Quadratic Non-Residue

Pulaksh Garg
(170010015)

Supervisor: Dr. Arpita Korwar

Problem Statement

> Given a prime number p, find a number n such that n is not a square number modulo p. Studying possible deterministic algorithm for the same.

Test to check Quadratic Residue

Euler's Criterion:

Here a is an element in F_p

$$a^{(p-1)/2} \equiv (a/p) \ (mod \ \mathrm{p})$$

Distribution of Quadratic Residues and Non-Residues

- Number(QR) = Number(NR)
- Randomly Occurring

Parallel Problem Statement

> Given a prime number p and a number n less than p, such that n is a quadratic residue, then find a number x such that the square of x is equivalent to n modulo p.

Algorithms for Root Finding
By Modifying Polynomial Factoring

Polynomial Factoring in $F_p[x]$

Polynomial Factoring in $F_p[x]$

Here a is the square root of n

Berlekamp’s Algorithm

Input: x^2-n, q

Output: x-a or x+a

Probability of success is 1/2

Berlekamp's Algorithm

1. c=1,d=0.
2. Take $r = gcd(f, x^{(q-1)/2} - 1)$.
3. Check if r != 1and r != f(a)
    a. if True, return c*r((x-d)/c)
    b. else, f=c*f((x-d)/c) randomly generate c,d in F_q then update f=f(cx+d) and repeat from step 2

Cantor Zassenhaus Algorithm

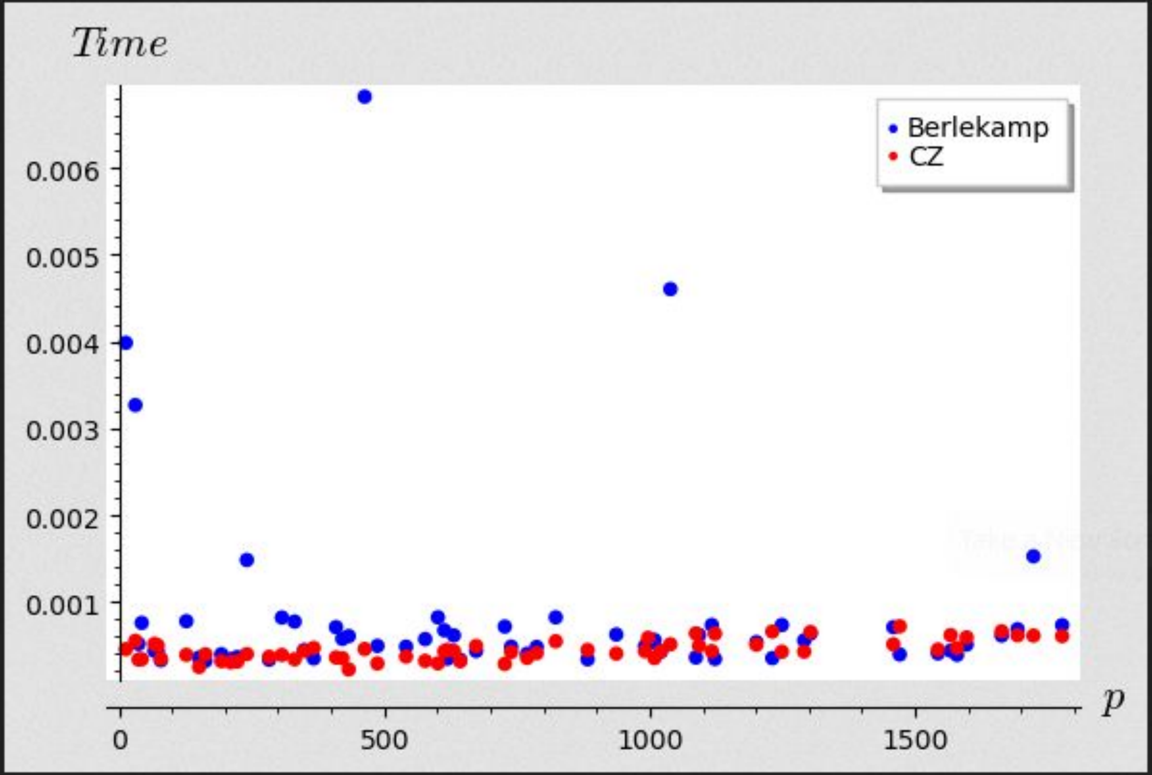
Input: x^2-n, q

Output: x-a or x+a

Cantor Zassenhaus Algorithm

1. Randomly generate $a \in F_q[x]$ but not in F_q.
2. Take $g1 = gcd(a, f)$
3. Check if $g1$!= 1and $g1$!= f
   a. if True, return g1
   b. else, compute $b = a^{(q^\wedge d - 1)/2}$ (rem f)
4. Take $g2 = gcd(b - 1, f)$
5. Check if $g2$!= 1 and $g2$!= f
   a. if True, return g2
   b. else, return "failure"

Results


Time
0.006
0.005
0.004
0.003
0.002
0.001
Berlekamp
CZ
0
500
1000
1500
p

Algorithm to generate Quadratic Non-Residue

> Given a prime number p, find a number n such that n is not a square number modulo p. Studying possible deterministic algorithm for the same.

1. Generate a random number in F_p, say r
2. Check if r is a non-residue:
   a. If True, return r
   b. Else, return “failed”

Major Future Works

- Quadratic Reciprocity in $F_p[x]$
- Improving the probability using distribution information

Main References

- Gallian, Joseph A. Contemporary Abstract Algebra. Ninth edition, Cengage Learning, 2017.
- Gathen, Joachim von zur, and Jürgen Gerhard. Modern Computer Algebra. Third edition, Cambridge University Press, 2013.
- Lidl, Rudolf, and Harald Niederreiter. Introduction to Finite Fields and Their Applications. Cambridge University Press, 2012.
- Silverman, Joseph H. A Friendly Introduction to Number Theory. 4th ed, Pearson, 2013.
- Wright, Steve. “Are Quadratic Residues Randomly Distributed?” Quadratic Residues and Non-Residues: Selected Topics, edited by Steve Wright, Springer International Publishing, 2016, pp. 273–83. Springer Link, doi:10.1007/978-3-319-45955-4_10.

Special Mentions

I would like to thank Dr. Franz lemmermeyer for providing his lectures notes.

Thank You

END