Odpowiedzi na pytania:

Reszty kwadratowe i symbol Legendre'a

Dla liczby pierwszej p i liczby całkowitej a, mówimy, że a jest resztą kwadratową modulo p, jeśli istnieje takie x, że $x^2 \equiv a \pmod p$. W przeciwnym razie a jest nieresztą kwadratową modulo p.

Symbol Legendre'a definiuje się jako:

(a/p) = 1 jeśli a jest resztą kwadratową mod p
(a/p) = -1 jeśli a jest nieresztą kwadratową mod p
(a/p) = 0 jeśli p | a

Własności:

- Multiplikatywność: (ab/p) = (a/p)(b/p)
- Prawo wzajemności kwadratowej: (p/q)(q/p) = (-1)^((p-1)(q-1)/4)
- Dodatkowe tożsamości: (-1/p) = (-1)^((p-1)/2), (2/p) = (-1)^((p^2-1)/8)

Chińskie Twierdzenie o Resztach (CRT)

Niech $n_1, n_2, \ldots, n_k$ będą parami względnie pierwsze. Dla dowolnych $a_1, a_2, \ldots, a_k$ istnieje dokładnie jedno x modulo $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ takie, że:
$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
...
$x \equiv a_k \pmod{n_k}$
Konstrukcja rozwiązania:
$x = \Sigma (a_i \cdot N_i \cdot y_i) \bmod N$,
gdzie $N_i = N/n_i$, a y_i jest odwrotnością modularną $N_i^{-1} \bmod n_i$.

Modularne pierwiastki kwadratowe i algorytm Tonelliego–Shanksa

Dla liczby pierwszej p i a takiego, że (a/p) = 1, chcemy znaleźć x takie, że $x^2 \equiv a \pmod p$.
Przypadek prosty ($p \equiv 3 \bmod 4$): x = a^((p+1)/4) mod p
Ogólny przypadek (algorytm Tonelliego–Shanksa):
1. Rozkład: $p - 1 = Q \cdot 2^S$, Q nieparzyste.

2. Znajdź niereszte kwadratową z mod p (czyli (z/p) = -1).
3. Ustal: M = S, c = z^Q mod p, t = a^Q mod p, R = a^((Q+1)/2) mod p.
4. Dopóki t ≠ 1:
   - znajdź najmniejsze i, dla którego t^(2^i) ≡ 1 mod p,
   - b = c^(2^(M−i−1)) mod p,
   - zaktualizuj: M = i, c = b^2 mod p, t = t·b^2 mod p, R = R·b mod p.
5. Wynik: x = R oraz p−R to dwa pierwiastki.