

Matematik, KTH

Bengt Ek

juli 2017

MATERIAL TILL KURSERNA
SF1679 OCH SF1688, DISKRET MATEMATIK:

Kinesiska restsatsen

Vi vet att för varje $m \in \mathbb{Z}_+$ och varje $a \in \mathbb{Z}$, ges alla $x \in \mathbb{Z}$ som uppfyller

$$x \equiv a \pmod{m}$$

av $x = a + tm$, för $t \in \mathbb{Z}$. Det följer ju direkt av definitionen av kongruens: $x \equiv a \pmod{m} \Leftrightarrow m \mid (x - a) \Leftrightarrow x - a = tm$ för något $t \in \mathbb{Z}$.

Men antag nu att vi har flera sådana kongruenser och vill finna de heltal x som uppfyller dem allesammans. Dvs, vi söker alla lösningar $x \in \mathbb{Z}$ till följande system av kongruenser:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \quad (*)$$

där $k, m_1, \dots, m_k \in \mathbb{Z}_+$ och $a_1, \dots, a_k \in \mathbb{Z}$. I det enklaste fallet, när modulerna m_i är parvis relativt prima, säger **Kinesiska restsatsen** (eng. **the Chinese remainder theorem, CRT**) att (för varje $k \in \mathbb{Z}_+$ och) för varje val av heltal $a_1, a_2, \dots, a_k$ finns lösningar till systemet och satsen anger också hur olika lösningar förhåller sig till varandra.

Den naturliga avbildningen $\mathbb{Z} \rightarrow (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k})$

Låt $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$ som vanligt beteckna mängden av alla k -tupler $(b_1, b_2, \dots, b_k)$, där $b_i \in \mathbb{Z}_{m_i}$, för $i = 1, \dots, k$. Vi definierar funktionen

$$F: \mathbb{Z} \rightarrow (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k})$$

enligt

$$F(x) = ([x]_{m_1}, [x]_{m_2}, \dots, [x]_{m_k})$$

där $[x]_{m_i} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{m_i}\}$, dvs $[x]_{m_i}$ är ” x betraktat som ett element i $\mathbb{Z}_{m_i}$ ”.

Exempel. Om vi tar $x = 718$, $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, finner vi

$$F(718) = ([718]_5, [718]_6, [718]_7) = ([3]_5, [4]_6, [4]_7), \text{ vanligen skrivet } (3, 4, 4).$$

(Slut på exemplet.)

Eftersom $[x]_{m_i} = [a_i]_{m_i} \Leftrightarrow x \equiv a_i \pmod{m_i}$, uppfylls $(*)$ av $x \in \mathbb{Z}$ omm

$$F(x) = ([a_1]_{m_1}, [a_2]_{m_2}, \dots, [a_k]_{m_k}).$$

Dessutom gäller

$$\begin{aligned} F(x) = F(y) &\Leftrightarrow [x]_{m_i} = [y]_{m_i} \text{ för } i = 1, \dots, k \Leftrightarrow \\ &\Leftrightarrow x \equiv y \pmod{m_i} \text{ för } i = 1, \dots, k \Leftrightarrow m_i \mid (x - y) \text{ för } i = 1, \dots, k \Leftrightarrow \\ &\Leftrightarrow \text{mgm}(m_1, \dots, m_k) \mid (x - y), \end{aligned}$$

så om x uppfyller $(*)$, gör y det **omm** $x \equiv y \pmod{\text{mgm}(m_1, \dots, m_k)}$.

Antag nu att modulerna m_i är parvis relativt prima och inför beteckningen $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$. Då är $\text{mgm}(m_1, \dots, m_k) = m$, så

$$F(x) = F(y) \Leftrightarrow m \mid (x - y) \Leftrightarrow [x]_m = [y]_m.$$

Det betyder att F definierar en funktion

$$f : \mathbb{Z}_m \rightarrow (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}) \text{ enligt } f([x]_m) = F(x).$$

$\Leftarrow$ ovan visar att olika $y \in [x]_m$ har samma $F(y)$, så f är väldefinierad.

$\Rightarrow$, å andra sidan, visar att $f([x]_m) = f([y]_m) \Rightarrow [x]_m = [y]_m$, så f är ett-till-ett (en injektion). Eftersom $|\mathbb{Z}_m| = m = m_1 \cdot \dots \cdot m_k = |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}|$ och f tar olika element i $\mathbb{Z}_m$ till olika element i $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ (och m är ändligt), antas alla värden i $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$, så **f är ett-till-ett och på** (en bijektion).

Exempel. Med $m_1 = 3$, $m_2 = 5$ (relativt prima, ju), som ger $m = 15$, finner vi funktionen $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$ (vi underförstår $[\cdot]_{15}$, $[\cdot]_3$, $[\cdot]_5$):

$$\begin{aligned} f(0) &= (0, 0), & f(5) &= (2, 0), & f(10) &= (1, 0) \\ f(1) &= (1, 1), & f(6) &= (0, 1), & f(11) &= (2, 1) \\ f(2) &= (2, 2), & f(7) &= (1, 2), & f(12) &= (0, 2) \\ f(3) &= (0, 3), & f(8) &= (2, 3), & f(13) &= (1, 3) \\ f(4) &= (1, 4), & f(9) &= (0, 4), & f(14) &= (2, 4) \end{aligned}$$

och vi ser att varje element i $\mathbb{Z}_3 \times \mathbb{Z}_5$ antas som värde precis en gång.

Isomorfin $(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}, +, \cdot)$

Vi definierar addition och multiplikation komponentvis i $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$,

$$\begin{aligned} ([x]_{m_1}, \dots, [x]_{m_k}) + ([y]_{m_1}, \dots, [y]_{m_k}) &= ([x]_{m_1} + [y]_{m_1}, \dots, [x]_{m_k} + [y]_{m_k}), \\ ([x]_{m_1}, \dots, [x]_{m_k}) \cdot ([y]_{m_1}, \dots, [y]_{m_k}) &= ([x]_{m_1} \cdot [y]_{m_1}, \dots, [x]_{m_k} \cdot [y]_{m_k}), \end{aligned}$$

(observera att $+$ och $\cdot$ i VL:en definieras här, medan $+$ och $\cdot$ i HL:en är i de olika $\mathbb{Z}_{m_i}$) och minns att $[x]_n + [y]_n = [x + y]_n$, $[x]_n \cdot [y]_n = [x \cdot y]_n$ (enligt definitionen av $+$ och $\cdot$ i $\mathbb{Z}_n$).

Vi finner då för $x, y \in \mathbb{Z}_m$:

$$f(x) + f(y) = f(x + y) \quad \text{och} \quad f(x) \cdot f(y) = f(x \cdot y).$$

($+$ och $\cdot$ i VL:en är definierade ovan och $+$ och $\cdot$ i HL:en är i $\mathbb{Z}_m$.)

Det betyder att $(\mathbb{Z}_m, +, \cdot)$ och $(\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}, +, \cdot)$ (om m_i :na är parvis relativt prima) är **isomorfa** (eng. **isomorphic**), betecknat

$$(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}, +, \cdot).$$

f är en **isomorfi** (eng. **isomorphism**) (strukturbevarande bijektion) mellan dem.

Vi har därmed visat följande

Sats:

Om $k, m_1, \dots, m_k \in \mathbb{Z}_+$, $\text{sgd}(m_i, m_j) = 1$ då $i \neq j$ och $m = m_1 \cdot \dots \cdot m_k$, så definierar den naturliga avbildningen $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ en isomorfi

$$(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}, +, \cdot)$$

Med denna isomorfi kan beräkningar och resonemang i $\mathbb{Z}_m$ ofta förenklas.

Om man t.ex. skall beräkna $x \cdot y$ (eller $x + y$) kan man göra det genom att bestämma $f(x)$ och $f(y)$, beräkna $f(x) \cdot f(y) = f(x \cdot y)$ (eller $f(x) + f(y) = f(x + y)$) (med enklare, oberoende beräkningar i $\mathbb{Z}_{m_i}$:na, eventuellt parallellt) och sedan "gå tillbaks" (eftersom f är bijektiv) för att finna $x \cdot y$ (eller $x + y$) i $\mathbb{Z}_m$.

Eftersom f är en isomorfi och $f(1) = ([1]_{m_1}, \dots, [1]_{m_k})$ ser vi också att

$$\begin{aligned} x \in \mathbb{Z}_m \text{ är inverterbar} &\Leftrightarrow \text{det finns ett } y \in \mathbb{Z}_m \text{ med } x \cdot y = 1 \Leftrightarrow \\ &\Leftrightarrow \text{det finns ett } y \in \mathbb{Z}_m \text{ med } f(x) \cdot f(y) = f(1) \Leftrightarrow \\ &\Leftrightarrow \text{det finns ett } y \in \mathbb{Z}_m \text{ med } [x]_{m_i} \cdot [y]_{m_i} = [1]_{m_i} \text{ för } i = 1, \dots, k \Leftrightarrow \\ &\Leftrightarrow [x]_{m_i} \text{ är inverterbart för } i = 1, \dots, k, \end{aligned}$$

så $x \in \mathbb{Z}_m$ är inverterbart (i $\mathbb{Z}_m$) om $[x]_{m_i}$ är inverterbart (i $\mathbb{Z}_{m_i}$) för $i = 1, \dots, k$ och då är $f(x^{-1}) = ([x]_{m_1}^{-1}, \dots, [x]_{m_k}^{-1})$.

Exempel. Om vi åter tar $m_1 = 3$, $m_2 = 5$ och $m = 15$, kan vi beräkna $9 \cdot 13$ i $\mathbb{Z}_{15}$ så här:

Enligt tabellen ovan är $f(9) = (0, 4)$, $f(13) = (1, 3)$, så $f(9 \cdot 13) = f(9) \cdot f(13) = (0 \cdot 1, 4 \cdot 3) = (0, 2) = f(12)$ (sista '=' enligt tabellen). Eftersom f är injektiv ger det att $9 \cdot 13 = 12$ i $\mathbb{Z}_{15}$.

På samma sätt finner vi $f(9 + 13) = (0, 4) + (1, 3) = (1, 2) = f(7)$, så $9 + 13 = 7$ i $\mathbb{Z}_{15}$.

$f(12) = (0, 2)$ visar också att 12 inte är inverterbart i $\mathbb{Z}_{15}$ (ty 0 är inte inverterbart i $\mathbb{Z}_3$) och $f(13) = (1, 3)$ ger att 13 är inverterbart i $\mathbb{Z}_{15}$ (ty $[1]_3$ och $[3]_5$ är inverterbara) och $f(13^{-1}) = (1^{-1}, 3^{-1}) = (1, 2) = f(7)$ ger $13^{-1} = 7$ i $\mathbb{Z}_{15}$.

(Slut på exemplet.)

Då man räknar med mycket stora tal (i $\mathbb{Z}$), särskilt om många additioner och multiplikationer skall utföras i följd, kan metoden som beskrivits här användas för att snabba upp beräkningarna (**snabb aritmetik**). Man använder då m_i :n av rimlig storlek och ett ganska stort k för att få ett mycket stort m . Beräkningarna i de olika $\mathbb{Z}_{m_i}$ kan (relativt snabbt) utföras parallellt och om man kan uppskatta att resultatet ligger i ett intervall av längd högst m , bestäms det av det beräknade värdet i $\mathbb{Z}_m$.

För att detta skall vara praktiskt användbart, måste vi kunna beräkna värden för f och f^{-1} (dvs finna ett värde för x med givet $([x]_{m_1}, \dots, [x]_{m_k})$) någotsånär snabbt. I exemplet fann vi x med hjälp av tabellen för f , men det är förstås inte möjligt då m är jättelikt. f fås med division med (de inte så stora) m_i , vilket går snabbt, och för f^{-1} skall vi finna en effektiv metod i nästa avsnitt.

Åter till Kinesiska restsatsen

Existensen av bijektionen $f: \mathbb{Z}_m \rightarrow (\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k})$ uttryckt i termer av lösningar till systemet av kongruenser $(*)$ som vi utgick från ger

Kinesiska restsatsen:

Om $k, m_1, \dots, m_k \in \mathbb{Z}_+$, $\text{sgd}(m_i, m_j) = 1$ då $i \neq j$, $m = m_1 \cdot \dots \cdot m_k$ och $a_1, \dots, a_k \in \mathbb{Z}$, så har systemet av kongruenser

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \quad (*)$$

en lösning och den är entydig modulo m

(dvs om x är en lösning, ges alla lösningar av $x + t \cdot m$, $t \in \mathbb{Z}$).

Det återstår att finna en enkel metod för att få fram en lösning $x \in \mathbb{Z}$ till $(*)$, då m_i :na och a_i :na är givna, dvs att finna x med $F(x) = (a_1, \dots, a_k)$.

Vi beskriver två metoder:

1. Med användning av F 's linearitet:

Antag att vi har heltal y_i , $i = 1, \dots, k$ som uppfyller

$F(y_i) = (0, \dots, 0, \overset{i}{1}, 0, \dots, 0)$, med den enda 1:an i position i . Då är

$$F(a_1 y_1 + \dots + a_k y_k) = ([a_1 y_1 + \dots + a_k y_k]_{m_1}, \dots) = ([a_1]_{m_1}, \dots, [a_k]_{m_k}),$$

så $\mathbf{x} = \mathbf{a}_1 \mathbf{y}_1 + \dots + \mathbf{a}_k \mathbf{y}_k$ är en lösning till $(*)$ (och $y \in \mathbb{Z}$ är en lösning omm $y \equiv_m x$).

Så, om vi har sådana y_i kan vi finna alla lösningar till $(*)$ mycket effektivt. Om vi speciellt vill lösa många system $(*)$ med olika a_i , räcker det att beräkna y_i :na en gång för alla (eftersom de inte beror av a_i :na). De kan lagras och användas varje gång de behövs (dvs när f^{-1} skall beräknas).

För att finna y_i , minns att det uppfyller $(*)$ med $a_i = 1$, $a_j = 0$ för $j \neq i$. Om vi låter $M_i = \frac{m}{m_i} = m_1 \cdot \dots \cdot m_i \cdot \dots \cdot m_k$ är $M_i \cdot b_i$ ett möjligt y_i om $M_i \cdot b_i \equiv_{m_i} 1$ och eftersom $\text{sgd}(M_i, m_i) = 1$ finns sådana b_i för $i = 1, \dots, k$.

Exempel. I ett tidigare exempel använde vi $m_1 = 5$, $m_2 = 6$, $m_3 = 7$ (parvis relativt prima), så $m = 5 \cdot 6 \cdot 7 = 210$, och fann $F(718) = (3, 4, 4)$. Det betyder för $719 = 89 \in \mathbb{Z}_{210}$ att $f(89) = (4, 5, 5)$ och vi ser att $f(89^{-1}) = (4^{-1}, 5^{-1}, 5^{-1}) = (4, 5, 3) \in (\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7)$. (718 är inte inverterbart i $\mathbb{Z}_{210}$ eftersom 4 inte är inverterbart i $\mathbb{Z}_6$).

För att finna 89^{-1} beräknar vi (ett möjligt val av) y_1, y_2, y_3 i detta fall:

$$y_1 = 6 \cdot 7 \cdot b_1 = 42b_1 \equiv_5 1 \Leftrightarrow 2b_1 \equiv_5 1 \text{ och vi kan ta } b_1 = 3, \text{ så } y_1 = 126.$$

(Här fann vi b_1 "med blotta ögat", men i ett realistiskt fall skulle man använda Euklides algoritmen för att finna $b_1 = M_1^{-1}$ i $\mathbb{Z}_{m_1}$.)

$$y_2 = 5 \cdot 7 \cdot b_2 = 35b_2 \equiv_6 1 \Leftrightarrow -b_2 \equiv_6 1. \text{ Vi tar } b_2 = -1, \text{ så } y_2 = -35.$$

$$y_3 = 5 \cdot 6 \cdot b_3 = 30b_3 \equiv_7 1 \Leftrightarrow 2b_3 \equiv_7 1. \text{ Vi tar } b_3 = 4, \text{ så } y_3 = 30 \cdot 4 = 120.$$

Eftersom $f(89^{-1}) = (4, 5, 3)$ får vi

$$89^{-1} = 4y_1 + 5y_2 + 3y_3 = 4 \cdot 126 + 5(-35) + 3 \cdot 120 = 689 \equiv_{210} 59 \text{ (i } \mathbb{Z}_{210}\text{)}.$$

(Slut på exemplet.)

Metoden i exemplet är antagligen mindre effektiv för att finna $89^{-1} \in \mathbb{Z}_{210}$ än Euklides algoritmen, men exemplet illustrerar hur man kan beräkna f^{-1} . Om man söker flera inverser i $\mathbb{Z}_{210}$ kan den metoden kanske vara användbar (eftersom y_1, y_2, y_3 bara behöver beräknas en gång).

För ett enda exempel går det dock ofta snabbare med en direkt metod:

2. Lösning av kongruenserna en och en:

Vi tar samma exempel som ovan och vill lösa

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{7}. \end{cases}$$

Den första ekvationen uppfylls om $x = 4 + 5s$ för något $s \in \mathbb{Z}$.

Dessa x uppfyller också den andra ekvationen om

$$4 + 5s \equiv_6 5 \Leftrightarrow -s \equiv_6 1 \Leftrightarrow s = -1 + 6t \text{ för något } t \in \mathbb{Z},$$

dvs om $x = 4 + 5(-1 + 6t) = -1 + 30t$ för något $t \in \mathbb{Z}$.

x uppfyller alla tre ekvationerna om

$$-1 + 30t \equiv_7 3 \Leftrightarrow 2t \equiv_7 4 \Leftrightarrow t \equiv_7 2 \Leftrightarrow t = 2 + 7n \text{ för något } n \in \mathbb{Z}$$

(där $\text{sgd}(2, 7) = 1$ använts i näst sista steget).

Så, alla tre kongruenserna uppfylls om $x = -1 + 30t = -1 + 30(2 + 7n) = 59 + 210n$ för något $n \in \mathbb{Z}$.

Det innebär att $[89]_{210}^{-1} = [59]_{210}$, som med metod 1.

Övningsexempel

1. Finn alla $x \in \mathbb{Z}$ sådana att

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7}. \end{cases}$$

Använd båda metoderna som presenteras i texten.

Finn också alla $y \in \mathbb{Z}$ sådana att för alla lösningar x ,
 $x \cdot y \equiv 1 \pmod{3}$, $\pmod{5}$ och $\pmod{7}$.

2. Finn alla heltal x med $0 \leq x \leq 3000$ sådana att

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{13}. \end{cases}$$

3. Låt $f : \mathbb{Z}_{315} \rightarrow (\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_9)$ vara som i texten.

a. Finn $f(3)$ och $f(43)$.

b. Finn $f^{-1}((1, 0, 0))$, $f^{-1}((0, 1, 0))$ och $f^{-1}((0, 0, 1))$.

c. Använd f och f^{-1} för att beräkna $(186 + 212) \cdot 88^{-1} + 167$ i $\mathbb{Z}_{315}$.

4. Finn alla $x \in \mathbb{Z}$ sådana att

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{6}. \end{cases}$$

5. Finn alla $k \in \mathbb{Z}_+$ sådana att

a. $7834^k \equiv 1 \pmod{8613}$.

b. $7834^k \equiv 6850 \pmod{8613}$.

c. $7834^k \equiv 2703 \pmod{8613}$.

d. $7834^k \equiv 1318 \pmod{8613}$.

[$8613 = 3^3 \cdot 11 \cdot 29$].

Svar

1. $x = 68 + 105m$, $m \in \mathbb{Z}$ och $y = 17 + 105n$, $n \in \mathbb{Z}$.

2. $x = 811$, 2527 .

3a. $(3, 3, 3)$ och $(3, 1, 7)$, b. 126 , 225 och 280 , c. 193 .

4. Det finns inga sådana x .

5a. $k = 630n$, $n \in \mathbb{Z}_+$, b. $k = 213 + 630n$, $n \in \mathbb{Z}_+$,

c., d. Det finns inga sådana k .

Lösningssanvisning till uppgift 5:

Med vår isomorfi $f : \mathbb{Z}_{8613} \rightarrow (\mathbb{Z}_{27} \times \mathbb{Z}_{11} \times \mathbb{Z}_{29})$ fås

$f(7834) = (4, 2, 4)$, $f(1) = (1, 1, 1)$, $f(6850) = (19, 8, 6)$,

$f(2703) = (3, 8, 6)$, $f(1318) = (22, 9, 13)$.

Potenser av $[4]_{27}$, $[2]_{11}$, $[4]_{29}$:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
4^k	4	16	10	13	25	19	22	7	1	...						i $\mathbb{Z}_{27}$
2^k	2	4	8	5	10	9	7	3	6	1	...					i $\mathbb{Z}_{11}$
4^k	4	16	6	24	9	7	28	25	13	23	5	20	22	1	...	i $\mathbb{Z}_{29}$

Villkoren på k blir:

i a: $k \equiv_9 0$, $\equiv_{10} 0$, $\equiv_{14} 0$,

i b: $k \equiv_9 6$, $\equiv_{10} 3$, $\equiv_{14} 3$,

i c finns inget k sådant att $4^k = 3$ i $\mathbb{Z}_{27}$,

i d: $k \equiv_9 7$, $\equiv_{10} 6$, $\equiv_{14} 9$.