

$$\begin{aligned} & \underline{0 \equiv 5 \equiv 10} \\ & \quad 1 \equiv 6 \\ & \quad 2 \equiv 7 \\ & \underline{3 \equiv 8} \\ & \quad 4 \equiv 9 \end{aligned} \quad \begin{array}{l} \nearrow \\ \searrow \end{array} \begin{array}{l} \text{Zyklus} \\ \text{früher} \\ \\ (\text{mod } 5) \end{array}$$

$$\begin{array}{l} \text{mod } 47 \quad \dots \quad -21 \equiv 26 \quad (47) \\ \quad \quad \quad \quad \quad \quad 90 \equiv 43 \quad (47) \end{array}$$

$$\begin{aligned} & m \mid a_1 - b_1, \quad m \mid a_2 - b_2 \\ & \Rightarrow m \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2) \end{aligned}$$

$$a_1 \equiv b_1 \rightarrow a_1 a_2 \equiv b_1 a_2 \equiv b_1 b_2$$

$\begin{matrix} \textcircled{1} \cdot a_2 & & b_1 \cdot \textcircled{1} \end{matrix}$

$$\begin{array}{l} a \equiv b \pmod{m} \\ k \equiv l \pmod{\phi(m)} \end{array} \xrightarrow{(a,m)=1} a^k \equiv b^l \pmod{m}$$

∇
0

$$2 \cdot 0 \equiv 2 \cdot 2 \pmod{4} \not\Rightarrow 0 \equiv 2 \pmod{4}$$

$$m \mid k \cdot a - k \cdot b = k \cdot (a - b) \rightarrow m \mid a - b$$

\uparrow

$$\dots \uparrow \\ (m, l) = 1$$

\equiv

$$a \equiv b \pmod{112} \Leftrightarrow \begin{matrix} a \equiv b & (7) \\ a \equiv b & (16) \end{matrix}$$

$$112 \mid a-b \Leftrightarrow \begin{matrix} 7 \mid a-b \\ 16 \mid a-b \end{matrix}$$

\equiv

$$112 \mid (835^5 + 6)^{18} - 1$$

$$\Leftrightarrow (835^5 + 6)^{18} \equiv 1 \pmod{112}$$

zjedn.

$$\Leftrightarrow (835^5 + 6)^{18} \equiv 1 \pmod{7}$$

$$(835^5 + 6)^{18} \equiv 1 \pmod{16}$$

$$835 \equiv 2 \pmod{7}$$

$$835^5 \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}$$

$$835^5 + 6 \equiv 4 + 6 \equiv 3 \pmod{7}$$

$$(835^5 + 6)^{18} \equiv 3^{18} \equiv ((3^2)^3)^3 \pmod{7}$$

$$\equiv \left(\frac{9}{8}\right)^3 \equiv \left(\frac{2}{1}\right)^3 \equiv 1 \pmod{7}$$

$$\Rightarrow 5^{20} \equiv ? \quad (26)$$

$$5^2 \equiv 25 \equiv -1 \quad (26)$$

$$5^{20} \equiv (5^2)^{10} \equiv (-1)^{10} \equiv 1 \quad (26)$$

$$\Rightarrow (a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \quad (2)$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \equiv a^3 + b^3 \quad (3)$$

$$\begin{array}{ccccccc} & & & & & & 1 \\ & & & & & & 1 & 1 \\ & & & & & & 1 & 2 & 1 \\ & & & & & & 1 & 3 & 3 & 1 \\ & & & & & & 1 & 4 & 6 & 4 & 1 \\ & & & & & & 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{k} a^{p-k} b^k + \dots + b^p$$

Cherchons: $p \mid \binom{p}{k}$ pro $k=1, \dots, p-1$

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{k \cdot (k-1) \cdot \dots \cdot 1}$$

$$39 \cdot x \equiv 1 \quad (47)$$

pour trouver

$$(39, 47) = 1$$

$$\begin{array}{cc|c} 1 & 0 & 47 \\ 0 & 1 & 39 \\ 1 & -1 & 8 \\ -4 & 5 & 7 \\ 5 & -6 & 1 \end{array}$$

$$5 \cdot 47 - 6 \cdot 39 = 1 \quad / \text{ mod } 47$$

$$\underbrace{5 \cdot 47}_{\equiv 0} - 6 \cdot 39 \equiv 1 \quad (47)$$

$$-6 \cdot 39 \equiv 1 \quad (47)$$

$$x \equiv -6 \equiv 41$$

$$47x \equiv 0$$

$$39x \equiv 1$$

$$8x \equiv -1$$

$$7x \equiv 5$$

$$x \equiv -6$$

$$(47) \leftarrow \text{plati' v2d}$$

$$(47)$$

$$\begin{array}{ccc} 0 & \xrightarrow{2x} & 0 \\ 1 & \searrow & 1 \\ 2 & \searrow & 2 \\ 3 & \searrow & 3 \\ 4 & \searrow & 4 \end{array}$$

$$(\text{mod } 5)$$

$$2x \equiv 2y \quad (5)$$

$$\Rightarrow x \equiv y$$

$$39x \equiv 41 \quad (47) \quad / \cdot 39^{-1} \equiv -6$$

$$\underbrace{(-6) \cdot 39} \cdot x \equiv (-6) \cdot 41 \quad (47)$$

1

$$x = (-6) \cdot 41 = \dots \quad (47)$$

Jihat: $47x = 0 \quad (47)$

$$39x = 41 \equiv -6$$

$$8x = 6$$

$$7x = -30 \equiv 17$$

$$x = -11$$

\Rightarrow

$$8x = 10 \quad (14)$$

\Rightarrow

$$14x = 0 \quad (14)$$

$$8x = 10 \quad (14)$$

$$6x = 4 \quad (14)$$

$$2x = 6 \quad (14) \iff x = 3 \quad (7)$$

$$0x = -14 \equiv 0 \quad x = 3 \quad (14)$$

mebu $x = 10 \quad (14)$