Density and Ramsey type results on algebraic equations with restricted solution sets

Péter Csikvári, András Sárközy[1]

Eötvös Loránd University, Department of Algebra, H–1117 Budapest, Pázmány Péter sétány 1/C, Hungary

Katalin Gyarmati[1]

Alfréd Rényi Institute of Mathematics, H–1053 Budapest, Reáltanoda u. 13–15, Hungary

---

Abstract

In earlier papers Sárközy studied the solvability of the equations

$$a + b = cd,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D},$$

resp.

$$ab + 1 = cd,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$$

where $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are "large" subsets of $\mathbb{F}_p$. Later Gyarmati and Sárközy generalized and extended these problems by studying these equations and also other algebraic equations with restricted solution sets over finite fields. Here we will continue the work by studying further special equations over finite fields and also algebraic equations with restricted solution sets over the set of the integers, resp. rationals. We will focus on the most interesting cases of algebraic equations with 3, resp. 4 variables. In the cases when there are no "density results" of the above type, we will be also looking for Ramsey type results, i.e., for monochromatic solutions of the given equation. While in the earlier papers character sum estimates were used, now combinatorial tools dominate.

Key words: algebraic equation, solution set, Ramsey type
2000 Mathematics Subject Classification: Primary 11B75.

Email addresses: `csiki@cs.elte.hu`, `sarkozy@cs.elte.hu` (Péter Csikvári, András Sárközy[1]), `gykati@cs.elte.hu` (Katalin Gyarmati[1]).

[1] Research partially supported by the Hungarian National Foundation for Scientific Research, Grants No. T 043623, T 043631 and T 049693.

1 Introduction

Throughout this paper $\mathbb{Z}, \mathbb{N}$ and $\mathbb{Q}$ denote the set of the integers, positive integers and rational numbers, respectively. p will denote a prime number. $\mathbb{F}_q$ denotes the finite field of order q, and we write $q = p^r$ (with $r \in \mathbb{N}$) and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Sárközy [9], [10] proved that if p is a prime and $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are "large" subsets of $\mathbb{F}_p$ (more precisely, $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|$ is greater than Cp^3 with an absolute constant C), then the equation

$$a + b = cd, \ a \in \mathcal{A}, \ b \in \mathcal{B}, \ c \in \mathcal{C}, \ d \in \mathcal{D}, \tag{1.1}$$

resp.

$$ab + 1 = cd, \ a \in \mathcal{A}, \ b \in \mathcal{B}, \ c \in \mathcal{C}, \ d \in \mathcal{D} \tag{1.2}$$

can be solved.

Gyarmati and Sárközy [6], [7] generalized these results to finite fields:

Theorem A *If q is a prime power, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$ and*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > q^3,$$

then (1.1) *can be solved.*

Theorem B *If q is a prime power, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$ and*

$$|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > 100q^3,$$

then (1.2) *can be solved.*

If a theorem says that a certain equation can be solved in "large" (in the infinite case, "dense") subset(s) of a given set $\mathcal{S}$, then we will call this result *a density result*. More precisely, if $\mathcal{S}$ is finite and our theorem says that there is a $c > 0$ so that in order to guarantee the solvability of the equation it suffices to assume that the size of the subset(s) is $> |\mathcal{S}|^{1-c}$, then we will call the result a *strong* density result, while if the corresponding lower bound is of form $> |\mathcal{S}|\big(f(|\mathcal{S}|)\big)^{-1}$ with some $f(N) \to +\infty$, $f(N) = N^{o(1)}$, then we will speak of *weak* density result. Moreover, if only one subset $\mathcal{A}$ is given and all the variables must assume values belonging to $\mathcal{A}$ (e.g., in (1.1) it is assumed that $\mathcal{A} = \mathcal{B} = \mathcal{C} = \mathcal{D}$), then we will call the result a *special* density result, otherwise we will speak of *general* density result. Finally, if a theorem says that for any k-coloring of $\mathcal{S}$ the given equation must have a monochromatic solution, then the result is called a Ramsey type theorem. Using this terminology we may say that Theorems A and B are strong general density results.

In [6] and [7] Theorems A and B were also generalized by considering equations

$$a + b = f(c, d), \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D},$$

resp.

$$ab = f(c, d),\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$$

with $f(x, y) \in \mathbb{F}_q[x, y]$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$, and it was shown that if $f(x, y)$ satisfies certain conditions, then these equations are solvable and, indeed, strong general density theorems of type Theorems A and B were proved.

Even more generally, we proposed to study general equations of form

$$F(a_1, \dots, a_n) = 0, \quad a_1 \in \mathcal{A}_1, \dots, a_n \in \mathcal{A}_n \tag{1.3}$$

(with $F(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$, $\mathcal{A}_1, \dots, \mathcal{A}_n \subset \mathbb{F}_q$) over $\mathbb{F}_q$. In particular, we studied the connection between the solvability and n, the number of variables. We showed that if $n = 2$, then there is no general density result:

Theorem C *Let q be a prime power, let $f(x, y) \in \mathbb{F}_q[x, y]$ be of degree u and v in x and y, resp., and assume that $u, v < \frac{q}{2}$. Then there are $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ with*

$$|\mathcal{A}| \geq \frac{q}{2}, \quad |\mathcal{B}| = \left[\frac{q}{2u}\right]$$

so that

$$f(a, b) = 0, \quad a \in \mathcal{A},\ b \in \mathcal{B}$$

cannot be solved.

By Theorems A, B and their generalizations, there are (strong general) density results with $n = 4$. However, we showed that not every polynomial F with $n = 4$ is "good":

Theorem D *Let $n \in \mathbb{N}$, $n \geq 2$, $d_1, \dots, d_n \in \mathbb{N}$ and $\varepsilon > 0$. Then there is a $p_0 = p_0(n, d_1, \dots, d_n, \varepsilon)$ so that if p is a prime with $p > p_0$ and $f_1(x) \in \mathbb{F}_p[x], \dots, f_n(x) \in \mathbb{F}_p[x]$ are polynomials of degree $d_1, \dots, d_n$, resp., then there are subsets $\mathcal{A}_1, \dots, \mathcal{A}_n$ of $\mathbb{F}_p$ so that*

$$|\mathcal{A}_i| > \left(\frac{1}{n} - \varepsilon\right) p \ \ \textit{for } i = 1, 2, \dots, n,$$

and

$$g(a_1, \dots, a_n) \stackrel{\text{def}}{=} f_1(a_1) + \dots + f_n(a_n) = 0, \quad a_1, \in \mathcal{A}_1, \dots, a_n \in \mathcal{A}_n \tag{1.4}$$

has no solution.

We also proved a similar theorem with

$$g(a_1, \dots, a_n) = f_1(a_1) \dots f_n(a_n) - 1$$

in place of the polynomial g in (1.4).

By Theorems A and B there are (strong) general density results with $n = 4$ but, by Theorem C, there is none with $n = 2$. We do not know what the situation for $n = 3$ is, so that in [7] we raised the following problem (here we formulate it in a slightly different form):

Problem A Is there a polynomial $F(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$ of three variables so that there is a general density result on the solvability of

$$F(a_1, a_2, a_3) = 0, \quad a_1 \in \mathcal{A}_1,\ a_2 \in \mathcal{A}_2,\ a_3 \in \mathcal{A}_3,$$

in $\mathbb{F}_q$ (for $q \to +\infty$)?

In [7] Gyarmati and Sárközy also proposed to study similar problems in $\mathbb{N}$ and infinite fields. In particular, we pointed out that there are no density theorems in $\mathbb{N}$ on the solvability of equations (1.1) and (1.2). On the other hand, we asked whether there are *Ramsey type* results in $\mathbb{N}$ on the solvability of these equations:

Problem B Does there exist a $k \in \mathbb{N}$ so that for any k-coloring of $\mathbb{N}$, (1.1) (to avoid trivialities, one should add the restriction $a \neq b$) has a monochromatic solution? If yes, then what is the greatest k with this property? If the answer is negative, then what weaker statements can be proved on the coloring of the solutions of (1.1)?

Problem C Does there exist a $k \in \mathbb{N}$ so that for any k-coloring of $\mathbb{N}$,

$$ab + 8 = cd$$

has a monochromatic solution? (Modulo 8 discussion shows that 1 in (1.2) must be replaced by, say, 8.) If yes, then what is the greatest k with this property?

Note that in the papers [6], [7], [9] and [10] character sums were used (and, indeed, [6] was devoted completely for deducing the necessary character sum estimates).

In this paper we will continue the work by focusing on the most interesting cases when n (the number of variables) is 3, resp. 4, and we will pay more attention to equations over $\mathbb{N}$, resp. $\mathbb{Q}$. These problems are beyond the reach of the analytical methods, thus here we will use elementary-combinatorial methods, and the statements proved will be weaker. First in Sections 2, 3, 4, 5 and 6 we will study equations with $n = 3$ (i.e., in 3 variables) over $\mathbb{N}$ and $\mathbb{F}_q$. Then in Sections 7, 8 and 9 we will study equations with $n = 4$. In Section 10 solvability in $\mathbb{Q}$ will be considered. Finally, in Section 11 we will present unsolved problems.

2 Arithmetic means in $\mathbb{N}$ and $\mathbb{F}_q$

The most important equation with $n = 3$ is, perhaps, the equation

$$a + b = 2c, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C}. \tag{2.1}$$

First consider this equation over $\mathbb{N}$. If $\mathcal{A}$ is the set of the even numbers, $\mathcal{B}$ is the set of the odd numbers and $\mathcal{C} = \mathbb{N}$, then (2.1) has no solution which shows that there is no *general* density theorem in this case.

Now consider the special case $\mathcal{A} = \mathcal{B} = \mathcal{C}$. Then $a = b = c$ is a trivial solution. We may restrict ourselves to look for nontrivial solutions:

$$a + b = 2c, \quad a, b, c \in \mathcal{A}, \quad a \neq b. \tag{2.2}$$

For $n \in \mathbb{N}$, let $r_3(n)$ denote the cardinality of the maximal set selected from $\{1, 2, \ldots, n\}$ so that (2.2) has no solution. Then by Roth's theorem [8] we have $r_3(n) < c\frac{n}{\log\log n}$ (and this has been improved to $r_3(n) < cn\left(\frac{\log\log n}{\log n}\right)^{1/2}$ by Bourgain [2]) so that there is a (weak) special density theorem. By Behrend's theorem [1] we have $r_3(n) > n\exp\left(-c(\log n)^{1/2}\right)$ which shows that there is no *strong* special density theorem.

Now consider equation (2.1) over $\mathbb{F}_q$. Let $q = p$ be a prime, $\mathcal{A} = \{2k+1 : 0 < 2k+1 < p/2\}$, $\mathcal{B} = \{2k : 0 < 2k < p/2\}$, $\mathcal{C} = \{k : 0 < k < p/2\}$. (Throughout this paper we identify $\mathbb{F}_p$ with the field of the modulo p residue classes, and we do not distinguish between an integer a and the modulo p residue class represented by a.) Then (2.1) has no solution so that again, there is no *general* density theorem. (Similar is the situation for $q = p^r$ with $p > 2$; we leave the details to the reader.)

Assume now that $q = p^r$ with $p \to +\infty$, $\mathcal{A} \subset \mathbb{F}_q$, and consider equation (2.2) over $\mathbb{F}_q$. $\mathbb{F}_q$ forms a linear vector space of dimension r over its prime field $\mathbb{F}_p$, let $e_1, e_2, \ldots, e_r$ be a basis of this vector space. Every $a \in \mathcal{A}$ has a unique representation in form

$$a = x_1(a)e_1 + \cdots + x_r(a)e_r \quad \text{with } x_1(a), \ldots, x_r(a) \in \mathbb{F}_p.$$

By the pigeon hole principle there are $y_2, \ldots, y_r$ so that writing $\mathcal{A}' = \{a : x_2(a) = y_2, \ldots, x_r(a) = y_r\}$ we have

$$|\mathcal{A}'| \geq \frac{|\mathcal{A}|}{p^{r-1}}. \tag{2.3}$$

If

$$|\mathcal{A}| > \frac{r_3(p)}{p}q,$$

then it follows from (2.3) that writing $\mathcal{B} = \{x_1(a) : a \in \mathcal{A}'\}$ we have

$$|\mathcal{B}| = |\mathcal{A}'| > r_3(p)$$

and $\mathcal{B} \subset \{1, 2, \ldots, p\}$ can be assumed. Then $\mathcal{B}$ contains a 3 term arithmetic progression, i.e., there are distinct elements $a_1, a_2, a_3 \in \mathcal{A}'$ so that $x_1(a_1), x_1(a_2), x_1(a_3)$ form a 3 term arithmetic progression. Then (2.2) holds with a_1, a_2, a_3 in place of a, b, c, and thus by Roth's theorem [8] there is a weak special density theorem over $\mathbb{F}_q$ for $p \to +\infty$. (Note that the case $q = 2^r$ is different: then (2.2) becomes

$$a + b = 0, \quad a, b \in \mathcal{A}, \quad a \neq b$$

which has no solution.)

On the other hand, if $q = p$ is a prime and $\mathcal{A}$ is a maximal set selected from $\{n : 0 < n < p/2\}$ such that it does not contain a 3 term arithmetic progression, then $\mathcal{A}$ as a subset of $\mathbb{F}_p$ is such that (2.2) cannot be solved, and by Behrend's theorem [1], we have

$$|\mathcal{A}| > p \exp\Big(-c(\log p)^{1/2}\Big).$$

This shows that there is no *strong* special density theorem over $\mathbb{F}_p$.

3 Geometric means in $\mathbb{N}$ and $\mathbb{F}_q$

The multiplicative analog of equation (2.1) is

$$ab = c^2, \quad a \in \mathcal{A}, \quad b \in \mathcal{B}, \quad c \in \mathcal{C}. \tag{3.1}$$

First consider this equation over $\mathbb{N}$. The example $\mathcal{A} = \{a : a \text{ is odd}\}$, $\mathcal{B} = \{b : b \equiv 2 \pmod 4\}$, $\mathcal{C} = \mathbb{N}$ shows that there is no *general* density theorem. In the special case $\mathcal{A} = \mathcal{B} = \mathcal{C}$ again we must assume that $a \neq b$:

$$ab = c^2, \quad a, b, c \in \mathcal{A}, \quad a \neq b. \tag{3.2}$$

Then the example $\mathcal{A} = \{n : |\mu(n)| = 1\}$ (where $\mu(n)$ is the Möbius function, i.e., $\mathcal{A}$ consists of the squarefree integers) shows that there is no *special* density theorem either.

On the other hand, there is a Ramsey type result over $\mathbb{N}$:

Proposition 1 *For every $k \in \mathbb{N}$ and every k-coloring of $\mathbb{N}$ the equation*

$$ab = c^2, \quad a \neq b \tag{3.3}$$

has a monochromatic solution in $\mathbb{N}$.

Proof. Define a *new* k-coloring of $\mathbb{N}$ so that $n \in \mathbb{N}$ should be of the same color as 2^n according to the *original* k-coloring. Then by van der Waerden's theorem [12] there is a 3 term arithmetic progression d, $d+e$, $d+2e$ (with $e \neq 0$) in $\mathbb{N}$ which is monochromatic in terms of the *new* k-coloring. Then $a = 2^d$, $b = 2^{d+2e}$, $c = 2^{d+e}$ is a monochromatic solution of (3.3) in terms of the *original* k-coloring. $\square$

Now consider $\mathbb{F}_q$. Let γ denote the quadratic character of $\mathbb{F}_q$, i.e., for $a \in \mathbb{F}_q$ we have

$$\gamma(a) = \begin{cases} +1 & \text{if } a \neq 0 \text{ and } x^2 = a \text{ has solution in } \mathbb{F}_q, \\ -1 & \text{if } a \neq 0 \text{ and } x^2 = a \text{ has no solution in } \mathbb{F}_q, \\ 0 & \text{if } a = 0. \end{cases}$$

Then for $\mathcal{A} = \{a : a \in \mathbb{F}_q, \gamma(a) = +1\}$, $\mathcal{B} = \{b : b \in \mathbb{F}_q, \gamma(b) = -1\}$, $\mathcal{C} = \mathbb{F}_q$ equation (3.1) has no solution which shows that there is no *general* density theorem.

On the other hand, there is a *weak special* density theorem over $\mathbb{F}_q$:

Proposition 2 *If* $\mathcal{A} \subset \mathbb{F}_q^*$ *and*

$$|\mathcal{A}| > r_3(q-1), \tag{3.4}$$

then equation (3.2) *can be solved.*

Proof. Let g be a primitive element of $\mathbb{F}_q$, and define $\mathcal{K}$ by

$$\mathcal{K} = \Big\{k : k \in \{1, 2, \ldots, q-1\}, g^k \in \mathcal{A}\Big\}.$$

By (3.4), $\mathcal{K}$ contains an arithmetic progression k, $k+d$, $k+2d$ (with $d > 0$). Then $a = g^k$, $b = g^{k+2d}$, $c = g^{k+d}$ is a solution of (3.2). $\square$

Indeed, by Roth's theorem [8] this can be considered as a *weak* special density theorem. On the other hand, there is no *strong* special density theorem in this case. To see this, define $\mathcal{L}$ so that it is a maximal set selected from $\{1, 2, \ldots, [(q-1)/2]\}$ which contains no arithmetic progression of 3 terms, and let $\mathcal{A} = \{g^\ell : \ell \in \mathcal{L}\}$ (where again g is a primitive element of $\mathbb{F}_q$). Then (3.2) has no solution, and by Behrend's theorem [1] we have

$$|\mathcal{A}| = |\mathcal{L}| = r_3\Big([(q-1)/2]\Big) > q \exp\Big(-c(\log q)^{1/2}\Big).$$

4 The equation $a(b+c) = bc$

We have seen that there is neither general nor special result on the second degree homogeneous equation (3.2) over $\mathbb{N}$, but there is a Ramsey type result in this case. Now we will show a less trivial example of this type.

Consider the equation

$$a(b+c) = bc, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C} \tag{4.1}$$

first over $\mathbb{N}$. Then the example $\mathcal{A} = \mathcal{B} = \mathcal{C} = \{n : n \in \mathbb{N},\ n \text{ is odd}\}$ shows that there is neither general nor special density theorem in this case. On the other hand, there is a Ramsey type theorem:

Theorem 1 *For every $k \in \mathbb{N}$ and every k-coloring of $\mathbb{N}$, the equation*

$$a(b+c) = bc,\ a, b, c \in \mathcal{A} \tag{4.2}$$

has a monochromatic solution.

Proof. We will need

Lemma 1 *For every $n \in \mathbb{N}$ there are different rational numbers $x_1, x_2, \dots, x_n$ so that for all $1 \le i < j \le n$ we have $\frac{1}{x_j - x_i} \in \mathbb{Z}$.*

Proof of Lemma 1. Let $t_1, t_2, \dots, t_n$ be different positive integers and set

$$x_i = \frac{1}{t_i \prod\limits_{u \ne v} (t_u - t_v)}.$$

Then we have

$$\begin{aligned} x_i - x_j &= \frac{1}{t_i \prod\limits_{u \ne v} (t_u - t_v)} - \frac{1}{t_j \prod\limits_{u \ne v} (t_u - t_v)} \\ &= \frac{t_j - t_i}{t_i t_j \prod\limits_{u \ne v} (t_u - t_v)} = \frac{1}{t_i t_j \prod\limits_{\substack{u \ne v \\ (u,v) \ne (j,i)}} (t_u - t_v)} \end{aligned}$$

whence $\frac{1}{x_i - x_j} \in \mathbb{Z}$ follows and this completes the proof of the lemma.

Now assume that n is a positive integer which is large enough in terms of k and which will be fixed later, and define the numbers $x_1, x_2, \dots, x_n$ as it is described in Lemma 1. Consider the complete graph of n vertices $P_1, P_2, \dots, P_n$, and k-color its edges so that the edge (P_i, P_j) should be colored by the same color as the positive integer $\frac{1}{|x_i - x_j|}$ in the given k-coloring of $\mathbb{N}$. Now we fix n: it should be so large that Ramsey's theorem guarantees a monochromatic triangle in any k-coloring of the complete graph of n vertices. Then in our graph we can find a monochromatic triangle with vertices, say, P_i, P_j, P_ℓ; without the loss of generality we may assume that $x_i > x_j > x_\ell$. Writing $a = \frac{1}{x_i - x_\ell}$, $b = \frac{1}{x_i - x_j}$ and $c = \frac{1}{x_j - x_\ell}$, clearly a, b, c is a monochromatic solution of the equation in (4.1) in $\mathbb{N}$. $\square$

Now consider equation (4.1) over $\mathbb{F}_q$. If $q = p$ is a prime, then the example $\mathcal{A} = \mathcal{B} = \mathcal{C} = \left\{a : a \in \mathbb{F}_q^*, \; a^{-1} \in \left\{1, 3, \ldots, 2\left[\frac{p}{4}\right] - 1\right\}\right\}$ shows that there is neither general, nor special density theorem (and examples of similar nature can be given for general q as well). On the other hand, again there is a Ramsey type theorem:

Theorem 2 *For every $k \in \mathbb{N}$ there is a number $q_0 = q_0(k)$ such that if $q > q_0$, then for every k-coloring of $\mathbb{F}_q$, equation* (4.2) *has a monochromatic solution.*

The method of the proof of Theorem 2 can be adjusted to prove this theorem, we leave the details to the reader.

5 The equation $a + b = c^2$

So far we have studied simple linear or second degree equations, and in each case it turned out that there is at least a Ramsey type theorem. Now we will study a further equation of this type where the situation is worse. Indeed, consider the equation

$$a + b = c^2, \quad a \in \mathcal{A}, \; b \in \mathcal{B}, \; c \in \mathcal{C} \tag{5.1}$$

over $\mathbb{N}$. The example $\mathcal{A} = \mathcal{B} = \mathcal{C} = \{n : n \in \mathbb{N}, \; n \text{ is odd}\}$ shows that there is neither general nor special density theorem in this case. We will show that there is no Ramsey type theorem either. More exactly, $a = b = c = 2$ is always a monochromatic solution which we will call trivial solution, and we will be looking only for nontrivial monochromatic solutions.

Theorem 3 $\mathbb{N}$ *can be colored by* 16 *colors so that the equation*

$$a + b = c^2 \tag{5.2}$$

has no nontrivial monochromatic solution.

Proof. We have to write $\mathbb{N}$ as the disjoint union of 16 sets so that, apart from the trivial solution, (5.2) cannot be solved in either of them. Define the 16 sets in the following way: let

$$
\begin{aligned}
\mathcal{A}_i &= \{n : n \in \mathbb{N},\ n \equiv i \pmod 5\} \text{ for } i = 1, 3 \text{ and } 4,\\
\mathcal{B}_i &= \{n : n \in \mathbb{N},\ n = m \cdot 5^{2^{2u}(2v+1)} \text{ with } m \equiv i \pmod 5),\ u, v = 0, 1, \dots\}\\
&\qquad\qquad\qquad\qquad\qquad \text{for } i = 1, 2, 3 \text{ and } 4,\\
\mathcal{C}_i &= \{n : n \in \mathbb{N},\ n = m \cdot 5^{2^{2u+1}(2v+1)} \text{ with } m \equiv i \pmod 5),\ u, v = 0, 1, \dots\}\\
&\qquad\qquad\qquad\qquad\qquad \text{for } i = 1, 2, 3 \text{ and } 4,\\
\mathcal{D}_i &= \{n : n \in \mathbb{N},\ n = m \cdot 5^u + 2 \text{ with } m \equiv i \pmod 5),\ u = 1, 2, \dots\}\\
&\qquad\qquad\qquad\qquad\qquad \text{for } i = 1, 2, 3 \text{ and } 4,\\
\mathcal{E} &= \{2\}.
\end{aligned}
$$

Then clearly, $\mathbb{N}$ is the disjoint union of these 16 sets. It remains to see that (5.2) cannot be solved in either of the first 15 sets.

Case 1. Assume that $a, b, c \in \mathcal{A}_i$ with $i = 1, 3$ or 4. Then clearly $a + b \equiv 2i \pmod 5$ and $c^2 \equiv i^2 \pmod 5$ and since $i^2 - 2i = i(i-2) \not\equiv 0 \pmod 5$ thus (5.2) cannot hold.

Case 2. Assume that $a, b, c \in \mathcal{B}_i$ with $i = 1, 2, 3$ or 4. Write

$$a = m(a)5^{2^{2u(a)}(2v(a)+1)},\ b = m(b)5^{2^{2u(b)}(2v(b)+1)},\ c = m(c)5^{2^{2u(c)}(2v(c)+1)}. \quad (5.3)$$

Then c^2 can be written in the form

$$c^2 = (m(c))^2 5^{2^{2u(c)+1}(2v(c)+1)} \text{ with } (m(c))^2 \equiv i^2 \not\equiv 0 \pmod 5. \quad (5.4)$$

Now we have to distinguish two cases.

Case 2a. Assume that a and b are divisible by different powers of 5. We may assume that a is divisible by higher power of 5 than b. Then $a + b$ is of the form

$$a + b = m(a+b)5^{2^{2u(b)}(2v(b)+1)} \text{ with } m(a+b) \equiv m(b) \equiv i \not\equiv 0 \pmod 5). \quad (5.5)$$

By (5.4) and (5.5), $a + b$, resp. c^2 are divisible by different powers of 5, thus (5.2) cannot hold.

Case 2b. Assume that a and b are divisible by the same power of 5 so that $u(b) = u(a)$, $v(b) = v(a)$. Then we have

$$a+b = (m(a)+m(b))5^{2^{u(a)}(2v(a)+1)} \text{ with } m(a)+m(b) \equiv 2i \not\equiv 0 \pmod 5). \quad (5.6)$$

By (5.4) and (5.6), again $a + b$, resp. c^2 are divisible by different powers of 5, thus (5.2) cannot hold.

Case 3. Assume that $a, b, c \in \mathcal{C}_i$ with $i = 1, 2, 3$ or 4. This case can be handled in exactly the same way as Case 2 thus we leave the details to the reader.

Case 4. Assume that $a, b, c \in \mathcal{D}_i$ with $i = 1, 2, 3$ or 4. Write

$$a = m(a)5^{u(a)} + 2, \quad b = m(b)5^{u(b)} + 2, \quad c = m(c)5^{u(c)} + 2. \tag{5.7}$$

Then c^2 can be written in the form

$$c^2 = (m(c))^2 5^{2u(c)} + 4m(c)5^{u(c)} + 4 = m(c^2)5^{u(c)} + 4 \tag{5.8}$$

with

$$m(c^2) \equiv 4m(c) \equiv 4i \not\equiv 0 \pmod 5. \tag{5.9}$$

Again we have to distinguish two cases.

Case 4a. Assume that $u(a) \neq u(b)$. We may assume that $u(a) > u(b)$. Then we have

$$a + b = \left(m(a)5^{u(a)} + 2\right) + \left(m(b)5^{u(b)} + 2\right) = m(a+b)5^{u(b)} + 4 \tag{5.10}$$

with

$$m(a+b) = m(a)5^{u(a)-u(b)} + m(b) \equiv m(b) \equiv i \not\equiv 0 \pmod 5. \tag{5.11}$$

By (5.8), (5.9), (5.10) and (5.11) and since

$$4i \not\equiv i \pmod 5 \qquad (\text{for } i \in \{1, 2, 3, 4\}),$$

thus (5.2) cannot hold.

Case 4b. Assume that $u(a) = u(b)$. Then we have

$$a + b = (m(a) + m(b))5^{u(a)} + 4 \text{ with } m(a) + m(b) \equiv 2i \pmod 5. \tag{5.12}$$

By (5.8), (5.9) and (5.12) and since

$$4i \not\equiv 2i \pmod 5 \quad (\text{for } i \in \{1, 2, 3, 4\}),$$

thus (5.2) cannot hold. $\square$

If p is a prime and we take

$$\mathcal{A} = \left\{ a :\ 0 < a < \frac{p}{4},\ a^2 \equiv \left[\frac{p}{2}\right] + 1, \dots, p-2,\ p-1 \pmod p \right\},$$

then it can be shown that $|\mathcal{A}| \gg p$ and, clearly, (5.2) has no solution with $a, b, c \in \mathcal{A}$ so that there is neither general nor special density theorem on the solvability of (5.2) in $\mathbb{F}_p$. We do not know whether there is a Ramsey type theorem in $\mathbb{F}_p$ (or more generally, in $\mathbb{F}_q$).

6 The Fermat equation in $\mathbb{F}_p$

By Schur's classical theorem [11] the Fermat equation

$$a^n + b^n = c^n, \ abc \neq 0 \quad (\text{with } n \in \mathbb{N}, \ n \geq 2) \tag{6.1}$$

is solvable in $\mathbb{F}_p$ for $p > p_0(n)$. Now we will sharpen this result by proving the following Ramsey type theorem:

Theorem 4 *For all $k, n \in \mathbb{N}$ there is a number $p_0 = p_0(k, n)$ such that if $p > p_0$, then for any k-coloring of $\mathbb{F}_p^*$ the equation*

$$a^n + b^n = c^n \tag{6.2}$$

has a monochromatic solution in $\mathbb{F}_p^*$.

Proof. Consider a k-coloring of $\mathbb{F}_p^*$, i.e., a partition of it into k disjoint sets:

$$\mathbb{F}_p^* = \bigcup_{i=1}^{k} \mathcal{A}_i, \quad \mathcal{A}_i \cap \mathcal{A}_j = \emptyset \text{ for } 1 \leq i < j \leq k.$$

Let g be a primitive root modulo p, and for $u \in \{1, 2, \ldots, p-1\}$ define $q(u), r(u) \in \mathbb{Z}$ by

$$u = q(u)n + r(u), \qquad 0 \leq r(u) < n.$$

Define a new coloring of $\mathbb{F}_p^*$ so that for $1 \leq u, v \leq p-1$, the elements g^u and g^v of $\mathbb{F}_p^*$ belong to the same colorclass if and only if $g^{q(u)}$ and $g^{q(v)}$ belong to the same colorclass $\mathcal{A}_i$: $g^{q(u)}, g^{q(v)} \in \mathcal{A}_i$ for some $1 \leq i \leq k$, and we also have $r(u) = r(v)$; there are kn color classes in this new coloring. Now we need a lemma of Schur [11] which was also used in the proof of his theorem on the solvability of (6.1):

Lemma 2 *For every $t \in \mathbb{N}$ and any t-coloring of the set $\{1, 2, \ldots, [t!e]\}$, the equation*

$$x + y = z$$

has a monochromatic solution in this set.

If $p-1 > (kn)!e$ then we may apply this lemma for the new coloring of $\mathbb{F}_p^*$, and we obtain that there are g^u, g^v, g^w which belong to the same new colorclass and satisfy

$$g^u + g^v = g^w,$$

i.e.,

$$g^{q(u)n+r(n)} + g^{q(v)n+r(v)} = g^{q(w)n+r(w)}$$

with $r(u) = r(v) = r(w)$. Dividing by $g^{r(u)}$ we obtain

$$(g^{q(u)})^n + (g^{q(v)})^n = (g^{q(w)})^n$$

so that $a = g^{q(u)}$, $b = g^{q(u)}$, $c = g^{q(w)}$ is a monochromatic solution of (6.2). $\square$

7 The equation $a + b = cd$

Unfortunately, we have not been able to settle Problem B on the existence of monochromatic solutions of

$$a + b = cd, \quad a \neq b \tag{7.1}$$

for any k-coloring of $\mathbb{N}$, but we have proved certain partial results. In particular, we have found several proofs for the following weaker result:

Theorem 5 *For every $k \in \mathbb{N}$ and for any k-coloring of $\mathbb{N}$, equation* (7.1) *can be solved so that a and b, resp. c and d are of the same color.*

Here we will present two proofs which sharpen this result in various directions. The first one provides further information on the integers a, b, c, d described in Theorem 5.

Theorem 6 *For every $k \in \mathbb{N}$ and any k-coloring of $\mathbb{N}$, i.e., for*

$$\mathbb{N} = \bigcup_{i=1}^{k} \mathcal{A}_i, \quad \mathcal{A}_i \cap \mathcal{A}_j = \emptyset \ \text{ for } 1 \leq i < j \leq k,$$

there is a color class $\mathcal{A}_\ell$ and a finite subset $\mathcal{D} \subset \mathcal{A}_\ell$ of it with the property that for every $c \in \mathcal{A}_\ell$ there are a $d \in \mathcal{D}$ and a, b of the same color so that a, b, c, d satisfy equation (7.1).

Proof. For $n \in \mathbb{N}$ let $i(n)$ denote the integer i with $n \in \mathcal{A}_i$. Consider the complete graph on the vertex set $\mathbb{N}$, and k-color it so that the edge joining the integers u, v ($u \neq v$) is colored by the color assigned to $\mathcal{A}_{i(u+v)}$. By Ramsey's theorem this graph contains arbitrarily large monochromatic clique thus, in particular, there are distinct positive integers $u_1, u_2, \ldots, u_{k+1}$ so that all the edges (u_r, u_s) ($1 \leq r < s \leq k+1$) are of the same color, i.e., there is a color class $\mathcal{A}_\ell$ so that $u_r + u_s \in \mathcal{A}_\ell$ for all $1 \leq r < s \leq k+1$. Let $\mathcal{D} = \{u_r + u_s : 1 \leq r < s \leq k+1\}$. For every $c \in \mathcal{A}_\ell$, by the pigeon hole principle there are $1 \leq m < n \leq k+1$ so that cu_m and cu_n are of the same color. Then $a = cu_m$, $b = cu_n$, c and $d = u_r + u_s$ satisfy all the requirements in the theorem. $\square$

The other sharpening of Theorem 5 provides estimate for the number of integers n which have representations in form

$$n = a + b = cd, \quad a \neq b \tag{7.2}$$

with a and b, resp. c and d of the same color. We will show that the *logarithmic density* of the integers which have representations of this form is large:

Theorem 7 *For a fixed k-coloring of $\mathbb{N}$, let $\mathcal{N}$ denote the set of the integers n which have representations in form* (7.2) *with a and b, resp. c and d of the same color. There is a positive absolute constant C such that if $k \in \mathbb{N}$, $N \in \mathbb{N}$ and $N > N_0(k)$, then for any k-coloring of $\mathbb{N}$ we have*

$$\sum_{\substack{n \leq N \\ n \in \mathcal{N}}} \frac{1}{n} > \frac{C}{k} \log N. \tag{7.3}$$

Proof. We will derive the result from a theorem of Erdős, Sárközy and T. Sós [4], and another theorem of Erdős and Sárközy [3]:

Lemma 3 [4] *For a fixed k-coloring of $\mathbb{N}$, let $\mathcal{M}$ denote the set of the even integers $2n$ which have a monochromatic representation in the form $a+b$ with $a \neq b$. Then to every $k \geq 2$ there exists an $M_0(k)$ such that for any k-coloring of $\mathbb{N}$ we have*

$$\left|\{n :\, 2n \leq M, 2n \in \mathcal{M}\}\right| > \frac{M}{2} - 3M^{1-2^{-k-1}} \quad \textit{for } M > M_0(k).$$

Lemma 4 [3] *There is a positive absolute constant C_1 such that if $k \in \mathbb{N}$, $M \in \mathbb{N}$, $M > M_0(k)$ and for a fixed k-coloring of $\mathbb{N}$, $\mathcal{B}$ denotes the set of the integers which have a monochromatic representation in the form cd, then*

$$\sum_{\substack{b \leq M \\ b \in \mathcal{B}}} \frac{1}{b} > \frac{C_1}{k} \log M.$$

(Indeed, Lemma 4 is a slightly weaker form of Theorem 2 in [3].)

In order to derive the statement of the theorem from these lemmas, first introduce a new coloring of $\mathbb{N}$: color $n \in \mathbb{N}$ by the same color which is used to color $2n$ in the original coloring given in the theorem. Let $\mathcal{B}$ denote the set of the integers which have a monochromatic representation in terms of the *original* coloring in the form cd, and let $\mathcal{B}'$ denote the set of the integers which have a monochromatic representation in terms of the *new* coloring in the form $c'd'$. Note that if $n' = c'd' \in \mathcal{B}'$, then $n = 4n' = 4(c'd') = (2c')(2d') \in \mathcal{B}$. Thus defining $\mathcal{N}$ as in the theorem and $\mathcal{M}$ as in Lemma 3 (both in terms of the original coloring) we have

$$\sum_{\substack{n\le N\\ n\in\mathcal{N}}}\frac{1}{n}\ge\sum_{\substack{n\le N,4|n\\ n\in\mathcal{N}}}\frac{1}{n}=\sum_{\substack{n\le N,4|n\\ n\in\mathcal{M}\cap\mathcal{B}}}\frac{1}{n} \tag{7.4}$$
$$=\sum_{\substack{n\le N,4|n\\ n\in\mathcal{B}}}\frac{1}{n}-\sum_{\substack{n\le N,4|n\\ n\in\mathcal{B},n\notin\mathcal{M}}}\frac{1}{n}\ge\sum_{\substack{4n'\le N\\ 4n'\in\mathcal{B}}}\frac{1}{4n'}-\sum_{\substack{n\le N,4|n\\ n\notin\mathcal{M}}}\frac{1}{n}\ge$$
$$\ge\frac{1}{4}\sum_{\substack{n'\le N/4\\ n'\in\mathcal{B}'}}\frac{1}{n'}-\sum_{\substack{n\le N,2|n\\ n\notin\mathcal{M}}}\frac{1}{n}.$$

If N is large enough in terms of k, then here we have

$$\sum_{\substack{n'\le N/4\\ n'\in\mathcal{B}'}}\frac{1}{n'}>\frac{C_1}{k}\log[N/4] \tag{7.5}$$

by Lemma 4, and

$$\sum_{\substack{n\le N,2|n\\ n\notin\mathcal{M}}}\frac{1}{n}<K \tag{7.6}$$

with a constant $K=K(k)$ depending only on k which follows from Lemma 3 by partial summation.

(7.3) follows from (7.4), (7.5) and (7.6) with $\frac{C_1}{5k}$ in place of C if N is large enough in terms of k. $\square$

(We remark that it follows from the results in [3] that the lower bound in (7.3) is the best possible apart from the value of C, and the lower bound (7.3) for the (lower) logarithmic density cannot be improved to a similar lower bound for the (lower) asymptotic density.)

8 An example

We have seen that writing $F(a,b,c,d)=a+b-cd$, for any k-coloring of N the equation

$$F(a,b,c,d)=0$$

has "many" solutions such that a and b, resp. c and d are of the same color. One may think that, perhaps, this implies that there is always at least one monochromatic solution. Thus one might like to answer the following question: does there exist a second degree polynomial $G(a,b,c,d)\in\mathbb{Z}[a,b,c,d]$ so that for any k-coloring of $\mathbb{N}$, the equation

$$G(a,b,c,d)=0 \tag{8.1}$$

has solution such that a and b, resp. c and d are of the same color, however, there is a k-coloring of $\mathbb{N}$ such that (8.1) has no monochromatic solution? We will show that such a polynomial does exist and, indeed, we will prove slightly more:

Theorem 8 *Write* $g(x,y) = (x+y+1)^2 + x$ *and*

$$G(a,b,c,d) = g(a,b) - g(c+1,d+1).$$

Then

(i) $\mathbb{N}$ *has a 2-coloring such that* (8.1) *has no monochromatic solution,*

(ii) *for any k-coloring of* $\mathbb{N}$, (8.1) *has solution such that a and b, resp. c and d are of the same color.*

Proof. The proof will be based on

Lemma 5

$$g(x,y) = g(u,v), \quad x,y,u,v \in \mathbb{N} \tag{8.2}$$

holds if and only if

$$x = u, \quad y = v.$$

Proof. Assume that (8.2) holds.

CASE 1. Assume first that

$$x + y = u + v. \tag{8.3}$$

Then by (8.2) we have

$$g(x,y) = (x+y+1)^2 + x = g(u,v) = (u+v+1)^2 + u = (x+y+1)^2 + u$$

whence $x = u$, and then $y = v$ also follows from (8.3).

CASE 2. Assume now that $x + y \neq u + v$. We may assume that

$$x + y < u + v.$$

Then we have

$$\begin{aligned} g(x,y) &= (x+y+1)^2 + x < (x+y+1)^2 + x + y \\ &\leq (u+v)^2 + u + v < (u+v+1)^2 < (u+v+1)^2 + u = g(u,v) \end{aligned}$$

which contradicts (8.2), thus this case cannot occur, and this completes the proof of the lemma.

(i) Consider the following 2-coloring, i.e., 2-partition of $\mathbb{N}$:

$$\mathbb{N} = \mathcal{A}_1 \cup \mathcal{A}_2, \quad \mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset \text{ with } \begin{array}{l} \mathcal{A}_1 = \{n : n \in \mathbb{N},\ n \text{ is odd}\} \\ \mathcal{A}_2 = \{n : n \in \mathbb{N},\ n \text{ is even}\}. \end{array}$$

By Lemma 5, the numbers a, b, c, d satisfy (8.1) if and only if

$$a = c + 1, \quad b = d + 1, \tag{8.4}$$

so that every solution (a, b, c, d) is of the form $(c+1, d+1, c, d)$, but $c+1$ and c (and $d+1$ and d) belong to different color classes.

(ii) Consider a k-coloring, i.e., a k-partition of $\mathbb{N}$:

$$\mathbb{N} = \bigcup_{i=1}^{k} \mathcal{A}_i, \quad \mathcal{A}_i \cap \mathcal{A}_j = \emptyset \text{ for } 1 \le i < j \le k.$$

Then by the pigeon hole principle there are $u, v \in \{1, 2, \ldots, k\}$ so that there are infinitely many $n \in \mathbb{N}$ with

$$n \in \mathcal{A}_u, \quad n + 1 \in \mathcal{A}_v. \tag{8.5}$$

Let $\mathcal{S}$ denote the set of the positive integers n satisfying (8.4). Then for any pair $c, d \in \mathcal{S}$, the numbers a, b defined by (8.4) form a solution of (8.1) with the property that a and b, resp. c and d are of the same color. $\square$

9 Generalizations of equations (1.1) and (1.2)

In this section we will study the following generalizations of the equations in (1.1) and (1.2):

$$a + b + m = cd, \tag{9.1}$$

resp.

$$ab + m = cd \tag{9.2}$$

where m is fixed. Over $\mathbb{F}_q$ these equations can be reduced easily to equations (1.1) and (1.2), and then it follows from Theorems A and B that there are density results on the solutions of these equations.

The case of $\mathbb{N}$ is more interesting; it is easy to see that there are no density results, but we may look for Ramsey type results. Consider first equation (9.1).

Theorem 9 (i) *For a fixed $m \in \mathbb{N}$ and k-coloring of $\mathbb{N}$, let $\mathcal{N}$ denote the set of the integers n which have representations in form*

$$n = a + b + m = cd$$

with a and b, resp. c and d of the same color. There is a positive absolute constant C such that if $m, k \in \mathbb{N}$, $N \in \mathbb{N}$ and $N > N_0(k, m)$, then for any k-coloring of $\mathbb{N}$ we have

$$\sum_{\substack{n \le N \\ n \in \mathcal{N}}} \frac{1}{n} > \frac{C}{k} \log N. \tag{9.3}$$

(ii) *If $m \in \mathbb{N}$ and $m+1$ is not a square:*

$$m + 1 \ne z^2 \quad \textit{for } z \in \mathbb{Z}, \tag{9.4}$$

then there is a $k \in \mathbb{N}$ and a k-coloring of $\mathbb{N}$ such that (9.1) *has no monochromatic solution.*

(Note that this theorem also shows that there exist polynomials $G(a, b, c, d)$ of the type that we were looking for in Section 8. However, there we proved a slightly sharper result in a relatively simple and direct way, while here we will also need the relatively deep results from [3].)

Proof. (i) The result can be derived from the following variant of Lemma 4:

Lemma 6 *There are positive absolute constants C_1, C_2 such that if $k \in \mathbb{N}$, $M \in \mathbb{N}$, $m > M_0(k)$ and for a fixed k-coloring of $\mathbb{N}$, $\mathcal{B}$ denotes the set of the integers which have a monochromatic representation in the form cd, then we have*

$$\sum_{\substack{b \le M, 2 | b \\ b \in \mathcal{B}}} \frac{1}{b} > \frac{C_1}{k} \log M \tag{9.5}$$

and

$$\sum_{\substack{b \le M, 2 \nmid b \\ b \in \mathcal{B}}} \frac{1}{b} > \frac{C_2}{k} \log M. \tag{9.6}$$

Proof. (9.5) can be derived from Theorem 2 in [3] and it is implicit in the proof of Theorem 7, while (9.6) can be proved by an easy modification of the proof of Theorem 2 in [3]; we leave the details to the reader.

To prove (9.3) one has to combine Lemma 3 with (9.5) if m is even and with (9.6) if m is odd (in the manner of the proof of Theorem 7); again we leave the details to the reader.

(ii) We will need

Lemma 7 *For every $m \in \mathbb{N}$ satisfying* (9.4) *there are infinitely many primes p such that*

$$\left(\frac{m+1}{p} \right) = -1 \tag{9.7}$$

$\left(\left(\frac{n}{p}\right)\right.$ *denotes the Legendre symbol*$\left.\right)$.

Proof. By (9.4) there is a prime q such that $m+1$ is divisible by an odd power of q, say, $q^{2t+1} \mid m+1$, $q^{2t+2} \nmid m+1$. Write $m+1 = q^{2t+1}q_1^{\alpha_1}\ldots q_r^{\alpha_r}$, and if $q \neq 2$, then let h be a quadratic non-residue modulo q. By the Chinese remainder theorem and Dirichlet's theorem, there are infinitely many primes p such that

$$p \equiv 5 \pmod 8$$

and

$$p \equiv 1 \pmod{q_i} \quad \text{for } i = 1, \ldots, r$$

if $q = 2$, and

$$\begin{aligned} &p \equiv h \pmod q, \\ &p \equiv 1 \pmod 8 \end{aligned}$$

and

$$p \equiv 1 \pmod{q_i} \quad \text{for } 1 \le i \le r,\ q_i \neq 2$$

if $q \neq 2$. Then by the quadratic reciprocity law, if $q = 2$ then we have

$$\left(\frac{m+1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q_1}{p}\right)^{\alpha_1}\cdots\left(\frac{q_r}{p}\right)^{\alpha_r} = (-1)\left(\frac{p}{q_1}\right)^{\alpha_1}\cdots\left(\frac{p}{q_r}\right)^{\alpha_r} = -1,$$

while for $q \neq 2$,

$$\left(\frac{m+1}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right)^{\alpha_1}\cdots\left(\frac{q_r}{p}\right)^{a_r} = \left(\frac{h}{q}\right)(+1)\ldots(+1) = -1$$

which completes the proof of the lemma.

Now let p be a prime such that

$$p > m+1 \tag{9.8}$$

and p satisfies (9.7). Define a p-coloring, i.e., a p-partition of $\mathbb{N}$ in the following way:

$$\mathbb{N} = \bigcup_{i=1}^{p} \mathcal{A}_i,\ \mathcal{A}_i \cap \mathcal{A}_j = \emptyset \ \text{ with } \mathcal{A}_i = \{n :\ n \equiv i \pmod p\} \text{ for } i = 1, \ldots, p.$$

We will show that for this p-coloring (9.1) has no monochromatic solution. Indeed, let $a, b, c, d \in \mathcal{A}_i$ so that

$$a \equiv b \equiv c \equiv d \equiv i \pmod p.$$

Then we have
$$a + b + m \equiv 2i + m \pmod p$$
and
$$cd \equiv i^2 \pmod p.$$
Thus it would follow from (9.1) that
$$2i + m \equiv i^2 \pmod p$$
whence
$$m + 1 \equiv (i-1)^2 \pmod p.$$
By (9.7) and (9.8) this cannot hold. $\square$

Now consider equation (9.2).

Theorem 10 *For every $m \in \mathbb{Z}$, $m \neq 0$, there is a $k \in \mathbb{N}$ and a k-coloring of $\mathbb{N}$ such that (9.2) has no monochromatic solution.*

Proof. Let p be a prime with $p \nmid m$, and consider the following p-coloring, i.e., p-partition of $\mathbb{N}$:
$$N = \bigcup_{i=1}^{p} \mathcal{A}_i,\ \mathcal{A}_i \cap \mathcal{A}_j \neq \emptyset \text{ with } \mathcal{A}_i = \{n\colon n \in \mathbb{N}, n \equiv i \pmod p\} \text{ for } i = 1, 2, ..., p.$$
We will show that for this p-coloring (9.2) has no monochromatic solution. Indeed, assume that $a, b, c, d \in \mathcal{A}_i$ so that
$$a \equiv b \equiv c \equiv d \equiv i \pmod p.$$
Then we have
$$ab + m \equiv i^2 + m \pmod p \tag{9.9}$$
and
$$cd \equiv i^2 \pmod p. \tag{9.10}$$
By $p \nmid m$ it follows from (9.9) and (9.10) that
$$ab + m \not\equiv cd \pmod p$$
thus (9.2) cannot hold. $\square$

Note that Theorem 10 settles Problem C: The answer to the question in Theorem 10 is negative.

We do not know whether for every $m \in \mathbb{N}$, $m \neq 0$ and any k-coloring of $\mathbb{N}$, equation (9.2) must have a solution such that a and b, resp. c and d are of the same color.

10 Equations over $\mathbb{Q}$

So far we have studied equations over $\mathbb{F}_q$, resp. $\mathbb{N}$. One may also ask similar questions on equations over $\mathbb{Q}$. In particular, one might like to study the connection between the behavior of an equation over $\mathbb{N}$, resp. $\mathbb{Q}$. E.g., one may ask the following question: does there exist a polynomial $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that for a suitable k-coloring of $\mathbb{N}$ the equation

$$F(x_1, \ldots, x_n) = 0$$

has no monochromatic solution in $\mathbb{N}$ but, on the other hand, for any k-coloring of $\mathbb{Q}$ it has monochromatic solution in $\mathbb{Q}$? We will show that the answer is affirmative:

Theorem 11 (i) *The equation*

$$2a + 2b - 2c - 1 = 0 \tag{10.1}$$

has no solution in $\mathbb{Z}$, *but*

(ii) *for every* $k \in \mathbb{N}$ *and* k*-coloring of* $\mathbb{Q}$, *equation* (10.1) *has a monochromatic solution in* $\mathbb{Q}$.

Proof. (i) is trivial. To prove (ii), rewrite (10.1) as

$$\left(a - \frac{1}{2}\right) + \left(b - \frac{1}{2}\right) = \left(c - \frac{1}{2}\right).$$

For a given k-coloring of $\mathbb{Q}$, define a new k-coloring of $\mathbb{Q}$ in the following way: assign to $x \in \mathbb{Q}$ the color of $x + \frac{1}{2}$ in the original coloring. Then by Lemma 2 (Schur's theorem [11]) the equation

$$x + y = z$$

has a monochromatic solution in terms of the new coloring. Then the numbers $a = x + \frac{1}{2}$, $b = y + \frac{1}{2}$, $c = z + \frac{1}{2}$ form a monochromatic solution (in terms of the original coloring) of (10.1) in $\mathbb{Q}$.

11 Unsolved problems

Finally, we will present several problems which we have not been able to settle. First for the sake of completeness we recall three further related problems from [7] (in a slightly modified form).

Problem 1 Are there Ramsey type results on the solvability of (1.1), resp. (1.2) in $\mathbb{Z}_m$ (with k, the number of colors fixed and $m \to +\infty$)? (It is easy to see that for composite m there are no density results.)

Problem 2 Can one sharpen Theorems A and B if we have a lower bound for $\min\{|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}|\}$ instead of $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}|$? More precisely, does there exist a $\delta > 0$ such that if $q > q_0$, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_q$ and

$$\min\Big\{|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, |\mathcal{D}|\Big\} > p^{\frac{3}{4}-\delta},$$

then (1.1), resp. (1.2) can be solved?

Problem 3 Does there exist an elementary-algebraic proof for Theorems A and B?

Some new problems:

Problem 4 Is it true that for all $\varepsilon > 0$ there is a $k_0 = k_0(\varepsilon)$ such that if $k \in \mathbb{N}$, $k > k_0$, $p > p_0 = p_0(\varepsilon, k)$ and $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with

$$\min\{|\mathcal{A}|, |\mathcal{B}|\} > p^{\varepsilon},$$

then

$$a_1 + a_2 = b_1 \dots b_k, \quad a_1, a_2 \in \mathcal{A},\ b_1, \dots, b_k \in \mathcal{B}$$

can be solved?

Note that as the special case $2 \nmid k$, $\mathcal{A} = \Big\{1, 2, \dots, [p^{\varepsilon}]+1\Big\}$, $\mathcal{B} = \Big\{b : \Big(\frac{b}{p}\Big) = -1\Big\}$ shows, it would follow from the affirmative answer that the least quadratic non-residue modulo p is $O(p^{\varepsilon})$. This shows that some of the problems of the type studied by us can be very difficult and, indeed, our work was motivated partly by trying to understand better the problem of the least quadratic non-residue.

Problem 5 By Theorem 3 there is no Ramsey type theorem on the solvability of the equation

$$a + b = c^2 \tag{11.1}$$

in $\mathbb{N}$. Is this also true with $\mathbb{F}_q$ in place of $\mathbb{N}$?

Problem 6 Gyarmati [5] studied the following generalization of the Fermat equation in $\mathbb{F}_p$:

$$x^m + y^n = z^r, \quad xyz \neq 0. \tag{11.2}$$

This motivates the following question: can one sharpen Theorem 4 so that for every $m, n, r, k \in \mathbb{N}$ there is a $p_0 = p_0(m, n, r, k)$ such that if p is a prime with $p > p_0$, then for any k-coloring of $\mathbb{F}_p$, equation (11.2) has a monochromatic solution?

Problem 7 Is it true that for every $k \in \mathbb{N}$ and every k-coloring of $\mathbb{Q}$, the equation

$$a + b = cd$$

has a monochromatic solution in $\mathbb{Q}$? (We conjecture that the answer is affirmative, in which case, perhaps, this can be shown without first settling the analog problem over $\mathbb{N}$.)

Problem 8 If m in Theorem 10 has only "large" prime factors, then the number $k = k(m)$ (the number of colors) in the proof is also large. Thus one might like to answer the following question: can one sharpen Theorem 10 by proving that there exists a universal K such that for every $m \in \mathbb{Z}$, $m \neq 0$, there is a $k \in \mathbb{N}$ with $k < K$ and a k-coloring of $\mathbb{N}$ so that (9.2) has no monochromatic solution?

Problem 9 Is it true that for every $k \in \mathbb{N}$ and every k-coloring of $\mathbb{N}$ the equation

$$ab + 1 = cd \tag{11.3}$$

has a solution such that a and b, resp. c and d are of the same color? More generally, is it true that this holds with equation (9.2) in place of (11.3) for every $m \in \mathbb{N}$, $m \neq 0$?

Problem 10 Can one extend Theorem 10 from $\mathbb{N}$ to $\mathbb{Q}$, i.e., is it true that for every $m \in \mathbb{Q}$, $m \neq 0$ there is a $k \in \mathbb{N}$ and a k-coloring of $\mathbb{Q}$ such that (9.2) has no monochromatic solution in $\mathbb{Q}$?

References

[1] F. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U. S. A.* **32** (1946), 331–332.

[2] J. Bourgain, On triples in arithmetic progressions, *Geom. Funct. Anal.* **9** (1999), 968–984.

[3] P. Erdős and A. Sárközy, On a conjecture of Roth and some related problems, II, in: *Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association (held at Banff Center, Banff, Alberta, April 17–27, 1988)*, ed. R. A. Mollin, Walter de Gruyter, Berlin–New York, 1990; 125–138.

[4] P. Erdős, A. Sárközy and V. T. Sós, On a conjecture of Roth and some related problems, I, in: *Irregularities of Partitions*, eds. G. Halász and V. T. Sós, Algorithms and Combinatorics 8, Springer-Verlag, Berlin–Heidelberg–New York, 1989; 47–59.

[5] K. Gyarmati, On a problem of Diophantus, *Acta Arith.* **97** (2001), 53–65.

[6] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, I (Character sums), *Acta Math. Hungar.*, to appear.

[7] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, II (Algebraic equations), submitted.

[8] K. F. Roth, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.

[9] A. Sárközy, On sums and products of residues modulo p, *Acta Arith.* **118** (2005), 403–409.

[10] A. Sárközy, On products and shifted products of residues modulo p, *Integers: JCNT*, to appear.

[11] J. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, *Jahresber. Deutschen Math. Verein.* **25** (1916), 114–117.

[12] B. L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wisk.* **15** (1927), 212–216.