Inledande diskret matematik, Ht 2019
Extra material i talteori (Kapitel 5)

Kinesiska restsatsen

På föreläsningarna och i boken har vi sett hur man löser ett kongruenssystem av typen

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{1}$$

då m och n är relativt prima. Kinesiska restsatsen säger i detta fall att det finns en unik lösning modulo mn och den ges av

$$x \equiv bum + avn \mod mn \tag{2}$$

där u och v är heltal sådana att $um + vn = 1$ (och som vi kan få fram genom Euklides algoritm "baklänges"). Beviset är enkelt: om vi ersätter um med $1 - vn$ eller vn med $1 - um$ i (2) så ser vi att x uppfyller båda kongruenserna i (1). För att få alla lösningar som tal och inte bara som en kongruensklass modulo mn, måste vi sedan lägga till kmn där k är ett godtyckligt heltal (alltså ett heltal vilket som helst),

$$x = bum + avn + kmn. \tag{3}$$

Däremot har det inte varit lika klart hur man löser ett kongruenssystem med fler än två kongruenser. I boken finns två metoder, där man i båda fallen börjar med att lösa ett delsystem bestående av bara två av de ursprungliga kongruenserna, men båda metoderna är ganska krångliga. Det finns dock en version av den kinesiska restsatsen som fungerar även för tre eller flera kongruenser, och som inte är mycket krångligare än den för två kongruenser.

Det ursprungliga problemet, som formulerades av den kinesiske författaren Sun-Tsu redan för omkring tvåtusen år sedan och som har gett upphov till namnet "kinesiska restsatsen", gällde faktiskt ett system med tre kongruenser: *Det finns ett obekant tal som vid division med 3 ger resten 2, med 5 resten 3 och med 7 resten 2. Vilket är talet?* Vi återkommer till lösningen. Först formulerar vi den allmänna versionen av den kinesiska restsatsen, med N kongruenser.

Sats. (Kinesiska restsatsen) *Antag att talen m_1, m_2, ..., m_N är parvis relativt prima. Då har kongruenssystemet*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_N \mod m_N \end{cases} \tag{4}$$

en entydig lösning modulo $m = m_1 m_2 \cdots m_N$.

BEVIS: För varje $i = 1, 2, \ldots, N$, sätt

$$M_i = \frac{m}{m_i} = \prod_{j \neq i} m_j. \tag{5}$$

Produkten går alltså från $j = 1$ till $j = N$, men vi hoppar över $j = i$, eftersom vi dividerar bort m_i från $m = m_1 m_2 \cdots m_N$. (Speciellt $M_1 = m_2 m_3 \cdots m_N$ och $M_N = m_1 m_2 \cdots m_{N-1}$.) Då är talen M_i och m_i relativt prima för varje i, och det finns heltal u_i och v_i sådana att

$$u_i M_i + v_i m_i = 1. \tag{6}$$

Sätt nu

$$x = \sum_{j=1}^{N} a_j u_j M_j = a_1 u_1 M_1 + a_2 u_2 M_2 + \cdots + a_N u_N M_N. \tag{7}$$

Då är $x \equiv a_i u_i M_i \mod m_i$ för alla $i = 1, 2, \ldots, N$, eftersom faktorn m_i finns med i alla produkterna M_j utom just den där $i = j$. Och om vi använder (6) så får vi

$$x \equiv a_i u_i M_i = a_i(1 - v_i m_i) = a_i - a_i v_i m_i \equiv a_i \mod m_i. \tag{8}$$

Alltså är x en lösning, och den är unik modulo m, för om x' vore en annan lösning finge vi $x \equiv x' \mod m_i$ för alla $i = 1, 2, \ldots, N$. Eftersom talen m_1, m_2, $\ldots$, m_N är parvis relativt prima måste då $x \equiv x' \mod m$. □

Vad innebär nu detta då $N = 3$? Jo, då säger satsen att den unika (mod $m_1 m_2 m_3$) lösningen till kongruenssystemet

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ x \equiv a_3 \mod m_3, \end{cases} \tag{9}$$

där m_1, m_2, m_3 är parvis relativt prima, har formen

$$\begin{aligned} x &= a_1 u_1 M_1 + a_2 u_2 M_2 + a_3 M_3 \\ &= a_1 u_1 (m_2 m_3) + a_2 u_2 (m_1 m_3) + a_3 u_3 (m_1 m_2), \end{aligned} \tag{10}$$

där u_1, u_2, u_3 kan bestämmas genom villkoren

$$\begin{aligned} u_1(m_2 m_3) + v_1 m_1 &= 1, \\ u_2(m_1 m_3) + v_2 m_2 &= 1, \\ u_3(m_1 m_2) + v_3 m_3 &= 1 \end{aligned} \tag{11}$$

för några heltal v_1, v_2, v_3 (som vi inte behöver använda explicit sedan). Man kan också uttrycka villkoren som

$$\begin{aligned} u_1(m_2m_3) &\equiv 1 \mod m_1, \\ u_2(m_1m_3) &\equiv 1 \mod m_2, \\ u_3(m_1m_2) &\equiv 1 \mod m_3. \end{aligned} \tag{12}$$

I det gamla kinesiska ursprungsproblemet hade vi kongruenssystemet

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7, \end{cases} \tag{13}$$

det vill säga

$$\begin{aligned} m_1 &= 3, & M_1 &= m_2m_3 = 35, \\ m_2 &= 5, & M_2 &= m_1m_3 = 21, \\ m_3 &= 7, & M_3 &= m_1m_2 = 15, \end{aligned} \tag{14}$$

och vi får

$$\begin{aligned} 2 \cdot 35 - 23 \cdot 3 &= 1, \\ 1 \cdot 21 - 4 \cdot 5 &= 1, \\ 1 \cdot 15 - 2 \cdot 7 &= 1. \end{aligned} \tag{15}$$

Alltså är

$$x = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 233 \tag{16}$$

en lösning till problemet, och den minsta positiva lösningen

$$233 - 2m = 233 - 210 = 23 \tag{17}$$

där $m = 3 \cdot 5 \cdot 7$.

I uppgift 5.25 i boken (som vi gick igenom på en föreläsning) hade vi

$$\begin{cases} x \equiv 7 \mod 17 \\ x \equiv 9 \mod 13 \\ x \equiv 3 \mod 12, \end{cases} \tag{18}$$

det vill säga

$$\begin{aligned} m_1 &= 17, & M_1 &= m_2m_3 = 156, \\ m_2 &= 13, & M_2 &= m_1m_3 = 204, \\ m_3 &= 12, & M_3 &= m_1m_2 = 221. \end{aligned} \tag{19}$$

För att lösa kongruenssystemet (18) behöver vi hitta heltal u_1, u_2, u_3 som uppfyller

$$\begin{aligned} 156u_1 &\equiv 1 \mod 17, \\ 204u_2 &\equiv 1 \mod 13, \\ 221u_3 &\equiv 1 \mod 12. \end{aligned} \tag{20}$$

Lösningarna är

$$\begin{aligned} u_1 &\equiv 6 \mod 17, \\ u_2 &\equiv 3 \mod 13, \\ u_2 &\equiv 5 \mod 12. \end{aligned} \tag{21}$$

vilket ger lösningen

$$x \equiv 7 \cdot 6 \cdot 156 + 9 \cdot 3 \cdot 204 + 3 \cdot 5 \cdot 221 \mod 17 \cdot 13 \cdot 12 \tag{22}$$

till (18). För att få något mindre tal och enklare räkningar kan man till exempel i (21) byta ut $u_2 \equiv 3 \mod 13$ mot $u_2 \equiv -10 \mod 13$. Då får vi

$$\begin{aligned} x &\equiv 7 \cdot 6 \cdot 156 - 90 \cdot 204 + 3 \cdot 5 \cdot 221 \\ &= -8493 \equiv 4 \cdot 2652 - 8493 = 10608 - 8493 = 2115 \mod 2652. \end{aligned} \tag{23}$$