$\boxed{A}$

1. $3^5 \bmod 100 = 43$

2. $1+i$

3. $(x^2+1)^2 \cdot (x+2)$

4. $(1, \alpha+1)$

$\boxed{B}$

$3^4 \bmod 100 = 81$

$1+i$

$(x^2+2)^2 \cdot (x-2)$

$(\alpha+1, 1)$

① $3^{5^{666}} \bmod 100 = ?$

Vím: $3^{20} \bmod 100 = 1$

Čili mě zajímá $5^{666} \bmod 20$.

Vidím, že $5^{666} \equiv 0 \pmod 5$

$5^{666} \equiv 1^{666} \equiv 1 \pmod 4$

Takže (ČVZ pro $m_1 = 5$, $m_2 = 4$)

$5^{666} \equiv 5 \pmod{20}$

$\uparrow$

jediné řešení mezi $0, \dots, 19$

Čili odpověď je $3^5 \bmod 100 = \underline{\underline{43}}$

$3^{4^{2025}} \bmod 100 = ?$

Vím: $3^{20} \bmod 100 = 1$

Čili mě zajímá $4^{2025} \bmod 20$.

Vidím, že $4^{2025} \equiv 0 \pmod 4$

$4^{2025} \equiv (-1)^{2025} \equiv 4 \pmod 5$

Takže (ČVZ pro $m_1 = 5$, $m_2 = 4$)

$4^{2025} \equiv 4 \pmod{20}$

$\uparrow$

jediné řešení mezi $0, \dots, 19$

Čili odpověď je $3^4 \bmod 100 = \underline{\underline{81}}$

Pozor, u obou exponentů není splněn předpoklad Eulerovy věty

($NSD(4,20) \neq 1 \neq NSD(5,20)$).

② $NSD(7-i, 11+3i) = ?$

$$7-i = (1+i)\cdot(2-i)^2$$

$$11+3i = (1-i)\cdot(2+i)\cdot(3+2i)$$

To zjistím pomocí rozkladu normy:

$$\nu(7-i) = 50 = 2\cdot 5^2$$

$$\nu(11+3i) = 130 = 2\cdot 5\cdot 13$$

Měl bych vědět, že

- prvky normy 2 jsou všechny $\parallel 1+i$
- prvky normy 5 jsou všechny $\parallel 2\pm i$

Zbytek zjistím dělením.

Protože $1+i \parallel 1-i$, ale $2+i \nparallel 2-i$,

tak $NSD(7-i, 11+3i) = \underline{\underline{1+i}}$

$NSD(13-i, 7+9i) = ?$

$$13-i = (1-i)\cdot(2+i)\cdot(4+i)$$

$$7+9i = (1+i)\cdot(2-i)\cdot(3+2i)$$

To zjistím pomocí rozkladu normy:

$$\nu(13-i) = 170 = 2\cdot 5\cdot 17$$

$$\nu(7+9i) = 130 = 2\cdot 5\cdot 13$$

Měl bych vědět, že

- prvky normy 2 jsou všechny $\parallel 1+i$
- prvky normy 5 jsou všechny $\parallel 2\pm i$

Zbytek zjistím dělením.

Protože $1+i \parallel 1-i$, ale $2+i \nparallel 2-i$,

tak $NSD(13-i, 7+9i) = \underline{\underline{1+i}}$

Alternativní řešení: Euklidův algoritmus.

③ Rozlož $x^5+2x^4+2x^3+x^2+x+2$ v $\mathbb{Z}_3[x]$.

Zkusmo $(x=0,1,2)$ zjistíme, že 1 je kořen, vydělením členem $x+2$ dostaneme rozklad

$$(x+2)\cdot(x^4+2x^2+1).$$

Ten druhý člen je zjevně čtverec, takže máme rozklad

$$(x+2)\cdot(x^2+1)^2.$$

Uvedené polynomy už jsou ireducibilní:

- $x+2$ je stupně 1
- x^2+1 je stupně 2 a nemá kořen v $\mathbb{Z}_3$

Rozlož $x^5-2x^4+4x^3-8x^2+4x-8$ v $\mathbb{Q}[x]$.

Pomocí kritéria racionálního kořene zjistíme, že 2 je kořen (možnosti: $\pm1, \pm2, \pm4, \pm8$), vydělením členem $x-2$ dostaneme rozklad

$$(x-2)\cdot(x^4+4x^2+4)$$

Ten druhý člen je zjevně čtverec, takže máme rozklad

$$(x-2)\cdot(x^2+2)^2$$

Uvedené polynomy už jsou ireducibilní:

- $x-2$ je stupně 1
- x^2+2 je stupně 2 a nemá kořen v $\mathbb{Q}$

Pozor, pokud polynom nemá kořen, nemusí být ireducibilní. Tato implikace platí pouze pro stupeň ≤ 3.

4

$$\left(\begin{array}{cc|c} \alpha & 1 & 1 \\ \alpha+1 & \alpha+1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha+1 & \alpha+1 \\ 1 & 1 & \alpha \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & \alpha+1 & \alpha+1 \\ 0 & \alpha & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cc|c} 1 & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha+1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & \alpha+1 \end{array}\right)$$

$$\left(\begin{array}{cc|c} \alpha & \alpha & \alpha+1 \\ \alpha+1 & 1 & \alpha+1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & \alpha \\ 1 & \alpha & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & \alpha \\ 0 & \alpha+1 & \alpha+1 \end{array}\right)$$

$$\sim \left(\begin{array}{cc|c} 1 & 1 & \alpha \\ 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & \alpha+1 \\ 0 & 1 & 1 \end{array}\right)$$

Využíváme charakteristiky 2,
a vlastností $\alpha^2 = \alpha+1$, $(\alpha+1)^2 = \alpha$, $\alpha(\alpha+1) = 1$.