Zad. 1

Chcemy policzyć $71^{71} \bmod 100$.

$100 = 25 \cdot 4$, $4 \perp 25$

- $71^{71} \equiv_4 3^{71} \equiv_4 3 \cdot 3^{70} \equiv_4 3 \cdot 9^{35} \equiv_4 3 \cdot 1^{35} \equiv_4 3$
- $71^{71} \equiv_{25} (-4)^{71} \equiv_{25} (-4)^{2 \cdot 5 \cdot 7 + 1} \equiv_{25} (-4) \cdot (-4)^{2 \cdot 5 \cdot 7} \equiv_{25} (-4)\left(\left((-4)^5\right)^2\right)^7$

$4^5 = 1024 \Rightarrow 4^5 \equiv_{25} -1$

$-(4^5) = (-4)^5 \equiv_{25} 1$

$71^{71} \equiv_{25} (-4)\left((1)^2\right)^7 \equiv_{25} -4 \equiv_{25} 21$

$$\begin{cases} x \bmod 4 = 3 \\ x \bmod 25 = 21 \end{cases}$$

Z chińskiego twierdzenia o resztach wiemy, że ten układ ma jedno rozwiązanie w przedziale $[1, 4 \cdot 25]$

Zatem dla drugiej kongruencji mamy 4 możliwości:

$21, 46, 71, 96$

$21 \bmod 4 = 1$, $46 \bmod 4 = 2$, $71 \bmod 4 = 3$

Czyli $71^{71} \bmod 100 = 71$ ■

Zad. 2

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

$x = 5t + 2$ Szukamy najmniejszego t, dla którego spełnione jest drugie równanie.

$x \equiv 17 \bmod (5 \cdot 7)$ $t = 3$

$x = 35u + 17$ Szukamy najmniejszego u, dla którego spełnione jest trzecie równanie.

$x \equiv 17 \bmod (5 \cdot 7 \cdot 13)$ $u = 0$

Najmniejsze rozwiązanie to $x = 17$, a rozwiązanie ogólne to $x = 17 + (5 \cdot 7 \cdot 13)k$

Zad. 3

Jeśli $2^n - 1$ jest liczbą pierwszą, to n też jest liczbą pierwszą.
(dla $n \geq 2$)

Dowód przez kontrapozycję:
pokażemy, że

Jeśli n nie jest liczbą pierwszą, to $2^n - 1$ też nie jest liczbą pierwszą.

Załóżmy, że n nie jest liczbą pierwszą

Zatem $\exists_{\substack{x,y \in \mathbb{Z} \\ x,y>1}} \; n = x \cdot y$

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

korzystamy z tego wzoru

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

Skoro $x > 1$ to $2^x - 1 > 1$ i skoro $y > 1$ to $2^x - 1 < 2^n - 1$,

a zatem $2^x - 1$ jest dzielnikiem 2^{n-1} i jest różny od 1 i $2^n - 1$,

więc $2^n - 1$ nie jest liczbą pierwszą. ■

Zad. 4

Zał. że $a^n - 1$ jest liczbą pierwszą (czyli $a \in \mathbb{N} \wedge a > 0$) $\boxed{n > 1}$

$$a^n - 1 = (a-1)\underbrace{(a^{n-1} + a^{n-2} + \ldots + a^1 + 1)}_{W(a)}$$

Zatem $a - 1$ jest dzielnikiem liczby $a^n - 1$.

Skoro $a^n - 1$ jest pierwsza to mamy dwie możliwości:

(1) $a - 1 = a^n - 1$

Wtedy jednak $W(a)$ musiałby być różny 1, a jest większy od 1
(bo wszystkie jego składniki są nieujemne)

Mamy zatem sprzeczność i odrzucamy ten przypadek.

(2) $a - 1 = 1$
$\Updownarrow$
$a = 2$

Zatem a musi być równe 2. ■

Zad. 5

Weźmy 2 kolejne wyrazy ciągu Fibonacciego:

a_{n-1} i a_n

Chcemy pokazać, że $NWD(a_n, a_{n-1}) = 1$

Korzystamy z algorytmu Euklidesa:

$NWD(a_n, a_{n-1}) = NWD(a_{n-2}+a_{n-1}, a_{n-1}) =$

$a_{n-2} < a_{n-1}$ więc $(a_{n-2}+a_{n-1}) \bmod a_{n-1} = a_{n-2}$

$= NWD(a_{n-1}, a_{n-2}) = NWD(a_{n-2}+a_{n-3}, a_{n-2}) =$

$= NWD(a_{n-2}, a_{n-3}) = \ldots = NWD(a_1, a_0) = NWD(1, 0) = 1$ ■

Tutaj zauważamy, że w każdym kolejnym kroku będziemy liczyć NWD dwóch kolejnych wyrazów ciągu Fibonacciego, zbliżając się do początku ciągu.

Zad. 5

Jeśli $2^n + 1$ - liczba pierwsza to n - potęga dwójki

Załóżmy, że 2^{n+1} jest liczbą pierwszą.

Weźmy takie p, że p jest nieparzyste i $p|n$

Wtedy $\exists_{k \in \mathbb{N}}\ n = p \cdot k$

$a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \ldots - a^1 + 1)$ - działa dla n nieparzystych

p - nieparzyste, więc możemy skorzystać z powyższego wzoru

$2^n + 1 = 2^{kp} + 1 = (2^k)^p + 1 = (2^k + 1)(2^{k(p-1)} - 2^{k(p-2)} + \ldots - 2^k + 1)$

Widzimy że w obydwu nawiasach mamy liczby > 1, co oznaczałoby, $2^n + 1$ nie jest liczbą pierwszą.

Jest to sprzeczne z założeniem, zatem p nie może liczbą parzystą.

Skoro n nie da się przedstawić jako iloczyn liczby nieparzystej i dodatniej liczby naturalnej, to znaczy, że n nie ma w rozkładzie na czynniki pierwsze żadnej liczby nieparzystej, a zatem n jest potęgą 2. _