Øving 9

EH.06.2

Vi skal finne $2007^{2006} \bmod 1000$

Har at $2007 = 3^2 \cdot 223$, dvs $\gcd(1000, 2007) = 1$

og vi kan derfor benytte oss av Eulers teorem. ($\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$)

$$2007^{400} \equiv 1 \pmod{1000}$$

Dvs

$$2007^{2006} = (2007^{400})^5 \, 2007^6$$

$$\equiv 1^5 \cdot 7^6 \pmod{1000}$$

$$\equiv 401 \cdot 49 \pmod{1000}$$

$$\equiv \underline{649} \pmod{1000}$$

$7^4 = 2401$ gir

$7^2 = 49$

$401 \cdot 49 = 19649$ gir

EH.06.5 (EH.06.6 se lf øving 8)

Her er $n = 55 = 5 \cdot 11$ og $\varphi(n) = (5-1)(11-1)$
$= 4 \cdot 10 = 40$

Vi må løse $37 \cdot d \equiv 1 \pmod{40}$

$$\left.\begin{aligned} 40 &= 37 + 3 \\ 37 &= 13 \cdot 3 + 1 \end{aligned}\right\} \Rightarrow \begin{aligned} 1 &= 37 - 13 \cdot 3 \\ &= 37 - 13(40 - 37) \\ &= 14 \cdot 37 - 13 \cdot 40 \end{aligned}$$

dvs $d \equiv 14 \pmod{40}$

altså $x = x' \equiv x^{37 \cdot 14} \equiv 12^{14} \pmod{55}$

$12^2 \equiv 34 \pmod{55}$
$12^4 \equiv 1 \pmod{55}$
$12^8 \equiv 1 \pmod{55}$

$12^{14} = 12^2 \cdot 12^4 \cdot 12^8 \equiv 34 \cdot 1 \cdot 1 = 34 \pmod{55}$

dvs $\underline{x \equiv 34 \pmod{55}}$.

EH.07.3

Her at $\frac{n}{2} = 28741$ og $\varphi(n) = (2-1)\cdot(p-1)(q-1)$

$= (p-1)(q-1)$

$= \varphi(\frac{n}{2})$.

$\varphi(n) = 28000 = 2^5 \cdot 5^3 \cdot 7$

p og q er nytten i 2.grads polynomet

$$X^2 + (\tfrac{n}{2} - \varphi(n) + 1)X + n$$

$$= X^2 - 742X + 28741$$

$$p,q = \frac{742 \pm \sqrt{742^2 - 4 \cdot 28741}}{2} = \frac{742 \pm 660}{2}$$

$$p = 41 \;,\; q = 701$$

EH.07.7

Dette svarer til et RSA-system med offentlig nøkkel $(n,e) = (299, 65)$. Vi må derfor finne dekrypteringseksponenten d, der løser $65 \cdot d \equiv 1 \pmod{264}$

$\varphi(n) = (13-1)(23-1)$.

Vi finner at $d \equiv 65 \pmod{264}$

dvs $x \equiv x^{65 \cdot 65} \equiv 210^{65} \equiv 123 \pmod{299}$

EH.07.8

Ved divisjons algoritmen kan vi skrive

$$j = k \cdot q + r$$

der $0 \le r \le k-1$

Altså vet

$$a^j = (a^k)^q \cdot a^r \equiv 1^q \cdot a^r$$
$$= a^r \pmod{n}$$

Anta at $a^j \equiv 1 \pmod{n}$

Dette betyr at

$$a^r \equiv 1 \pmod{n}$$

der $0 \le r < k$. Dette er umulig da k er den minste positive eksponenten slik at $a^k \equiv 1 \pmod{n}$.

Dvs vi må ha at $r = 0$ og får at $j = k \cdot q$ dvs $k \mid j$.

Anta k er minimal s.a. $a^k \equiv 1 \pmod{71}$

dvs dersom $a^{101} \equiv 1 \pmod{71}$ betyr at $k \mid 101$.

Siden 101 er primtall må $k = 1$ eller $k = 101$.

$k = 1$ gir at $a \equiv 1 \pmod{71}$. Siden 71 er primtall så gjelder Fermats lille, dvs

$$a^{70} \equiv 1 \pmod{71}. \quad \left(\text{for } p \nmid a \text{ dvs } a \not\equiv 0 \pmod{p}\right)$$

Dette betyr at $k \mid 70$, men $k = 101$ dersom $a^{101} \equiv 1 \pmod{71}$ skal ha løsning.

Dvs. $a^{101} \equiv 1 \pmod{71}$ har ingen ikke-triviell løsning.

EH.08.5

Vi finner først løsningen av

$$173 \cdot d \equiv 1 \pmod{288}$$

der $\varphi(323) = 288$. Vi finner at $d = 5$ er en løsning. Vi løser kongruensen

$$x^{173} \equiv 291 \pmod{323}$$

ved å beregne $291^5 \pmod{323}$:

$$291^2 \equiv 55 \pmod{323}$$
$$291^4 \equiv 55^2 \equiv 118 \pmod{323}$$

Dette gir at

$$291^5 = 291^4 \cdot 291 \equiv 118 \cdot 291 \pmod{323}$$
$$\equiv 100 \pmod{323}$$