Matematyka dyskretna L, Lista 4 - Tomasz Woszczyński

Zadanie 1
Chcemy obliczyć dwie ostatnie cyfry liczby 71^{71}, więc rozwiązujemy równanie:

$$71^{71} \bmod 100 \equiv 71^{64+4+2+1} \bmod 100$$

Policzmy najpierw kolejne potęgi korzystając z zależności

$$(a \cdot b) \bmod \mathrm{n} = ((a \bmod \mathrm{n}) \cdot (b \bmod \mathrm{n})) \bmod \mathrm{n}$$

$$\begin{aligned}
71^1 &\equiv 71 \bmod 100 \\
71^2 &\equiv 41 \bmod 100 \\
71^4 &\equiv 71^2 \bmod 100 \cdot 71^2 \bmod 100 && \equiv 41 \cdot 41 \bmod 100 \equiv 1681 \bmod 100 && \equiv 81 \bmod 100 \\
71^8 &\equiv 71^4 \bmod 100 \cdot 71^4 \bmod 100 && \equiv 81 \cdot 81 \bmod 100 \equiv 6561 \bmod 100 && \equiv 61 \bmod 100 \\
71^{16} &\equiv 71^8 \bmod 100 \cdot 71^8 \bmod 100 && \equiv 61 \cdot 61 \bmod 100 \equiv 3721 \bmod 100 && \equiv 21 \bmod 100 \\
71^{32} &\equiv 71^{16} \bmod 100 \cdot 71^{16} \bmod 100 && \equiv 21 \cdot 21 \bmod 100 \equiv 441 \bmod 100 && \equiv 41 \bmod 100 \\
71^{64} &\equiv 71^{32} \bmod 100 \cdot 71^{32} \bmod 100 && \equiv 41 \cdot 41 \bmod 100 \equiv 1681 \bmod 100 && \equiv 81 \bmod 100
\end{aligned}$$

Wiemy, że $71 = 64+4+2+1$, dzięki czemu możemy obliczyć wynik całego działania:

$$\begin{aligned}
71^{71} \bmod 100 &\equiv 71^{64+4+2+1} \bmod 100 \\
&\equiv 71^{64} \cdot 71^4 \cdot 71^2 \cdot 71^1 \bmod 100 \\
&\equiv (81 \cdot 81 \bmod 100) \cdot 71^2 \cdot 71^1 \bmod 100 \\
&\equiv (61 \cdot 41 \bmod 100) \cdot 71^1 \bmod 100 \\
&\equiv 1 \cdot 71 \bmod 100 \\
&\equiv 71 \bmod 100
\end{aligned}$$

Zadanie 2
Należy rozwiązać układ kongurencji:

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

Ogólne rozwiązanie pierwszego równania to $2 + 5i$, szukamy więc najmniejszego i takiego, że $x = 2 + 5i$ spełnia drugie równanie:

$$2(0), 7(1), 12(2), 17(3), \text{ bo } 17 \bmod 7 \equiv 3$$

więc najmniejsze i to 3. Z dwóch pierwszych równań uzyskujemy kongurencję $x \equiv 17 \bmod 35$. Ogólnym rozwiązaniem dwóch pierwszych równań jest $17 + (5 \cdot 7)j$, szukamy więc najmniejszego j takiego, że $x = 17 + 35j$ spełnia trzecie równanie:

$$17(0), \text{ bo } 17 \bmod 13 \equiv 4$$

Najmniejszym rozwiązaniem jest więc 17, a ogólnym $17 + (5 \cdot 7 \cdot 13)k$ dla $k \in \mathbb{N}$.

Zadanie 3
Należy wykazać, że jeśli $2^n - 1$ jest liczbą pierwszą, to n jest liczbą pierwszą.

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

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \cdot \left(2^{a\cdot(b-1)} + 2^{a\cdot(b-2)} + \cdots + 2^a + 1\right)$$

zatem $2 \leqslant 2^a - 1 < 2^n - 1$, czyli $(2^a - 1)$ jest dzielnikiem $2^n - 1$, a więc liczba $2^n - 1$ nie jest liczbą pierwszą. Dochodzimy do sprzeczności, więc n musi być liczbą pierwszą, aby $2^n - 1$ było liczbą pierwszą, co kończy dowód.

Zadanie 4
Należy wykazać, że jeśli $a^n - 1$ jest liczbą pierwszą, to $a = 2$.

W podobny sposób jak wyżej rozpiszmy $a^n - 1$:

$$a^n - 1 = \underbrace{(a-1) \cdot (a^{n-1} + a^{n-2} + \cdots + a + 1)}_{\substack{\text{wyrazy } a \text{ i } a^{n-1} \text{ dają } a^n\text{, a } -1 \text{ i } 1 \text{ dają } -1\text{,} \\ \text{pozostałe wyrazy się wzajemnie wykluczają}}}$$

Aby $a^n - 1$ było liczbą pierwszą, to musi być $(a-1) = 1$, a jeśli $(a-1) = 1 \Rightarrow a = 2$.

Zadanie 8
Mamy pokazać, że dwie kolejne liczby Fibonacciego są względnie pierwsze i powinniśmy skorzystać z algorytmu Euklidesa.

Wiemy, że kolejnymi wyrazami ciągu Fibonacciego są $F_1 = 1, F_2 = 1, F_3 = 2, \ldots$, a kolejne wyrazy są zdefiniowane wzorem $F_n = F_{n-1} + F_{n-2}$. Możemy więc indukcyjnie po n (dla F_n) udowodnić twierdzenie z zadania.

1. Podstawa indukcji: $n = 1$, wtedy $\gcd(F_1, F_2) = \gcd(1, 1) = 1$. ✓
2. Krok indukcyjny: załóżmy, że dla n zachodzi $\gcd(F_n, F_{n+1}) = 1$, pokażemy, że dla $n + 1$ zachodzi $\gcd(F_{n+1}, F_{n+2}) = 1$:

$$\begin{aligned}
\gcd(F_{n+1}, F_{n+2}) &= \gcd(F_{n+1}, F_n + F_{n+1}) && \text{(definicja liczb Fibonacciego)} \\
&= \gcd(F_{n+1}, F_n) && \text{(bo } \gcd(a+b, b) = \gcd(a, b)\text{)} \\
&= \gcd(F_n, F_{n+1}) && \text{(przemienność wyrazów w gcd)} \\
&= 1 && \text{(założenie indukcyjne)}
\end{aligned}$$

Udowodniliśmy więc, że dwie kolejne liczby Fibonacciego są względnie pierwsze.