} \frac{n}{d}\right) = \prod_{d|n} n = n^{\tau(n)}$.

16.6 $\sum_{n=1}^{N} \tau(n) = \sum_{k=1}^{N} \lfloor \frac{N}{k} \rfloor$, $\quad \sum_{n=1}^{N} \sigma(n) = \sum_{k=1}^{N} k \lfloor \frac{N}{k} \rfloor$

16.7 a) 1 b) 0 c) -1

16.9 a) $(-1)^r$ b) $(-1)^r p_1 p_2 \cdots p_r$ c) $(2-p_1)(2-p_2)\cdots(2-p_r)$ d) 2^r

16.10 Använd formeln i övning 16.6.

16.13 b) Sätt $n = 2^{m-1}a$, där $m \geq 2$ och a är udda. Om n är ett perfekt tal så är $2^m a = 2n = \sigma(n) = (2^m - 1)\sigma(a)$, vilket medför att $2^m \mid \sigma(a)$. Skriv $\sigma(a) = 2^m k$; då är $a = (2^m - 1)k$, och vi drar slutsatsen att k är udda eftersom a är udda. Om $k \geq 3$, så är

$$\sigma(a) = \sigma((2^m - 1)k) \geq 1 + (2^m - 1) + k + (2^m - 1)k = 2^m(1 + k) > 2^m k,$$

och om $k = 1$ och $2^m - 1$ inte är ett primtal är

$$\sigma(a) = \sigma(2^m - 1)) > 1 + (2^m - 1) = 2^m k.$$

I båda dessa fall blir därför

$$\sigma(n) = (2^m - 1)\sigma(a) > (2^m - 1)2^m k = 2^m a = 2n,$$

vilket är en motsägelse. Alltså är $k = 1$ och $2^m - 1$ är ett primtal, och n har formen $2^{m-1}(2^m - 1)$.

17.1 98 och 4680

17.2 Använd lemma 17.2.

17.4 Nödvändigheten av villkoret $p \equiv 1 \pmod 4$ följer av lemma 17.2 (och av att summan $n^2 + (n+1)^2$ är udda). För att visa tillräckligheten utnyttjar vi att -1 är en kvadratisk rest modulo p, om $p \equiv 1 \pmod 4$, genom att välja talet i så att $i^2 \equiv -1 \pmod p$ och $2 \leq i \leq p - 2$. Talet p delar $n^2 + (n+1)^2$ om och endast om $(n+1)^2 \equiv -n^2 \equiv (in)^2 \pmod p$, vilket gäller om $n + 1 \equiv in \pmod p$. Den sistnämnda kongruensen är ekvivalent med $(i-1)n \equiv 1 \pmod p$, som är lösbar eftersom $\text{sgd}(i-1, p) = 1$.

17.5 $1547 = 54^2 - 37^2 = 66^2 - 53^2 = 114^2 - 107^2 = 774^2 - 773^2$. (Skriv ekvationen $x^2 - y^2 = 1547$ på formen $(x+y)(x-y) = 1547$.)

17.6 a) $2m + 1 = (m+1)^2 - m^2$

17.7 Om påståendet är felaktigt så finns det ett minsta k så att $4^k(8m+7) = a^2+b^2+c^2$ är en summa av tre kvadrater. För $k=0$ får vi en motsägelse genom att räkna modulo 8, så det följer att $k \geq 1$. Vi får nu $a^2+b^2+c^2 \equiv 0 \pmod 4$, varav lätt följer att a, b och c är alla jämna tal. Med $a = 2A$, $b = 2B$ och $c = 2C$ får vi då $4^{k-1}(8m+7) = A^2+B^2+C^2$, vilket motsäger att k var den minsta exponenten.

17.8 Sätt $q = \lfloor (3/2)^k \rfloor$; då är $q < (3/2)^k$, så det följer att $n = 2^k q - 1 < 3^k$. För att representera n som en summa av k-potenser kan vi således enbart använda 1^k och 2^k. För att få minimalt antal k-potenser skall vi använda så många kopior av 2^k som möjligt, nämligen $q-1$ stycken. Då återstår det att representera talet $n-(q-1)2^k = 2^k-1$ vilket förstås kräver 2^k-1 kopior av 1^k. Därför behöver vi minst $(q-1)+2^k-1 = 2^k+q-2$ stycken k-potenser för att representera n.

18.1 $(3,4,5)$, $(5,12,13)$, $(8,15,17)$, $(7,24,25)$ och $(20,21,29)$.

18.2 $(32,126)$, $(50,120)$, $(66,112)$ och $(78,104)$.

18.3 a) $(399,40,401)$ och $(9,40,41)$
b) $(399,40,401)$, $(9,40,41)$, $(198,40,202)$, $(42,40,58)$, $(75,40,85)$, $(96,40,104)$ och $(30,40,50)$

18.4 a), c) För en primitiv pythagoreisk trippel (x,y,z) gäller att

$$xyz = 2ab(a^4-b^4) = 2(a^5b-ab^5).$$

Genom att utnyttja Fermats sats ser man att detta är kongruent med 0 modulo 3 och modulo 5.

18.5 Om n är jämnt är $(n^2/4-1, n, n^2/4+1)$ en pythagoreisk trippel, och om n är udda är $((n^2-1)/2, n, (n^2+1)/2)$ en pythagoreisk trippel.

18.6 a) $(5,12,13)$, $(9,12,15)$, $(12,16,20)$ och $(12,35,37)$
b) $(5,12,13)$ och $(13,84,85)$

18.7 $(2n+1, 2n^2+2n, 2n^2+2n+1)$ är för varje n en pythagoreisk trippel med $z = y+1$.

19.1 $x = y = 1$, $z = 2$

19.2 $(x,y) = (3,6)$, $(4,4)$ eller $(6,3)$. (Visa först att $x \leq 4$ eller $y \leq 4$.)

19.4 Antag att $x^4+y^2 = z^4$, där x, y och z är positiva heltal med minsta möjliga värde på z. Visa först att talen är relativt prima. (x^2, y, z^2) är alltså en primitiv pythagoreisk taltrippel.
Om talet y är jämnt finns det därför positiva heltal s och t sådana att $x^2 = s^2-t^2$ och $z^2 = s^2+t^2$. Ihopmultiplikation ger $(xz)^2 = s^4-t^4$, dvs. (t, xz, s) är en ny positiv heltalslösning till den givna diofantiska ekvationen, och eftersom $s < z$ är detta en motsägelse.
Om istället y är udda, kan vi skriva $y = s^2-t^2$, $x^2 = 2st$ och $z^2 = s^2+t^2$, där s och t är relativt prima positiva heltal av olika paritet. Antag att talet s är jämnt (fallet t jämnt är analogt). Eftersom $s/2$ och t är relativt prima och $(s/2)t = (x/2)^2$ är kvadraten på ett heltal, måste såväl $s/2$ som t vara heltalskvadrater, $s = 2m^2$ och $t = n^2$, säg. Eftersom (s,t,z) är en primitiv pythagoreisk trippel finns det vidare relativt prima tal u och v sådana att $s = 2uv$, $t = u^2-v^2$ och $z = u^2+v^2$. Det följer att $uv = m^2$,

så såväl u som v är heltalskvadrater, $u = a^2$ och $v = b^2$, säg. Följaktligen är $n^2 = t = a^4 - b^4$, dvs. (b, n, a) är en ny positiv heltalslösning till den ursprungliga ekvationen, och eftersom $a = \sqrt{u} \leq u^2 < z$ är detta en motsägelse.

19.5 Antag att $a^2+b^2 = c^2$ och $a^2-b^2 = d^2$. Då är $a^4-b^4 = (cd)^2$ (och $d \neq 0$), så ekvationen $x^4+y^2 = z^4$ har en positiv heltalslösning, vilket strider mot övning 19.4.

19.6 Följer av sats 19.2 och övning 19.4.

19.7 Man visar först att om $x^4 + 4y^4 = z^2$, där x, y och z är positiva heltal med minimalt z, så är $(x^2, 2y^2, z)$ en primitiv pythagoreisk trippel. Därför finns det positiva heltal s och t med $(s,t) = 1$ sådana att $x^2 = s^2 - t^2$ och $2y^2 = 2st$. Det följer nu att s och t är heltalskvadrater, $s = m^2$ och $t = n^2$, säg. Men då är $n^4 + x^2 = m^4$, vilket strider mot övning 19.4.

19.8 $x^2 + y^2 = z^2$ och $xy = 2w^2$ medför efter elimination av y att $x^4 + 4w^4 = (xz)^2$. Detta är omöjligt på grund av övning 19.7.

20.1 a) $\langle 0, 4, 1, 1, 9\rangle$ b) $\langle 3, 7\rangle$

20.2 a) 5/3 b) 496/447 c) 496/81 d) 225/43

20.3 a) $\langle 0, a_0, a_1, \ldots, a_n\rangle$ b) $\langle a_0 + 1, a_1, a_2, \ldots, a_n\rangle$

20.4 1, 3/2, 10/7, 43/30, 225/157

20.5 $x = -92 + 327n, \quad y = 83 - 295n, \quad n \in \mathbf{Z}$

20.6 a) $\sqrt{2}$ b) $\frac{1}{2}(1+\sqrt{3})$ c) $\frac{1}{6}(5+\sqrt{13})$ d) $\frac{1}{2}(\sqrt{15}-1)$ e) $\frac{1}{3}(4+\sqrt{37})$

20.7 a) Utnyttja att $q_k/q_{k-1} = a_k + q_{k-2}/q_{k-1}$ för $k \geq 2$, och $q_1/q_0 = a_1$.
b) Utnyttja att $p_k/p_{k-1} = a_k + p_{k-2}/p_{k-1}$ för $k \geq 1$, och $p_0/p_{-1} = a_0$.
Om $a_0 = 0$ är $p_n/p_{n-1} = \langle a_n, a_{n-1}, \ldots, a_2\rangle$.

21.1 a) $\langle 19, 1, 6, 7\rangle$ b) $\langle 3, 7, 16, 11\rangle$ c) $\langle 2, \overline{4}\rangle$ d) $\langle \overline{1}\rangle$ e) $\langle 3, \overline{3, 6}\rangle$
f) $\langle 3, \overline{1, 2, 1, 6}\rangle$

21.2 a) $\langle 2, 1, 2, 1, 1, 4, 1, 1, \ldots\rangle$ b) $\langle 3, 7, 15, \ldots\rangle$ eller $\langle 3, 7, 16, \ldots\rangle$
c) $\langle 1, 3, 1, 5, 1, 1, \ldots\rangle$

21.5 b) $p_1 = 0$ om och endast om $a_0 = -1$ och $a_1 = 1$.

21.7 Utnyttja övning 20.7 b) och satserna 20.5 (ii) och 21.2.

22.1 $p_5/q_5 = 99/70$, $\frac{1}{70\cdot 239} < \frac{99}{70} - \sqrt{2} < \frac{1}{70\cdot 169}$, vilket ger att
$1,41420 < \sqrt{2} < 1,41423$.
$p_6/q_6 = 239/169$, $\frac{1}{169\cdot 577} < \sqrt{2} - \frac{239}{169} < \frac{1}{169\cdot 408}$, vilket ger att
$1,414211 < \sqrt{2} < 1,414216$.

22.2 a) $a = 99$, $b = 70$, nästa $b = 169$ b) $a = 97$, $b = 56$, nästa $b = 153$
c) $a = 22$, $b = 7$, nästa $b = 106$ d) $a = 193$, $b = 71$, nästa $b = 465$,
e) $a = 31$, $b = 14$, nästa $b = 471$

22.3 T.ex. 2/1, 7/4 och 26/15

22.4 Utnyttja att $\dfrac{1}{yb} < \dfrac{bx-ay}{yb} = \dfrac{x}{y} - \dfrac{a}{b} < \dfrac{c}{d} - \dfrac{a}{b} = \dfrac{bc-ad}{db} = \dfrac{1}{db}$ för att få $y > d$.

22.5 a) Visa att derivatan $c'_{n,t}$ (med avseende på t) har konstant tecken.
b) Det gäller att $p_0/q_0 \le a/b \le c_{0,1} = a_0 + 1$. Ty om $a/b < p_0/q_0 = p_0/1$ $(< \xi)$, så är $p_0/1$ en bättre approximation till ξ än vad a/b är, vilket är en motsägelse. Och om $a/b > a_0 + 1$ $(= c_{0,1} \ge c_{0,a_1} = c_1 = p_1/q_1 > \xi)$, så är a_0+1 en bättre approximation, vilket också är en motsägelse. Det följer nu att om a/b inte är en konvergent eller en mellankonvergent, så finns det två mellankonvergenter (eller en konvergent och mellankonvergent) $c_{n,t}$ och $c_{n,t+1}$ så att a/b ligger strikt mellan dessa båda tal. Vidare ligger $c_{n,t}$ och $c_{n,t+1}$ på samma sida om ξ. Genom att använda föregående övning sluter vi oss nu till att nämnarna i $c_{n,t}$ och $c_{n,t+1}$ båda är strikt mindre än b. Detta är en motsägelse eftersom det ena av de båda talen ligger närmare ξ än vad a/b gör.
c) $10/7$ är en mellankonvergent, men $|\sqrt{2} - 7/5| < |\sqrt{2} - 10/7|$.

22.6 a) $140/99$ b) $168/97$ c) $311/99$ d) $193/71$ e) $31/14$

22.7 T.ex. $2/1$, $7/4$ och $26/15$

23.1 Utnyttja att $v_n v_{n+1} = d - u_{n+1}^2$ och $v_{n-1} v_n = d - u_n^2$. Subtraktion ger

$$v_n(v_{n+1} - v_{n-1}) = u_n^2 - u_{n+1}^2 = (u_n - u_{n+1})(u_n + u_{n+1}).$$

Genom att utnyttja att $u_n + u_{n+1} = a_n v_n$ får vi den sökta formeln efter division med v_n.

25.1 a) $(x, y) = (9, 4)$ b) $(x, y) = (8, 3)$

25.2 a) $(x, y) = (2049, 320)$ b) $(x, y) = (32, 5)$

25.3 $(x, y) = (2, 1)$, $(7, 4)$, $(26, 15)$, $(97, 56)$

25.4 Betrakta ekvationen $x^2 - k^2 dy^2 = 1$.

Sakregister