Zad 8 INDUKCJA

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

$$NWD(f_1, f_2) = 1$$

2) załóżmy, że $NWD(f_n, f_{n+1}) = 1$

Pokażmy, że $NWD(f_{n+1}, f_{n+2}) = 1$

$\boxed{NWD(a,b) = NWD(a-b, b)}$

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

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

$$= 1.$$

więc $\forall n > 0 \ NWD(f_n, f_{n+1}) = 1$ $\blacksquare$

Zad 1

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

$100 =$; $4 \perp 25$

$$71 \equiv 3 \pmod 4$$

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

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

$71 \equiv 21 \pmod{25}$

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

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

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

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

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

więc:

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

$\langle 1; 100 \rangle$

21, 46, 71, 96

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

z Chińskiego tw. o resztach

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

Zad 3

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

Dowód przez kontrapozycję: $n \notin \mathbb{P} \Rightarrow 2^n - 1 \notin \mathbb{P}$

D-d:

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

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

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

$\Rightarrow$ $2^n - 1$ jest złożona (bo $2^r - 1 > 0$ oraz też) (bo $r,s > 1$)

więc $2^n - 1 \notin \mathbb{P}$

$\blacksquare$

Zad 4

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

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

więc $a - 1 \mid a^n - 1$ ale $a^n - 1 \in \mathbb{P}$ więc

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

Zad 5

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

załóżmy, że $n = m \cdot p$ gdzie $p \in \mathbb{P} \setminus \{2\}$

więc

$$2^n+1 = (2^m)^p + 1 =$$

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

więc 2^k+1 jest wtedy złożone

więc n nie może być podzielne przez liczby pierwsze nieparzyste. Zatem

n musi być postaci 2^k

Zad 2

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

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

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

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

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

$6k \equiv 6 \pmod{7} \; / \cdot 2$

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

$$5k \equiv 5 \pmod 7 \quad / \cdot 3$$

$$15k \equiv 15 \pmod 7$$

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

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

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

$$x = 91l + 17$$

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

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

$$l \equiv 0 \pmod 5$$

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

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

wszystkie rozw. są postaci $\underline{455t + 17}$

$t \in \mathbb{Z}$