Grundkurs i talteori

av

Boris Sjöberg

Utgivet av Sigma vid Åbo Akademi

Åbo 1992

Grundkurs i talteori

av

Boris Sjöberg

Utgivet av Sigma vid Åbo Akademi

Åbo 1992

Innehållsförteckning

§ 1. Tals delbarhet och upplösning i faktorer

1.1 Välordnings- och induktionsprincipen

Talteorin har uppstått ur studiet av de hela talens egenskaper. Fortfarande utgör teorin för de hela talen en central del av talteorin. Vi kommer därför i föreliggande grundkurs huvudsakligen att uppehålla oss vid denna del av talteorin, väl medvetna om att talteorin i modern tid har expanderat i flera olika riktningar, vilka inte får rum i en elementär kurs som denna. Talteorin har under senare år fått många nya tillämpningar, t.ex. inom datatekniken och kryptografin. En sådan tillämpning kommer att behandlas i denna kurs (§ 7).

Vi uppfattar i denna kurs de hela talen $0, \pm 1, \pm 2, \ldots$ som en del av de reella talens mängd R, vars axiomsystem har behandlats i andra kurser (se t.ex. [1]). Därför introduceras inte de hela talen axiomatiskt i denna kurs. (Ett axiomsystem för de hela talen har getts bl.a. av den italienske matematikern Peano, 1858–1932). De hela talens mängd betecknas i denna kurs med Z. Delmängd av Z är de positiva (resp. negativa) talens mängd $Z_+ = \{1, 2, 3, \ldots\}$ (resp. $Z_- = \{-1, -2, -3, \ldots\}$).

Vi skall i detta avsnitt påminna om två viktiga egenskaper hos de hela talens mängd, vilka ofta kommer till användning i det följande. Den första egenskapen är

Välordningsprincipen. *Varje uppåt (nedåt) begränsad mängd av hela tal har ett största (minsta) tal.* (Se t.ex. [1], lemma 1.3).

Ett specialfall av välordningsprincipen är

Sats 1.1. *Varje mängd av positiva heltal har ett minsta tal.*

Det förutsättes givetvis såväl i välordningsprincipen som i sats 1.1 att de betraktade mängderna är icke-tomma. Den andra egenskapen, som ofta kommer till användning i bevis, är den välkända

Induktionsprincipen. *Låt H vara en mängd av positiva heltal, som innehåller talet 1. Då gäller: Om $n \in H$ medför att $n+1 \in H$, så omfattar H alla positiva heltal.*

Bevis: Antag som antites att H inte omfattar alla positiva heltal. Mängden $S = Z_+ \setminus H$ är då icke-tom. Enligt sats 1.1 har den ett minsta tal $n > 1$. Talet $n-1$ tillhör då H. Enligt satsens antagande gäller att $n = (n-1)+1 \in H$, vilket strider mot att $n \in S$. Detta visar att $H = Z_+$. □

Induktionsprincipen kallas stundom "fullständig induktion". Den användes vanligen i bevisföring på följande sätt: Man vill visa att ett visst påstående P (t.ex. en formel) gäller för alla positiva heltal n. Man visar då att P gäller för talet 1 och att $P(n) \Rightarrow P(n+1)$. (Med $P(n)$ avses att P gäller för talet n). Induktionsprincipen visar då att P gäller för alla positiva heltal. En variant av induktionsprincipen är

Sats 1.2. *Låt H vara en mängd av positiva heltal, som innehåller talet 1. Då gäller: Om $1, 2, 3, \ldots, k \in H$ medför att $k+1 \in H$, så omfattar H alla positiva heltal.*

Bevis: Låt T beteckna mängden av alla positiva heltal n, sådana att $1, 2, \ldots, n \in H$. Det är klart att $T \subseteq H$ och att $1 \in T$. Vidare gäller enligt satsens antagande att $k \in T \Rightarrow k+1 \in T$. Induktionsprincipen ger att $T = Z_+$ och således även $H = Z_+$. □

1.2 Tals delbarhet

I fortsättningen använder vi stundom, såvida missförstånd ej kan uppstå, benämningen "tal", då vi avser hela tal. Till de grundläggande begreppen i talteorin hör begreppet delbarhet. Vi ger följande

Definition: Låt a och b vara hela tal. Vi säger att a *delar* b (eller att b är *delbart* eller *divisibelt* med a), om det existerar ett sådant heltal c, att $b = ac$. Talet a säges då utgöra en *divisor (faktor)* i b. Vi säger också att b utgör en *multipel* av a. Att a delar b betecknas $a \mid b$. I motsatt fall skriver vi $a \nmid b$.

Exempelvis gäller att $6 \mid 18$, $-5 \mid 30$, $-4 \mid -8$ och $17 \mid 0$. Talen ± 1 utgör divisorer i alla hela tal. Varje heltal n ($\neq 0$) har talen $\pm n$ och ± 1 som divisorer. Talet 0 är delbart med varje heltal. Några enkla egenskaper rörande tals delbarhet finns sammanställda i följande sats.

Sats 1.3. *Låt a, b, c, d vara hela tal. Då gäller:*

(a) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(b) $a \mid b \Rightarrow a \mid bc$

(c) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd.$

Bevisen för dessa egenskaper följer omedelbart ur definitionen ovan och överlämnas åt läsaren. Av ovanstående definition följer även

Sats 1.4. *Om heltalen a_1, a_2, ..., a_n är delbara med heltalet b, så är även deras summa $a_1 + a_2 + \cdots + a_n$ delbar med b.*

Då denna sats kombineras med sats 1.3 (b), fås

Kor. 1.4. *Om heltalen a_1, a_2, ..., a_n alla är delbara med heltalet b, så är även summan $k_1a_1 + k_2a_2 + \cdots + k_na_n$ delbar med b ($k_i \in Z$).*

Däremot gäller:

Sats 1.5. *Om av talen a_1, a_2, ..., a_n alla utom ett är delbara med talet b, så är summan $a_1 + a_2 + \cdots + a_n$ inte delbar med b.*

Bevis: Antag att $b \nmid a_k$, medan $b \mid a_i$ för $i \neq k$. Enligt sats 1.4 är summan $\sum_{i\neq k} a_i$ delbar med b. Vore nu $\sum_{i=1}^{n} a_i$ delbar med b, så vore enligt kor. 1.4 även $a_k = \sum_{i=1}^{n} a_i - \sum_{i\neq k} a_i$ delbar med b i strid med antagandet. Detta bevisar påståendet. □

Innan vi går vidare i teorin för tals delbarhet, skall vi införa en beteckning, som visat sig vara mycket praktisk i dylika sammanhang. Låt x vara ett godtyckligt reellt tal. Med $[x]$ avses det största hela talet, som är $\leq x$. Vi kallar $[x]$ *heltalsdelen* av x. Exempelvis gäller att $[2,4] = 2$, $[-3,6] = -4$, $[6] = 6$ och $[-6] = -6$. Allmänt gäller:

$$x - 1 < [x] \leq x. \tag{1.1}$$

När ett positivt heltal a divideras med ett annat positivt heltal b, finns det som bekant två möjligheter: 1) Divisionen går inte jämnt upp, varvid vi får en heltalskvot q och en divisionsrest r, som uppfyller olikheten $0 < r < b$. 2) Divisionen går jämnt upp, i vilket fall resten $r = 0$. I bägge fallen gäller att $a = bq + r$. Denna formel går under namn av *divisionsalgoritmen.* Vi formulerar den i följande sats, där vi tillåter att a är ett godtyckligt heltal.

Sats 1.6. (Divisionsalgoritmen). *Om a och b är hela tal med $b > 0$, så existerar det entydigt bestämda hela tal q och r, sådana att $a = bq + r$ och $0 \leq r < b$.*

Bevis: Sätt $q = [a/b]$ och $r = a - b[a/b]$. Då är $a = bq + r$. Ur formel (1.1) följer att $(a/b) - 1 < [a/b] \leq a/b$. Multiplikation med b ger: $a - b < b[a/b] \leq a$. Härur fås genom omflyttning av termerna: $-a \leq -b[a/b] < b - a$. Då a adderas till alla tre leden, fås slutligen: $0 \leq a - b[a/b] < b$, dvs. $0 \leq r < b$. För att visa att q och r är entydigt bestämda, antar vi att vi skulle ha två framställningar $a = bq_1 + r_1$ och $a = bq_2 + r_2$ med $0 \leq r_1 < b$ och $0 \leq r_2 < b$. Genom subtraktion fås $0 = b(q_1 - q_2) + (r_1 - r_2)$, som ger $r_2 - r_1 = b(q_1 - q_2)$. Detta visar att b utgör en divisor i $r_2 - r_1$. Å andra sidan är $|r_2 - r_1| < b$, varav framgår att $r_2 - r_1 = 0$, dvs. $r_1 = r_2$. Ur ekvationen $r_2 - r_1 = b(q_1 - q_2)$ följer nu omedelbart att $q_1 = q_2$. Talen q och r är alltså entydigt bestämda. □

Som en tillämpning av sats 1.6 väljer vi $a = 1028$, $b = 34$. Då är $q = [1028/34] = 30$ och $r = 1028 - 34 \cdot 30 = 8$. Med $a = -380$, $b = 75$ får vi $q = [-380/75] = -6$ och $r = -380 - 75(-6) = 70$.

1.3 Primtal

Talet 1 har endast en positiv divisor, nämligen 1. Alla övriga positiva heltal n har åtminstone två positiva divisorer 1 och n. Sådana positiva heltal, som har exakt två positiva divisorer, spelar en stor roll i talteorin; de kallas primtal. Alltså gäller:

Definition: Ett heltal $n > 1$, som inte är delbart med några andra positiva heltal än 1 och n, kallas *primtal.* Alla övriga heltal $n > 1$ kallas *sammansatta.*

Talet 1 är sålunda varken primtal eller sammansatt. De första primtalen är 2, 3, 5, 7, 11, ... Varje sammansatt tal n kan skrivas i formen $n = ab$, där a och b är heltal med egenskapen $1 < a < n$ och $1 < b < n$. Primtalens betydelse ligger däri, att de s.a.s. utgör "byggstenar" i de sammansatta talen. Det visar sig nämligen att varje sammansatt tal kan skrivas som en produkt av primtal. I själva verket gäller:

Sats 1.7. *Varje heltal $n > 1$ kan skrivas som en produkt av primtal.*

Bevis: Antag som antites att det existerar något heltal $n > 1$, som inte utgör produkt av primtal. Låt H beteckna mängden av alla dylika heltal. H har då enligt sats 1.1 ett minsta element m. Talet m kan inte vara ett primtal, ty i så fall vore det ju en produkt av primtal (nämligen talet självt). Alltså är m sammansatt. Antag t.ex. att $m = ab$, där $1 < a < m$ och $1 < b < m$. Men då a och b är mindre än m, måste de enligt m:s definition vara en produkt av primtal. Då blir även $m = ab$ en produkt av primtal, vilket strider mot att $m \in H$. Således är antitesen falsk och satsen riktig. □

Observera att sats 1.7 inte garanterar att primtalsuppdelningen av talet n är entydig. Senare skall vi dock visa att primtalssönderdelningen faktiskt är entydig (sats 3.10).

Finns det oändligt många primtal? Frågan besvarades jakande redan av *Euklides* (ca 300 f.Kr.) i hans berömda verk *Elementa* (sats 20 i bok IX). Således gäller:

Sats 1.8. *Det existerar oändligt många primtal.*

Bevis: Tag ett godtyckligt primtal p och bilda talet $n = (2 \cdot 3 \cdot 5 \cdots p) + 1$, där talet inom parentesen utgör produkten av alla primtal t.o.m. talet p. Talet n är enligt sats 1.5 inte delbart med något av primtalen 2, 3, 5, ..., p. Men enligt sats 1.7 innehåller n någon primtalsfaktor q. Således är $q > p$. Till varje primtal p existerar alltså ett större primtal q, vilket visar att antalet primtal är oändligt. □

På grund av sats 1.8 kan vi i heltalsföljden 1, 2, 3, ... finna godtyckligt stora primtal. Å andra sidan kan man konstruera godtyckligt långa räckor av på varandra följande heltal, som

saknar primtal. Låt nämligen n vara ett godtyckligt positivt heltal. Vi betraktar då talföljden $t_2, t_3, \ldots, t_{n+1}$, där

$$t_\nu = (n+1)! + \nu \qquad (\nu = 2, 3, \ldots, n+1).$$

Talet t_ν är delbart med ν för $\nu = 2, 3, \ldots, n+1$ (sats 1.4). De n på varandra följande heltalen $t_2, t_3, \ldots, t_{n+1}$ är alltså alla sammansatta.

1.4 Eratosthenes såll

Hur skall man finna alla primtal i ett visst intervall $[m, n]$, om man inte har tillgång till en primtalstabell? För detta ändamål existerar en enkel (men arbetsdryg) metod kallad *Eratosthenes såll*. Metoden går helt enkelt ut på att man stryker alla sammansatta tal i intervallet. Detta tillgår så, att man först stryker alla tal delbara med 2 (utom talet 2 självt om det tillhör intervallet). Därefter stryker man i tur och ordning alla tal delbara med primtalen 3, 5, 7, 11, ... (utom dessa tal själva). Sedan man sålunda strukit de heltaliga multiplerna av alla primtal $\leq \sqrt{n}$, återstår primtalen i intervallet $[m, n]$. Varför behöver man endast stryka multipler av primtal $\leq \sqrt{n}$? Svaret framgår av följande

Lemma 1.9. *Om talet n är sammansatt, har det säkert någon primtalsfaktor, som är $\leq \sqrt{n}$.*

Bevis: Då $n = ab$ med $1 < a < n$, $1 < b < n$, måste antingen a eller b vara $\leq \sqrt{n}$. Vore nämligen $a > \sqrt{n}$ och $b > \sqrt{n}$, så vore $ab > n$, vilket är omöjligt. Antag t.ex. att $a \leq \sqrt{n}$. Talet a har enligt sats 1.7 någon primtalsfaktor $p \leq a$. Således har n någon primtalsfaktor $p \leq \sqrt{n}$. □

Metoden att bestämma alla primtal i intervallet $[m, n]$ med Eratosthenes såll är mycket arbetskrävande för stora värden på m och n. Med lämpliga modifikationer av metoden ifråga kan man dock nedbringa arbetet avsevärt. Sedan datorer har tagits i användning för dylika beräkningar, har man kunnat upprätta mycket omfattande primtalstabeller. Som exempel kan nämnas att *C.L. Baker* och *F.J. Gruenberger* år 1959 utgav en primtalstabell över alla primtal ≤ 104395289. Tabellen innehåller exakt sex miljoner primtal. På sid. 98 i slutet av detta kompendium finns en tabell över alla primtal ≤ 3331.

Övningsuppgifter

Uppgift 1.1 Bestäm talen q och r i divisionsalgoritmen, då a) $a = 406$, $b = 30$, b) $a = -631$, $b = 28$.

Uppgift 1.2 Låt a och b vara hela tal med $a > 0$, $b \neq 0$. Visa att $a \mid b \Rightarrow a \leq |b|$.

Uppgift 1.3 Visa att av n på varandra följande heltal $a+1, a+2, \ldots, a+n$ $(a \in Z)$ exakt ett är divisibelt med n.

Uppgift 1.4 Visa att talet $a^3 - a$ alltid är delbart med 3, då a är ett heltal.

Uppgift 1.5 Låt x och y vara godtyckliga reella tal, som i fallet (b) nedan är ≥ 0. Visa att

(a) $[x+y] \geq [x] + [y]$
(b) $[xy] \geq [x][y]$

Uppgift 1.6 Bestäm $[x] + [-x]$ för godtyckligt reellt x.

Uppgift 1.7 Ge ett annat bevis för divisionsalgoritmen genom att utnyttja välordningsprincipen. (Ledning: Betrakta mängden av alla tal av formen $a - bq$, där q genomlöper alla heltal. Visa att det i denna mängd finns tal ≥ 0 och låt r vara det minsta av dem).

Uppgift 1.8 Divisionsalgoritmens rest r kallas den *minsta positiva resten*, då heltalet a divideras med heltalet $b > 0$. Visa att man kan bilda en alternativ divisionsalgoritm $a = bq + r$ med en heltalskvot q och en rest r, som uppfyller olikheten $|r| \leq b/2$. Denna rest kallas den *minsta absoluta resten.*

Uppgift 1.9 Låt n vara ett sammansatt tal och låt p vara den minsta primtalsfaktorn i talet n. Visa att om $p > \sqrt[3]{n}$, så är n/p ett primtal.

Uppgift 1.10 Bestäm alla primtal i intervallet $[100, 200]$ med Eratosthenes såll.

§ 2. Primtalens fördelning

2.1 Primtalssatsen

När man studerar hur primtalen fördelar sig i heltalsföljden 1, 2, 3, ..., märker man snart att de uppträder tämligen oregelbundet. Räknar man t.ex. antalet primtal i de lika långa intervallen $[1,100]$, $[101,200]$, ..., $[901,1000]$, finner man följande värden: 25, 21, 16, 16, 17, 14, 16, 14, 15, 14. Någon lagbundenhet kan man knappast utläsa ur denna talserie. Talen tycks dock ha en tendens att minska ju längre fram i serien man går. Denna tendens blir mera markant, om vi anger antalet primtal i de lika långa intervallen $[1,1000]$, $[1001,2000]$, ..., $[9001,10000]$. Dessa antal är: 168, 135, 127, 120, 119, 114, 117, 107, 110, 112. Det är uppenbart att primtalstätheten minskar ju längre fram i heltalsföljden 1, 2, 3, ... vi går. Detta beror på att sannolikheten att ett på måfå valt heltal n skall vara sammansatt växer med n, eftersom antalet primtal $\leq \sqrt{n}$ då även tilltar.

Frågan om primtalens fördelning skulle vara definitivt löst, om man kunde finna någon enkel formel, som anger antalet primtal $\leq$ ett givet reellt tal x. Man brukar beteckna detta antal med $\pi(x)$. Tyvärr har man emellertid inte lyckats finna något *enkelt* analytiskt uttryck för $\pi(x)$. Den enklaste (men samtidigt mest räknekrävande) formeln härrör från *Legendre* (1752–1833). Denna formel är av rekursionstyp och förutsätter att man känner $\pi(\sqrt{x})$ samt alla primtal $\leq \sqrt{x}$, när man skall beräkna $\pi(x)$. Legendres formel innehåller endast de fyra enkla räknesätten. Andra formler för $\pi(x)$, som är betydligt mera komplicerade men bättre lämpade för numerisk räkning, existerar också. Då man sålunda inte har någon enkel formel för $\pi(x)$, har man försökt finna enkla analytiska uttryck, som approximerar $\pi(x)$. Genom att studera primtalstabeller fann Legendre och *Gauß* (1777–1855), att funktionerna

$$f(x) = \frac{x}{\log x} \quad \text{resp.} \quad \mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$$

är goda approximationer för $\pi(x)$ för stora värden på x. Funktionen li kallas *integrallogaritmen*. Det gäller visserligen inte att $\pi(x) - f(x)$ och $\pi(x) - \mathrm{li}(x)$ går mot noll när $x \to \infty$. Gauß förmodade däremot att kvoterna $\pi(x) : f(x)$ och $\pi(x) : \mathrm{li}(x)$ närmar sig talet 1 när $x \to \infty$, dvs. att $f(x)$ och $\mathrm{li}(x)$ är goda *relativa* approximationer av $\pi(x)$ för stora värden på x. Han lyckades dock inte bevisa sin hypotes. *Tchebycheff* visade omkring år 1850 att om ovannämnda kvoter har ett gränsvärde när $x \to \infty$, så är detta gränsvärde $= 1$. Han visade även att olikheten

$$\frac{7}{8}\,\frac{x}{\log x} < \pi(x) < \frac{9}{8}\,\frac{x}{\log x}$$

gäller för alla tillräckligt stora värden på x. Frågan löstes definitivt år 1896, då *Hadamard* och *de la Vallée-Poussin* oberoende av varandra bevisade den s.k.

Sats 2.1. (Primtalssatsen).

$$\lim_{x\to\infty} \pi(x) : \frac{x}{\log x} = 1.$$

Satsen gäller även om $\frac{x}{\log x}$ utbytes mot integrallogaritmen. Hadamard och de la Vallée-Poussin använde funktionsteoretiska hjälpmedel i sina bevis. År 1948 lyckades norrmannen *Atle Selberg* finna ett elementärt (men ingalunda enkelt) bevis för primtalssatsen.

För att visa hur $\frac{x}{\log x}$ och $\mathrm{li}(x)$ approximerar $\pi(x)$ anför vi här nedan en tabell över dessa funktioner jämte kvoterna $\pi(x) : \frac{x}{\log x}$ och $\pi(x) : \mathrm{li}(x)$. Av tabellen framgår att $\mathrm{li}(x)$ i regel är en bättre approximation av $\pi(x)$ än $\frac{x}{\log x}$. Av tabellen kunde man förledas att tro att $\frac{x}{\log x} < \pi(x)$ och $\mathrm{li}(x) > \pi(x)$ för alla värden på x. Så är dock inte fallet. Den förra olikheten gäller för $x \geq 11$, medan *Littlewood* har visat att differensen $\mathrm{li}(x) - \pi(x)$ är både positiv och negativ för oändligt många värden på x. Teckenbytena tycks dock inträffa för mycket stora värden på x. Exempelvis har *H.J.J. te Riele* visat år 1986 att ett teckenbyte säkert inträffar för något $x < 6{,}69 \cdot 10^{370}$.

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$li(x)$	$\pi(x)/li(x)$
10^3	168	144.8	1.160	178	0.9438202
10^4	1229	1085.7	1.132	1246	0.9863563
10^5	9592	8685.9	1.104	9630	0.9960540
10^6	78498	72382.4	1.085	78628	0.9983466
10^7	664579	620420.7	1.071	664918	0.9998944
10^8	5761455	5428681.0	1.061	5762209	0.9998691
10^9	50847534	48254942.4	1.054	50849235	0.9999665
10^{10}	455052512	434294481.9	1.048	455055614	0.9999932
10^{11}	4118054131	3948131663.7	1.043	4118165401	0.9999731
10^{12}	37607912018	36191206825.3	1.039	37607950281	0.9999990
10^{13}	346065535898	33407267837.1	1.036	346065645810	0.9999997

Tabell 1. Approximationer av $\pi(x)$.

2.2 Riemanns ζ-funktion

Primtalens fördelning har ett nära samband med en analytisk funktion, kallad *Riemanns ζ-funktion.* Den definieras för reellt $s > 1$ genom den oändliga serien

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2.1}$$

Genom analytisk fortsättning kan definitionen utsträckas till alla komplexa $s = \sigma + i\tau$ utom $s = 1$, där funktionen har en enkel pol. Det visar sig att ζ-funktionen har nollställen i punkterna $s = -2, -4, -6, \ldots$ Dessa kallas triviala nollställen. Alla övriga nollställen ligger i parallellstrimlan $0 \leq \sigma \leq 1$. Dessa är oändligt många och kallas icke-triviala. *Riemanns hypotes*, som ännu (1991) är obevisad, utsäger att alla icke-triviala nollställen ligger på räta linjen $\sigma = \frac{1}{2}$. Om man ordnar de icke-triviala nollställena efter storleken på deras imaginära del, så har man med superdatorer kunnat visa, att de 41 miljarder första nollställena alla ligger på linjen $\sigma = \frac{1}{2}$. Det förefaller alltså mycket troligt att Riemanns hypotes är sann.

Sambandet mellan Riemanns ζ-funktion och primtalen framgår av *Eulers identitet*

$$\zeta(s) = \prod_{(p)} \frac{1}{1 - p^{-s}}, \tag{2.2}$$

där den oändliga produkten utsträckes över alla primtal p. Detta samband utnyttjades av Hadamard och de la Vallée-Poussin i beviset av primtalssatsen. Många öppna frågor i teorin för primtalens fördelning skulle kunna avgöras, om man kunde bevisa Riemanns hypotes. Ett dylikt resultat är t.ex. följande: Om Riemanns hypotes är sann, så är $|\pi(x) - \mathrm{li}(x)| < c\sqrt{x}\log x$, där c är en lämpligt vald konstant.

2.3 Andra frågor rörande primtal

Heltalsräckan 1, 2, 3, ... innehåller som bekant oändligt många primtal (sats 1.8). Eftersom alla primtal utom talet 2 är udda, innehåller även följden 1, 3, 5, ... oändligt många primtal. Däremot innehåller följden 2, 4, 6, ... endast primtalet 2. Ovanstående talräckor är exempel på s.k. *aritmetiska följder (räckor)*, vilka som bekant karakteriseras av att differensen mellan två på varandra följande tal i räckan är konstant. Betrakta nu en godtycklig aritmetisk heltalsföljd $(an+b)$, där $n = 0, 1, 2, \ldots$ $(a, b \in Z)$. Vi kan härvid anta att $a \geq 1, 0 \leq b < a$. Om a och b har en gemensam divisor $d > 1$, utgör d en divisor i samtliga tal i följden (sats 1.4). Talföljden kan då på sin höjd innehålla endast ett primtal. Ett nödvändigt villkor för att följden skall innehålla oändligt många primtal är alltså att a och b saknar gemensamma divisorer $d > 1$. Är detta villkor även tillräckligt? Legendre trodde sig ha funnit ett bevis för att så är fallet, men det visade sig vara felaktigt. Ett korrekt bevis gavs första gången av *Dirichlet* (1837). Således gäller:

Sats 2.2. *Låt a och b vara heltal utan gemensam divisor $d > 1$, sådana att $a \geq 1$, $0 \leq b < a$. Då finns det oändligt många primtal p av formen $p = an + b$ $(n = 0, 1, 2, \ldots)$.*

Beviset för denna sats är rätt komplicerat och kan inte återges här, För vissa aritmetiska räckor kan man dock påvisa satsen med elementära metoder (se t.ex. övningsuppgift 2.4). Av sats 2.2 följer t.ex. att det finns oändligt många primtal som slutar på 33333. Alla tal som slutar på 33333 är nämligen av formen $100000n + 33333$ $(n = 0, 1, 2, \ldots)$, och talen $a = 100000$, $b = 33333$ saknar gemensamma divisorer $d > 1$. Som exempel på dylika primtal kan nämnas 733333, 1133333 och 2633333.

En annan fråga rörande primtalens fördelning gäller de s.k. primtalstvillingarna. Med en *primtalstvilling* avses ett par $(p, p+2)$ av primtal, vars differens $= 2$. Sådana par är t.ex. (3,5), (5,7), (11,13) o.s.v. Man kan tämligen lätt visa att alla primtalstvillingar utom (3,5) är av formen $(6n - 1, 6n + 1)$ $(n = 1, 2, 3, \ldots)$. (Se övningsuppgift 2.3). Det är ännu inte klarlagt, huruvida antalet primtalstvillingar är ändligt eller oändligt. Mycket tyder på att det är oändligt. Man har visserligen lyckats visa, att summan av primtalstvillingarnas inversa värden

$$(\frac{1}{3} + \frac{1}{5}) + (\frac{1}{5} + \frac{1}{7}) + (\frac{1}{11} + \frac{1}{13}) + \cdots$$

är ändlig, men detta säger ingenting om antalet primtalstvillingar. I detta sammanhang kan nämnas att serien $\sum_{(p)} \frac{1}{p}$, som bildas av primtalens inversa värden, är divergent. Detta ger ett nytt bevis för att antalet primtal är oändligt.

En tysk matematiker, *Christian Goldbach*, uppställde år 1742 följande postulat:

1. *Varje jämnt tal ≥ 6 kan framställas som en summa av två udda primtal.*
2. *Varje udda tal ≥ 9 kan framställas som en summa av tre udda primtal.*

Man ser lätt att det andra påståendet följer ur det första. Låt nämligen n vara ett udda tal ≥ 9. Då är $n-3$ ett jämnt tal ≥ 6, som enligt påstående 1 kan skrivas i formen $n - 3 = p + q$, där p och q är udda primtal. Alltså är $n = 3 + p + q$ en summa av tre udda primtal. Problemet är att ingen ännu har lyckats bevisa Goldbachs första postulat. Det har därför fått namnet *Goldbachs förmodan.* Den finländske matematikern *Nils Pipping* (professor vid Åbo Akademi 1930–1953) verifierade genom direkt uträkning att Goldbachs förmodan är riktig för alla jämna tal ≤ 100000. Senare har man med datorers hjälp utsträckt verifikationen upp till 100 miljoner. Den ryske matematikern *I.M. Vinogradov* visade år 1937 att Goldbachs andra postulat gäller för alla tillräckligt stora udda tal (oberoende av om Goldbachs förmodan är riktig eller ej).

Ett problem, som länge intresserat matematikerna, är frågan om det existerar någon "enkel" funktion, som producerar enbart primtal för heltaliga argumentvärden. Närmast till hands ligger då polynom med heltaliga koefficienter. Som exempel kan nämnas polynomet $x^2 - x + 41$, som framställer primtal för $x = 0, \pm 1, \pm 2, \ldots, \pm 39$ och 40. Nu frågas: Finns det något polynom, som framställer enbart primtal för *alla* heltaliga argumentvärden? Ifråga om polynom i en variabel

är svaret nekande. Man kan nämligen lätt visa, att ett polynom $P(x)$ med heltaliga koefficienter inte kan framställa enbart primtal för alla heltalsvärden på x större än någon någon lämpligt vald konstant (se t.ex. sats 31 i [2]). Vad flervariabelspolynom beträffar var problemet länge olöst. Frågan fick sin lösning år 1970 som en följd av att den ryske matematikern *Yuri Matijasevic* löste Hilberts tionde problem (vilket egentligen handlade om diofantiska ekvationer). Som en biprodukt av denna lösning följer nämligen att det existerar polynom i flera variabler med heltaliga koefficienter, vilkas positiva funktionsvärden utgör exakt mängden av alla primtal. Det dröjde dock ända till år 1977, innan man lyckades explicit konstruera ett dylikt polynom. Detta polynom har 26 variabler och är av 25:te graden.

Övningsuppgifter

Uppgift 2.1 Visa att primtalstätheten $\frac{\pi(x)}{x}$ i intervallet $[0,x]$ går mot noll när $x \to \infty$.

Uppgift 2.2 Enligt *Rosser* [3] gäller följande uppskattning av $\pi(x)$ för $x \geq 59$:

$$\frac{x}{\log x}\left(1+\frac{1}{2\log x}\right) < \pi(x) < \frac{x}{\log x}\left(1+\frac{3}{2\log x}\right).$$

Härled på basen härav en undre och en övre gräns för det relativa felet

$$\frac{\pi(x)-\frac{x}{\log x}}{\pi(x)},$$

när $\pi(x)$ uppskattas med $\frac{x}{\log x}$, samt visa att detta fel går mot noll när $x \to \infty$.

Uppgift 2.3 Visa att alla primtal utom talen 2 och 3 är av formen $6n \pm 1$ $(n = 1,2,3,\ldots)$. Härav följer bl.a. att alla primtalstvillingar utom (3,5) är av formen $(6n-1, 6n+1)$ $(n = 1,2,3,\ldots)$.

Uppgift 2.4 Visa att det finns oändligt många primtal av formen $6n-1$ $(n = 1,2,3,\ldots)$. (Ledning: Låt p vara ett godtyckligt primtal av formen $p = 6n-1$ samt bilda talet $N = (2\cdot 3\cdot 5\cdot 7\cdots p)-1$, där talet inom parentes utgör produkten av alla primtal till och med talet p. Visa med samma metod som i beviset av sats 1.8 att det finns ett primtal $q > p$ av formen $q = 6m-1$).

Uppgift 2.5 Visa att om talet $2^n - 1$ är ett primtal, så är även n ett primtal.

Uppgift 2.6 En taltrippel av formen $(p, p+2, p+4)$ kallas en primtalstrilling, om alla tre talen i trippeln är primtal. Visa att det inte finns några andra primtalstrillingar än (3,5,7).

§ 3. Största gemensamma divisorn. Talteorins fundamentalsats

3.1 Största gemensamma divisorn

Låt $a_1, a_2, \ldots, a_n$ vara hela tal, icke alla $= 0$. Talen ± 1 utgör uppenbarligen gemensamma divisorer till alla dessa tal. I den mån andra gemensamma divisorer existerar, kan ingen av dem överstiga $\min\{|a_i| : a_i \neq 0\}$. Det finns alltså enligt välordningsprincipen en *största gemensam divisor* (st.g.d.) $d \geq 1$. Vi inför beteckningen

$$d = (a_1, a_2, \ldots, a_n). \tag{3.1}$$

Om $d = 1$, säger vi att talen $a_1, a_2, \ldots, a_n$ är *relativt prima (primiska)*. Om $(a_i, a_j) = 1$ för alla olika i och j, säger vi att talen $a_1, a_2, \ldots, a_n$ är *parvis relativt prima (primiska)*. Sålunda är t.ex. talen 8, 9, 10, 12 relativt prima, medan talen 5, 8, 9, 11 är parvis relativt prima. Tal som är parvis relativt prima, är självfallet även relativt prima.

Utöver definitionen finns det andra sätt att karakterisera den största gemensamma divisorn. Vi skall i det följande ge ett par sådana karakteriseringar. Låt $a_1, a_2, \ldots, a_n$ fortfarande beteckna hela tal, icke alla $= 0$. Ett uttryck av formen

$$m_1 a_1 + m_2 a_2 + \cdots + m_n a_n,$$

där $m_1, m_2, \ldots, m_n$ är hela tal, kallas en *linjärkombination* av talen $a_1, a_2, \ldots, a_n$. Må L beteckna mängden av alla linjärkombinationer av dessa tal. Mängden L innehåller säkert något positivt heltal. (Ty om t.ex. $a_k \neq 0$, så betraktar vi de två linjärkombinationer, där alla $m_i = 0$ utom m_k, som vi sätter $= \pm 1$. Vi får då linjärkombinationerna $\pm a_k$, av vilka den ena > 0). Mängden av positiva linjärkombinationer har enligt sats 1.1 ett minsta tal d. Således

$$d = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n \tag{3.2}$$

för lämpligt valda heltal $m_1, m_2, \ldots, m_n$. Vi påstår nu att $d = (a_1, a_2, \ldots, a_n)$. Enligt divisionsalgoritmen kan vi skriva

$$a_1 = dq_1 + r_1,$$

där $0 \leq r_1 < d$. Detta ger med beaktande av (3.2)

$$r_1 = a_1 - dq_1 = a_1(1 - q_1 m_1) - q_1(m_2 a_2 + \cdots + m_n a_n).$$

Härav framgår att r_1 utgör en linjärkombination av $a_1, a_2, \ldots, a_n$, dvs. $r_1 \in L$. Då $0 \leq r_1 < d$ och d är det minsta positiva talet i L, ser vi att $r_1 = 0$. Detta visar att d är en divisor i a_1. På samma sätt inses att d är en divisor i $a_2, a_3, \ldots, a_n$. Talet d är m.a.o. en gemensam divisor till talen $a_1, a_2, \ldots, a_n$. Låt nu d_0 vara en godtycklig gemensam divisor till dessa tal. Av (3.2) framgår då att d_0 även är divisor i talet d (kor. 1.4). Härav sluter vi att d är den största gemensamma divisorn till talen $a_1, a_2, \ldots, a_n$. Därmed har vi bevisat

Sats 3.1. *Den största gemensamma divisorn till de hela talen $a_1, a_2, \ldots, a_n$ (icke alla $= 0$) är det minsta positiva heltalet d, som kan skrivas i formen*

$$d = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n,$$

där $m_1, m_2, \ldots, m_n$ är hela tal.

Kor. 3.1. *Om $d = (a_1, a_2, \ldots, a_n)$, så existerar det hela tal $m_1, m_2, \ldots, m_n$, sådana att d kan skrivas i formen*

$$d = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n. \tag{3.3}$$

I det speciella fall att $d = 1$ får vi

Sats 3.2. *Om talen $a_1, a_2, \ldots, a_n$ är relativt prima, så finns det hela tal $m_1, m_2, \ldots, m_n$, sådana att*

$$1 = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n. \tag{3.4}$$

Ett annat sätt att karakterisera st.g.d. ges av följande sats.

Sats 3.3. *Det positiva heltalet d är största gemensamma divisorn till talen $a_1, a_2, \ldots, a_n$, om och endast om följande villkor är uppfyllda:*

(a) *d är en gemensam divisor till talen $a_1, a_2, \ldots, a_n$.*
(b) *d är delbar med alla gemensamma divisorer till talen $a_1, a_2, \ldots, a_n$.*

Bevis: Antag först att $d = (a_1, a_2, \ldots, a_n)$. Det är då klart att (a) gäller. Om d_0 är en godtycklig gemensam divisor till talen $a_1, a_2, \ldots, a_n$, så är d_0 även divisor i d på grund av framställningen (3.3). Alltså gäller (b). Omvänt, om (a) och (b) gäller, så är d uppenbarligen den största gemensamma divisorn till talen $a_1, a_2, \ldots, a_n$. □

Några enkla egenskaper hos största gemensamma divisorn finns sammanställda i följande sats.

Sats 3.4. *Låt $a, b, c, k, a_1, a_2, \ldots, a_n$ vara hela tal med $c > 0$. Då gäller:*

$$(a, b) = (a + kb, b) \tag{3.5}$$

$$(ca_1, ca_2, \ldots, ca_n) = c(a_1, a_2, \ldots, a_n) \tag{3.6}$$

$$d = (a, b) \Rightarrow (a/d, b/d) = 1. \tag{3.7}$$

Bevis: Varje gemensam divisor till a och b är även en gemensam divisor till $a + kb$ och b. Omvänt är varje gemensam divisor till $a + kb$ och b en gemensam divisor till a och b, emedan $a = (a + kb) - kb$. Alltså har talen a och b samma gemensamma divisorer som talen $a + kb$ och b. Härav följer (3.5). För att bevisa (3.6) sätter vi $d = (a_1, a_2, \ldots, a_n)$, $D = (ca_1, ca_2, \ldots, ca_n)$. Vi skall visa att $D = cd$. Eftersom d är en gemensam divisor för talen a_i, så är cd en gemensam divisor för talen ca_i $(i = 1, 2, \ldots, n)$. Detta ger $cd \mid D$ (sats 3.3 (b)). Vidare gäller enligt kor. 3.1:

$$d = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n,$$

där m_1, m_2, ..., m_n är hela tal. Multiplikation med c ger:

$$cd = m_1(ca_1) + m_2(ca_2) + \cdots + m_n(ca_n).$$

Men då D är en gemensam divisor till talen ca_i, kan vi skriva $ca_i = k_i D$, där $k_i \in Z$. Detta ger:

$$cd = D(m_1 k_1 + m_2 k_2 + \cdots + m_n k_n),$$

varav följer att $D \mid cd$. Ur $cd \mid D$ och $D \mid cd$ fås nu $D = cd$. Därmed är (3.6) bevisat. För bevis av (3.7) sättes $m = a/d$, $n = b/d$. Vore nu $(m, n) \neq 1$, så skulle m och n ha en gemensam divisor $d' > 1$. Då vore $m = m'd'$, $n = n'd'$, där m' och n' är hela tal. Således vore $a = m'd'd$ och $b = n'd'd$. Talen a och b skulle alltså ha en gemensam divisor $d'd > d$, vilket strider mot definitionen på d. Således är $(m, n) = 1$. Därmed är sats 3.4 fullständigt bevisad. □

Vi kommer i nästa avsnitt ge en enkel algoritm för bestämning av st.g.d. till två tal a och b. För att bestämma st.g.d. till tre tal a, b och c kan man betjäna sig av formeln

$$(a, b, c) = ((a, b), c). \tag{3.8}$$

Riktigheten av denna formel inses på följande sätt: Sätt $d = (a, b, c)$, $d_0 = (a, b)$. Eftersom d är en divisor i a och b, är d även en divisor i d_0 (sats 3.3). Således är d en gemensam divisor för d_0 och c. Låt nu d_1 vara en godtycklig gemensam divisor för d_0 och c. Då är d_1 en gemensam divisor till a, b och c, varav följer att $d_1 \mid d$ (sats 3.3). Således är d en sådan gemensam divisor till talen d_0 och c, som är delbar med varje annan gemensam divisor till dessa tal. Sats 3.3 ger då att $d = (d_0, c)$. Därmed är formel (3.8) bevisad. Som exempel på användning av denna formel finner vi att (18,30,45) = ((18,30),45) = (6,45) = 3.

Formel (3.8) kan givetvis generaliseras till att bestämma största gemensamma divisorn d till ett godtyckligt antal heltal a_1, a_2, ..., a_n. Detta tillgår så, att man först bestämmer $d_2 = (a_1, a_2)$, därefter $d_3 = (d_2, a_3)$, sedan $d_4 = (d_3, a_4)$ o.s.v. Slutligen fås $d = d_n = (d_{n-1}, a_n)$.

3.2 Euklides algoritm

I Euklides Elementa, bok VII, ges en enkel metod för bestämning av st.g.d. till två givna heltal a och b. Metoden kallas *Euklides algoritm.* Innan vi redogör för denna metod, inskjuter vi följande

Lemma 3.5. *Låt a och b vara heltal med $b > 0$. Om $a = bq + r$ $(0 \leq r < b)$, så är $(a, b) = (b, r)$.*

Bevis: Om d delar a och b, så delar d även b och r, emedan $r = a - bq$. Omvänt om e delar b och r, så delar e även a och b på grund av att $a = bq + r$. Paren a, b och b, r har alltså samma gemensamma divisorer. Följaktligen har de även samma största gemensamma divisor. □

Vi går nu till att bestämma st.g.d. till två givna heltal a och b med hjälp av Euklides algoritm. Vi kan härvid anta att a och b bägge är positiva, emedan $(a, b) = (|a|, |b|)$. Vi sätter $r_0 = a$, $r_1 = b$ och använder divisionsalgoritmen på talen r_0 och r_1. Vi får då

$$r_0 = r_1 q_1 + r_2 \qquad (0 \leq r_2 < r_1).$$

Om $r_2 \neq 0$ tillämpar vi divisionsalgoritmen på r_1 och r_2 och får

$$r_1 = r_2 q_2 + r_3 \qquad (0 \leq r_3 < r_2).$$

Då vi fortsätter på detta sätt, så länge resterna $\neq 0$, får vi följande identiteter:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && (0 < r_2 < r_1) \\
r_1 &= r_2 q_2 + r_3 && (0 < r_3 < r_2) \\
r_2 &= r_3 q_3 + r_4 && (0 < r_4 < r_3) \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && (0 < r_n < r_{n-1}) \\
r_{n-1} &= r_n q_n.
\end{aligned} \tag{3.9}$$

Vi kan anta att $r_{n+1} = 0$, ty resterna bildar en avtagande följd av heltal $r_1 > r_2 > r_3 > \cdots \geq 0$. Efter ett ändligt antal steg måste därför värdet 0 uppnås. Av lemma 3.5 följer nu att

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Största gemensamma divisorn till talen a och b är alltså den sista från noll skilda resten r_n. Därmed har vi bevisat

Sats 3.6. *Om vi tillämpar Euklides algoritm på två positiva heltal, tills vi får en rest $= 0$, så är talens största gemensamma divisor $=$ den sista från noll skilda resten.*

Som en tillämpning skall vi bestämma (252,198). Då vi tillämpar Euklides algoritm på talen $a = 252$ och $b = 198$, får vi följande identiteter:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

Således är $(252, 198) = 18$.

Euklides algoritm har mångsidig användning i talteorin. Som exempel på detta skall vi visa hur man med Euklides algoritm bestämmer talen m_i i framställningen (3.3) för st.g.d., i det fall att antalet givna heltal a_i är två. Låt alltså a och b vara två givna heltal. Liksom i det föregående kan vi anta att a och b vardera är positiva, eftersom ett teckenbyte hos någotdera talet ej ändrar deras st.g.d. Genom att tillämpa Euklides algoritm på talen a och b får vi en följd av kvoter $q_1, q_2, \ldots, q_n$, såsom schemat (3.9) utvisar. Med hjälp av dessa kvoter kan vi nu bilda två ändliga talföljder $s_0, s_1, \ldots, s_n$ resp. $t_0, t_1, \ldots, t_n$ genom rekursionsformlerna

$$\begin{aligned} s_i &= s_{i-2} - q_{i-1}s_{i-1} \qquad (i = 2, 3, \ldots, n) \\ t_i &= t_{i-2} - q_{i-1}t_{i-1} \qquad (i = 2, 3, \ldots, n), \end{aligned} \tag{3.10}$$

där $s_0 = t_1 = 1$ och $s_1 = t_0 = 0$. Vi påstår nu att resterna r_i i schemat (3.9) erhålles ur ekvationerna

$$r_i = s_i a + t_i b \qquad (i = 0, 1, 2, \ldots, n). \tag{3.11}$$

Beviset sker med hjälp av (den utvidgade) induktionsprincipen (sats 1.2). Formel (3.11) gäller för $i = 0, 1$, ty $s_0 a + t_0 b = 1 \cdot a + 0 \cdot b = a = r_0$ och $s_1 a + t_1 b = 0 \cdot a + 1 \cdot b = b = r_1$. Antag nu att formeln gäller för $i = 2, 3, \ldots, k-1$. Ur schemat (3.9) erhålles

$$r_k = r_{k-2} - r_{k-1}q_{k-1}.$$

Insättes här värdena på r_{k-2} och r_{k-1} enligt induktionsantagandet (3.11) fås med beaktande av (3.10):

$$\begin{aligned} r_k &= (s_{k-2}a + t_{k-2}b) - q_{k-1}(s_{k-1}a + t_{k-1}b) \\ &= a(s_{k-2} - q_{k-1}s_{k-1}) + b(t_{k-2} - q_{k-1}t_{k-1}) \\ &= s_k a + t_k b, \end{aligned}$$

dvs. (3.11) gäller även för $i = k$. Sats 1.2 ger då att (3.11) gäller för alla ifrågakommande värden på i, dvs. för $i = 0, 1, 2, \ldots, n$. Med stöd av sats (3.6) får vi nu $(a, b) = r_n = s_n a + t_n b$. Således gäller:

Sats 3.7. *Om a och b är positiva heltal, så är*

$$(a, b) = s_n a + t_n b, \tag{3.12}$$

där s_n och t_n är "slutelementen" i de två talföljder (s_i) och (t_i), som bildas enligt (3.10) *med hjälp av kvoterna q_i i Euklides algoritm.*

Fördelen med sats 3.7 är att den ger oss möjlighet att explicit beräkna koefficienterna s_n och t_n i linjärkombinationen (3.12), medan kor. 3.1 endast garanterar linjärkombinationens existens. Som en tillämpning av sats 3.7 skall vi bestämma en linjärkombination för st.g.d. till talen $a = 252$ och $b = 198$. Vi visade redan att (252,198) = 18. Euklides algoritm gav oss härvid följande kvoter: $q_1 = 1$, $q_2 = 3$, $q_3 = 1$ och $q_4 = 2$. (Här är således $n = 4$). Genom att successivt insätta dessa kvoter i (3.10) får vi följande talföljder (s_i) och (t_i):

$$s_0 = 1, \quad s_1 = 0, \quad s_2 = 1, \quad s_3 = -3, \quad s_4 = 4,$$
$$t_0 = 0, \quad t_1 = 1, \quad t_2 = -1, \quad t_3 = 4, \quad t_4 = -5.$$

Således har vi enligt sats 3.7 följande framställning för st.g.d. 18:

$$18 = 4 \cdot 252 - 5 \cdot 198,$$

vars riktighet naturligtvis kan kontrolleras genom direkt uträkning.

3.3 Talteorins fundamentalsats

I avsnitt 1.3 visades att varje heltal $n > 1$ kan skrivas som en produkt av primtal (sats 1.7). Denna sats garanterar emellertid inte att primtalsuppdelningen är entydigt bestämd av talet n. Vi skall nu visa att så faktiskt är fallet. Eftersom den entydiga primtalsuppdelningen är av fundamental betydelse för talteorin, har detta resultat kallats *talteorins (aritmetikens) fundamentalsats.* Först måste vi emellertid bevisa ett par förberedande satser.

Sats 3.8. *Låt a, b och c vara hela tal. Om a och b är relativt prima och om a delar produkten bc, så delar a talet c.*

Bevis: Enligt sats 3.2 existerar det hela tal m och n, sådana att $ma + nb = 1$. Multiplikation med c ger: $mac + nbc = c$. Enligt antagandet gäller att $a \mid bc$. Således delar a såväl termen mac som termen nbc, vilket medför att $a \mid (mac + nbc)$, dvs. $a \mid c$. □

Kor. 3.8. *Låt a och b vara heltal och p ett primtal. Om p delar produkten ab, så delar p åtminstone den ena av faktorerna a och b.*

Bevis: Antag att $p \nmid a$. Då är $(p, a) = 1$, och sats 3.8 ger: $p \mid b$. Analogt fås: $p \nmid b \Rightarrow p \mid a$. □

Kor. 3.8 kan generaliseras till en produkt av ett godtyckligt (ändligt) antal faktorer. Man får då följande

Sats 3.9. *Om primtalet p delar produkten $a_1 a_2 \cdots a_n$ av heltalen a_i $(i = 1, 2, \ldots, n)$, så delar p åtminstone en av faktorerna a_i.*

Bevis: Vi använder induktionsprincipen. Satsen är trivial i fallet $n = 1$. Antag nu att satsen gäller för en produkt av n faktorer. Vi betraktar produkten $a_1 a_2 \cdots a_{n+1}$ och antar att $p \mid (a_1 a_2 \cdots a_{n+1})$. Vi skriver $a_1 a_2 \cdots a_{n+1} = (a_1 a_2 \cdots a_n) a_{n+1}$. Enligt kor. 3.8 delar p antingen faktorn $(a_1 a_2 \cdots a_n)$ eller faktorn a_{n+1}. I det förra fallet delar p någon av faktorerna $a_1, a_2, \ldots, a_n$ på grund av induktionsantagandet. I det senare fallet gäller att $p \mid a_{n+1}$. Alltså delar p någon av faktorerna $a_1, a_2, \ldots, a_{n+1}$, dvs. satsen gäller även för en produkt av $n+1$ faktorer. Induktionsprincipen ger nu resultatet. □

Kor. 3.9. *Om heltalet a är relativt primiskt till vart och ett av heltalen $b_1, b_2, \ldots, b_n$, så är det även relativt primiskt till produkten $b_1 b_2 \cdots b_n$.*

Bevis: Vore a och $b_1 b_2 \cdots b_n$ inte relativt primiska, så skulle de ha någon primfaktor p gemensam. Enligt sats 3.9 skulle p då dela något av talen b_i, t.ex. b_{i_0}. Då skulle a och b_{i_0} ha faktorn p gemensam i strid med antagandet. Alltså är a och produkten $b_1 b_2 \cdots b_n$ relativt primiska. □

Vi är nu i stånd att bevisa den redan aviserade fundamentalsatsen.

Sats 3.10. (Talteorins fundamentalsats). *Varje heltal $n > 1$ kan skrivas som en produkt av primtal. Primtalsuppdelningen är entydig bortsett från faktorernas ordningsföljd.*

Bevis: Satsens första del bevisades i sats 1.7. Antag nu att talet $n > 1$ skulle ha två primfaktoriseringar:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s. \tag{a}$$

Vi kan härvid anta att $r \leq s$. Av (a) framgår att $p_1 \mid (q_1 q_2 \cdots q_s)$. Sats 3.9 ger då att p_1 delar något av talen $q_1, q_2, \ldots, q_s$. Vi kan t.ex. anta att $p_1 \mid q_1$. (Detta kan alltid åstadkommas genom omnumrering av q-faktorerna). Men då p_1 och q_1 bägge är primtal, måste vi ha $p_1 = q_1$. Vi kan alltså i likheten (a) förkorta bort faktorerna p_1 och q_1. Då återstår likheten

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Som ovan kan vi nu visa att $p_2 =$ någon av faktorerna $q_2, q_3, \ldots, q_s$, t.ex. $p_2 = q_2$. Då vi fortsätter på detta sätt, kan vi successivt förkorta bort faktorerna $p_2, p_3, \ldots, p_r$ samt $q_2, q_3, \ldots, q_r$, eftersom $r \leq s$. Vore nu $r < s$, skulle vi slutligen få den omöjliga likheten

$$1 = q_{r+1} q_{r+2} \cdots q_s.$$

Alltså är $r = s$, och vi har $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$. Primtalsuppdelningen är alltså entydig. □

När man uppskriver primfaktoriseringen av ett tal $n > 1$, ordnar man vanligen faktorerna i växande ordningsföljd $p_1 < p_2 < \cdots < p_k$. Om vi har a_1 faktorer p_1, a_2 faktorer p_2 o.s.v., får vi framställningen

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \tag{3.13}$$

Exempelvis gäller för talet 360 primfaktoriseringen $360 = 2^3 3^2 5$. Med hjälp av primtalsuppdelningen kan man lätt bestämma alla positiva divisorer i ett givet heltal $n > 1$. Antag att n har primtalsuppdelningen (3.13). De positiva divisorerna i talet n är då alla av formen

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

där heltalen $\alpha_1, \alpha_2, \ldots, \alpha_k$ uppfyller olikheterna $0 \leq \alpha_1 \leq a_1$, $0 \leq \alpha_2 \leq a_2, \ldots, 0 \leq \alpha_k \leq a_k$. Man ser lätt att *antalet positiva divisorer i talet n* är

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1). \tag{3.14}$$

Som exempel betraktar vi återigen talet 360, som uppenbarligen har $4 \cdot 3 \cdot 2 = 24$ positiva divisorer. Dessa är

$2^0 3^0 5^0 = 1$	$2^2 3^1 5^0 = 12$	$2^0 3^0 5^1 = 5$	$2^2 3^1 5^1 = 60$
$2^1 3^0 5^0 = 2$	$2^3 3^1 5^0 = 24$	$2^1 3^0 5^1 = 10$	$2^3 3^1 5^1 = 120$
$2^2 3^0 5^0 = 4$	$2^0 3^2 5^0 = 9$	$2^2 3^0 5^1 = 20$	$2^0 3^2 5^1 = 45$
$2^3 3^0 5^0 = 8$	$2^1 3^2 5^0 = 18$	$2^3 3^0 5^1 = 40$	$2^1 3^2 5^1 = 90$
$2^0 3^1 5^0 = 3$	$2^2 3^2 5^0 = 36$	$2^0 3^1 5^1 = 15$	$2^2 3^2 5^1 = 180$
$2^1 3^1 5^0 = 6$	$2^3 3^2 5^0 = 72$	$2^1 3^1 5^1 = 30$	$2^3 3^2 5^1 = 360$

Medels uppdelningen i primfaktorer kan man även bestämma största gemensamma divisorn till två eller flera tal. Antag att vi skall bestämma st.g.d. till de positiva heltalen $a_1, a_2, \ldots, a_n$. Vi kan härvid anta att alla $a_i > 1$, ty om något $a_i = 1$, blir även st.g.d. $= 1$. Detta fall saknar intresse. Talet a_i må ha primfaktoruppdelningen

$$a_i = p_1^{\alpha_{i1}} p_2^{\alpha_{i2}} \cdots p_k^{\alpha_{ik}} \qquad (i = 1, 2, \ldots, n). \tag{3.15}$$

Talen $p_1, p_2, \ldots, p_k$ betecknar här alla primfaktorerna i talen a_i. Om ett a_i saknar en primfaktor p_j, har vi blott att sätta motsvarande exponent $\alpha_{ij} = 0$. Sätt

$$m_j = \min(\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}) \qquad (j = 1, 2, \ldots, k). \tag{3.16}$$

Antalet faktorer p_j i $(a_1, a_2, \ldots, a_n)$ är uppenbarligen m_j. Vi får alltså:

$$(a_1, a_2, \ldots, a_n) = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}. \tag{3.17}$$

Som en tillämpning av denna formel skall vi bestämma (144,240,360). Vi har primfaktoruppdelningarna

$$144 = 2^4 3^2, \quad 240 = 2^4 3 \cdot 5, \quad 360 = 2^3 3^2 5.$$

Formel (3.17) ger nu $(144, 240, 360) = 2^3 3 = 24$.

Ett med största gemensamma divisorn besläktat begrepp är den minsta gemensamma multipeln till två eller flera heltal. Låt $a_1, a_2, \ldots, a_n$ vara heltal, alla $\neq 0$. Med en *gemensam multipel* till talen a_i förstås ett tal, som är divisibelt med vart och ett av dessa tal. Sådana tal existerar säkert, t.ex. talen $\pm a_1 a_2 \cdots a_n$. Låt M beteckna mängden av alla *positiva* gemensamma multipler. M har enligt sats 1.1 ett minsta tal m. Vi kallar m den *minsta (positiva) gemensamma multipeln* (m.g.m.) och skriver

$$m = [a_1, a_2, \ldots, a_n]. \tag{3.18}$$

Det finns även ett annat sätt att karakterisera minsta gemensamma multipeln, vilket endast utnyttjar delbarhetsegenskaperna hos multipeln ifråga. Detta sätt är en motsvarighet till sats 3.3 för största gemensamma divisorn.

Sats 3.11. *Det positiva heltalet m är minsta gemensamma multipeln till talen $a_1, a_2, \ldots, a_n$, om och endast om följande villkor är uppfyllda:*

(a) *m är en gemensam multipel till talen $a_1, a_2, \ldots, a_n$.*
(b) *m delar alla gemensamma multipler till talen $a_1, a_2, \ldots, a_n$.*

Bevis: Antag först att $m = [a_1, a_2, \ldots, a_n]$. Det är då klart att (a) gäller. Låt nu M vara en godtycklig gemensam multipel till talen $a_1, a_2, \ldots, a_n$. Vi tillämpar divisionsalgoritmen på talen m och M, varvid vi får: $M = mq + r$, där $0 \leq r < m$. Då nu både M och m är gemensamma multipler till talen $a_1, a_2, \ldots, a_n$, så är även $r = M - mq$ en gemensam multipel till dessa tal. Nu är emellertid m den minsta (positiva) gemensamma multipeln, och $0 \leq r < m$. Detta innebär att $r = 0$. Således är $M = mq$, dvs. $m \mid M$. Därmed är (b) ådagalagt. Omvänt om (a) och (b) gäller, så är m uppenbarligen den minsta gemensamma multipeln till talen $a_1, a_2, \ldots, a_n$. □

En äldre benämning på minsta gemensamma multipeln är "minsta gemensamma dividenden". Som bekant utnyttjas m.g.m. vid bråks liknämniggörande som den gemensamma nämnaren. Härvid bestämmer man vanligen m.g.m. genom att upplösa de givna talen i primfaktorer. Vi skall nu närmare redogöra för denna metod. Låt alltså $a_1, a_2, \ldots, a_n$ vara positiva heltal, vilkas m.g.m. skall bestämmas. Vi kan härvid anta att alla $a_i > 1$, ty om något $a_i = 1$, kan detta tal bortlämnas utan att det påverkar m.g.m. Antag att talet a_i har uppdelningen (3.15) i primfaktorer. Sätt

$$M_j = \max(\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}) \qquad (j = 1, 2, \ldots, k). \tag{3.19}$$

Varje gemensam multipel till talen $a_1, a_2, \ldots, a_n$ måste då innehålla åtminstone M_j faktorer p_j. Men eftersom vi söker den *minsta*-gemensamma multipeln, är M_j faktorer även tillräckligt. Således

$$[a_1, a_2, \ldots, a_n] = p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k}. \tag{3.20}$$

I det speciella fall att talen $a_1, a_2, \ldots, a_n$ är parvis relativt prima, får vi ett enkelt uttryck för deras m.g.m. I detta fall förekommer nämligen varje primfaktor p_j endast hos ett av talen a_i. Motsvarande M_j är alltså = p_j:s exponent i det tal, där p_j förekommer. Således är

$$p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k} = a_1 a_2 \cdots a_n.$$

Därmed har vi bevisat

Sats 3.12. *Om de positiva heltalen $a_1, a_2, \ldots, a_n$ är parvis relativt prima, så gäller:*

$$[a_1, a_2, \ldots, a_n] = a_1 a_2 \cdots a_n. \tag{3.21}$$

Det existerar ett enkelt samband mellan två tals st.g.d. och m.g.m., som gör det möjligt att beräkna det ena värdet ur det andra. Detta samband ges i följande sats.

Sats 3.13. *Låt a och b vara heltal > 1. Då gäller:*

$$(a, b)[a, b] = ab. \tag{3.22}$$

Bevis: Vi antar att a och b har primfaktoriseringarna

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Sätt $m_i = \min(a_i, b_i)$, $M_i = \max(a_i, b_i)$ för $i = 1, 2, \ldots, k$. Lätt inses att $m_i + M_i = a_i + b_i$. Detta ger med beaktande av formlerna (3.17) och (3.20):

$$\begin{aligned}
(a, b)[a, b] &= (p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \left(p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k} \right) \\
&= p_1^{m_1 + M_1} p_2^{m_2 + M_2} \cdots p_k^{m_k + M_k} \\
&= p_1^{a_1 + b_1} p_2^{a_2 + b_2} \cdots p_k^{a_k + b_k} \\
&= (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) \\
&= ab.
\end{aligned}$$

Därmed är formel (3.22) bevisad. □

Sambandet (3.22) gör det möjligt att beräkna $[a, b]$, då man känner (a, b). Detta är stundom en fördel, eftersom upplösningen av a och b i primfaktorer kan bereda svårigheter, om a och b är stora tal. För beräkningen av (a, b) kan man däremot med fördel använda Euklides algoritm, även då a och b är stora tal.

Varning! I det fall att man har tre tal a, b och c, gäller *icke* $(a, b, c)[a, b, c] = abc$, vilket man måhända skulle kunna tro på basen av formel (3.22). I själva verket gäller:

$$\frac{[a, b, c]}{(a, b, c)} = \frac{abc}{(a, b)(a, c)(b, c)}. \tag{3.23}$$

Beviset för denna formel ges som övningsuppgift 3.17.

3.4 Diofantiska ekvationer av första graden

Exempel 1 Antag att man skall sända ett paket på posten. Paketportot är 16 mk. Till förfogande har man endast frimärken i valörerna 2,10 mk och 3,50 mk. Kan man med dessa frimärken frankera paketet?

Exempel 2 En person vill köpa resechecker i en bank för 5100 mk. Banken har endast 200 mk:s och 500 mk:s checker till förfogande. Är det möjligt att med dessa checker komma till den önskade summan, och hur många checker av vartdera slaget skall han i så fall köpa?

Ovanstående problem ger upphov till s.k. diofantiska ekvationer, där man söker heltalslösningar och där antalet obekanta i regel är större än antalet ekvationer. Om man nämligen i det första exemplet betecknar antalet frimärken av valörerna 2,10 mk och 3,50 mk med x resp. y, får man ekvationen (då prisen anges i penni):

$$210x + 350y = 1600, \tag{3.24}$$

där vi söker en lösning (x, y) i positiva hela tal. I det andra exemplet får man på samma sätt ekvationen

$$200x + 500y = 5100. \tag{3.25}$$

Allmänt gäller att en *diofantisk ekvation av första graden* i n obekanta x_1, x_2, ..., x_n är av formen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

där koefficienterna a_1, a_2, ..., a_n och b är heltal och där vi söker en lösning i hela tal x_1, x_2, ..., x_n. Benämningen "diofantisk" härrör från den grekiske matematikern *Diofantos* (ca 350 e.Kr.), som skrev ett omfattande verk i talteori, *Arithmetica*, bestående av 13 böcker, av vilka 6 är bevarade.

I detta avsnitt kommer vi endast att behandla diofantiska ekvationer av första graden med två obekanta, således ekvationer av formen

$$ax + by = c, \tag{3.26}$$

där a, b och c är hela tal. För dessa ekvationer gäller följande grundläggande sats.

Sats 3.14. *Ekvationen* (3.26) *har heltalslösningar* (x, y), *om och endast om* $d = (a, b)$ *är en divisor i talet* c. *I detta fall gäller: Om* (x_0, y_0) *är en partikulär lösning, fås alla lösningar ur ekvationssystemet*

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t, \tag{3.27}$$

där t *genomlöper alla heltal.*

Bevis: Antag först att ekvationen (3.26) är lösbar. Det existerar alltså sådana heltal x_1, y_1 att $ax_1 + by_1 = c$. Då d är en divisor i a och b, måste d även vara en divisor i c (kor. 1.4). Villkoret $d \mid c$ är alltså nödvändigt. Antag nu att detta villkor är uppfyllt. Sätt $e = c/d$. Enligt kor. 3.1 existerar det hela tal m och n, sådana att $am + bn = d$. Multiplikation med e ger: $aem + ben = c$. Härav framgår att $x_0 = em$, $y_0 = en$ är en lösning till ekvationen. Villkoret $d \mid c$ är alltså tillräckligt för att ekvationen skall ha en lösning.

Det återstår nu att visa, att alla lösningar är av formen (3.27) i det fall att lösningar existerar. Genom direkt insättning av (3.27) i ekvationens vänstra led fås

$$ax_0 + a(b/d)t + by_0 - b(a/d)t = ax_0 + by_0 = c,$$

eftersom (x_0, y_0) är en partikulär lösning. Alltså utgör alla tal x, y av formen (3.27) lösningar till ekvationen. Ytterligare bör visas att *alla* lösningar kan skrivas i denna form. Låt fördenskull (x, y) vara en godtycklig lösning till ekvationen. Då gäller dels $ax + by = c$, dels $ax_0 + by_0 = c$. Härur fås: $ax + by = ax_0 + by_0$, vilket kan skrivas: $a(x - x_0) = -b(y - y_0)$. Division med d ger: $(a/d)(x - x_0) = -(b/d)(y - y_0)$. Härvid är talen a/d och b/d relativt primiska (sats 3.4). Vidare är produkten $(a/d)(x - x_0)$ delbar med b/d. Således är talet $x - x_0$ delbart med b/d (sats 3.8). Vi kan alltså sätta $x - x_0 = (b/d)t$, där t är ett helt tal. Detta ger: $x = x_0 + (b/d)t$. Insättes detta värde på x i ekvationen (3.26) och löses med avseende på y fås: $y = y_0 - (a/d)t$. Sålunda har vi visat att varje heltalslösning (x, y) till ekvationen (3.26) är av formen (3.27). Sats 3.14 är därmed fullständigt bevisad. □

Den allmänna lösningen (3.27) till ekvationen (3.26) förutsätter att man känner en partikulär lösning (x_0, y_0). Denna kan i regel hittas genom prövning, om talen a, b och c är små. Ett sätt, som säkert leder till resultat, är att utnyttja algoritmen i sats 3.7. Enligt denna algoritm kan vi finna sådana heltal s_n och t_n, att $as_n + bt_n = d$, då $d = (a, b)$. Multipliceras nu denna likhet med $e = c/d$ (som ju är ett heltal), fås $aes_n + bet_n = c$. Härav framgår att $x_0 = es_n$, $y_0 = et_n$ är en partikulär lösning till ekvationen.

Som en tillämpning av ovanstående teori skall vi behandla ekvationerna (3.24) och (3.25) i de bägge exemplen i början av detta avsnitt. Beträffande ekvationen (3.24) konstaterar vi att $(210, 350) = 70$ och att talet 1600 *inte* är delbart med 70. Ekvationen (3.24) saknar alltså lösning i hela tal x, y. Det är således inte möjligt att frankera paketet i exempel 1 med de angivna frimärkena. Vi övergår till ekvationen (3.25). Här är $(200, 500) = 100$, och 5100 är divisibelt med 100. Ekvationen är alltså lösbar. Vi dividerar ekvationen med den gemensamma divisorn 100 och får då den enklare ekvationen $2x + 5y = 51$. Vi börjar med att söka en partikulär lösning (x_0, y_0) och använder algoritmen i sats 3.7. (Prövning skulle givetvis här ett snabbare resultat). Med $a = 2$, $b = 5$ ger oss Euklides algoritm följande kvoter: $q_1 = 0$, $q_2 = 2$, $q_3 = 2$. Således är $n = 3$. Vi bildar nu talräckorna (s_i) och (t_i) $(i = 0, 1, 2, 3)$ enligt rekursionsformlerna (3.10). Då fås

$$s_0 = 1, \quad s_1 = 0, \quad s_2 = 1, \quad s_3 = -2,$$

$$t_0 = 0, \quad t_1 = 1, \quad t_2 = 0, \quad t_3 = 1.$$

Således är $2(-2)+5(1) = 1$ i enlighet med sats 3.7. Multiplikation med 51 ger: $2(-102)+5(51) = 51$. En partikulär lösning är alltså: $x_0 = -102$, $y_0 = 51$. Denna kan emellertid ej godkännas som en lösning på problemet i exempel 2, emedan detta problem kräver *positiva* heltalslösningar. Vi skall därför ur den allmänna lösningen $x = -102 + 5t$, $y = 51 - 2t$ utgripa sådana lösningar, för vilka $x \geq 0$, $y \geq 0$. Dessa villkor ger: $20,4 \leq t \leq 25,5$. Möjliga t-värden är alltså: $t = 21, 22, 23, 24, 25$. Motsvarande lösningspar (x, y) är: (3,9), (8,7), (13,5), (18,3) och (23,1). Dessa ger alltså fem olika alternativ för val av resechecker.

Övningsuppgifter

Uppgift 3.1 Uttryck följande taltripplars st.g.d. som en linjärkombination av talen ifråga: a) 6, 10, 15, b) 70, 98, 105.

Uppgift 3.2 Låt a och b vara hela tal, ej bägge = 0. Visa att $d = (a, b)$, om och endast om det existerar hela tal m och n, sådana att $a = md$, $b = nd$ och $(m, n) = 1$.

Uppgift 3.3 Bestäm a) $(26910, 58786)$, b) $(180127, 169979, 280663)$.

Uppgift 3.4 Visa att talen $3k + 2$ och $5k + 3$ alltid är relativt prima, då k är ett positivt heltal.

Uppgift 3.5 Låt a, m och n vara positiva heltal med $a \geq 2$. Visa att $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$. (Ledning: Antag att $m \geq n$ och tillämpa Euklides algoritm på talen $a^m - 1$ och $a^n - 1$).

Uppgift 3.6 Bestäm hela tal m och n, sådana att $(26910, 58786) = 26910m + 58786n$.

Uppgift 3.7 Betrakta Fibonacci-följden 1, 2, 3, 5, 8, 13, 21, ..., där varje tal fr.o.m. det tredje är summan av de två föregående talen. Visa att två på varandra följande tal alltid är relativt prima.

Uppgift 3.8 Visa att om talen a och b är relativt prima, så är även talen $a + b$ och ab relativt prima.

Uppgift 3.9 Upplös följande tal i primfaktorer: a) 169400, b) 9999, c) 140777.

Uppgift 3.10 Upplös följande tal i primfaktorer: a) $10^6 - 1$, b) $2^{24} - 1$, c) $3^{18} - 1$.

Uppgift 3.11 Låt n vara ett positivt heltal och p ett primtal. Visa att primfaktoriseringen av $n!$ innehåller talet p i potensen

$$[n/p] + [n/p^2] + [n/p^3] + \cdots$$

(Serien är ändlig, emedan endast ett ändligt antal termer $\neq 0$). Bestäm med användning av detta resultat primfaktoriseringen av 20!.

Uppgift 3.12 Bestäm a) [1001, 1071], b) [25641, 142857].

Uppgift 3.13 Bestäm [180127, 169979, 280663].

Uppgift 3.14 För vilka positiva heltal a och b gäller: $(a, b) = 18$, $[a, b] = 540$.

Uppgift 3.15 Låt a och b vara positiva heltal. Visa att $(a, b) = (a+b, [a, b])$. (Ledning: Uppgift 3.8 kan användas).

Uppgift 3.16 Bestäm två positiva heltal, vilkas summa = 798 och vilkas m.g.m. = 10780. (Ledning: Utnyttja resultatet i föregående uppgift).

Uppgift 3.17 Bevisa riktigheten av formel (3.23). (Ledning: Visa först att för godtyckliga reella tal x, y och z gäller: $\max(x, y, z) - \min(x, y, z) = x + y + z - \min(x, y) - \min(x, z) - \min(y, z)$).

Uppgift 3.18 Undersök huruvida följande diofantiska ekvationer har heltalslösningar och angiv i jakande fall den allmänna lösningen: a) $21x + 14y = 147$, b) $60x + 18y = 97$, c) $1402x - 1969y = 1$.

Uppgift 3.19 Ett sällskap på 30 personer reser med en bilfärja från Åbo till Stockholm. Resenärerna kan välja mellan tre olika hyttkategorier A, B och C. Priset/person i dessa hyttkategorier är (inklusive priset för överfarten): 298 mk, 250 mk resp. 172 mk. Totalt kostade resan för hela sällskapet 6960 mk. Huru många personer valde hyttkategori A, B resp. C?

Uppgift 3.20 Vi anknyter till exempel 2 i början av avsnitt 3.4.

(a) Visa att man inte kan köpa resechecker för 100 mk och 300 mk.

(b) Visa att man kan köpa resechecker för 200 mk samt för alla summor av formen $n \cdot 100$ mk, där n är ett heltal ≥ 4.

§ 4. Representation av tal

4.1 Historisk översikt

Vi skall i denna paragraf ta upp frågan om olika sätt att representera tal. Allmänt kan väl sägas att tal framställs med symboler (siffror) av ett eller annat slag. Vårt vanliga sätt att skriva tal är ett *positionssystem*, där varje siffras plats i talet anger dess värde i tiopotenser. Om någon tiopotens saknas, anges detta med siffran 0 på motsvarande plats i talet. Exempelvis är

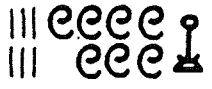
$$3705,28 = 3 \cdot 10^3 + 7 \cdot 10^2 + 5 \cdot 10^0 + 2 \cdot 10^{-1} + 8 \cdot 10^{-2}.$$

Eftersom detta system bygger på potenser av tio, kallas det ett *decimalsystem (tiosystem)*. Talet 10 kallas systemets *bas*.

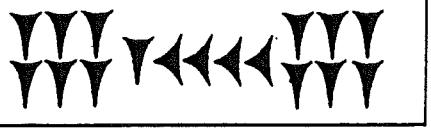
Tal har ingalunda alltid betecknats på samma sätt som i vårt decimala positionssystem. I det forna Egypten användes även tio som bas, men man hade olika tecken för de olika tiopotenserna. Dessa tecken upprepades så många gånger som ifrågavarande tiopotens förekom i talet. Egypternas system var alltså ett *additionssystem*. Detsamma kan sägas om romarnas sätt att beteckna tal. Man hade som bekant särskilda tecken för talen 1, 10, 100 och 1000, nämligen I, X, C och M. Därjämte hade man tecken för de halva tiopotenserna 5, 50 och 500, nämligen V, L och D. I övrigt sammanställdes talet ifråga genom en additions- och subtraktionsprincip. Sålunda skrevs t.ex. talet 1984 som MCMLXXXIV, där C:et framför det andra M:et anger att 100 skall subtraheras från 1000 för att ge 900. Likaså betecknar "ettan" framför "femman" talet 4. Talet 1991 skrivs MCMXCI med romerska siffror. Dessa siffror var delvis i bruk ännu på 1800-talet i Europa men hade redan på 1200-talet börjat undanträngas av vårt nuvarande decimalsystem med indisk-arabiska siffror.

Ett stort framsteg gjordes av babylonierna i och med att de använde ett positionssystem med 60 som bas. Man hade sålunda samma tecken för exempelvis 1, 60, 60^2, ..., medan tecknets position i talet angav tecknets värde i potenser av 60. Till att börja med hade man ingen nolla. Sålunda skrevs t.ex. talen $123 = 2 \cdot 60^1 + 3 \cdot 60^0$ och $7203 = 2 \cdot 60^2 + 3 \cdot 60^0$ på samma sätt, nämligen med tecknen för 2 och 3 efter varandra. Sammanhanget fick avgöra vilket tal som avsågs. Småningom infördes dock en nolla i mellanposition men ej i slutet av ett tal. Babylonierna skrev sina siffror med kilskrift på lertavlor. Kilskriften hade de övertagit av sumererna. Se figur 1 på följande sida.

Egypterna hade samma additionsprincip men byggde mer konsekvent på 10 som bas:

1	10	100	1 000	Exempel: 1706 (läses från höger)
				

Babylonierna använde additionssystemet för tal under 60, men däröver ett positionssystem:

1	10	60	10X60	60X60	Exempel: 21,706 = 6X60X60+1X60+46
					

Figur 1 Egypternas och babyloniernas talbeteckningssystem

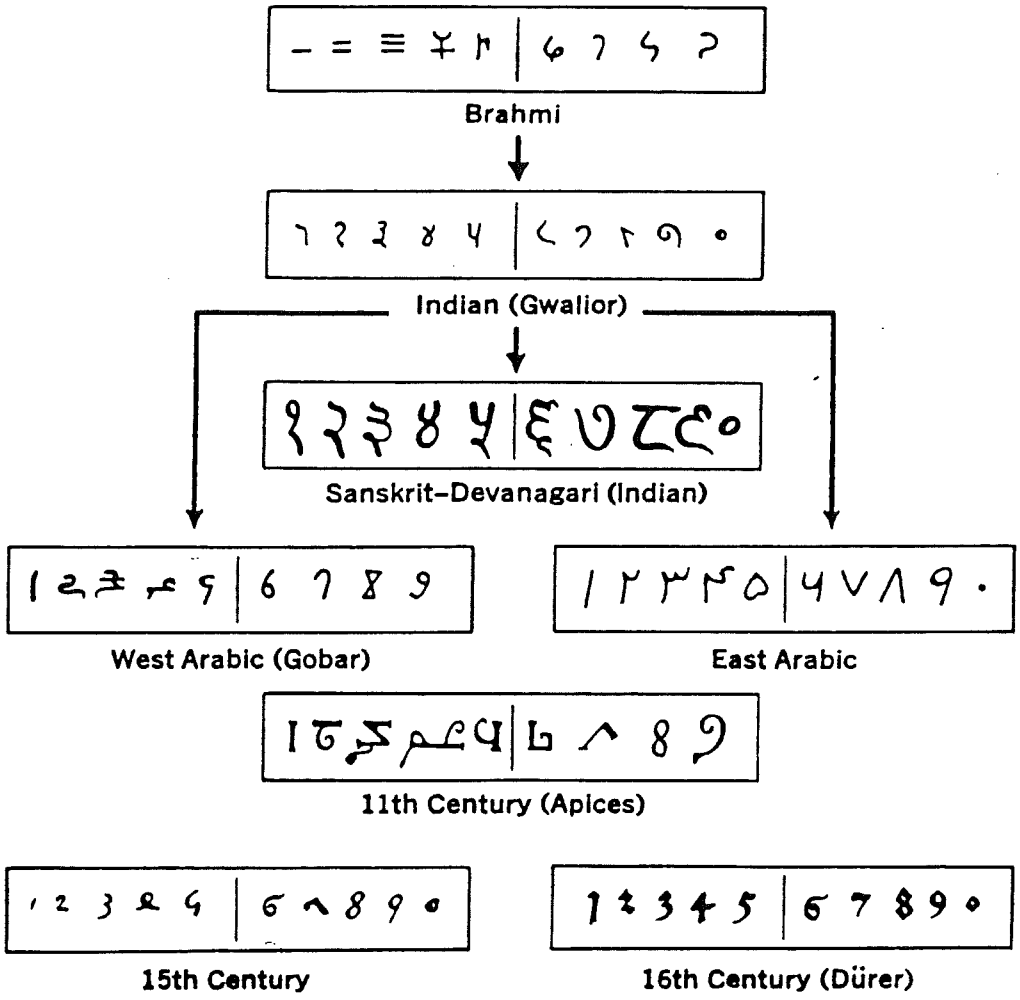
Grekerna förefaller att ha använt två olika talbeteckningssystem. I det yngre av dessa system, det s.k. joniska systemet, använde man hela grekiska alfabetet (stora bokstäver) utökat med tre äldre bokstäver. De nio första bokstäverna betecknade entalen 1-9, de nio följande bokstäverna tiotalen 10, 20, ..., 90, medan de nio sista bokstäverna betecknade hundratalen 100, 200, ..., 900. Systemet var additivt till sin uppbyggnad och krävde ingen särskild symbol för talet 0. Sedan de små bokstäverna introducerats i det grekiska alfabetet, övergick man till att använda dessa som taltecken. Med detta beteckningssätt skrevs t.ex. talet 8888 som $/\eta\omega\pi\eta$, där bokstäverna η, π och ω betecknar resp. 8, 80 och 800. Strecket framför det första "etat" anger att talet 8 skall multipliceras med 1000 för att ge 8000. Tack vare detta tilläggsstreck kunde man framställa varje tal < 10000 med endast fyra bokstäver. Se figur 2, som i likhet med figur 1 är lånad från [4].

Grekerna använde under hellenistisk tid konsekvent hela sitt alfabet (med en del extra tecken) för att beteckna talvärden. Första tredjedelen angav ental, andra tredjedelen tiotal, sista tredjedelen hundratal. Ett snedstreck framför en bokstav multiplicerade denna med 1 000:

	1 2 3 4 5 6 7 8 9	Exempel: 1706
ental		
tiotal		
hundratal		

Figur 2 Det grekiska talbeteckningssystemet

Varifrån härstammar då vårt decimala positionssystem? Det anses allmänt att detta system har uppstått i Indien, varifrån det genom arabernas förmedling kommit till Europa. Det är ej klarlagt om indierna själva utvecklat systemet eller om de möjligen varit påverkade av andra kulturer (babylonisk, grekisk och/eller kinesisk). Ett viktigt indiskt bidrag var dock införandet av nollan som tecken för avsaknad av tiopotens. Genom introduktionen av nollan (såväl inne i ett tal som i slutet av talet) blev vårt positionssystem fulländat. Beträffande våra siffertecken kan sägas, att de genomgått en lång utveckling ända från de s.k. Brahmi-siffrorna i Indien över olika typer av arabiska siffror fram till våra dagars siffror 0, 1, 2, ..., 9. Några skeden i denna utveckling illustreras i figur 3, som är lånad från [5].



Figur 3 Våra siffrors utveckling

4.2 Bassystem

Vi skall nu undersöka talrepresentation med en godtycklig bas $b \geq 2$. Den fråga vi närmast önskar besvara är följande: Kan varje positivt heltal n alltid skrivas i formen

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \tag{4.1}$$

där $a_k \neq 0$ och varje a_i är ett heltal, som uppfyller olikheten $0 \leq a_i < b$ för $i = 0, 1, 2, \ldots, k$. Vi frågar m.a.o. om talet n alltid kan framställas i ett givet bassystem $b \geq 2$ med hjälp av "siffrorna" a_k, a_{k-1}, ..., a_1, a_0. Vi skall visa att en sådan framställning är möjlig och att den är entydig. Först skall vi emellertid ge en algoritm, enligt vilken vi kan beräkna talen a_0, a_1, ..., a_{k-1}, a_k. Vi börjar med att tillämpa divisionsalgoritmen på talen n och b. Vi får då

$$n = bq_0 + a_0 \qquad (0 \leq a_0 < b).$$

Därefter divideras q_0 med b, varvid fås:

$$q_0 = bq_1 + a_1 \qquad (0 \leq a_1 < b).$$

I följande steg divideras q_1 med b. Detta ger:

$$q_1 = bq_2 + a_2 \qquad (0 \leq a_2 < b).$$

Genom att fortsätta på detta sätt, tills vi får en kvot $q_k = 0$, erhåller vi följande schema:

$$\begin{aligned}
n &= bq_0 + a_0 && (0 \leq a_0 < b) \\
q_0 &= bq_1 + a_1 && (0 \leq a_1 < b) \\
q_1 &= bq_2 + a_2 && (0 \leq a_2 < b) \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
q_{k-2} &= bq_{k-1} + a_{k-1} && (0 \leq a_{k-1} < b) \\
q_{k-1} &= b \cdot 0 + a_k && (0 \leq a_k < b).
\end{aligned} \tag{4.2}$$

Eftersom talen $n > q_0 > q_1 > q_2 > \cdots \geq 0$ bildar en strikt avtagande följd av heltal (då $b \geq 2$), måste processen upphöra efter ett ändligt antag steg. Algoritmen (4.2) har alltså gett en heltalsföljd a_0, a_1, a_2, ..., a_k med $0 \leq a_i < b$ för $i = 0, 1, 2, \ldots, k$. Vi skall nu visa att talen a_i satisfierar ekvationen (4.1). Vi insätter fördenskull värdet på q_0, taget ur den andra ekvationen (4.2), i den första ekvationen (4.2). Vi får då:

$$n = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0.$$

I detta uttryck insättes nu värdet på q_1, taget ur den tredje ekvationen (4.2). Då fås:

$$n = b^2(bq_2 + a_2) + a_1 b + a_0 = b^3 q_2 + a_2 b^2 + a_1 b + a_0.$$

Då vi fortsätter på detta sätt och successivt insätter värdena på q_2, q_3, ..., q_{k-1}, får vi följande schema:

$$\begin{aligned}
n &= bq_0 + a_0 \\
n &= b^2q_1 + a_1b + a_0 \\
n &= b^3q_2 + a_2b^2 + a_1b + a_0 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
n &= b^{k-1}q_{k-2} + a_{k-2}b^{k-2} + \cdots + a_1b + a_0 \\
n &= b^kq_{k-1} + a_{k-1}b^{k-1} + \cdots + a_1b + a_0 \\
&= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0,
\end{aligned}$$

ty $a_k = q_{k-1} \neq 0$ på grund av den sista ekvationen (4.2). Därmed har vi visat att talen a_i, såsom de framgår ur schemat (4.2), faktiskt satisfierar ekvationen (4.1). Det återstår nu att visa, att framställningen (4.1) för talet n är entydig, så snart basen b (≥ 2) är given.

Antag som antites att vi skulle ha två olika framställningar:

$$n = a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0 \tag{4.3}$$

$$n = c_kb^k + c_{k-1}b^{k-1} + \cdots + c_1b + c_0, \tag{4.4}$$

där $0 \leq a_i < b$ och $0 \leq c_i < b$ för $i = 0, 1, 2, \ldots, k$. (De två framställningarna behöver egentligen inte ha samma antal $(k+1)$ termer, men vi kan tänka oss att vi till den som har färre termer har adderat termer med 0-koefficienter, så att antalet blir lika). Då framställningarna (4.3) och (4.4) är olika, måste vi ha $a_i \neq c_i$ för något i. Låt j vara det minsta indexet, för vilket detta inträffar. Genom att subtrahera (4.4) från (4.3) får vi då:

$$\begin{aligned}
&(a_k - c_k)b^k + \cdots + (a_{j+1} - c_{j+1})b^{j+1} + (a_j - c_j)b^j = \\
&= b^j\left[(a_k - c_k)b^{k-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)\right] = 0.
\end{aligned}$$

Härav följer att

$$(a_k - c_k)b^{k-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0,$$

vilket i sin tur ger

$$a_j - c_j = b\left[(c_k - a_k)b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1})\right].$$

Härav framgår att $b \mid (a_j - c_j)$. Å andra sidan vet vi att $|a_j - c_j| < b$, emedan $0 \leq a_j < b$ och $0 \leq c_j < b$. Således måste vi ha $a_j = c_j$, vilket strider mot att vi antog $a_j \neq c_j$. Denna motsägelse visar att antitesen är falsk. Framställningen (4.1) är alltså entydig. Vi sammanfattar våra resultat i följande sats.

Sats 4.1. *Varje positivt heltal n kan, så snart heltalet $b \geq 2$ är givet, entydigt framställas i formen* (4.1), *där $a_k \neq 0$ och $0 \leq a_i < b$ för $i = 0, 1, 2, \ldots, k$.*

I det speciella fall att $b = 2$ få vi

Kor. 4.1. *Varje positivt heltal n kan entydigt framställas i formen*

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0,$$

där $a_k \neq 0$ och $a_i = 0$ eller 1 för $i = 0, 1, 2, \ldots, k$.

Såsom tidigare nämnts, kallas talet b i formel (4.1) *bas* eller *bassystem* för framställningen ifråga. Koefficienterna a_i kallas talet n:s *siffror* i bassystemet b. Vissa speciella bassystem har särskilda namn. Om $b = 10$ talar vi som känt om det *decimala* systemet. Systemet med basen 2 kallas det *binära* systemet. Vi återkommer strax till detta system. I fallen $b = 8$ och $b = 16$ talar vi om det *oktala* resp. *hexadecimala* systemet. Om vi vill ange att talet n har siffrorna a_k, a_{k-1}, ..., a_1, a_0 i systemet med basen b, skriver vi

$$n = (a_k a_{k-1} \ldots a_1 a_0)_b.$$

Om basen b ej anges, förutsättes i allmänhet att talet ifråga är skrivet i decimalsystemet.

Som en tillämpning av det ovanstående skall vi förvandla talet 2386 till systemet med basen 5 (5-systemet). Vi tillämpar algoritmen (4.2) med $n = 2386$ och $b = 5$, varvid vi får:

$$\begin{aligned} 2386 &= 5 \cdot 477 + 1 \\ 477 &= 5 \cdot 95 + 2 \\ 95 &= 5 \cdot 19 + 0 \\ 19 &= 5 \cdot 3 + 4 \\ 3 &= 5 \cdot 0 + 3 \end{aligned}$$

Vi får således $2386 = (34021)_5$. I 5-systemet behövs endast siffrorna 0, 1, 2, 3, 4. För att uttrycka ett tal i det hexadecimala systemet behöver vi däremot 16 siffror. Då våra vanliga siffror sålunda ej räcker till, tar vi bokstäver till hjälp. Vi kan t.ex. utnyttja bokstäverna A, B, C, D, E, F och sätta $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, $F = 15$. Om vi exempelvis skall förvandla talet $(A35B0F)_{16}$ till 10-systemet, får vi följande uträkning:

$$(A35B0F)_{16} = 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 16^2 + 15 = 10705679.$$

4.3 Det binära systemet

Det binära systemet har talet 2 som bas. I detta system användes sålunda endast siffrorna 0 och 1. På grund härav har det binära systemet fått många användningar, speciellt inom datatekniken. Datorer representerar internt sina data i det binära systemet, eller som man ofta säger *binärt*. Orsaken är enkel: Man behöver endast två olika "tillstånd" för att framställa talen 0 och 1. Hur dessa "tillstånd" förverkligas rent tekniskt, skall vi här inte gå in på.

I det följande skall vi se hur man kan utföra den grundläggande räkneoperationen, additionen, inom det binära systemet. Antag att vi önskar addera talen $a = (a_{n-1}a_{n-2}\dots a_1a_0)_2$ och $b = (b_{n-1}b_{n-2}\dots b_1b_0)_2$ binärt. (Genom ett eventuellt tillägg av nollor i början av det ena talet kan vi åstadkomma att talen har samma antal (n) siffror). Eftersom

$$a = \sum_{i=0}^{n-1} a_i \cdot 2^i, \qquad b = \sum_{i=0}^{n-1} b_i \cdot 2^i,$$

får vi

$$a + b = \sum_{i=0}^{n-1} (a_i + b_i)2^i. \tag{4.5}$$

Enligt divisionsalgoritmen kan vi skriva

$$a_0 + b_0 = 2q_0 + r_0,$$

där $r_0 = 0$ eller 1. Då summan $a_0 + b_0$ endast kan anta värdena 0, 1 eller 2, är $q_0 = 0$ eller 1. Vi kallar q_0 *minnessiffran*, som skall föras över till nästa steg. I detta steg tillämpar vi divisionsalgoritmen på talen $a_1 + b_1 + q_0$ och 2, varvid vi får

$$a_1 + b_1 + q_0 = 2q_1 + r_1,$$

där q_1 och r_1 har värdena 0 eller 1. Då vi fortsätter på samma sätt, får vi följande schema, där talen q_i och r_i antar värdena 0 eller 1:

$$\begin{aligned}
a_0 + b_0 &= 2q_0 + r_0 \\
a_1 + b_1 + q_0 &= 2q_1 + r_1 \\
a_2 + b_2 + q_1 &= 2q_2 + r_2 \\
&\dots\dots\dots\dots\dots\dots \\
a_{n-1} + b_{n-1} + q_{n-2} &= 2q_{n-1} + r_{n-1} \\
q_{n-1} &= r_n.
\end{aligned} \tag{4.6}$$

I den sista ekvationen har vi endast minnessiffran q_{n-1} att dividera med 2, och då denna minnessiffra $= 0$ eller 1, får vi $q_{n-1} = 2 \cdot 0 + r_n$, dvs. $q_{n-1} = r_n$. Multipliceras nu den första ekvationen (4.6) med 2^0, den andra med 2^1, den tredje med 2^2 och slutligen den sista med 2^n, får vi efter addition led för led (ty minnessiffrorna "tar ut" varandra):

$$\sum_{i=0}^{n} (a_i + b_i)2^i = \sum_{i=0}^{n} r_i \cdot 2^i.$$

(I summan till vänster är $a_n = b_n = 0$, emedan dessa siffror saknas i den binära framställningen av talen a och b). En jämförelse med (4.5) visar nu att

$$a + b = \sum_{i=0}^{n} r_i \cdot 2^i.$$

Den binära framställningen av summan $a + b$ är alltså:

$$a + b = (r_n r_{n-1} \ldots r_1 r_0)_2, \tag{4.7}$$

där siffrorna r_0, r_1, ..., r_{n-1}, r_n framgår av schemat (4.6). Eftersom talen a_i, b_i och q_{i-1} endast kan vara = 0 eller 1 och additionen $a_i + b_i + q_{i-1}$ kan ske så, att vi först bildar summan $a_i + b_i$ och därefter adderar minnessiffran q_{i-1}, är det tillräckligt att komma ihåg följande *additionstabell:*

$$\begin{aligned} 0 + 0 &= 0 \\ 1 + 0 &= 1 \\ 0 + 1 &= 1 \\ 1 + 1 &= 0 \quad \text{(minnessiffra = 1).} \end{aligned}$$

Det bereder ingen svårighet att konstruera elektriska kretsar, som s.a.s. kan denna additionstabell "utantill". På denna princip bygger datorns sätt att addera. Vi illustrerar ovanstående teori med följande

Exempel Utför additionen $(1001110)_2 + (1011101)_2$ i det binära systemet. Vi gör den vanliga additionsuppställningen och utnyttjar additionstabellen ovan. Vi får då:

$$\begin{array}{r} 1\ \ 1\ 1\ 1 \\ 1\ 0\ 0\ 1\ 1\ 1\ 0 \\ 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ \hline 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1 \end{array}$$

Således är $(1001110)_2 + (1011101)_2 = (10101011)_2$. Om vi skriver talen i decimalsystemet, får vi additionen $78 + 93 = 171$.

För de övriga räknesätten kan man bilda liknande algoritmer i det binära systemet. Man finner då att man vid det praktiska utförandet av operationerna kan förfara på samma sätt som i decimalsystemet, blott man beaktar att systemets bas = 2.

Vi avslutar detta kapitel med att redogöra för en metod att utföra en multiplikation, som baserar sig på det binära systemet (ehuru talen ifråga inte skrivs binärt). Detta sätt att multiplicera två tal användes bl.a. i det forna Egypten och kallas därför ofta *egyptisk multiplikation.* Antag t.ex. att vi skall multiplicera talen 37 och 43. Vi skriver då upp de heltaliga potenserna av talet 2 i en kolumn och i kolumnen bredvid talet 43 multiplicerat med dessa potenser. Sistnämnda tal fås i praktiken genom successiva fördubblingar av talet 43. Vi får då:

1	43
2	86
4	172
8	344
16	688
32	1376

Nu söker vi i den vänstra kolumnen upp de potenser av 2, vilkas summa = 37. Sådana potenser existerar på grund av kor. 4.1. I vårt fall får vi potenserna 1, 4 och 32. Motsvarande tal i den högra kolumnen är 43, 172 och 1376. Dessa adderas och ger summan 1591. Vi påstår nu att $1591 = 37 \cdot 43$. För att inse detta betraktar vi det allmänna fallet med två positiva heltal a och b, vilkas produkt sökes. Vi tänker oss talet a skrivet i binär form:

$$a = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2 + a_0,$$

varvid $a_i = 0$ eller 1. Antag t.ex. att $a_i = 1$ för $i = i_0, i_1, \ldots, i_k$, medan övriga $a_i = 0$. Således är

$$a = 2^{i_0} + 2^{i_1} + \cdots + 2^{i_k}.$$

Härur fås

$$ab = b \cdot 2^{i_0} + b \cdot 2^{i_1} + \cdots + b \cdot 2^{i_k}.$$

Vi ser alltså att produkten ab = summan av de multipler av b, som svarar mot de potenser av 2, vilka ger summan a. Därmed är förfarandet i den egyptiska multiplikationen motiverat.

Övningsuppgifter

Uppgift 4.1 Förvandla talet $(34051)_6$ till 10-systemet.

Uppgift 4.2 Förvandla talet 37865 till 7-systemet.

Uppgift 4.3 Förvandla talet $(65435)_8$ från 8-systemet till 5-systemet.

Uppgift 4.4 Utför additionen $(5843)_9 + (36845)_9 + (10372)_9$ i 9-systemet.

Uppgift 4.5 Uppskriv multiplikationstabellen i 5-systemet (endast siffrorna 0-4 får användas) och utför i detta system multiplikationen $(3401)_5 \cdot (2314)_5$.

Uppgift 4.6 Utför additionen $(ABBA)_{16} + (BABA)_{16}$ i 16-systemet med de värden på A och B, som angivits i texten.

Uppgift 4.7 Utför additionen $(101111011)_2 + (1100111011)_2$ i det binära systemet.

Uppgift 4.8 Utför subtraktionen $(1101101100)_2 - (101110101)_2$ i det binära systemet.

Uppgift 4.9 Uppskriv multiplikationstabellen i det binära systemet och utför i detta system multiplikationen $(11101)_2 \cdot (110001)_2$.

Uppgift 4.10 Beskriv hur man på enklast möjliga sätt kan förvandla ett tal från det binära till det hexadecimala systemet. Motivera svaret!

§ 5. Kongruenser

5.1 Några grundläggande satser

I denna paragraf skall vi införa ett nytt talteoretiskt begrepp, kongruensbegreppet, som visat sig vara mycket användbart i talteorin. Begreppet infördes av Gauß i hans berömda verk *Disquisitiones arithmeticae* (1801), vilket kan sägas lägga grunden till den moderna talteorin.

I detta avsnitt betecknar a, b, c och d genomgående godtyckliga heltal och m ett *positivt* heltal, såvida ej annat särskilt påpekas.

Definition: Talen a och b säges vara *kongruenta modulo* m (a *är kongruent med* b *modulo* m), om $m \mid (a-b)$. Detta betecknas: $a \equiv b \pmod{m}$. I motsatt fall skriver vi: $a \not\equiv b \pmod{m}$ och säger att a *är inkongruent med* b *modulo* m.

Exempelvis gäller: $25 \equiv 11 \pmod{7}$, $13 \equiv -7 \pmod{5}$ och $-19 \equiv -3 \pmod{4}$. När man opererar med kongruenser, kan det stundom vara fördelaktigt att förvandla dem till likheter. För detta ändamål har vi följande

Sats 5.1. $a \equiv b \pmod{m}$, *om och endast om det existerar ett heltal* k *med egenskapen* $a = b + km$.

Satsen följer omedelbart ur det faktum att $m \mid (a-b) \Leftrightarrow a - b = km$ för något heltal k. I de följande satserna skall vi ge några grundläggande egenskaper hos kongruenser.

Sats 5.2. *Kongruensrelationen är en ekvivalensrelation, dvs.*

(a) $a \equiv a \pmod{m}$

(b) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(c) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Bevis: (a) gäller emedan $a - a = 0$ är divisibelt med m. Om $a - b$ är delbart med m, så är även $b - a$ delbart med m. Alltså gäller (b). Om $a - b$ och $b - c$ är divisibla med m, så är även $a - c = (a-b) + (b-c)$ divisibelt med m. Härav följer (c). □

Det visar sig att man kan operera med kongruenser ungefär på samma sätt som med vanliga likheter. Detta framgår av de följande satserna.

Sats 5.3. *För kongruenser modulo m gäller:*

(a) $$a \equiv b \wedge c \equiv d \Rightarrow a \pm c \equiv b \pm d$$

(b) $$a \equiv b \wedge c \equiv d \Rightarrow ac \equiv bd.$$

Bevis: Då $a-b$ och $c-d$ är delbara med m, så är även talet $(a \pm c)-(b \pm d) = (a-b) \pm (c-d)$ delbart med m (sats 1.4). Härav följer (a). Formel (b) följer ur identiteten

$$ac - bd = a(c-d) + d(a-b).$$

Därmed är satsen bevisad. □

Eftersom $c \equiv c$ för varje modul m, så ger sats 5.3 följande

Kor. 5.3. *Om* $a \equiv b \pmod{m}$, *så är*

(a) $$a \pm c \equiv b \pm c \pmod{m}$$

(b) $$ac \equiv bc \pmod{m}.$$

Vi kan alltså öka eller minska de bägge leden i en kongruens med samma tal utan att kongruensen upphör att gälla. Likaså kan vi multiplicera de bägge leden i en kongruens med en och samma konstant. Hur är det med division? Kan vi dividera bort en gemensam faktor ur de bägge leden i en kongruens? Vi har t.ex. $48 \equiv 18 \pmod{15}$. Men $8 \not\equiv 3 \pmod{15}$. Å andra sidan gäller: $8 \equiv 3 \pmod{5}$. Vi blir tydligen tvungna att även ändra på moduln för att division med en gemensam faktor skall bibehålla kongruensen. Hur detta sker, framgår av följande sats.

Sats 5.4. *Ur* $ac \equiv bc \pmod{m}$ *följer* $a \equiv b \pmod{m/d}$, *där* $d = (c, m)$.

Bevis: Av sats 5.1 följer att det finns ett heltal k med egenskapen $c(a-b) = ac - bc = km$. Division med d ger: $(c/d)(a-b) = k(m/d)$. Produkten $(c/d)(a-b)$ är alltså delbar med m/d. Vidare är $(c/d, m/d) = 1$ enligt sats 3.4. Således är talet $a-b$ delbart med m/d (sats 3.8), vilket betyder att $a \equiv b \pmod{m/d}$. □

I specialfallet $(c, m) = 1$ får vi följande korollarium.

Kor. 5.4. *Om talen c och m är relativt primiska, så gäller:*

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}.$$

Upprepad användning av sats 5.3 (b) ger med $a = c$ och $b = d$:

Sats 5.5. *Ur* $a \equiv b \pmod{m}$ *följer* $a^k \equiv b^k \pmod{m}$, *där k är ett positivt heltal.*

Genom att kombinera resultaten i satserna 5.3 och 5.5 får vi:

Sats 5.6. *Om $f(x)$ är ett polynom i x med heltalskoefficienter och om $a \equiv b \pmod{m}$, så är $f(a) \equiv f(b) \pmod{m}$.*

Det händer stundom att man har att göra med kongruenser med olika moduler. För dylika kongruenser gäller bl.a. följande sats.

Sats 5.7. *Låt $m_1, m_2, \ldots, m_k$ vara positiva heltal. Då gäller med $M = [m_1, m_2, \ldots, m_k]$:*

$$a \equiv b \pmod{m_1} \wedge a \equiv b \pmod{m_2} \wedge \ldots \wedge a \equiv b \pmod{m_k} \Rightarrow a \equiv b \pmod{M}.$$

Bevis: Av antagandena följer att $a - b$ är divisibelt med vart och ett av talen $m_1, m_2, \ldots, m_k$. Talet $a - b$ är m.a.o. en gemensam multipel till talen $m_1, m_2, \ldots, m_k$. Enligt sats 3.11 är då $a - b$ delbart med M, dvs. $a \equiv b \pmod{M}$. □

I det speciella fall att talen $m_1, m_2, \ldots, m_k$ är parvis relativt prima, gäller enligt sats 3.12: $M = m_1 m_2 \cdots m_k$. Vi får i detta fall följande korollarium.

Kor. 5.7. *Om de positiva heltalen $m_1, m_2, \ldots, m_k$ är parvis relativt prima, så gäller:*

$$a \equiv b \pmod{m_1} \wedge a \equiv b \pmod{m_2} \wedge \ldots \wedge a \equiv b \pmod{m_k} \Rightarrow a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

5.2 Restklasser och restsystem

Låt liksom tidigare m beteckna ett positivt heltal. Enligt sats 5.2 är kongruensrelationen en ekvivalensrelation. Detta medför att varje kongruens modulo m indelar de hela talens mängd Z i ekvivalensklasser, här kallade *restklasser*, på sådant sätt att tal inom samma klass är sinsemellan kongruenta, medan tal ur olika klasser är inkongruenta modulo m. För att bestämma dessa restklasser tar vi ett godtyckligt tal $a \in Z$ och tillämpar divisionsalgoritmen på a och m. Vi får då $a = mq + r$, där r är ett heltal med $0 \leq r < m$. Således är $a \equiv r \pmod{m}$. Talet r kan endast anta något av värdena 0, 1, 2, ..., $m - 1$, och dessa tal är sinsemellan inkongruenta modulo m. Varje heltal a är alltså kongruent med ett och endast ett av de sinsemellan inkongruenta talen $0, 1, 2, \ldots, m-1$. Detta betyder att heltalsmängden Z av kongruensen modulo m indelas i m restklasser och att talen 0, 1, 2, ..., $m - 1$ utgör representanter för dessa restklasser. Talen i en och samma restklass modulo m är alltså av formen $mq + r$, där q genomlöper alla heltal och där r är ett fixt heltal med $0 \leq r \leq m - 1$. Talen 0, 1, 2, ..., $m - 1$ bildar ett s.k. fullständigt restsystem modulo m. Allmänt gäller nämligen följande

Definition: De m heltalen $r_1, r_2, \ldots, r_m$ kallas ett *fullständigt restsystem modulo m*, om de är parvis inkongruenta modulo m.

Varje tal i ett fullständigt restsystem utgör alltså representant för var sin restklass. Restsystemet $\{0, 1, 2, \ldots, m-1\}$ kallas de *minsta positiva resterna* eller *huvudresterna modulo* m. Andra fullständiga restsystem existerar också. T.ex. om m är ett positivt udda tal, så bildar talen

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2} \tag{5.1}$$

ett fullständigt restsystem modulo m. De är nämligen m till antalet och sinsemellan inkongruenta modulo m. Talen (5.1) kallas de *minsta absoluta resterna modulo* m (när m är udda).

Vi belyser det ovansagda med ett enkelt exempel. Antag att $m = 5$. Vi erhåller då fem restklasser $K_r = \{5q + r : q \in Z\}$, där r genomlöper ett fullständigt restsystem modulo 5, t.ex. $r = 0, 1, 2, 3, 4$. Vi får sålunda

$$\begin{aligned}
K_0 &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \\
K_1 &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \\
K_2 &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \\
K_3 &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} \\
K_4 &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

Genom att plocka ett tal ur varje restklass får vi ett fullständigt restsystem modulo 5. Ett sådant system är t.ex. $\{10, 16, -3, 8, -11\}$.

Vi återgår till den allmänna teorin. Följande sats visar hur man utgående från ett givet fullständigt restsystem kan bilda ett annat fullständigt restsystem.

Sats 5.8. *Vi antar att a, b och m är givna heltal med $m > 0$. Vidare antas att a och m är relativt prima. Då gäller: Om $\{r_1, r_2, \ldots, r_m\}$ är ett fullständigt restsystem modulo m, så bildar även talen*

$$ar_1 + b,\ ar_2 + b, \ldots,\ ar_m + b \tag{5.2}$$

ett fullständigt restsystem modulo m.

Bevis: Vi bör visa att talen (5.2) är parvis inkongruenta modulo m. Antag som antites att vi skulle ha $ar_h + b \equiv ar_k + b \pmod{m}$ för något indexpar (h, k). Då är $ar_h \equiv ar_k \pmod{m}$ enligt kor. 5.3, och då $(a, m) = 1$, kan den sistnämnda kongruensen divideras med a (kor. 5.4). Vi skulle alltså ha $r_h \equiv r_k \pmod{m}$, vilket strider mot att talen $r_1, r_2, \ldots, r_m$ bildar ett fullständigt restsystem modulo m. Således utgör talen (5.2) ett fullständigt restsystem modulo m. □

Om man i sats 5.8 speciellt väljer $r_1 = 0$, $r_2 = 1$, $r_3 = 2$, ..., $r_m = m - 1$, får man följande korollarium.

Kor. 5.8. *Låt a, b och m vara givna heltal med $m > 0$ och $(a, m) = 1$. Då gäller: Talen*

$$0 \cdot a + b,\ 1 \cdot a + b,\ 2 \cdot a + b, \ldots,\ (m-1)a + b \tag{5.3}$$

bildar ett fullständigt restsystem modulo m.

Det förekommer rätt ofta, när man opererar med numeriska värden, att man önskar reducera ett givet tal a till ett annat (i regel numeriskt mindre) tal a', som är kongruent med a med avseende på någon given modul m. Det vanligaste fallet är att man söker a:s huvudrest modulo m, dvs. talet r i divisionsalgoritmen $a = mq + r$. Man brukar därför använda beteckningen

$$a \bmod m = a\text{:s huvudrest modulo } m. \tag{5.4}$$

I princip kan $r = a \bmod m$ naturligtvis bestämmas genom divisionen a/m, varvid $r = a - [a/m]m$. Emellertid inträffar det inte så sällan, att talet a är mycket stort, så att divisionen a/m är besvärlig eller rentav omöjlig att utföra i praktiken (t.o.m. med dator). Detta inträffar t.ex. om a är givet i formen $a = b^k$, där $b > 1$ och k är ett relativt stort positivt heltal. I sådana fall är det fördelaktigt att med stöd av satserna 5.3–5.5 utföra reduktionen stegvis, så att varje steg ger ett numeriskt mindre tal $a' \equiv a \pmod m$. Vi belyser detta med ett par exempel.

Exempel 1 Beräkna $52(169^9 + 87^7) \bmod 11$. Sätt $n = 52(169^9 + 87^7)$. Man finner genom vanlig division:

$$52 \equiv 8 \pmod{11}$$
$$169 \equiv 4 \pmod{11}$$
$$87 \equiv -1 \pmod{11}.$$

Således gäller enligt satserna 5.3 och 5.5:

$$n \equiv 8(4^9 + (-1)^7) \pmod{11}.$$

Vidare gäller enligt sats 5.5:

$$4^2 = 16 \equiv 5 \pmod{11}$$
$$4^4 \equiv 25 \equiv 3 \pmod{11}$$
$$4^8 \equiv 9 \pmod{11}$$
$$4^9 \equiv 36 \equiv 3 \pmod{11}.$$

Således är $n \equiv 8(3 - 1) = 16 \equiv 5 \pmod{11}$. Därmed har vi resultatet: $n \bmod 11 = 5$.

Exempel 2 I detta exempel skall vi visa hur man beräknar huvudresten modulo m av ett tal av formen a^k, då a, k och m är positiva heltal. Välj t.ex. $a = 35$, $k = 308$ och $m = 23$. Vi söker

alltså 35^{308} mod 23. Talet 35^{308} innehåller 476 siffror, varför det skulle vara oerhört arbetskrävande (åtminstone utan datorhjälp) att först beräkna 35^{308} och därefter utföra divisionen med 23. Vi skall därför anvisa en annan metod, som kräver endast måttligt räknearbete. Genom successiva kvadreringar och reduceringar modulo 23 bildar vi först huvudresterna modulo 23 av talen 35, 35^2, 35^4, ..., 35^{256}. Således

$$35 \equiv 12 \pmod{23}$$
$$35^2 \equiv 144 \equiv 6 \pmod{23}$$
$$35^4 \equiv 36 \equiv 13 \pmod{23}$$
$$35^8 \equiv 169 \equiv 8 \pmod{23}$$
$$35^{16} \equiv 64 \equiv 18 \pmod{23}$$
$$35^{32} \equiv 324 \equiv 2 \pmod{23}$$
$$35^{64} \equiv 4 \pmod{23}$$
$$35^{128} \equiv 16 \pmod{23}$$
$$35^{256} \equiv 256 \equiv 3 \pmod{23}.$$

Nu är $308 = 4 + 16 + 32 + 256$, vilket medför att $35^{308} \equiv 13 \cdot 18 \cdot 2 \cdot 3 = 1404 \equiv 1 \pmod{23}$. Vi har alltså slutresultatet: $35^{308} \bmod 23 = 1$.

Exempel 2 illustrerar vad man brukar kalla *modulär potensering*. Teorin, som ligger till grund för denna metod, är följande. Antag att vi skall beräkna $a^k \bmod m$, då a, k och m är positiva heltal. Vi tänker oss talet k skrivet i binär form: $k = (k_n, k_{n-1}, \ldots, k_1, k_0)_2$, där talen $k_i = 0$ eller 1. Antag t.ex. att $k_i = 1$ för $i = i_1, i_2, \ldots, i_p$. Då är

$$k = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_p},$$

och således

$$a^k = a^{2^{i_1}} \cdot a^{2^{i_2}} \cdots a^{2^{i_p}}.$$

Härav följer med stöd av sats 5.3 (b):

$$a^k \equiv (a^{2^{i_1}} \bmod m) \cdot (a^{2^{i_2}} \bmod m) \cdots (a^{2^{i_p}} \bmod m) \pmod{m}. \tag{5.5}$$

Produkten i högra ledet av (5.5) reduceras slutligen till sin huvudrest modulo m. I vårt numeriska exempel har vi först genom successiva kvadreringar och reduceringar modulo $m = 23$ beräknat huvudresterna för potenserna a, a^2, a^4, ..., a^{2^n} med $a = 35$, varefter vi har multiplicerat huvudresterna för de potenser a^{2^i}, för vilka motsvarande $k_i = 1$, precis såsom formel (5.5) föreskriver.

5.3 Linjära kongruenser

Linjära kongruenser är en motsvarighet till linjära ekvationer. Det är alltså fråga om kongruenser, där vi har en eller flera obekanta i första potens. Den enklaste linjära kongruensen är av formen

$$ax \equiv b \pmod{m}. \tag{5.6}$$

Linjära kongruenser med flera obekanta $x_1, x_2, \ldots, x_n$ är av formen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}. \tag{5.7}$$

Vidare förekommer system av linjära kongruenser, t.ex. av formen

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned} \tag{5.8}$$

Vi kommer i detta och följande avsnitt att behandla kongruenserna (5.6) resp. (5.8).

Betrakta kongruensen (5.6), där vi antar att a, b och m är givna heltal med $m > 0$. Vi söker alla heltalslösningar x, som satisfierar kongruensen. Om x_0 är en partikulär lösning, så är varje heltal x_1 med $x_1 \equiv x_0 \pmod{m}$ även en lösning, eftersom $ax_1 \equiv ax_0 \equiv b \pmod{m}$ enligt kor. 5.3 (b). Hela restklassen $x \equiv x_0 \pmod{m}$ utgör alltså lösningar till kongruensen (5.6). Man frågar sig nu huru många av de m restklasserna modulo m, som utgör lösningar till kongruensen. Vi frågar m.a.o. huru många inkongruenta lösningar modulo m det existerar. Svaret ges av följande sats.

Sats 5.9. *Låt a, b och m vara heltal med $m > 0$. Sätt $d = (a, m)$. Om $d \nmid b$ har kongruensen (5.6) inga lösningar. Om $d \mid b$ har kongruensen exakt d inkongruenta lösningar modulo m. Om x_0 är en partikulär lösning, kan alla lösningar skrivas i formen*

$$x = x_0 + (m/d)t \qquad (t \in Z). \tag{5.9}$$

Bevis: Av sats 5.1 följer att kongruensen (5.6) är ekvivalent med den diofantiska ekvationen

$$ax - my = b. \tag{5.10}$$

Enligt sats 3.14 har ekvationen (5.10) lösningar, om och endast om $d \mid b$. I detta fall har ekvationen oändligt många lösningar (x, y), som kan skrivas i formen (jfr. formel (3.27)):

$$x = x_0 + (m/d)t, \qquad y = y_0 + (a/d)t \qquad (t \in Z),$$

där (x_0, y_0) är en partikulär lösning. Därmed är formel (5.9) ådagalagd. Det återstår nu blott att visa, att exakt d av lösningarna (5.9) är inkongruenta modulo m. Betrakta fördenskull två godtyckliga lösningar

$$x_1 = x_0 + (m/d)t_1 \quad \text{och} \quad x_2 = x_0 + (m/d)t_2.$$

Vi konstaterar att $x_1 \equiv x_2 \pmod{m}$, om och endast om

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}. \tag{5.11}$$

Nu är $(m, m/d) = m/d$, eftersom $(m/d) \mid m$. Enligt sats 5.4 kan kongruensen (5.11) divideras med den gemensamma faktorn m/d, om modulen m samtidigt divideras med m/d. Vi får då

$$t_1 \equiv t_2 \pmod{d}. \tag{5.12}$$

Omvänt inses lätt att (5.11) följer ur (5.12). Två godtyckliga lösningar x_1 och x_2 är således kongruenta modulo m, om och endast om motsvarande t-värden är kongruenta modulo d. Inkongruenta lösningar modulo m alstras alltså, då och endast då t genomlöper ett fullständigt restsystem modulo d. Emedan varje sådant system består av d tal, får vi d inkongruenta lösningar modulo m. □

I det speciella fall att talen a och m i sats 5.9 är relativt prima, varvid $d = 1$, får vi följande korollarium.

Kor. 5.9. *Låt a, b och m vara heltal med $m > 0$. Om a och m är relativt prima, så har kongruensen (5.6) exakt en lösning modulo m, representerande alla tal i en och samma restklass modulo m. Om x_0 är en sådan lösning, kan alla lösningarna skrivas i formen*

$$x = x_0 + mt \qquad (t \in Z). \tag{5.13}$$

Sats 5.9 och dess korollarium ger ingen anvisning om hur man skall finna den partikulära lösningen x_0. Om talen a, b och m är små, sker detta enklast genom prövning. För större tal kan man lämpligen använda den metod, som beskrivits på sid. 23 för diofantiska ekvationer, eftersom kongruensen (5.6) är ekvivalent med den diofantiska ekvationen (5.10).

Låt oss för ett ögonblick betrakta den speciella kongruensen

$$ax \equiv 1 \pmod{m}. \tag{5.14}$$

Av sats 5.9 följer att kongruensen är lösbar, om och endast om $(a, m) = 1$. I detta fall är alla lösningar kongruenta modulo m. En godtycklig lösning till kongruensen (5.14) kallas en *invers till a modulo m* och betecknas $\bar{a}$. Om $\bar{a}$ är en dylik invers, kan således alla lösningar till kongruensen (5.14) skrivas i formen $x \equiv \bar{a} \pmod{m}$. Vi kan utnyttja inversen $\bar{a}$ för att lösa den allmänna kongruensen $ax \equiv b \pmod{m}$ i det fall att $(a, m) = 1$. Multipliceras nämligen sistnämnda kongruens med $\bar{a}$, erhålles $a\bar{a}x \equiv \bar{a}b \pmod{m}$. Nu är emellertid $a\bar{a} \equiv 1 \pmod{m}$, varför vi får $x \equiv \bar{a}b \pmod{m}$. Detta ger den fullständiga lösningen till kongruensen $ax \equiv b \pmod{m}$ i det fall att $(a, m) = 1$.

Exempel 1 Lös kongruensen $9x \equiv 12 \pmod{15}$. Här är $a = 9$, $b = 12$, $m = 15$ och således $d = (9, 15) = 3$. Emedan $3 \mid 12$ är kongruensen lösbar och har 3 inkongruenta lösningar modulo 15. Genom prövning finner man lätt att $x_0 = 3$ är en partikulär lösning. Enligt formel (5.9) ges den allmänna lösningen då av

$$x = 3 + 5t \qquad (t \in Z).$$

Av dessa x-värden är t.ex. $x_0 = 3$, $x_1 = 8$, $x_2 = 13$ inkongruenta modulo 15. Ett fullständigt system av inkongruenta lösningar modulo 15 är alltså: $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$ och $x \equiv 13 \pmod{15}$.

Exempel 2 Lös kongruensen $128x \equiv 833 \pmod{1001}$. Här är $a = 128$, $b = 833$, $m = 1001$. Man ser lätt att $(128, 1001) = 1$. Enligt kor. 5.9 har kongruensen exakt en lösning modulo 1001. Kongruensen är ekvivalent med den diofantiska ekvationen

$$128x - 1001y = 833. \tag{5.15}$$

För att finna en partikulär lösning tillämpar vi Euklides algoritm på talen 1001 och 128. Vi får då

$$\begin{aligned}
1001 &= 7 \cdot 128 + 105 \\
128 &= 1 \cdot 105 + 23 \\
105 &= 4 \cdot 23 + 13 \\
23 &= 1 \cdot 13 + 10 \\
13 &= 1 \cdot 10 + 3 \\
10 &= 3 \cdot 3 + 1 \\
3 &= 3 \cdot 1.
\end{aligned}$$

Vi kan nu framställa talet $1 = (128, 1001)$ som en linjär kombination av 128 och 1001 genom att tillämpa sats 3.7. En annan möjlighet, som ger samma slutresultat, är att "räkna baklänges" i Euklides algoritm ovan på följande sätt:

$$\begin{aligned}
1 &= 10 - 3 \cdot 3 = 10 - 3(13 - 10) = -3 \cdot 13 + 4 \cdot 10 \\
&= -3 \cdot 13 + 4(23 - 13) = 4 \cdot 23 - 7 \cdot 13 \\
&= 4 \cdot 23 - 7(105 - 4 \cdot 23) = -7 \cdot 105 + 32 \cdot 23 \\
&= -7 \cdot 105 + 32(128 - 105) = 32 \cdot 128 - 39 \cdot 105 \\
&= 32 \cdot 128 - 39(1001 - 7 \cdot 128) = -39 \cdot 1001 + 305 \cdot 128.
\end{aligned}$$

Vi har sålunda $305 \cdot 128 - 39 \cdot 1001 = 1$. Multiplikation med 833 ger: $254065 \cdot 128 - 32487 \cdot 1001 = 833$. En partikulär lösning till den diofantiska ekvationen (5.15) är alltså: $x_0 = 254065$, $y_0 = 32487$. Lösningen till den givna kongruensen kan då skrivas i formen $x \equiv 254065 \pmod{1001}$. Utbytes 254065 mot dess huvudrest modulo 1001 fås lösningen i den enklare formen: $x \equiv 812 \pmod{1001}$.

5.4 Kinesiska restteoremet

I gamla kinesiska skrifter kunde man hitta problem av följande typ: Sök ett tal, som dividerat med 3 ger resten 1, dividerat med 5 ger resten 2 och dividerat med 7 ger resten 3. Om vi betecknar talet ifråga med x, får vi följande kongruenser:

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 3 \pmod 7. \tag{5.16}$$

Vi har alltså ett system av kongruenser med olika moduler av den allmänna typen (5.8). Vi skall nu visa att ett dylikt system alltid har en lösning, förutsatt att modulerna är parvis relativt prima. På grund av sitt kinesiska ursprung har denna sats fått namnet

Sats 5.10. (Kinesiska restteoremet). *Kongruenssystemet* (5.8) *har en entydig lösning modulo* $M = m_1 m_2 \cdots m_k$ *under förutsättning att talen* $m_1, m_2, \ldots, m_k$ *är parvis relativt prima.*

Bevis: Sätt $M_i = M/m_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$ $(i = 1, 2, \ldots, k)$. Eftersom m_i är relativt primiskt till vart och ett av talen m_j $(j \neq i)$, är m_i relativt primiskt även till deras produkt M_i (kor. 3.9). Således $(m_i, M_i) = 1$ för $i = 1, 2, \ldots, k$. Då har kongruensen $M_i y_i \equiv 1 \pmod{m_i}$ en entydig lösning y_i modulo m_i (kor. 5.9). Vi bildar nu summan

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k \tag{5.17}$$

och påstår att denna utgör en lösning till kongruenssystemet (5.8). Man har nämligen $m_i \mid M_j$ för $i \neq j$. Detta medför att $M_j \equiv 0 \pmod{m_i}$ för $i \neq j$. I summan (5.17) är alltså alla termer kongruenta med 0 modulo m_i utom termen $a_i M_i y_i$. För denna term gäller kongruensen $a_i M_i y_i \equiv a_i \pmod{m_i}$, emedan $M_i y_i \equiv 1 \pmod{m_i}$. Således är $x \equiv a_i \pmod{m_i}$ för $i = 1, 2, \ldots, k$. Därmed är påvisat att x utgör en lösning till kongruenssystemet (5.8). Det återstår nu att visa att två godtyckliga lösningar x_1 och x_2 är kongruenta modulo M. Ur kongruenserna $x_1 \equiv a_i \pmod{m_i}$ och $x_2 \equiv a_i \pmod{m_i}$ följer $x_1 \equiv x_2 \pmod{m_i}$ för $i = 1, 2, \ldots, k$. Då nu talen m_i är parvis relativt prima, fås härav med stöd av kor. 5.7: $x_1 \equiv x_2 \pmod M$. Två godtyckliga lösningar till systemet (5.8) är alltså kongruenta modulo M. Därmed är satsen bevisad. □

Exempel 1 Som en tillämpning av sats 5.10 skall vi lösa kongruenssystemet (5.16). Eftersom talen 3, 5 och 7 är parvis relativt prima, har systemet en entydig lösning modulo $M = 105 = 3 \cdot 5 \cdot 7$. Sätt $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$ och $M_3 = 105/7 = 15$ i enlighet med beviset ovan. Vi har då att lösa kongruenserna

$$35y_1 \equiv 1 \pmod 3, \qquad 21y_2 \equiv 1 \pmod 5, \qquad 15y_3 \equiv 1 \pmod 7.$$

Dessa är ekvivalenta med de enklare kongruenserna

$$2y_1 \equiv 1 \pmod 3, \qquad y_2 \equiv 1 \pmod 5, \qquad y_3 \equiv 1 \pmod 7, \tag{5.18}$$

som fås då talen 35, 21 och 15 ersättes med sina huvudrester modulo 3, 5 resp. 7. Man ser lätt att kongruenserna (5.18) har lösningarna $y_1 \equiv 2 \pmod 3$, $y_2 \equiv 1 \pmod 5$, $y_3 \equiv 1 \pmod 7$. Insättes dessa y-värden jämte $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $M_1 = 35$, $M_2 = 21$ och $M_3 = 15$ i formel (5.17) fås

$$x = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157.$$

Lösningen till kongruenssystemet (5.16) lyder alltså: $x \equiv 157 \pmod{105}$, vilken lösning även kan skrivas i formen $x \equiv 52 \pmod{105}$.

Det finns även ett annat sätt att lösa kongruenssystem av typ (5.8), såsom vi nu skall visa. Metoden kallas *substitutionsmetoden* och är analog med motsvarande metod vid lösning av vanliga ekvationssystem. Vi tillämpar metoden på kongruenssystemet (5.16), varvid principen torde framgå. Den första kongruensen (5.16) ger $x = 1 + 3t$, där t är ett heltal. Då detta värde på x insättes i den andra kongruensen, fås $1 + 3t \equiv 2 \pmod 5$, som ger $3t \equiv 1 \pmod 5$. Löses nu denna kongruens med avseende på t, erhålles $t \equiv 2 \pmod 5$. Detta innebär att $t = 2 + 5u$, där u är ett heltal. Då vi insätter detta uttryck för t i ekvationen $x = 1 + 3t$, får vi $x = 7 + 15u$. Detta uttryck för x insättes slutligen i den tredje kongruensen (5.16). Man får då (efter en liten hyfsning): $15u \equiv 3 \pmod 7$, som ger lösningen $u \equiv 3 \pmod 7$. Alltså är $u = 3 + 7v$, där v är ett heltal. Insättning i ekvationen $x = 7 + 15u$ ger $x = 52 + 105v$. Detta innebär att $x \equiv 52 \pmod{105}$ är den slutliga lösningen.

Observera! Substitutionsmetoden kan användas för att lösa ett kongruenssystem även i det fall att modulerna inte är parvis relativt prima. Ett kongruenssystem kan nämligen vara lösbart även om villkoret i sats 5.10 inte är uppfyllt. Detta är ju blott ett tillräckligt men ingalunda nödvändigt villkor för att kongruenssystemet (5.8) skall vara lösbart.

Exempel 2 Antag att vi har en fickräknare med 10 siffrors kapacitet i sifferindikatorn (display). (Internt räknar den då med 12–13 siffror). Antag vidare att vi med denna fickräknare önskar multiplicera två positiva heltal a och b, vartdera innehållande högst 9 siffror. Produkten ab innehåller då högst 18 siffror och kan sålunda överstiga fickräknarens kapacitet. Hur skall man förfara för att få fram alla siffrorna i produkten? Metodiken bygger på kinesiska restteoremet. Av detta teorem följer ju, att om man känner huvudresterna för ett obekant tal x modulo talen $m_1, m_2, \ldots, m_k$, vilka antages vara parvis relativt prima, så kan x bestämmas modulo $M = m_1 m_2 \cdots m_k$. Som givna moduler väljer vi nu $m = 2^8 = 256$ och $n = 5^8 = 390625$. Dessa är relativt prima och har produkten $mn = 10^8$. Vi bestämmer nu huvudresterna

$$a_1 = a \bmod m \qquad b_1 = b \bmod m$$
$$a_2 = a \bmod n \qquad b_2 = b \bmod n.$$

Då är $ab \equiv a_1 b_1 \pmod m$ och $ab \equiv a_2 b_2 \pmod n$. Dessa kongruenser består, om vi ersätter talen $a_1 b_1$ och $a_2 b_2$ med deras huvudrester $(a_1 b_1)'$ och $(a_2 b_2)'$ modulo m resp. n. Produkten ab

utgör alltså en lösning till kongruenssystemet

$$\begin{aligned} x &\equiv (a_1 b_1)' \pmod{m} \\ x &\equiv (a_2 b_2)' \pmod{n}. \end{aligned} \tag{5.19}$$

Eftersom lösningarna till detta system är kongruenta modulo 10^8, så finns det en lösning x_0 med $0 \leq x_0 < 10^8$. Denna lösning kan bestämmas med någon av de metoder, som beskrivits i det föregående. (Om fickräknaren är programmerbar, kan lösningsalgoritmen programmeras in på förhand). Om vi nu tänker oss produkten ab skriven i formen $ab = p \cdot 10^8 + q$, så ser vi att $q = x_0$, medan $p = [ab/10^8]$. De 8 sista siffrorna i produkten ab utgöres alltså av lösningen x_0 till kongruenssystemet (5.19), medan de övriga siffrorna bildar heltalsdelen av $ab/10^8$. Emedan denna heltalsdel består av högst 10 siffror, har fickräknaren kapacitet att visa dem alla. Därmed blir talet ab fullständigt bestämt.

Anmärkning. Som den intelligente läsaren måhända har märkt, så kan produkten $a_2 b_2$ i det föregående innehålla upp till 12 siffror, emedan a_2 och b_2 kan vara sexsiffriga tal. Därmed skulle produkten $a_2 b_2$ kunna överstiga fickräknarens sifferindikatorkapacitet. Nu är emellertid $a_2 b_2$ blott ett mellanresultat, som kan lagras direkt i något av fickräknarens minnen, och dessa har i regel den erforderliga kapaciteten. Det kan f.ö. nämnas, att man även i datorer använder metoder, som baserar sig på kinesiska restteoremet, när man har att göra med tal, som normalt överstiger datorns kapacitet.

5.5 Delbarhetstest

Vi skall ägna resten av denna paragraf åt några tillämpningar av kongruenser. I detta avsnitt skall vi först härleda ett par enkla regler, enligt vilka man kan avgöra om ett givet tal är delbart med någon potens av 2 eller 5. Därefter härleder vi regler för delbarhet med 3, 9 och 11. Slutligen skall vi redogöra för det s.k. nioprovet vid multiplikation.

Låt n vara ett positivt heltal, skrivet i decimalform:

$$n = a_p \cdot 10^p + a_{p-1} \cdot 10^{p-1} + \cdots + a_1 \cdot 10 + a_0. \tag{5.20}$$

Emedan $10^k = 2^k \cdot 5^k$ $(k = 1, 2, \ldots)$, så är $10^k \equiv 0 \pmod{2^k}$ och $10^k \equiv 0 \pmod{5^k}$. De termer, vilkas tioexponenter $\geq k$, är alltså alla kongruenta med noll modulo 2^k och 5^k. Härav sluter vi att

$$n \equiv a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \cdots + a_1 \cdot 10 + a_0 \pmod{2^k} \quad \text{och} \quad \pmod{5^k}.$$

Detta ger oss följande delbarhetsregler:

Sats 5.11. *Ett heltal, skrivet i decimalform, är delbart med 2^k eller 5^k, om och endast om det tal, som bildas av dess k sista siffror, är delbart med 2^k resp. 5^k.*

Så är t.ex. talet $n = 32688048$ delbart med $2^4 = 16$, emedan $16 \mid 8048$. Däremot är n inte delbart med $2^5 = 32$, eftersom $32 \nmid 88048$. Likaså är talet $m = 15535375$ delbart med $5^3 = 125$, emedan $125 \mid 375$. Däremot är m inte delbart med $5^4 = 625$, eftersom $625 \nmid 5375$.

Vi övergår till att testa delbarhet med 3 och 9. Fördenskull inför vi polynomet

$$P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0.$$

Enligt (5.20) är $P(10) = n$. Vidare inför vi beteckningen

$$S(n) = a_p + a_{p-1} + \cdots + a_1 + a_0 \tag{5.21}$$

för siffersumman i talet n. Då nu $10 \equiv 1 \pmod 3$ och $\pmod 9$, så sluter vi av sats 5.6: $n = P(10) \equiv P(1) = S(n) \pmod 3$ och $\pmod 9$. Således

$$n \equiv S(n) \pmod 3 \quad \text{och} \quad \pmod 9. \tag{5.22}$$

Detta ger följande delbarhetstest:

Sats 5.12. *Ett heltal n, skrivet i decimalform, är delbart med 3 eller 9, om och endast om dess siffersumma $S(n)$ är delbar med 3 resp. 9.*

Om $S(n)$ inte är ett ensiffrigt tal, kan man bilda siffersummorna $S(S(n))$, $S(S(S(n)))$, o.s.v., tills man får ett ensiffrigt tal. På grund av (5.22) är var och en av dessa siffersummor kongruenta med n modulo 3 och 9. I fortsättningen må $s(n)$ beteckna *den (till ensiffrigt tal) reducerade siffersumman* i talet n. Då är

$$n \equiv s(n) \pmod 3 \quad \text{och} \quad \pmod 9. \tag{5.23}$$

Vi kan sålunda i sats 5.12 byta ut siffersumman $S(n)$ mot den reducerade siffersumman $s(n)$. Ifråga om delbarhet med 11 gäller följande regel:

Sats 5.13. *Ett heltal n av formen (5.20) är delbart med 11, om och endast om dess alternerande siffersumma*

$$\bar{S}(n) = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^p a_p \tag{5.24}$$

är delbar med 11.

Ur kongruensen $10 \equiv -1 \pmod{11}$ följer nämligen $n = P(10) \equiv P(-1) = \bar{S}(n) \pmod{11}$, varav satsen omedelbart framgår.

Antag nu att vi önskar multiplicera två positiva heltal m och n. Enligt (5.23) är $m \equiv s(m)$ och $n \equiv s(n) \pmod 9$. Multiplikation ger:

$$mn \equiv s(m)s(n) \equiv s(s(m)s(n)) \pmod 9.$$

Å andra sidan är $mn \equiv s(mn) \pmod 9$. Således

$$s(mn) \equiv s(s(m)s(n)) \pmod 9.$$

Men eftersom de reducerade siffersummorna är ensiffriga tal, är den sistnämnda kongruensen de facto en likhet. Alltså:

$$s(mn) = s(s(m)s(n)). \tag{5.25}$$

Man kan använda denna likhet för att kontrollera om multiplikationen mn är rätt utförd, såsom följande exempel visar. Antag att $m = 8597$, $n = 637$. Då är $mn = 5476289$. Å andra sidan fås siffersummorna:

$$S(m) = 29, \quad S(S(m)) = 11, \quad s(m) = 2$$
$$S(n) = 16, \quad s(n) = 7$$
$$S(mn) = 41, \quad s(mn) = 5.$$

Om multiplikationen är rätt utförd, skall vi enligt (5.25) ha:

$$5 = s(mn) = s(s(m)s(n)) = s(14) = 5.$$

Likheten (5.25) stämmer alltså i vårt exempel. Därav kan vi emellertid *inte* dra den slutsatsen, att multiplikationen mn är rätt utförd. Det kan ju tänkas att vi vid multiplikationen begått ett fel, som inte ändrar på siffersummorna. Däremot kan vi påstå, att om likheten (5.25) inte stämmer, så är multiplikationen felaktig, förutsatt att siffersummorna uträknats korrekt. Detta sätt att testa en multiplikation kallas *nioprovet.*

5.6 Beräkning av veckodagen för ett givet datum

I detta avsnitt skall vi härleda en formel för bestämning av veckodagen för ett givet datum i vår gregorianska kalender. Denna kalender infördes år 1582 av påven Gregorius XIII genom att man dels ändrade på skottårsregeln, dels hoppade över 10 dagar i almanackan. På den 4 oktober nämnda år följde sålunda den 15 oktober. Orsaken härtill var att den tidigare kalendern, den julianska, som infördes av kejsar Julius Caesar år 46 f.Kr., hade kommit i otakt med årstiderna på grund av att årets längd inte helt stämde överens med jordens omloppstid kring solen. Alla länder accepterade dock inte den nya kalendern med detsamma. Till en början antogs den nya kalendern endast i de katolska länderna, medan de protestantiska stretade emot. Detta ledde dock till trassel och förvirring i de politiska och kommersiella relationerna, varför man i slutet av 1600-talet och i början av 1700-talet övergick till den "nya stilen" i de protestantiska delarna av Tyskland samt i Holland, Danmark och Norge. I Sverige-Finland infördes den gregorianska kalendern så sent som år 1753.

I de grekisk-ortodoxa länderna ställde man sig i det längsta helt avvisande. Sålunda infördes den gregorianska kalendern i Sovjet år 1917, i Jugoslavien och Rumänien år 1919 och i Grekland år 1923. Man måste hålla dylika fakta i minnet, när man anger historiska data.

I den gregorianska kalendern är vart fjärde år skottår utom de jämna sekelår, som inte är delbara med 400. Denna regel infördes för att årets längd i medeltal så nära som möjligt skall överensstämma med jordens omloppstid kring solen, som är $365,_{2422}$ dygn. Under en 400-årsperiod har vi alltså 303 "normala" år och 97 skottår. Detta ger årsmedellängden $365,_{2425}$ dygn. På ca 3300 år uppgår skillnaden till en dag. Därför har man bestämt att år 4840 inte skall vara skottår, fastän talet 4840 är delbart med 4. Den som lever får se!

Efter dessa preludier rörande vår tideräkning skall vi nu ange en metod att bestämma veckodagen för ett godtyckligt datum i den gregorianska kalendern. Veckodagen kommer att anges med ett tal enligt följande kod: söndag = 0, måndag = 1, tisdag = 2, onsdag = 3, torsdag = 4, fredag = 5 och lördag = 6. Den sökta veckodagen betecknas enligt denna kod med talet W. Det är klart att W endast behöver anges modulo 7. Datum, för vilket veckodagen sökes, anges på följande sätt: Årtalet = N, månadens nummer = m och datum i månaden = d. Dessutom skriver vi $N = 100C + Y$, varvid C betecknar århundradet (century) och Y året (year) i århundradet ifråga. Beträffande månadsnumret m skall vi göra följande justering: Eftersom skottdagen infaller i februari, är det av räknetekniska skäl lämpligt att ta mars som utgångspunkt för månadsnumreringen. Månaderna mars – december får dock bibehålla sina vanliga nummer (3 – 12), medan *januari och februari räknas som månad* 13 *resp.* 14 *för föregående år.* T.ex. den 15 februari 1992 anges med $N = 1991$, $m = 14$, $d = 15$.

För att göra räkningarna så enkla som möjligt tar vi den 1 mars år 0 som utgångspunkt. Vi betecknar denna veckodag med d_0 enligt koden ovan. Nu kan man mot detta invända att den gregorianska kalendern inte gällde år 0. Detta spelar emellertid ingen roll. Vi räknar som om kalendern hade gällt från och med år 0 samt bestämmer sedan det värde d_0 då skulle ha haft. Veckodagen den 1 mars år N betecknas d_N. Då ett "normalt" år har 365 dagar och $365 \equiv 1 \pmod 7$, sker en förskjutning ifråga om veckodagen med en dag per år under "vanliga" år och med två dagar per år under skottår. För att beräkna d_N utgående från d_0 måste vi alltså veta huru många skottår (S), som infallit under perioden från år 0 till år N. Som redan nämnts, är i den gregorianska kalendern ett år skottår, om årtalet är delbart med 4, dock med undantag av de jämna sekelår, som inte är delbara med 400. Under tidsperioden $0 - N$ är alltså antalet skottår

$$S = [N/4] - [N/100] + [N/400].$$

Insättes här $N = 100C + Y$, fås efter diverse förenklingar:

$$\begin{aligned} S &= 24C + [C/4] + [Y/4] \\ &\equiv 3C + [C/4] + [Y/4] \pmod 7. \end{aligned} \tag{5.26}$$

Vid dessa förenklingar har vi bl.a. beaktat att

$$[25C + (Y/4)] = 25C + [Y/4]$$
$$[C + (Y/100)] = C$$
$$[(C/4) + (Y/400)] = [C/4].$$

Från den 1 mars år 0 till den 1 mars år N har veckodagen ökat med beloppet $N + S$. Detta ger med beaktande av (5.26):

$$d_N \equiv d_0 + 100C + Y + 3C + [C/4] + [Y/4] \pmod 7 \tag{5.27}$$
$$\equiv d_0 - 2C + Y + [C/4] + [Y/4] \pmod 7.$$

Vi vet att den 1 mars 1991 var en fredag. Således är $d_N = 5$ för $C = 19$, $Y = 91$. Insättes detta i (5.27) fås $d_0 \equiv -74 \equiv 3 \pmod 7$. Den 1 mars år 0 skulle alltså ha varit en onsdag, om den gregorianska kalendern hade gällt då. Således är

$$d_N \equiv 3 - 2C + Y + [C/4] + [Y/4] \pmod 7. \tag{5.28}$$

Nu återstår blott att räkna fram veckodagen utgående från den 1 mars till det givna datumet. Om alla månader vore 28 dagar, skulle ingen förskjutning ifråga om veckodagen ske från månad till månad. Veckodagen d_w för dagen d i en godtycklig månad vore då

$$d_w \equiv d_N + d - 1 \pmod 7. \tag{5.29}$$

Nu är tyvärr inte alla månader 28 dagar, och vi måste därför göra olika tillägg till d_w för olika månader. Genom att successivt addera ihop antalet dagar, som respektive månad överskrider 28, får vi följande tabell över det totala tillägget t_m i månad nummer m:

m:	3	4	5	6	7	8	9	10	11	12	13	14
t_m:	0	3	5	8	10	13	16	18	21	23	26	29

Det skulle nu gälla att hitta en formel, som anger sambandet mellan m och t_m. Emedan funktionen t_m endast antar heltaliga värden, kan man förmoda att heltalsfunktionen $[x]$ skall kunna användas. Genom att pröva sig fram finner man att

$$t_m = [2{,}6(m + 1)] - 10 \tag{5.30}$$

ger just de rätta värdena på t_m. Den sökta veckodagen W är alltså $W = d_w + t_m$. Insättes här värdena (5.29) och (5.30) på d_w och t_m, fås

$$W \equiv d_N + d + 3 + [2{,}6(m + 1)] \pmod 7.$$

Härvid har vi beaktat att $-11 \equiv 3 \pmod 7$. Det återstår nu blott att insätta värdet (5.28) på d_N, varvid vi erhåller *slutresultatet:*

$$W \equiv (d - 1) + [2{,}6(m + 1)] + (Y - 2C) + [Y/4] + [C/4] \pmod 7. \tag{5.31}$$

Som en tillämpning skall vi bestämma veckodagen för den 15 september 1991. Vi har: $d = 15$, $m = 9$, $Y = 91$, $C = 19$. Insättning i (5.31) ger: $W \equiv 119 \equiv 0 \pmod 7$. Den 15 september 1991 är alltså en söndag, vilket torde stämma överens med almanackan. För den 29 februari 1992 har vi: $d = 29$, $m = 14$, $Y = 91$, $C = 19$. Detta ger $W \equiv 146 \equiv 6 \pmod 7$, alltså en lördag.

Övningsuppgifter

Uppgift 5.1 För vilka positiva heltal m gäller följande kongruenser: a) $27 \equiv 5 \pmod{m}$, b) $1000 \equiv 1 \pmod{m}$, c) $1331 \equiv 0 \pmod{m}$.

Uppgift 5.2 Visa att $a \equiv b \pmod{c} \Rightarrow (a,c) = (b,c)$, om a, b och c är hela tal med $c > 0$.

Uppgift 5.3 Vilken slutsats kan man dra av kongruensen $a^2 \equiv b^2 \pmod{p}$, då a och b är heltal och p ett primtal.

Uppgift 5.4 Visa att om $n \equiv 3 \pmod{4}$, så kan n inte vara summan av två heltalskvadrater.

Uppgift 5.5 Bestäm den minsta positiva resten modulo 13 av a) 1000, b) -1000, c) 3757.

Uppgift 5.6 Bestäm den minsta absoluta resten modulo 13 av a) 375, b) -375, c) -6247.

Uppgift 5.7 Bestäm huvudresten modulo 47 av a) 2^{200}, b) 3^{46}.

Uppgift 5.8 Bestäm huvudresten modulo 23 av talet $(233 \cdot 756^{10} - 63)^5$.

Uppgift 5.9 Bestäm de två sista siffrorna i talet $2^5 + 2^{5^2} + 2^{5^3} + \cdots + 2^{5^{1991}}$. (Ledning: Visa först att $2^{5^k} \equiv 32 \pmod{100}$ för alla heltaliga $k \geq 1$). Uppgiften ingick i den nordiska matematiktävlingen för gymnasister i april 1991.

Uppgift 5.10 Lös följande linjära kongruenser: a) $3x \equiv 2 \pmod{7}$, b) $6x \equiv 3 \pmod{9}$.

Uppgift 5.11 Lös kongruenserna: a) $15x \equiv 9 \pmod{25}$, b) $987x \equiv 610 \pmod{1597}$.

Uppgift 5.12 Vilka är inverserna till talen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 modulo 11? Bestäm med stöd härav den minsta absoluta resten modulo 11 av talet 10!.

Uppgift 5.13 Lös kongruenserna: a) $2x + 3y \equiv 1 \pmod{7}$, b) $2x + 4y \equiv 6 \pmod{8}$. (Dessa kongruenser har alltså två obekanta).

Uppgift 5.14 En god 10000 m:s löpare tränar sin specialsträcka på en 400 m:s bana genom att springa 25 varv. Vid starten sätter han igång sitt tidtagarur, som visar minuter och sekunder samt tiondelar av sekunder. När han stannar klockan vid målet, upptäcker han att den har tappat minutvisaren. Sekundvisaren står på 15,0. Vilken är den mest sannolika tiden för loppet, och vilken är den motsvarande varvtiden i medeltal? Det antages härvid att denna varvtid utgör ett helt antal sekunder.

Uppgift 5.15 Lös följande system av linjära kongruenser:
$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$.

Uppgift 5.16 Lös följande system av linjära kongruenser:
$x \equiv 4 \pmod 6$
$x \equiv 13 \pmod{15}$.

Uppgift 5.17 Lös följande system av linjära kongruenser:
$x \equiv 7 \pmod{10}$
$x \equiv 4 \pmod{15}$.

Uppgift 5.18 Lös kongruensen $(x-1)(2x-1) \equiv 0 \pmod 6$.

Uppgift 5.19 Enligt teorin för människans biorytm finns det i människans liv tre olika cykler, den fysiska, den emotionella och den intellektuella cykeln. De tre cyklerna har en period om 23, 28 resp. 33 dagar. Alla tre cyklerna varierar i enlighet med en sinuskurva, som startar vid noll i födelseögonblicket och gör en fullständig svängning under den ifrågavarande cykelns period. Efter en fjärdedels period har kurvan sålunda uppnått sitt maximum. Finns det några ögonblick i en människas liv, då alla tre cyklerna samtidigt a) uppnår sitt maximum, b) passerar noll från minus till plus? Angiv i jakande fall vilka dagar detta inträffar. (Ledning: Använd ett fjärdedels dygn som tidsenhet i moment a) för att alla tider skall bli heltaliga).

Uppgift 5.20 Bestäm den högsta potens av 2, varmed följande tal är delbara: a) 201984, b) 1423408, c) 89375744.

Uppgift 5.21 Bestäm på snabbast möjliga sätt (utan användning av kalkylator) vilka av följande tal, som är delbara med 9: a) 65412351, b) 987654321, c) 78918239735.

Uppgift 5.22 Bestäm på snabbast möjliga sätt (utan användning av kalkylator) vilka av följande tal, som är delbara med 11: a) 10763732, b) 1086320015.

Uppgift 5.23 Härled följande regel för delbarhet med 7, 11 eller 13: Talet delas först i block om tre siffror i varje med början från slutet. De så erhållna tresiffriga talen (det sista kan innehålla färre än tre siffror) förses från slutet räknat med växelvis plus- och minustecken. Om summan av dessa tal (tagna med tecken) är delbar med 7, 11 eller 13, är även det givna talet delbart med 7, 11 resp. 13.

Uppgift 5.24 Är följande multiplikationer korrekt utförda: a) $875961 \cdot 2753 = 24105520633$, b) $24789 \cdot 43717 = 1092700713$. (Kalkylator får ej användas).

Uppgift 5.25 Använd nioprovet för att fylla i den felande siffran, som markerats med ett frågetecken: $89878 \cdot 58965 = 5299?56270$.

Uppgift 5.26 På vilken veckodag infaller den 1 januari år 2000?

Uppgift 5.27 Bestäm på vilken veckodag du själv är född. Vilka av dina födelsedagar till och med den 50:de infaller på denna veckodag?

Uppgift 5.28 I februari 1992 finns det fem lördagar. Under vilka andra år på 1900-talet innehåller februari månad fem lördagar? Lös uppgiften med kongruenser!

Uppgift 5.29 Visa att för veckodagen W i den julianska kalendern gäller:

$$W \equiv (d+4) + [2{,}6(m+1)] + (Y - C) + [Y/4] \pmod 7,$$

då storheterna d, m, Y och C har samma betydelser som i avsnitt 5.6. Härvid får man utnyttja att den 1 mars 1582 var en torsdag enligt den julianska kalendern.

Uppgift 5.30 Det påstås att fredagen den 13:e är en olycksdag. Är det faktiskt så (som endel påstår) att den 13:e i månaden oftare infaller på en fredag än på någon annan veckodag? Om alla veckodagar är lika sannolika, borde ju sannolikheten för att den 13:e i månaden skall vara en fredag vara $= 1/7$. Beräkna den verkliga sannolikheten genom att bestämma veckodagen för den 13:e i varje månad under en 400-årsperiod, t.ex. 1600–1999. (För att lösa denna uppgift bör du helst ha tillgång till en dator eller åtminstone en programmerbar kalkylator).

§ 6. Några speciella kongruenser

6.1 Wilsons sats

I denna paragraf skall vi behandla några speciella kongruenser, vilka uppkallats efter mer eller mindre berömda matematiker. Vi börjar med en sats, som fått sitt namn efter en engelsk matematiker, *John Wilson* (1741–1793), vilken framlade denna sats som en hypotes men aldrig lyckades bevisa den. Satsen bevisades av den franske matematikern *Joseph-Louis Lagrange* år 1770.

Vi inleder med ett förberedande lemma. I avsnitt 5.3 definierade vi en invers till heltalet a modulo m ($m > 0$) som en lösning x till kongruensen $ax \equiv 1 \pmod{m}$, under förutsättning att $(a, m) = 1$. Vi konstaterade då att inversen är entydig modulo m. I det fall att m är ett primtal gäller följande lemma.

Lemma 6.1. *Låt p vara ett primtal. Det positiva heltalet a är sin egen invers modulo p, om och endast om $a \equiv \pm 1 \pmod{p}$.*

Bevis: Om $a \equiv \pm 1 \pmod{p}$, så är $a^2 \equiv 1 \pmod{p}$ enligt sats 5.5. Alltså är a sin egen invers modulo p. Antag nu omvänt att a är sin egen invers. Då är $a^2 \equiv 1 \pmod{p}$, varav fås $p \mid (a-1)(a+1)$. Detta ger $p \mid (a-1)$ eller $p \mid (a+1)$ på grund av kor. 3.8. Men detta är ekvivalent med att $a \equiv \pm 1 \pmod{p}$. □

Sats 6.2. (Wilsons sats). *Om p är ett primtal, så är $(p-1)! \equiv -1 \pmod{p}$.*

Bevis: Satsen gäller uppenbarligen för $p = 2$, ty $1 \equiv -1 \pmod{2}$. Vi kan alltså anta att $p > 2$. Enligt kor. 5.9 har då varje heltal a med $1 \leq a \leq p-1$ en entydig invers $\bar{a}$ modulo p. Inverserna tillhör således mängden $\{1, 2, \ldots, p-1\}$. Två olika $a_1, a_2 \in [1, p-1]$ kan inte ge upphov till samma invers, ty om $a_1\bar{a} \equiv 1$ och $a_2\bar{a} \equiv 1 \pmod{p}$, så är $a_1\bar{a} \equiv a_2\bar{a} \pmod{p}$ och således $a_1 \equiv a_2 \pmod{p}$, vilket är omöjligt. Inverserna omfattar alltså hela mängden $\{1, 2, \ldots, p-1\}$. Enligt lemma 6.1 är talen 1 och $p-1$ de enda i denna mängd, som är sina egna inverser. Alla tal a med $2 \leq a \leq p-2$ har alltså en invers $\bar{a} \neq a$. Vi parar nu ihop varje dylikt a med sin invers $\bar{a}$ och konstaterar med stöd av sats 5.3 att produkten av dessa par är $\equiv 1 \pmod{p}$. Återstår talen 1 och $p-1$. För dessa gäller: $1 \equiv 1$ och $p-1 \equiv -1 \pmod{p}$. Således är $(p-1)! \equiv -1 \pmod{p}$. □

Det visar sig att även omvändningen av Wilsons sats gäller. Man har nämligen

Sats 6.3. *Om för ett positivt heltal n gäller att* $(n-1)! \equiv -1 \pmod{n}$, *så är n ett primtal.*

Bevis: Antag som antites att n är sammansatt, således $n = ab$ med $1 < a < n$ och $1 < b < n$. Satsens antagande ger: $n \mid ((n-1)! + 1)$. Alltså gäller även

$$a \mid ((n-1)! + 1). \tag{a}$$

Vidare gäller: $a \mid (n-1)!$ och $a \nmid 1$, emedan $1 < a < n$. Härur fås enligt sats 1.5: $a \nmid ((n-1)! + 1)$, vilket strider mot (a). Denna motsägelse visar att antitesen är falsk och satsen riktig. □

Av satserna 6.2 och 6.3 följer att n är ett primtal, om och endast om $(n-1)! \equiv -1 \pmod{n}$. Man kan alltså använda denna kongruens för att testa om n är ett primtal. Detta är dock ett mycket opraktiskt primtalstest i det fall att n är stort, eftersom vi har att utföra $n-1$ multiplikationer modulo n. I nästa avsnitt skall vi bekanta oss med en annan typ av primtalstest.

6.2 Fermat's lilla sats

Pierre de Fermat (1601–1665) var en fransk matematiker och jurist, som gett viktiga bidrag till talteorin. Bland de satser, som bär hans namn, skall vi i denna kurs ta upp endast två: "Fermat's lilla sats" och "Fermat's stora sats", av vilka den senare behandlas längre fram. Fermat's lilla sats behandlar kongruenser med primtalsmodul och har på senare tid blivit ett viktigt hjälpmedel i samband med primtalstest. Satsen lyder som följer:

Sats 6.4. (Fermat's lilla sats). *Om p är ett primtal och a ett heltal, som inte är divisibelt med p, så gäller:*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{6.1}$$

Bevis: Antagandet $p \nmid a$ innebär att $(a, p) = 1$, eftersom p är ett primtal. Enligt kor. 5.8 bildar då talen $0 \cdot a,\ 1 \cdot a,\ 2 \cdot a, \ldots,\ (p-1)a$ ett fullständigt restsystem modulo p. På samma sätt bildar talen 0, 1, 2, ..., $p-1$ ett fullständigt restsystem modulo p. Då det första talet är detsamma i bägge systemen, så är talen $1 \cdot a,\ 2 \cdot a, \ldots,\ (p-1)a$ i någon ordning kongruenta modulo p med talen 1, 2, ..., $p-1$. Multipliceras dessa $p-1$ kongruenser med varandra, fås enligt sats 5.3 (b):

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

Nu är $((p-1)!, p) = 1$, varför vi enligt kor. 5.4 kan dividera kongruensen med $(p-1)!$. Vi får då relationen (6.1), och Fermat's lilla sats är bevisad. □

I Fermat's lilla sats krävde vi att $p \nmid a$. Vi kan befria oss från detta antagande genom att modifiera satsen något. Man har nämligen

Sats 6.5. *Om a är ett heltal och p ett primtal, så gäller:*

$$a^p \equiv a \pmod{p}. \tag{6.2}$$

Bevis: Om $p \nmid a$, så följer (6.2) ur (6.1) genom multiplikation med a. Om $p \mid a$, så gäller även $p \mid a^p$. I detta fall är alltså $a \equiv 0$ och $a^p \equiv 0 \pmod{p}$, vilket ger $a^p \equiv a \pmod{p}$. Därmed är satsen bevisad. □

Fermat's lilla sats kan ofta användas för att beräkna minsta positiva resten för uttryck av formen a^k med avseende på en primtalsmodul p. Härvid behöver k ingalunda vara $= p-1$ för att satsen skall kunna användas. De två följande exemplen belyser detta.

Exempel 1 Beräkna 35^{308} mod 23. (Jfr. exempel 2 i avsnitt 5.2). Eftersom 23 är ett primtal och $23 \nmid 35$, så ger Fermat's lilla sats: $35^{22} \equiv 1 \pmod{23}$. Nu "råkar" 308 vara $= 22 \cdot 14$, varför vi får

$$35^{308} = (35^{22})^{14} \equiv 1 \pmod{23}.$$

Alltså: $35^{308} \bmod 23 = 1$. Vi har sålunda nått samma resultat som i exempel 2, avsnitt 5.2, med betydligt färre räkningar.

Exempel 2 Beräkna 17^{345} mod 11. Emedan $345 = 10 \cdot 34 + 5$, får vi med stöd av Fermat's lilla sats samt satserna 5.3 och 5.5:

$$17^{345} = (17^{10})^{34} \cdot 17^5 \equiv 17^5 \equiv 6^5 = 2^5 3^5 = 32 \cdot 243 \equiv 10 \cdot 1 = 10 \pmod{11}.$$

Alltså: $17^{345} \bmod 11 = 10$.

Exempel 2 illustrerar en metod, som alltid kan användas för att beräkna uttryck av typen a^k mod p, förutsatt att a och p uppfyller villkoren i Fermat's lilla sats. Om man nämligen tillämpar divisionsalgoritmen på talen k och $p-1$ och skriver $k = (p-1)q + r$, där $0 \leq r < p-1$, får man enligt Fermat's lilla sats:

$$a^k = (a^{p-1})^q \cdot a^r \equiv a^r \pmod{p}.$$

Om $a > p$, kan detta uttryck ytterligare förenklas genom att man skriver $a = mp+n$, där $0 \leq n < p$, varefter man får $a^r \equiv n^r \pmod{p}$.

Enligt sats 6.5 är $a^n \equiv a \pmod{n}$, om n är ett primtal. Detta betyder att om vi för något heltal a funnit att $a^n \not\equiv a \pmod{n}$, så måste n vara sammansatt. Tyvärr existerar det ingen omvändning av sats 6.5, vilken – om den existerade – skulle kunna fungera som ett utmärkt primtalstest. Visserligen trodde de forna kineserna, att om $2^n - 2$ är delbart med n eller med andra ord om $2^n \equiv 2 \pmod{n}$, så måste n vara ett primtal, men det visade sig vara fel, såsom följande exempel visar. Sätt $n = 341 = 11 \cdot 31$. Då gäller enligt Fermat's lilla sats:

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$$
$$2^{340} = (2^{30})^{11} \cdot 2^{10} \equiv 2^{10} = (2^5)^2 \equiv 1 \pmod{31}.$$

Således: $2^{340} \equiv 1 \pmod{11}$ och $2^{340} \equiv 1 \pmod{31}$. Då talen 11 och 31 är relativt primiska, fås härur med stöd av kor. 5.7: $2^{340} \equiv 1 \pmod{341}$. Multipliceras nu denna kongruens med 2, fås $2^{341} \equiv 2 \pmod{341}$, trots att talet 341 är sammansatt.

Det visar sig dock att det inträffar relativt sällan att $a^n \equiv a \pmod{n}$, när talet n är sammansatt. Om man sålunda för flera heltal a funnit att $a^n \equiv a \pmod{n}$, så är n med relativt stor sannolikhet ett primtal. Man kan alltså använda kongruensen $a^n \equiv a \pmod{n}$ som ett preliminärt primtalstest. Full säkerhet kan givetvis inte nås på detta sätt. Ett sammansatt tal $n > 0$, som satisfierar kongruensen $a^n \equiv a \pmod{n}$ för något heltal $a > 0$, kallas ett *pseudoprimtal till basen a*. Exempelvis är talet 341 ett pseudoprimtal till basen 2, såsom ovan visades. Däremot är 341 inte ett pseudoprimtal till basen 7, ty $7^{341} \not\equiv 7 \pmod{341}$. Man har kunnat visa att det existerar oändligt många pseudoprimtal till varje bas. Det oaktat är antalet pseudoprimtal mycket litet jämfört med antalet primtal inom samma intervall. Exempelvis finns det 455052511 primtal $< 10^{10}$, medan antalet pseudoprimtal till basen 2 inom samma intervall är 14884. Proportionen pseudoprimtal/primtal är alltså i detta fall ca $0,000033$.

Många av de primtalstest, som används för närvarande, har utvecklats ur pseudoprimtalstestet. Låt oss anta att man vill undersöka om ett givet heltal n är primtal. Man utväljer då någon kongruens K_b, som innehåller en parameter b och som är sådan, att om n är sammansatt, så är sannolikheten att n skall satisfiera kongruensen relativt liten. Om n satisfierar kongruensen ifråga, säger vi att n har passerat K_b-testet för parametervärdet b. Ett sådant test är t.ex. *Miller's test*, där sannolikheten för passage $< 1/4$ för varje parametervärde b, när n är sammansatt. Sannolikheten att ett sammansatt tal n skall passera Miller's test för k olika parametervärden, valda på måfå, är då $< (1/4)^k$. Väljer vi t.ex. $k = 100$, får vi en sannolikhet $< 10^{-60}$ för passage. Ett tal n, som passerat alla dessa 100 test, är alltså med en till visshet gränsande sannolikhet ett primtal. Sannolikheten att testet slagit fel (dvs. att n är sammansatt) är knappast större än att datorn, som utfört testet ifråga, begått något räknefel.

6.3 Eulers sats

I detta avsnitt kommer vi att behandla en sats, som kan betraktas som en generalisering av Fermat's lilla sats till det fall då moduln är ett godtyckligt positivt heltal. För detta ändamål måste vi först införa begreppen "Eulers ϕ-funktion" och "reducerat restsystem modulo n".

I det följande må n beteckna ett positivt heltal. Antalet positiva heltal $\leq n$, som är relativt primiska till n, betecknas $\phi(n)$. Funktionen ϕ kallas *Eulers ϕ-funktion.* T.ex. för $n = 15$ är $\phi(15) = 8$, ty det finns 8 positiva heltal ≤ 15, som är relativt primiska till 15, nämligen talen 1, 2, 4, 7, 8, 11, 13 och 14. Speciellt gäller att $\phi(1) = 1$, ty talet 1 är relativt primiskt till sig självt, emedan $(1,1) = 1$. Vi kommer i nästa avsnitt att härleda en formel för $\phi(n)$ utgående från n:s uppdelning i primfaktorer.

Definition: Med ett *reducerat restsystem modulo n* avses en mängd av $\phi(n)$ heltal, som är relativt primiska till n och som är sinsemellan inkongruenta modulo n.

Exempelvis bildar talen 1, 2, 4, 7, 8, 11, 13 och 14 ett reducerat restsystem modulo 15. Likaså bildar talen 1, 8, -11, -16, 17, -23, 26 och 28 ett reducerat restsystem modulo 15. Man kan säga att ett reducerat restsystem modulo n utgör den delmängd av ett fullständigt restsystem modulo n, som består av tal relativt primiska till n. Ett annat sätt att karakterisera ett reducerat restsystem modulo n är följande. Talen i en och samma restklass modulo n är av formen $an+b$, där a genomlöper alla heltal och där b är ett fixt heltal (jfr. avsnitt 5.2). Eftersom $(an + b, n) = (b, n)$ (sats 3.4), så är restklassens tal relativt primiska till n, om och endast om b och n är relativt primiska. En restklass, vars alla tal är relativt primiska till n, kallas en *primitiv restklass modulo n.* Det finns alltså $\phi(n)$ primitiva restklasser modulo n. Ett reducerat restsystem modulo n innehåller sålunda exakt en representant för var och en av dessa $\phi(n)$ restklasser.

Sats 6.6. *Om talen $r_1, r_2, \ldots, r_{\phi(n)}$ bildar ett reducerat restsystem modulo n och om heltalet a är relativt primiskt till n, så bildar även talen $ar_1, ar_2, \ldots, ar_{\phi(n)}$ ett reducerat restsystem modulo n.*

Bevis: Talet n är relativt primiskt till såväl a som r_i för $i = 1, 2, \ldots, \phi(n)$. Således är n relativt primiskt till ar_i (kor. 3.9). Återstår att visa att talen ar_i är parvis inkongruenta modulo n. Vore $ar_h \equiv ar_k \pmod{n}$ för något indexpar (h, k) med $h \neq k$, så kunde kongruensen divideras med a, eftersom $(a, n) = 1$ (kor. 5.4). Vi skulle då få $r_h \equiv r_k \pmod{n}$, vilket strider mot att talen r_i är parvis inkongruenta modulo n. Således är talen ar_i $(i = 1, 2, \ldots, \phi(n))$ parvis inkongruenta modulo n. □

Som en tillämpning av sats 6.6 finner vi t.ex. att talen 4, 8, 16, 28, 32, 44, 52 och 56 bildar ett reducerat restsystem modulo 15, eftersom de erhållits ur talen 1, 2, 4, 7, 8, 11, 13 och 14 genom multiplikation med 4, som är relativt primiskt till 15.

Vi är nu i stånd att bevisa den redan aviserade generaliseringen av Fermat's lilla sats. Den härrör från *Leonard Euler* (1707–1783), en schweizisk matematiker, som verkade en stor del av sitt liv i S:t Petersburg.

Sats 6.7. (Eulers sats). *Låt a vara ett heltal och n ett positivt heltal, som är relativt primiskt till a. Då gäller:*

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{6.3}$$

Bevis: Må $r_1, r_2, \ldots, r_{\phi(n)}$ vara det reducerade restsystem modulo n, som består av alla positiva heltal $\leq n$, vilka är relativt primiska till n. Då bildar även talen $ar_1, ar_2, \ldots, ar_{\phi(n)}$ ett reducerat restsystem modulo n (sats 6.6). Således är talen i det förstnämnda systemet i någon ordning kongruenta med talen i det senare systemet. Multipliceras dessa $\phi(n)$ kongruenser med varandra, fås

$$r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \pmod{n}. \tag{a}$$

Då n är relativt primiskt till vart och ett av talen $r_1, r_2, \ldots, r_{\phi(n)}$, är n även relativt primiskt till deras produkt (kor. 3.9). Alltså får kongruensen (a) enligt kor. 5.4 divideras med denna produkt. Detta ger (6.3), och Eulers sats är bevisad. □

I det fall att n är ett primtal p, är $\phi(p) = p - 1$. Eulers sats ger då $a^{p-1} \equiv 1 \pmod{p}$, varav framgår att Eulers sats är en generalisering av Fermat's lilla sats.

Vi kan utnyttja Eulers sats till att bestämma inversen modulo n till ett givet heltal a, som är relativt primiskt till n. Eftersom $a \cdot a^{\phi(n)-1} = a^{\phi(n)} \equiv 1 \pmod{n}$, så är

$$\bar{a} = a^{\phi(n)-1} \tag{6.4}$$

uppenbarligen en invers till a modulo n. Inversen är som bekant entydigt bestämd modulo n. Med hjälp av inversen kan vi även lösa den linjära kongruensen $ax \equiv b \pmod{n}$, när a och n är relativt prima. Hur detta sker visades redan i avsnitt 5.3. Vi fann då att $x \equiv \bar{a}b \pmod{n}$ ger den fullständiga lösningen till kongruensen. Insättes nu värdet (6.4) på $\bar{a}$, fås

$$x \equiv a^{\phi(n)-1} b \pmod{n}. \tag{6.5}$$

Denna lösning förutsätter dock att man kan beräkna $\phi(n)$ för givet n. Hur detta sker, skall visas i följande avsnitt.

6.4 Eulers ϕ-funktion

I detta avsnitt skall vi härleda en formel för beräkning av $\phi(n)$ utgående från n:s primfaktoruppdelning. För detta ändamål behöver vi en sats, som utsäger att ϕ är en s.k. multiplikativ funktion.

Sats 6.8. *Låt m och n vara positiva heltal, som är relativt prima. Då gäller:* $\phi(mn) = \phi(m)\phi(n)$.

Bevis: Satsen utsäger att antalet primitiva restklasser modulo mn utgör produkten av antalet primitiva restklasser modulo m resp. n, när $(m,n) = 1$. Ett heltal a tillhör en primitiv restklass modulo mn, om och endast om det tillhör en primitiv restklass modulo m och en primitiv restklass modulo n. Detta följer av ekvivalensen

$$(a, mn) = 1 \iff (a, m) = 1 \wedge (a, n) = 1,$$

i vilken implikationen $\Rightarrow$ är trivial, medan omvändningen följer av kor. 3.9. De tal, som samtidigt tillhör en godtycklig (ej nödvändigtvis primitiv) restklass modulo m och en godtycklig restklass modulo n, bildar enligt kinesiska restteoremet en restklass modulo mn, eftersom $(m,n) = 1$. Då nu var och en av de $\phi(m)$ primitiva restklasserna modulo m kombineras med var och en av de $\phi(n)$ primitiva restklasserna modulo n, får vi $\phi(m)\phi(n)$ primitiva restklasser modulo mn. Å andra sidan är detta antal $= \phi(mn)$. Alltså: $\phi(mn) = \phi(m)\phi(n)$. □

Kor. 6.8. *Om de positiva heltalen m_1, m_2, ..., m_k är parvis relativt prima, så gäller:*

$$\phi(m_1 m_2 \cdots m_k) = \phi(m_1)\phi(m_2)\cdots\phi(m_k). \tag{6.6}$$

Bevis: Vi bevisar satsen med fullständig induktion. Satsen är trivial i fallet $k = 1$. Antag nu att satsen gäller för en produkt av $k-1$ faktorer m_i. Vi skriver då produkten $m_1 m_2 \cdots m_k$ i formen $m_1(m_2 m_3 \cdots m_k)$ och konstaterar att m_1 är relativt primiskt till produkten $m_2 m_3 \cdots m_k$, emedan m_1 är relativt primiskt till var och en av produktens faktorer (kor. 3.9). Enligt sats 6.8 gäller då:

$$\phi(m_1 m_2 \cdots m_k) = \phi(m_1)\phi(m_2 m_3 \cdots m_k). \tag{a}$$

Den senare faktorn i högra ledet kan emellertid enligt induktionsantagandet skrivas i formen

$$\phi(m_2 m_3 \cdots m_k) = \phi(m_2)\phi(m_3)\cdots\phi(m_k). \tag{b}$$

Då vi kombinerar (a) och (b), får vi (6.6). Induktionsprincipen visar att (6.6) gäller för varje värde på $k \in Z_+$. □

Vi skall nu bestämma värdet av $\phi(p^a)$, då p är ett primtal och a ett positivt heltal. Vi skall m.a.o. bestämma hur många av talen 1, 2, 3, ..., p^a, som är relativt primiska till p^a. Av dessa p^a tal

är endast talen p, $2p$, $3p$, ..., $p^{a-1}p$ delbara med p, dvs. p^{a-1} stycken. De återstående $p^a - p^{a-1}$ talen är relativt primiska till p och därmed även till p^a. Således är

$$\phi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p}). \tag{6.7}$$

Vi är nu i stånd att härleda den aviserade formeln för $\phi(n)$, då n är ett godtyckligt positivt heltal. Vi kan härvid anta att $n > 1$. (Tidigare har ju konstaterats att $\phi(1) = 1$). Talet n må ha primfaktoriseringen

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \tag{6.8}$$

Talen $p_1^{a_1}$, $p_2^{a_2}$, ..., $p_k^{a_k}$ är parvis relativt prima. Kor. 6.8 ger då:

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}),$$

vilket enligt (6.7) kan skrivas i formen

$$\phi(n) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Med beaktande av (6.8) får vi alltså *slutresultatet:*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{6.9}$$

Som en tillämpning skall vi beräkna $\phi(360)$. Eftersom $360 = 2^3 3^2 5$, får vi

$$\phi(360) = 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 96.$$

Det finns alltså 96 positiva heltal ≤ 360, som är relativt primiska till 360. Ett annat sätt att uttrycka saken: Det finns 96 oförkortbara, egentliga bråk med nämnaren 360. (Ett bråk p/q säges som bekant vara egentligt om $0 < p/q < 1$).

Antalet positiva divisorer till det positiva heltalet n har i avsnitt 3.3 betecknats med $\tau(n)$ (se formel 3.14). Om dessa divisorer är d_1, d_2, ..., $d_{\tau(n)}$, så gäller följande samband:

$$n = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_{\tau(n)}). \tag{6.10}$$

Bevis: För varje heltal m med $1 \leq m \leq n$ är (m, n) en positiv divisor i talet n. Låt nu d vara en godtycklig positiv divisor i talet n. Vi säger då att talet m, där $1 \leq m \leq n$, tillhör klassen C_d, om $(m, n) = d$. När d genomlöper divisorerna d_1, d_2, ..., $d_{\tau(n)}$, blir på detta sätt alla heltal från 1 till n indelade i $\tau(n)$ disjunkta klasser. Av sats 3.4 följer att $m \in C_d$, om och endast om $(m/d, n/d) = 1$. Talen i klassen C_d är alltså alla tal av formen kd $(1 \leq k \leq n/d)$, för vilka k är relativt primiskt till n/d. Deras antal är $\phi(n/d)$. Eftersom totalantalet element i de $\tau(n)$ klasserna är $= n$, fås

$$n = \phi(n/d_1) + \phi(n/d_2) + \cdots + \phi(n/d_{\tau(n)}).$$

Nu är emellertid talen $n/d_1, n/d_2, \ldots, n/d_{\tau(n)}$ precis de $\tau(n)$ divisorerna $d_1, d_2, \ldots, d_{\tau(n)}$, tagna i annan ordningsföljd. Således gäller (6.10). □

Vi testar formel (6.10) på fallet $n = 24$. Talet 24 har 8 positiva divisorer, nämligen 1, 2, 3, 4, 6, 8, 12 och 24. Man finner lätt (t.ex. med stöd av formel (6.9)) att $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(6) = 2$, $\phi(8) = 4$, $\phi(12) = 4$, $\phi(24) = 8$. Summan av dessa tal är 24, precis såsom formel (6.10) föreskriver.

6.5 Perfekta tal och Mersennes tal

Betrakta ett givet heltal $n > 1$ och antag att n har primfaktoriseringen (6.8). Vi skall först härleda en formel för summan av de positiva divisorerna i n. Dessa divisorer är av formen (se avsnitt 3.3)

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{6.11}$$

där heltalen α_κ uppfyller olikheterna $0 \leq \alpha_\kappa \leq a_\kappa$ $(\kappa = 1, 2, \ldots, k)$. Vi bildar nu produkten

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{a_k}) \tag{6.12}$$

och konstaterar att man vid hopmultiplikation av parenteserna får en summa av termer bestående av alla tal av formen (6.11). Produkten (6.12) representerar alltså summan av de positiva divisorerna i talet n. Om vi betecknar denna summa med $\sigma(n)$ och uttrycker parenteserna i (6.12) med hjälp av summaformeln för en ändlig geometrisk serie, får vi följande uttryck för $\sigma(n)$:

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}. \tag{6.13}$$

Definition Talet n säges vara *perfekt*, om $\sigma(n) = 2n$.

Talet n är alltså perfekt, om summan de positiva divisorer i n, vilka är $< n$, är lika med talet självt. Perfekta tal är t.ex. 6, 28 och 496. Alla kända perfekta tal är jämna. Man har alltså inte kunnat finna ett enda udda perfekt tal, och frågan om deras existens är tillsvidare helt olöst. För jämna perfekta tal gäller bl.a. följande sats, som återfinnes i Euklides Elementa (bok IX):

Sats 6.9. *Om $2^m - 1$ är ett primtal, så är $n = 2^{m-1}(2^m - 1)$ ett perfekt tal.*

Bevis: Av antagandet följer, att $2^{m-1}(2^m - 1)$ är primfaktoriseringen av talet n. Således gäller enligt (6.13):

$$\sigma(n) = \frac{2^m - 1}{2 - 1} \cdot \frac{(2^m - 1)^2 - 1}{(2^m - 1) - 1} = (2^m - 1)[(2^m - 1) + 1] = 2n. \square$$

Omvänt gäller att varje jämnt perfekt tal måste ha den i sats 6.9 angivna formen. Detta bevisades av Euler. För att finna perfekta tal kan man alltså söka primtal av formen $2^m - 1$. Om $2^m - 1$ är ett primtal, så är även m ett primtal (övningsuppgift 2.5). Omvändningen gäller däremot ej: Det finns sammansatta tal av formen $2^m - 1$, där m är ett primtal. Ett sådant tal är t.ex. $2^{11} - 1 = 2047 = 23 \cdot 89$. Tal av formen $M_m = 2^m - 1$ kallas *Mersennes tal* efter en fransk munk, *Marin Mersenne*, som levde på 1600-talet. Om $M_p = 2^p - 1$ är ett primtal, talar man om ett *Mersennes primtal.* Det för närvarande (mars 1992) *största kända primtalet* är av Mersenne-typ, nämligen talet $2^{756839} - 1$, som har 227832 siffror.

Övningsuppgifter

Uppgift 6.1 Bestäm huvudresten modulo 13 för talet 25!/13! med tillhjälp av Wilsons sats.

Uppgift 6.2 Låt p vara ett primtal och k ett heltal med $0 < k < p$. Visa med stöd av Wilsons sats att $(k-1)!(p-k)! \equiv (-1)^k \pmod{p}$.

Uppgift 6.3 Bestäm $2^{1000000} \bmod 13$.

Uppgift 6.4 Bestäm den sista siffran i talet 3^{100}, skrivet i 7-systemet.

Uppgift 6.5 Låt p och q vara två olika primtal. Visa att $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Uppgift 6.6 Visa att talet 341 inte är ett pseudoprimtal till basen 7.

Uppgift 6.7 Visa att talet $161038 = 2 \cdot 73 \cdot 1103$ är ett pseudoprimtal till basen 2. (Nämnda tal är det minsta jämna pseudoprimtalet till basen 2).

Uppgift 6.8 Vilken är den sista siffran i talet 7^{1000}?

Uppgift 6.9 Visa att om a är ett heltal, relativt primiskt till 63, så gäller: $a^6 \equiv 1 \pmod{63}$.

Uppgift 6.10 Bestäm $3^{100000} \bmod 35$.

Uppgift 6.11 Bestäm alla positiva heltal n, för vilka gäller: a) $\phi(n) = 6$, b) $\phi(n) = 14$.

Uppgift 6.12 Visa att om m och n är positiva heltal med egenskapen $m \mid n$, så gäller: $\phi(m) \mid \phi(n)$.

Uppgift 6.13 Visa att ett positivt heltal n är sammansatt, om och endast om $\phi(n) \leq n - \sqrt{n}$.

Uppgift 6.14 Bevisa att summan av inversa värdena till divisorerna i ett perfekt tal är $= 2$.

§ 7. En tillämpning på kryptografi

7.1 Allmänt om kryptografi

Kryptografin (eller kryptologin) kan sägas vara läran om hur man "förvanskar" (krypterar) meddelanden, så att obehöriga inte skall kunna ta del av dem. Mottagaren av ett krypterat meddelande bör känna till krypteringsmetoden, så att han kan återställa (dekryptera) meddelandet i dess ursprungliga form. Behovet av krypteringsmetoder har ökat kraftigt på senare tid, när elektroniska kommunikationssystem vunnit allt större spridning. För att säkerställa sekretessen är man ofta tvungen att sända meddelanden i krypterad form.

Ett konventionellt kryptosystem består i regel av en *krypteringsfunktion* E_K, med vars hjälp man krypterar ett meddelande M (även kallad *klartext*) till en *kryptotext* $C = E_K(M)$. Här betecknar K den hemliga *nyckeln*, med vilken man konstruerar krypteringsfunktionen E_K. Kryptotexten kan nu sändas via en oskyddad kanal till mottagaren, som dekrypterar texten med en *dekrypteringsfunktion* D_K, vilken är invers till E_K. Härvid återfås klartexten $M = D_K(C) = D_K(E_K(M))$. Då någon utomstående med andra metoder försöker återvinna klartexten, talar man om *forcering*. För att ett dylikt kryptosystem skall fungera, måste bägge kommunikanterna (avsändare och mottagare) ha tillgång till den hemliga nyckeln K. Denna måste alltså meddelas i förväg via någon skyddad kanal. Detta innebär emellertid en olägenhet, eftersom även en skyddad kanal löper risk att bli "avlyssnad". Dessutom kan det medföra svårigheter att snabbt ändra nyckeln (t.ex. om krypteringsmetoden blivit avslöjad), emedan bägge kommunikanterna måste komma överens om nyckeln.

För att råda bot på dylika olägenheter presenterade *Diffie* och *Hellman* [6] år 1976 idén till en helt ny typ av kryptosystem, s.k. *offentliga kryptosystem* (Public-Key Cryptosystem). Idén är mycket enkel. Krypteringsfunktionen E skall bero av en hemlig parameter P, sådan att dekrypteringsfunktionen $D = E^{-1}$ är lätt att bestämma, då man känner P, men medför oöverstigliga svårigheter, om man inte känner P. Den som önskar ta emot krypterade meddelanden kan då öppet publicera krypteringsfunktionen E för alla tänkbara avsändare, medan han behåller den hemliga parametern P för sig själv. En sådan krypteringsfunktion E kallas även en *falluckefunktion* (trap door function). Vi skall i denna paragraf redogöra för ett dylikt offentligt kryptosystem, som vunnit stor spridning på senare tid. Offentliga kryptosystem behandlas utförligt i en nyutkommen bok av *Arto Salomaa* [7].

7.2 RSA-systemet

År 1978 publicerade *Rivest, Shamir* och *Adleman* [8] ett offentligt kryptosystem, som sedermera fått namnet *RSA-systemet.* I detta system utgår man från två mycket stora primtal p och q samt sätter $n = pq$. Då är $\phi(n) = (p-1)(q-1)$ enligt formel (6.9). Välj nu ett positivt heltal e, sådant att $(e, \phi(n)) = 1$, och bestäm därefter en invers d till e modulo $\phi(n)$. Talet d skall m.a.o. satisfiera kongruensen

$$ed \equiv 1 \pmod{\phi(n)}. \tag{7.1}$$

Existensen av ett dylikt tal d garanteras av kor. 5.9, då e och $\phi(n)$ är relativt primiska. Låt vidare a vara ett heltal i intervallet $[0, n-1]$. Sätt

$$b = a^e \bmod n. \tag{7.2}$$

Vi påstår nu att $a = b^d \bmod n$. Detta är innehållet i följande sats.

Sats 7.1. *Låt a, d, e och n ha samma betydelser som ovan. Då gäller: Om $b = a^e \bmod n$, så är*

$$a = b^d \bmod n. \tag{7.3}$$

Bevis: Då $ed \equiv 1 \pmod{\phi(n)}$, så existerar ett heltal k med egenskapen att $ed = 1 + k\phi(n)$. Antag först att a och n är relativt prima. Då är

$$b^d \equiv (a^e)^d = a^{ed} = a^{1+k\phi(n)} = a(a^{\phi(n)})^k \pmod{n}.$$

Nu är emellertid $a^{\phi(n)} \equiv 1 \pmod{n}$ enligt Eulers sats, varför vi får $b^d \equiv a \pmod{n}$. Således gäller (7.3), eftersom talet a ligger i intervallet $[0, n-1]$. Om a och n inte är relativt prima, så är a delbart med antingen p eller q (men ej med vardera). Antag t.ex. att $p \mid a$. Fermat's lilla sats ger då: $a^{q-1} \equiv 1 \pmod{q}$. Upphöjning till potensen $k(p-1)$ ger $a^{k\phi(n)} \equiv 1 \pmod{q}$ eller m.a.o. $a^{ed-1} \equiv 1 \pmod{q}$, varur fås $a^{ed} \equiv a \pmod{q}$. Å andra sidan är $a^{ed} \equiv a \pmod{p}$, eftersom p delar a och därmed även a^{ed}. Kor. 5.7 ger nu att $a^{ed} \equiv a \pmod{n}$, då ju p och q är relativt prima. Men detta innebär att $b^d \equiv a \pmod{n}$. Därmed är satsen bevisad. □

Ovanstående teori kan nu användas inom kryptografin på följande sätt. Antag att en person önskar ta emot krypterade meddelanden i form av heltal. (Hur man förvandlar vanlig text till heltal visas senare). Han väljer då två mycket stora primtal p och q samt bestämmer talen n, e och d som ovan samt publicerar talen n och e. Däremot hemlighåller han talet d. Var och en som önskar sända honom ett meddelande i form av ett heltal $a \in [0, n-1]$ kan nu kryptera a genom ekvationen (7.2). Talet b representerar alltså kryptotexten. Mottagaren dekrypterar slutligen talet b

genom ekvationen (7.3). Talen e och d kallas fördenskull *krypterings-* resp. *dekrypteringsexponenter.* Talet n kallas *krypteringsmodul.*

Att denna metod fungerar så väl, beror på att den som önskar dekryptera talet b, måste känna till dekrypteringsexponenten d. Men d kan endast beräknas med stöd av (7.1), om man känner $\phi(n)$, vilket i sin tur förutsätter kännedom om talen p och q. För att forcera systemet måste man alltså finna primfaktorerna p och q i talet n, vilket är praktiskt taget omöjligt, om p och q är mycket stora tal (exempelvis av storleksordningen 10^{100}). Den öppna nyckeln utgöres alltså av paret (n, e), medan den hemliga parametern kan sägas vara något av talen p, q, $\phi(n)$ eller d. Om man känner något av talen p, q eller $\phi(n)$, så kan d lätt beräknas, varvid dekrypteringsfunktionen blir bekant.

7.3 Ett exempel på kryptering enligt RSA-metoden

Vi skall nu med ett enkelt exempel visa hur man i praktiken kan kryptera enligt RSA-metoden. Eftersom klartexten i regel är skriven med vanliga bokstäver, måste dessa först transformeras till hela tal. Man kan t.ex. låta bokstäverna A – Ö i det svenska alfabetet motsvara talen 1 – 28 enligt följande tabell:

(7.4)

A	01	H	08	O	15	V	22
B	02	I	09	P	16	X	23
C	03	J	10	Q	17	Y	24
D	04	K	11	R	18	Z	25
E	05	L	12	S	19	Å	26
F	06	M	13	T	20	Ä	27
G	07	N	14	U	21	Ö	28

Vi väljer nu $p = 5$, $q = 11$, vilket ger $n = 55$, $\phi(n) = 40$. (Vi har här valt små värden på p och q för att underlätta räkningarna). Följande steg består i att välja en lämplig krypteringsexponent e, sådan att $(e, 40) = 1$. Självfallet måste $e = 1$ uteslutas, eftersom detta värde skulle ge en kryptotext, som är identisk med klartexten. Vi kan t.ex. välja $e = 7$. Därefter har vi att bestämma dekrypteringsexponenten d, så att $7d \equiv 1 \pmod{40}$. Denna kongruens är ekvivalent med den diofantiska ekvationen $7d - 40y = 1$, där d och y är obekanta. Denna ekvation kan t.ex. lösas med metodiken i avsnitt 3.4. Man finner att $d = 23 + 40t$ $(t \in Z)$. Vi väljer lämpligen det minsta positiva värdet på d, dvs. $d = 23$. Krypteringen och dekrypteringen sker alltså enligt ekvationerna

$$b = a^7 \bmod 55 \qquad \text{resp.} \qquad a = b^{23} \bmod 55.$$

Härvid ligger heltalen a och b i intervallet $[0, 54]$. Antag t.ex. att vi skall kryptera budskapet

SÄND MERA PENGAR

Vi kan då kryptera bokstav för bokstav, sedan bokstäverna översatts till tal enligt tabell (7.4). Denna översättning ger talserien

(a) 19 27 14 04 13 05 18 01 16 05 14 07 01 18

(Mellanrummen mellan orden har utelämnats, eftersom budskapet är begripligt även utan dessa mellanrum). Vi har nu att beräkna $b = a^7 \bmod 55$ för $a = 19, 27, 14, 4, \ldots$. Härvid kan man lämpligen utnyttja metoden för modulär potensering, som beskrivits i exempel 2 i avsnitt 5.2. Sedan dessa räkningar utförts, får man talserien

(b) 24 03 09 49 07 25 17 01 36 25 09 28 01 17

Denna talserie representerar alltså vår kryptotext. Beräkningen av $a^7 \bmod 55$ är naturligtvis något besvärlig, om räkningarna utföres för hand. Med en programmerbar fickräknare eller dator kan räkningarna givetvis utföras mycket snabbare. Den som skall dekryptera talserien (b) har nu att beräkna $a = b^{23} \bmod 55$ för $b = 24, 3, 9, 49, \ldots$. Då återfår man talserien (a), som i sin tur översätts till bokstäver med hjälp av tabell (7.4). Därmed är budskapet klarlagt.

Väljer man något större värden på p och q, kan även a och b ha större värden. T.ex. om $p = 47$, $q = 61$ och således $n = 2867$, så skall a och b ligga i intervallet $[0, 2866]$. I detta fall kan man sammanföra bokstäverna i klartexten två och två och låta varje bokstavspar bilda ett fyrsiffrigt tal. Eftersom det största av dessa tal = 2828 (svarande mot bokstavsparet ÖÖ), så ligger dessa fyrsiffriga tal i det föreskrivna intervallet. Budskapet SÄND MERA PENGAR skrivs nu som SÄ ND ME RA PE NG AR, vilket ger talserien

1927 1404 1305 1801 1605 1407 0118

Skulle antalet bokstäver i klartexten vara udda, kan det sista fyrsiffriga talet lämpligen fyllas ut med 00. Vi har visserligen nu fått större tal att operera med men i gengäld endast hälften så många.

Som redan nämnts, måste talen p och q väljas mycket stora vid verklig kryptering för att motstå forcering. Då uppstår problemet att finna tillräckligt stora primtal. Det lönar sig inte att ta p och q ur någon primtalstabell, eftersom dessa tabeller inte sträcker sig tillräckligt långt i heltalsserien. I stället väljer man på måfå något stort udda tal (kanske 100-siffrigt) och testar dess primalitet med något lämpligt primtalstest, t.ex. av den typ som omnämnts i slutet av avsnitt 6.2. Man kan tämligen lätt visa, att sannolikheten att ett på måfå valt 100-siffrigt, udda tal skall vara ett primtal är approximativt 0,00868. Om man undersöker 80 sådana tal, har man mer än 50% chans att påträffa ett primtal. Dylika undersökningar måste givetvis utföras med dator.

7.4 Signerade budskap

Antag att A skall sända ett meddelande M till B i krypterad form enligt RSA-metoden. B har då publicerat sin krypteringsfunktion E_B med krypteringsmoduln n_B och krypteringsexponenten e_B. Eftersom dessa parametrar är allmänt bekanta, kan vem som helst sända ett meddelande till B och härvid uppge sig vara A. Detta är självfallet inte önskvärt. För att undvika denna olägenhet kan man förfara på följande sätt. A och B förser sig med var sin krypteringsmodul n_A resp. n_B ($n_A < n_B$) med krypteringsexponenterna e_A resp. e_B. Dessa kan publiceras. Däremot hemlighåller A och B sina dekrypteringsexponenter d_A resp. d_B. Avsändaren A *dekrypterar* nu budskapet M med sin egen dekrypteringsfunktion D_A och bildar den *signerade texten*

$$S = D_A(M) = M^{d_A} \bmod n_A.$$

Därefter *krypterar* han texten S med B:s krypteringsfunktion E_B (som ju är bekant), varefter han till B översänder kryptotexten

$$C = E_B(S) = S^{e_B} \bmod n_B.$$

Mottagaren B dekrypterar först texten C med användning av sin egen dekrypteringsfunktion D_B, varvid han får den signerade texten

$$D_B(C) = D_B(E_B(S)) = S.$$

Därefter opererar han med A:s krypteringsfunktion E_A på S och får klartexten

$$E_A(S) = E_A(D_A(M)) = M.$$

Kombinationen av klartexten M och den signerade texten S övertygar nu B om att A är den rätte avsändaren. Ingen annan än A skulle nämligen ha kunnat bilda den signerade texten S utgående från budskapet M, eftersom endast A är i besittning av dekrypteringsfunktionen D_A.

Övningsuppgifter

Uppgift 7.1 Kryptera budskapet KOM HEM med RSA-metoden, då $n = 55$, $e = 7$. (För bokstavstransformationen användes tabell (7.4)).

Uppgift 7.2 Vid en kryptering enligt RSA-metoden med $n = 55$, $e = 7$ har man fått kryptotexten 02 10 03 23 36. Dekryptera budskapet och bestäm klartexten. (Bokstäverna transformeras med tabell (7.4)).

Uppgift 7.3 Visa att krypterings- och dekrypteringsexponenterna sammanfaller, om man i RSA-systemet använder krypteringsmoduln 35.

Uppgift 7.4 Bestäm talen p och q i ett RSA-system, där $n = 4386607$ och $\phi(n) = 4382136$.

§ 8. Primitiva rötter

8.1 Ett tals exponent med avseende på en modul

I detta avsnitt betecknar a och n hela tal med $n > 1$ och $(a, n) = 1$. Då är $a^{\phi(n)} \equiv 1 \pmod{n}$ enligt Eulers sats. Det existerar alltså åtminstone ett positivt heltal m, för vilket $a^m \equiv 1 \pmod{n}$. *Låt d vara det minsta positiva heltalet med egenskapen $a^d \equiv 1 \pmod{n}$.* Existensen av ett dylikt tal garanteras av sats 1.1. Vi säger då att *a hör till exponenten d modulo n* eller att *a:s ordning modulo n är d.* Detta betecknas $d = \mathrm{ord}_n a$.

Som exempel kan vi betrakta fallet $a = 2$, $n = 7$. Då är

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}.$$

Således hör 2 till exponenten 3 modulo 7. Med $a = 3$, $n = 7$ fås följande kongruenser modulo 7:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1.$$

Alltså är $\mathrm{ord}_7 3 = 6$. Vi konstaterar att tal, som är kongruenta modulo n, alltid hör till samma exponent modulo n. Ty om $a \equiv b \pmod{n}$, så är $a^m \equiv b^m \pmod{n}$ för varje positivt heltal m (sats 5.5).

I det följande skall vi härleda några grundläggande egenskaper hos ordningstalet d. Liksom ovan betecknar härvid *a och n relativt prima heltal med $n > 1$*, utan att detta varje gång särskilt påpekas.

Sats 8.1. *Om a hör till exponenten d modulo n, så gäller för varje positivt heltal m:*

$$a^m \equiv 1 \pmod{n} \iff d \mid m. \tag{8.1}$$

Bevis: Enligt divisionsalgoritmen är $m = dq + r$, där $0 \leq r < d$. Detta ger:

$$a^m = a^{dq+r} = (a^d)^q \cdot a^r \equiv a^r \pmod{n}. \tag{a}$$

Om nu $d \mid m$, så är $r = 0$, vilket ger $a^r \equiv 1 \pmod{n}$. Därmed är även $a^m \equiv 1 \pmod{n}$. Omvänt, om sistnämnda kongruens gäller, så följer ur (a) att $a^r \equiv 1 \pmod{n}$. Då nu $0 \leq r < d$, så följer av d:s definition att $r = 0$ och således att $d \mid m$. □

Kor. 8.1. *Om a hör till exponenten d modulo n, så är d en divisor i $\phi(n)$.*

Resultatet följer omedelbart ur sats 8.1, eftersom $a^{\phi(n)} \equiv 1 \pmod{n}$. Av detta korollarium följer att vi behöver beräkna a^m modulo n endast för de positiva heltal m, vilka är divisorer i $\phi(n)$, då vi söker a:s ordning modulo n. T.ex. om $a = 5$, $n = 18$, så är $\phi(n) = 6$. Divisorerna i 6 är 1, 2, 3, 6. Vi får då följande kongruenser modulo 18:

$$5^1 \equiv 5, \quad 5^2 \equiv 25 \equiv 7, \quad 5^3 \equiv 35 \equiv 17, \quad 5^6 \equiv 289 \equiv 1.$$

Således är $\mathrm{ord}_{18}5 = 6$.

Sats 8.2. *Antag att a hör till exponenten d modulo n. Då gäller för godtyckliga positiva heltal h och k:*

$$a^h \equiv a^k \pmod{n} \iff h \equiv k \pmod{d}. \tag{8.2}$$

Bevis: Antag t.ex. att $h \geq k$. Då $(a, n) = 1$, är även $(a^k, n) = 1$. Kongruensen i vänstra ledet av (8.2) är alltså ekvivalent med kongruensen $a^{h-k} \equiv 1 \pmod{n}$. (Jfr. korollarierna 5.3 och 5.4). Men enligt sats 8.1 gäller sistnämnda kongruens, om och endast om $d \mid (h-k)$, dvs. om och endast om $h \equiv k \pmod{d}$. □

Sats 8.3. *Om a hör till exponenten d modulo n, så är talen*

$$a, a^2, a^3, \ldots, a^d \tag{8.3}$$

parvis inkongruenta modulo n.

Bevis: Vore $a^h \equiv a^k \pmod{n}$ för något par h, k med $1 \leq h < k \leq d$, så skulle vi ha $h \equiv k \pmod{d}$ enligt sats 8.2. Men detta är omöjligt, då $0 < k - h < d$. Alltså är talen (8.3) parvis inkongruenta modulo n. □

Sats 8.4. *Antag att a hör till exponenten d modulo n och låt m vara ett positivt heltal. Då hör talet a^m till exponenten $\frac{d}{(m,d)}$ modulo n.*

Bevis: Sätt $(m, d) = e$. Då är $m = m'e$, $d = d'e$ för heltaliga m' och d' med $(m', d') = 1$ (sats 3.4). Vi bör alltså visa att a^m hör till exponenten d' modulo n. Eftersom $a^d \equiv 1 \pmod{n}$ fås:

$$(a^m)^{d'} = a^{md'} = a^{dm'} = (a^d)^{m'} \equiv 1 \pmod{n}. \tag{a}$$

Nu skall visas att det inte existerar någon annan positiv exponent $c < d'$ med $(a^m)^c \equiv 1 \pmod{n}$. Betrakta fördenskull talföljden

$$a^m, a^{2m}, a^{3m}, \ldots, a^{d'm}. \tag{b}$$

Dessa tal är parvis inkongruenta modulo n, ty vore $a^{hm} \equiv a^{km} \pmod{n}$ för något par h, k med $1 \leq h < k \leq d'$, så skulle vi enligt sats 8.2 ha $hm \equiv km \pmod{d}$. Detta skulle innebära att $d \mid m(k-h)$ och således även $d' \mid m'(k-h)$. Men detta är omöjligt, då $(d', m') = 1$ och $0 < k - h < d'$ (sats 3.8). Talen (b) är alltså parvis inkongruenta modulo n, varför enligt (a) endast det sista talet i följden är $\equiv 1 \pmod{n}$. Därmed är visat att a^m hör till exponenten d' modulo n. □

Kor. 8.4. *Antag att a hör till exponenten d modulo n. Av talen (8.3) hör då de a^m, för vilka $(m, d) = 1$, till exponenten d modulo n. Deras antal är således $= \phi(d)$.*

8.2 Primitiva rötter

Låt liksom tidigare a och n vara relativt prima heltal med $n > 1$. Vidare antas att a hör till exponenten d modulo n. Vi inför följande

Definition: Talet a säges vara en *primitiv rot modulo n* eller en *primitiv rot till talet n*, om $d = \phi(n)$.

Exempelvis är 3 en primitiv rot till talet 7 och 5 en primitiv rot till talet 18, såsom av exemplen i föregående avsnitt framgår. Alla heltal har ingalunda primitiva rötter. Sålunda finns det inga primitiva rötter modulo 8. Detta inses på följande sätt: De tal, som skulle kunna komma ifråga, är de till 8 primiska talen 1, 3, 5, 7. Nu finner man lätt att $\operatorname{ord}_8 1 = 1$, $\operatorname{ord}_8 3 = \operatorname{ord}_8 5 = \operatorname{ord}_8 7 = 2$, medan $\phi(8) = 4$. Talet 8 saknar alltså primitiva rötter.

I det följande skall vi härleda ett par satser för primitiva rötter, under förutsättning att deras existens är garanterad. Dessa satser fås mer eller mindre som direkta resultat av satserna i föregående avsnitt för det fall att $d = \phi(n)$.

Sats 8.5. *Om a är en primitiv rot till talet n, så bildar talen*

$$a, a^2, a^3, \ldots, a^{\phi(n)} \tag{8.4}$$

ett reducerat restsystem modulo n.

Bevis: Eftersom $(a, n) = 1$, så är även $(a^k, n) = 1$ för varje positivt heltal k (kor. 3.9). Talen (8.4) är alltså relativt primiska till talet n. De är dessutom parvis inkongruenta modulo n på grund av sats 8.3, eftersom vi nu har $d = \phi(n)$. Därmed är satsen bevisad. □

Ovan konstaterades att 5 är en primitiv rot till talet 18 och att $\phi(18) = 6$. Enligt sats 8.5 bildar alltså talen $5, 5^2, 5^3, 5^4, 5^5, 5^6$ ett reducerat restsystem modulo 18. Detta framgår tydligare, om vi reducerar talen ifråga modulo 18. Man får då

$$5 \equiv 5, \quad 5^2 \equiv 7, \quad 5^3 \equiv 17, \quad 5^4 \equiv 13, \quad 5^5 \equiv 11, \quad 5^6 \equiv 1.$$

Eftersom varje primitiv rot till talet n bör vara relativt primisk till n, så följer av sats 8.5 att alla primitiva rötter modulo n ingår i talföljden (8.4). Vilka av dessa tal, som faktiskt är primitiva rötter, framgår av följande sats.

Sats 8.6. *Låt a vara en primitiv rot modulo n. Då är a^m en primitiv rot modulo n, om och endast om $(m, \phi(n)) = 1$.*

Bevis: Satsen är en direkt följd av kor. 8.4, då vi beaktar att $d = \phi(n)$ i detta fall. □

Kor. 8.6. *Om heltalet $n > 1$ har en primitiv rot, så har det exakt $\phi(\phi(n))$ primitiva rötter, som är inkongruenta modulo n.*

Bevis: Låt a vara en primitiv rot till talet n. Vi vet att alla primitiva rötter återfinnes i talföljden (8.4). Primitiva rötter är de tal i följden, vilkas exponent är relativt primisk till $\phi(n)$ (sats 8.6). Antalet dylika tal är uppenbarligen $\phi(\phi(n))$. Dessa tal är parvis inkongruenta modulo n på grund av sats 8.5. □

8.3 Primitiva rötter med primtalsmodul

I detta avsnitt skall vi speciellt undersöka primitiva rötter i det fall, då moduln är ett primtal. Vår avsikt är att visa att varje sådan modul har åtminstone en primitiv rot. Fördenskull måste vi först bevisa några förberedande satser.

Låt $P(x)$ vara ett polynom av formen

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \tag{8.5}$$

där koefficienterna $a_0, a_1, \ldots, a_n$ är hela tal. Vidare må p vara ett primtal, som inte delar a_n. Vi säger då att heltalet b utgör en *rot* eller en *lösning* till kongruensen

$$P(x) \equiv 0 \pmod{p}, \tag{8.6}$$

om $P(b) \equiv 0 \pmod{p}$. Om $b \equiv c \pmod{p}$ och om b utgör en rot till kongruensen (8.6), så är även c en rot till nämnda kongruens. Detta följer omedelbart av sats 5.6. Vid bestämningen av rötterna till kongruensen (8.6) behöver vi alltså endast beakta sådana rötter, som är parvis inkongruenta modulo p. Beträffande antalet dylika rötter gäller följande sats.

Sats 8.7. (Lagrange's teorem). *Under ovannämnda förutsättningar beträffande polynomet $P(x)$ och primtalet p har kongruensen (8.6) högst n inkongruenta rötter modulo p.*

Bevis: Vi bevisar satsen med induktionsprincipen. I fallet $n = 1$ är kongruensen av formen $a_1 x \equiv -a_0 \pmod{p}$, varvid $p \nmid a_1$. Denna kongruens är av samma typ som den linjära kongruensen (5.6) i avsnitt (5.3). Antagandet $p \nmid a_1$ är ekvivalent med att $(p, a_1) = 1$, då p är ett primtal. Enligt kor. 5.9 har ovannämnda kongruens exakt en lösning modulo p, varför satsen är riktig i fallet $n = 1$. Antag nu att satsen är riktig för alla polynom av graden $n - 1$, vilka uppfyller satsens förutsättningar. Vi skall då visa att satsen även gäller för polynomet (8.5) av graden n. Antag som antites att kongruensen (8.6) skulle ha $n + 1$ modulo p inkongruenta rötter b_0, b_1, b_2, ..., b_n. Således är $P(b_k) \equiv 0 \pmod{p}$ för $k = 0, 1, 2, \ldots, n$. Eftersom

$$P(x) - P(b_0) = a_n(x^n - b_0^n) + a_{n-1}(x^{n-1} - b_0^{n-1}) + \cdots + a_1(x - b_0),$$

så kan faktorn $(x - b_0)$ utbrytas ur högra ledet, varvid vi får

(a) $$P(x) - P(b_0) = (x - b_0)Q(x),$$

där $Q(x)$ är ett polynom av graden $n-1$, i vilket koefficienten för x^{n-1} är a_n. Tag nu ett godtyckligt index k med $1 \leq k \leq n$ och insätt $x = b_k$ i (a). Då fås:

$$P(b_k) - P(b_0) = (b_k - b_0)Q(b_k).$$

Enligt antitesen är $P(b_k) \equiv P(b_0) \equiv 0 \pmod{p}$. Detta ger: $(b_k - b_0)Q(b_k) \equiv 0 \pmod{p}$. Talet $(b_k - b_0)Q(b_k)$ är alltså delbart med p. Härvid är $b_k - b_0$ inte delbart med p, eftersom rötterna b_0, b_1, b_2, ..., b_n är inkongruenta modulo p. Följaktligen är $Q(b_k)$ delbart med p, och således $Q(b_k) \equiv 0 \pmod{p}$ (sats 3.9). Talet b_k är alltså en rot till kongruensen $Q(x) \equiv 0 \pmod{p}$, och då detta gäller för $k = 1, 2, \ldots, n$ har nämnda kongruens n inkongruenta rötter modulo p i strid med induktionsantagandet. Antitesen är alltså oriktig, vilket betyder att kongruensen (8.6) har högst n inkongruenta rötter modulo p. Induktionsprincipen visar nu att detta gäller för alla gradtal n. □

Antag nu att heltalet a hör till exponenten d modulo primtalet p. Härvid gäller att $d \mid (p - 1)$ på grund av kor. 8.1, eftersom $\phi(p) = p - 1$. Vi betraktar nu kongruensen

(8.7) $$x^d \equiv 1 \pmod{p}$$

och påstår att talen

(8.8) $$a, a^2, a^3, \ldots, a^d$$

representerar *alla* modulo p inkongruenta rötter till nämnda kongruens. Först och främst är talen (8.8) rötter till kongruensen ifråga, eftersom $(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$ för varje positivt heltal k. Vidare är talen (8.8) parvis inkongruenta modulo p enligt sats 8.3. Slutligen följer av sats 8.7 att kongruensen (8.7) inte kan ha mer än d inkongruenta rötter modulo p. Därmed är påståendet ovan bevisat.

På grund av kor. 8.4 hör de tal a^k i följden (8.8), för vilka $(k,d)=1$, till exponenten d modulo p. Dessas antal $=\phi(d)$. Sammanfattningsvis finner vi alltså, att om det överhuvudtaget finns ett tal a, som hör till exponenten d modulo primtalet p, så existerar det exakt $\phi(d)$ tal, som hör till denna exponent modulo p, och dessa $\phi(d)$ tal ingår alla i följden (8.8).

Man frågar sig nu, om det för *varje* positiv divisor d i talet $p-1$ (p = primtal) finns något heltal a, som hör till exponenten d modulo p. Denna fråga besvaras jakande av följande sats.

Sats 8.8. *Om p är ett primtal och d en positiv divisor i talet $p-1$, så hör till exponenten d exakt $\phi(d)$ tal, vilka är parvis inkongruenta modulo p.*

Bevis: Låt $d_1, d_2, \ldots, d_k$ vara de positiva divisorerna i talet $p-1$. Antag att det till exponenten d_ν hör $\psi(d_\nu)$ tal, som är parvis inkongruenta modulo p. Av det ovansagda följer att

$$\psi(d_\nu)=\phi(d_\nu) \qquad \text{eller} \qquad \psi(d_\nu)=0, \tag{8.9}$$

beroende på om det finns något eller inget tal a, som hör till exponenten d_ν modulo p. Eftersom talen 1, 2, 3, ..., $p-1$ representerar ett reducerat restsystem modulo p, så måste vart och ett av dessa tal höra till någon exponent d_ν modulo p. Således är

$$\psi(d_1)+\psi(d_2)+\cdots+\psi(d_k)=p-1. \tag{8.10}$$

Å andra sidan gäller enligt formel (6.10):

$$\phi(d_1)+\phi(d_2)+\cdots+\phi(d_k)=p-1. \tag{8.11}$$

Formlerna (8.9) – (8.11) visar nu att $\psi(d_\nu)=\phi(d_\nu)$ för $\nu=1,2,3,\ldots,k$, eftersom de betraktade talen alla är icke-negativa. Därmed är satsen bevisad. □

Vi är nu i stånd att bevisa den redan aviserade satsen, som garanterar att varje primtal har åtminstone en primitiv rot. I själva verket gäller:

Sats 8.9. *Om p är ett primtal, så existerar det exakt $\phi(p-1)$ primitiva rötter till talet p, vilka är parvis inkongruenta modulo p. Om a är en sådan rot, så representerar de tal a^m $(1\le m\le p-1)$, för vilka $(m,p-1)=1$, ett dylikt system av $\phi(p-1)$ primitiva rötter, vilka är parvis inkongruenta modulo p.*

Bevis: Satsens första del följer omedelbart av sats 8.8, då vi sätter $d=\phi(p)=p-1$. Satsens senare del följer av satserna 8.5 och 8.6 med $n=p$. □

Varje primtal har alltså primitiva rötter. Man kan fråga sig i vilken mån sammansatta tal har primitiva rötter. Vi har sett i avsnitt 8.1 att talet 18 har 5 som en primitiv rot, medan talet 8 helt saknar primitiva rötter (avsnitt 8.2). Uppenbarligen har vissa sammansatta tal primitiva rötter, andra ej. Vi ger här utan bevis den sats, som fullständigt besvarar frågan, vilka positiva heltal som har primitiva rötter.

Sats 8.10. *Heltalet $n > 1$ har primitiva rötter, om och endast om $n = 2$, $n = 4$, $n = p^k$ eller $n = 2p^k$, där p är ett udda primtal och k ett positivt heltal.*

8.4 Ett tals index för en primitiv rot

Låt $n > 1$ vara ett heltal, som har primitiva rötter. Om r är en av dessa rötter, så bildar talen

$$r, r^2, r^3, \ldots, r^{\phi(n)} \tag{8.12}$$

ett reducerat restsystem modulo n (sats 8.5). Låt nu a vara ett godtyckligt heltal, *som är relativt primiskt till* n. Då finns det bland talen (8.12) exakt ett tal r^i $(1 \leq i \leq \phi(n))$, sådant att

$$r^i \equiv a \pmod{n}. \tag{8.13}$$

Talet i kallas *a:s index för basen r modulo n* och betecknas $i = \mathrm{ind}_r a$ eller kortare $i = \mathrm{ind}\, a$, om inget missförstånd kan uppstå. Observera att man vanligen bortlämnar moduln n ur beteckningen, eftersom den antas vara fixerad. Indexet är entydigt bestämt modulo $\phi(n)$, ty $j \equiv i \pmod{\phi(n)}$ medför $r^j \equiv r^i \equiv a \pmod{n}$. (Jfr. sats 8.2, där vi nu har $d = \phi(n)$).

Som exempel kan vi betrakta fallet $n = 7$. Vi har i avsnitt 8.2 konstaterat att 3 är en primitiv rot till 7, emedan följande kongruenser gäller modulo 7 (se avsnitt 8.1):

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1.$$

Således får vi följande index för basen 3 modulo 7:

$$\mathrm{ind}_3 1 = 6, \quad \mathrm{ind}_3 2 = 2, \quad \mathrm{ind}_3 3 = 1, \quad \mathrm{ind}_3 4 = 4, \quad \mathrm{ind}_3 5 = 5, \quad \mathrm{ind}_3 6 = 3.$$

Med en annan primitiv rot som bas får vi andra värden på indexen. Exempelvis gäller att även 5 är en primitiv rot till talet 7, ty man har följande kongruenser modulo 7:

$$5^1 \equiv 5, \quad 5^2 \equiv 4, \quad 5^3 \equiv 6, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1.$$

Detta ger följande index för basen 5 modulo 7:

$$\mathrm{ind}_5 1 = 6, \quad \mathrm{ind}_5 2 = 4, \quad \mathrm{ind}_5 3 = 5, \quad \mathrm{ind}_5 4 = 2, \quad \mathrm{ind}_5 5 = 1, \quad \mathrm{ind}_5 6 = 3.$$

Av definitionen på index följer omedelbart följande sats.

Sats 8.11. *Låt n vara ett heltal > 1 med den primitiva roten r. Vidare må heltalen a och b vara relativt primiska till n. Då gäller: $a \equiv b \pmod{n} \Rightarrow \mathrm{ind}_r a = \mathrm{ind}_r b$.*

Tack vare denna sats kan man stundom förenkla indexberäkningen för ett tal a genom att först reducera talet modulo n. Sålunda gäller t.ex. med $n = 7$: $\mathrm{ind}_5 81 = \mathrm{ind}_5 4 = 2$, eftersom vi har $81 \equiv 4 \pmod{7}$.

För räkning med index gäller regler, som påminner om de logaritmiska räknereglerna. I stället för likheter får vi nu kongruenser modulo $\phi(n)$. Detta framgår av följande sats.

Sats 8.12. *Låt n vara ett heltal > 1 med den primitiva roten r. Antag vidare att a och b är relativt primiska till n. Slutligen må k vara ett positivt heltal. Då gäller följande räkneregler för index med basen r (som utelämnats ur beteckningarna):*

(a) $$\operatorname{ind} 1 \equiv 0 \pmod{\phi(n)}$$

(b) $$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\phi(n)}$$

(c) $$\operatorname{ind} a^k \equiv k \cdot \operatorname{ind} a \pmod{\phi(n)}.$$

Bevis: (a) Enligt Eulers sats är $r^{\phi(n)} \equiv 1 \pmod{n}$. Då r är en primitiv rot modulo n, finns det ingen lägre potens av r, som är $\equiv 1 \pmod{n}$. Alltså är $\operatorname{ind} 1 = \phi(n) \equiv 0 \pmod{\phi(n)}$.

(b) Av definitionen på index följer:

$$r^{\operatorname{ind}(ab)} \equiv ab \pmod{n}$$

samt

$$r^{\operatorname{ind} a + \operatorname{ind} b} = r^{\operatorname{ind} a} \cdot r^{\operatorname{ind} b} \equiv ab \pmod{n}.$$

Således gäller:

$$r^{\operatorname{ind}(ab)} \equiv r^{\operatorname{ind} a + \operatorname{ind} b} \pmod{n}.$$

Härur följer nu (b), då vi tillämpar sats 8.2 och beaktar att $d = \phi(n)$.

(c) Definitionen på index ger

$$r^{\operatorname{ind} a^k} \equiv a^k \pmod{n}$$

och

$$r^{k \cdot \operatorname{ind} a} = (r^{\operatorname{ind} a})^k \equiv a^k \pmod{n},$$

varav framgår att

$$r^{\operatorname{ind} a^k} \equiv r^{k \cdot \operatorname{ind} a} \pmod{n}.$$

Sats 8.2 ger nu (c), då vi beaktar att $d = \phi(n)$. □

Index kan användas vid lösning av vissa kongruensproblem, såsom vi strax skall visa. Fördenskull är det önskvärt att ha tillgång till indextabeller. I tabell 3 på sid. 99 anges index för alla positiva heltal $< p$ för primtalsmoduler $p \leq 31$. Härvid är basen (som inte anges i tabellen) alltid den minsta primitiva roten till talet p. Samma tabell innehåller även det tal, som svarar mot ett givet index, för primtalsmoduler $p \leq 31$. Vi skall nu med ett par exempel visa hur man kan använda dessa tabeller vid lösning av kongruenser.

Exempel 1 Lös kongruensen $6x^{12} \equiv 11 \pmod{17}$. Den minsta primitiva roten till talet 17 är 3. Vi tar därför alla index med basen 3, som inte utskrives i nedanstående räkningar. Enligt sats 8.11

har vartdera ledet i kongruensen samma index (för basen 3) modulo 17. Genom att i tabell 3 uppsöka ind 11 för $p = 17$ får vi $\text{ind}(6x^{12}) = 7$. Nu gäller enligt sats 8.12 (b) och (c), eftersom $\phi(17) = 16$:

$$\text{ind}(6x^{12}) \equiv \text{ind}\, 6 + 12 \cdot \text{ind}\, x \pmod{16}.$$

Efter insättning av $\text{ind}\, 6 = 15$ får vi således, då de bägge uttrycken för $\text{ind}(6x^{12})$ jämföres:

$$12 \cdot \text{ind}\, x \equiv 8 \pmod{16}.$$

Enligt sats 5.4 kan denna kongruens divideras med 4, varvid vi får $3 \cdot \text{ind}\, x \equiv 2 \pmod 4$. Denna kongruens har lösningen $\text{ind}\, x \equiv 2 \pmod 4$. De modulo 16 inkongruenta lösningarna är således:

$$\text{ind}\, x \equiv 2,\ 6,\ 10,\ 14 \pmod{16}.$$

Vi har slutligen att i tabell 3 uppsöka de tal, som svarar mot dessa index modulo 17. Då fås lösningarna

$$x \equiv 9,\ 15,\ 8,\ 2 \pmod{17}.$$

Exempel 2 Lös kongruensen $7^x \equiv 5 \pmod{17}$. Vi kan även här använda 3 som bas för indexen. Eftersom $\text{ind}\, 7 = 11$ och $\text{ind}\, 5 = 5$ (tabell 3), fås med stöd av sats 8.12: $11x \equiv 5 \pmod{16}$. Då 3 är en invers till talet 11 modulo 16 (ty $11 \cdot 3 \equiv 1 \pmod{16}$), så multiplicerar vi kongruensen med 3 och får slutresultatet: $x \equiv 15 \pmod{16}$.

Övningsuppgifter

Uppgift 8.1 Bestäm de exponenter, till vilka talen 1, 2, 3,..., 12 hör modulo 13.

Uppgift 8.2 Bestäm a) $\text{ord}_5 2$, b) $\text{ord}_{10} 3$, c) $\text{ord}_{13} 10$.

Uppgift 8.3 Bestäm alla heltal a, som är relativt primiska till 15 och för vilka $\text{ord}_{15} a = 4$.

Uppgift 8.4 Visa att om $\bar{a}$ är en invers till heltalet a modulo $n > 1$, så gäller: $\text{ord}_n a = \text{ord}_n \bar{a}$.

Uppgift 8.5 Antag att a och b är relativt primiska till heltalet $n > 1$. Antag vidare att a och b hör till exponenterna d resp. e modulo n och att $(d, e) = 1$. Visa att ab hör till exponenten de modulo n. (Ledning: Undersök först för vilka positiva heltal m kongruensen $(ab)^m \equiv 1 \pmod n$ gäller).

Uppgift 8.6 Låt n vara ett heltal > 1 och a ett heltal, relativt primiskt till n. Visa att om a hör till exponenten $n - 1$ modulo n, så är n ett primtal. (Ledning: Uppgift 6.13 kan tillämpas).

Uppgift 8.7 Bestäm alla primitiva rötter modulo a) 22, b) 12.

Uppgift 8.8 Visa att 5 är en primitiv rot modulo 23 och bestäm därefter alla modulo 23 inkongruenta, primitiva rötter till talet 23. Svaret bör anges med positiva heltal ≤ 23.

Uppgift 8.9 Låt p vara ett primtal med $p \equiv 1 \pmod 4$. Visa att det existerar ett heltal a med $a^2 \equiv -1 \pmod p$.

Uppgift 8.10 Talet 5 är som bekant en primitiv rot till 18. Uppgör med 5 som bas en indextabell modulo 18.

Uppgift 8.11 Lös kongruenserna a) $5x^7 \equiv 6 \pmod{13}$, b) $x^9 \equiv 8 \pmod{13}$.

Uppgift 8.12 Lös kongruensen $4x^{15} \equiv 5 \pmod{13}$.

Uppgift 8.13 För vilka positiva heltal a är kongruensen $ax^4 \equiv 2 \pmod{13}$ lösbar? Lös kongruensen för dessa värden på a.

Uppgift 8.14 Låt $n > 1$ vara ett heltal och låt r och s vara två primitiva rötter till n, vilka är inkongruenta modulo n. Låt vidare a vara ett heltal, som är relativt primiskt till n. Visa att a) $\mathrm{ind}_s a \equiv (\mathrm{ind}_s r)(\mathrm{ind}_r a) \pmod{\phi(n)}$, b) $(\mathrm{ind}_s r)(\mathrm{ind}_r s) \equiv 1 \pmod{\phi(n)}$.

Uppgift 8.15 Låt p vara ett udda primtal. Visa att $\mathrm{ind}_r(-1) = (p-1)/2$ för varje primitiv rot r till p.

§ 9. Kvadratiska rester

9.1 Legendre's symbol och Eulers kriterium

I denna paragraf skall vi studera kongruensen

$$x^2 \equiv a \pmod{p}, \tag{9.1}$$

där p *är ett primtal och* a *ett heltal, som inte är divisibelt med* p. Sistnämnda antagande innebär att a och p är relativt prima. Vi inför följande

Definition: Talet a säges vara en *kvadratisk rest modulo* p eller *till* p, om kongruensen (9.1) har någon lösning x. I motsatt fall kallas a en *kvadratisk ickerest modulo* p eller *till* p.

Det är klart att om a är en kvadratisk rest (resp. ickerest) modulo p, så är även varje tal i den restklass modulo p, som a representerar, en kvadratisk rest (resp. ickerest). Vi sökandet efter kvadratiska rester eller ickerester behöver vi alltså endast beakta sådana tal a, som är sinsemellan inkongruenta modulo p. Då a dessutom skall vara relativt primiskt till p, kan vi följaktligen inskränka oss till ett reducerat restsystem modulo p, t.ex. till talen $1, 2, \ldots, p-1$. Detsamma gäller eventuella rötter x till kongruensen (9.1), ty om x är en sådan rot, så är även varje y med $x \equiv y \pmod{p}$ en rot. Vidare måste varje rot x vara relativt primisk till p, ty då $x^2 - a$ är delbart med p, så vore även a delbart med p i den händelse att vi skulle ha $x = kp$ för något heltal k. Möjliga rötter till kongruensen (9.1) finns alltså att söka bland talen $1, 2, \ldots, p-1$.

Exempel 1 Betrakta fallet $p = 11$. För att utröna vilka tal, som är kvadratiska rester resp. ickerester till 11, kvadrerar vi de möjliga rötterna x till kongruensen $x^2 \equiv a \pmod{11}$, dvs. talen $1, 2, \ldots, 10$, och reducerar kvadraterna modulo 11. Vi får då följande kongruenser modulo 11:

$$1^2 \equiv 10^2 \equiv 1, \quad 2^2 \equiv 9^2 \equiv 4, \quad 3^2 \equiv 8^2 \equiv 9, \quad 4^2 \equiv 7^2 \equiv 5, \quad 5^2 \equiv 6^2 \equiv 3.$$

Vi ser alltså att talen 1, 3, 4, 5 och 9 är kvadratiska rester, medan talen 2, 6, 7, 8 och 10 är kvadratiska ickerester modulo 11. Antalet kvadratiska rester och ickerester är alltså lika i detta fall. Detta gäller allmänt, när p är ett udda primtal, såsom följande sats utvisar.

Sats 9.1. *Om p är ett udda primtal, så existerar det $(p-1)/2$ inkongruenta kvadratiska rester (ickerester) modulo p. Ett dylikt system av inkongruenta kvadratiska rester modulo p är t.ex. talen*

$$1^2,\ 2^2,\ 3^2,\ldots,\ \left(\frac{p-1}{2}\right)^2. \tag{9.2}$$

Bevis: Genom att som i exempel 1 kvadrera talen $1, 2, \ldots, p-1$ och reducera modulo p får vi alla kvadratiska rester a i intervallet $[1, p-1]$. Mot varje dylikt a svarar två heltal h och $p-h$ i intervallet $[1, p-1]$, eftersom $h^2 \equiv (p-h)^2 \pmod{p}$ för $h = 1, 2, \ldots, (p-1)/2$. Antalet kvadratiska rester blir alltså $= (p-1)/2$. Då är antalet kvadratiska ickerester modulo p även $= (p-1)/2$, emedan summan av antalet kvadratiska rester och ickerester är $= p-1$. Talen (9.2) är uppenbarligen kvadratiska rester modulo p. De är dessutom inkongruenta modulo p, ty vore $h^2 \equiv k^2 \pmod{p}$ för något par h, k med $1 \leq h < k \leq (p-1)/2$, så vore $(h-k)(h+k)$ delbart med p, vilket enligt kor. 3.8 skulle innebära att $h-k$ eller $h+k$ vore delbart med p. Men detta är omöjligt, då $|h-k| < (p-1)/2$ och $0 < h+k < p$. Talen (9.2) representerar alltså ett fullständigt system av inkongruenta kvadratiska rester modulo p. □

Vi skall nu införa en ny beteckning, som visat sig vara mycket praktisk vid räkning med kvadratiska rester. Vi antar liksom tidigare att p är ett primtal och a ett heltal, som inte är delbart med p. Då definieras *Legendre's symbol* $\left(\frac{a}{p}\right)$ på följande sätt:

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

Av exempel 1 framgår att

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$
$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Eftersom två tal, som tillhör samma restklass modulo p, antingen bägge är kvadratiska rester eller bägge kvadratiska ickerester modulo p, så gäller:

Sats 9.2. *Om $a \equiv b \pmod{p}$, så är $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

När man vill undersöka om ett givet tal a är en kvadratisk rest till p, kan man testa huruvida a är kongruent med något av talen (9.2). I jakande fall är a en kvadratisk rest, i nekande fall är a en kvadratisk ickerest modulo p. Ett annat sätt att avgöra denna fråga innehålles i följande sats.

Sats 9.3. (Eulers kriterium). *Om p är ett udda primtal och a ett heltal, som inte är delbart med p, så gäller:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{9.3}$$

Bevis: Satsen utsäger att

(9.4) $a^{(p-1)/2} \equiv 1 \pmod{p}$, om a är en kvadratisk rest modulo p

och

(9.5) $a^{(p-1)/2} \equiv -1 \pmod{p}$, om a är en kvadratisk ickerest modulo p.

Vi bör alltså påvisa riktigheten av (9.4) och (9.5). Enligt Fermat's lilla sats är $a^{p-1} \equiv 1 \pmod{p}$. Talet $(a^{p-1}-1) = (a^{(p-1)/2}-1)(a^{(p-1)/2}+1)$ är alltså divisibelt med p. Detta medför enligt kor. 3.8 att a satisfierar någondera kongruensen

(a) $$x^{(p-1)/2} \equiv 1 \pmod{p}$$

eller

(b) $$x^{(p-1)/2} \equiv -1 \pmod{p}.$$

Antag nu att a är en kvadratisk rest modulo p. Då är $a \equiv h^2 \pmod{p}$ för något heltal h, som inte är delbart med p. Då sistnämnda kongruens upphöjes till potensen $(p-1)/2$, fås med beaktande av Fermat's lilla sats:

$$a^{(p-1)/2} \equiv h^{p-1} \equiv 1 \pmod{p}.$$

Varje kvadratisk rest a till p satisfierar alltså kongruensen (a). Enligt sats 9.1 är antalet inkongruenta kvadratiska rester modulo p lika med $(p-1)/2$. Eftersom kongruensen (a) enligt Lagranges sats inte kan ha flere än $(p-1)/2$ inkongruenta rötter modulo p, så måste alla kvadratiska ickerester till p satisfiera kongruensen (b). Därmed har vi påvisat riktigheten av (9.4) och (9.5), dvs. Eulers kriterium är bevisat. □

Eulers kriterium är ofta bekvämt att använda vid härledning av olika egenskaper hos Legendre's symbol. Detta framgår av de följande satserna.

Sats 9.4. *Låt p vara ett udda primtal samt a och b hela tal, som inte är divisibla med p. Då gäller:*

(9.6) $$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Bevis: Enligt Eulers kriterium är

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \quad \text{och} \quad \left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod{p}.$$

Då dessa kongruenser multipliceras, fås

(a) $$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{(p-1)/2} \pmod{p}.$$

Å andra sidan gäller enligt Eulers kriterium:

$$\text{(b)} \qquad \left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \pmod{p}.$$

Ur (a) och (b) följer nu

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Eftersom vartdera ledet i denna kongruens är antingen $+1$ eller -1, så måste bägge leden vara lika, då ju $p > 2$. Alltså gäller (9.6). □

Av sats 9.4 framgår att produkten av två kvadratiska rester eller två ickerester är en kvadratisk rest, medan produkten av en kvadratisk rest och en ickerest är en kvadratisk ickerest. Om vi i formel (9.6) sätter $a = b$, får vi

$$\left(\frac{a^2}{p}\right) = 1, \tag{9.7}$$

vilket uttrycker det självklara faktum att varje jämn kvadrat, som inte är delbar med p, är en kvadratisk rest modulo p.

Varje udda primtal p är antingen av formen $p = 4n + 1$ eller av formen $p = 4n - 1$. Värdet av $\left(\frac{-1}{p}\right)$ är beroende av vilketdera av dessa fall som inträffar. Detta framgår av följande sats.

Sats 9.5. *Talet -1 är en kvadratisk rest till alla primtal p av formen $p = 4n + 1$ och en kvadratisk ickerest till alla primtal p av formen $p = 4n - 1$. Dessa resultat kan sammanfattas i formeln*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{9.8}$$

Bevis: Enligt Eulers kriterium är

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

Då vartdera ledet i denna kongruens är antingen $+1$ eller -1, finner vi precis som i föregående bevis att

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Högra ledet i denna likhet är nu $= +1$ eller $= -1$, beroende på om $p = 4n + 1$ eller $p = 4n - 1$. Därmed är satsen bevisad. □

Genom att kombinera formlerna (9.6) och (9.8) får vi för varje positivt heltal a, som inte är delbart med primtalet $p > 2$:

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{(p-1)/2}\left(\frac{a}{p}\right). \tag{9.9}$$

Vi ser alltså att problemet att bestämma huruvida ett negativt heltal är en kvadratisk rest eller ej alltid kan återföras på motsvarande problem för talets absoluta belopp.

9.2 Gauß lemma och reciprocitetssatsen

I detta avsnitt skall vi härleda en berömd sats, som går under namn av (den kvadratiska) reciprocitetssatsen. Den ger ett samband mellan $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$, när p och q är två olika udda primtal. För detta ändamål behöver vi en hjälpsats, som kallas Gauß lemma och som ger ett nytt sätt att beräkna $\left(\frac{a}{p}\right)$.

Sats 9.6. (Gauß lemma). *Låt p vara ett udda primtal och a ett heltal, som inte är divisibelt med p. Då gäller:*

$$\left(\frac{a}{p}\right) = (-1)^s, \tag{9.10}$$

där s betecknar antalet av de tal i följden

$$a,\ 2a,\ 3a,\ldots,\ \frac{p-1}{2}\cdot a, \tag{9.11}$$

vilkas huvudrester modulo p är $> p/2$.

Bevis: Vi konstaterar först att talen (9.11) är parvis inkongruenta modulo p, ty de utgör en del av ett fullständigt restsystem modulo p (jfr. kor. 5.8 med $b = 0$). Inget av talen är delbart med p (kor. 3.8), varför ingen av huvudresterna $= 0$. Huvudresterna ligger alltså alla i intervallet $[1, p-1]$. Låt nu $\alpha_1, \alpha_2, \ldots, \alpha_s$ vara de huvudrester, som är $> p/2$, och $\beta_1, \beta_2, \ldots, \beta_t$ de huvudrester, som är $< p/2$. Då är $s+t = (p-1)/2$. Talen α_μ och β_ν är alla olika, eftersom talen (9.11) är inkongruenta modulo p. Dessutom är talen

$$p-\alpha_1,\ p-\alpha_2,\ldots,\ p-\alpha_s,\ \beta_1,\ \beta_2,\ldots,\ \beta_t \tag{a}$$

alla olika. Antag nämligen att vi skulle ha $p - \alpha_\mu = \beta_\nu$ för något par μ, ν. Eftersom $\alpha_\mu \equiv ma$ och $\beta_\nu \equiv na \pmod{p}$, där $1 \le m, n \le (p-1)/2$, så skulle vi få $(m+n)a \equiv 0 \pmod{p}$. Men detta är omöjligt, då varken $m+n$ eller a är delbart med p. Talen (a) är alltså alla olika. Då de dessutom ligger i intervallet $[1, (p-1)/2]$ och är $(p-1)/2$ till antalet, så är de i någon ordning lika med talen $1, 2, 3, \ldots, (p-1)/2$. Således gäller:

$$(p-\alpha_1)(p-\alpha_2)\cdots(p-\alpha_s)\beta_1\beta_2\cdots\beta_t = \left(\frac{p-1}{2}\right)!$$

Om vi ersätter varje $p - \alpha_\mu$ med det därmed kongruenta $-\alpha_\mu$, får vi

$$(-1)^s\alpha_1\alpha_2\cdots\alpha_s\beta_1\beta_2\cdots\beta_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p}. \tag{b}$$

Å andra sidan är talen $\alpha_1, \alpha_2, \ldots, \alpha_s, \beta_1, \beta_2, \ldots, \beta_t$ i någon ordning kongruenta med talen (9.11). Detta ger

$$\alpha_1\alpha_2\cdots\alpha_s\beta_1\beta_2\cdots\beta_t \equiv a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p}. \tag{c}$$

Då (b) och (c) jämföres, fås

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

Denna kongruens kan enligt kor. 5.4 divideras med $(\frac{p-1}{2})!$, som är relativt primiskt till p. Således

$$a^{(p-1)/2} \equiv (-1)^s \pmod{p}.$$

Med användning av Eulers kriterium (9.3) får vi härav

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

vilket med beaktande av att vartdera ledet endast kan anta värdena ± 1 ger den eftersträvade formeln (9.10). □

Med hjälp av Gauß lemma kan vi t.ex. bestämma värdet av $(\frac{2}{p})$, då p är ett udda primtal. Vi har då att i Gauß lemma insätta $a = 2$ och betrakta talföljden

(d) $$2,\ 4,\ 6, \ldots,\ p-1.$$

Eftersom dessa positiva tal alla är $< p$, utgör de även sina egna huvudrester modulo p. Det gäller nu att bestämma huru många av talen (d) som är $> p/2$. Vi kallar detta antal s, såsom i Gauß lemma. Talen (d) är av formen $2u$, där $u = 1, 2, 3, \ldots, (p-1)/2$. Villkoret $2u > p/2$ ger $u > p/4$. Det minsta heltalet u, som uppfyller denna olikhet, är $u = (p+1)/4$ eller $u = (p+3)/4$, beroende på vilket av talen $p+1$ eller $p+3$ som är delbart med 4. I det förra fallet är p av formen $p = 4m-1$, i det senare fallet av formen $p = 4m+1$. I fallet $p = 4m-1$ får vi

$$s = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4} = m,$$

och i fallet $p = 4m+1$:

$$s = \frac{p-1}{2} - \frac{p+3}{4} + 1 = \frac{p-1}{4} = m.$$

I bägge fallen är alltså $s = m$. Enligt Gauß lemma är då: $(\frac{2}{p}) = (-1)^m$. Talet 2 är sålunda en kvadratisk rest eller ickerest modulo p, alltefter som m är jämnt eller udda. Om m är jämnt, så är p av formen $p = 8n \pm 1$, om m är udda, så är p av formen $p = 8n \pm 3$. Vi får därmed följande resultat:

Sats 9.7. *Talet 2 är en kvadratisk rest till alla primtal p av formen $p = 8n \pm 1$ och en kvadratisk ickerest till alla primtal p av formen $p = 8n \pm 3$.*

Eftersom uttrycket $(p^2-1)/8$ antar värdet $8n^2 \pm 2n$ för $p = 8n \pm 1$ och värdet $8n^2 \pm 6n + 1$ för $p = 8n \pm 3$, så ser vi att $(p^2-1)/8$ är jämnt i det förra fallet och udda i det senare. Detta medför att resultatet i sats 9.7 även kan bringas i formen:

Kor. 9.7. *Om p är ett udda primtal, så är*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{9.12}$$

Exempel 1 Beräkna $\left(\frac{89}{13}\right)$. Vi reducerar först talet 89 modulo 13 och får $89 \equiv -2 \pmod{13}$. Med användning av sats 9.2 samt formlerna (9.9) och (9.12) få vi sålunda:

$$\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = (-1)^6(-1)^{21} = -1.$$

Vi skall nu bevisa den kvadratiska reciprocitetssatsen. Innan vi formulerar satsen, kan det vara skäl att ge ett par historiska notiser om dess tillkomst. Satsen publicerades första gången år 1783 av Euler utan bevis. Legendre återupptäckte satsen två år senare men lyckades inte ge ett korrekt bevis. Det första bindande beviset gavs år 1796 av Gauß, som hade upptäckt satsen ett år tidigare på empirisk väg. Det tog honom sålunda ett år att finna det korrekta beviset. Han säger själv: "Under ett helt år plågades jag av satsen, och den krävde all min energi, tills jag slutligen fann ett bevis." Gauß presterade sedermera ytterligare sju olika bevis för satsen. Sedan dess har en mängd olika bevis publicerats, bl.a. av *Cauchy*, *Jacobi* och *Kronecker*. För några år sedan presenterade en matematiker vad han påstod vara det 152:dra beviset för satsen.

Sats 9.8. (Reciprocitetssatsen). *Om p och q är två olika udda primtal, så gäller:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{9.13}$$

Bevis: Vi betraktar talräckorna

$$p,\ 2p,\ 3p,\ldots,\ \frac{q-1}{2}\cdot p \tag{9.14}$$

och

$$q,\ 2q,\ 3q,\ldots,\ \frac{p-1}{2}\cdot q. \tag{9.15}$$

Antalet av de tal i följden (9.14), vilkas huvudrester modulo q är $> q/2$, må vara s. Analogt betecknar t antalet av de huvudrester modulo p i följden (9.15), vilka är $> p/2$. Enligt Gauß lemma gäller då:

$$\left(\frac{p}{q}\right) = (-1)^s \quad \text{och} \quad \left(\frac{q}{p}\right) = (-1)^t.$$

Multiplikation ger:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s+t}.$$

Satsen är sålunda bevisad, om vi kan påvisa att

$$\frac{p-1}{2}\cdot\frac{q-1}{2} \equiv s+t \pmod{2}. \tag{9.16}$$

Vi konstaterar först att antalet huvudrester $> q/2$ i talräckan (9.14) är = antalet minsta absoluta rester < 0, alla rester tagna modulo q. Ty mot varje huvudrest r med $(q/2) < r < q$ svarar en absolut rest $r-q$ med $-(q/2) < r-q < 0$. Detsamma gäller givetvis talräckan (9.15):s motsvarande rester modulo p. Vi kan alltså i fortsättningen operera med minsta absoluta rester < 0, när vi skall bestämma talen s och t.

Låt nu hp vara något av talen (9.14). Dess minsta absoluta rest modulo q fås genom att bilda $hp-kq$, där k är det entydigt bestämda (positiva) heltal, för vilket gäller: $-(q/2) < hp-kq < (q/2)$. För en negativ rest $hp-kq$ blir k bestämt av olikheterna

$$-\frac{q}{2} < hp - kq < 0. \tag{9.17}$$

Härvid är kq något av talen (9.15), ty vore $k \geq (p+1)/2$, så skulle vi ha

$$hp - kq \leq \frac{q-1}{2} \cdot p - \frac{p+1}{2} \cdot q = -\frac{p}{2} - \frac{q}{2} < -\frac{q}{2},$$

vilket strider mot (9.17). Enligt våra antaganden finns det således i talräckorna (9.14) och (9.15) s talpar (hp, kq), som uppfyller olikheterna (9.17). På analogt sätt visas att det i samma talräckor finns t talpar (hp, kq), som uppfyller olikheterna

$$-\frac{p}{2} < kq - hp < 0. \tag{9.18}$$

Av (9.17) och (9.18) följer att det i talräckorna (9.14) och (9.15) finns $s+t$ talpar (hp, kq), som uppfyller olikheterna

$$-\frac{q}{2} < hp - kq < \frac{p}{2}. \tag{9.19}$$

Alla övriga talpar (hp, kq) i räckorna (9.14) och (9.15) uppfyller således någondera av olikheterna

$$hp - kq < -\frac{q}{2} \quad \text{eller} \quad hp - kq > \frac{p}{2}. \tag{9.20}$$

Sätt $h' = (q+1)/2 - h$ $(1 \leq h \leq (q-1)/2)$ och $k' = (p+1)/2 - k$ $(1 \leq k \leq (p-1)/2)$. Då är $h'p$ det h:te talet i räckan (9.14) från slutet räknat. Likaså är $k'q$ det k:te talet i räckan (9.15) från slutet räknat. En enkel räkning visar att

$$(hp - kq) + (h'p - k'q) = \frac{p}{2} - \frac{q}{2}.$$

Antag nu att $hp - kq$ uppfyller den första av olikheterna (9.20). Då är

$$h'p - k'q = \frac{p}{2} - \frac{q}{2} - (hp - kq) > \frac{p}{2} - \frac{q}{2} + \frac{q}{2} = \frac{p}{2}.$$

Alltså om $hp-kq$ uppfyller den första av olikheterna (9.20), så uppfyller $h'p-k'q$ den andra. Analogt kan man visa att om $hp-kq$ uppfyller den andra olikheten (9.20), så uppfyller $h'p-k'q$ den första. Således om talparet (hp, kq) uppfyller den ena av olikheterna (9.20), så uppfyller talparet $(h'p, k'q)$

den andra. Antag nu att den finns u talpar (hp, kq), som uppfyller den första olikheten (9.20). Då finns det även u talpar, som uppfyller den andra olikheten (9.20). Det finns alltså totalt $2u$ talpar (hp, kq), som uppfyller någondera olikheten (9.20). Av talräckorna (9.14) och (9.15) kan man bilda $\frac{p-1}{2} \cdot \frac{q-1}{2}$ talpar (hp, kq). Av dessa uppfyller $s+t$ stycken olikheterna (9.19), medan de övriga $2u$ talparen uppfyller någondera olikheten (9.20). Således är

$$s + t + 2u = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

vilket innebär att kongruensen (9.16) gäller. Därmed är reciprocitetssatsen bevisad. □

Genom att undersöka huru tecknet hos högra ledet av (9.13) beror av talen p och q finner man följande alternativa formulering av reciprocitetssatsen:

Kor. 9.8. *Om p och q är två olika udda primtal, så gäller:*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{om } p \text{ eller } q \text{ (eller båda) är av formen } 4n+1, \\ -\left(\frac{q}{p}\right), & \text{om } p \text{ och } q \text{ är av formen } 4n-1. \end{cases} \tag{9.21}$$

Legendre-symbolerna $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$ är alltså lika utom i det fall att p och q vardera är av formen $4n-1$, då de är varandras motsatta tal.

Bevis: Eftersom $\left(\frac{p}{q}\right)$ och $\left(\frac{q}{p}\right)$ vardera har absolutbeloppet 1, så gäller $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ eller $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, beroende på om högra ledet i formel (9.13) antar värdet $+1$ eller -1. Värdet -1 antas, om och endast om $\frac{p-1}{2}$ och $\frac{q-1}{2}$ bägge är udda tal. Detta inträffar, då och endast då p och q vardera är av formen $4n-1$. I alla övriga fall antar högra ledet i formel (9.13) värdet $+1$. Därmed är korollariet bevisat. □

Exempel 2 Beräkna $\left(\frac{713}{1009}\right)$. Vi konstaterar först att $713 = 23 \cdot 31$ och att 1009 är ett primtal. Sats 9.4 ger då:

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right). \tag{a}$$

Vi tillämpar nu reciprocitetssatsen på Legendre-symbolerna i högra ledet av (a). Eftersom talet 1009 är av formen $4n+1$, får vi enligt kor. 9.8:

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right) \quad \text{och} \quad \left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right). \tag{b}$$

Nu är $1009 \equiv 20 \pmod{23}$ och $1009 \equiv 17 \pmod{31}$. Sats 9.2 ger då:

$$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) \quad \text{och} \quad \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right). \tag{c}$$

Eftersom $20 = 2^2 5$, får vi enligt formlerna (9.6) och (9.7):

$$\left(\frac{20}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right). \tag{d}$$

Upprepad användning av reciprocitetssatsen och sats 9.2 ger:

(e) $$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

varvid den sista Legendre-symbolen har beräknats enligt sats 9.7. Då vi nu sammanställer resultaten i formlerna (b) – (e), får vi

(f) $$\left(\frac{23}{1009}\right) = -1.$$

Vi skall nu beräkna $\left(\frac{17}{31}\right)$. Satserna 9.2, 9.4, 9.7, 9.8 och formel (9.7) ger:

$$\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2^2}{3}\right) = -1.$$

Då detta resultat sammanställes med formlerna (b) och (c), fås

(g) $$\left(\frac{31}{1009}\right) = -1.$$

Med stöd av formlerna (a), (f) och (g) får vi nu slutresultatet:

$$\left(\frac{713}{1009}\right) = (-1)(-1) = 1.$$

9.3 Kongruenser av andra graden

Betrakta en allmän kongruens av andra graden

(9.22) $$ax^2 + bx + c \equiv 0 \pmod{p},$$

där a, b och c är heltal och p ett udda primtal, som inte delar a. Vi skall undersöka antalet rötter till denna kongruens. Enligt Lagrange's sats (sats 8.7) kan den inte ha mer än två inkongruenta rötter modulo p. Sedan kongruensen multiplicerats med $4a$, kan den bringas i formen

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

eller om vi sätter $D = b^2 - 4ac$:

(9.23) $$(2ax + b)^2 \equiv D \pmod{p}.$$

Liksom i ekvationsläran kallas D kongruensens *diskriminant*. Vi får rötterna till kongruensen (9.23) och därmed även till den givna kongruensen (9.22), om vi först löser kongruensen

(9.24) $$y^2 \equiv D \pmod{p}$$

och därefter den linjära kongruensen

$$2ax + b \equiv y \pmod{p}. \tag{9.25}$$

Vi särskiljer nu tre fall:

1) D är en kvadratisk rest modulo p. Då har kongruensen (9.24) någon rot $y_1 \neq 0$. Härvid är även $-y_1$ en rot, som är inkongruent med y_1 modulo p. Vore nämligen $y_1 \equiv -y_1 \pmod{p}$, så skulle vi ha $2y_1 \equiv 0 \pmod{p}$. Detta skulle innebära att $p \mid y_1$ och därmed även $p \mid D$ på grund av (9.24). Men detta är omöjligt, då D är en kvadratisk rest modulo p. Kongruensen (9.24) har alltså i detta fall två inkongruenta rötter modulo p. Mot vardera roten y_1 och $-y_1$ svarar enligt kor. 5.9 en modulo p entydigt bestämd rot x_1 resp. x_2 till kongruensen (9.25). Dessa rötter är då även rötter till kongruensen (9.22). Vidare är x_1 och x_2 inkongruenta modulo p. Vore nämligen $x_1 \equiv x_2 \pmod{p}$, så vore även $y_1 \equiv -y_1 \pmod{p}$ på grund av (9.25), vilket är omöjligt. Kongruensen (9.22) har alltså i detta fall två inkongruenta rötter modulo p.

2) $D \equiv 0 \pmod{p}$. Kongruensen (9.24) har då den enda lösningen $y \equiv 0 \pmod{p}$, ty om primtalet p delar y^2, så delar det även y (kor. 3.8). Därmed har kongruensen (9.25) och således även kongruensen (9.22) en enda lösning modulo p.

3) D är en kvadratisk ickerest modulo p. Kongruensen (9.24) saknar då lösning och därmed även kongruensen (9.25). Detta betyder att kongruensen (9.22) saknar rötter.

Vi sammanfattar våra resultat i följande sats.

Sats 9.9. *Vi antar att a, b och c är heltal samt p ett udda primtal, som inte delar a. Sätt $D = b^2 - 4ac$. Då är antalet modulo p inkongruenta rötter till kongruensen* (9.22)*:*

1) *två, om D är en kvadratisk rest modulo p,*
2) *en, om $D \equiv 0 \pmod{p}$,*
3) *ingen, om D är en kvadratisk ickerest modulo p.*

Övningsuppgifter

Uppgift 9.1 Bestäm alla kvadratiska rester modulo 17.

Uppgift 9.2 Bestäm $\left(\frac{a}{7}\right)$ för $a = 1, 2, 3, 4, 5, 6$.

Uppgift 9.3 Bestäm $\left(\frac{7}{13}\right)$ med användning av a) Eulers kriterium, b) Gauß lemma.

Uppgift 9.4 Visa att talet -2 är en kvadratisk rest till alla primtal p av formen $p = 8n + 1$ och $p = 8n + 3$ samt en kvadratisk ickerest till alla primtal p av formen $p = 8n - 1$ och $p = 8n - 3$.

Uppgift 9.5 Beräkna a) $\left(\frac{7}{79}\right)$, b) $\left(\frac{31}{641}\right)$.

Uppgift 9.6 Beräkna $\left(\frac{371}{1367}\right)$.

Uppgift 9.7 Låt p vara ett primtal > 3. Visa att

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & \text{om } p \text{ är av formen } p = 12n \pm 1, \\ -1, & \text{om } p \text{ är av formen } p = 12n \pm 5. \end{cases}$$

(Ledning: Tillämpa reciprocitetssatsen och beakta att varje primtal > 3 är av formen $6n \pm 1$).

Uppgift 9.8 Låt p vara ett udda primtal och a ett heltal, som inte är delbart med p. Visa att

$$\left(\frac{a}{p}\right) + \left(\frac{2a}{p}\right) + \left(\frac{3a}{p}\right) + \cdots + \left(\frac{(p-1)a}{p}\right) = 0.$$

Uppgift 9.9 Bestäm de udda primtal, till vilka 5 är en kvadratisk a) rest, b) ickerest.

Uppgift 9.10 Bestäm alla lösningar till kongruenserna

a) $x^2 + x + 1 \equiv 0 \pmod 7$

b) $x^2 + 5x + 1 \equiv 0 \pmod 7$

c) $x^2 + 3x + 1 \equiv 0 \pmod 7$.

§ 10. Pytagoreiska tal och Fermat's stora sats

10.1 Pytagoreiska tal

Om x och y betecknar längderna av kateterna i en rätvinklig triangel, där hypotenusans längd $= z$, så gäller som bekant enligt Pytagoras sats:

$$x^2 + y^2 = z^2. \tag{10.1}$$

Av speciellt intresse är *heltalslösningar* till ekvationen (10.1). Vi inför fördenskull följande definition:

Definition: Tre positiva heltal x, y, z, som utgör en lösning till ekvationen (10.1), kallas en *pytagoreisk trippel (pytagoreiska tal).*

Pytagoreiska tal är t.ex. $x = 3$, $y = 4$, $z = 5$ eller $x = 7$, $y = 24$, $z = 25$. Vi ställer oss nu problemet att finna *alla* heltalslösningar x, y, z till ekvationen (10.1). Vi konstaterar först att om x, y, z är en sådan lösning, så är även kx, ky, kz ($k \in Z_+$) en lösning. Omvänt om en lösning x, y, z innehåller en gemensam faktor $k \in Z_+$, så att $x = kx'$, $y = ky'$, $z = kz'$, så är även x', y', z' en lösning. Det är sålunda tillräckligt att söka lösningar, som saknar gemensamma faktorer $k > 1$, eftersom alla andra lösningar kan fås ur dessa genom multiplikation med en konstant faktor. Vi uppställer fördenskull följande definition:

Definition: En pytagoreisk trippel x, y, z kallas *primitiv*, om $(x, y, z) = 1$.

Innan vi härleder en allmän formel för alla heltalslösningar till ekvationen (10.1), skall vi bevisa några förberedande lemmor.

Lemma 10.1. *I en primitiv pytagoreisk trippel är talen parvis relativt prima.*

Bevis: Låt x, y, z var en primitiv pytagoreisk trippel och antag t.ex. att talen x och y inte är relativt prima. De innehåller då någon gemensam primfaktor p, så att $x = px'$, $y = py'$. Ekvationen (10.1) ger $z^2 = p^2(x'^2 + y'^2)$, varav följer att $p \mid z^2$ och således även $p \mid z$ (kor. 3.8). Alltså innehåller även talet z primfaktorn p, vilket strider mot att x, y, z är en primitiv pytagoreisk trippel. På analogt sätt visas att paren x, z och y, z vardera är relativt prima. □

Definition Två heltal säges vara av *samma paritet*, om båda är jämna eller båda är udda. De är av *olika paritet*, om det det ena talet är jämnt och det andra udda.

Två heltal är således av samma paritet, om de tillhör samma restklass modulo 2. De är av olika paritet, när de tillhör var sin restklass modulo 2.

Lemma 10.2. *Om x, y, z är en primitiv pytagoreisk trippel, så är talen x och y av olika paritet.*

Bevis: Talen x och y kan inte båda vara jämna, emedan $(x, y) = 1$ enligt lemma 10.1. Antag nu att båda skulle vara udda, t.ex. $x = 2m+1$ och $y = 2n+1$. Då är $z^2 = x^2+y^2 = 4(m^2+n^2+m+n)+2$, vilket medför att $z^2 \equiv 2 \pmod 4$. Men detta är omöjligt, ty för varje jämn kvadrat gäller: $a^2 \equiv 0$ eller $a^2 \equiv 1 \pmod 4$, beroende på om a är jämnt eller udda. Alltså är talen x och y av olika paritet. □

Lemma 10.3. *Om a och b är relativt prima positiva heltal med $ab = c^2$ ($c \in Z_+$), så är a och b jämna kvadrater.*

Bevis: Satsen är trivial, om något av talen a eller $b = 1$. Vi kan alltså anta att $a > 1$ och $b > 1$. Låt primfaktoriseringen av a och b vara

$$a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}, \qquad b = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}.$$

Härav fås

$$ab = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}. \tag{10.2}$$

Då a och b är relativt prima, är primfaktorerna p_1, p_2, ..., p_m, q_1, q_2, ..., q_n alla olika. Låt primfaktoriseringen av talet c vara

$$c = r_1^{c_1} r_2^{c_2} \cdots r_k^{c_k},$$

vilket ger

$$c^2 = r_1^{2c_1} r_2^{2c_2} \cdots r_k^{2c_k}. \tag{10.3}$$

Då nu $ab = c^2$ och primtalsuppdelningen är entydig, så är primfaktorerna i högra ledet av (10.2) i någon ordning identiska med primfaktorerna i högra ledet av (10.3). Detta betyder bl.a. att talen a_μ ($\mu = 1, 2, \ldots, m$) och b_ν ($\nu = 1, 2, \ldots, n$) är jämna. Vi kan alltså skriva $a_\mu = 2\alpha_\mu$ och $b_\nu = 2\beta_\nu$. Då är

$$a = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m})^2, \qquad b = (q_1^{\beta_1} q_1^{\beta_2} \cdots q_n^{\beta_n})^2,$$

dvs. a och b är jämna kvadrater. □

Vi skall nu härleda en allmän formel för alla primitiva heltalslösningar till ekvationen (10.1). Antag först att x, y, z är en sådan lösning. Då talen x och y enligt lemma 10.2 är av olika paritet,

kan vi t.ex. anta att x är jämnt och y udda. Då är även z udda. Vi skriver ekvationen (10.1) i formen

$$x^2 = z^2 - y^2 = (z+y)(z-y). \tag{10.4}$$

Talen $z+y$ och $z-y$ är bägge jämna. Således kan vi skriva

$$z+y = 2u, \qquad z-y = 2v, \tag{10.5}$$

varav fås

$$y = u - v, \qquad z = u + v. \tag{10.6}$$

Eftersom $z > y > 0$, så följer av (10.5) och (10.6) att $u > v > 0$. Vidare är talen u och v relativt prima, emedan y och z är relativt prima. Detta följer omedelbart av (10.6). Ekvationen (10.4) kan nu skrivas i formen

$$uv = \left(\frac{x}{2}\right)^2. \tag{10.7}$$

Av lemma 10.3 följer då att u och v är jämna kvadrater. Således

$$u = m^2, \qquad v = n^2. \tag{10.8}$$

Härvid är talen m och n relativt prima, eftersom u och v är relativt prima. Vidare gäller att $m > n > 0$. Genom att insätta värdena (10.8) på u och v i formlerna (10.6) och (10.7) får vi den slutliga framställningen för x, y och z:

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2. \tag{10.9}$$

Talen m och n är av olika paritet, eftersom y är udda. Därmed har vi visat: Om x, y, z är en primitiv pytagoreisk trippel, så existerar det relativt prima heltal m och n av olika paritet med $m > n > 0$, sådana att x, y och z kan skrivas i formen (10.9). Antag nu omvänt att m och n är givna heltal med de nyssnämnda egenskaperna. Om vi då definierar talen x, y och z genom formlerna (10.9), så visar en enkel räkning, att x, y och z satisfierar ekvationen (10.1). Talen x, y och z är uppenbarligen positiva heltal, varvid x och y är av olika paritet (x jämnt och y udda). Vidare är x, y och z relativt prima. Ty om dessa tal hade en primfaktor $p > 2$ gemensam, så följer av relationerna $z + y = 2m^2$ och $z - y = 2n^2$, att p skulle dela såväl m som n. Men detta är omöjligt, då m och n är relativt prima. Talen x, y, z bildar alltså en primitiv pytagoreisk trippel. Vi sammanfattar våra resultat i följande sats.

Sats 10.4. *Tre heltal x, y, z bildar en primitiv pytagoreisk trippel, om och endast om det existerar relativt prima heltal m och n av olika paritet med $m > n > 0$, sådana att x, y och z kan framställas genom ekvationerna* (10.9). *Alla övriga pytagoreiska tripplar kan skrivas i formen kx, ky, kz, där k är ett heltal > 1.*

Anmärkning. Eftersom x och y ingår symmetriskt i ekvationen (10.1), kan dessa tal byta roller i ekvationerna (10.9). De så erhållna lösningarna betraktas dock inte som skilda lösningar.

Genom att i formlerna (10.9) successivt insätta värden på m och n, som uppfyller villkoren i sats 10.4, får vi en tabell över primitiva pytagoreiska tripplar. Nedan ges en sådan tabell för alla $m \leq 5$. I tabellen har vi ordnat talen x, y, z i växande storleksordning. Detta har till följd att talen x och y i vissa fall är omkastade i förhållande till formlerna (10.9). Detta är tillåtet enligt anmärkningen ovan.

m	n	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	8	15	17
4	3	7	24	25
5	2	20	21	29
5	4	9	40	41

10.2 Fermat's stora sats

Pierre de Fermat var en gång sysselsatt med att läsa igenom Diofantos' "Arithmetica" (omnämnd i avsnitt 5.4). När han kom till det ställe i boken, där Diofantos härledde formlerna (10.9) och sålunda visade att det finns oändligt många kvadrater, som kan skrivas som en summa av två andra kvadrater, skrev Fermat i marginalen: "Däremot är det omöjligt att dela en kub i två kuber, en fjärde potens i två fjärde potenser, eller i allmänhet någon högre potens än den andra i två potenser av samma grad. Jag har funnit ett verkligt underbart bevis, vilket dock inte får rum i marginalen". I modernt språkbruk innebär Fermat's anmärkning i marginalen att följande sats skulle vara sann:

Sats 10.5. (Fermat's stora sats, Fermat's sista sats). *Ekvationen*

$$x^n + y^n = z^n \tag{10.10}$$

saknar positiva heltalslösningar x, y, z för alla heltal $n \geq 3$.

Fermat's eget exemplar av boken har gått förlorat, men hans son gav år 1670 (efter faderns död) ut en ny upplaga av Diofantos "Arithmetica", som även innehöll Fermat's egna anteckningar. Tack vara detta har många av Fermat's satser blivit bevarade åt eftervärlden. Fermat brukade i allmänhet inte nedteckna bevisen för sina påståenden i marginalen. Men under årens lopp har alla hans satser blivit bevisade utom denna ena rörande de n:te potenserna. Därför kallas den också "Fermat's sista sats". Tusentals matematiker har under 300 års tid förgäves försökt bevisa Fermat's sista sats. Man kan därför med gott fog säga att denna sats för närvarande utgör det mest berömda olösta problemet i matematiken.

Vad har man då åstadkommit ifråga om Fermat's stora sats? För det första är det klart att man inte behöver bevisa satsen för alla heltalsexponenter $n \geq 3$. Har man nämligen bevisat satsen för en viss exponent n, så är den också bevisad för alla heltaliga multipler kn av n. Ty då

$$x^{kn} + y^{kn} = z^{kn} \Longleftrightarrow (x^k)^n + (y^k)^n = (z^k)^n,$$

så skulle en heltalslösning x, y, z till den vänstra ekvationen medföra att ekvationen (10.10) har lösningen x^k, y^k, z^k, vilket är omöjligt på grund av antagandet. Detta betyder att vi endast behöver bevisa Fermat's sats för $n = 4$ och för alla udda primtalsexponenter. Varje helt tal $n \geq 3$ är nämligen divisibelt med 4 eller med något udda primtal (eller med vardera). Ty om n inte är divisibelt med något udda primtal, så är det av formen $n = 2^m$ med $m \geq 2$ och således delbart med 4. Det är mycket troligt att Fermat hade ett bevis i fallet $n = 4$. Han visade nämligen att ekvationssystemet $x^2 + y^2 = z^2$, $u^2 = xy/2$ saknar heltalslösningar, och fallet $n = 4$ kan härledas ur denna sats.

Vi övergår nu till fallet $n = 3$. I ett brev till Christian Goldbach år 1753 påstod Leonard Euler att han hade bevisat Fermat's sats för $n = 3$. Brevet innehöll emellertid inget bevis. Först år 1770 publicerade han ett bevis, som emellertid visade sig vara bristfälligt. Felet i beviset går dock tämligen lätt att reparera, varför Euler brukar få äran av att ha bevisat Fermat's stora sats i fallet $n = 3$. Följande steg är fallet $n = 5$. Detta fall bevisades år 1825 av Dirichlet och Legendre. Därefter bevisades satsen för $n = 7$ av *Gabriel Lamé* år 1839. Åtta år senare trodde han sig ha funnit ett bevis i det allmänna fallet ($n \geq 3$) och presenterade detta för vetenskapsakademin i Paris. Efter att mycket entusiastiskt ha redogjort för sitt bevis togs han ned på jorden igen av *Joseph Liouville*, som påpekade att beviset innehöll ett allvarligt fel. Lamé tillbringade därefter flera veckor med att försöka reparera felet men utan resultat. Följande stora framsteg i teorin för Fermat's sats gjordes i medlet av 1800–talet av *Ernst Eduard Kummer* (1810–1893). Han utvecklade då den s.k. *idealteorin*, med vars hjälp han år 1847 bevisade Fermat's sats för alla udda primtalsexponenter $p < 100$ utom för $p = 37$, 59 och 67. Senare lyckades han med andra metoder bevisa satsen även för dessa exponenter. Kummers idealteori har visat sig vara mycket användbar även inom andra grenar av talteorin.

På detta sätt har man under årens lopp lyckats bevisa Fermat's sats för allt större och större exponenter n. I detta nu vet man att satsen är riktig åtminstone för alla $n \leq 150000$ (*Tanner* och *Wagstaff*, 1987). Detta betyder att om det finns någon heltalslösning x, y, z till Fermat's ekvation, så måste n vara större än 150000. Dessutom visade *Grünert* redan år 1856 att i en dylik lösning talen x, y, z måste vara minst lika stora som n. Senare har denna gräns höjts ytterligare, bl.a. av *Inkeri* (1953). I ett motexempel till Fermat's sats måste man alltså behandla tal av minst storleksordningen $(150000)^{150000}$. Av allt det ovansagda följer, att det förefaller mycket sannolikt att Fermat's sats är riktig. Hur kommer det sig då, att ingen har lyckats rekonstruera Fermat's bevis? Det kan mycket väl hända, att Fermat's bevis innehöll något fel, som visserligen inte kullkastar satsen men som gör att det korrekta beviset måhända inte är så enkelt och underbart som Fermat trodde.

Ett stort genombrott skedde sommaren 1983, då en ung tysk matematikprofessor, *Gerd Faltings*, bevisade Mordells förmodan. En konsekvens av denna förmodan (som egentligen handlar om vissa algebraiska kurvor) är nämligen följande sats.

Sats 10.6. *Om ekvationen* (10.10) *har någon heltalslösning* x, y, z *för* $n \geq 3$, *så existerar det endast ett ändligt antal sådana lösningar.*

Vid en ytlig betraktelse kan det måhända förefalla ovidkommande, om ekvationen (10.10) har ett ändligt eller oändligt antal lösningar, när Fermat själv påstod att den saknar lösningar. Men i matematiken betyder steget mellan oändligt och ändligt, att problemet s.a.s. har förts ned på ett helt nytt plan. Därför måste Faltings bevis av Mordells förmodan betraktas som ett stort genombrott ifråga om Fermat's stora sats. För denna bedrift fick Faltings år 1986 Fields-medaljen, av många kallad "matematikens nobelpris". Många tror nu att det slutliga beviset kan komma inom en nära framtid.

Övningsuppgifter

Uppgift 10.1 Bestäm a) alla primitiva, b) alla pytagoreiska tripplar x, y, z för vilka $z \leq 50$.

Uppgift 10.2 Visa att varje pytagoreisk trippel x, y, z med $z = y + 1$ är av formen $x = 2n + 1$, $y = 2n(n + 1)$, $z = 2n(n + 1) + 1$ $(n \in Z_+)$. Bestäm alla sådana tripplar, för vilka $z < 100$.

Uppgift 10.3 Visa att om x, y, z är en primitiv pytagoreisk trippel, så är antingen x eller y delbart med 3.

Uppgift 10.4 Visa att om x, y, z är en primitiv pytagoreisk trippel, så är exakt ett av talen x, y och z delbart med 5.

Uppgift 10.5 Fermat bevisade att det inte existerar någon rätvinklig triangel med heltaliga sidor, vars yta är en jämn kvadrat, eller m.a.o. att ekvationssystemet $x^2 + y^2 = z^2$, $u^2 = xy/2$ saknar positiva heltalslösningar. Visa att detta medför att ekvationen (10.10) saknar positiva heltalslösningar för $n = 4$. (Ledning: Antag att vi skulle ha $x^4 + y^4 = z^4$ för heltaliga x, y, z och sätt $a = y^4$, $b = 2x^2z^2$, $c = x^4 + z^4$, $d = xy^2z$).

Uppgift 10.6 Visa att en pytagoreisk trippel inte kan satisfiera ekvationen (10.10) för $n \geq 3$.

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331

Tabell 2. Primtalen ≤ 3331. (Tabellen är lånad från [9]).

$p = 3$

0	1	2
N	0	1	2
0		0	1

$p = 5$

0	1	2	4	3
N	0	1	2	3	4
0		0	1	3	2

$p = 7$

0	1	3	2	6	4	5
N	0	1	2	3	4	5	6
0		0	2	1	4	5	3

$p = 11$

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

$p = 13$

0	1	2	4	8	3	6	12	11	9	5
1	10	7								
N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

$p = 17$

0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				
N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

$p = 19$

0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		
N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

$p = 23$

0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								
N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

$p = 29$

0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		
N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

$p = 31$

0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21
N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

Tabell 3. Indextabell för alla udda primtalsmoduler $p \leq 31$. Basen är alltid den minsta primitiva roten till p. Tabellen används på följande sätt: Antag t.ex. att man söker index för talet 16 modulo 29. Man går då in i tabellen $p = 29$ och tar den första siffran 1 ur kolumnen längst till vänster (nedre halvan). Den andra siffran 6 tas ur den mellersta raden N. Där ettans rad och sexans kolumn skär varandra, får man det sökta indexet 4. Således $\text{ind}\, 16 = 4$. Om man söker det tal, som har ett givet index, förfar man på samma sätt med den skillnaden att man nu tar den första siffran i indexet ur *övre halvan* av kolumnen längst till vänster. Exempelvis gäller för $p = 29$: Om $\text{ind}\, x = 18$, så är $x = 13$. Basen är f.ö. alltid det tal, vars index = 1, i detta fall 2. (Tabellen är lånad från [10]).

Litteraturhänvisningar

Nedan anges de källor, till vilka vi hänvisat i texten med beteckningen [ ].

[1] B. Sjöberg: Inledning till den högre analysen, kompendium utgivet av Sigma vid Åbo Akademi, 1985.

[2] T. Nagell: Elementär talteori, Almqvist & Wiksell, Uppsala 1950.

[3] J.B. Rosser & L. Schoenfeld: Approximate formulas for some functions of prime numbers, Illinois journal of mathematics, vol.6 (1962), sid. 64–94.

[4] Bra Böckers lexikon, band 20, Bokförlaget Bra Böcker, Höganäs 1981.

[5] C.B. Boyer: A History of Mathematics, John Wiley & Sons, New York 1968.

[6] W. Diffie and M. Hellman: New directions in cryptography, IEEE Transactions on Information Theory, IT-22 (1976), sid. 644–654.

[7] A. Salomaa: Public-Key Cryptography, Springer-Verlag, Berlin Heidelberg 1990.

[8] M. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, ACM Communications 21 (1978), sid. 120–126.

[9] D.E. Flath: Introduction to Number Theory, John Wiley & Sons, New York 1989.

[10] W.J. LeVeque: Fundamentals of Number Theory, Addison-Wesley Publishing Company, Reading, Massachusetts 1977.

Övrig använd litteratur

K.H. Rosen: Elementary Number Theory and Its Applications, Addison-Wesley Publishing Company, Reading, Massachusetts 1984.

K. Väisälä: Lukuteorian ja korkeamman algebran alkeet, Otava, Helsinki 1950.

H. Riesel: En bok om primtal, Studentlitteratur 1968.

K. Devlin: Mathematics: The Golden Age, Penguin Books, London 1988.

P. Ribenboim: 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York Heidelberg Berlin 1979.