8 - Algorytm Tonellego-Shanksa

Thursday, 20 June 2024 15:31

Pierwiastek dyskretny

Mamy cykliczną grupę G i $a \in G$.

Znajdź x: $x^2 = a$

$\mathbb{Z}_p$

Istnieje rozwiązanie iff $a^{\frac{p-1}{2}} = 1$.

- Jeśli $|G| = 2m+1$ to $x := a^{m+1}$ działa
- Jeśli $|G| = 2m$ to dokładnie połowa elementów to reszty kwadratowe.
- Każdy kwadrat ma dwa rozwiązania.

Wylosujmy z nie będące resztą kwadratową.

$Q := \frac{n}{2}$, $t = n$

while $2 | a$

  $Q = \frac{Q}{2}$

  $t = \frac{t}{2}$

  if $a^Q \cdot z^t \neq 1$

    $t = t + \frac{n}{2}$

return $a^{\frac{Q+1}{2}} \cdot z^{\frac{t}{2}}$

$a^Q \cdot z^t = 1$