Note on an Additive Characterization of Quadratic Residues Modulo p

Chris Monico, Michele Elia

Draft of January 27, 2006

Abstract

It is shown that an even partition $A \cup B$ of the set $\mathcal{R} = \{1, 2, \ldots, p-1\}$ of positive residues modulo an odd prime p is the partition into quadratic residues and quadratic non-residues if and only if the elements of A and B satisfy certain additive properties, thus providing a purely additive characterization of the set of quadratic residues.

1 Additive properties of quadratic residues

An integer a which is not a multiple of a prime p is called a quadratic residue modulo p if the quadratic equation $x^2 = a \bmod p$ has a solution. If it has no solution then a is called a quadratic non-residue modulo p. The set $\mathcal{R} = \{1, 2, \cdots, p-1\}$ of non-zero residues modulo p is evenly partitioned by the quadratic residue character into two sets, A and B, of quadratic residues and quadratic non-residues, respectively. The property of being a quadratic residue or a quadratic non-residue is inherently a multiplicative property, by its definition in terms of field product operations. The paper shows that the set of quadratic residues modulo p can also be characterized strictly in terms of field addition operations. Specifically, it determines the number of ways in which an element c of $\mathcal{R}$ can be written as a sum of two elements from A or two elements from B. The answer depends only on whether c is itself an element of A or B. We then show that this property completely determines the sets A and B, providing a purely additive characterization of the set of quadratic residues.

Let p be an odd prime, and let QR and QNR stand for quadratic residue and quadratic non-residue, respectively, in the prime field $\mathbb{F}_p$ of p elements. Two generating polynomials for the sets of QR and QNR are defined as

$$r_p(x) = \sum_{\substack{1 \le j < p \\ (j \,|\, p) = 1}} x^j, \qquad q_p(x) = \sum_{\substack{1 \le j < p \\ (j \,|\, p) = -1}} x^j.$$

The canonical representatives of $r_p(x)^2$ and $q_p(x)^2$ modulo $\langle x^p - 1 \rangle$ in $\mathbb{F}_p[x]$ are denoted by

$$\begin{aligned} r_p(x)^2 &\equiv a_0 + a_1 x + \cdots + a_{p-1} x^{p-1} \pmod{\langle \mathrm{x^p} - 1 \rangle} \\ q_p(x)^2 &\equiv b_0 + b_1 x + \cdots + b_{p-1} x^{p-1} \pmod{\langle \mathrm{x^p} - 1 \rangle} \end{aligned}$$

where a_j, b_j are non-negative integers smaller than p. It is observed that a_j [or b_j] is precisely the number of ways in which j can be written as a sum of two quadratic residues [or non-residues]. Thus, a_j, b_j can be considered as elements of the set $\{0, 1, 2, \cdots, p-1\}$ of canonical representatives of $\mathbb{Z}/p\mathbb{Z}$.

Lemma 1.1 *Let p be an odd prime and a_i, b_i as defined above. Then for $i, j \in \mathcal{R}$, the following hold:*

1. $b_j - a_j = (j \,|\, p)$.
2. *If* $(i \,|\, p) = (j \,|\, p)$, *then* $a_i = a_j$ *and* $b_i = b_j$.

Proof: Observe first that $r_p(x) + q_p(x) = x + x^2 + \cdots + x^{p-1} = \frac{x^p-1}{x-1} - 1$. Since there are precisely $(p-1)/2$ quadratic residues and the same number of non-residues, it follows that $r_p(1) - q_p(1) = 0$, whence $(x-1)|(r_p(x) - q_p(x))$, that is $r_p(x) - q_p(x) = (x-1)f_p(x)$. It follows that modulo $\langle x^p - 1\rangle$ we have

$$\begin{aligned} r_p(x)^2 - q_p(x)^2 &= (x-1)f_p(x)\left[\frac{x^p-1}{x-1} - 1\right] \\ &= f_p(x)(x^p - 1) - (x-1)f_p(x) \\ &\equiv (1-x)f_p(x) \\ &\equiv q_p(x) - r_p(x) \pmod{\langle \mathrm{x}^{\mathrm{p}} - 1\rangle}. \end{aligned}$$

Thus, $r_p(x)^2 + r_p(x) \equiv q_p(x)^2 + q_p(x) \pmod{\langle \mathrm{x}^{\mathrm{p}} - 1\rangle}$, which proves part 1.

Suppose now that $i, j \in \{1, 2, \ldots, p-1\}$ are both quadratic residues modulo p. Then there exist quadratic residues $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ so that $i\alpha \equiv j \pmod{\mathrm{p}}$, $i \equiv j\beta \pmod{\mathrm{p}}$. If x, y are quadratic residues with $i \equiv x + y \pmod{\mathrm{p}}$, it follows that $j \equiv x\alpha + y\alpha \pmod{\mathrm{p}}$ and $x\alpha, y\alpha$ are also quadratic residues. Similarly, if x, y are quadratic residues with $j \equiv x + y \pmod{\mathrm{p}}$, it follows that $i \equiv x\beta + y\beta \pmod{\mathrm{p}}$, and $x\beta, y\beta$ are quadratic residues. Thus, if i, j are both quadratic residues, we have the equality $a_i = a_j$. By similar arguments, we obtain $a_i = a_j$ for $(i \,|\, p) = (j \,|\, p)$. It then follows from the first part of the lemma that $b_i = b_j$ for $(i \,|\, p) = (j \,|\, p)$. □

Let α_1, α_{-1} denote the common value of the a_i with $(i \,|\, p) = 1, -1$, respectively. Similarly, define β_1, β_{-1} to be the common values of the b_i for $(i \,|\, p) = 1, -1$, respectively. Our immediate goal is to explicitly determine these quantities. It follows from simply counting the number of sums of quadratic [non-]residues that

$$\alpha_1 + \alpha_{-1} = \beta_1 + \beta_{-1} = \begin{cases} \frac{p-3}{2}, & \text{if } p \equiv 1 \pmod 4 \\ \frac{p-1}{2}, & \text{if } p \equiv 3 \pmod 4 \end{cases}. \tag{1.1}$$

The different cases above result from the fact that, if $p \equiv 1 \pmod 4$, then 0 can be written as a sum of quadratic residues in exactly $p-1$ ways, whereas if $p \equiv 3 \pmod 4$, then 0 cannot be written as any sum of two quadratic non-residues.

Theorem 1.2 *Let p be an odd prime and set*

$$d_p = \begin{cases} \frac{p-1}{4} & , \text{ if } p \equiv 1 \pmod 4 \\ \frac{p+1}{4} & , \text{ if } p \equiv 3 \pmod 4 \end{cases} . \tag{1.2}$$

Then every quadratic residue [non-residue] can be written as a sum of two quadratic residues [non-residues] in exactly $d_p - 1$ ways. Every quadratic residue [non-residue] can be written as a sum of two quadratic non-residues [residues] in exactly d_p ways. Moreover, every non-zero residue can be written as a sum of a QR and a QNR in exactly $p - 1 - 2d_p$ ways.

Proof: As above, let α_1, β_1 denote respectively the number of ways in which a quadratic residue can be written as a sum of two quadratic residues or non-residues. Let α_{-1}, β_{-1} denote respectively the number of ways in which a quadratic non-residue can be written as a sum of two quadratic residues or non-residues. It is necessary to show that $d_p = \alpha_{-1} = \beta_1$ and $d_p - 1 = \alpha_1 = \beta_{-1}$. Notice that there is a bijection between sums of quadratic residues equaling a quadratic residue and sums of non-residues equaling a non-residue (induced by multiplication by a non-residue) whence $\alpha_1 = \beta_{-1}$. Combining this with the result from Lemma 1.1 that $\beta_1 - \alpha_1 = 1$, we have $\beta_1 - \beta_{-1} = 1$. The results then follow by applying Equation 1.1.
The equation $x_1 + x_2 = a$ in $\mathbf{F}_p$ has $p-2$ solutions with neither x_1 nor x_2 equal 0. Therefore, the number of solutions with x_1 a QR, and x_2 a QNR, or vice-versa, is $p - 2 - (2d_p - 1)$. □

2 The converse

The goal of this section is to show that the additive properties given in Section 1 completely characterize the quadratic residues. Let d_p be defined as in Equation (1.2), and, for the remainder of this section, suppose A and B form an even partition of $F_p \setminus \{0\}$ such that

1. Every element of A [B] can be written as a sum of two elements from A [B] in exactly $d_p - 1$ ways.

2. Every element of A [B] can be written as a sum of two elements from B [A] in exactly d_p ways.

Define two polynomials in $\mathbb{F}_p[x]$,

$$a(x) = \sum_{a \in A} x^a, \qquad b(x) = \sum_{b \in B} x^b.$$

It follows from the assumptions on the sets A and B that

$$\begin{aligned} a(x)^2 &\equiv (d_p - 1)a(x) + d_p b(x) + c_p \\ &\equiv d_p(x + x^2 + \cdots + x^{p-1}) - a(x) + c_p \pmod{\langle \mathrm{x}^{\mathrm{p}} - 1 \rangle}, \end{aligned}$$

where c_p is the number of ways in which zero can be written as a sum of two elements of A. Evaluation at $x = 1$ shows that $c_p = \frac{p-1}{2}$ if $p \equiv 1 \pmod 4$ and $c_p = 0$ if $p \equiv 3 \pmod 4$. Thus,

$$a(x)^2 + a(x) \equiv d_p\left((x-1)^{p-1} - 1\right) + c_p \qquad (\text{mod } \langle \mathrm{x^p} - 1\rangle) \tag{2.3}$$

Similarly, we find that

$$b(x)^2 + b(x) \equiv d_p\left((x-1)^{p-1} - 1\right) + c_p \qquad (\text{mod } \langle \mathrm{x^p} - 1\rangle) \tag{2.4}$$

We will use the following Hensel-like lemma to show that $\{a(x), b(x)\} = \{r_p(x), q_p(x)\}$.

Lemma 2.1 *Let p be an odd prime, and $R_k := \mathbb{F}_p[x]/\langle (x-1)^k\rangle$ for $k \geq 1$. Then each invertible element of R_k has at most two distinct square roots.*

Proof: We proceed by induction on k. The base case is obvious since $R_1 \cong \mathbb{F}_p$. Suppose now that the result holds for all $1 \leq k \leq N$. Further suppose that $a, b, c, g \in \mathbb{F}_p[x]$ are invertible modulo $\langle (x-1)^{N+1}\rangle$ and

$$a^2 + \langle (x-1)^{N+1}\rangle = b^2 + \langle (x-1)^{N+1}\rangle = c^2 + \langle (x-1)^{N+1}\rangle = g + \langle (x-1)^{N+1}\rangle.$$

By canonical projection onto R_N, it follows that $a^2 + \langle (x-1)^N\rangle = b^2 + \langle (x-1)^N\rangle = c^2 + \langle (x-1)^N\rangle = g + \langle (x-1)^N\rangle$, so that two of these must be equal by the induction hypothesis, say $a + \langle (x-1)^N\rangle = b + \langle (x-1)^N\rangle$. It follows that $a = b + (x-1)^N f$ for some $f \in \mathbb{F}_p[x]$. Thus,

$$\begin{aligned} b^2 + \langle (x-1)^{N+1}\rangle &= a^2 + \langle (x-1)^{N+1}\rangle \\ &= (b + (x-1)^N f)^2 + \langle (x-1)^{N+1}\rangle \\ &= b^2 + 2(x-1)^N bf + (x-1)^{2N} f^2 + \langle (x-1)^{N+1}\rangle \\ &= b^2 + 2(x-1)^N bf + \langle (x-1)^{N+1}\rangle. \end{aligned}$$

So $2(x-1)^N bf \in \langle (x-1)^{N+1}\rangle$, but since $2b$ is invertible modulo $\langle (x-1)^{N+1}\rangle$, it follows that $(x-1) \mid f$, so that $a + \langle (x-1)^{N+1}\rangle = b + \langle (x-1)^{N+1}\rangle$. □

Theorem 2.2 *Let p be an odd prime and let d_p be defined as in Equation (1.2). Suppose $A \subset \mathbb{F}_p^*$ and $B = \mathbb{F}_p^* \setminus A$. Then A is precisely the set of quadratic residues of $\mathbb{F}_p$ if and only if*

1. $|A| = (p-1)/2$,
2. $1 \in A$,
3. *Every element of A can be written as a sum of two elements from A in exactly $d_p - 1$ ways.*
4. *Every element of B can be written as a sum of two elements from A in exactly d_p ways.*

Proof: As in Equation 2.3, it follows from the hypotheses that

$$a(x)^2 + a(x) \equiv d_p\left((x-1)^{p-1} - 1\right) + c_p \qquad (\mathrm{mod}\ \langle \mathrm{x^p} - 1\rangle)\,,$$

where

$$c_p = \begin{cases} \frac{p-1}{2}, & \text{if } p \equiv 1 \pmod 4 \\ 0, & \text{if } p \equiv 3 \pmod 4\,. \end{cases}$$

It is an immediate corollary of Lemma 2.1 that a quadratic equation in $R_k[y]$ with invertible coefficients has at most two solutions (this follows from a completing-the-square argument). In particular, the equation $y^2+y-d_p\left((x-1)^{p-1}-1\right)-c_p = 0$ has coefficients invertible in R_p so that it has at most two distinct solutions in $R_p = \mathbb{F}_p[x]/\langle(x-1)^p\rangle = \mathbb{F}_p[x]/\langle x^p-1\rangle$. From the proof of 1.1, we have that $r_p(x)$ and $q_p(x)$ are two distinct solutions, so that $a(x) = r_p(x)$ or $a(x) = q_p(x)$. But since $1 \in A$ and A, B are disjoint by assumption, it must be the case that $a(x) = r_p(x)$. □

2.1 A second proof

In this section, we present an alternate derivation and proof of the results in the first two sections. Let $\mathcal{R}$ and $\mathcal{Q}$ be the subsets of $\mathbb{F}_p$ consisting of QRs and QNRs, respectively. Let $(j\,|\,p)$ denote the Legendre symbol. The characteristic functions of $\mathcal{R}$ and $\mathcal{Q}$ are

$$\begin{cases} r(0) = 0 \quad \text{and} \quad r(j) = \dfrac{1+(j\,|\,p)}{2} \quad , \quad j \in \mathbb{Z}_p \\ \\ q(0) = 0 \quad \text{and} \quad q(j) = \dfrac{1-(j\,|\,p)}{2} \quad , \quad j \in \mathbb{Z}_p\ , \end{cases}$$

respectively, and their generating functions are

$$\begin{cases} r_p(x) = \displaystyle\sum_{j=1}^{p-1} \frac{1+(j\,|\,p)}{2} x^j = \frac{1}{2}\left(z_p(x) + g(x) - 1\right) \\ q_p(x) = \displaystyle\sum_{j=1}^{p-1} \frac{1-(j\,|\,p)}{2} x^j = \frac{1}{2}\left(z_p(x) - g(x) - 1\right) \end{cases} \tag{2.5}$$

where $z_p(x) = \sum_{j=0}^{p-1} x^j$ is the generating function of the characteristic function of $\mathbb{F}_p$, and $g(x) = \sum_{i=0}^{p-1}(i\,|\,p)x^i$ is a Gaussian-like sum.

The conclusions of Section 1, can be rewritten in terms of generating polynomials $r_p(x)$ and $q_p(x)$ as follows

$$\begin{cases} r_p(x)^2 + r_p(x) = \dfrac{p-(-1\,|\,p)}{4}\left(z_p(x) + (-1\,|\,p)\right) \qquad \mathrm{mod}\ x^p - 1 \\ \\ r_p(x) + q_p(x) = z_p(x) - 1\ . \end{cases} \tag{2.6}$$

Conversely, $r_p(x)$ and $q_p(x)$ are the only polynomials with $0, 1$ coefficients that satisfy equation (2.6). To prove this using a different argument from that given in the previous section, let $\mathcal{A}$ and $\mathcal{B}$ be two subsets forming an even partition of $\mathbb{F}_p \backslash \{0\}$, as above. Let the generating polynomials of their characteristic functions satisfy the conditions

$$\begin{cases} a(x)^2 + a(x) &= \frac{p-(-1\,|\,p)}{4}\,(z_p(x) + (-1\,|\,p)) \qquad \bmod x^p - 1 \\ a(x) + b(x) &= z_p(x) - 1 \ . \end{cases} \tag{2.7}$$

Therefore $A(m) = a(\zeta_p^m)$ satisfies the equation $A(m)^2 + A(m) = \frac{p(-1\,|\,p)-1}{4}$, $\forall m \neq 0$, and $A(0) = \frac{(p-1)}{2}$, thus

$$A(m) = -\frac{1}{2} \pm \frac{\sqrt{(-1\,|\,p)p}}{2} \quad \forall m \neq 0 \ ,$$

where the only uncertainty lies in the sign. Hence any $A(m)$ is in the quadratic field $\mathbb{Q}(\sqrt{(-1\,|\,p)p})$, which is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$ [6, Exer. 1,p.17]. Since the numerical value of the so-called Gauss sum $g(\zeta_p^m)$ is $(m\,|\,p)g(\zeta_p) = \pm\sqrt{(-1\,|\,p)p}\ \forall m \neq 0$, [3, Equation (5),p.7], (where the uncertainty of the sign is due to the choice of the primitive root ζ_p, as Davenport pointed out in [3, p.13]), it follows that

$$A(m) = -\frac{1}{2} \pm \frac{1}{2}(m\,|\,p)g(\zeta_p) \quad , \quad m \neq 0.$$

The degree of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $p-1$, [6, Theorem 2.5, p.11], and an integral basis is $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$, thus the representation $A(m) = \sum_{j \in \mathcal{R}} \zeta_p^j$ is *unique* except for a choice of the primitive root ζ_p. This uniqueness of representation in a given integral basis of every element of an algebraic number field, implies that the only partition of $\mathbb{F}_p$, whose generating function satisfies (2.7), is $\mathbb{F}_p = \mathcal{R} \cup \mathcal{Q}$.

□

3 Conclusions

For completeness, we compute the number of solutions to

$$n \equiv a + b \ (\text{mod p}) \ , \qquad (ab\,|\,p) = -1, \ \text{for } p \not| n$$

which is simply obtained by observing that $n = a+b$ has p solutions in total and $d_p + (d_p - 1)$ solutions with $(ab\,|\,p) = 0$. Additionally, there are two solutions with $(ab\,|\,p) = 0$, so that the number of solutions with $(ab\,|\,p) = -1$ is given by

$$p - (2d_p - 1) - 2 = p - 2d_p - 1 = \frac{p - 2 + (-1\,|\,p)}{2}.$$

It is finally remarked that Theorem 1.2 is obtained using elementary techniques, while the proofs of the converse in Section 2 require some tools from commutative algebra and/or algebraic number theory. It is an open problem to find a more direct proof that these additive properties characterize the quadratic residues.

References

[1] G.E. Andrews. *Number Theory*, New York: Dover, 1994.

[2] R. Crandall, C. Pomerance. *Prime Numbers, A Computational Perspective*, New York: Springer, 2001.

[3] H. Davenport. *Multiplicative Number Theory*, New York: Springer, 1980.

[4] K.F. Gauss. *Disquisitiones Arithmeticae*, New York: Springer, 1986.

[5] H.L. Montgomery. *Topics in Multiplicative Number Theory*, New York: Springer, 1971.

[6] L.C. Washington. *Introduction to Cyclotomic fields*, New York: Springer, 1997.

[7] H. Weyl. *Algebraic Theory of Numbers*, Princeton, NJ: Princeton Univ. Press, 1980.