$71 \equiv_{100} (6\ldots$

1. Szukamy dwóch ostatnich cyfr 71^{71}

$$71^{71} = (70+1)^{71} = \binom{71}{0}70^{71} + \ldots \binom{71}{71-2}70^{2} + \binom{71}{70}70 + \binom{71}{71}70^{0}.$$

$\%100 = 0$, czyli całego iloczynu też

$$71^{71} \equiv_{100} 71 \cdot 70 + 1 \equiv_{100} (70+1)70 + 1 \equiv_{100} 70^{2} + 70 + 1 \equiv_{100} 70^{2} + 71 \equiv_{100} 71$$

4900, $\%100 = 0$.

Zatem dwie ostatnie cyfry 71^{71} to 71.

2

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

(2) $1 \le x \le 5 \cdot 7 \Rightarrow 1 \le x \le 35$

Wypiszmy ciąg liczb spełniających równanie (1)

$2, 7, 12, 17, 22, 27, 32$

Widać, że z powyższych liczb równanie (2) spełnia tylko 17.

Rozwiązujemy teraz taki układ:

$$\begin{cases} x \equiv 17 \mod 35 \\ x \equiv 4 \mod 13 \end{cases}$$

Od razu widać, że $17 \mod 35 \equiv 17 = 4 \mod 13$.

Czyli rozwiązanie najmniejsze to 17 a ogólne:

$$x = 17 + (5 \cdot 7 \cdot 13)k, \quad k \in \mathbb{Z}$$

(2) $p \Rightarrow q$, to $\neg q \Rightarrow \neg p$

Pokażmy, że $2^n - 1$ pierwsza $\Rightarrow n$ pierwsza.

Załóżmy, że n jest liczbą złożoną.

Wtedy $n = ab$ dla ~~ab~~ jakichś $a, b \geq 2$

$$2^n - 1 = (2^a)^b - 1 \overset{p = 2^a}{=\!=} p^b - 1 = (p-1)(p^{b-1} + p^{b-2} + \ldots + p^1 + p^0) =$$

$$(2^a - 1)(2^{a(b-1)} + \ldots + 2^{b-1} + 1).$$

Czyli $2^a - 1$ dzieli $2^n - 1$, więc $2^n - 1$ jest liczbą złożoną.

Zatem przez kontrapozycję pokazano, że jeśli $2^n - 1$ pierwsze, to n też.

Czyli, przez kontrapozycji, pokaza[illegible], że [illegible] jest potęgą 2.

(4) $a^n - 1$ pierwsze $\Rightarrow a = 2$

$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$. Jeśli $a = 0$, to $a^n - 1 = -1$ ×.
Jeśli $a = 1$, to $a^n - 1 = 0$. × Jeśli $a = 2$, to $a^n - 1 = (2-1)(a^{n-1} + \ldots + 1) = a^{n-1} + \ldots + 1$. ✓ Jeśli $a > 2$, to $a - 1 > 1$, czyli $a^n - 1$ ma jakiś pierwszy dzielnik, czyli nie jest pierwsze. × Zatem $a = 2$.

8 Dowód prez indukcję.

Jeśli $W(n)$ zachodzi, to $W(n+1)$ też. $n \in \mathbb{N}$

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

$F_n = k$

$F_{n+1} = k+m$

$F_{n+2} = 2k+m$

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

Baza indukcji:

$n=0 \quad W(0) = NWD(F_0, F_1) = NWD(0,1) = 1.$

Krok indukcyjny:

Zał. że $W(n)$ zachodzi, czyli $NWD(F_n, F_{n+1})$.

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