I dette notatet skal vi se på hvordan vi kan løse et likningssystem bestående av flere kongruenser med ulik modulus:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Vi begynner med å se på systemer av to kongruenslikninger, for å få tak i noen av ideene vi trenger uten at det blir altfor mye å holde styr på. Etterpå tar vi for oss det generelle tilfellet med r likninger, og beviser *det kinesiske restteoremet*, som beskriver nøyaktig hva løsningene av et slikt system er.

Bakgrunnen for det litt underlige navnet «det kinesiske restteoremet» er at den eldste kjente beskrivelsen av et problem som tilsvarer et system av kongruenslikninger ble gitt i den omtrent 1500 år gamle kinesiske teksten 孙子算经 (*Sunzi Suanjing*).

Systemer av to likninger

La oss først se på et enkelt eksempel.

Eksempel. Vi vil løse systemet

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{4} \end{cases}$$

Vi kan observere at hvis to tall er kongruente modulo $3 \cdot 4 = 12$, så er de også kongruente modulo både 3 og 4. For å sjekke om et gitt tall x er en løsning av systemet, er det altså tilstrekkelig å sjekke om x mod 12 er en løsning.

Vi lager en tabell der vi skriver opp både x mod 3 og x mod 4 for forskjellige verdier av x mod 12:

x mod 12:	0	1	2	3	4	5	6	7	8	9	10	11
x mod 3:	0	1	2	0	1	2	0	1	2	0	1	2
x mod 4:	0	1	2	3	0	1	2	3	0	1	2	3

Vi ser i tabellen at det er ett tilfelle der vi får både $x \equiv 1 \pmod 3$ og $x \equiv 3 \pmod 4$ samtidig, og det er når x er kongruent med 7 modulo 12. Alle løsninger av systemet vårt er altså gitt ved:

$$x \equiv 7 \pmod{12}$$

Nå har vi løst systemet, men la oss se litt mer på tabellen vi lagde. Vi kan stokke om på den slik:

x mod 12:	0	9	6	3	4	1	10	7	8	5	2	11
x mod 3:	0	0	0	0	1	1	1	1	2	2	2	2
x mod 4:	0	1	2	3	0	1	2	3	0	1	2	3

Da er det lett å se at ethvert system på formen

$$\begin{cases} x \equiv a \pmod{3} \\ x \equiv b \pmod{4} \end{cases}$$

har en løsning, og løsningen er entydig modulo 12. Hvis vi for eksempel har $a = 0$ og $b = 1$, så gir tabellen at løsningen er $x \equiv 9 \pmod{12}$. Hvis vi har $a = 2$ og $b = 3$, så er løsningen $x \equiv 11 \pmod{12}$. △

La oss nå se på et vilkårlig system

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

av to likninger. Vi antar at de to modulusene m og n er relativt primiske, for det viser seg at det gjør ting mye greiere (mer om dette etterpå).

Kan vi klare å finne løsningen på et slikt system på en enklere måte enn ved å lage en tabell slik som i eksempelet? Siden vi antar at $m \perp n$, sier teorem 5.3 at det finnes heltall u og v slik at $mu + nv = 1$. Da har vi følgende:

$$\begin{aligned} mu &\equiv 0 \pmod{m} & \qquad nv &\equiv 1 \pmod{m} \\ mu &\equiv 1 \pmod{n} & \qquad nv &\equiv 0 \pmod{n} \end{aligned}$$

La c være følgende tall:

$$c = anv + bmu$$

Da er c en løsning av systemet, siden vi har

$$\begin{aligned} c = anv + bmu &\equiv a \cdot 1 + b \cdot 0 = a \pmod{m} \\ c = anv + bmu &\equiv a \cdot 0 + b \cdot 1 = b \pmod{n} \end{aligned}$$

Vi kan dessuten observere at løsningen er entydig modulo mn: Hvis x er en løsning av systemet, så må x være kongruent med c modulo både m og n. Det vil si at $m \mid (x - c)$ og $n \mid (x - c)$, så teorem 5.5 gir at $mn \mid (x - c)$, og da har vi $x \equiv c \pmod{mn}$. Alle løsninger av systemet er altså kongruente med c modulo mn.

Vi oppsummerer det vi har vist nå i et teorem:

Teorem 15.1. *Vi ser på følgende likningssystem*:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Anta at m og n er relativt primiske, og la u og v være heltall slik at $mu + nv = 1$. Da er alle løsninger av systemet gitt ved

$$x \equiv anv + bmu \pmod{mn}.$$

(Når vi skal velge tallene u og v er det egentlig ikke nødvendig at vi har $mu + nv = 1$; det viktige er at u er en invers til m modulo n og at v er en invers til n modulo m.)

Eksempel. Vi løser systemet

$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 9 \pmod{17} \end{cases}$$

ved å bruke teorem 15.1. Modulusene 10 og 17 er relativt primiske, og ved å bruke Euklids algoritme får vi:

$$10 \cdot (-5) + 17 \cdot 3 = 1$$

Det betyr at vi kan velge $u = -5$ og $v = 3$. Løsningen av systemet er:

$$\begin{aligned} x &\equiv 4 \cdot 17 \cdot 3 + 9 \cdot 10 \cdot (-5) = -246 \\ &\equiv 94 \pmod{170} \end{aligned}$$

△

Hvorfor antok vi at de to modulusene i systemet vårt skulle være relativt primiske? La oss se på et par eksempler som viser hva som kan skje hvis de ikke er det.

Eksempel. Vi ser på systemet

$$\begin{cases} x \equiv 4 \pmod 8 \\ x \equiv 9 \pmod{26} \end{cases}$$

der de to modulusene 8 og 26 har en felles faktor 2. Her medfører den første kongruensen at x må være et partall, mens den andre medfører at x må være et oddetall. Dermed finnes det ingen x som oppfyller begge kongruensene. △

Eksempel. Vi ser på systemet

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 9 \end{cases}$$

der de to modulusene 6 og 9 har en felles faktor 3. Ved å prøve oss frem med alle tallene mellom 0 og $6 \cdot 9 = 54$ finner vi ut at både 14, 32 og 50 er løsninger av systemet. △

Hvis modulusene m og n ikke er relativt primiske, kan det altså hende at systemet ikke har noen løsning, eller at det har flere forskjellige løsninger modulo mn. Men hvis m og n *er* relativt primiske, har vi vist både at det finnes en løsning, og at den er entydig modulo mn.

Helt til slutt i notatet skal vi se at vi med litt ekstra jobb kan klare å også håndtere systemer der modulusene ikke er relativt primiske. Men først vil vi generalisere teorem 15.1 til systemer med vilkårlig mange likninger.

Vilkårlig mange likninger

Nå tar vi for oss det generelle tilfellet, altså et system med vilkårlig mange likninger. Da vi skulle løse systemer av to likninger antok vi at modulusene var relativt primiske. Nå vil vi anta at hver modulus er relativt primisk til alle de andre. Vi definerer et navn på denne egenskapen:

Definisjon. La $n_1, n_2, \ldots, n_r$ være en liste med tall. Vi sier at disse tallene er *parvis relativt primiske* dersom n_i er relativt primisk til n_j for alle $i \neq j$. △

Eksempel. Tallene 4, 7 og 15 er parvis relativt primiske, siden vi har $4 \perp 7$ og $4 \perp 15$ og $7 \perp 15$. △

Eksempel. Tallene 32, 5, 17 og 12 er ikke parvis relativt primiske, fordi 32 og 12 ikke er relativt primiske. △

Vi viser først at hvis vi har en liste med tall som er relativt primiske, så er det å være kongruent modulo alle disse tallene det samme som å være kongruent modulo produktet deres:

Lemma 15.2. *La $m_1, m_2, \ldots, m_r$ være naturlige tall som er parvis relativt primiske, og la*

$$M = m_1 \cdot m_2 \cdots m_r$$

være produktet av disse tallene. Da er to tall kongruente modulo M hvis og bare hvis de er kongruente modulo alle tallene $m_1, m_2, \ldots, m_r$. Med andre ord: For alle heltall a og b har vi

$$a \equiv b \pmod M \iff \begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ \vdots \\ a \equiv b \pmod{m_r} \end{cases}$$

Bevis. Det er lett å se at dersom a og b er kongruente modulo M, så er de også kongruente modulo hver m_i: Siden $m_i \mid M$ og $M \mid (a-b)$, gir teorem 2.1 (d) at $m_i \mid (a-b)$.

Anta nå at a og b er kongruente modulo alle tallene $m_1, m_2, \ldots, m_r$, altså at alle disse tallene deler $(a-b)$. Ved å anvende teorem 5.5 flere ganger får vi at $M \mid (a-b)$, altså at $a \equiv b \pmod M$. □

Nå er vi klare for å vise det kinesiske restteoremet. Dette er helt tilsvarende som teorem 15.1 som vi beviste over, men med et system bestående av vilkårlig mange likninger istedenfor bare to.

Teorem 15.3 (Det kinesiske restteoremet)**.** *Vi ser på det følgende systemet av kongruenslikninger*:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Anta at modulusene $m_1, m_2, \ldots, m_r$ er parvis relativt primiske, og la $M = m_1 \cdot m_2 \cdots m_r$ være produktet av modulusene. Da har systemet en entydig løsning modulo M.

Vi kan finne løsningen av systemet på følgende måte. For hver $i \in \{1, 2, \ldots, r\}$: La $M_i = M/m_i$, og la k_i være en invers til M_i modulo m_i. Løsningen av systemet er da gitt ved:

$$x \equiv \sum_{i=1}^{r} a_i M_i k_i \pmod M$$

Bevis. La oss først sjekke at det går an å gjøre det vi sier i teoremet. Vi sa at hver k_i skal være en invers til M_i modulo m_i. Kan vi være sikre på at det finnes en slik invers? Vel, vi har antatt at modulusene er parvis relativt primiske, og vi har definert M_i til å være produktet av alle modulusene unntatt m_i. Det medfører at M_i og m_i er relativt primiske, og dermed har M_i en invers modulo m_i.

Så vil vi sjekke at vi virkelig får en løsning ved å gjøre det teoremet sier. La

$$c = \sum_{i=1}^{r} a_i M_i k_i$$

Vi vil vise at dette tallet er en løsning av alle kongruensene i systemet. Hvis vi lar l være et vilkårlig tall i mengden $\{1, 2, \ldots, r\}$, vil vi altså vise at vi har $c \equiv a_l \pmod{m_l}$. Vi kan først se at enhver M_j med

$j \neq l$ inneholder m_l som en faktor, så alle disse blir bare 0 modulo m_l. Dermed har vi:

$$c = \sum_{i=1}^{r} a_i M_i k_i \equiv a_l M_l k_l \pmod{m_l}$$

Men siden k_l er en invers til M_l modulo m_l har vi $M_l k_l \equiv 1 \pmod{m_l}$, og vi får

$$c \equiv a_l M_l k_l \equiv a_l \cdot 1 \equiv a_l \pmod{m_l}.$$

Siden dette holder for hver $l \in \{1, 2, \ldots, r\}$, har vi:

$$\begin{aligned} a_1 &\equiv c \pmod{m_1} \\ a_2 &\equiv c \pmod{m_2} \\ &\vdots \\ a_r &\equiv c \pmod{m_r} \end{aligned}$$

Dermed kan vi bruke lemma 15.2 og få følgende ekvivalenser:

$$\begin{aligned} x \equiv c \pmod{M} &\iff \left\{ \begin{array}{ll} x \equiv c & \pmod{m_1} \\ x \equiv c & \pmod{m_2} \\ \quad \vdots & \\ x \equiv c & \pmod{m_r} \end{array} \right\} \\ &\iff \left\{ \begin{array}{ll} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ \quad \vdots & \\ x \equiv a_r & \pmod{m_r} \end{array} \right\} \end{aligned}$$

Vi har dermed vist at løsningene av systemet er nøyaktig de tallene som er kongruente med c modulo M. □

Eksempel. Vi løser systemet

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \end{cases}$$

Siden modulusene er parvis relativt primiske, sier det kinesiske restteoremet at systemet har en løsning, som er entydig modulo $M = 3 \cdot 4 \cdot 5 = 60$. La oss nå konstruere løsningen etter oppskriften i teoremet. Vi får

$$M_1 = 20, \qquad M_2 = 15, \qquad M_3 = 12.$$

Vi vet at k_1 skal være en invers til $M_1 = 20$ modulo $m_1 = 3$. Men siden $20 \equiv 2 \pmod 3$ er dette det samme som en invers til 2 modulo 3. Det er lett å se at 2 er sin egen invers modulo 3, siden $2 \cdot 2 = 4 \equiv 1 \pmod 3$. Vi regner ut de andre inversene vi trenger, og får

$$k_1 = 2, \qquad k_2 = 3, \qquad k_3 = 3.$$

Dermed har vi løsningen

$$\begin{aligned} x &\equiv 1 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 2 \cdot 12 \cdot 3 = 247 \\ &\equiv 7 \pmod{60}. \end{aligned}$$

△

Splitt og hersk

Vanligvis bruker vi det kinesiske restteoremet til å løse systemer av kongruenslikninger. Men noen ganger kan det være nyttig å bruke det selv om vi i utgangspunktet bare har én kongruenslikning. Vi ser på et eksempel:

Eksempel. Vi vil regne ut $36! \bmod 1517$. Med andre ord vil vi finne det minste ikkenegative heltallet x slik at $x \equiv 36! \pmod{1517}$.

Vi vet at ved å bruke Wilsons teorem kan vi lett forenkle $36!$ modulo et primtall som er litt større enn 36. Hvis vi primtallsfaktoriserer modulusen vår, ser vi at $1517 = 37 \cdot 41$. Lemma 15.2 forteller oss at kongruensen $x \equiv 36! \pmod{1517}$ er ekvivalent med systemet

$$\begin{cases} x \equiv 36! \pmod{37} \\ x \equiv 36! \pmod{41} \end{cases}$$

Med Wilsons teorem og litt regning kan vi forenkle dette systemet til:

$$\begin{cases} x \equiv -1 \pmod{37} \\ x \equiv 29 \pmod{41} \end{cases}$$

Nå kan vi bruke det kinesiske restteoremet på dette systemet. Vi regner ut at -9 er en invers til 41 modulo 37, og 10 er en invers til 37 modulo 41. Dermed får vi at systemet har følgende løsning:

$$\begin{aligned} x &\equiv -1 \cdot 41 \cdot (-9) + 29 \cdot 37 \cdot 10 = 11099 \\ &\equiv 480 \pmod{1517} \end{aligned}$$

Men systemet var ekvivalent med kongruensen

$$x \equiv 36! \pmod{1517},$$

så løsningen av systemet må være nøyaktig det samme som løsningen av denne. Dermed har vi:

$$36! \equiv 480 \pmod{1517}$$

Det betyr at $36! \bmod 1517 = 480$. △

Vi kan tenke på det vi gjorde i dette eksemplet som en «splitt og hersk»-strategi: Vi startet med én vanskelig kongruens, og splittet den opp i to mer håndterlige kongruenser.

Litt mer generelt kan den samme ideen beskrives slik: Vi starter med en kongruens $x \equiv s \pmod{M}$, der s er et uttrykk som er vanskelig å forenkle modulo M. Vi skriver M som et produkt

$$M = m_1 \cdot m_2 \cdots m_r$$

av parvis relativt primiske tall, og bruker lemma 15.2 til å skrive om kongruensen vår til systemet

$$\begin{cases} x \equiv s \pmod{m_1} \\ x \equiv s \pmod{m_2} \\ \quad \vdots \\ x \equiv s \pmod{m_r} \end{cases}$$

Nå er det (forhåpentligvis) mulig å forenkle uttrykket s modulo hver av de nye og mindre modulusene,

og vi finner små tall $a_1, a_2, \ldots, a_r$ som er kongruente med s modulo henholdsvis $m_1, m_2, \ldots, m_r$. Dermed kan systemet over skrives om til

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Til slutt bruker vi det kinesiske restteoremet for å komme tilbake til én kongruens modulo M.

Ikke relativt primiske moduluser

Ved hjelp av det kinesiske restteoremet vet vi alt vi trenger å vite om systemer

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

der modulusene $m_1, m_2, \ldots, m_r$ er parvis relativt primiske: Vi vet at det finnes en løsning, at den er entydig modulo $M = m_1 \cdot m_2 \cdots m_r$, og vi vet hvordan vi kan finne løsningen.

Men hva om vi vil løse et system der modulusene *ikke* er parvis relativt primiske? Hva kan vi gjøre da?

Da kan vi ikke være sikre på at det finnes en løsning (se det første eksempelet på s. 30). På den annen side kan vi heller ikke være sikre på at det *ikke* finnes en løsning (se det andre eksempelet på s. 30).

Det vi må gjøre med et slikt system er for det første å finne ut om det har noen løsning eller ikke. Da kan vi se på alle par av likninger i systemet som ikke har relativt primiske moduluser, og sjekke om de er i konflikt med hverandre. For eksempel er kongruensene

$$\begin{cases} x \equiv 12 \pmod{20} \\ x \equiv 29 \pmod{35} \end{cases}$$

i konflikt med hverandre, fordi den første av dem medfører at $x \equiv 2 \pmod 5$, mens den andre medfører at $x \equiv 4 \pmod 5$. Da er det ikke mulig at begge er oppfylt samtidig.

Hvis ingen av kongruensene i systemet har slike konflikter, kan vi skrive om systemet til et nytt system der modulusene er parvis relativt primiske. Det følgende eksempelet viser hvordan dette kan gjøres.

Eksempel. Vi vil løse dette systemet:

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 5 \pmod{9} \\ x \equiv 11 \pmod{12} \end{cases}$$

Modulusene er ikke parvis relativt primiske, siden $\gcd(4, 12) = 4$ og $\gcd(9, 12) = 3$. Men ved lemma 15.2 vet vi at kongruensen

$$x \equiv 11 \pmod{12}$$

er ekvivalent med de to kongruensene

$$\begin{cases} x \equiv 11 \pmod 3 \\ x \equiv 11 \pmod 4 \end{cases}$$

(siden $12 = 3 \cdot 4$ og $3 \perp 4$). Disse kan vi forenkle til:

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

Vi kan altså sette inn disse to likningene istedenfor $x \equiv 11 \pmod{12}$ i systemet vårt, og få et ekvivalent system:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 7 \\ x \equiv 5 \pmod 9 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \end{cases}$$

Her kan vi for det første legge merke til at den samme likningen, $x \equiv 3 \pmod 4$, står to ganger, så vi kan sløyfe den ene av dem. Videre kan vi observere at hvis $x \equiv 5 \pmod 9$ er oppfylt, så må også $x \equiv 2 \pmod 3$ være oppfylt, slik at den sistnevnte er overflødig.

Systemet kan dermed forenkles til:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 7 \\ x \equiv 5 \pmod 9 \end{cases}$$

Nå har vi endelig fått et system der modulusene er parvis relativt primiske, og dermed kan vi løse det med det kinesiske restteoremet. Da finner vi løsningen

$$x \equiv 203 \pmod{252}. \qquad \triangle$$

Her brukte vi «splitt og hersk»-strategien vår på kongruensen med 12 som modulus, og erstattet den med kongruenser modulo henholdsvis 3 og 4, som vi så sammenlignet med de andre kongruensene i systemet.

Det kan være fristende å prøve å splitte opp kongruensen med 9 som modulus på samme måte: Siden $9 = 3 \cdot 3$, kan vi vel splitte den opp i to kongruenser som begge har 3 som modulus? Men nei, det kan vi ikke gjøre, siden 3 ikke er relativt primisk til seg selv. Når vi vil splitte en kongruens i flere på denne måten, må vi alltid passe på at de nye modulusene er parvis relativt primiske.

Det vi gjorde isteden, var å sammenligne de to kongruensene

$$\begin{cases} x \equiv 5 \pmod 9 \\ x \equiv 2 \pmod 3 \end{cases}$$

og se at den første av dem medfører den andre. Her er det viktig å legge merke til at disse to kongruensene ikke sier nøyaktig det samme, for den første stiller sterkere krav til x enn den andre gjør (for eksempel er 8 en løsning av den andre kongruensen, men ikke av den første). Dermed kan vi beholde den første og sløyfe den andre uten at det påvirker hvilke løsninger vi får, men vi kan ikke sløyfe den første og beholde den andre.

Med det kinesiske restteoremet og ideene fra dette eksempelet er vi i stand til å håndtere et hvilket som helst system av kongruenslikninger. (Hurra!)