6-1-2003

Quadratic Nonresidues and Applications

Nelson A. Carella
Pace University

SCHOOL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

TECHNICAL REPORT

Number 190, June 2003

Quadratic Nonresidues and Applications

Nelson A. Carella

PACE UNIVERSITY

Nelson A. Carella, a mathematician who hails from the City University of New York, adjuncts in the Information Systems Department at Pace University in Manhattan.

Quadratic Nonresidues and Applications

Nelson A. Carella

Abstract: This note will show that there is a deterministic polynomial time algorithm for computing quadratic nonresidues z of absolute values $|z| \leq O(\log(p)^c)$ for all primes p, and $c > 0$ a fixed constant. Further, the same method is used to determine the least quadratic nonresidues $n_p \leq O(\log(p)^c)$ of any prime $p \neq 8n - 1$.

1 Introduction

A quadratic residue a modulo a prime p is simply a square modulo p. Every square integer is a square modulo p, but not every square modulo p is a square integer. The quadratic symbol

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } x^2 \equiv a \bmod p \text{ has no solution,} \\ 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution,} \end{cases} \tag{1}$$

is the standard method of identifying squares and nonsquare elements. A nonzero element $a < p$ is a quadratic residues if the quadratic symbol has the value 1. Otherwise it has the value -1 and the element is called quadratic nonresidue. The problem of determining the complexity of constructing quadratic nonresidues is an open problem of interest in algorithmic number theory because it is a step in several algorithms, for instance, square roots computing, quadratic form representations of integers etc.

A quadratic nonresidue modulo p is constructible in nondeterministic polynomial time $O(\log(p)^3)$ bit operations or better: Simply choose $a \in \mathbf{F}_p$ at random and compute the $a^{(p-1)/2} \bmod p$. Since there are $(p-1)/2$ nonzero quadratic nonresidues in $\mathbf{F}_p$, the expected number of trials is 2. In contrast, there is no deterministic polynomial time algorithm to construct a quadratic nonresidue modulo a prime p, see [Crandall et al., p. 94], [Menezes et al., p. 74], or

similar references. In this note it will be shown that the construction of quadratic nonresidues is a deterministic polynomial time operation for any prime.

The existence of a deterministic polynomial time algorithm does not necessarily improve the current computational methods of generating quadratic nonresidues nor supersede the random algorithms, as the one described above, since all these algorithms are very efficient and essentially the same.

2 Preliminaries

This section provides some background information on a few concepts and results used in later sections, and establishes the notations used. The discussions are of limited scopes, and the readers should consult the literature for finer analysis.

Densities of Some Primes

The order $ord_p(a) = \min\{ k : a^k \equiv 1 \bmod p \}$ of an integer a modulo p is the maximal number of distinct powers

$$1, a, a^2, a^3, \ldots$$

modulo a prime p. The order is an equivalent class invariant defined for all pairs (a, p) of integers, and it is a divisor of $p - 1 = \varphi(p)$.

The distribution of the orders $ord_p(a)$ of a fixed integer a as the prime p varies over the primes has been investigated for quite some time. The parity of the simplest case $ord_p(2)$ is essentially solved using elementary methods. For example, $ord_p(2)$ is even for any prime $p = 8k \pm 3$, and for infinitely many primes $p = 8k + 1$.

Let $N(x, b, s, r) = \#\{ p \le x : s^r \parallel ord_p(b) \}$, the symbol $p^v \parallel N$ denotes the maximal prime power p^v divisor of N.

Lemma 1. (Wiertelak 1977) If b is not a square of an integer, and $2^{r+2} \le \text{loglog}(x) / \text{logloglog}(x)$, then the density of the primes p for which the order is even is given by

$$N(x,b,2,r) = \alpha(b,2,r)\frac{x}{\log x} + O\left(\frac{1}{2^{r/2}}\frac{x}{\log(x)}\sqrt{\frac{\log\log\log(x)}{\log\log(x)}}\right), \qquad (2)$$

where the implied constant depends on b, and the density $\alpha(b, 2, r) > 0$ for $b \ne 2a^2$ is

$$\alpha(b,2,r) = \begin{cases} \frac{1}{3} & \text{if } r = 0, \\ \frac{1}{3}\frac{1}{2^{r-1}} & \text{if } r \geq 1. \end{cases} \tag{3}$$

and for $b = 2a^2$ it is

$$\alpha(b,2,r) = \begin{cases} \frac{7}{24} & \text{if } r = 0,1 \\ \frac{1}{3} & \text{if } r = 2, \\ \frac{1}{3}\frac{1}{2^{r-1}} & \text{if } r > 2. \end{cases} \tag{4}$$

A similar result in [Odoni] gives the distribution as

$$N(x,b,2,1) = \beta(b,2,1)li(x) + O\left(li(x)\exp\left(-c_1 \frac{\log\log(x)}{\log\log\log(x)} \right) \right) \tag{5}$$

where $li(x) = \int_2^x \frac{dt}{\ln t} = \frac{x}{\ln x} + \frac{x}{\ln^2 x} + O(\frac{x}{\ln^3 x})$ is the logarithmic integral, and the implied constants are absolute.

The constants $\alpha(b,2,1)$ and $\beta(b,2,1)$, both positive and less than 1, are computed using different methods, but both densities match on any given parameters. These densities depend only on the arithmetic structures of the integers a in the field extensions $\mathbb{Q}(1^{1/\nu}, a^{1/\nu})$ of the rational field $\mathbb{Q}$. The error terms in (2) and (5) depend on the behavior of the zeros of the zeta functions of the field extensions.

These results give specific information on the distribution of the orders $ord_p(a)$ of a fixed integer a as the prime p varies over the primes.

***Corollary* 2.** If a is a fixed squarefree integer, then the set of primes is partitioned as follows:

$$\{ \text{ set of primes } p \} = \{ p : ord_p(a) = 2^0 n \} \cup \{ p : ord_p(a) = 2^1 n \} \cup \{ p : ord_p(a) = 2^k n \},$$

where n is odd, and $k \geq 2$.

3 The Time Complexity Of Quadratic Nonresidues

The traditional approach to the determination of a quadratic nonresidue attempts to find the least positive quadratic nonresidue n_p modulo p. In the 1800's it was determined that $n_p < p^{1/2} + 1$, [Gauss , Art. 129]. The modern methods are by means of exponential sums and/or L-functions analysis. For example, estimating the least integer $M > 1$ for which exponential sum

$$\sum_{x=1}^{M}\left(\frac{x}{p}\right) < M . \tag{6}$$

Around the 1950's several authors used exponential sums analysis to reduce the estimate $n_p < p^{1/2} + 1$ to $n_p < p^{1/4\sqrt{e}+\varepsilon}$, $e = 2.71...$, and $\varepsilon > 0$, see [Burgess]. The well known Vinogradov's conjecture claims that $n_p = O(p^{\varepsilon})$, $\varepsilon > 0$. A combinatorial method is used in [Hudson et al.] to derive $n_p < p^{2/5} + 12p^{1/5} + 33$ for $p \not\equiv 1 \bmod 8$. Further, on the basis of the extended Riemann hypothesis for L-functions it has been established that $n_p = O(\log(p)^2)$, see [Ankeny]. This last conditional result implies that a quadratic nonresidue is constructible in $O(\log(p)^5)$ bit operations. In the other direction, it has been unconditionally proven that there are infinitely many primes for which $n_p \geq c_0 \log(p)\log\log\log(p)$, c_0 an absolute constant, see [Graham et al].

Using the Quadratic Reciprocity Law

$$(1)\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \tag{7}$$

$$(2)\ \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

it is straightforward to obtain the following quadratic nonresidues:

(1) If $p = 8n + 3$, then $q = -1$ and 2 are quadratic nonresidues.
(2) If $p = 8n + 5$, then $q = 2$ is a quadratic nonresidue.
(3) If $p = 8n + 7$, then $q = -1$ is a quadratic nonresidue.

These are quadratic nonresidues z of least or the least absolute values $|z| \leq O(\log(p)^c)$, fixed $c > 0$. The QRL readily produces quadratic nonresidues of any equivalence class of primes $p \neq 2^k n + 1$, n odd. However, this is not practical: repeatedly using (7) to obtain quadratic nonresidues for $k = 4, 5, \ldots$ requires infinitely many equivalence classes to cover all the primes.

Note that a single quadratic nonresidue z is sufficient to generate the entire set of quadratic nonresidues. This is accomplished by multiplication by squares: $s \to sz$, where s runs over the set of quadratic residues $Q = \{ x^2 \bmod p : 0 < x < p/2 \}$. Likewise, long sequences of consecutive pairs and equally spaced pairs are generated by

$$z_s = \frac{(sz \pm 1)^2}{4sz},\ z_s \mp 1, \quad \text{and} \quad z_s = \frac{(sz \pm v)^2}{4sz},\ z_s \mp v. \tag{8}$$

***Theorem* 3.** For every sufficiently large prime p there exists a quadratic nonresidue z of absolute value $|z| \le O(\log(p)^c)$, where $c > 0$ is a fixed constant.

Proof: Fix a sufficiently large prime $p = 4n + 1$, and a constant $c > 0$, (for $p = 4n + 3$ take $z = -1$ or 2). The density of the primes q for which the orders $ord_q(p)$ is odd is 1/3, this follows from either [Odoni] or [Wiertelak], see Lemma 1. Consequently, the density of primes q for which the orders $ord_q(p)$ is even is 2/3. This implies that the set of primes q such that the orders $ord_q(p)$ is even contains primes of the form $q = 4n + 3$. Now since $p = 4n + 1$ is a quadratic nonresidue modulo $q = 4n + 3$ whenever $ord_q(p)$ is even, it follows that $\left(\frac{q}{p}\right) \equiv -1 \bmod p$. Further, to show that there are some primes $q \le O(\log(p)^c)$, observe that for a sufficiently large fixed prime p, and $x = O(\log(p)^c)$, the number of primes $q \le x$ for which orders $ord_q(p)$ is even is asymptotic to

$$\sum_{\substack{q \le x \\ ord_q p = 2m}} 1 = \frac{2}{3} li(x) + O\left(li(x) \exp\left(-c_1 \frac{\log\log(x)}{\log\log\log(x)} \right) \right). \tag{9}$$

For sufficiently large x, the error term in (9) is sufficiently small to provide a nontrivial count > 0. ■

***Corollary* 4.** If $p \neq 8n + 7$ is a sufficiently large prime and $c > 0$ is a fixed constant, then the followings hold.

(1) The least quadratic nonresidue $n_p \le O(\log(p)^c)$.

(2) There exists some integer $M \le O(\log(p)^c)$ such that $\sum_{x=1}^{M} \left(\frac{x}{p}\right) < M$.

Numerical Data

The algorithm used to generate quadratic nonresidue is given below, the choice of parameters $O(\log(p)^c) = 2(\log(p)^2)$ conform with the Riemann hypothesis.

Algorithm I
Input p.
Output z = quadratic nonresidue.
(1) If $p \neq 8n + 1$, then return $z = -1$ or 2 and terminate.
(2) While $x \not\equiv -1 \bmod p$, and $q = 2k + 1 \leq 2(\log(p)^2)$, do $x \equiv p^{(q-1)/2} \bmod q$.
(3) Return $z = q$.

The data of the numerical experiment for the primes $p = 4n + 1 \leq 200$, and $x = 2(\log(p)^2)$ is tabulated below. The data suggests that the main result holds for all primes, not just sufficiently large primes. The entries in column K are the actual count, and the entries in column $N = x / 3\log(x)$ are the estimated numbers of primes $q = 4n + 3 \leq x \leq 2(\log(p)^2$ with $\text{ord}_q(p) = \text{even}$.

p	K	N	p	K	N
5	1	1.05	97	3	3.74
13	2	1.70	101	3	3.78
17	3	1.93	109	3	3.88
29	3	2.42	113	4	3.92
37	2	2.67	137	5	4.16
41	4	2.77	149	4	4.27
53	4	3.05	157	3	4.33
61	4	3.20	173	4	4.46
73	3	3.40	181	5	4.52
89	5	3.63	193	4	4.60

4 Application to Square Roots Computations

The square roots of elements modulo a prime p can be determined efficiently using nondeterministic polynomial time algorithms. These algorithms are fast and easy to implement, see [Bach et al.], [Menezes et al.,], or [Peralta] etc for descriptions. On the other hand, the deterministic polynomial time algorithm has a higher running time complexity and it is complicated. This algorithm runs in $O(|x|^{1/2+\varepsilon}\log(p)^9)$ bit operations, any $\varepsilon > 0$. Moreover, there is a dependence on the absolute value of the argument x, for $p \not\equiv 1 \bmod 16$, it is not dependent on $| x |$, see [Schoof].

The main result is utilized to complete a random square root algorithm into deterministic polynomial time algorithms. This algorithm is derived from one of the random square root algorithms that require the determination of a quadratic nonresidue, only one type is given.

***Theorem* 4.** Algorithm II computes a square root modulo p in deterministic polynomial time for any prime p.

Algorithm II
Input p, and a square a mod p.
Output $\pm\sqrt{a}$.

(1) Use algorithm I to compute a quadratic nonresidue.

(2) Compute the series $\omega_0 = a^n$, $\omega_{i+1} = \omega_i z^{2^{k-m_i} n}$, up to $\omega_i = 1$,

where 2^{m_i} is the order of ω_i modulo p, which is a divisor of $2^{m_{i-1}-1} < 2^k$.

(3) Compute the series $x_0 = a^{(n+1)/2}$, $x_{i+1} = x_i z^{2^{k-m_i-1} n}$,

all calculations are modulo p.

(4) Return $x_i = \pm\sqrt{a}$.

Mechanism of the Algorithm
Algorithm II is a deterministic version of the Tonelli's algorithm, circa 1890. The basic probabilistic algorithm has undergone several stages of developments by several authors. A root of the equation $x^2 - a \equiv 0 \bmod p$, $a^{(p-1)/2} \equiv 1 \bmod p$, is determined by a series of successive approximations. The number of iterations in the algorithm is mostly a function of the 2-adic valuation $v_2(p-1) = k$.

To uncover its mechanism, write $p - 1 = 2^k n$, n odd, let $x_0 = a^{(n+1)/2}$, and let $\omega = z^n$, where z is a quadratic nonresidue modulo p. Then

$$\left(a^{-1} x_0^2\right)^{2^{k-1}} = 1, \tag{10}$$

and $a^{-1} x_0^2 = \omega^t$ is a primitive 2^{k-1}th root of unity, $0 \le t < 2^{k-1}$. Thus the integer $x_0 \equiv a^{(n+1)/2} \bmod p$ is the square root of a or it is nearly the square root of a. In the later case the square root of a is $\sqrt{a} = \pm x_0 \omega^{-t/2}$. The correction factor ω^t is in the 2-Sylow subgroup $S_{2^k} = \{ z^n, z^{2n}, z^{3n}, ..., z^{2^k n} \}$ of the multiplicative group of $\mathbf{F}_p$. The determination of the integer ω^t can be accomplished using about two different techniques.

(1) A direct search in the set $S_{2^k} = \{ z^n, z^{2n}, z^{3n}, ..., z^{2^k n} \}$, this is practical for small k.

(2) Using a successive approximations algorithm, this is practical for all k.

The later technique determines the integer ω^t by repeatedly taking powers of 2 of the expression

$$a^{-1}x_0^2 = \omega^{t_0+t_1 2+t_2 2^2+\cdots+t_{k-2}2^{k-2}}. \tag{11}$$

This process recursively computes the binary digits of the integer $t = t_{k-2}2^{k-2} + t_{k-3}2^{k-3} + \cdots + t_2 2^2 + t_1 2 + t_0$. A variation of this technique, which is given here, appears in [Kumanduri et al., p. 223]. This technique exploits the fact that the 2-Sylow group has a chain decomposition into cyclic subgroups

$$1 \subset S_2 \subset S_{2^2} \subset S_{2^3} \subset \cdots \subset S_{2^k} \tag{12}$$

and the correction factor ω^t is in one of them.

To verify the correctness of algorithm II, observe that the sequence of integers

$$\omega_0 = a^n,\ \omega_1 = \omega_0 z^{n2^{k-m_0}},\ \omega_2 = \omega_1 z^{n2^{k-m_1}},\ ...,\ \omega_{i+1} = \omega_i z^{n2^{k-m_i}} = 1 \tag{13}$$

decrease to 1. This is due to the fact that the sequence of orders of the ω_i is a decreasing sequence of integers:

$$ord_p\omega_0 = 2^{m_0},\ m_0 < k,\ ord_p\omega_1 = 2^{m_1},\ m_1 < m_0,\ ...,\ ord_p\omega_{i+1} = 1. \tag{14}$$

Accordingly, there is a sequence of successive approximations

$$(0)\ a\omega_0 = a^{n+1} = \left(a^{(n+1)/2}\right)^2 = x_0^2 \tag{15}$$

$$(1)\ a\omega_1 = a\omega_0 z^{n2^{k-m_0}} = x_0^2\left(z^{n2^{k-m_0-1}}\right)^2$$

$$(2)\ a\omega_2 = a\omega_1 z^{n2^{k-m_1}} = x_0^2\left(z^{n(2^{k-m_0-1}+2^{k-m_1-1})}\right)^2$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$(i{+}1)\ a\omega_{i+1} = a\omega_i z^{n2^{k-m_i}} = x_0^2\left(z^{n(2^{k-m_0-1}+2^{k-m_1-1}+\cdots+2^{k-m_i-1})}\right)^2 = \left(a^{(n+1)/2} z^{n(2^{k-m_0-1}+2^{k-m_1-1}+\cdots+2^{k-m_i-1})}\right)^2.$$

Therefore

$$\sqrt{a} = \pm a^{(n+1)/2}\omega^{-t/2} = \pm a^{(n+1)/2} z^{n(2^{k-m_0-1}+2^{k-m_1-1}+\cdots+2^{k-m_i-1})}. \qquad (16)$$

A single quadratic nonresidue is sufficient to compute square roots modulo a fixed prime p. Moreover, for some parameters k, n the algorithm can be simplified. For example, if $k = 1, 2$, and n is an arbitrary odd integer. The simplifications are as follows.

For $k = 1$, the primes are necessarily of the form $p \equiv 3 \bmod 4$, and the square root formula (11) or (15) reduces to

$$(1)\ \sqrt{a} \equiv \pm a^{(p+1)/4} \bmod p \quad \text{if } a^{(p-1)/2} \equiv 1 \bmod p. \qquad (17)$$

According to [Turner], 2/3 of all random choices of p and a are handled with this formula.

For $k = 2$, the primes are necessarily of the form $p \equiv 5 \bmod 8$, and the square root formula (11) or (15) reduces to

$$(2)\ \sqrt{a} \equiv \frac{\pm 1}{2}\left(a^{(p+3)/8}(a^{(p-1)/4}+1) + 2^{(p-1)/4}a^{(p+3)/8}(a^{(p-1)/4}-1)\right) \bmod p. \qquad (18)$$

These two formulae are well known. Formulae of this type are called polynomial representations of square roots, a few new ones are given in [Agou et al.].

REFERENCES:

[1] SJ Agou, M Deleglise, JL Nicolas, *Short Polynomial Representations for Square Roots Modulo p*, Designs, Codes, Cryptography, 28, 33-44, 2003.

[2] NC Ankeny, *The least quadratic nonresidue.* Ann. of Math. 55, (1952). 65—72.

[3] E Bach, K Huber, *Note on taking square roots modulo N*, IEEE Trans. On Infor. Theory Vol. 45, No.2, 1999, pp.807-809.

[4] E Bach, A *Note on square roots in Finite Fields*, IEEE Trans. On Infor. Theory Vol. 36, No.1, 1990, pp.55-64.

[5] A Burgess, *The Distribution Of Quadratic Residues And Quadratic Nonresidues,* Mathematicka, Vol. 8, 1957, pp. 106-112.

[6]R Crandall, C Pomerance, **Prime Numbers. A Computational Perspective**. *Springer-Verlag, New York,* 2001.

[7] CF Gauss, Disquisitiones Arithmeticae, Springer-Verlag, NY 1986.

[8] SW Grahm, CJ Ringrove, *Lower bounds for least quadratic nonresidues*, Progress in Math. Vol. 85, 1990.

[9] RH Hudson, HR Williams, *On The Least Quadratic Nonresidue Of A Prime*, J. Reine Ang. Math., Vol. 318, 1980, pp. 106-109.

[10] R Kumanduri, Cristina Romero, **Number Theory with Computer Applications**, Prentice Hall 1998.

[11] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone et al., **Handbook of Cryptography**, CRC Press, Boca Raton,1997.

[12] RWK Odoni, *A conjecture of Krishnamurthy on decimal periods and allied problems*, J. Number Theory 13 (1981), 303-319.

[13] RC Peralta, *A simple and fast probabilistic algorithm for computing square roots modulo a prime*, IEEE Trans. On Infor. Theory Vol. 32, No.6, 1986, pp.846-847.

[14] R Schoof, *Elliptic Curve Over Finite Fields And The Computation Of Square Roots Mod p*, Math. Computation Vol. 44, No. 170, 1985, pp. 483-494.

[15] SM Turner, *Square roots mod p*, Amer. Math. Soc., Vol. 101, No. 5, 1999, pp. 443-449.

[16] K Wiertelak, *On the density of some sets of primes* I, II, Acta Arith. 34 (1977/78), 183-196, 197-210.

School of Computer Science and Information Systems
Pace University
Technical Report Series

EDITORIAL BOARD

The School of Computer Science and Information Systems, through the Technical Report Series, provides members of the community an opportunity to disseminate the results of their research by publishing monographs, working papers, and tutorials. *Technical Reports* is a place where scholarly striving is respected.

All preprints and recent reprints are requested and accepted. New manuscripts are read by two members of the editorial board; the editor decides upon publication. Authors, please note that production is Xerographic from the pages you have submitted. Statements of policy and mission may be found in issues #29 (April 1990) and #34 (September 1990).

Please direct submissions as well as requests for single copies to:

Allen Stix
School of CS & IS - Suite 412 Graduate Center
Pace University
1 Martine Avenue
White Plains, NY 10606-1932