$+$ $\times$

$-$ $\div$

1)
$$x \equiv 1 \mod 8$$
$$x \equiv 1 \mod 9$$
$$x \equiv 2 \mod 11$$
$$x \equiv 0 \mod 13$$

$$8 \cdot 9 \cdot 11 \cdot 13 = 10296$$

$$m_1 = \frac{10296}{8} = 1287 \rightarrow m_1^{-1} = 1287 \mod 8 = 7$$

$$m_2 = \frac{10296}{9} = 1144 \rightarrow m_2^{-1} = 1144 \mod 9 = 1$$

$$m_3 = \frac{10296}{11} = 936 \rightarrow m_3^{-1} = 936 \mod 11 = 1$$

$$m_4 = \frac{10296}{13} = 792 \rightarrow m_4^{-1} = 792 \mod 13 = 12$$

$$X = (1 \cdot 1287 \cdot 7) + (1 \cdot 1144 \cdot 1) + (2 \cdot 936 \cdot 1) + (0 \ldots) \mod 10296$$
$$= (9009 + 1144 + 1872) \mod 10296$$
$$= 12025 \mod 10296 = 9$$

$$\begin{array}{r} 8025 \\ 0296 \\ \hline 1729 \end{array}$$

2) RSA $\rightarrow$ $c = 14,\ n = 201,\ e = 23$

$n = 3 \cdot 67$

$\phi = (3-1) \cdot (67-1)$

$= 2 \cdot 66 = 132$

$d = e^{-1}$ in $\mathbb{Z}_{132}$

$132 = 5 \cdot 23 + 17$

$23 = 1 \cdot 17 + 6$

$17 = 2 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1 \rightarrow$ ggd

$5 = 1 \cdot 5 + 0$

$\Rightarrow 23 \cdot x + 132 y = 1$

$1 = 6 - 1 \cdot 5$

$= 3 \cdot 6 - 17$

$= 3 \cdot 23 - 4 \cdot 17$

$= 3 \cdot 23 - 4 \cdot 132 + 10 \cdot 23$

$= 23 \cdot 23 - 4 \cdot 132$

$x = 13 \qquad d = 23$

$m = 14^{23}$ mod mod 201

$23 = 11 \cdot 2 + 1$ 0

$11 = 5 \cdot 2 + 1$ 1

$5 = 2 \cdot 2 + 1$ 2

$2 = 1 \cdot 2 + 0$ 3

$1 = 0 \cdot 2 + 1$ 4

$$\begin{array}{r} 196 \\ 196 \\ \hline 1176 \\ 17640 \\ 19600 \\ \hline 1 \\ \hline 38416 \end{array}$$

$$\begin{array}{r|l} 38416 & 201 \\ 201 & 191 \\ \hline 1831 & \\ 1809 & \\ \hline 226 & \\ 201 & \\ 25 & \end{array}$$

$2^0 + 2^1 + 2^2 + 2^4 =$

$1 + 2 + 4 + 16$

$14 \cdot 14^2 \cdot 14^4\ 14^{16}$ mod 201

14 mod $201 = 14$

14^2 mod $201 = 196$

14^4 mod $201 = 25$

14^8 mod $201 = 22$

14^{16} mod $201 = 82$

$14 \cdot 196 \cdot 25 \cdot 82$ mod 201

$25 \cdot 82$ mod $201 = 2050$ mod 201

$= 40$

$14 \cdot 196 = 2744$ mod $201 = 131$

$40 \cdot 131$ mod $201 = 5240$ mod 201

$$\begin{array}{r|l} 5240 & 201 \\ 402 & 26 \\ \hline 1220 & \\ 1206 & \\ \hline 14 & \end{array}$$

$d = e^{-1}$ in $\mathbb{Z}_{..}$: $\gcd(e, n) = 1$

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

$n = p \cdot q$

$$c = 83, \quad n = 91 \quad e = 25$$

$$b = (7-1)(13-1)$$

$$= 6 \cdot 12 = 72$$

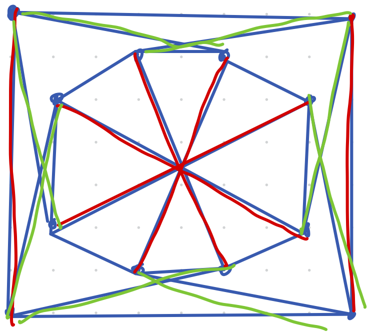
$$d = 25^{-1} \text{ in } \mathbb{Z}_{72}$$

$$72 = 2 \cdot 25 + 22$$
$$25 = 1 \cdot 22 + 3$$
$$22 = 7 \cdot 3 + 1 \rightarrow \gcd$$
$$3 = 3 \cdot 1 + 0$$

$$1 = 22 - 7 \cdot 3$$
$$= 22 - 7 \cdot (25 - 1 \cdot 22)$$
$$= 8 \cdot 22 - 7 \cdot 25$$
$$= 8 \cdot (72 - 2 \cdot 25) - 7 \cdot 25$$
$$= 8 \cdot 72 - 23 \cdot 25$$

$$d = -23 = 49$$

$$83^{49} \bmod 91$$



$W \sum \deg(v) \geq 27$

9 toppen dus gem $\frac{27}{9} = 3 \deg$

dus $\exists$ een top met y zodat ≥ 27

W

VW

W

VW

maximum $\frac{E(y)}{2} = 3$