Int. J. Contemp. Math. Sciences, Vol. 6, 2011, no. 2, 87 - 96

Partitions of a Residue into Quadratic Residues

Rafael Jakimczuk

División Matemática, Universidad Nacional de Luján
Buenos Aires, Argentina
jakimczu@mail.unlu.edu.ar

Abstract

Let us consider a odd prime $p > t$. In this article we obtain polynomial formulae that give us the number of sums of t quadratic residues whose result is a fixed quadratic residue, quadratic nonresidue or zero (the order of the summands is irrelevant). That is, we study the number of partitions of a quadratic residue (quadratic nonresidue or zero) in t quadratic residues.

Mathematics Subject Classification: 11A99

Keywords: Sums of quadratic residues

1 Introduction

Let p be a odd positive prime. Let $C0$ be a quadratic residue mod p and $C1$ a quadratic nonresidue mod p. Note that in this notation we have:

$$C0\ C0 = C0 \qquad C1\ C1 = C0 \qquad C0\ C1 = C1 \qquad C1\ C0 = C1$$

Let $Ci + Cj = Ck$ be the set of sums such that the first summand is a Ci ($i = 0, 1$), the second summand is a Cj ($j = 0, 1$) and the result of the sum is a fixed Ck ($k = 0, 1$).

Let $Ci + Cj = 0$ the set of sums such that the first summand is a Ci ($i = 0, 1$), the second summand is a Cj ($j = 0, 1$) and the result of the sum is zero.

We have the following Table (see [1]).

TABLE

If p is a prime of the form $4N+1$, then

$$The\ set\quad C0+C0=0\quad has\quad (p-1)/2\quad sums.$$

$$The\ set\quad C0+C0=C0\quad has\quad (p-5)/4\quad sums.$$

$$The\ set\quad C0+C0=C1\quad has\quad (p-1)/4\quad sums.$$

$$The\ set\quad C1+C1=0\quad has\quad (p-1)/2\quad sums.$$

$$The\ set\quad C1+C1=C0\quad has\quad (p-1)/4\quad sums.$$

$$The\ set\quad C1+C1=C1\quad has\quad (p-5)/4\quad sums.$$

$$The\ set\quad C0+C1=0\quad has\quad 0\quad sums.$$

$$The\ set\quad C0+C1=C0\quad has\quad (p-1)/4\quad sums.$$

$$The\ set\quad C0+C1=C1\quad has\quad (p-1)/4\quad sums.$$

$$The\ set\quad C1+C0=0\quad has\quad 0\quad sums.$$

$$The\ set\quad C1+C0=C0\quad has\quad (p-1)/4\quad sums.$$

$$The\ set\quad C1+C0=C1\quad has\quad (p-1)/4\quad sums.$$

If p is a prime of the form $4N+3$, then

$$The\ set\quad C0+C0=0\quad has\quad 0\quad sums.$$

$$The\ set\quad C0+C0=C0\quad has\quad (p-3)/4\quad sums.$$

$$The\ set\quad C0+C0=C1\quad has\quad (p+1)/4\quad sums.$$

$$The\ set\quad C1+C1=0\quad has\quad 0\quad sums.$$

$$The\ set\quad C1+C1=C0\quad has\quad (p+1)/4\quad sums.$$

$$The\ set\quad C1+C1=C1\quad has\quad (p-3)/4\quad sums.$$

$$The\ set\quad C0+C1=0\quad has\quad (p-1)/2\quad sums.$$

$$The\ set\quad C0+C1=C0\quad has\quad (p-3)/4\quad sums.$$

$$The\ set\quad C0+C1=C1\quad has\quad (p-3)/4\quad sums.$$

$$The\ set\quad C1+C0=0\quad has\quad (p-1)/2\quad sums.$$

$$The\ set\quad C1+C0=C0\quad has\quad (p-3)/4\quad sums.$$

$$The\ set\quad C1+C0=C1\quad has\quad (p-3)/4\quad sums.$$

2 Structures. Set of Structures. Notation.

Let t be a positive integer and p a odd prime such that $p > t$. Let us consider the set of all sums (the order of the summands is irrelevant) of t quadratic residues whose result is a fixed quadratic residue (quadratic nonresidue or zero) where there are L distinct quadratic residues and such that:

L_1 distinct quadratic residues repeat K_1 times each.

L_2 distinct quadratic residues repeat K_2 times each.

$$\vdots$$

L_m distinct quadratic residues repeat K_m times each.

Where

$$K_1 > K_2 > \cdots > K_m$$

Note that then we have:

$$L_1 + L_2 + \cdots + L_m = L$$

$$L_1K_1 + L_2K_2 + \cdots + L_mK_m = t$$

We shall call this set of sums structure. This set can be empty or not.

We shall denote a structure whose sums have result a fixed quadratic residue E in the form:

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/E)$$

We shall denote a structure whose sums have result a fixed quadratic non-residue F in the form:

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/F)$$

We shall denote a structure whose sums have result zero in the form:

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0)$$

Besides, some times, we shall indicate the number of sums in a structure using this same notation.

The notation

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0)$$

where the quadratic residue $C0$ is not indicated represent a set of structures, that is, a structure for each value of $C0$. Clearly the number of sums in each structure does not depend of $C0$. The notation

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1)$$

where the nonquadratic residue $C1$ is not indicated represent a set of structures, that is, a structure for each value of $C1$. Clearly the number of sums in each structure does not depend of $C1$. The notation (for sake of simplicity)

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0)$$

also we shall consider a set of structures.

Besides, some times, we shall indicate the number of sums in each structure in a set of structures using this same notation.

Example 2.1 *a) If* $p = 17$ *the sum*

$$1+1+1+1+8+8+8+8+2+2+13+13+9+15+4 = 9$$

pertains to the structure $(2, 4 : 2, 2 : 3, 1/9)$. *In this structure* $L_1 = 2$, $K_1 = 4$, $L_2 = 2$, $K_2 = 2$,$L_3 = 3$, $K_3 = 1$, $m = 3$, $L = 7$ *and* $t = 15$.

On the other hand, structure $(2, 4 : 2, 2 : 3, 1/9)$ *pertains to the set of structures* $(2, 4 : 2, 2 : 3, 1/C0)$

b)If $p = 11$ *we have*

$$(1, 3 : 4, 1/1) = 0 \qquad (1, 3 : 4, 1/10) = 1 \qquad (1, 3 : 4, 1/0) = 0$$

and

$$(1, 3 : 4, 1/C0) = 0 \qquad (1, 3 : 4, 1/C1) = 1 \qquad (1, 3 : 4, 1/0) = 0$$

Since

$$1+1+1+4+9+5+3 = 2 \quad 4+4+4+1+9+5+3 = 8 \quad 9+9+9+1+4+5+3 = 7$$

$$5+5+5+1+4+9+3 = 10 \quad 3+3+3+1+4+9+5 = 6$$

The following sets of structures where $L = 1$ we shall call basic sets of structures.

$$(1, t/C0) \qquad (1, t/C1) \qquad (1, t/0)$$

The proof of the following theorem is immediate.

Theorem 2.2 *Let* p *be a odd prime and* $1 \leq t < p$. *If* t *is a quadratic residue, then*

$$(1, t/C0) = 1 \qquad (1, t/C1) = 0 \qquad (1, t/0) = 0$$

If t *is a quadratic nonresidue, then*

$$(1, t/C0) = 0 \qquad (1, t/C1) = 1 \qquad (1, t/0) = 0$$

3 A Combinatorial Theorem.

Theorem 3.1 *Let p be a odd prime and $t < p$. Let us consider the following three sets of structures where $L \geq 2$. We shall call the structures in these sets of structures, structures A. In the right side of each set of structures we indicate the number of sums in each structure. Thus, for example, the set of structures 1 has A0 sums in each structure.*

$$1) \quad (L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0) \quad (A0)$$

$$2) \quad (L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1) \quad (A1)$$

$$3) \quad (L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0) \quad (A2)$$

The sums in each structure A have L distinct summands and t summands. That is

$$L_1 + L_2 + \cdots + L_m = L$$

$$L_1K_1 + L_2K_2 + \cdots + L_mK_m = t$$

Let us consider the following three sets of structures. We shall call the structures in these sets of structures, structures B. The sums in each structure B have $L-1$ distinct summands and $t - K_1$ summands.

$$4) \quad (L_1 - 1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0) \quad (B0)$$

$$5) \quad (L_1 - 1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1) \quad (B1)$$

$$6) \quad (L_1 - 1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0) \quad (B2)$$

Now, let us consider the following m sets with three sets of structures each. We shall call the structures in these sets of structures, structures D. The sums in each structure D have $L-1$ distinct summands and t summands.

$$1.0) \quad (1, K_1 + K_1 : L_1 - 2, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0) \quad (D1.0)$$

$$1.1) \quad (1, K_1 + K_1 : L_1 - 2, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1) \quad (D1.1)$$

$$1.2) \quad (1, K_1 + K_1 : L1 - 2, K1 : L2, K2 : \ldots : Lm, Km/0) \quad (D1.2)$$

$$2.0) \quad (1, K_1 + K_2 : L_1 - 1, K_1 : L_2 - 1, K_2 : \ldots : L_m, K_m/C0) \quad (D2.0)$$

$$2.1) \quad (1, K_1 + K_2 : L_1 - 1, K_1 : L_2 - 1, K_2 : \ldots : L_m, K_m/C1) \quad (D2.1)$$

$$2.2) \quad (1, K_1 + K_2 : L_1 - 1, K_1 : L_2 - 1, K_2 : \ldots : L_m, K_m/0) \quad (D2.2)$$

$$\vdots$$

$$m.0) \quad (1, K_1 + K_m : L_1 - 1, K_1 : L_2, K_2 : \ldots : L_m - 1, K_m/C0) \quad (Dm.0)$$

$m.1)$ $(1, K_1 + K_m : L_1 - 1, K_1 : L_2, K_2 : \ldots : L_m - 1, K_m/C1)$ $(Dm.1)$

$m.2)$ $(1, K_1 + K_m : L_1 - 1, K1 : L_2, K_2 : \ldots : L_m - 1, K_m/0)$ $(Dm.2)$

The following formulas hold.

If p is a prime of the form $4N + 1$ and K_1 is a quadratic residue.

$$A0 = \frac{1}{L_1}\left[\left(\frac{p-5}{4}\right)B0 + \left(\frac{p-1}{4}\right)B1 + B2 - (D1.0 + \cdots + Dm.0)\right] \quad (1)$$

$$A1 = \frac{1}{L_1}\left[\left(\frac{p-1}{4}\right)B0 + \left(\frac{p-1}{4}\right)B1 - (D1.1 + \cdots + Dm.1)\right] \quad (2)$$

$$A2 = \frac{1}{L_1}\left[\left(\frac{p-1}{2}\right)B0 - (D1.2 + \cdots + Dm.2)\right] \quad (3)$$

If p is a prime of the form $4N + 1$ and K_1 is a quadratic nonresidue.

$$A0 = \frac{1}{L_1}\left[\left(\frac{p-1}{4}\right)B0 + \left(\frac{p-1}{4}\right)B1 - (D1.0 + \cdots + Dm.0)\right] \quad (4)$$

$$A1 = \frac{1}{L_1}\left[\left(\frac{p-1}{4}\right)B0 + \left(\frac{p-5}{4}\right)B1 + B2 - (D1.1 + \cdots + Dm.1)\right] \quad (5)$$

$$A2 = \frac{1}{L_1}\left[\left(\frac{p-1}{2}\right)B1 - (D1.2 + \cdots + Dm.2)\right] \quad (6)$$

If p is a prime of the form $4N + 3$ and K_1 is a quadratic residue.

$$A0 = \frac{1}{L_1}\left[\left(\frac{p-3}{4}\right)B0 + \left(\frac{p-3}{4}\right)B1 + B2 - (D1.0 + \cdots + Dm.0)\right] \quad (7)$$

$$A1 = \frac{1}{L_1}\left[\left(\frac{p+1}{4}\right)B0 + \left(\frac{p-3}{4}\right)B1 - (D1.1 + \cdots + Dm.1)\right] \quad (8)$$

$$A2 = \frac{1}{L_1}\left[\left(\frac{p-1}{2}\right)B1 - (D1.2 + \cdots + Dm.2)\right] \quad (9)$$

If p is a prime of the form $4N + 3$ and K_1 is a quadratic nonresidue.

$$A0 = \frac{1}{L_1}\left[\left(\frac{p-3}{4}\right)B0 + \left(\frac{p+1}{4}\right)B1 - (D1.0 + \cdots + Dm.0)\right] \quad (10)$$

$$A1 = \frac{1}{L_1}\left[\left(\frac{p-3}{4}\right)B0 + \left(\frac{p-3}{4}\right)B1 + B2 - (D1.1 + \cdots + Dm.1)\right] \quad (11)$$

$$A2 = \frac{1}{L_1}\left[\left(\frac{p-1}{2}\right)B0 - (D1.2 + \cdots + Dm.2)\right] \quad (12)$$

Remark 3.2 *Note that the sums in structures A have L distinct summands. On the other hand, sums in structures B and D have $L-1$ distinct summands. This fact is important in the proof of Theorem 4.1.*

Remark 3.3 *If $L_1 = 1$ there exist $m-1$ sets with three sets of structures each instead of m. Since in this case the sets of structures 1.0, 1.1 and 1.2 do not exist.*

Proof. We shall prove formula (1).

Suppose that p is a prime of the form $4N+1$ and K_1 is a quadratic residue.

Let X be a quadratic residue. Let us consider the $\frac{p-1}{2}$ sums with two summands whose first summand is a quadratic residue and whose result is X. In these $\frac{p-1}{2}$ sums the second summands will be (use the Table of section 1) $\frac{p-5}{4}$ quadratic residues, $\frac{p-1}{4}$ quadratic nonresidues and a residue 0.

Replace each first summand by the sum of K_1 equal quadratic residues.

Now, replace each second summand using the structures B, that is, the structures in the sets of structures 4, 5 and 6.

There exist $B0$ sums whose result is a quadratic residue (see the set of structures 4). There exist $B1$ sums whose result is a quadratic nonresidue (see the set of structures 5). Finally, there exist $B2$ sums whose result is 0 (see the set of structures 6).

Replacing the $\frac{p-1}{2}$ second summands using these sums we obtain a set W with $\left[\frac{p-5}{4}B0 + \frac{p-1}{4}B1 + B2\right]$ sums whose result is the quadratic residue X. The sums in the set W clearly pertain to the structures (whose sums have result X) in the sets of structures 1, 1.0, 2.0,. . ., m.0. The set W can be empty or not.

Suppose that the set W is not empty. Consequently some set of structures 1, 1.0, 2.0,. . ., m.0 has a positive number of sums.

Suppose that $Dj.0$ where j pertain to the set $\{1, 2, \ldots, m\}$ is non zero. Then clearly all $Dj.0$ sums whose result is X (in the structure pertaining to the set of structures j.0) will be in the set W. On the other hand each of these $Dj.0$ sums appear only one times in the set W since K_1 is the greater K_i (see section 2).

Suppose that $A0$ is nonzero. Then clearly all $A0$ sums whose result is X (in the structure pertaining to the set of structures 1) will be in the set W. On the other hand each of these $A0$ sums appear L_1 times in the set W.

Consequently we obtain,

$$A0 = \frac{1}{L_1}\left[\left(\frac{p-5}{4}\right)B0 + \left(\frac{p-1}{4}\right)B1 + B2 - (D1.0 + \cdots + Dm.0)\right]$$

That is, formula (1).

If the set W is empty, then $Dj.0 = 0$ $(j = 1, 2 \ldots, m)$ and $A0 = 0$.

Therefore formula (1) is true in all possible cases. Formula (1) is proved.

The others formulae can be proved in the same way using the Table of section 1. The theorem is proved.

4 Polynomial Formulas.

Let $t \geq 2$. Let us consider the set $\{1, 2, \ldots, t\}$. In this set there exist a number s of prime numbers. Each prime number can be a quadratic residue or a quadratic nonresidue. There are 2^s possibilities. Consequently there are 2^s possible sequences of quadratic and nonquadratic residues in the set $\{1, 2, \ldots, t\}$. For example, if $t = 6$ and 2 is a quadratic residue, 3 is a quadratic non residue and 5 is a quadratic residue then 1 is a quadratic residue, 2 is a quadratic residue, 3 is a quadratic nonresidue, 4 is a quadratic residue, 5 is a quadratic residue and 6 is a quadratic non residue.

Theorem 4.1 *Let us consider the following three sets of structures with* $L \geq 2$

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0)$$

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1)$$

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0)$$

Where

$$L_1 + L_2 + \cdots + L_m = L$$

$$L_1K_1 + L_2K_2 + \cdots + L_mK_m = t$$

Now, consider a sequence of quadratic and nonquadratic residues in the set $\{1, 2, \ldots, t\}$*. Then for all prime* $p > t$ *of the form* $4N + 1$ *(*$4N + 3$*) with this sequence, there exist three polynomials* $Q_0(p)$*,* $Q_1(p)$ *and* $Q_2(p)$ *of rational coefficients such that,*

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C0) = Q_0(p)$$

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/C1) = Q_1(p)$$

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m/0) = Q_2(p)$$

Proof. It is an immediate consequence of the successive application of the formulae in theorem 3.1 (note that in each application L decrease in 1) and of the formulae in Theorem 2.2. The theorem is proved.

The proof of theorem 4.1 give us a building method to obtain the polynomials $Q_0(p)$, $Q_1(p)$ and $Q_2(p)$. In the next section we give an example.

5 Building Method. An Example.

Consider $t = 3$ and the sequence: 1 quadratic residue, 2 quadratic residue, 3 quadratic nonresidue. Suppose that $p > t$ (of the form 4N+3) has this sequence. We shall determine the polynomials that correspond to the following three sets of structures with $L = 3$.

$$(3, 1/C0) \qquad (3, 1/C1) \qquad (3, 1/0)$$

Since $K_1 = 1$ is a quadratic residue we apply the formulae (7), (8) and (9). Therefore

$$\begin{aligned}(3, 1/C0) &= \frac{1}{3}\left[\left(\frac{p-3}{4}\right)(2, 1/C0) + \left(\frac{p-3}{4}\right)(2, 1/C1) + (2, 1/0)\right. \\ &- \left.(1, 2 : 1, 1/C0)\right]\end{aligned} \tag{13}$$

$$\begin{aligned}(3, 1/C1) &= \frac{1}{3}\left[\left(\frac{p+1}{4}\right)(2, 1/C0) + \left(\frac{p-3}{4}\right)(2, 1/C1)\right. \\ &- \left.(1, 2 : 1, 1/C1)\right]\end{aligned} \tag{14}$$

$$(3, 1/0) = \frac{1}{3}\left[\left(\frac{p-1}{2}\right)(2, 1/C1) - (1, 2 : 1, 1/0)\right] \tag{15}$$

Note that the sets of structures in the right hand of (13), (14) and (15) have $L = 2$ (see Remark 3.2).

Since $K_1 = 1$ is a quadratic residue we apply the formulae (7), (8) and (9) and Theorem 2.2. Therefore we obtain.

$$\begin{aligned}(2, 1/C0) &= \frac{1}{2}\left[\left(\frac{p-3}{4}\right)(1, 1/C0) + \left(\frac{p-3}{4}\right)(1, 1/C1)\right. \\ &+ \left.(1, 1/0) - (1, 2/C0)\right] = \frac{p-7}{8}\end{aligned} \tag{16}$$

$$\begin{aligned}(2, 1/C1) &= \frac{1}{2}\left[\left(\frac{p+1}{4}\right)(1, 1/C0) + \left(\frac{p-3}{4}\right)(1, 1/C1)\right. \\ &- \left.(1, 2/C1)\right] = \frac{p+1}{8}\end{aligned} \tag{17}$$

$$(2, 1/0) = \frac{1}{2}\left[\left(\frac{p-1}{2}\right)(1, 1/C1) - (1, 2/0)\right] = 0 \tag{18}$$

Since $K_1 = 2$ is a quadratic residue we apply the formulae (7), (8) and (9) and Theorem 2.2. Therefore we obtain.

$$\begin{aligned}(1,2:1,1/C0) &= \left[\binom{\frac{p-3}{4}}{}(1,1/C0)+\binom{\frac{p-3}{4}}{}(1,1/C1)\right.\\ &+ \left.(1,1/0)-(1,3/C0)\right]=\frac{p-3}{4} \qquad (19)\end{aligned}$$

$$\begin{aligned}(1,2:1,1/C1) &= \left[\binom{\frac{p+1}{4}}{}(1,1/C0)+\binom{\frac{p-3}{4}}{}(1,1/C1)\right.\\ &- \left.(1,3/C1)\right]=\frac{p-3}{4} \qquad (20)\end{aligned}$$

$$(1,2:1,1/0)=\left[\binom{\frac{p-1}{2}}{}(1,1/C1)-(1,3/0)\right]=0 \qquad (21)$$

Note that the sets of structures in the right hand of (16), (17), (18), (19), (20) and (21) have $L=1$ (see Remark 3.2). That is, they are basic sets of structures.

Finally, substituting (16), (17), (18), (19), (20) and (21) into (13), (14) and (15) we obtain the wished polynomials.

$$(3,1/C0)=\frac{p^2-10p+21}{48} \qquad (3,1/C1)=\frac{p^2-8p+7}{48} \qquad (3,1/0)=\frac{p^2-1}{48}$$

For example if $p=7$ we have

$$(3,1/C0)=0 \qquad (3,1/C1)=0 \qquad (3,1/0)=1$$

Since in this case there is an unique sum of 3 distinct quadratic residues. Namely

$$1+4+2=0$$

Remark 5.1 *Note that we have the following equality*

$$\begin{aligned}&\binom{\frac{p-1}{2}}{}(3,1/C0)+\binom{\frac{p-1}{2}}{}(3,1/C1)+(3,1/0)\\ &=\binom{\frac{p-1}{2}}{3}=\frac{\frac{p-1}{2}\left(\frac{p-1}{2}-1\right)\left(\frac{p-1}{2}-2\right)}{3!}\end{aligned}$$

ACKNOWLEDGEMENTS. The author is very grateful to Universidad Nacional de Luján.

References

[1] R. Jakimczuk, The quadratic equation in Fp and the quadratic reciprocity law, *International Journal of Contemporary Mathematical Sciences,* **4** (2009), 419 - 431.

Received: August, 2010