On the distribution of quadratic residues and nonresidues modulo a prime number

René Peralta *

Department of Electrical Engineering and Computer Science

University of Wisconsin - Milwaukee

P.O. Box 784

Milwaukee, WI. 53201

*Supported by National Science Foundation grant No. CCR-8909657

Proposed running head : "quadratic residues mod P".

corresponding author:

René Peralta
Computer Science Department
University of Wisconsin - Milwaukee
P.O. Box 784
Milwaukee, WI. 53201
peralta@cvax.cs.uwm.edu

Abstract

Let P be a prime number and $a_1, ..., a_t$ be distinct integers modulo P. Let x be chosen at random with uniform distribution in Z_P and let $y_i = x + a_i$. We prove that the joint distribution of the quadratic characters of the y_i's deviates from the distribution of independent fair coins by no more than $\frac{t(3+\sqrt{P})}{P}$. That is, the probability of $(y_1, ..., y_t)$ matching any particular quadratic character sequence of length t is in the range $(1/2)^t \pm \frac{t(3+\sqrt{P})}{P}$. We establish the implications of this bound on the number of occurrences of arbitrary patterns of quadratic residues and nonresidues modulo P. We then explore the randomness complexity of finding these patterns in polynomial time. We give (exponentially low) upper bounds for the probability of failure achievable in polynomial time using, as a source of randomness, no more that one random number modulo P.

1 Introduction

There is an extensive literature on the distribution of quadratic residues and nonresidues modulo a prime number. Much of it is dedicated to the question of how small is the smallest quadratic nonresidue of a prime P congruent to ± 1 modulo 8. Gauss published the first non-trivial result on this problem: he showed that if P is congruent to 1 modulo 8 then the least quadratic nonresidue is less than $2\sqrt{P}+1$ (art. 129 in [8]). The best upper bound currently known is $O(P^{\alpha})$ for any fixed $\alpha > \frac{1}{4\sqrt{e}}$ and is due to Burgess [5].

Not much is known about the number of occurrences of arbitrary patterns of quadratic residues and nonresidues among the integers $1, 2, ..., P-1$ modulo P. Denote by RN the number of occurrences of a quadratic residue followed by a nonresidue modulo P. We can similarly denote the number of occurrences of any pattern of quadratic residues and nonresidues modulo P. Exact formulas are known for RR, RN, NR, NN [1] (as expected, these are all approximately $\frac{P}{4}$). Upper bounds of the form $\frac{P}{2^3} + O(\sqrt{P})$ were obtained by Davenport [6] for RRR and NNN. In a later work Davenport obtained upper bounds of the form $\frac{P}{2^t} + P^{c_t}$ for all patterns of length t ($4 \leq t \leq 9$) [7]. For each of these bounds $c_t \geq \frac{2}{3}$ (the actual values are not of interest here since they will be improved in this work). Even less seems to be known regarding lower bounds for these quantities. Denote by R_t and N_t the number of occurrences of t consecutive quadratic residues and nonresidues respectively. Brauer, in 1928, showed that for any t and large enough P, both R_t and N_t are greater than 0 (see [4]). More recently, Hudson showed that $RRNR > 0$ and $RNRR > 0$ for large enough P [9].

In this paper, some combinatorial implications of Weil's bound on character sums are explored. Among these is the following result :

> Map the integers $0, 1, 2, ..., P-1$ to a circular arrangement of R's and N's according to their quadratic character modulo P (0 follows $P-1$ and is considered a residue). Then the number of occurrences of an arbitrary pattern of length t of quadratic residues and nonresidues is in the range

$\frac{P}{2^t} \pm t(3+\sqrt{P})$.

We next turn to the question of the randomness complexity of finding an arbitrary pattern of quadratic residues and nonresidues. We give (exponentially low) upper bounds for the probability of failure achievable in polynomial time using, as a source of randomness, no more that one random number modulo P.

2 Notation and a result from algebraic geometry

Following terminology in [3], we call the sequence $x+1, x+2, ..., x+t$ the "increment sequence" of length t and seed x. Throughout this paper,

- Θ will denote a set of integers.
- f_Θ will denote the polynomial $\prod_{i\in\Theta}(x+i)$.
- P will denote an odd prime number.
- X_P will denote the quadratic character modulo the prime P, i.e. $\mathrm{X}_P(x) = x^{(P-1)/2}$ modulo P, considered as an integer in $\{-1, 0, +1\}$.

We will make use of the inequality

$$|\sum_{x\in Z_P} \mathrm{X}_P(f_\Theta(x))| < \|\Theta\|\sqrt{P}.$$

We will refer to this inequality simply as the "Weil bound", since it follows from a more general theorem due to Weil (see theorem 2C, page 43, in [11]). Most of the results in this paper will follow from the Weil bound and the combinatorial lemmas of the following section. For notational simplicity the expression $\log_2 P$ denotes the integer part of $\log_2 P$ when it is clear that we are referring to an integer value.

3 Epsilon Independence of random variables

Let $S = \{A_1, ..., A_k\}$ be a set of random variables which can take values 0 or 1. If T is a non-empty subset of S then XOR_T denotes the probability that an odd number of A_i's in T is 1. If the A_i's are outcomes of a fair coin, then they are independent random variables if and only if $XOR_T = (1/2)$ for all non-empty subsets T of S. We are interested in deviations from this condition by a factor of ϵ. We say that S is a set of ϵ-independent random variables if XOR_T is within ϵ of $(1/2)$ for all non-empty subsets T of S. We will show that if S is a set of ϵ-independent random variables then the joint distribution of the variables in S deviates from the joint distribution of independent fair coins by no more than 2ϵ. In particular, the probability that all A_i in S are 1 is within 2ϵ of $(1/2)^{\|S\|}$.

For simplicity of notation we identify the symbol A_i with the event $A_i = 1$. Thus, $prob(A_i)$ denotes the probability that $A_i = 1$. Let

$$G_T = prob(\bigwedge_{i \in T} A_i).$$

Lemma 1 $XOR_S = \sum_{\phi \neq T \subseteq S} \ (-2)^{\|T\|-1} G_T$.

proof : Let α be an atomic event and let $U = \{i \mid \alpha \in A_i\}$. The number of times the event α is counted in the expression $\sum_{\phi \neq T \subseteq S} \ (-2)^{\|T\|-1} G_T$ is $\sum_{i=1}^{\|U\|} (-2)^{i-1} \begin{pmatrix} \|U\| \\ i \end{pmatrix}$. This is equal to $(1/2)(1 - (-1)^{\|U\|})$, which is 0 if $\|U\|$ is even and 1 if $\|U\|$ is odd. Thus the atomic events counted are precisely those which appear in an odd number of A_i's .□

Corollary 1 *For all $T \subseteq S$ we have*

$$G_T = (-1/2)^{\|T\|-1} \left[XOR_T - \sum_{\phi \neq U \subset T} (-2)^{\|U\|-1} G_U \right]$$

where the inclusion $U \subset T$ is proper.

Lemma 1 and corollary 1 imply the following lemma:

Lemma 2 $G_S = (1/2)^{\|S\|} \left[-2 \sum_{\phi \neq T \subseteq S} (-1)^{\|T\|} \ XOR_T \right]$

proof : By induction on the cardinality of S. The base case $\|S\| = 1$ is easily verifiable. Assume the lemma is true for all proper subsets of S. By corollary 1 we have

$$G_S = (-1/2)^{\|S\|-1}\left[XOR_S - \sum_{\phi\neq U\subset S}(-2)^{\|U\|-1}G_U\right].$$

By the induction hypothesis we may substitute G_U by

$$(1/2)^{\|U\|}\left[-2\sum_{\phi\neq T\subseteq U}(-1)^{\|T\|}\ XOR_T\right].$$

Substituting and simplifying, we get

$$G_S = (-1/2)^{\|S\|-1}\left[XOR_S - \sum_{\phi\neq U\subset S}(-1)^{\|U\|}\left[\sum_{\phi\neq T\subseteq U}(-1)^{\|T\|}\ XOR_T\right]\right].$$

The right side of this equation expands to a linear combination of XOR_T's. In this equation the coefficient of XOR_S is $(-1/2)^{\|S\|-1}$ which is equal to $-2(1/2)^{\|S\|}(-1)^{\|S\|}$, as predicted by the lemma. Thus we need only show that the coefficients match for proper subsets of S. Let c_T be the coefficient of XOR_T for an arbitrary subset T of S. Then

$$\begin{aligned}
c_T &= -(-1/2)^{\|S\|-1}\sum_{T\subseteq U\subset S}(-1)^{\|U\|}(-1)^{\|T\|}\\
&= 2(-1/2)^{\|S\|}(-1)^{\|T\|}\sum_{i=0}^{\|S\|-\|T\|-1}\binom{\|S\|-\|T\|}{i}(-1)^{i+\|T\|}\\
&= 2(-1/2)^{\|S\|}\sum_{i=0}^{\|S\|-\|T\|-1}\binom{\|S\|-\|T\|}{i}(-1)^{i}\\
&= 2(-1/2)^{\|S\|}(-(-1)^{\|S\|-\|T\|})\\
&= -2(1/2)^{\|S\|}(-1)^{\|T\|}
\end{aligned}$$

$\cdot\square$

Corollary 2 *Let $\epsilon_T = XOR_T - (1/2)$, then*

$$G_S = (1/2)^{\|S\|}\left[1 - 2\sum_{\phi\neq T\subseteq S}(-1)^{\|T\|}\epsilon_T\right].$$

proof : Using lemma 2,

$$
\begin{aligned}
G_S &= (1/2)^{\|S\|}\left[-2\sum_{\phi\neq T\subseteq S}(-1)^{\|T\|}\,XOR_T\right]\\
&= (1/2)^{\|S\|}\left[-2\sum_{\phi\neq T\subseteq S}(-1)^{\|T\|}((1/2)+\epsilon_T)\right]\\
&= (1/2)^{\|S\|}\left[1-2\sum_{\phi\neq T\subseteq S}(-1)^{\|T\|}\epsilon_T\right]
\end{aligned}
$$

$\cdot\Box$

Up to this point we have not assumed ϵ-independence. Lemma 1 and lemma 2 apply to any set of binary-valued random variables. Now suppose that S is a set of ϵ-independent random variables. Corollary 2 gives us a bound on the probability that all $A_i \in S$ hold:

Corollary 3 *If S is a set of ϵ-independent random variables then the probability that all A_i hold deviates from $(1/2)^{\|S\|}$ by no more than 2ϵ.*

proof : Let ϵ_T be as in corollary 2 and note that $|\epsilon_T| < \epsilon$. Then, by corollary 2,

$$
\begin{aligned}
|G_S-(1/2)^{\|S\|}| &= 2(1/2)^{\|S\|}\left|\sum_{\phi\neq T\subseteq S}(-1)^{\|T\|}\epsilon_T\right|\\
&\leq 2(1/2)^{\|S\|}\sum_{\phi\neq T\subseteq S}|(-1)^{\|T\|}\epsilon_T|\\
&< 2\epsilon
\end{aligned}
$$

$\cdot\Box$

The notion of ϵ-independence carries to random variables which take any two distinct values u and v (i.e. not just 0 or 1). In this case, we arbitrarily label u with "1" and v with "0", with the XOR and negation operators defined in the natural way. Note that if we replace any of the A_i's by their negation, then ϵ-independence is preserved. Therefore the previous corollary implies the main lemma in this section:

Lemma 3 *If S is a set of ϵ-independent random variables then the joint distribution of the A_i's deviates from the joint distribution of independent fair coins by no more than 2ϵ.*

4 Quadratic residues and nonresidues modulo a prime number

An element $y \in Z_P$ is a quadratic residue if $X_P(y) = 1$ or 0. Otherwise y is a quadratic nonresidue. Let x be chosen with uniform distribution in Z_P. Statistical independence among fair coins is, in some sense, lack of structure in the system comprising the coins. We will show that the quadratic characters of the integers in the range $x+1, ..., x+t$ are ϵ-independent with $\epsilon = \frac{t(3+\sqrt{P})}{2P}$. We offer this as an explanation for the observed lack of structure in the sequence of quadratic character values modulo a prime number.

Theorem 1 *Let x be a random number in Z_P. Let $S = \{A_i \mid 0 < i \leq t\}$ be a set of random variables such that A_i takes the value 1 if $x+i$ is a quadratic nonresidue modulo P and 0 otherwise. Then the A_i's are ϵ-independent with $\epsilon = \frac{t(3+\sqrt{P})}{2P}$.*

proof : Let T be any non-empty subset of S, and $\Theta = \{i | A_i \in T\}$. Let X^+ be the number of elements x in Z_P such that $X_P(f_\Theta(x)) = 1$ and X^- be the number of elements such that $X_P(f_\Theta(x)) = -1$. By the Weil bound, and the fact that $X^+ + X^- = P - \|\Theta\|$, we have

$$\begin{aligned} \|\Theta\|\sqrt{P} &> |\sum_{x \in Z_P} X_P(f_\Theta(x))| \\ &= |X^+ - X^-| \\ &= |P - \|\Theta\| - 2X^-|. \end{aligned}$$

Dividing by $2P$, we have $\frac{\|\Theta\|}{2\sqrt{P}} > |(1/2) - \frac{\|\Theta\|}{2P} - \frac{X^-}{P}|$. But $\frac{X^-}{P}$ is the probability that $f_\Theta(x)$ evaluates to a quadratic nonresidue. Therefore this probability deviates from $(1/2)$ by no more than $\frac{\|\Theta\|}{2P} + \frac{\|\Theta\|}{2\sqrt{P}}$. Note that if $f_\Theta(x) \neq 0$ then $f_\Theta(x)$ is a nonresidue if and only if XOR_T. Since the probability that $f_\Theta(x) = 0$ is $\frac{\|\Theta\|}{P}$, we have that XOR_T deviates from $(1/2)$ by no more than $\frac{\|\Theta\|}{P} + \frac{\|\Theta\|}{2P} + \frac{\|\Theta\|}{2\sqrt{P}} = \frac{\|\Theta\|(3+\sqrt{P})}{2P}$. Since $\|\Theta\| \leq t$, the A_i's are ϵ-independent with $\epsilon = \frac{t(3+\sqrt{P})}{2P}$.$\square$

Let $\vec{b}$ be a vector of R's and N's (e.g. $\vec{b} = RNRNRRR$). We call such a vector a "quadratic character sequence". We denote the i'th letter of $\vec{b}$ by b_i. If x is such that

$x+i$ is a quadratic residue if and only if $b_i = R$ then we say that x "induces" $\vec{b}$ in Z_P. We say Z_P "contains" the quadratic character sequence $\vec{b}$ if some $x \in Z_P$ induces $\vec{b}$.

Corollary 4 *Fix a quadratic character sequence $\vec{b}$ of length t. Let x be random in Z_P. Then the probability that x induces $\vec{b}$ is in the range $(1/2)^t \pm \frac{t(3+\sqrt{P})}{P}$.*

proof : By theorem 1 and lemma 3 .□

Corollary 5 *Fix a quadratic character sequence $\vec{b}$ of length t. The number of occurrences of $\vec{b}$ in Z_P is in the range $P(1/2)^t \pm t(3+\sqrt{P})$. In particular, if $P(1/2)^t > t(3+\sqrt{P})$ then the sequence $\vec{b}$ must occur in Z_P.*

Corollary 6 *Let $u < (1/2)$. Then for all but finitely many primes P, Z_P contains all possible quadratic character sequences of length $u \log_2 P$.*

proof : By the previous corollary and the fact that $P(1/2)^{u \log_2 P}$ is asymptotically greater than $(3+\sqrt{P}) \log_2 P$ when u is less than $(1/2)$.□

5 The ρ-complexity of finding patterns of residues and nonresidues.

There is no known deterministic polynomial-time algorithm for finding quadratic nonresidues modulo a prime number P (unless the Extended Riemann Hypothesis is assumed, see [2]). If in fact no such algorithm exists, then there is some amount of randomness inherently necessary to effectively solve this problem. The following definition has been proposed as one measure of the amount of randomness needed to solve a search problem in polynomial time [10].

Definition 1 *the $\rho-$complexity of a search problem is less than or equal to $\rho(n)$ if there exists a polynomial-time algorithm which uses at most n bits of randomness for each input of size n and solves the problem with failure probability asymptotically bounded above by $\rho(n)$.*

The next corollary implies that with access to one random number modulo P, any constant number of nonresidues can be found, with exponentially low probability of failure, in an interval of length $\lfloor \log_2 P \rfloor$. Thus the ρ-complexity of this problem is exponentially low.

Corollary 7 *Suppose P is prime and $k \leq \lfloor \log_2 P \rfloor$. Then the probability that the increment sequence of length $\lfloor \log_2 P \rfloor$ and random seed contains less than k nonresidues modulo P is bounded above by* $4\frac{\log_2 P}{\sqrt{P}} \sum_{i=0}^{k-1} \begin{pmatrix} \lfloor \log_2 P \rfloor \\ i \end{pmatrix}$.

proof : Let A_i $(i = 1 \ldots \lfloor \log_2 P \rfloor)$ take the value 1 if $x + i$ is a quadratic nonresidue modulo P and 0 otherwise. By lemma 3 and theorem 1 the joint distribution of the A_i's differs from independent fair coins by at most $\frac{(3+\sqrt{P})\lfloor \log_2 P \rfloor}{P}$. Thus the probability that the increment sequence of length $\lfloor \log_2 P \rfloor$ contains less than k nonresidues is at most

$$\sum_{i=0}^{k-1} \begin{pmatrix} \lfloor \log_2 P \rfloor \\ i \end{pmatrix} ((1/2)^{\lfloor \log_2 P \rfloor} + \frac{(3+\sqrt{P})\lfloor \log_2 P \rfloor}{P}) \leq 4\frac{\log_2 P}{\sqrt{P}} \sum_{i=0}^{k-1} \begin{pmatrix} \lfloor \log_2 P \rfloor \\ i \end{pmatrix}$$

$\bullet\Box$

No particular significance is attached to the constant 4 in corollary 7. The constant can be made arbitrarily close to 1 by assuming P is large enough.

Restricting k to 1 in the previous corollary gives us a bound of $4\frac{\log_2 P}{\sqrt{P}}$ on the ρ complexity of finding one nonresidue modulo P. Our next concern is the ρ-complexity of finding specified quadratic character sequences of length $k > 1$ modulo P. Given a constant c, we will denote by c^+ a constant bigger than c and by c^- a constant smaller than c.

Lemma 4 *Let P be prime. Let $\vec{b}$ be a quadratic character sequence of length $k > 1$. The ρ-complexity of finding the sequence $\vec{b}$ in Z_P is bounded above by*

$$(1/P)^{(1/2)^- - \frac{k}{4k-2\log_2(2^k-1)}}.$$

proof : The algorithm is, given random $x \in Z_P$, to search for the pattern $\vec{b}$ in $x+1, x+2, ..., x+t$, where t is a multiple of k to be quantified below. Let $B_{\vec{b},t}$

be the set of strings of R's and N's of length t which do not contain $\vec{b}$. We have $\mid B_{\vec{b},t} \mid < (2^k-1)^{t/k}$, since if we divide a string in $B_{\vec{b},t}$ into t/k pieces of length k, then each piece must be different from $\vec{b}$. Let ρ be the probability that $\vec{b}$ does not appear in the quadratic characters of $x+1, x+2, ..., x+t$. Then by lemma 3 and theorem 1

$$\begin{aligned} \rho &\leq \mid B_{\vec{b},t} \mid((1/2)^t + \frac{t(3+\sqrt{P})}{P}) \\ &< (2^k-1)^{t/k}((1/2)^t + \frac{1^+ t}{\sqrt{P}}) \\ &< \left(\frac{2^k-1}{2^k}\right)^{t/k} + (\frac{1^+ t 2^t}{\sqrt{P}}) \end{aligned}$$

for P large enough.

Let $t = u \log_2 P$. Then the previous inequality implies

$$\begin{aligned} \rho &< \left(\frac{2^k-1}{2^k}\right)^{(u/k)\log_2 P} + (\frac{1^+ u(\log_2 P)P^u}{\sqrt{P}}) \\ &< \left(\frac{2^k-1}{2^k}\right)^{(u/k)\log_2 P} + (\frac{1}{P^{1/2-u^+}}) \\ &= (1/2)^a + (1/2)^b \end{aligned}$$

where $a = (\log_2\left(\frac{2^k}{2^k-1}\right))(\log_2 P)(u/k)$ and $b = ((1/2)-u^+)\log_2 P$. Now, if $k > 1$ and $u = \frac{k}{4k-2\log_2(2^k-1)}$ then $a = ((1/2)-u)\log_2 P > b$. Thus, for this value of u, $\rho < 2(1/2)^b = 2(1/P)^{(1/2)-u^+}$. Therefore ρ is asymptotically bounded above by $(1/P)^{(1/2)^- - \frac{k}{4k-2\log_2(2^k-1)}}$. $\square$

Acknowledgements

Several discussions on this subject with Eric Bach are gratefully acknowledged.

References

[1] N.S. Aladov. On the distribution of quadratic residues and non-residues of a prime number p in the sequence 1,2,...,p-1. *Mat. Sbornik*, 18:61–75, 1896. in russian.

[2] Eric Bach. *Analytic methods in the analysis and design of number-theoretic algorithms*. MIT press: Cambridge, 1985.

[3] Eric Bach. Realistic analysis of some randomized algorithms. *Journal of Computer and System Sciences*, 42(1):30–53, 1991.

[4] A. Brauer. Combinatorial methods in the distribution of k-th. power residues. In *Combinatorial mathematics and its applications*, pages 14–37. University of North Carolina Press, 1969.

[5] D. A. Burgess. The distribution of quadratic residues and non-residues. *Mathematika*, 4:106–112, 1957.

[6] H. Davenport. On the distribution of quadratic residues (mod p). *J. London Mathematical Society*, 6:49–54, 1931.

[7] H. Davenport. On the distribution of quadratic residues (mod p). *J. London Mathematical Society*, 8:46–52, 1933.

[8] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, 1986. english edition.

[9] R. H. Hudson. On the first occurrence of certain patterns of quadratic residues and non-residues. *Israel Journal of Mathematics*, 44(1):23–32, 1983.

[10] R. Peralta. On the randomness complexity of algorithms. Technical Report TR 90-1, Electrical Engineering and Computer Science Department, University of Wisconsin-Milwaukee, 1990.

[11] W. Schmidt. *Equations over finite fields*. Springer Verlag, 1976.