Zadanie 1)

$71^{71} = 71^1 \cdot 71^2 \cdot 71^4 \cdot 71^{64}$

$71^1 \bmod 100 = 71$

$71^2 \bmod 100 = 41$

$71^4 \bmod 100 = (71^2 \cdot 71^2) \bmod 100 = 81$

$71^8 \bmod 100 = (71^4 \cdot 71^4) \bmod 100 = 61$

$71^{16} \bmod 100 = (71^8 \cdot 71^8) \bmod 100 = 21$

$71^{32} \bmod 100 = (71^{16} \cdot 71^{16}) \bmod 100 = 41$

$71^{64} \bmod 100 = (71^{32} \cdot 71^{32}) \bmod 100 = 81$

$71^{71} \bmod 100 = 71^1 \cdot 71^2 \cdot 71^4 \cdot 71^{64} \bmod 100$

$= (71 \cdot 41 \bmod 100) \cdot 71^4 \cdot 71^{64} \bmod 100$

$= (11 \cdot 81 \bmod 100) \cdot 71^{64} \bmod 100$

$= (91 \cdot 81) \bmod 100$

$= 71$

Zadanie 2)

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

Z pierwszego równania x jest postaci $5a+2$

z dwóch pierwszych równań $5a + 2 \equiv 3 \bmod 7$

najmniejszym a spełniającym to równanie jest $a = 3$

Zatem $x \equiv 17 \pmod{35}$

dokładając trzecie równanie $17 + 35b \equiv 4 \pmod{13}$

$b = 0 \quad 17 \equiv 4 \pmod{13}$

Zatem $x = 17$

$$\begin{cases} 17 \bmod 5 = 2 \\ 17 \bmod 7 = 3 \\ 17 \bmod 13 = 4 \end{cases}$$

Zadanie 3) Wykaż, że jeśli 2^n-1 jest liczbą pierwszą, to n jest liczbą pierwszą

Załóżmy nie wprost, że 2^n-1 jest liczbą pierwszą, ale n nie jest liczbą pierwszą. Wtedy $n = a \cdot b$ dla $a, b \in \mathbb{N}_{>1}$

Skorzystam ze wzoru $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$

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

podstawiając do wzoru $x^n - 1$
$x = 2^a$, $x^n = (2^a)^b$, $x^{n-1} = (2^a)^{(b-1)}$, ...

dochodzimy do sprzeczności, ponieważ $2^a - 1$ jest dzielnikiem $2^n - 1$, $2^a - 1 \neq 1$, $2^a - 1 \neq 2^n - 1$, więc $2^n - 1$ nie jest l. pierwszą

Aby $2^n - 1$ było liczbą pierwszą, n musi być liczbą pierwszą

Zadanie 4) Wykaż, że jeśli $a^n - 1$ jest liczbą pierwszą, to $a = 2$

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

aby $a^n - 1$ było liczbą pierwszą, to liczba $a-1$ musi być jedynką (inaczej $a^n - 1$ nie byłoby l. pierwszą), zatem $a = 2$

Zadanie 5) Wykaż, że jeśli 2^n+1 jest liczbą pierwszą, to n jest potęgą 2

Załóżmy nie wprost, że 2^n+1 jest liczbą pierwszą, ale n nie jest potęgą 2

Wtedy n można zapisać jako $a \cdot b$, gdzie a jest liczbą nieparzystą > 1

$$2^{n}+1 = (2^b)^a + 1 = (2^b)^a + (-1)^a = (2^b-(-1))(2^{a-1} + 2^{a-2}(-1) + 2^{a-3}(-1)^2 + \ldots + (-1)^{a-1})$$

↑ ponieważ a jest nieparzyste

(ten wzór wziął się z $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + xy^{n-2} + y^{n-1})$)

Otrzymaliśmy $2^n + 1 = (2^b + 1)(2^{a-1} - 2^{a-2} + 2^{a-3} - 2^{a-4} + \dots + (-1)^{a-1})$

$2^n + 1$ jest podzielne przez $2^b + 1$, zatem dosliśmy do sprzeczności, ponieważ w założeniu $2^n + 1$ jest 1. pierwsza. Zatem jeśli $2^n + 1$ jest 1. pierwsza, to n musi być potęgą dwójki

Zadanie 7) a, b ∈ ℤ założenie $a^3 | b^2$

Jeśli a^3 dzieli b^2, to istnieje taka liczba k, że $a^3 \cdot k = b^2$

Niech $l = a^2 k$, wtedy $a \cdot l = b^2 \Rightarrow a | b^2$