On monochromatic solutions of equations in groups

Peter J. Cameron* Javier Cilleruelo† Oriol Serra‡

Abstract

We show that the number of monochromatic solutions of the equation $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r} = g$ in a 2-coloring of a finite group G, where $\alpha_1,\ldots,\alpha_r$ are permutations and $g \in G$, depends only on the cardinalities of the chromatic classes but not on their distribution. We give some applications to arithmetic Ramsey statements.

1 Introduction

A well-known theorem of Schur establishes that, for $n \geq n_0(k)$ and every coloring of the integers in $[1,n]$ with a finite number k of colors, there is a monochromatic triple (x,y,z) satisfying $x+y=z$. Graham, Rödl and Ruczinsky [3] proved that the number $S(n)$ of Schur triples in a 2-coloring of $[1,n]$ verifies $S(n) \geq n^2/38 + O(n)$ and enquired about the value of the limit $S(n)/n^2$ as $n \to \infty$. The answer $S(n) = n^2/22 + O(n)$ was given in three independent papers by Robertson and Zeilberger [5], Schoen [4] and Datskovsky [1].

In the last reference, Datskovsky also shows the somewhat surprising fact that the number of Schur triples in a 2-coloring of $\mathbb{Z}/n\mathbb{Z}$ depends only on the cardinalities of the color classes (and not on the distribution of the colors.) The purpose of this note is to show that such phenomenon occurs in a broader combinatorial setting which can be applied to other Ramsey arithmetical statements.

Our main theorem is a result about 2-colorings of orthogonal arrays, stated and proved in the next section of the paper. The result immediately specialises to a statement about finite groups as follows:

Theorem 1.1 *Let G be a finite group, $\alpha_1,\ldots,\alpha_r$ a set of permutations of G and $g \in G$. For any 2-coloring of the elements of G with color classes A and B, let A^* and B^* denote the sets of r-tuples $(x_1,\ldots,x_r)$ satisfying the equation*

$$x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r} = g, \tag{1}$$

*School of Mathematical Sciences Queen Mary, University of London, UK

†Dept. de Matemáticas, Facultat de Ciencias, Universidad Autónoma de Madrid, Spain

‡Dept. Matemàtica Aplicada IV, Univ. Politècnica de Catalunya, Barcelona, Spain

with all elements in A and B respectively. Then,

$$|A^*| + (-1)^{r+1}|B^*| = \frac{1}{|G|}(|A|^r + (-1)^{r+1}|B|^r).$$

Note that this theorem can be specialised to the equation

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r = g$$

in an abelian group G, where $\alpha_1, \ldots, \alpha_r$ are integers coprime to the order of G.

We present applications of this result in three areas: monochromatic arithmetic progressions, monochromatic Schur triples, and Pythagorean triples. These are discussed in the following three sections of the paper.

2 The main theorem for orthogonal arrays and groups

A set S of r-vectors with entries in a finite set X is an *orthogonal array* of degree r, strength k and index λ if, for any choice of k columns, each k-vector of X^k appears exactly in λ vectors of S.

Theorem 2.1 *Let S an orthogonal array of strength k and index λ. Given a 2-coloring of X with color classes A and B, let u_i denote the number of r-vectors in S with exactly i elements in A. Then*

$$\sum_{j=0}^{k} \binom{r}{j} (-1)^j n^{r-j} |A|^j = \lambda(u_0 + \sum_{i=k+1}^{r} (-1)^k \binom{i-1}{k} u_i).$$

Proof Let f be a function assigning to each subset $J \subset \{1, \ldots, r\}$ of cardinality at most k a subset $f(J)$ such that $J \cap f(J) = \emptyset$ and $|J| + |f(J)| = k$.

For each subset $J \subset \{1, \ldots, r\}$ of cardinality $j \leq k$, choose an arbitrary j-vector $(x_i, i \in J) \in A^j$ and an arbitrary $(k-j)$-vector $(x_i, i \in f(J)) \in X^{k-j}$. Since S is an orthogonal array with strength k and index λ, each such choice determines exactly λ r-vectors of S. In the multiset of the obtained vectors from S, each vector with exactly i entries from A is counted $\lambda\binom{i}{j}$ times (where $\binom{i}{j} = 0$ if $0 < j < i$ and $\binom{0}{0} = 1$.) Therefore, we get the following linear system in the variables u_i:

$$\binom{r}{j} n^{k-j} |A|^j = \lambda \sum_{i=0}^{r} \binom{i}{j} u_i, \ j = 0, 1, \ldots, k. \tag{2}$$

The alternating sum of the equations in (2) gives

$$\begin{aligned}\sum_{j=0}^{k}\binom{r}{j}(-1)^j n^{k-j}|A|^j &= \sum_{j=0}^{k}(-1)^j\lambda\sum_{i=0}^{r}\binom{i}{j}u_i \\ &= \lambda\sum_{i=0}^{r}u_i\sum_{j=0}^{k}(-1)^j\binom{i}{j} \\ &= \lambda(u_0+\sum_{i=k+1}^{r}(-1)^k\binom{i-1}{k}u_i),\end{aligned}$$

as claimed. □

Theorem 1.1 is a direct consequence of Theorem 2.1, as the set S of solutions of the equation

$$x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r}=g,$$

forms an orthogonal array of degree r, strength $k=r-1$ and index $\lambda=1$ with entries in G.

3 Schur triples

In a group G, a *Schur triple* is a triple (x,y,z) of group elements satisfying $xy=z$. More generally, a *Schur r-tuple* has the form $(x_1,\ldots,x_{r-1},z)$, where $x_1\cdots x_{r-1}=z$.

Corollary 3.1 *Let G be a finite group. For any 2-coloring of the elements of G with color classes A and B, the number of Schur triples (x,y,z) is*

$$|A|^2-|A|\cdot|B|+|B|^2.$$

In particular, there are at least $n^2/4$ monochromatic Schur triples in any 2-coloring of G.

Proof This is immediate from our main theorem, on taking α_1 and α_2 to be the identity permutation, α_3 to be inversion, and $g=1$. The last sentence follows because the function $x^2-x(n-x)+(n-x)^2=3x^2-3nx+n^2$ has its minimum value when $x=n/2$. □

Almost exactly the same proof gives the following result:

Corollary 3.2 (Datskovsky [1] Corollary 1) *Let $S_r(A,B,n)$ denote the number of monochromatic Schur r-tuples in a 2-coloring of $\mathbb{Z}/n\mathbb{Z}$ with color classes A and B. Then, for r odd,*

$$S_r(A,B,n)=\frac{1}{n}(|A|^r+|B|^r).$$

Our proof is purely combinatorial. A proof can be also obtained by using trigonometric sums as in [1].

4 Arithmetic progressions

An *arithmetic progression* in a group G is a set of elements of the form $\{a, ad, ad^2, \ldots, ad^{k-1}\}$. It is *degenerate* if $d = 1$ and *non-degenerate* otherwise.

If the order of G contains no prime factors smaller than k, then the elements of a non-degenerate arithmetic progression are all distinct. If it contains no prime factors smaller than $2k-1$, then such a progression determines a and d up to just two possibilities, the other being obtained by reading the progression backwards. For if the first two terms are taken to be ad^i and ad^j, with $\{i, j\} \neq \{0, 1\}$ and $\{i, j\} \neq \{n, n-1\}$, then some member of the progression will have the form ad^l where l is outside the range $[0, k-1]$ but in the range $[-(k-1), 2k-2]$; but no such element can belong to the interval $[0, k-1]$ if the order of d is at least $2k-1$.

Corollary 4.1 *In any 2-coloring of a group of order coprime to 6, the number of monochromatic 3-term arithmetic progressions with no repeated elements is*

$$\frac{1}{2}(|A|^2 - |A| \cdot |B| + |B|^2 - n),$$

where A and B are the color classes. In particular, there are at least $\frac{1}{8}n^2 - \frac{1}{2}n$ such triples.

Proof The set of 3-term arithmetic progressions in a group G of odd order forms an orthogonal array of degree 3, strength 2 and index 1. (To show that a and ad^2 determine d, use the fact that every element of such a group has a unique square root.) We remark that if G is abelian, then this set can be expressed as in our main theorem, but in the non-abelian case the more general result about orthogonal arrays seems to be needed.

Now as in the proof of Corollary 3.1, there are $|A|^2 - |A| \cdot |B| + |B|^2$ monochromatic ordered arithmetic progressions of length 3; we have to subtract n (the number of degenerate progressions) and divide by 2 (for the possible orderings of the progression), since the smallest prime divisor of G is at least 5 by assumption. □

The extension to 3-colorings is a little more complicated. We first show the following extension of the main theorem.

Theorem 4.2 *Let G be a finite group, $\alpha_1, \alpha_2, \alpha_3$ permutations of G and $g \in G$. For any 3-coloring of the elements of G with color classes A_1, A_2 and A_3, let M (Monochromatic) and R (Rainbow) denote the sets of 3-tuples (x_1, x_2, x_3) satisfying the equation*

$$x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} = g, \tag{3}$$

with all elements in the same color, and the three different colors respectively. Then,

$$|M| = \frac{1}{2}\left(3(|A_1|^2 + |A_2|^2 + |A_3|^2) - |G|^2 + |R|\right).$$

Proof Consider the 2-coloring $G = (A_i \cup A_j) \cup A_k$. Then

$$|(A_i \cup A_j)^*| + |A_k^*| = (|A_i| + |A_j|)^2 - (|A_i| + |A_j|)|A_k| + |A_k|^2. \quad (4)$$

We can write $|(A_i \cup A_j)^*| = |A_i^*| + |A_j^*| + |\{\text{3-tuples using the two colors } A_i \text{ and } A_j\}|$. We write the last term X_{ij} for short. Then

$$|M| = (|A_i| + |A_j|)^2 - (|A_i| + |A_j|)|A_k| + |A_k|^2 - |X_{ij}| \quad (5)$$

Adding this identity for $(i, j, k) = (1, 2, 3), (i, j, k)$ and $(2, 3, 1)$ we have

$$3|M| = 3(|A_1|^2 + |A_2|^2 + |A_3|^2) - |X_{12}| - |X_{13}| - |X_{23}| \quad (6)$$

On the other hand it is clear that

$$|G|^2 = |M| + |X_{12}| + |X_{13}| + |X_{23}| + |R|. \quad (7)$$

Putting this in the formula above we obtain the theorem. □

Corollary 4.3 *Any* 3*-coloring of a group of order* n *whose smallest prime divisor is at least* 17 *has at least* $\frac{n^2+15n+32}{48}$ *monochromatic arithmetic progressions of length* 3*.*

Proof We look at 9-term arithmetic progressions in the group, noting that, by our assumption, each unordered progression can be ordered in just two ways (the reverses of each other).

In the table below we have marked in bold a monochromatic or rainbow arithmetic progression in each 3-coloring of the 9-tuples. This proves that any 3-coloring of any 9-tuple contains a non-degenerate arithmetic progression of length 3 belonging to M or R.

But the number of non-degenerate 9-tuples is $n^2 - n$ and the number of non-degenerate 3-tuples contained in a 9-tuple is exactly 16 (corresponding to positions $(1, 2, 3), \ldots, (7, 8, 9), (1, 3, 5), \ldots, (5, 7, 9), (1, 4, 7), \ldots, (3, 6, 9)$, and $(1, 5, 9)$). Then $|M| + |R| \geq \frac{p^2-p}{16} + p$, where the last p counts the degenerate progressions. We obtain the result adding the two inequalities. □

1 1 1 ∗ ∗ ∗ ∗ ∗ ∗ 1 1 **2 2 1** 2 2 **1** ∗ 1 2 1 2 2 **1 1 1** ∗ 1 2 2 1 **2 1 3** ∗ ∗
1 1 2 **1 1 1** ∗ ∗ ∗ 1 1 2 2 1 **2 2 2** ∗ 1 **2** 1 2 **2** 1 1 **2** ∗ **1** 2 2 1 2 2 **1** ∗ ∗
1 1 2 **1** 1 2 **1** ∗ ∗ 1 1 2 2 1 2 **3 1** 1 2 1 **2** 2 **1** 1 **3** ∗ 1 2 2 1 **2 2 2** ∗ ∗
1 **1** 2 1 **1** 2 2 **1** ∗ 1 1 **2** 2 1 **2** 2 3 **2** 1 2 **1** 2 2 **1** 2 1 **1** 1 2 2 1 2 **3 1** ∗
1 1 2 1 1 **2 2 2** ∗ 1 1 2 2 **1** 2 **2** 3 **3** 1 2 1 2 **2** 1 **2** 1 **2** 1 **2** 2 **2** 3 **2** ∗
1 1 2 **1** 1 **2** 2 **3** ∗ 1 1 2 2 **1 2 3** ∗ ∗ 1 2 1 2 2 1 **2 1 3** 1 2 2 **1** 2 2 3 **3** ∗
1 1 2 1 **1 2 3** ∗ ∗ 1 1 2 **2 1 3** ∗ ∗∗ 1 **2** 1 2 **2** 1 2 **2** ∗ 1 2 2 **1 2 3** ∗ ∗ ∗
1 1 2 **1** 1 3 **1** ∗ ∗ 1 1 **2 2 2** ∗ ∗ ∗ ∗ 1 2 1 2 2 **1 2 3** ∗ 1 2 **2 1 3** ∗ ∗ ∗ ∗
1 1 2 1 **1 3 2** ∗ ∗ **1** 1 **2** 2 **3** ∗ ∗ ∗ ∗ 1 2 1 2 **2 1 3** ∗ ∗ 1 **2 2 2** ∗ ∗ ∗ ∗ ∗
1 1 **2** 1 **1** 3 **3** ∗ ∗ 1 **1 2 3** ∗ ∗ ∗ ∗∗ 1 2 1 **2 2 2** ∗ ∗ ∗ 1 2 **2 3 1** ∗ ∗ ∗ ∗
1 **1** 2 **1** 2 **1** ∗ ∗ ∗ 1 2 **1 1 1** ∗ ∗ ∗ ∗ 1 2 1 2 **2 3 1** ∗ ∗ 1 2 2 **3 2 1** ∗ ∗ ∗
1 1 2 **1** 2 2 **1** ∗ ∗ **1** 2 1 1 2 1 **1** ∗ ∗ 1 2 1 2 2 **3 2 1** ∗ 1 2 2 **3** 2 **2** 1 **1** ∗
1 1 2 1 **2 2 2** ∗ ∗ 1 2 1 **1** 2 **1** 2 **1** ∗ 1 2 **1** 2 2 **3** 2 **2** ∗ 1 **2** 2 3 **2** 2 1 **2** ∗
1 1 2 1 2 **2 3 1** ∗ 1 **2** 1 1 **2** 1 2 **2** ∗ 1 2 1 2 2 3 **2 3 1** 1 2 2 3 2 **2 1 3** ∗
1 1 2 1 2 2 **3 2 1** 1 2 1 1 2 **1 2 3** ∗ 1 2 1 2 **2** 3 **2** 3 **2** 1 2 2 3 **2 2 2** ∗ ∗
1 1 **2** 1 2 **2** 3 2 **2** 1 2 1 1 **2 1 3** ∗ ∗ 1 2 1 **2** 2 3 2 3 **3** 1 2 2 3 2 **2 3 1** ∗
1 1 2 1 **2** 2 3 2 **3** **1** 2 1 1 2 2 **1** ∗ ∗ 1 2 **1** 2 **2** 3 **3** ∗ ∗ 1 **2** 2 3 **2** 2 3 **2** ∗
1 1 2 **1** 2 **2** 3 **3** ∗ 1 2 1 1 **2 2 2** ∗ ∗ 1 2 **1 2 3** ∗ ∗ ∗ ∗ 1 2 2 3 **2 2** 3 3 **1**
1 1 2 **1 2 3** ∗ ∗ ∗ 1 2 **1** 1 2 2 **3** ∗ ∗ 1 **2 1 3** ∗ ∗ ∗ ∗ ∗ 1 2 **2** 3 2 **2** 3 3 **2**
1 1 **2 1 3** ∗ ∗ ∗ ∗ 1 2 1 **1 2 3** ∗ ∗ ∗ 1 2 2 **1 1 1** ∗ ∗ ∗ 1 2 2 3 2 2 **3 3 3**
1 1 2 2 **1 1 1** ∗ ∗ **1** 2 1 1 3 1 **1** ∗ ∗ **1** 2 2 1 1 2 **1** ∗ ∗ 1 2 2 3 **2 3 1** ∗ ∗
1 **1** 2 2 1 1 2 **1** ∗ 1 2 1 1 **3 1 2** ∗ ∗ **1** 2 2 1 1 2 2 1 **1** 1 **2** 2 3 **2** 3 **2** ∗ ∗
1 1 2 2 **1** 1 2 2 **1** 1 2 1 1 3 **1** 3 1 ∗ 1 2 **2** 1 1 **2** 2 1 **2** 1 2 **3** 2 **3** 3 1 **1**
1 1 2 2 1 1 **2 2 2** 1 2 1 1 3 **1 3 2** ∗ 1 2 2 1 1 2 **2 1 3** 1 2 2 3 2 3 **3 1 2**
1 1 2 2 **1** 1 **2** 2 **3** 1 2 **1** 1 3 **1** 3 3 **1** 1 2 2 1 1 **2 2 2** ∗ **1** 2 2 3 **2** 3 3 1 **3**
1 1 2 2 1 **1 2 3** ∗ **1** 2 1 1 **3** 1 3 3 **2** 1 2 2 **1** 1 **2** 2 **3** ∗ 1 **2** 2 3 **2** 3 3 **2** ∗
1 1 **2** 2 **1** 1 **3** ∗ ∗ 1 2 1 1 3 1 **3 3 3** 1 2 2 1 **1 2 3** ∗ ∗ 1 2 2 3 2 **3 3 3** ∗
1 **1** 2 2 1 2 1 **1** ∗ 1 2 1 **1 3 2** ∗ ∗ ∗ 1 **2** 2 1 1 **3** ∗ ∗ ∗ **1** 2 **2** 3 **3** ∗ ∗ ∗ ∗
1 1 2 **2** 1 **2** 1 **2** ∗ 1 **2** 1 1 **3 3** ∗ ∗ ∗ **1** 2 2 1 2 1 **1** ∗ ∗ **1 2 3** ∗ ∗ ∗ ∗ ∗ ∗
1 1 2 2 1 **2 1 3** ∗ **1** 2 **1** 2 **1** ∗ ∗ ∗ ∗ 1 2 **2** 1 **2** 1 **2** ∗ ∗

Remark The result of this theorem can be improved. For example, a similar table shows that, in any 3-colored 11-term arithmetic progression, we can find at least two 3-term arithmetic progressions which are either monochromatic or rainbow. This improves the factor 1/16 in the proof to 2/25, and 1/48 in the result of the theorem to 2/75.

Computation using GAP [2] shows that this can be further improved. The best fraction we found to replace the constant 1/16 was 7/60, which is demonstrated by the fact that any 3-colored 28-term arithmetic progression contains at least 32 monochromatic or rainbow 3-term progressions.

Of course, these improvements require further restrictions on the group: in the last case, we have to assume that the smallest prime divisor of the

group order is at least 59.

This suggests the combinatorial problem:

> *What can be said about the function $f(n)$, the least number m such that any 3-coloured m-term arithmetic progression contains at least n monochromatic or rainbow 3-term progressions?*

For 4-term arithmetic progressions we have the following result:

Theorem 4.4 *Any 4-coloring of a group of order n whose smallest prime divisor is at least 13 has at least $\frac{n^2-16n+15}{40}$ monochromatic arithmetic progressions of length 4.*

Proof The set of four-term arithmetic progressions in G (including the degenerate ones (a, ad, ad^2, ad^3) with $d = 1$) forms an orthogonal array of degree $r = 4$, strength $k = 2$ and index $\lambda = 1$ of 4-tuples, since any element of G has a unique square root or cube root. By Theorem 2.1 we have

$$n^2 - 4n|A| + 6|A|^2 = u_0 + u_3 + 3u_4, \tag{8}$$

where, as in Theorem 2.1, A is one of the color classes and u_i is the number of solutions with exactly i elements from A. By exchanging the role of A and B we get

$$n^2 - 4n|B| + 6|B|^2 = u_4 + u_1 + 3u_0. \tag{9}$$

By adding (8) and (9) we have

$$6(|A|^2 + |B|^2) - 2n^2 = 4(u_0 + u_4) + (u_1 + u_3). \tag{10}$$

The identity $u_0 + u_1 + u_2 + u_3 + u_4 = n^2$ gives

$$u_0 + u_4 = \frac{u_2}{3} + 2(|A|^2 + |B|^2) - n^2 \geq \frac{u_2}{3} + 1. \tag{11}$$

Let us show that

$$u_0 + u_2 + u_4 \geq \frac{n^2 - n}{5} + n. \tag{12}$$

Note that each arithmetic progression of length 7 contains at least one arithmetic progression counted in $u_0+u_2+u_4$ (see the table below). On the other hand, each 4-term progression is contained in five 7-progressions, those in which it occurs in positions $(1, 2, 3, 4)$, $\ldots$, $(4, 5, 6, 7)$ or $(1, 3, 5, 7)$. Since there are $n(n-1)$ non-degenerate 7-progressions and n degenerate ones, we get inequality (12). Combining (12) and (10) we obtain

$$u_0 + u_4 \geq \frac{n^2 + 4n + 15}{20}.$$

Our assumptions also show that a given 4-set which is an arithmetic progression occurs as such in just two orders, one the reverse of the other. This

gives the lower bound $(n^2-16n+15)/40$ for the number of monochromatic 4-progressions. □

1 1 1 1 $*\,*\,*$	1 **1 1 2 2** $*\,*$	1 **1 2 1 2** $*\,*$	$1\,2\,1$ **1 1 2 2**	$1\,2$ **2 2 1 1** $*$
1 $1\,1\,2$ **1** $1\,1$	$1\,1\,2$ **1 1 1 1**	**1 1 2 2** $*\,*\,*$	1 **2 1 1 2** $*\,*$	$1\,2\,2$ **2 1 2 1**
$1\,1\,1$ **2 1 1 2**	**1 1** $2\,1\,1\,2$	$1\,2$ **1 1 1 1** $*$	**1 2 1 2** $*\,*\,*$	**1** $2\,2\,2\,1\,2$ **2**
$1\,1$ **1 2 1 2** $*$	$1\,1$ **2 1 1 2** $*$	**1** $2\,1\,1\,1\,2$ **1**	**1 2 2 1** $*\,*\,*$	1 **2 2 2 2** $*\,*$

Remark Just as for Theorem 4.2, this can be improved. We found by a similar computation that among progressions of length 33 we can always find at least 40 four-term progressions with the patterns counted by $u_0+u_2+u_4$; this allows us to replace the constant $1/5$ by $8/33$. As before, we can formulate a combinatorial problem here.

5 Pythagorean triples

Corollary 3.1 can be used to count the number of Pythagorean triples in $\mathbb{Z}/p\mathbb{Z}$. A *Pythagorean triple* is any 3-tuple (x^2,y^2,z^2) satisfying $x^2+y^2=z^2$, and is *non-degenerate* if $xyz\neq 0$. For any $r\neq 0$, we define $\epsilon_p(r)=1$ if the equation $x^2\equiv r \pmod p$ has solution and $\epsilon_p(r)=0$ otherwise. Theorem 5.1, Theorem 5.2 and Corollary 5.3 are well known but these proofs are new.

Theorem 5.1 *Let p be an odd prime. The number of Pythagorean triples in $\mathbb{Z}/p\mathbb{Z}$ is*

$$\frac{(p+1)(p+3)}{8}+\epsilon_p(-1)\frac{p-1}{4}$$

and the number of non-degenerate Pythagorean triples in $\mathbb{Z}/p\mathbb{Z}$ is

$$\frac{(p-1)(p-3)}{8}-\epsilon_p(-1)\frac{p-1}{4}.$$

Proof Consider the 2-coloring of $\mathbb{Z}/p\mathbb{Z}$ given by $\mathbb{Z}/p\mathbb{Z}=S\cup N$ with $S=\{x^2 : x\in\mathbb{Z}/p\mathbb{Z}\}$ the set of squares and $N=(\mathbb{Z}/p\mathbb{Z})\setminus S$. Denote by U_i the set of Schur triples with exactly i elements in S, so that U_3 is the set of Pythagorean triples. By Corollary 3.2 we have

$$|U_0|+|U_3|=\left(\frac{p+1}{2}\right)^2-\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)+\left(\frac{p-1}{2}\right)^2=\frac{p^2+3}{4}.$$

Let $U_3'=\{(a,b,c)\in U_3 : abc=0\}$. For r a non quadratic residue modulo p, the map $(a,b,c)\mapsto(ra,rb,rc)$ is a bijection between U_0 and $U_3\setminus U_3'$. Therefore,

$$|U_3|=|U_0|+|U_3'|=\frac{p^2+3}{8}+\frac{|U_3'|}{2}.$$

The triples in U_3' are $(0,0,0)$, $\{(0,x^2,x^2 : x\in S\setminus\{0\}\}$, $\{(x^2,0,x^2 : x\in S\setminus\{0\}\}$ and, if $-1\in S$, $\{(x^2,-x^2,0),\ x\in S\}$, so that $|U_3'|=p+\epsilon(p)(p-1)/2$, which gives the result. □

Of course it is well known for which primes p the equation $x^2 \equiv -1 \pmod{p}$ has a solution, but we want to present it as a consequence of the next result.

Theorem 5.2 *For any $t \neq 0$ let $R_p(t)$ denote the set of the pairs $(x^2, y^2) \in \mathbb{Z}_p \setminus \{0\}$ such that $x^2 + y^2 = t$. Then $|R_p(t)| = \frac{p+1-2\epsilon_p(-1)}{4} - \epsilon_p(t)$.*

Proof There exists an obvious bijection between $R_p(t)$ and $R_p(t')$ if t, t' are quadratic residues or are both non quadratic residues. If t is a quadratic residue we have that

$$|\{(x^2, y^2, z^2),\ x^2+y^2 = z^2,\ xyz \neq 0\}| = \sum_{r \text{ quadratic residue}} |R_p(r)| = |R_p(t)|\frac{p-1}{2}$$

and we obtain the theorem by applying the result obtained in theorem 5.1.

If t is a non quadratic residue we can write

$$\begin{aligned}\left(\frac{p-1}{2}\right)^2 &= \sum_{r \text{ quadratic residue}} |R_p(r)| + \sum_{r \text{ non quadratic residue}} |R_p(r)| + |R_p(0)| \\ &= \frac{(p-1)(p-3)}{8} - \epsilon_p(-1)\frac{p-1}{4} + \frac{p-1}{2}|R_p(t)| + \epsilon_p(-1)\frac{p-1}{2},\end{aligned}$$

and we can compute $|R_p(t)|$. □

Corollary 5.3 *For any odd prime p we have*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{4}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Proof To calculate $\left(\frac{-1}{p}\right)$, observe $|R_p(1)| = \frac{p+1-2\epsilon_p(-1)}{4} - 1$ must be an integer. To calculate $\left(\frac{2}{p}\right)$, notice that $|R_p(2)| = \frac{p+1-2\epsilon_p(-1)}{4} - \epsilon_p(2)$ is always an odd number because $x^2 + y^2 = y^2 + x^2 = 2$ give two solutions except in the case $1 + 1 = 2$. □

Acknowledgement The authors are grateful to M. W. Newman who suggested the possibility of improving Theorems 4.2 and 4.4 along the lines given in the remarks following those theorems.

References

[1] B.A. Datskovsky, On the number of monochromatic Schur triples, *Advances in Applied Mathematics* **31** (2003) 193–198.

[2] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002,
`http://www-gap.dcs.st-and.ac.uk/~gap`

[3] R. Graham, V. Rödl and A. Ruciński, On Schur properties of random subsets of integers, *J. Numb. Theory* **61** (1996), 388-408.

[4] T. Schoen, The Number of Monochromatic Schur Triples, *Europ. J. Combinatorics* **20** (1999) 855-866.

[5] A. Robertson and D. Zeilberger, A 2-coloring of $[1, N]$ can have $(1/22)N^2 + O(N)$ monochromatic Schur triples, but not less!, *Electron. J. Combin.* **5** (1998) #R19.