H2023

Oppg 1 Euklids alg på 72 og 177:

$$\left.\begin{aligned} 177 &= 2\cdot 72 + 33 \\ 72 &= 2\cdot 33 + 6 \\ 33 &= 5\cdot 6 + 3 \\ 6 &= 2\cdot 3 + 0 \end{aligned}\right\} \text{ så } \gcd(72,177)=3 \ (\Rightarrow \text{løsbar siden } 3\mid 6)$$

Bakover:

$$3 = 33 - 5\cdot 6 = 33 - 5(72-2\cdot 33) = 11\cdot 33 - 5\cdot 72$$
$$= 11(177-2\cdot 72) - 5\cdot 72 = 72\cdot(-27) + 177\cdot 11$$

$$\Rightarrow 6 = 2\cdot(72\cdot(-27) + 177\cdot 11)$$
$$= 72\cdot(-54) + 177\cdot 22$$

Så en løsn er $x_0 = -54$, $y_0 = 22$. Alle løsn:

$$\left.\begin{aligned} x &= -54 + {}^{177}/_{3}\, t = -54 + 59t \\ y &= 22 - {}^{72}/_{3}\, t = 22 - 24t \end{aligned}\right\} t \in \mathbb{Z}$$

Oppg 2 Sett $N_1 = 7\cdot 11 = 77$, $N_2 = 6\cdot 11 = 66$, $N_3 = 6\cdot 7 = 42$. Løser så disse individuelt:

$$77x_1 \equiv 1 \pmod 6 \longrightarrow x_1 = -1 \text{ en løsn}$$
$$66x_2 \equiv 1 \pmod 7 \longrightarrow x_2 = -2 \text{ en løsn}$$
$$42x_3 \equiv 1 \pmod{11} \longrightarrow x_3 = 5 \text{ en løsn}$$

Gir $\bar{x} = 3\cdot 77\cdot(-1) + (-4)\cdot 66\cdot(-2) + 2\cdot 42\cdot 5 = 717$

Så ved det kinesiske restteorem er løsn av syst:

$$x \equiv 717 \pmod{462} \qquad (462 = 6\cdot 7\cdot 11)$$

Oppg 3 (a) Har $33 = 3\cdot 11$ og $3 \nmid 1301$ og $11 \nmid 1301$, så $\gcd(1301, 33) = 1$. Da gir Eulers teorem at $1301^{\phi(33)} \equiv 1 \pmod{33}$. Har

$$\phi(33) = (3-1)(11-1) = 20$$

$$\Rightarrow 1301^{20} \equiv 1 \pmod{33}$$

$$\Rightarrow 1301^{2020} \equiv 1301^{20\cdot 101} \equiv (1301^{20})^{101} \equiv 1^{101} \equiv 1 \pmod{33}$$

$$\Rightarrow 1301^{2023} \equiv 1301^3 \cdot 1301^{2020} \equiv 1301^3 \equiv 121^3 \equiv 27424$$
$$\equiv 5 \pmod{33}$$

Så vi får <u>5 i rest</u>

(b) Siden 1301 er prim gir Wilsons teorem at

$$1300! \equiv -1 \equiv 1300 \pmod{1301}$$
$$\Rightarrow 1299! \equiv 1 \pmod{1301}$$ (siden $\gcd(1301, 1300) = 1$ kan vi dele ut 1300)
$$\Rightarrow 2023 \cdot (1299!) \equiv 2023 \equiv 722 \pmod{1301}$$

Så vi får <u>722 i rest</u>.

<u>Oppg 4</u> (a)

Har $\phi(221) = (13-1)(17-1) = 192$ (og $e = 169$ tilfredsstiller $1 < e < 192$ og $\gcd(e, 192) = 1$). Eksponenten d er minste pos løsn av

$$ex \equiv 1 \pmod{\phi(n)}$$

dvs $169x \equiv 1 \pmod{192}$

Euklids alg:

$$\left.\begin{aligned} 192 &= 169 + 23 \\ 169 &= 7 \cdot 23 + 8 \\ 23 &= 2 \cdot 8 + 7 \\ 8 &= 7 + 1 \end{aligned}\right\} \Rightarrow 1 = 8 - 7 = 8 - (23 - 2 \cdot 8) = 3 \cdot 8 - 23$$
$$= 3(169 - 7 \cdot 23) - 23 = 3 \cdot 169 - 22 \cdot 23$$
$$= 3 \cdot 169 - 22(192 - 169) = 25 \cdot 169 - 22 \cdot 192$$
$$\Rightarrow 192 \mid (169 \cdot 25 - 1)$$

Så $x_0 = 25$ er en løsn av $169x \equiv 1 \pmod{192}$. Dette er minste pos løsn, så <u>$d = 25$</u>

(b) Må finne minste ikke-neg r med $c^d \equiv r \pmod{n}$, dvs

$$6^{25} \equiv r \pmod{221}$$

Har

$$6^3 \equiv 216 \equiv -5 \pmod{221}$$
$$\Rightarrow 6^{24} \equiv (6^3)^8 \equiv (-5)^8 \equiv 390625 \equiv 118 \pmod{221}$$
$$\Rightarrow 6^{25} \equiv 6 \cdot 118 \equiv 708 \equiv 45 \pmod{221}$$

Så <u>vi får 45</u> når vi dekrypterer $c = 6$

Oppg 5

For $n=1$ er venstre side $1^3 = 1$, mens høyre side er

$$\frac{1^2 \cdot (1+1)^2}{4} = 1$$

Så det stemmer for $n=1$. Anta nå at det stemmer for en k, dvs

$$1^3 + 2^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}$$

Da blir

$$\begin{aligned}
1^3 + 2^3 + \cdots + (k+1)^3 &= \left(1^3 + 2^3 + \cdots + k^3\right) + (k+1)^3 \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
&= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\
&= \frac{(k+1)^2\left(k^2 + 4(k+1)\right)}{4} \\
&= \frac{(k+1)^2(k^2+4k+4)}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4} \\
&= \frac{(k+1)^2\left((k+1)+1\right)^2}{4}
\end{aligned}$$

Så da stemmer det også for $k+1$. Altså stemmer det $\forall n \geq 1$.

Oppg 6 (a)

Har $\phi(11) = 10 = 2 \cdot 5$. Siden ordenen til et tall modulo 11 må dele $\phi(11) = 10$, må ordenen være en av $1, 2, 5, 10$. Modulo 11 har vi:

$1^1 \equiv 1$

$2^1, 2^2, 2^5 \not\equiv 1 \Rightarrow$ 2 har orden 10

$3^5 \equiv 1$

$4^5 \equiv 1$

$5^5 \equiv 1$

$6^1, 6^2, 6^5 \not\equiv 1 \Rightarrow$ 6 har orden 10

$7^1, 7^2, 7^5 \not\equiv 1 \Rightarrow$ 7 har orden 10

$8^1, 8^2, 8^5 \not\equiv 1 \Rightarrow$ 8 har orden 10

Så 2, 6, 7, 8 er primitive røtter for 11. Siden $\phi(11-1) = 4$ er dette alle.

For 8 må vi sjekke 1, 3, 5, 7, siden disse representerer alle a med $\gcd(a, 8) = 1$. Modulo 8 har vi:

$1^1 \equiv 1$

$3^2 \equiv 1$

$5^2 \equiv 1$

$7^2 \equiv 1$

Siden $\phi(8) = 4$ har da 8 ingen p.r.

(b) For $p = 2$ er $n = 8$, som ikke har p.r. ifra (a). Anta nå at p er odde. Siden $\gcd(4, p) = 1$ er da

$$\phi(n) = \phi(4) \cdot \phi(p) = 2(p-1)$$

La nå $a \in \mathbb{Z}$ med $\gcd(a, n) = 1$. Da er

$$\gcd(a, 4) = 1 = \gcd(a, p)$$

så Eulers teorem gir

$$a^{\phi(4)} \equiv 1 \pmod 4 \Rightarrow a^2 \equiv 1 \pmod 4$$

$$a^{\phi(p)} \equiv 1 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p \quad \text{(evt Fermats teorem her)}$$

Siden p er odde er $p-1$ partall, så $p - 1 = 2k$ for en $k \geq 1$

$$\Rightarrow a^{p-1} \equiv (a^2)^k \equiv 1^k \equiv 1 \pmod 4$$

Altså: $4 \mid (a^{p-1} - 1)$ og $p \mid (a^{p-1} - 1)$. Siden $\gcd(4, p) = 1$ vil da

$$4p \mid (a^{p-1} - 1)$$

dvs $a^{p-1} \equiv 1 \pmod n$

Da har a ikke orden $\phi(n) = 2(p-1)$, så n har ingen p.r.

Oppg 7

Se på Legendre-symbolet $\left(\frac{p}{q}\right)$. Loven om kvadratisk gjensidighet gir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot 2p} = 1 \quad \left(\begin{array}{l} p \text{ er odde, og det er} \\ \text{også } q = 4p+1 \end{array}\right)$$

Siden $q = 4p + 1$ er $q \equiv 1 \pmod p$, så $\left(\frac{q}{p}\right) = \left(\frac{1}{p}\right) = 1$

$$\Rightarrow \left(\frac{p}{q}\right) = 1$$

$\Rightarrow x^2 \equiv p \pmod q$ løsbar