L4 Z1

$$71^{71} = (70+1)^{71} = \underbrace{\binom{71}{0}70^{71} + \binom{71}{1}\cdot 70^{70} + \binom{71}{2}\cdot 70^{69} + \ldots}_{\text{Tu dwie ostatnie cyfry wynoszą 00}} + \binom{71}{70}\cdot 70^{1} + \binom{71}{71}\cdot 1$$

$\binom{71}{70}\cdot 70 = 4970$

$\binom{71}{71}\cdot 1 = 1$

Tylko dwa ~~zera~~ os

A więc dwie ostatnie cyfry 71^{71} to 71

L4 22

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

Z pierwszego równania

$$x = 5k + 2$$

Najmniejsze takie k spełniające pierwsze równanie to 3

Z dwóch pierwszych równań mamy więc

$$x = 17 \pmod{21}$$

$$x = 21j + 17$$

najmniejsze $j = 0$

Czyli ogólne rozwiązanie to

$$x = 17 + (5 \cdot 7 \cdot 13)l$$

najmniejszy taki $x = 17$

L4 Z3

2^n-1 jest liczbą pierwszą $\Rightarrow$ n jest liczbą pierwszą

Zał. że n nie jest liczbą pierwszą. Wtedy $\exists x,y>1 \quad n=x\cdot y$

$$2^n-1 = 2^{xy}-1 = (2^x)^y - 1^y = (2^x-1)(2^{x(y-1)} + 2^{x(y-2)} + \ldots + 2^x + 1)$$

Jako że $x>1$ to $(2^x-1)>1$ czyli 2^n-1 ma dzielnik większy od 1 i mniejszy od niego czyli 2^n-1 nie jest liczbą pierwszą

Przez prawo kontrapozycji

$$(\neg q \Rightarrow \neg p) \Leftrightarrow (p \Rightarrow q)$$

L4 z5

2^n+1 jest liczbą pierwszą $\Rightarrow$ $n=2^m$

Zał. że n nie jest potęgą dwójki czyli $n=s\cdot 2^m$ // s jest liczbą nieparzystą

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

Więc 2^n+1 nie jest liczbą pierwszą

czyli n nie może być podzielne przez nieparzystą liczbę, czyli musi być postaci $n=2^m$

L4 Z8

Dowód przez indukcję $NWD(F_n, F_{n+1}) = 1$

1° Podstawa indukcji

$n = 2$

$NWD(F_2, F_3) = NWD(2,3) = 1$ ✓

2° krok ind.

Zał. ind. $NWD(F_n, F_{n+1}) = 1$

Pokazać że $NWD(F_{n+1}, F_{n+2}) = 1$

$F_{n+2} = F_{n+1} + F_n$

$F_n = F_{n+2} - F_{n+1}$

Alg. Euklidesa ↓

$NWD(F_{n+1}, F_{n+2}) = NWD(F_{n+1}, F_{n+2} - F_{n+1}) = NWD(F_{n+1}, F_n) =$

$= NWD(F_n, F_{n+1}) = 1$