Odpowiedzi na pytania:

1. Własności operacji XOR

Dla liczb całkowitych x, y, z:

- Przemienność: $x \oplus y = y \oplus x$
- Łączność: $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- Tożsamość: $x \oplus 0 = x$
- Samowyzerowanie: $x \oplus x = 0$
- Odwracalność: jeśli $x \oplus y = z$, to $x = y \oplus z$ i $y = x \oplus z$

XOR działa jak „dodawanie modulo 2” na poziomie bitów.

2. Liczby względnie pierwsze

- Liczby a i b są względnie pierwsze, jeśli gcd(a, b) = 1.
- Jeśli a jest liczbą pierwszą i b < a, to gcd(a, b) = 1, ponieważ liczba pierwsza ma tylko dzielniki 1 i siebie samą.
- Jeśli b > a, to gcd(a, b) może być różne od 1, np. jeśli b jest wielokrotnością a, wtedy gcd(a, b) = a.

3. Małe twierdzenie Fermata i odwrotność modulo

- Dla liczby całkowitej $a \not\equiv 0 \bmod p$ i liczby pierwszej p:
  $a^{(p-1)} \equiv 1 \bmod p$
- Stąd odwrotność multiplikatywna $a^{-1} \bmod p$ wynika z:
  $a * a^{(p-2)} \equiv 1 \bmod p \Rightarrow a^{-1} \equiv a^{(p-2)} \bmod p$
- Wykorzystuje się to w praktyce np. w kryptografii (RSA, pola skończone).