Avsnitt 4

RESTARITMETIKER

När man adderar eller multiplicerar två tal som t ex

$$\begin{array}{rr} & 128 \\ + & 39 \\ \hline & ..7 \end{array} \qquad\qquad \begin{array}{rr} & 128 \\ \times & 43 \\ \hline & ..4 \end{array}$$

så bestämmer man först den sista siffran. De operationer som leder till resultatet kallas addition och multiplikation modulo 10. Man adderar $8+9$ på vanligt sätt, men sista siffran är resten av $8+9$ vid division med 10. På liknande sätt har vi $3 \cdot 8 = 24$, men som sista siffran får vi 4 dvs resten av 24 vid division med 10. Om talen är givna i binära systemet (bas 2) som t ex

$$\begin{array}{rr} & 1011 \\ + & 101 \\ \hline & \ldots 0 \end{array} \qquad\qquad \begin{array}{rr} & 1011 \\ \times & 111 \\ \hline & \ldots 1 \end{array}$$

så räknar man modulo 2 dvs först som vanligt, men därefter tar man resten vid division med 2. Operationerna modulo 10 eller 2 eller modulo ett godtyckligt annat naturligt tal har stor betydelse inom talteorin och dess tillämpningar i datalogi och datateknik.

I restaritmetiker arbetar man med rester av heltal vid division med ett fixerat naturligt tal n. Vi skall förutsätta att $n > 1$, ty annars har vi bara resten 0. Om a är ett heltal så är

$$a = nq + r,$$

där q är kvoten och r är resten. Resten r kan alltid väljas så att $0 \leq r < n$ dvs det finns n stycken rester : $0, 1, ..., n-1$. Mängden av dessa betecknas ofta med $\mathbb{Z}_n$ (eller $\mathbb{Z}/(n)$). Alltså är $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. T ex $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ osv.

Vi skall skriva $r = [a]_n$ för att uttrycka det faktum att r är resten vid division av a med n. T ex är $3 = [8]_5$ (dvs resten av 8 vid division med 5 är lika med 3), $5 = [38]_{11}$ (ty $38 = 11 \cdot 3 + 5$), $4 = [-11]_5$ (ty $-11 = 5(-3) + 4$). Följande viktiga egenskap hos rester kommer att utnyttjas många gånger:

(4.1) Lemma. *$[a]_n = [b]_n$ då och endast då $n|a - b$ *. Med andra ord ger a och b samma rest vid division med n då och endast då n är en delare till deras skillnad $a - b$.*

Bevis. Om $[a]_n = [b]_n$ så är $a = nq_1 + r$ och $b = nq_2 + r$, vilket ger $a - b = n(q_1 - q_2)$ dvs $n|a - b$.

Omvänt, låt $n|a - b$ dvs $a - b = nq$. Om $a = nq_1 + r_1$ och $b = nq_2 + r_2$ så är

$$a - b = n(q_1 - q_2) + r_1 - r_2$$

dvs

$$r_1 - r_2 = (a - b) - n(q_1 - q_2) = n[q - (q_1 - q_2)].$$

Detta betyder att $n|r_1 - r_2$. Men $0 \leq r_1, r_2 < n$ så att $r_1 - r_2$ är delbart med n endast om $r_1 - r_2 = 0$ dvs $[a]_n = [b]_n$. □

(4.2) Exempel. (a) $[3]_5 = [-2]_5$ ty $5|3 - (-2) = 5$.
(b) $[n - 1]_n = [-1]_n$ ty $n|(n - 1) - (-1) = n$. □

(4.3) Anmärkning. C.F. Gauss introducerade en mycket viktig beteckning för att uttrycka likheten $[a]_n = [b]_n$ (dvs $n|a - b$). Han skrev:

$$a \equiv b \pmod{n}$$

vilket utläses "a **är kongruent med** b **modulo** n". Relationen " $\equiv$ " kallas **kongruens** (här modulo n). Vi kommer att använda den beteckningen ganska ofta. □

Kan man helt allmänt addera och multiplicera rester (precis som de sista siffrorna vid addition och multiplikation av heltal)? Det är helt klart att det går men en formell definition är nödvändig. Vi skall skriva $\oplus$ och $\odot$ för att ha en distinktion mellan addition av vanliga heltal och rester. Men den distinktionen är inte nödvändig (man kan skriva " $+$ " och " $\cdot$ " om man så vill).

(4.4) Definition. $[a]_n \oplus [b]_n = [a + b]_n$ och $[a]_n \odot [b]_n = [ab]_n$. □

*Man skriver $d|a$ och säger att "d är en delare till a om $a = dq$ för något heltal q. Man säger också att a är en multipel av d. Om d inte är en delare till a skriver man $d \nmid b$.

Definitionen säger att summan av resterna $[a]_n$ och $[b]_n$ får man genom att addera talen a och b på vanligt sätt och därefter ta resten vid division av $a+b$ med n. Samma sak gäller för produkten. Här finns det dock en liten detalj som kräver en stunds eftertanke. Om man har två helt godtyckliga heltal a och b som slutar, låt oss säga, på 3 och 8 dvs $[a]_{10}=3$ och $[b]_{10}=8$ så får man alltid samma slutsiffra för $a+b$ och ab dvs $[a+b]_{10}=1$ och $[ab]_{10}=4$. Gäller samma sak helt allmänt då man ersätter 10 med någon annan modul t ex 3 eller 4? Med andra ord är höger led i definitionen (4.4) alltid samma oberoende av a och b till vänster? Frågan kan också formuleras så här: är definitionen (4.4) korrekt? Låt oss kontrollera att den är helt korrekt! Låt:

$$[a]_n=[a']_n \text{ och } [b]_n=[b']_n. \tag{4.5}$$

Vi vill visa att

$$[a+b]_n=[a'+b']_n \quad \text{och} \quad [ab]_n=[a'b']_n. \tag{4.6}$$

Med beteckningen " $\equiv$ " betyder det att

$$a\equiv a' \pmod n \text{ och } b\equiv b' \pmod n$$

ger

$$a+b\equiv a'+b' \pmod n \quad \text{och} \quad ab\equiv a'b' \pmod n$$

dvs *kongruenser, precis som likheter, kan adderas och multipliceras ledvis.* I synnerhet gäller att om $a\equiv b \pmod n$ så är $a^2\equiv b^2 \pmod n$, och mera allmänt, $a^k\equiv b^k \pmod n$ för varje naturlig exponent k dvs *kongruenser kan exponentieras ledvis.*

Bevis. $[a]_n=[a']_n$ och $[b]_n=[b']_n$ betyder att $a-a'=nq_1$ och $b-b'=nq_2$. Alltså är

$$(a+b)-(a'+b')=n(q_1+q_2)\ ,$$

dvs

$$[a+b]_n=[a'+b']_n\,.$$

Vidare är

$$ab - a'b' = (a - a')b + a'(b - b') = n(q_1 b + q_2 a')$$

dvs

$$[ab]_n = [a'b']_n.$$

□

Nu kan vi konstatera följande:

(4.7) Sats. *Alla rester vid division med n kan adderas och multipliceras i enlighet med följande formler:*

$$[a]_n \oplus [b]_n = [a + b]_n$$

och

$$[a]_n \odot [b]_n = [ab]_n.$$

Både addition och multiplikation är associativa och kommutativa. Dessutom är multiplikation distributiv med avseende på addition.

Bevis. Vi vet redan att summan och produkten av rester är rester. Associativiteten för addition:

$$([a]_n \oplus [b]_n) \oplus [c]_n = [a]_n \oplus ([b]_n \oplus [c]_n)$$

får vi enkelt ty

$$VL = ([a]_n \oplus [b]_n) \oplus [c]_n = [a + b]_n \oplus [c]_n = [(a + b) + c]_n,$$

och

$$HL = [a]_n \oplus ([b]_n \oplus [c]_n) = [a]_n \oplus [b + c]_n = [a + (b + c)]_n,$$

så att $VL = HL$. Lika enkelt är det med kommutativiteten av addition:

$$[a]_n \oplus [b]_n = [a+b]_n = [b+a]_n = [b]_n \oplus [a]_n.$$

På liknande sätt kontrollerar vi att multiplikation av rester är både associativ och kommutativ (man ersätter bara $\oplus$ med $\odot$ ovan). Den distributiva lagen

$$[a]_n \odot ([b]_n \oplus [c]_n) = [a]_n \odot [b]_n \oplus [a]_n \odot [c]_n$$

får vi utan svårigheter:

$$VL = [a]_n \odot ([b]_n \oplus [c]_n) = [a]_n \odot [b+c]_n = [ab+ac]_n$$

och

$$HL = [a]_n \odot [b]_n \oplus [a]_n \odot [c]_n = [ab]_n \oplus [ac]_n = [ab+ac]_n$$

dvs $VL = HL$ □

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ med addition och multiplikation av rester kallas ofta för **restaritmetiken modulo** n eller **restringen modulo** n.

Låt oss som exempel skriva ut additions och multiplikationstabellerna för restringen $\mathbf{Z}_3$:

$\oplus$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\odot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

Ofta kommer vi att utelämna $[\ ]_n$ när det är klart vilka rester vi menar. T ex är tabellerna för restringen $\mathbb{Z}_4$ följande:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

I praktiska tillämpningar (utanför matematiken) är $\mathbb{Z}_2$ en av de viktigaste ringarna: Den har följande räknelagar:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

En viktig fråga är när det inträffar att en rest i $\mathbb{Z}_n$ har **invers**. Detta betyder att för en rest $r \in \mathbb{Z}_n$ finns det en rest $s \in \mathbb{Z}_n$ så att $r \odot s = 1$. Resten s betecknas ofta som r^{-1}.

Låt oss betrakta några exempel. I $\mathbb{Z}_5$ har vi $1 \odot 1 = 1$, $2 \odot 3 = 1$ och $4 \odot 4 = 1$ så att 1,2,3 och 4 har invers (1 och 4 är sina egna inverser, medan 2 och 3 är varandras inverser). I $\mathbb{Z}_3$ har vi $1 \odot 1 = 1$ och $2 \odot 2 = 1$ så att både 1 och 2 har invers. I $\mathbb{Z}_4$ har både 1 och 3 invers ty $1 \odot 1 = 1$ och $3 \odot 3 = 1$. Resten 2 i $\mathbb{Z}_4$ saknar invers därför att om $2 \odot s = 1$ så kan vi multiplicera bägge leden med 2 och vi får $2 \odot 2 \odot s = 2$ dvs $0 = 2$ (vi har $4 = 0$ i $\mathbb{Z}_4$). Man säger att $\mathbb{Z}_n$ är en **kropp** om varje nollskild rest $r \in \mathbb{Z}_n$ har en invers r^{-1}. Som vi har sett är $\mathbb{Z}_3$ och $\mathbb{Z}_5$ kroppar, medan $\mathbb{Z}_4$ är inte en kropp. Vad är det som gör att $\mathbb{Z}_n$ är en kropp? Svaret är ganska överraskande: $\mathbb{Z}_n$ är en kropp då och endast då n är ett primtal. Vi skall bevisa det om en stund.

Låt oss betrakta några ytterligare exempel. I $\mathbb{Z}_7$ har alla rester $\neq 0$ inverser ty 7 är ett primtal och således är $\mathbb{Z}_7$ en kropp: $1 \odot 1 = 1$, $2 \odot 4 = 1$, $3 \odot 5 = 1$, $6 \odot 6 = 1$. Det är också så i den enklaste kroppen: $\mathbb{Z}_2 = \{0, 1\}$ – resten 1 är självklart sin egen invers. Nu är det också klart varför $\mathbb{Z}_4$ inte är en kropp (2 saknar invers) – 4 är inte ett primtal. Kropparna $\mathbb{Z}_p$ för olika primtal p har många viktiga tillämpningar både i talteori och i olika praktiska sammanhang i samband med kodning och kryptering. Vi skall bevisa en mera allmän sats om inverser som gäller i alla restringar $\mathbb{Z}_n$:

(4.8) Sats. *$r \in \mathbb{Z}_n$ har invers då och endast då r och n är relativt prima dvs* $\mathrm{SGD}(r, n) = 1$.

Vårt bevis av satsen utnyttjar en mycket viktig egenskap som Du kommer att möta många gånger: Låt a, b vara två heltal. Då finns det heltal x, y sådana att

$$ax + by = SGD(a, b)^{\dagger}. \tag{4.9}$$

Bevis. Om $SGD(r, n) = 1$ så finns det två heltal x, y sådana att

$$rx + ny = 1$$

Alltså är $[rx + ny]_n = [1]_n$. Men $[ny]_n = [0]_n$ så att $[rx]_n = [r]_n \odot [x]_n = [1]_n$ dvs $s = [x]_n$ är inversen till $[r]_n = r$.

Omvänt. Låt $[r]_n \odot [s]_n = [1]_n$ dvs $[rs]_n = [1]_n$. Enligt (4.1) får vi $n | rs - 1$ dvs $rs - 1 = nq$ så att $rs - nq = 1$. Den likheten säger att $SGD(r, n) = 1$ ty en gemensam delare $d > 0$ till r och n är en delare till 1 dvs $d = 1$. □

[†]Denna likhet är en mycket enkel konsekvens av Euklides algoritm. Se avsnittet om "Delbarhet och primtal".

Nu får vi omedelbart:

(4.10) Följdsats. *$\mathbb{Z}_n$ är en kropp då och endast då n är ett primtal.*

Bevis. Om $n = p$ är ett primtal så har varje rest $r \neq 0$ invers därför att resterna $1, 2, ..., p-1$ i $\mathbb{Z}_p$ saknar gemensamma delare med p dvs $SGD(r, p) = 1$ då $r = 1, 2, ..., p-1$. Om däremot n är sammansatt dvs $n = kl$, där $1 < k < n$ och $1 < l < n$ så är $SGD(k, n) = k > 1$, vilket innebär att resten k saknar invers enligt (4.8). □

Nu skall vi gå igenom några mycket berömda satser i talteorin som enkelt kan bevisas med hjälp av restaritmetiker. På senare år visade det sig att dessa satser har mycket väsentliga tillämpningar i samband med datorberäkningar och datasäkerhet. Men talteori (fast lite mer avancerad) har också kommit in i teoretisk fysik i samband med strängteorin.

Vi skall börja med en sats som visades redan år 1682 av G.W. Leibniz [‡], men som kallas Wilsons sats. John Wilson levde senare än Leibniz och lämnade matematiken för juridik.

(4.11) Wilson's sats. *Om p är ett primtal så är $p|(p-1)! + 1$.*[§]

Innan vi bevisar satsen låt oss betrakta ett exempel. Tag $p = 13$. Satsen säger att $13|12! + 1$. Modulo 13 har vi

$$1 \odot 1 = 1,\ 2 \odot 7 = 1,\ 3 \odot 9 = 1,\ 4 \odot 10 = 1,\ 5 \odot 8 = 1,\ 6 \odot 11 = 1,\ 12 \odot 12 = 1.$$

Alltså är (modulo 13):

$$1 \odot 2 \odot 3 \odot 4 \odot 5 \odot 6 \odot 7 \odot 8 \odot 9 \odot 10 \odot 11 \odot 12 =$$
$$= 1 \odot (2 \odot 7) \odot (3 \odot 9) \odot (4 \odot 10) \odot (5 \odot 8) \odot (6 \odot 11) \odot 12 = 12 = -1$$

dvs $13|12! + 1$.

Bevis. Betrakta kroppen $\mathbb{Z}_p$. Vi skall beräkna $[(p-1)!]_p = [1 \cdot 2 \cdot ... \cdot (p-1)]_p$ och visa att $[(p-1)!]_p = [-1]_p$ vilket just är satsens innehåll.

Varje faktor r i produkten $1 \odot 2 \odot ... \odot (p-1)$ har sin invers s modulo p dvs $r \odot s = 1$. Om $r \neq s$ så kan man utelämna både r och s. Men det kan inträffa att $r = s$ dvs $r \odot r = 1$. När? Vi har $[r^2]_p = [1]_p$ då och endast då $p|r^2 - 1 = (r-1)(r+1)$ dvs $p|r-1$ eller $p|r+1$. Men

[‡]Gottfrid Wilhelm Leibniz (1/7 1646 – 14/11 1716) var en framstående tysk matematiker som skapade differential och integralkalkylen (oberoende av I.Newton).

[§]$n! = 1 \cdot 2 \cdot 3 \cdots n$, vilket utläses "$n$ fakultet"

$0 \leq r \leq p-1$ så att $r = 1$ eller $r = p-1$. Alltså finns det två faktorer i produkten $1 \odot 2 \odot ... \odot (p-1)$ som är kvar: 1 och $p-1$ dvs

$$1 \odot 2 \odot ... \odot (p-1) = 1 \odot (p-1) \ .$$

Men $p - 1 \equiv -1 \pmod{p}$ så att $[(p-1)!]_p = [-1]_p$, vilket visar satsen. □

(4.12) Anmärkning. Wilsons sats karakteriserar primtalen i den meningen att om $n|(n-1)!+1$ så är n ett primtal (vi lämnar detta påstående som en bra och enkel övning – se övning 5). Man kan testa med hjälp av datorer om n är ett primtal genom att dividera $(n-1)!+1$ med n. Men den metoden är inte särskilt bra därför att $(n-1)!$ växer mycket snabbt med n. □

Nu vill vi visa en av de mest berömda satserna inom talteorin – Fermats [¶] lilla sats (om den stora får du höra under föreläsningarna). Innan vi formulerar och bevisar satsen låt oss notera en enkel egenskap hos rester r i $\mathbb{Z}_n$ som har invers s dvs $r \odot s = 1$. Låt $x, y \in \mathbb{Z}_n$. Då gäller

$$x \odot r = y \odot r \Rightarrow x = y. \tag{4.13}$$

I själva verket ger likheten $x \odot r = y \odot r$ att $x \odot r \odot s = y \odot r \odot s$ dvs $x = y$ (ty $r \odot s = 1$). Vi kan säga att en likhet i $\mathbb{Z}_n$ kan delas ledvis med en rest som har invers. Notera också att om r_1 och r_2 har invers så har också $r_1 \odot r_2$ invers ty $r_1 \odot s_1 = 1$ och $r_2 \odot s_2 = 1$ ger $r_1 \odot r_2 \odot s_1 \odot s_2 = 1$.

(4.14) Fermats lilla sats. *Om p är ett primtal och a är ett heltal så är $p|a^p - a$, med andra ord, $a^p \equiv a \pmod{p}$.*

Tag ett exempel först. Om $p = 5$ och $a = 3$ får vi $5|3^5 - 3 = 240$.

Bevis. Om $p|a$ så är påståendet klart. Låt oss anta då att $p \nmid a$ dvs $r = [a]_p \neq 0$. Låt s beteckna inversen till r. Betrakta resterna $1, 2, ..., p-1 \in Z_p$ och låt oss multiplicera alla dessa rester med $r \neq 0$. Då får vi $(p-1)$ olika rester i Z_p:

$$1 \odot r,\ 2 \odot r, ..., (p-1) \odot r$$

I själva verket måste alla dessa produkter vara olika eftersom om $i \odot r = j \odot r$ så är $i = j$ (se (4.13)). Alltså återfår vi resterna $1, 2, ..., p-1$ (eventuellt i någon annan ordning). I varje fall är

[¶] Pierre de Fermat (20/8 1601 – 12/1 1663).

$$1 \odot r \odot 2 \odot r \odot ... \ \odot (p-1) \odot r = 1 \odot 2 \odot ... \ \odot (p-1).$$

Nu kan vi stryka $1, 2, ..., p-1$ till vänster och till höger (vi kan multiplicera varje rest till höger och till vänster med dess invers) och vi får

$$r^{p-1} = 1$$

dvs

$$[a^{p-1}]_p = [1]_p,$$

vilket betyder att $p|a^{p-1} - 1$. Men i så fall är också $p|a(a^{p-1} - 1) = a^p - a$. □

(4.15) Anmärkning. Observera att beviset ger att $a^{p-1} \equiv 1 \pmod{p}$ om $p \nmid a$. Detta påstående förekommer ofta som formulering av Fermats lilla sats. □

Fermats lilla sats har en generalisering som visades 100 år senare av L. Euler [‖]. (Eulers sats utgör grunden för konstruktionen av de mest använda krypteringssystemen inom datasäkerhetstekniken — så kallade RSA-krypton. Se övningarna). Innan vi visar Eulers sats[**] måste vi säga några ord om Eulers funktion φ.

Hur många rester i $\mathbb{Z}_n$ har invers? Antalet sådana rester betecknas med $\varphi(n)$. Funktionen $\varphi(n)$ kallas Eulers funktion. Enligt villkoret i (4.8) har vi:

$$\varphi(n) = \text{antalet } r \text{ sådana att } 0 \leq r < n \text{ och } SGD(r, n) = 1. \tag{4.16}$$

Det är lätt att beräkna: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$ osv. Vi återkommer till Eulers funktion i samband med övningarna. Nu kan vi formulera och bevisa Eulers sats:

(4.17) Eulers sats. *Låt a och n vara heltal sådana att $SGD(a, n) = 1$. Då är*

$$n|a^{\varphi(n)} - 1,$$

dvs $a^{\varphi(n)} \equiv 1 \pmod{n}$.

[‖] Leonard Euler (15/4 1707 - 18/9 1783), schweizisk matematiker, den störste matematikern under 1700-talet och en av de mest betydelsefulla i matematikens historia.

[**] Du behöver inte läsa efterföljande texten om Du inte är intresserad av den övning som handlar om tillämpningar av restringar på kryptering.

Först ett exempel. Om $n = 10$ och $a = 3$ så är $10|3^4 - 1 = 80$ (ty $\varphi(10) = 4$).

Bevis. Betrakta restringen $\mathbb{Z}_n$. Enligt förutsättningen har $r = [a]_n \neq 0$ en invers i $\mathbb{Z}_n$ (ty $SGD(a, n) = 1$). Låt $r_1, r_2, ..., r_{\varphi(n)}$ vara alla rester som har invers i $\mathbb{Z}_n$, och låt oss multiplicera alla dem med r. Då får vi $\varphi(n)$ olika produkter (se (4.13)):

$$r \odot r_1,\ r \odot r_2, \ldots,\ r \odot r_{\varphi(n)}.$$

Alltså får vi alla rester i $\mathbb{Z}_n$ som har invers igen (möjligen i en annan ordning). I varje fall är

$$r \odot r_1 \odot r \odot r_2 \odot \ldots.\ \odot r \odot r_{\varphi(n)} = r_1 \odot r_2 \odot \ldots.\ \odot r_{\varphi(n)}.$$

Nu kan vi stryka $r_1, r_2, ..., r_{\varphi(n)}$ till vänster och till höger (vi kan) och vi får

$$r^{\varphi(n)} = 1$$

dvs

$$[a^{\varphi(n)}]_n = [1]_n$$

vilket betyder att $n|a^{\varphi(n)} - 1$. □

Vi skall avsluta detta avsnitt med ännu en berömd sats som är ca 2000 år gammal. Satsen heter Kinesiska restsatsen och säger följande:

(4.18) Kinesiska restsatsen. *Om $n_1, n_2, ..., n_k$ är parvis relativt prima heltal (dvs den största gemensamma delaren till n_i och n_j är 1 då $i \neq j$) och $r_1, r_2, ..., r_k$ är godtyckliga heltal så existerar ett heltal x sådant att*

$$x \equiv r_1 \pmod{n_1},\ \ x \equiv r_2 \pmod{n_2},\ \ldots,\ x \equiv r_k \pmod{n_k}.$$

Dessutom finns det bara ett sådant x modulo $n_1 n_2 \cdots n_k$ (dvs ett x med $0 \leq x < n_1 n_2 \cdots n_k$).

Betrakta ett exempel. Om vi vill hitta x så att x lämnar resten 2 vid division med 3, resten 3 vid division med 4 och resten 4 vid division med 5 så betyder det att x skall uppfylla

$$x \equiv 2 \pmod{3},\ \ x \equiv 3 \pmod{4},\ \ x \equiv 4 \pmod{5}. \tag{4.19}$$

Här är $x = 59$ den enda lösningen modulo $60 = 3 \cdot 4 \cdot 5$. Vårt bevis ger också information om hur man hittar x (se exempel (4.22)).

Bevis. Låt $n = n_1 n_2 ... n_k$. Betrakta $\mathbb{Z}_{n_i}$. Enligt förutsättningen har vi $SGD(n_i, \frac{n}{n_i}) = 1$. Därför har $\frac{n}{n_i}$ en invers modulo n_i dvs det finns $x_i \in \mathbb{Z}_n$ så att

$$\left[\frac{n}{n_i} x_i\right]_{n_i} = [1]_{n_i},$$

eller med andra ord,

$$\frac{n}{n_i} x_i \equiv 1 \pmod{n_i}.$$

Nu påstår vi att

$$x = \frac{n}{n_1} x_1 r_1 + \frac{n}{n_2} x_2 r_2 + \ldots + \frac{n}{n_k} x_k r_k \tag{4.20}$$

är den sökta lösningen. För att kontrollera det, observera först att

$$\left[\frac{n}{n_i} x_i\right]_{n_j} = 0 \text{ då } i \neq j,$$

ty $n_j | \frac{n}{n_i}$. Därför har vi:

$$[x]_{n_i} = \left[\frac{n}{n_1} x_1 r_1\right]_{n_i} + \left[\frac{n}{n_i} x_2 r_2\right]_{n_i} + \ldots + \left[\frac{n}{n_k} x_k r_k\right]_{n_i} = \left[\frac{n}{n_i} x_i r_i\right]_{n_i} = [r_i]_{n_i}$$

dvs $x \equiv r_i \pmod{n_i}$

Om x och x' är två lösningar dvs $[x]_{n_i} = [x']_{n_i}$ då $i = 1, 2, ..., k$ så är $n_i | x - x'$. Men talen $n_1, n_2, ..., n_k$ är relativt prima så att $n = n_1 n_2 ... n_k | x - x'$[††] dvs $[x]_n = [x']_n$. □

Hur hittar man x rent praktiskt? Det är klart att man behöver x_i dvs man måste lösa

$$\frac{n}{n_i} x_i \equiv 1 \pmod{n_i}. \tag{4.21}$$

Detta betyder att man vill finna tal x_i sådana att $\frac{n}{n_i} x_i - 1 = n_i q$ dvs

[††]Om $a|c$ och $b|c$ samt $SGD(a, b) = 1$ så $ab|c$ – se avsnitt "Delbarhet och primtal"

$$\frac{n}{n_i}x_i - n_i q = 1.$$

Här känner vi igen (4.9) med $a = \frac{n}{n_i}$, $b = n_i$, $x = x_i$ och $y = -q$. x_i hittar man mycket enkelt med hjälp av Euklides algoritm.

(4.22) Exempel. Vi återkommer till (4.19) där $n_1 = 3, n_2 = 4, n_3 = 5$ och $r_1 = 2, r_2 = 3, r_3 = 4$. Alltså är $n = n_1 n_2 n_3 = 60$ och man måste lösa kongruenserna (4.21) dvs

$$20x_1 \equiv 1 \pmod 3, \quad 15x_2 \equiv 1 \pmod 4, \quad 12x_3 \equiv 1 \pmod 5.$$

Man hittar mycket lätt (utan Euklides algoritm) att $x_1 = 2, x_2 = 3, x_3 = 3$. Alltså är

$$x = \frac{n}{n_1}x_1 r_1 + \frac{n}{n_2}x_2 r_2 + \frac{n}{n_3}x_3 r_3 = 359$$

så att den enda lösningen modulo 60 är 59, ty $359 \equiv 59 \pmod{60}$. □

Exempel: RSA-krypteringssystem[‡‡]. En person som brukar kallas Alice, vilket förkortas till A, vill ta emot meddelanden. Hon väljer två stycken mycket stora primtal p och q (vanligen med c:a 150 siffror). Primtalen är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, \ldots$$

dvs positiva heltal som saknar delare större än 1 och mindre än talet självt. Alice räknar därefter $N = pq$ och dessutom väljer ett heltal e som inte delar $p-1$ och $q-1$. Hon publicerar N och e som är krypteringsnyckeln, men behåller hemligt både p och q. Hon publicerar också en "ordbok" som säger att A skall översättas till t ex 10, B till 11, C till 12, osv. Alice måste också beräkna sin dekrypteringsnyckeln som hon behåller för sig själv. Denna nyckeln är ett tal d sådant att ed skall ge resten 1 vid division med både $p-1$ och $q-1$. Det är mycket lätt att beräkna d och flera datorprogram gör sådana beräkningar ögonblickligt.

Låt oss anta nu att en annan person, som vi kallar Bo och förkortar till B, vill skicka ett meddelande x till A. Bo räknar ut resten vid division av x^e med N och skickar till Alice.

Alice räknar då resten vid division av $(x^e)^d$ med N och får tillbaka meddelandet x dvs $(x^e)^d = x$. Eulers sats garanterar att $(x^e)^d = x$ dvs garanterar att Alice kan förvandla den krypterade texten i klartext (se nedan).

Låt oss betrakta ett mycket konkret exempel.

[‡‡]Konstruktionen av systemet publicerades av R.L.Rivest, A.Shamir och L.Adleman 1978.

- Alice väljer $\mathbf{p{=}61, q{=}101}$ så $\mathbf{N{=}pq{=}61 \cdot 101{=}6161}$.
- Alice väljer t ex $\mathbf{e{=}17}$ som inte delar $\mathbf{p-1=60}$ och $\mathbf{q-1=100}$.
- Alice räknar ut $\mathbf{d}$ så att $\mathbf{ed}$ ger resten 1 vid division med $\mathbf{p-1=60}$ och $\mathbf{q-1=100}$. Hon kan välja $\mathbf{d=353}$ ty $\mathbf{ed=17 \cdot 353=6001}$ ger resten 1 vid dessa divisioner.
- Alice publicerar $\mathbf{N{=}6161, e{=}17}$ (och en "ordbok" t ex A = 10, B = 11, C = 12, D = 13, E = 14, ..., I =18, ..., K = 20,..., M = 22, ..., T = 29,..., Z = 35). Primtalen $\mathbf{p, q}$ och $\mathbf{d}$ är hemliga.

Kryptera: MATEMATIK

MA = 2210 $\longmapsto$ $[\mathbf{2210^{17}}]_{\mathbf{6161}}{=}\mathbf{4013}$

TE = 2914 $\longmapsto$ $[\mathbf{2914^{17}}]_{\mathbf{6161}}{=}\mathbf{135}$

MA = 2210 $\longmapsto$ $[\mathbf{2210^{17}}]_{\mathbf{6161}}{=}\mathbf{4013}$

TI = 2918 $\longmapsto$ $[\mathbf{2918^{17}}]_{\mathbf{6161}}{=}\mathbf{1527}$

K = 20 $\longmapsto$ $[\mathbf{20^{17}}]_{\mathbf{6161}}{=}\mathbf{4487}$

Dekryptera: 4013 135 4013 1527 4487

4013 $\longmapsto$ $[\mathbf{4013^{353}}]_{\mathbf{6161}}{=}\mathbf{2210}$ = MA

135 $\longmapsto$ $[\mathbf{135^{353}}]_{\mathbf{6161}}{=}\mathbf{2914}$ = TE

4013 $\longmapsto$ $[\mathbf{4013^{353}}]_{\mathbf{6161}}{=}\mathbf{2210}$ = MA

1527 $\longmapsto$ $[\mathbf{1527^{353}}]_{\mathbf{6161}}{=}\mathbf{2918}$ = TI

2487 $\longmapsto$ $[\mathbf{4487^{353}}]_{\mathbf{6161}}{=}\mathbf{20}$ = K

Varför är RSA–metoden så effektiv att den används mycket flitigt i moderna kommunikationssystem? Svaret är att det är mycket svårt och idag inte möjligt att beräkna d då N och e är kända (om talen p och q är tillräckligt stora) . ed skall ge resten 1 vid division med både $p-1$ och $q-1$. Om man känner till dessa två tal är det mycket lätt att beräkna d. För att komma åt $p-1$ och $q-1$ måste man känna till p och q. Man utgår ifrån att dessa två tal endast kan beräknas om man kan uppdela talet $N=pq$ i dess primfaktorer p och q. Denna beräkning dvs uppdelning av N i primfaktorer är mycket komplicerad och tar mycket lång tid. De bästa kända metoderna kräver c:a $\sqrt[5]{N}$ räkneoperationer. Om t ex p och q har 100 siffror så har N c:a 200 siffror och antalet räkneoperationer som behövs för att

faktoruppdela talet N är 10^{40}. Om man antar att en räkneoperation tar $1\mu s$ så krävs det $10^{40}\mu s \approx 3 \cdot 10^{26}$ år för att genomföra beräkningarna för N (10^6 datorer var och en kapabel att utföra en räkneoperation på $1\mu s$ skulle behöva $3 \cdot 10^{26}$ år för dessa beräkningar). Trots det betraktas idag val av primtal med 100 siffror som inte helt säkra och man väljer snarare primtal med 150.

Slutligen formulerar vi några övningar som förklarar varför RSA-kryptering fungerar.

(a) Välj två olika primtal p, q och beräkna $N = pq$ (p, q är vanligen mycket stora, säg, av storleksordningen 10^{100}).

(b) Beräkna $\varphi(N) = (p-1)(q-1)$ och välj e så att $SGD(e, \varphi(N)) = 1$. Beräkna även d, så att $ed \equiv 1 \pmod{\varphi(N)}$.

(c) Publicera N, e och en ordbok för översättning av meddelanden till exempel:

$$A = 10,\ B = 11, ...,\ Z = 35$$

(då $n > 35$)

(d) Den som vill sända meddelanden till Dig krypterar med hjälp av den kända funktionen

$$E(r) = r^e,\ r \in \mathbb{Z}_N$$

Du är den ende (förhoppningsvis) som kan dekryptera med hjälp av funktionen

$$D(r) = r^d$$

d är hemligt och

$$D \circ E(r) = D(r^e) = r^{ed} = r$$

Visa den sista likheten!

Ledning. $ed = 1 + \varphi(N)m$ för ett heltal $m \geq 1$. Utnyttja Eulers sats som i det här fallet kan formuleras så att $r^{\varphi(N)+1} \equiv r \pmod{N}$!

(e) Låt $N = 17 \cdot 23 = 391$. Välj krypteringsnyckeln $e = 3$ och kryptera NEJ (med "ordboken" som i (c)). Beräkna d och dekryptera 121 268 358.