

Zad 8

INPUT CJA

1)

$$f_1 = 1 \quad f_2 = 1$$

$$\text{NWD}(f_1, f_2) = 1$$

2) ~~zertreibig~~, i.e. $\text{NWD}(f_n, f_{n+1}) = 1$

Polno-izg, i.e. $\text{NWD}(f_{n+1}, f_{n+2}) = 1$

$\text{NWD}(a, b) = \text{NWD}(a+b, b)$

$$\text{NWD}(f_{n+1}, f_{n+2}) = \text{NWD}(f_{n+1}, f_{n+1} + f_n) =$$

$$= \text{NWD}(f_{n+1}, \cancel{f_{n+1}} + f_n - \cancel{f_{n+1}}) = \text{NWD}(f_{n+1}, f_n) =$$

$$= 1.$$

Wieso $\forall n > 0 \quad \text{NWD}(f_n, f_{n+1}) = 1$

Zad 1

$$71^71 \equiv ? \pmod{100}$$

$$100 = 4 \perp 25$$

$$71 \equiv 3 \pmod{4}$$

$$71^2 \equiv 9 \equiv 1 \pmod{4}$$

$$71^{71} = (71^2)^{35} \cdot 71^1 \equiv 1^{35} \cdot 3 \equiv 3 \pmod{4}$$

$$71 \equiv 21 \pmod{25}$$

$$71^2 \equiv 441 \equiv 16 \pmod{25}$$

$$71^3 \equiv 21 \cdot 16 \equiv 336 \equiv 11 \pmod{25}$$

$$71^4 \equiv 11 \cdot 21 \equiv 231 \equiv 6 \pmod{25}$$

$$71^5 \equiv 6 \cdot 21 \equiv 126 \equiv 1 \pmod{25}$$

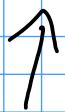
$$71^{71} \equiv (71^5)^{14} \cdot 71^1 \equiv 1^{14} \cdot 21 \equiv 21 \pmod{25}$$

wie c:

$$\begin{cases} 71^{71} \equiv 3 \pmod{4} \\ 71^{71} \equiv 21 \pmod{25} \end{cases}$$

$$\langle 1:100 \rangle$$

$$21, 76, 71, 96$$



$$71 \equiv 3 \pmod{4} : 71 \equiv 21 \pmod{25}$$

\equiv (Hinweis: 25 ist ein Vielfaches von 5)

$$\underline{\underline{71^{71} \equiv 71 \pmod{100}}}$$

Zad 3

$$2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P}$$

Powód przed kontrapozycję: $n \notin \mathbb{P} \Rightarrow 2^n - 1 \notin \mathbb{P}$

Durchweis:

$$n \notin P \Rightarrow n > 1 ; \exists_{r,s \geq 1} n = r \cdot s$$

$$2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1^s =$$

$$= [2^r - 1] \left[(2^r)^{s-1} + (2^r)^{s-2} + \dots + 2^r + 1 \right]$$

$\Rightarrow 2^n - 1$ ist ein Produkt aus $(2^r - 1) \geq 0$ (bzw. $r \geq 1$) und $(2^r + 1)$ (bzw. $r \geq 1$)

wie $2^n - 1 \notin P$

■

Zad 4

$$\alpha^n - 1 \in P \Rightarrow \alpha = 2$$

$$\alpha^n - 1 = (\alpha - 1)(\alpha^{n-1} + \alpha^{n-2} + \dots + \alpha + 1)$$

wie $\alpha - 1 \mid \alpha^n - 1$ alle $\alpha^n - 1 \in P$ wie

$$\alpha - 1 = 1 \Rightarrow \underline{\underline{\alpha = 2}}$$

Zad 5

$$2^n + 1 \in P \Rightarrow n = 2^k ; k \in \mathbb{N}$$

Zuweisung, da $n = m \cdot p$ ganze $p \in P \setminus \{2\}$

wie

$$2^n + 1 = (2^m)^p + 1 = \\ = (2^m + 1) (1 - 2^m + 2^{2m} - 2^{3m} + \dots + 2^{(p-1)m})$$

wiel 2^k + 1 jest wielokrotnością

wiel m niewiele być podzielne przez

lubby pierwne nieparzyste. Zatem

m musi być postaci 2^k

Zad 2

$$\begin{cases} (1) & x \equiv 2 \pmod{5} \\ (2) & x \equiv 3 \pmod{7} \\ (3) & x \equiv 4 \pmod{13} \end{cases}$$

$$2 (3) \quad x = 13k + 4 \quad ; \quad k \in \mathbb{Z}$$

$$2 (2) \quad 13k + 4 \equiv 3 \pmod{7}$$

$$13k \equiv (-1) \pmod{7}$$

$$13k \equiv 6 \pmod{7}$$

$$6k \equiv 6 \pmod{7} \quad | \cdot 2$$

$$12k \equiv 12 \equiv 5 \pmod{7}$$

$$5k \equiv 5 \pmod{7} \quad | \cdot 3$$

$$15k \equiv 15 \pmod{7}$$

$$\underbrace{k \equiv 1 \pmod{7}}$$

$$k = 7l + 1; l \in \mathbb{Z}$$

$$x = 13k + 4 = 13(7l + 1) + 4$$

$$x = 91l + 17$$

$$\text{z (1)} \quad 91l + 17 \equiv 2 \pmod{5}$$

$$91l \equiv (-15) \pmod{5}$$

$$l \equiv 0 \pmod{5}$$

$$l = 5t; t \in \mathbb{Z}$$

$$x = 91l + 17 = 91 \cdot 5t + 17 = \underline{\underline{455t + 17}}$$

अग्रस्थी रूप से प्रत्येक $\frac{455t + 17}{t \in \mathbb{Z}}$