RAMSEY TYPE RESULTS ON THE SOLVABILITY OF CERTAIN EQUATION IN $\mathbb{Z}_M$

Péter Pál Pach[1]
Department of Algebra and Number Theory, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary;
Department of Computer Science and Information Theory, Budapest University of Technology and Economics, 1521 Budapest, Magyar tudósok körútja 2., Hungary
ppp24@cs.elte.hu,ppp@cs.bme.hu

Received: , Revised: , Accepted: , Published:

Abstract

Csikvári, Gyarmati and Sárközy asked whether there exist Ramsey type theorems for the equations $a + b = cd$ and $ab + 1 = cd$ in $\mathbb{Z}_m$ for large enough m. In this paper it is proved that for any r-colouring of $\mathbb{Z}_m$ the more general equation $a_1 + \cdots + a_n = cd$ has a nontrivial monochromatic solution. Furthermore, an example is presented which shows that the corresponding statement does not hold for the equation $ab + 1 = cd$. We reformulate this problem with an additional natural condition, and give a partial positive answer.

1. Introduction

Sárközy [10], [11] proved that if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are "large enough" subsets of $\mathbb{Z}_p$, then the equations

$$a + b = cd \tag{1}$$

and

$$ab + 1 = cd \tag{2}$$

can be solved with $a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$. Gyarmati and Sárközy [5] generalized these results on the solvability of (1) and (2) to finite fields. Moreover, there are several papers written on the solvability of equations similar to (1) and (2) over a finite field, especially over $\mathbb{Z}_p$. (See for example, [3], [4].) It is natural to consider the solvability of these equations in $\mathbb{Z}_m$, as well ([8]). However, in [1] and [5] the authors note that for composite m no density-type theorem can be proved for equations (1) and (2) in $\mathbb{Z}_m$, which shows that $\mathbb{Z}_p$ and $\mathbb{Z}_m$ behave differently. Furthermore, it is

[1] *Key words and phrases*: algebraic equation, Ramsey type, solution set

asked whether there exist Ramsey type results: Is it true that for every r-colouring of $\mathbb{Z}_m$ equation (1) (or (2)) has a monochromatic solution, if r, the number of colours, is fixed and $m > N(r)$?

Problem 1. *Are there Ramsey type results on the solvability of* (1)*, resp.* (2) *in* $\mathbb{Z}_m$*?*

Hindman answered the analogue of this question over $\mathbb{N}$ positively ([6]). He showed that for every r-colouring of $\mathbb{N}$ the equation $a_1 + \dots + a_n = b_1 \dots b_n$ has a solution where not only the numbers $a_1, \dots, a_n, b_1, \dots, b_n$, but also the sums $\sum\limits_{i \in I} a_i$ (where $\emptyset \neq I \subseteq \{1, \dots, n\}$) and products $\prod\limits_{j \in J} b_j$ (where $\emptyset \neq J \subseteq \{1, \dots, n\}$) are all distinct (except $\sum\limits_{i=1}^{n} a_i$ and $\prod\limits_{j=1}^{n} b_j$), and all of these sums and products have the same colour.

In this paper we consider Problem 1 in $\mathbb{Z}_m$. First note that in the case of equation (1) trivial monochromatic solutions like $0 + 0 = 0 \cdot 0$ or $2 + 2 = 2 \cdot 2$ exist, naturally these have to be excluded. This kind of solution, where $a = b = c = d$ is called trivial. In Section 2 we prove that a nontrivial monochromatic solution of (1) always exists. On the other hand in Section 3 a counterexample is presented in the case of equation (2), namely we show a colouring of $\mathbb{Z}_m$ for infinitely many m such that (2) does not have a monochromatic solution. Therefore, instead of $m > N(r)$ the condition $p(m) > N(r)$ (where $p(m)$ denotes the smallest prime divisor of m) has to be assumed, otherwise no Ramsey type result exists. Finally, we show that the answer is affirmative to this modified question in the special case when m is a squarefree number satisfying $r \sum\limits_{p \mid m} \frac{1}{p^{1/4}} \leq \frac{1}{\sqrt{10}}$. To avoid confusion, throughout the paper the notion $(a)_m$ is going to be used for the modulo m residue class of $a \in \mathbb{Z}$ if more than one moduli are used.

2. The equation $a_1 + \dots + a_n = cd$

In this section the equation $a + b = cd$, and more generally, the equation $a_1 + \dots + a_n = cd$ will be studied. The case of prime moduli is well-known by the following theorem of Sárközy:

Theorem A (Sárközy, [10]). *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$, $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > p^3$, then equation* (1) *has a solution in $\mathbb{Z}_p$ satisfying $a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$.*

In Theorem A the prime p cannot be replaced by an arbitrary $m \in \mathbb{N}$. Moreover, there is no density theorem for equation (1) in $\mathbb{Z}_m$ for arbitrary m, that is, there exists a constant $c > 0$ such that for infinitely many m there exists a set $\mathcal{A} \subseteq \mathbb{Z}_m$ having at least cm elements such that (1) does not have a solution in $\mathcal{A}$.

Example 2.1. *Let $4|m$ and $\mathcal{A} = \{3, 7, 11, \dots, m-1\} \subseteq \mathbb{Z}_m$. The size of $\mathcal{A}$ is $\frac{m}{4}$. If $a, b, c, d \in \mathcal{A}$, then $a + b \equiv 2$ (mod 4), $cd \equiv 1$ (mod 4), hence* (1) *does not have a solution in $\mathcal{A}$.*

Now our aim is to prove that while there is no density theorem, a Ramsey type result exists for the equation $a + b = cd$ over $\mathbb{Z}_m$. Note that in general there are many trivial solutions. First we have to determine all the trivial solutions, and to do this we have to solve the congruence $a^2 \equiv 2a \pmod{m}$. Let $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ be the canonical form of the number m. By the Chinese Remainder Theorem, it is enough to determine the trivial solutions in $\mathbb{Z}_{p_i^{\alpha_i}}$. Let us denote the number of solutions of the congruence $a^2 \equiv 2a \pmod{p^\alpha}$ by $s(p^\alpha)$. The following cases have to be considered:

- $p > 2$: the congruence $a^2 \equiv 2a \pmod{p^\alpha}$ has 2 solutions, namely $a \equiv 0$ and $a \equiv 2$, hence $s(p^\alpha) = 2$.
- $p^\alpha = 2$: $a \equiv 0$ is the only solution: $s(2) = 1$.
- $p^\alpha = 4$: the 2 solutions are $a \equiv 0$ and $a \equiv 2$, so $s(4) = 2$.
- $p = 2, \alpha \geq 3$: there are four solutions: $a \equiv 0, 2, 2^{\alpha-1}, 2^{\alpha-1} + 2$, hence $s(2^\alpha) = 4$.

By the Chinese Remainder Theorem, the congruence $a + b \equiv cd \pmod{m}$ has $\prod_{i=1}^{r} s(p_i^{\alpha_i})$ trivial solutions.

Naturally, our goal is to prove that there exists a nontrivial solution of (1), as well. To see this we will show that even the more general equation

$$a_1 + \dots + a_n = cd \tag{3}$$

always has a monochromatic solution such that $a_1, \dots, a_n, c, d \in \mathbb{Z}_m$ are pairwise distinct. These solutions, where $a_1, \dots, a_n, c, d \in \mathbb{Z}_m$ are pairwise distinct, will be called primitive. The proof of this result is based on the following version of Rado's theorem ([7], Theorem 9.4):

Rado's Theorem. *Let $v \geq 2$. Let $c_i \in \mathbb{Z} \setminus \{0\}$, $1 \leq i \leq v$ be constants such that there exists a nonempty set $D \subseteq \{i : 1 \leq i \leq v\}$ with $\sum_{i \in D} c_i = 0$. If there exist distinct (not necessarily positive) integers y_i such that $\sum_{i=1}^{v} c_i y_i = 0$, then for every natural number r there exists some t such that for every r-colouring of the set $\{1, 2, \dots, t\}$ the equation*

$$c_1 x_1 + \dots + c_v x_v = 0$$

has a monochromatic solution $b_1, \dots, b_v$ in $\{1, 2, \dots, t\}$, where the b_i-s are distinct.

For more details on Rado's theorems, see [2], [7] and [9]. The following observation is also needed:

Lemma 1. *Let $T \in \mathbb{N}$ and $N = T^T$. If $m > N$, then m has a prime power divisor greater than T.*

Proof. For the sake of contradiction, suppose the contrary. Then each prime divisor of m is at most T, therefore m is the product of at most T prime powers. Since each prime power divisor is at most T, we have that $m \leq T^T$, which contradicts our assumption. □

Theorem 2. *For every $n, r \in \mathbb{N}$ there exists some $N = N(n, r)$ such that for every $N < m \in \mathbb{N}$ and every r-colouring of $\mathbb{Z}_m$ equation (3) has a primitive monochromatic solution in $\mathbb{Z}_m$.*

Proof. First assume that $n \geq 2$. Let $\alpha_i = (1-n) + 2(i-1)$ (for $i = 1, \ldots, n$),$\gamma = n, \delta = -n$. Note that the numbers $\alpha_1, \ldots, \alpha_n, \gamma, \delta$ are distinct integers and $\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0$. Therefore, the equation $\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0$ has a solution in $\mathbb{Z}$ where the α_i, γ, δ are distinct. Moreover, the sum of the coefficients of $\alpha_1, \ldots, \alpha_n, \gamma$ is $1 + \cdots + 1 - n = 0$, thus the equation $\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0$ satisfies the conditions of Rado's theorem, so the equation has a primitive monochromatic solution in $\{1, 2, \ldots, K\}$ for every r-colouring of $\{1, 2, \ldots, K\}$, if K is large enough, say $K \geq K_0$. Let $C = \max(K_0, r^4(n+2)^4)$.

Take an arbitrary r-colouring of $\mathbb{Z}_m$. By applying Lemma 1 with $T = C^3$ we obtain that if $m > N = T^T$, then m has a prime power divisor greater than T.

Now we prove that $N = T^T$ satisfies the condition of the theorem. In the proof we distinguish two cases: the prime power divisor guaranteed by Lemma 1 is itself a prime or it is not.

As the first case suppose that $p > r^4(n+2)^4$ is a prime divisor of m such that $p^2 \nmid m$. Therefore, p and m/p are coprime, since $p \nmid m/p$. For $1 \leq i \leq p$ define the mod m residue class $(x_i)_m$ by the congruences $x_i \equiv i \pmod{p}$ and $x_i \equiv 0 \pmod{m/p}$. Now, we define an r-colouring of $\mathbb{Z}_p$ depending on the given r-colouring of $\mathbb{Z}_m$ in the following way: For $1 \leq i \leq p$ let the colour of $(i)_p \in \mathbb{Z}_p$ be the colour of $(x_i)_m$. Note that $\mathbb{Z}_p$ is coloured by r colours, so we can choose (at least) $\frac{p}{r}$ elements having the same colour. Let us denote the set of these (at least) $\frac{p}{r}$ elements by $\mathcal{S}$. Now we partition $\mathcal{S} \subseteq \mathbb{Z}_p$ into $n+2$ disjoint sets $\mathcal{S}_1, \ldots, \mathcal{S}_{n+2} \subseteq \mathcal{S}$ such that the size of any two of them differ by at most 1. Since $p \geq r^4(n+2)^4 \geq 2r(n+2)$, each of the sets $\mathcal{S}_i$ has size at least $\lfloor \frac{p}{r(n+2)} \rfloor \geq \frac{p}{2r(n+2)}$. Now let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ be defined in the following way: $\mathcal{A} = \mathcal{S}_1$, $\mathcal{B} = \mathcal{S}_2 + \cdots + \mathcal{S}_n = \{s_2 + \cdots + s_n | s_2 \in \mathcal{S}_2, \ldots, s_n \in \mathcal{S}_n\}$, $\mathcal{C} = \mathcal{S}_{n+1}$, $\mathcal{D} = \mathcal{S}_{n+2}$. By $p > r^4(n+2)^4$ we obtain that $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \geq \left(\frac{p}{r(n+2)}\right)^4 > p^3$, so Theorem A can be applied, which yields that there exist $a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$ such that $a + b = cd$ in $\mathbb{Z}_p$. As $b \in \mathcal{B}$, we have $b = a_2 + \cdots + a_n$ for some $a_i \in \mathcal{S}_i$. Let $a_1 = a$. Therefore, there exist $a_1, \ldots, a_n, c, d \in \{1, 2, \ldots, p\}$ such that the corresponding mod p residue classes have the same colour, and the congruence

$$a_1 + \cdots + a_n \equiv cd \pmod{p}$$

holds. The elements $(x_{a_1})_m, \ldots, (x_{a_n})_m, (x_c)_m, (x_d)_m \in \mathbb{Z}_m$ have the same colour with $(a_1)_p, \ldots, (a_n)_p, (c)_p, (d)_p \in \mathbb{Z}_p$, moreover they are distinct, since $(a_1)_p, \ldots,$ $(a_n)_p$, $(c)_p, (d)_p \in \mathbb{Z}_p$ are distinct as well. Furthermore, $(x_{a_1})_m, \ldots, (x_{a_n})_m$, $(x_c)_m$, $(x_d)_m$ is a solution of (3), since

- $(x_{a_1})_{m/p} \ldots (x_{a_n})_{m/p} \equiv (x_c)_{m/p}(x_d)_{m/p} \pmod{m/p}$, as $x_i \equiv 0 \pmod{m/p}$ for every i, and
- $(x_{a_1})_p \ldots (x_{a_n})_p \equiv (x_c)_p(x_d)_p \pmod{p}$, as $x_i \equiv i \pmod{p}$ for every i and $a_1 \ldots a_n \equiv cd \pmod{p}$.

Hence, $(x_{a_1})_m, \ldots, (x_{a_n})_m, (x_c)_m, (x_d)_m$ form a primitive monochromatic solution of (3) in $\mathbb{Z}_m$.

As the 2nd case assume that for a prime power (but not prime) $p^t \geq C^3$ we have $p^t | m$, where $t \geq 2$ and t is the largest integer such that $p^t | m$. Let $t_0 = \lfloor t/2 \rfloor$. As $t_0 \geq t/3$, we have $p^{t_0} \geq C$. We show that a monochromatic solution of the equation $a_1 + \cdots + a_n \equiv cd \pmod{m}$ can be found among the residue classes of the form $(y \cdot \frac{m}{p^{t_0}} + n)_m$. Note that the congruence

$$\left(\alpha_1 \cdot \frac{m}{p^{t_0}} + n\right)_m + \cdots + \left(\alpha_n \cdot \frac{m}{p^{t_0}} + n\right)_m \equiv \left(\gamma \cdot \frac{m}{p^{t_0}} + n\right)_m \left(\delta \cdot \frac{m}{p^{t_0}} + n\right)_m \pmod{m} \quad (4)$$

is equivalent to

$$\alpha_1 + \cdots + \alpha_n \equiv n\gamma + n\delta \pmod{p^{t_0}}.$$

As the next step we define an r-colouring of $\mathbb{N}$ depending on the given r-colouring of $\mathbb{Z}_m$. Let the colour of $y \in \mathbb{N}$ be the colour of $(y \cdot \frac{m}{p^{t_0}} + n)_m \in \mathbb{Z}_m$.

Since $C \geq K_0$, Rado's theorem implies that there exist distinct integers $\alpha_1, \ldots,$ $\alpha_n, \gamma, \delta \in \{1, 2, \ldots, C\}$ having the same colour and satisfying $\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0$. The residue classes $a_i = (\alpha_i \cdot \frac{m}{p^{t_0}} + n)_m, c = (\gamma \cdot \frac{m}{p^{t_0}} + n)_m, d = (\delta \cdot \frac{m}{p^{t_0}} + n)_m$ give a solution of (3), moreover they are distinct, since $\alpha_1, \ldots, \alpha_n, \gamma, \delta \in \{1, 2, \ldots, C\}$ are distinct and $p^{t_0} \geq C$.

Finally, let us examine the case when $n = 1$. By Rado's theorem for every $r \in \mathbb{N}$ there exists some $M = M(r)$ such that for every r-colouring of $\mathbb{N}$ the equation $\alpha = \gamma + \delta$ has a primitive monochromatic solution in $\{1, \ldots, M\}$. Suppose that $2^M < m$ and take an arbitrary r-colouring of $\mathbb{Z}_m$. Define a colouring of $\mathbb{N}$ in the following way: Let the colour of $a \in \mathbb{N}$ be the colour of $(2^a)_m$ in $\mathbb{Z}_m$. Rado's theorem yields that there exist three distinct positive integers $\alpha, \gamma, \delta \in \{1, \ldots, M\}$ having the same colour such that $\alpha = \gamma + \delta$. Then $a = (2^\alpha)_m, c = (2^\gamma)_m, d = (2^\delta)_m$ is a primitive monochromatic solution of $a = cd$ in $\mathbb{Z}_m$.

Hence, we showed that if $m > N = T^T$, then (3) has a nontrivial monochromatic solution in $\mathbb{Z}_m$.

□

3. The equation $ab + 1 = cd$

In this section equation (2) will be studied. First, we will show that if m has a small prime divisor, then there is no Ramsey type theorem on the solvability of $ab + 1 = cd$ in $\mathbb{Z}_m$ in the classical sense: If we fix the number of colours r and m is large enough, then a monochromatic solution need not exist.

Example 3.1. *Let $p|m$ and the colour of $(x)_m \in \mathbb{Z}_m$ be the mod p residue class containing x. If $(a)_m, (b)_m, (c)_m, (d)_m \in \mathbb{Z}_m$ have the same colour, then $ab \equiv cd \pmod p$, so $ab + 1 \neq cd$ in $\mathbb{Z}_m$.*

In this example we coloured $\mathbb{Z}_m$ by p colours, where $p|m$, and there is no monochromatic solution of the equation $ab + 1 = cd$, which shows that the least prime divisor of m, denoted by $p(m)$, has to be greater than the number of colours. To exclude counterexamples of this kind we reformulate the problem in the following way:

Problem 2. *Are there Ramsey type results on the solvability of $ab + 1 = cd$ in $\mathbb{Z}_m$ if r, the number of colours is fixed and $p(m)$ is large enough in terms of r?*

We give a partial positive answer to this question, namely we show that the answer is affirmative, if m is squarefree and

$$r \sum_{p|m} \frac{1}{p^{1/4}} \leq \frac{1}{\sqrt{10}}.$$

To prove this result the following theorem of Sárközy is needed:

Theorem B (Sárközy, [11]). *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$, $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > 100p^3$, then the equation $ab + 1 = cd$ has a solution in $\mathbb{Z}_p$ satisfying $a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$.*

Now we are ready to solve Problem 2 under a certain condition.

Theorem 3. *Let $m = p_1 \ldots p_s$ be the product of s different primes. Let $\mathcal{A} \subseteq \mathbb{Z}_m$ and $\alpha = \frac{|\mathcal{A}|}{m}$. If $\displaystyle\sum_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \frac{\alpha}{\sqrt{10}}$, then there exist $a, b, c, d \in \mathcal{A}$ satisfying the equation $ab + 1 = cd$.*

Proof. The main idea of the proof is to solve the congruence system $ab + 1 \equiv cd \pmod{p_i}$ (for $1 \leq i \leq s$) step by step. Our aim is to obtain a solution finally where $(a)_m, (b)_m, (c)_m, (d)_m$ lie in $\mathcal{A}$. As the first step we show that the following statement holds: Let $m = m_1 m_2 \dots m_s$, where $m_1, m_2, \dots, m_s$ are pairwise coprime. Let $\mathcal{A} \subseteq \mathbb{Z}_m = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$, $\alpha = \frac{|\mathcal{A}|}{m}$ and $\alpha_1, \dots, \alpha_s \geq 0$ satisfying $\alpha_1 + \cdots + \alpha_s \leq \alpha$. Then there exist sets $\mathcal{A}_1 \subseteq \mathbb{Z}_{m_1}$, $\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{m_j}$ (for every $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2(a_1)$, and so on, $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \dots, a_{j-2})$) satisfying the following conditions:

- $|\mathcal{A}_1| \geq \alpha_1 m_1$
- For every $2 \leq j \leq r$, for every $a_1 \in \mathcal{A}_1$, for every $a_2 \in \mathcal{A}_2(a_1)$, for every $a_3 \in \mathcal{A}_3(a_1, a_2)$ and so on, for every $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \dots, a_{j-2})$ the set $\mathcal{A}_j(a_1, \dots, a_{j-1})$ has at least $\alpha_j m_j$ elements.
- If $a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2(a_1), \dots, a_s \in \mathcal{A}_s(a_1, \dots, a_{s-1})$, then $(a_1, \dots, a_s) \in \mathcal{A}$.

So $\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{m_j}$ contains at least $\alpha_j m_j$ possible continuations of the vector $(a_1, \dots, a_{j-1}) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{j-1}}$. More precisely, we could add at least $\alpha_j m_j$ elements $a_j \in \mathbb{Z}_{m_j}$ as the j-th coordinate to the vector $(a_1, \dots, a_{j-1})$ such that after the s-th step we have vectors belonging to $\mathcal{A} \subseteq \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$.

We prove this assertion by induction on s. For $s = 1$ the statement holds trivially. Let $s = 2$. Let $\mathcal{A}_2(a_1) = \{a_2 \in \mathbb{Z}_{m_2} : (a_1, a_2) \in \mathcal{A}\}$. Then let $\mathcal{A}_1 = \{a_1 \in \mathbb{Z}_{m_1} : |\mathcal{A}_2(a_1)| \geq \alpha_2 m_2\}$. As $\mathcal{A} = \bigcup\limits_{a_1 \in \mathcal{A}_1} \{a_1\} \times \mathcal{A}_2(a_1) \cup \bigcup\limits_{a_1 \in \mathbb{Z}_{m_1} \setminus \mathcal{A}_1} \{a_1\} \times \mathcal{A}_2(a_1)$, we have

$$\alpha m_1 m_2 = |\mathcal{A}| \leq |\mathcal{A}_1| m_2 + (m_1 - |\mathcal{A}_1|)\alpha_2 m_2 \leq |\mathcal{A}_1| m_2 + \alpha_2 m_1 m_2.$$

Thus the size of $\mathcal{A}_1$ is at least $\alpha_1 m_1$, as needed. Applying this repeatedly we get that the statement is true for every $s > 2$ as well.

This implies that in $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$ at least $\alpha_1 m_1$ first coordinates can be chosen, the set $\mathcal{A}_1$ contains them. For every $a_1 \in \mathcal{A}_1$, $\alpha_2 m_2$ second coordinates can be chosen, the set $\mathcal{A}_2(a_1)$ contains them. And so on. Finally, $\alpha_s m_s$ s-th coordinates can be chosen in such a way that all of the elements $(a_1, a_2, \dots, a_s)$ obtained in $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$ lie in $\mathcal{A}$.

As the second step let $m = p_1 \dots p_s$. As $\mathbb{Z}_m = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$ by the Chinese Remainder theorem, the modulo m residue class of a can be identified by an ordered s-tuple where the jth coordinate is the mod p_j residue of the residue class of a: $a \leftrightarrow (a_1, \dots, a_s)$, where $(a)_{p_j} = (a_j)_{p_j}$ for every $1 \leq j \leq s$. Solving the equation $ab + 1 = cd$ in $\mathcal{A} \subseteq \mathbb{Z}_m$ is equivalent to solve the system of equations $a_i b_i + 1 = c_i d_i$ in $\mathbb{Z}_{p_i}$ (where $1 \leq i \leq s$) in such a way that $(a_1, \dots, a_s), (b_1, \dots, b_s), (c_1, \dots, c_s), (d_1, \dots, d_s) \in \mathcal{A}$. We have just proved that for every $\alpha_1, \dots, \alpha_s \geq 0$ satisfying $\alpha_1 + \cdots + \alpha_s \leq \alpha$ subsets $\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{p_j}$ can be chosen which satisfy the following conditions:

- $|\mathcal{A}_1| \geq \alpha_1 p_1$.
- For every $2 \leq j \leq s$, for every $a_1 \in \mathcal{A}_1$, for every $a_2 \in \mathcal{A}_2(a_1)$, for every $a_3 \in \mathcal{A}_3(a_1, a_2)$ and so on, for every $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \ldots, a_{j-2})$ the set $\mathcal{A}_j(a_1, \ldots, a_{j-1})$ has at least $\alpha_j p_j$ elements,
- If $a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2(a_1), \ldots, a_s \in \mathcal{A}_s(a_1, \ldots, a_{s-1})$, then $(a_1, \ldots, a_s) \in \mathcal{A}$.

As a next step we are going to apply Theorem B repeatedly. In order to do this the inequalities $(\alpha_j p_j)^4 \geq 100 p_j^3$ $(1 \leq j \leq s)$ have to hold. Therefore, let $\alpha_j = \frac{\sqrt{10}}{p_j^{1/4}}$ (for every $1 \leq j \leq s$). Now note that $\sum\limits_{j=1}^{s} \alpha_j = \sqrt{10} \sum\limits_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \alpha$, so the previous statement can be applied, and the sets $\mathcal{A}_j(a_1, \ldots, a_{j-1})$ can be chosen. As $|\mathcal{A}_1| \geq \alpha_1 p_1$, Theorem B yields that the equation $a_1 b_1 + 1 = c_1 d_1$ (in $\mathbb{Z}_{p_1}$) can be solved in $\mathcal{A}_1$. Fix this solution. Since each of the sets $\mathcal{A}_2(a_1), \mathcal{A}_2(b_1), \mathcal{A}_2(c_1), \mathcal{A}_2(d_1)$ has cardinality at least $\alpha_2 p_2$, the equation $a_2 b_2 + 1 = c_2 d_2$ (in $\mathbb{Z}_{p_2}$) has a solution such that $a_2 \in \mathcal{A}_2(a_1), b_2 \in \mathcal{A}_2(b_1), c_2 \in \mathcal{A}_2(c_1), d_2 \in \mathcal{A}_2(d_1)$. In the general step $a_1, \ldots, a_j, b_1, \ldots, b_j, c_1, \ldots, c_j, d_1, \ldots, d_j$ are already fixed. Since each of the sets $\mathcal{A}_{j+1}(a_1, \ldots, a_j)$, $\mathcal{A}_{j+1}(b_1, \ldots, b_j)$, $\mathcal{A}_{j+1}(c_1, \ldots, c_j)$, $\mathcal{A}_{j+1}(d_1, \ldots, d_j)$ has cardinality at least $\alpha_{j+1} p_{j+1}$, the equation $a_{j+1} b_{j+1} + 1 = c_{j+1} d_{j+1}$ (in $\mathbb{Z}_{p_{j+1}}$) has a solution such that $a_{j+1} \in \mathcal{A}_{j+1}(a_1, \ldots, a_j)$, $b_{j+1} \in \mathcal{A}_{j+1}(b_1, \ldots, b_j)$, $c_{j+1} \in \mathcal{A}_{j+1}(c_1, \ldots, c_j)$, $d_{j+1} \in \mathcal{A}_{j+1}(d_1, \ldots, d_j)$. At the end, since each of the sets $\mathcal{A}_s(a_1, \ldots, a_{s-1})$, $\mathcal{A}_s(b_1, \ldots, b_{s-1})$, $\mathcal{A}_s(c_1, \ldots, c_{s-1})$, $\mathcal{A}_s(d_1, \ldots, d_{s-1})$ has cardinality at least $\alpha_s p_s$, the equation $a_s b_s + 1 = c_s d_s$ (in $\mathbb{Z}_{p_s}$) has a solution such that $a_s \in \mathcal{A}_s(a_1, \ldots, a_{s-1})$, $b_s \in \mathcal{A}_s(b_1, \ldots, b_{s-1})$, $c_s \in \mathcal{A}_s(c_1, \ldots, c_{s-1})$, $d_s \in \mathcal{A}_s(d_1, \ldots, d_{s-1})$.

Therefore, for $a = (a_1, \ldots, a_s), b = (b_1, \ldots, b_s), c = (c_1, \ldots, c_s), d = (d_1, \ldots, d_s) \in \mathcal{A}$ we have $ab + 1 = cd$ (in $\mathbb{Z}_m$).

□

Corollary 4. *Let $m = p_1 \ldots p_s$ be the product of s different primes. If $r \sum\limits_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \frac{1}{\sqrt{10}}$, then for every r-colouring of $\mathbb{Z}_m$ the equation $ab+1 = cd$ has a monochromatic solution.*

4. Acknowledgements

The author is thankful to A. Sárközy for turning his attention to this topic and for the useful hints.

References

[1] P. Csikvári, K. Gyarmati, A. Sárközy: *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica, to appear.

[2] R. L. Graham, B. L. Rotschild, J. H. Spencer: *Ramsey Theory.* Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, 1990.

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

[4] K. Gyarmati, A. Sárközy: *Equations in finite fields with restricted solution sets, I. (Character sums)*, Acta Math. Hungar. 118 (2008), 129-148.

[5] K. Gyarmati, A. Sárközy: *Equations in finite fields with restricted solution sets, II (Algebraic equations)*, Acta Math. Hungar. 119 (2008), 259-280.

[6] N. Hindman: *Monochromatic sums equal to products in* $\mathbb{N}$, Integers 11A (2011), Article 10, 1-10.

[7] B. M. Landman, A. Robertson: *Ramsey Theory on the Integers*, American Mathematical Society, 2003.

[8] C. Pomerance, A. Schinzel: *Multiplicative properties of sets of residues*, Moscow J. Combin. and Number Theory 1 (2011), 52–66.

[9] R. Rado: *Studien zur Kombinatorik*, Math. Z. 36 (1) (1933), pp. 424-470.

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

[11] A. Sárközy: *On products and shifted products of residues modulo p*, Integers 8 (2008), A9, 8pp.