Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 116 (2017) 198–205

Procedia Computer Science

www.elsevier.com/locate/procedia

2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI 2017, 13-14 October 2017, Bali, Indonesia

An Algorithm to Find Square Root of Quadratic Residues over Finite Fields using Primitive Elements

Faisal[a], Wikaria Gazali[a]

[a]*Mathematics Department, School of Computer Science, Bina Nusantara University, Jl. K.H. Syahdan No. 9 Palmerah, Jakarta Barat 11480, Indonesia*

Abstract

Quadratic residue is an important concept in number theory because it has both theoretical and practical application in mathematics and other areas such as computer science and communication. We also have a same concept of quadratic residue in general finite fields. Finding a square root of a quadratic residue in finite fields is an essential problem in computational algebra. In this paper we present an algorithm of computing square root of quadratic residue in finite fields using a primitive element.

Keywords: quadratic residue, square root; finite field; polynomial, primitive element.

1. Introduction

Finding square roots of quadratic residue in finite fields is an important problems in computational algebra. It is a generalization of modular square roots problem in number theory. Calculation of roots in finite fields plays an essential role in cryptosystems based on elliptic curves. Another application of computing square roots can be found in Rabin[1] cryptosystem, point compression in Miller[2]. Let p be a prime number and F_p be a finite field. If a is quadratic residue in F_p^*, the square root of a is the solutions of the quadratic congruence $x^2 \equiv a(\bmod p)$. In the case $p \equiv 3(\bmod 4)$, we have an explicit solution $x \equiv \pm a^{\frac{p+1}{4}}(\bmod p)$. For the case $p \equiv 1(\bmod 4)$, no general solution is known. However, there are explicit solutions for computing a square root in F_p when $p \equiv 5(\bmod 8)$ in Cohen and Frey[3]. The remaining case $p \equiv 1(\bmod 8)$ is non trivial. There are many probabilistic algorithms to compute a square root in this case. Two classical, non-deterministic algorithm for this case are the Tonelli[4]-Shanks and the Cipolla[5]-Lehmer algorithms.

[*] Corresponding author. Tel.: +62-21-534-5830 ext 2230
E-mail address: faisal@binus.edu

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.
10.1016/j.procs.2017.10.033

Many authors have studied the square root problem in finite fields. For the case F_q with q is an odd prime power. In P. S. L. M. Bareto and Scott[6], they presented an algorithm that can compute square roots for $q \equiv 3(\bmod 4)$ or $q \equiv 5(\bmod 8)$.

The rest of this paper organized as follows. In Section 2 we give the original theory of quadratics residue in number theory and the basic theory of finite fields. In Section 3 we present the general quadratic residue in an finite fields. Then, in Section 4 we explain our algorithms using primitive elements.

2. Preliminaries

2.1. Quadratic Residues

The concept of quadratic residue appears in order to determine whether the general quadratic congruence

$$ax^2 + bx + c \equiv 0(\bmod m), \text{ with } a \not\equiv 0(\bmod m)$$

has a solution or not. Suppose that p is an odd prime and a is an integer with $(a, p) = 1$. Recall that a is a quadratic residue of p if $(a, p) = 1$ and the congruence $x^2 \equiv a \pmod p$ has a solution. If the congruence $x^2 \equiv a (\bmod p)$ has no solution, we say that a is a quadratic nonresidue of p.

Proposition 1. *Let p be an odd prime. The congruence*

$$ax^2 + bx + c \equiv 0(\,mod\; p), \; with\; a \not\equiv 0(\,mod\; p)$$

has a solution if and only if

$$x^2 \equiv b^2 - 4ac(\,mod\; p)$$

The above proposition tells us that the solution of the general quadratic congruence is depends on whether $b^2 - 4ac$ is quadratic residue or not. Complete characterization of quadratic residue has been found and can be studied in many textbook of number theory. For an odd prime p, we have known the number of quadratic residues and the quadratic nonresidues of p.

Theorem 1. *For an odd prime p, the number of quadratic residues modulo p in* $\{1, 2, \ldots, p-1\}$ *is* $(p-1)/2$. *Hence, the number of quadratic nonresidues in* $\{1, 2, \ldots, p-1\}$ *is* $(p-1)/2$.

Proof. See Rosen[7]. □

The French mathematician *Adrien-Marie Legendre* introduce the special notation associated with quadratic residues.

Definition 1. Let p be an odd prime and a be an integer not divisible by p. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$