Advances in Theoretical and Applied Mathematics.
ISSN 0973-4554 Volume 2 Number 1 (2007), pp. 77-82

http://www.ripublication.com/atam.htm

Counting the Number of Pythagorean Triples in Finite Fields[1]

Gökhan Soydan and Musa Demirci
Department of Mathematics, Uludağ University,
16059 Bursa, Turkey
E-mail: gsoydan@uludag.edu.tr, mdemirci@uludag.edu.tr

Nazlı Yıldız Ikikardeş
Department of Mathematics, Balıkesir University,
10100 Balıkesir, Turkey
E-mail: nyildiz@balikesir.edu.tr

Ismail Naci Cangül
Department of Mathematics, Uludağ University,
16059 Bursa, Turkey
E-mail: cangul@uludag.edu.tr

Abstract

It is well-known that the set of quadratic residues modulo prime p forms a multiplicative group. Apart from special cases there is no result concerning the sum of two quadratic residues. Here the authors consider these sums. Formulae for the total number of quadratic residues which can be stated as the sum of two quadratic residues are obtained. These formulae have been used to obtain the integer triples satisfying the Pythagorean equation in prime modes.

AMS Subject Classification: 11G20, 14G05.
Keywords: Elliptic curves over finite fields, rational points, Schur triples.

1. Introduction

In [5] the conditions on x, y and z for Pythagorean triples (x, y, z) where x, y, z are considered in small modes are determined. In [6], the number of Pythagorean triples in $\mathbb{Z}_p$ is determined as a result of the study concerning monochromatic solutions of

equations in groups. In [9], considering [10], the number of monochromatic Schur triples modulo n is given.

In the study of rational points on elliptic curves $y^2 \equiv x^3 + a^3$ over finite fields $\mathbb{Z}_p$, the authors encountered the problem of determining whether or not the sum of two quadratic residues is a quadratic residue, see [8]. In [7], they answered this question together with the questions about the sum of two quadratic non-residues and the sum of a quadratic residue with a non-residue. Here we use the former problem to determine the total number of Pythagorean triples (x, y, z) over finite fields. Here we have given results concerning this number by a different approach, which uses quadratic residues, than Datskovsky had.

First we give some results about the additive structure of Q_p, the set of quadratic residues modulo p, and secondly use all these results to determine the above number. Also by $Q_p^{'}$, we denote the set of quadratic non-residues modulo p.

2. The Additive Structure of Q_p

Now we discuss under what conditions the sum of two quadratic residues is again a quadratic residue. First we need the following well-known result.

Lemma 2.1. Let p be an odd prime. Then $-1 \in Q_p$ iff $p \equiv 1 (\mathrm{mod}\, 4)$.

Remark 2.2. Lemma 1 implies that "$-1 \in Q_p'$ iff $p \equiv 3 (\mathrm{mod}\, 4)$". Also when $p \equiv 1 (\mathrm{mod}\, 4)$, both x and $p - x$ are Q_p or Q_p'.

Let now $x, y \in Q_p$. We want to determine the values $x + y$ lying in Q_p and those in Q_p'.

Let, first, $p \equiv 1 (\mathrm{mod}\, 4)$ be prime. Then by Remark 2, $t \in Q_p$ iff $p - t \in Q_p$. This means that all entries at the second diagonal of the table consisting of the values of $x + y$ are equal to 0. See the tables below for $p = 5$ and 13:

$x \diagdown y$	1	4
1	2	0
4	0	3

Table I

$x \diagdown y$	1	3	4	9	10	12
1	2	4	5	10	11	0
3	4	6	7	12	0	2
4	5	7	8	0	1	3
9	10	12	0	5	6	8
10	11	0	1	6	7	9
12	0	2	3	8	9	11

Table II

We know that $1 \in Q_p$ for all primes. Taking $y = 1$, we can determine the values $x+1$ and place them into the first column of the table. As there are $\frac{p-1}{2}$ values at each column, $\frac{p-1}{2} - 1 = \frac{p-3}{2}$ values are non-zero. By [4], we know that the number of pairs of consecutive quadratic residues modulo p is given by the formula

$$n_p = \frac{1}{4}\left(p - 4 - (-1)^{\frac{p-1}{2}}\right)$$

and this becomes

$$n_p = \frac{p-5}{4}$$

considering the fact that $p \equiv 1 (\mathrm{mod}\, 4)$. This means that there are $\frac{p-5}{4}$ values of $x+1$'s lying in Q_p for the values of x in Q_p. Each column has equal number of elements in Q_p. Therefore the number of non-zero non-residues at each column is

$$\frac{p-3}{2} - n_p = \frac{p-1}{4}$$

Theorem 2.3. Let $p \equiv 1 (\mathrm{mod}\, 4)$ be prime. If x and $y \in Q_p$ are any elements, then out of $\left(\frac{p-1}{2}\right)^2$ values of $x+y$ in whole table, there are $\frac{p-1}{2}$ zeroes, $\frac{p-1}{2}.\frac{p-5}{4}$ values lying in Q_p and $\frac{p-1}{2}.\frac{p-1}{4}$ values in Q'_p.

Proof. Note that the total number of non-zero elements in the whole table is

$$\left(\frac{p-1}{2}\right)^2 - \frac{p-1}{2} = \frac{p-1}{2}.\frac{p-3}{2}$$

As above, there are $\frac{p-5}{4}$ values at each column lying in Q_p, and as there are $\frac{p-1}{2}$ columns at all, the total number of the values of $x+y$ lying in Q_p is $\frac{p-1}{2}.\frac{p-5}{4}$. Similarly, we find the total number of quadratic non-residues. ■

Let, secondly, $p \equiv 3(\mathrm{mod}\,4)$ be prime. By Remark 2, only one of t and $p-t$, for each t, lies in Q_p. Therefore, we are adding two elements of Q_p, we never get zeroes in the table. So each entry in the table is a quadratic residue or non-residue.

$n_p = \dfrac{p-3}{4}$ is the number of quadratic residues at each column and hence we obtain the following result. We omit the proof which is similar to Theorem 2.4.

Theorem 2.4. Let $p \equiv 3(\mathrm{mod}\,4)$ be prime. If x and $y \in Q_p$ are any elements, then there are $\dfrac{p-1}{2}.\dfrac{p-3}{4}$ values in Q_p and $\dfrac{p-1}{2}.\dfrac{p+1}{4}$ values in Q'_p.

Hence we have

Theorem 2.5. If only one of x and y belongs to Q_p i.e. if $\left(\dfrac{xy}{p}\right) = -1$ where $\left(\dfrac{\cdot}{\cdot}\right)$ denotes the Legendre symbol, then $x+y$ could never take the value 0.

Let us now suppose that x varies on Q'_p and $y \in Q_p$ be fixed. The case where y varies on Q'_p and $x \in Q_p$ is fixed is treated similarly as the addition on $\mathbb{F}_p$ is abelian. As every column (and row) has the same number of quadratic residues (and non-residues), we can consider the column consisting of the entries $x+1$ (taking $y = 1 \in Q_p$) for all possible $x \in Q'_p$. As the number of pairs of consecutive elements where the first is a non-residue and second is a residue is given by

$$n_p = \frac{1}{4}\left(p - 2 + (-1)^{\frac{p-1}{2}}\right)$$

by [4]. This can be reduced to

$$n_p = \frac{p-1}{4}$$

using the fact that $p \equiv 1(\mathrm{mod}\,4)$.

Then the remaning $\dfrac{p-1}{4}$ entries are quadratic non-residues.

If $p \equiv 1(\mathrm{mod}\,4)$, then by Remark 2, either both or none of t and $p-t$ are in Q_p. Therefore the table of the values $x+y$ contains $\dfrac{p-1}{2}$ entries equal to 0.

3. The Number of Pythagorean Triples in Modulo Prime p

Now we will formulate the total number of Pythagorean triples (x, y, z) in modulo p.

Theorem 3.1. Let p be prime and let N_p denote the number of Pythagorean triples (x, y, z) in modulo p where $x.y.z \neq 0$. Then

$$p \equiv 1(\mathrm{mod}\,4) \text{ iff } N_p = (p-1).(p-5)$$

and

$$p \equiv 3(\mathrm{mod}\,4) \text{ iff } N_p = (p-1).(p-3).$$

Proof. We know that, as x^2 and y^2 lie in Q_p, if $p \equiv 1(\text{mod}\,4)$ is prime, then the total number of values of $x^2 + y^2$ lying in Q_p is $\frac{p-1}{2}.\frac{p-5}{4}$ and if $p \equiv 3(\text{mod}\,4)$ is prime then the total number of values of $x^2 + y^2$ lying in Q_p is $\frac{p-1}{2}.\frac{p-3}{4}$. As for a Pythagorean triple (x, y, z) satisfying the relation $x^2 + y^2 = z^2$, all the triples $(\mp x, \mp y, \mp z)$ will also be solutions, implying $N_p = 8.(\frac{p-1}{2}.\frac{p-5}{4}) = (p-1).(p-5)$ and $N_p = 8.(\frac{p-1}{2}.\frac{p-3}{4}) = (p-1).(p-3)$, respectively.

Example 3.2. Let first $p = 5$. By the former formula in Theorem 7, there are no triples in mod 5. Let secondly $p = 7$. Then we get 24 Pythagorean triples by the latter formula $N_p = (p-1).(p-3)$. As $Q_7 = \{1, 2, 4\}$, $1+1 \equiv 2$, $1+2 \equiv 3$, $1+4 \equiv 5$, $2+1 \equiv 3$, $2+2 \equiv 4$, $2+4 \equiv 6$, $4+1 \equiv 5$, $4+2 \equiv 6$, $4+4 \equiv 1$ (mod 7). When the sums are equal 1, 2 or 4, we get the required x^2 and y^2's. Then $x^2 \equiv y^2 \equiv 1$ (mod 7) implying that $x \equiv 1$ or 6, $y \equiv 1$ or 6 (mod 7) and hence we get $z \equiv 3$ or 4 (mod 7). Also $x^2 \equiv y^2 \equiv 2$ (mod 7) implies $x \equiv 3$ or 4, $y \equiv 3$ or 4 (mod 7) and hence we get $z \equiv 2$ or 5 (mod 7). Finally $x^2 \equiv y^2 \equiv 4$ (mod 7) implies that $x \equiv 2$ or 5, $y \equiv 2$ or 5 (mod 7) and therefore we get $z \equiv 1$ or 6 (mod 7). Finally, in modulo 7, Pythagorean triples (x, y, z) are (1, 1, 3), (1, 1, 4), (1, 6, 3), (1, 6, 4), (6, 1, 3), (6, 1, 4), (6, 6, 3), (6, 6, 4), (3, 3, 2), (3, 3, 5), (3, 4, 2), (3, 4, 5), (4, 3, 2), (4, 3, 5), (4, 4, 2), (4, 4, 5), (2, 5, 1), (2, 5, 6), (2, 2, 1), (2, 2, 6), (5, 2, 1), (5, 2, 6), (5, 5, 6), (5, 5, 1).

References

[1] G.A. Jones and J.M. Jones. Elementary Number Theory, Springer-Verlag, (1998), ISBN 3-540-76197-7.

[2] J. Esmonde and M.R. Murty. Problems in Algebraic Number Theory, Springer-Verlag, (1999), ISBN 0-387-98617-0.

[3] A.H. Beiler. Recreations in the Theory of Numbers, Dover Publications, (1966), ISBN 0-486-210960.

[4] G.E. Andrews. Number Theory, Dover Publications, (1971), ISBN 0-486-68252-8.

[5] J.E. Schultz and W.F. Burger. An Approach to Problem Solving Using Equivalence Classes Modulo n, *The College Mathematics Journal*, 15(5):401–405, 1994.

[6] P.J. Cameron, J. Cillervelo, and O. Serra. On Monochromatic Solutions of Equations in Groups, Revista Matematica Iberoamericana, Preprint.

[7] G. Soydan, N.Y. İkikardeş, M. Demirci, and İ.N. Cangül. On the additive structure of the set of quadratic residues modulo p, *Advanced Studies in Contemporary Math.*, 14(2):251–257, 2007.

[8] M. Demirci, G. Soydan, İ.N. Cangül. Rational points on elliptic curves $y^2 = x^3 + a^3$ in $F_p$where $p \equiv 1 (\mathrm{mod}\, 6)$ is prime, *Rocky Mountain Journal of Math.*, Preprint 2007.

[9] B.A. Datskovsky. On the number of monochromatic schur triples, *Advances in Applied Mathematics*, 31:193–198, 2003.

[10] I. Schur. Über die Kongruenz $x^m + y^m \equiv z^m (\mathrm{mod}\ p)$, *Jahresber. Deutsche Math. -Verein.*, 25:114–116, 1916.