Mårten Wadenbäck

Kinesiska restsatsen

Om $x \equiv a \mod n$ kan vi omedelbart ange alla x som uppfyller kongruensen. Dessa får vi direkt ur definitionen: $x \equiv a \mod n \Leftrightarrow n \mid x-a \Leftrightarrow x-a=kn \Leftrightarrow x=a+kn$ för $k \in \mathbb{Z}$. Detta är alla element i klassen $[a]$. Vi skall nu se på vilka x som uppfyller flera kongruenser samtidigt.

Sats (Kinesiska restsatsen): Låt m_1 och m_2 vara heltal, större än eller lika med två, sådana att $\mathrm{sgd}(m_1, m_2)=1$. Antag att a_1 och a_2 är heltal. Då har ekvationssystemet

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

en lösning $x=x_0$, och allmänna lösningen ges av $x=x_0+km_1m_2$ för $k \in \mathbb{Z}$.

Bevis: Då m_1 och m_2 är relativt prima finns det heltal u och v sådana att $m_1u+m_2v=1$.

Vi shall se att $x_0=a_2m_1u+a_1m_2v$ är en lösning:

$$x_0 \equiv a_2m_1u+a_1m_2v \equiv a_2m_1u+a_1(1-m_1u) \equiv a_1+m_1u(a_2-a_1) \equiv a_1 \mod m_1$$

och

$$x_0 \equiv a_2m_1u+a_1m_2v \equiv a_2(1-m_2v)+a_1m_2v \equiv a_2+m_2v(a_1-a_2) \equiv a_2 \mod m_2.$$

När vi vet att x_0 är en lösning är det lätt att inse att även $x_0+km_1m_2$ är en lösning, ty $x_0+km_1m_2 \equiv x_0 \mod m_1$ och $x_0+km_1m_2 \equiv x_0 \mod m_2$.

Att det inte kan finnas några ytterligare lösningar ser vi på följande sätt. Om x är en lösning gäller

$$\begin{cases} x \equiv a_1 \equiv x_0 \mod m_1 \\ x \equiv a_2 \equiv x_0 \mod m_2, \end{cases}$$

så $m_1 \mid x-x_0 \Leftrightarrow x=x_0+rm_1$ och $m_2 \mid x-x_0 \Leftrightarrow m_2 \mid rm_1$. Eftersom $sgd(m_1,m_2)=1$ måste $m_2 \mid r$, så $r=km_2$ och alltså $x=x_0+km_1m_2$.

Exempel: Bestäm alla x som uppfyller

$$\begin{cases} x \equiv 6 \mod 12 \\ x \equiv 3 \mod 5. \end{cases}$$

Vi börjar med att kontrollera att $sgd(12,5)=1$ och beräkna u och v så att $12u+5v=1$ med Euklides algoritm:

$$12 = 2\cdot 5 + 2$$
$$5 = 2\cdot 2 + 1 \qquad \text{och} \qquad 1 = 5-2\cdot 2 = 5 - 2(12-2\cdot 5) =$$
$$2 = 2\cdot 1, \qquad = \underbrace{-2}_{u}\cdot 12 + \underbrace{5}_{v}\cdot 5.$$

Lösningarna till systemet ges nu av

$$x = a_2 m_1 u + a_1 m_2 v + k m_1 m_2 = 3\cdot 12\cdot(-2) + 6\cdot 5\cdot 5 + k\cdot 12\cdot 5 =$$
$$= -72 + 150 + k\cdot 60 = 78 + 60k,$$

där k är heltal.

Anmärkning: Svaret kan se ut på många sätt, men det är samma mängd av tal. I exemplet hade vi kanske hellre angivit lösningarna som $x = 18 + 60k$, $k \in \mathbb{Z}$.

Vi kan utöka Kinesiska restsatsen till fallet då vi har fler än två kongruenser. Om

$$\begin{cases} x \equiv a_1 & \text{mod } m_1 \\ x \equiv a_2 & \text{mod } m_2 \\ \vdots & \\ x \equiv a_n & \text{mod } m_n \end{cases}$$

där $m_1, \ldots, m_n$ alla är relativt prima lovar Kinesiska restsatsen att systemet är ekvivalent med systemet

$$\begin{cases} x \equiv x_0 & \text{mod } m_1 m_2 \\ x \equiv a_3 & \text{mod } m_3 \\ \vdots & \\ x \equiv a_n & \text{mod } m_n, \end{cases}$$

och detta är i sin tur ekvivalent med

$$\begin{cases} x \equiv x_1 & \text{mod } m_1 m_2 m_3 \\ x \equiv a_4 & \text{mod } m_4 \\ \vdots & \\ x \equiv a_n & \text{mod } m_n. \end{cases}$$

Vi kan på detta sätt reducera ned systemet genom upprepad användning av Kinesiska restsatsen.

Exempel: Bestäm alla x som uppfyller

$$\begin{cases} x \equiv 6 & \text{mod } 12 \\ x \equiv 3 & \text{mod } 5 \\ x \equiv 2 & \text{mod } 7. \end{cases}$$

Från förra exemplet kan vi ta $x_0 = 78$, och vi får ett ekvivalent system

$$\begin{cases} x \equiv 78 & \text{mod } 60 \\ x \equiv 2 & \text{mod } 7 \end{cases} \iff \begin{cases} x \equiv 18 & \text{mod } 60 \\ x \equiv 2 & \text{mod } 7. \end{cases}$$

Vi söker nu u och v som uppfyller $60u + 7v = 1$:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1, \end{aligned}$$

och

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 = 4 - 1 \cdot (7 - 1 \cdot 4) = \\ &= -1 \cdot 7 + 2 \cdot 4 = -1 \cdot 7 + 2 \cdot (60 - 8 \cdot 7) = \\ &= \underbrace{2}_{u} \cdot 60 \underbrace{-17}_{v} \cdot 7. \end{aligned}$$

Lösningarna blir nu

$$x = 2 \cdot 60 \cdot 2 + 18 \cdot 7 \cdot (-17) + k \cdot 60 \cdot 7 = -1902 + k \cdot 420.$$

Metoden ger tyvärr ofta stora tal. En annan metod, som kan ge mindre tal vid handräkning, är att helt enkelt lösa en rad i taget och substituera i nästa rad.

Exempel: Bestäm alla x som uppfyller

$$\begin{cases} x \equiv 6 & \text{mod } 12 \\ x \equiv 3 & \text{mod } 5 \\ x \equiv 2 & \text{mod } 7. \end{cases}$$

Första kongruensen ger att $x = 6 + 12s$ för något heltal s. Sätter vi in detta i andra kongruensen får vi att $6 + 12s \equiv 3 \mod 5 \Leftrightarrow 12s \equiv -3 \mod 5 \Leftrightarrow$ $2s \equiv 2 \mod 5$. Eftersom $sgd(2,5) = 1$ har $[2]$ en invers i $\mathbb{Z}_5$ som kan beräknas med Euklides algoritm (eller genom att testa de fyra elementen $[1], [2], [3]$, och $[4]$), och vi kommer att komma fram till att iversen till $[2]$ är $[3]$. Genom att multiplicera med 3 (inversen) på båda sidor får vi

$$2s \equiv 2 \mod 5 \Leftrightarrow 3 \cdot 2s \equiv 3 \cdot 2 \mod 5 \Leftrightarrow s \equiv 1 \mod 5,$$

så $s = 1 + 5t$ för något heltal t, och alltså $x = 6 + 12(1+5t) = 18 + 60t$. Insättning i tredje ekvationen ger $18 + 60t \equiv 2 \mod 7 \Leftrightarrow 4 + 4t \equiv 2 \mod 7 \Leftrightarrow$

$$4t \equiv -2 \mod 7 \Leftrightarrow 4t \equiv 5 \mod 7.$$

Vi använder Euklides algoritm för att bestämma inversen till [4] i $\mathbb{Z}_7$:

$$7 = 1\cdot 4 + 3$$
$$4 = 1\cdot 3 + 1$$
$$3 = 3\cdot 1,$$

så $1 = 4 - 1\cdot 3 = 4 - 1\cdot(7 - 1\cdot 4) = -1\cdot 7 + 2\cdot 4$, och inversen är därför [2]. Vi multiplicerar båda led med två och får

$$4t \equiv 5 \mod 7 \iff 2\cdot 4t \equiv 2\cdot 5 \mod 7 \iff$$

$$t \equiv 3 \mod 7 \iff t = 3 + 7k \text{ för } k \in \mathbb{Z}.$$

Detta ger $x = 18 + 60t = 18 + 60(3 + 7k) =$

$$= 18 + 180 + 420k = 198 + 420k.$$