Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

# MA1301 Tallteori
# Høst 2020

**Løsningsforslag — Øving 5**

**4.3.1** Vi ser at $53 = 32 + 16 + 4 + 1 = 2^5 + 2^4 + 2^2 + 2^0$, så vi regner ut $19^2 \pmod{503}$ for $0 \leq j \leq 5$.

$$\begin{aligned} 19^2 &\equiv 361 \pmod{503} \\ 19^4 \equiv 361^2 &\equiv 130132 \equiv 44 \pmod{503} \\ 19^8 \equiv 44^2 &\equiv 1936 \equiv 427 \pmod{503} \\ 19^{16} \equiv 427^2 &\equiv 182329 \equiv 243 \pmod{503} \\ 19^{32} \equiv 243^2 &\equiv 59049 \equiv 198 \pmod{503} \end{aligned}$$

Dermed får vi at

$$\begin{aligned} 19^{53} &= 19^{32+16+4+1} \\ &= 19^{32} \cdot 19^{16} \cdot 19^4 \cdot 19^1 \\ &\equiv 198 \cdot 243 \cdot 44 \cdot 19 \equiv 36201316 \equiv 406 \pmod{503} \end{aligned}$$

På samme måte ser vi at $47 = 32 + 8 + 4 + 2 + 1$, så vi regner ut $141^{2^j}$ for $0 \leq j \leq 5$.

$$\begin{aligned} 141^2 &\equiv -100 \pmod{1537} \\ 141^4 &\equiv 778 \pmod{1537} \\ 141^8 &\equiv -294 \pmod{1537} \\ 141^{16} &\equiv 364 \pmod{1537} \\ 141^{32} &\equiv 314 \pmod{1537} \end{aligned}$$

Dermed får vi at

$$\begin{aligned} 141^{47} &= 141^{32+8+4+2+1} \\ &= 141^{32} \cdot 141^8 \cdot 141^4 \cdot 141^2 \cdot 141^1 \\ &\equiv 314 \cdot (-294) \cdot 778 \cdot (-100) \cdot 141 \equiv 658 \pmod{1537} \end{aligned}$$

**4.3.9** Vi ser at $4444 = 2 \cdot 2222$, og at $2222 \equiv (-1) \pmod 9$ (lett å se, siden $2223 = 2222 + 1$ har tverrsum lik 9, og dermed er delelig på 9). Altså får vi at

$$\begin{aligned} 4444^{4444} &\equiv 2^{4444} \cdot 2222^{4444} \pmod 9 \\ &\equiv 2 \cdot 2^{3 \cdot 1481} \cdot (-1)^{4444} \pmod 9 \\ &\equiv 2 \cdot (-1)^{1481} \cdot 1 \pmod 9 \\ &\equiv 2 \cdot (-1) \equiv 7 \pmod 9 \end{aligned}$$

Altså er resten når vi deler $4444^{4444}$ på 9 lik 7.

**4.3.25** Vi skal vise at $10^{2p} - 10^p + 1$ er delelig på 13 for alle primtall $p > 3$. Hintet vi har fått sier at $3^3 \equiv 1 \pmod{13}$, så for å kunne benytte oss av det må vi finne en måte å modifisere uttrykket til noe som inneholder 3 på en eller annen måte. Vi legger merke til at $10 \equiv (-3) \equiv (-1) \cdot 3 \pmod{13}$, som betyr at

$$10^p \equiv (-1)^p \cdot 3^p$$

Nå bruker vi hintet: siden $p$ er et oddetall vil $(-1)^p = (-1)$, og siden $p$ ikke er delelig på 3 kan den skrives som $p = 3k + r$ hvor $r \in \{1, 2\}$. Dermed blir

$$(-1)^p \cdot 3^p \equiv (-1) \cdot 3^{3k+r} \equiv (-1) \cdot (3^3)^k \cdot 3^r \equiv -3^r \pmod{13}$$

Hvor den siste kongruensen kommer av at $3^3 \equiv 1 \pmod{13}$. Altså er $10^p \equiv -3^r \pmod{13}$, og følgelig er $10^{2p} \equiv (-3^r)^2 \equiv 3^{2r} \pmod{13}$, hvor $r \in \{1, 2\}$. Hvis vi setter dette inn i uttrykket fra starten, får vi

$$10^{2p} - 10^p + 1 \equiv 3^{2r} + 3^r + 1 \equiv \begin{cases} 3^2 + 3 + 1 \equiv 0 \pmod{13}, & \text{hvis } r = 1 \\ 3^4 + 3^2 + 1 \equiv 0 \pmod{13}, & \text{hvis } r = 2 \end{cases}$$

Altså er $10^{2p} - 10^p + 1$ alltid delelig på 13 når $p > 3$ er et primtall.

**4.3.27a)** Vi setter inn tallet 0-07-232569-0 i formelen, og får

$$\begin{aligned} \sum_{k=1}^{9} k a_k &= 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 3 + 6 \cdot 2 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 9 \\ &= 0 + 0 + 21 + 8 + 15 + 12 + 35 + 48 + 81 \\ &= 220 \\ &\equiv 0 \pmod{11} \end{aligned}$$

Siden $a_{10} = 0$ betyr dette at tallet er et gyldig ISBN.

**4.4.1b)** Vi observerer først at $\gcd(5, 26) = 1$, og siden $1 \mid 2$ har kongruensligningen en løsning, og den er unik modulo 26. La oss nå finne løsningen. Vi ser at

$$25 \equiv -1 \pmod{26},$$

så hvis vi ganger kongruensligningen med 5 på begge sidene får vi

$$\begin{aligned} 5 \cdot 5x \equiv 25x \equiv -x &\equiv 10 \pmod{26} \\ x &\equiv -10 \equiv 16 \pmod{26} \end{aligned}$$

**4.4.5** Vi skal løse kongruensligningen $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ ved å løse systemet

$$\begin{aligned} 17x &\equiv 3 \pmod{2} \\ 17x &\equiv 3 \pmod{3} \\ 17x &\equiv 3 \pmod{5} \\ 17x &\equiv 3 \pmod{7} \end{aligned}$$

Vi løser kongruensene hver for seg

$$\begin{aligned} 17x \equiv x \equiv 3 &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 2 \end{aligned}$$

$$\begin{aligned} 17x \equiv -x \equiv 3 &\equiv 0 \pmod 3 \\ x &\equiv 0 \pmod 3 \end{aligned}$$

$$\begin{aligned} 17x \equiv -3x &\equiv 3 \pmod 5 \\ x &\equiv -1 \pmod 5 \end{aligned}$$

$$\begin{aligned} 17x \equiv 3x &\equiv 3 \pmod 7 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

Nå kan vi bruke det kinesiske restteoremet (siden $2, 3, 5, 7$ er parvis relativt primiske) til å si at den lineære kongruensen vi begynte med har en unik løsning modulo $2 \cdot 3 \cdot 5 \cdot 7 = 210$. Vi regner ut

$$\frac{210}{2} = 105, \qquad \frac{210}{3} = 70, \qquad \frac{210}{5} = 42, \qquad \frac{210}{7} = 30$$

Nå setter vi opp de lineære kongruensene

$$105x \equiv 1 \pmod 2, \quad 70x \equiv 1 \pmod 3, \quad 42x \equiv 1 \pmod 5, \quad 30x \equiv 1 \pmod 7$$

som har løsninger hhv. $x_1 = 1, x_2 = 1, x_3 = 3, x_4 = 4$. Vi setter dette inn i formelen som er gitt i beviset til teorem 4.8 i boken, og får at løsningen er gitt ved

$$\begin{aligned} x &= 1 \cdot (3 \cdot 5 \cdot 7) \cdot 1 + 0 \cdot (2 \cdot 5 \cdot 7) \cdot 1 + (-1) \cdot (2 \cdot 3 \cdot 7) \cdot 3 + 1 \cdot (2 \cdot 3 \cdot 5) \cdot 4 \\ &= 105 + 0 - 126 + 120 \\ &= 99 \end{aligned}$$

Dermed får vi at løsningen til den lineære kongruensen er $x \equiv 99 \pmod{210}$.

**4.4.6** Vi begynner med å oversette oppgaven til et system av lineære kongruenser. Vi skal finne det minste heltallet $a > 2$ som tilfredsstiller systemet

$$\begin{aligned} a &\equiv 0 \pmod 2 \\ a \equiv -1 &\equiv 2 \pmod 3 \\ a \equiv -2 &\equiv 2 \pmod 4 \\ a \equiv -3 &\equiv 2 \pmod 5 \\ a \equiv -4 &\equiv 2 \pmod 6 \end{aligned}$$

Vi ser at den tredje kongruensen gjør den første overflødig, og den andre og tredje gjør til sammen den siste overflødig (om du ikke ser hvorfor, prøv å skrive ned hva

det er disse kongruensene faktisk sier om $a$). Altså er dette systemet ekvivalent med systemet

$$\begin{aligned} a &\equiv 2 \pmod 3 \\ a &\equiv 2 \pmod 4 \\ a &\equiv 2 \pmod 5 \end{aligned}$$

hvor $3, 4$ og $5$ er parvis relativt primiske. Dermed kan vi bruke det kinesiske restteoremet til å si at systemet har en unik løsning modulo $3 \cdot 4 \cdot 5 = 60$. Nå holder det å observere at 2 er en løsning til systemet, og siden løsningen er unik modulo 60 vil det minste tallet $a > 2$ som oppfyller alle kongruensene være $2 + 60 = 62$.

Hvis vi ikke hadde lagt merke til at 2 er en løsning, kunne vi regnet det ut på samme måte som i forrige oppgave. først finner vi

$$\frac{60}{3} = 20, \qquad \frac{60}{4} = 15, \qquad \frac{60}{5} = 12,$$

og løser kongruensene

$$20x \equiv 1 \pmod 3, \quad 15x \equiv 1 \pmod 4, \quad 12x \equiv 1 \pmod 5).$$

Vi ser at hhv. $x_1 = 2, x_2 = 3, x_3 = 3$ løser dem. Setter dette inn i formelen fra beviset for det kinesiske restteoremet, og får

$$\begin{aligned} a &= 2 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 2 \cdot 12 \cdot 3 \\ &= 80 + 90 + 72 \\ &= 242 \end{aligned}$$

Dermed er $a \equiv 242 \equiv 62 \pmod{60}$, som betyr at det minste tallet $a > 2$ som oppfyller alle delelighetskravene fra oppgaven er 62.

**Eksamen H2019 oppg. 5** Denne oppgaven kan også løses på samme måte som de to forrige oppgavene, men for treningens skyld bruker vi den alternative metoden for å løse system av lineære kongruenser. Vi har systemet

$$\begin{aligned} 3x &\equiv 1 \pmod 7 \\ x &\equiv 0 \pmod 5 \\ 5x &\equiv 1 \pmod 9 \end{aligned}$$

Ved å bruke at $5 \cdot 3 \equiv 1 \pmod 7$ og $5 \cdot 2 \equiv 1 \pmod 9$ skriver vi om systemet til standardform

$$\begin{aligned} x &\equiv 5 \pmod 7 \\ x &\equiv 0 \pmod 5 \\ x &\equiv 2 \pmod 9 \end{aligned}$$

Fra den andre kongruensen ser vi at $x = 5t$ for $t \in \mathbb{Z}$. Dermed kan vi sette dette inn i den første kongruensen, og få at

$$\begin{aligned} x \equiv 5t &\equiv 5 \pmod 7 \\ t &\equiv 1 \pmod 7 \end{aligned}$$

Altså må $t = 1 + 7s$ for $s \in \mathbb{Z}$. Dette gir at $x = 5t = 5 + 35s$. Vi setter inn dette i den siste kongruensen i systemet, og får

$$\begin{aligned} x &\equiv 5 + 35s \equiv 2 \pmod 9 \\ 35s &\equiv (-1) \cdot s \equiv -3 \pmod 9 \\ s &\equiv 3 \pmod 9 \end{aligned}$$

Dette gir at $s = 3 + 9r$, for $r \in \mathbb{Z}$, som igjen betyr at $x = 5 + 35s = 5 + 35(3 + 9r) = 110 + 315r$. Så alle heltallsløsninger til det gitte systemet er på formen $110 + 315r$ for $r \in \mathbb{Z}$.

Eksamen K2019 oppg. 3 Vi skal finne alle heltallsløsninger til systemet

$$\begin{aligned} x &\equiv -7 \pmod 8 \\ 5x &\equiv 1 \pmod 3 \\ x &\equiv -2 \pmod 5 \end{aligned}$$

Igjen kan vi løse det på to måter, og vi velger å følge den alternative metoden, slik vi gjorde i forrige oppgave. Vi bruker at $2 \cdot 5 \equiv 1 \pmod 3$ til å skrive om systemet til standardform

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Den første kongruensen sier at $x = 1 + 8t$ for $t \in \mathbb{Z}$. Vi setter dette inn i den andre kongruensen, og får at

$$\begin{aligned} x &\equiv 1 + 8t \equiv 2 \pmod 3 \\ 8t &\equiv 2t \equiv 1 \pmod 3 \\ t &\equiv 2 \pmod 3 \end{aligned}$$

Dermed er $t = 2 + 3s$ for $s \in \mathbb{Z}$, som betyr at $x = 1 + 8t = 1 + 8(2 + 3s) = 17 + 24s$. Vi setter dette inn i den siste kongruensen, og får

$$\begin{aligned} x &\equiv 17 + 24s \equiv 3 \pmod 5 \\ 24s &\equiv -s \equiv -14 \equiv 1 \pmod 5 \\ s &\equiv -1 \pmod 5 \end{aligned}$$

Dermed er $s = 5r - 1$ for $r \in \mathbb{Z}$, som betyr at $x = 17 + 24s = 17 + 24(5r - 1) = 120r - 7$. Altså er alle heltallsløsningene til systemet i oppgaven gitt som $120r - 7$, for $r \in \mathbb{Z}$.