Øving 5

4.4.1 e: $34x \equiv 60 \pmod{98}$.

Ser at $\gcd(34,98) = 2$ og man finner at $2 = 34(-23) + 98 \cdot 8$. Mult. med 30 gir

$$60 = 34(-690) + 98(240)$$

mao

$$x_0 = -690 \quad \text{er en løsning.}$$

Siden $\gcd(34,98) = 2$ skal vi ha 2 inkongruente løsninger modulo 98, de er gitt som

$$x = -690 + \tfrac{98}{2} \cdot t \quad , \; t \in \mathbb{Z}$$

De minste (positive) løsningen er da

$$x_0 = 45 \quad \text{og} \quad x_0 = 94 \quad (\text{modulo } 98)$$

4.4.4 c:

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$$

Løser først

$$187x \equiv 1 \pmod 6 \iff x \equiv 1 \pmod 6$$
$$102x \equiv 1 \pmod{11} \iff 3x \equiv 1 \pmod{11}$$
$$66x \equiv 1 \pmod{17} \iff 15x \equiv 1 \pmod{17}$$

som gir $x_1 = 1$, $x_2 = 4$, $x_3 = 8$

La så $X = 5\cdot 187\cdot 1 + 4\cdot 102\cdot 4 + 3\cdot 66\cdot 8$

$$= 935 + 1632 + 1584$$

$$= 4151$$

La $N = 6\cdot 11\cdot 17 = 1122$. Får så at

$$\underline{X \equiv 785 \pmod{1122}}$$

<u>4.4.10</u> $x :=$ gullungenter

$$x \equiv 3 \pmod{17}$$
$$x \equiv 10 \pmod{16}$$
$$x \equiv 0 \pmod{15}$$

Løser først

$$240x \equiv 1 \pmod{17} \iff 2x \equiv 1 \pmod{17}$$
$$255x \equiv 1 \pmod{16} \iff -x \equiv 1 \pmod{16}$$
$$(*) \quad 272x \equiv 1 \pmod{15}$$

<u>Merk:</u> Vi trenger ikke å løse (*) da det ikke bidrar i den endelige løsningen.

Får $x_1 = 9$, $x_2 = -1$, som gir

$$X = 3\cdot 240\cdot 9 + 10\cdot 255\cdot(-1) + 0$$

$$= 6480 - 2550 = \underline{\underline{3930}} \pmod{\underset{15\cdot 16\cdot 17}{\overset{\shortparallel}{4080}}}$$

4.4.13 Anta $x \equiv a \pmod{n}$. Dette er det samme som at $x - a = k \cdot n$. Nå har vi to tilfeller a betrakte: enten $2 \mid k$ eller ikke. Dersom $2 \mid k$, har vi $k = 2t$, $t \in \mathbb{Z}$. dvs $x - a = 2n \cdot t \iff x \equiv a \pmod{2n}$ og vi er i mål. Dersom $2 \nmid k$, så sier div. alg at $k = 2t+1$, $t \in \mathbb{Z}$, Altså har vi $x - a = (2t+1)n = 2nt + n$ som gir at $2n \mid x - a - n \iff$

$x \equiv a + n \pmod{2n}$

Som var det vi skulle vise.

4.4.14: Har følgende kongruenser:

$$x \equiv 1 \pmod{9}$$
$$x \equiv 2 \pmod{11}$$
$$x \equiv 6 \pmod{13}$$

Løser først:

$$143x \equiv 1 \pmod{9} \iff -x \equiv 1 \pmod{9}$$
$$117x \equiv 1 \pmod{11} \iff 7x \equiv 1 \pmod{11}$$
$$99x \equiv 1 \pmod{13} \iff -5x \equiv 1 \pmod{13}$$

og får $x_1 = -1$, $x_2 = -3$, $x_3 = 5$

La $X = 1\cdot(-1)\cdot 143 + 2\cdot(-3)\cdot 117 + 6\cdot 5\cdot 99$

$= -143 - 702 + 2970$

$= 2125 \equiv 838 \pmod{1287}$

5.2.2a Anta $\gcd(a, 35) = 1$, dvs $\gcd(a, 5) = 1$ og $\gcd(a, 7) = 1$. Vi kan da bruke Fermats lille:

$$a^4 \equiv 1 \pmod 5$$

og

$$a^6 \equiv 1 \pmod 7$$

Får da at $a^{12} = (a^4)^3 \equiv 1^3 = 1 \pmod 5$

og $a^{12} = (a^6)^2 \equiv 1^2 = 1 \pmod 7$

siden $\gcd(5, 7) = 1$ får vi at

$$a^{12} \equiv 1 \pmod{35}.$$

5.2.4a Ved Korollaret til Fermats lille har vi at $a^5 \equiv a \pmod 5$. Får da at

$$a^{21} = a^{20}\cdot a = (a^5)^4\cdot a \equiv a^4\cdot a = a^5 \equiv a \pmod 5.$$

5.2.10a Antag $\gcd(a,p)=\gcd(b,p)=1$ og $a^p \equiv b^p \pmod p$. Ved Fermats lille (Korollaret) har vi at

$$a \underset{\text{Fermat}}{\equiv} a^p \equiv b^p \underset{\text{Fermat.}}{\equiv} b \pmod p$$

5.3.1a Wilsons teorem giver at

$$16! \equiv -1 \pmod{17}$$

$$\Rightarrow \quad 15! \cdot 16 \equiv -1 \pmod{17}$$

men $16 \equiv -1 \pmod{17}$

$$\Rightarrow \quad 15! \cdot (-1) \equiv -1 \pmod{17}$$

(mult. med -1)

$$\Rightarrow \quad 15! \equiv 1 \pmod{17}$$

5.3.6 Wilson giver at $(p-1)! \equiv -1 \pmod p$ men $-1 \equiv p-1 \pmod p$, dvs $(p-1)! \equiv p-1 \pmod p$. Har også trivielt at $(p-1)! \equiv p-1 \pmod{(p-1)}$, siden $p-1 \equiv 0 \pmod{(p-1)}$, dette giver da at $2\cdot(p-1)! \equiv 2(p-1) \pmod{p-1}$. Antag vi at $p>2$, vi kan da konkludere: $(p-1)! \equiv p-1 \pmod{\frac{p-1}{2}}$ siden $\gcd(p, p-\frac{1}{2})=1$ får vi $(p-1)! \equiv p-1 \pmod{\frac{p(p-1)}{2}}$ dvs $1+2+3+\dots+p-1 = \frac{p(p-1)}{2}$

HO4.3 Vi har

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 1 \pmod 7 \end{cases}$$

Løser først:

$42x \equiv 1 \pmod 5 \iff 2x \equiv 1 \pmod 5$

$35x \equiv 1 \pmod 6 \iff -x \equiv 1 \pmod 6$

$30x \equiv 1 \pmod 7 \iff 2x \equiv 1 \pmod 7$

Som gir $x_1 = 3$, $x_2 = -1$, $x_3 = 4$.

La så $X = 2 \cdot 42 \cdot 3 - 1 \cdot 35 \cdot 1 + 1 \cdot 30 \cdot 4$

$= 252 - 35 + 120$

$= 337$

$X = 347 \equiv 127 \pmod{210}$

HO4.4. Wilson gir at $36! \equiv -1 \pmod{37}$

$\Rightarrow 35!\,36 \equiv 35! \cdot (-1) \pmod{37}$

$\Rightarrow 35! \equiv 1 \pmod{37}$

$\Rightarrow 35! - 35 \equiv 1 - 35 \equiv 1 + 2 = 3 \pmod{37}$

H06.3

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

Vi gjør om og får

$x \equiv 2 \pmod 3$

$x \equiv 4 \pmod 5$ (siden $2 \cdot 3 = 6 \equiv 1 \pmod 5$)

$x \equiv 6 \pmod 7$ (siden $3 \cdot 5 = 15 \equiv 1 \pmod 7$)

som gir

$$x \equiv 104 \pmod{105}$$