Balanced sets and the vector game

Zhivko Nedev[*] Anthony Quas[†]

March 24, 2008

Abstract

We consider the notion of a balanced set modulo N. A nonempty set S of residues modulo N is balanced if for each $x \in S$, there is a d with $0 < d \leq N/2$ such that $x \pm d \bmod N$ both lie in S. We define $\alpha(N)$ to be the minimum cardinality of a balanced set modulo N. This notion arises in the context of a two-player game that we introduce and has interesting connections to the prime factorization of N.

We demonstrate that for p prime, $\alpha(p) = \Theta(\log p)$, giving an explicit algorithmic upper bound and a lower bound using finite field theory and show that for N composite, $\alpha(N) = \min_{p|N} \alpha(p)$.

1 Introduction

Most of our work will concern the following problem. A nonempty subset of $\{0, \ldots, N-1\}$ will be called *balanced modulo* N if each element x is the midpoint of two elements of the set that are distinct from x. That is, a set S is balanced if for all $x \in S$, there is a solution to the following equation:

$$2x = y + z \pmod{N} \text{ where } y, z \in S \setminus \{x\}. \tag{1}$$

Given a set S, a point $x \in S$ will be said to be *balanced with respect to* S if there is a solution to the above equation; this means that a set is balanced if all of its elements are balanced with respect to the set.

Problem 1. *For an integer $N > 1$, what is the size of a smallest balanced set modulo N? How can such a set be constructed algorithmically?*

We define $\alpha(N)$ to be the minimal size of a balanced set modulo N.

Example. *For $N = 13$, $\alpha(13) = 6$ and one balanced set modulo 13 of minimal size is $\{0, 1, 2, 3, 5, 8\}$. This is because 0 is balanced by 5 and 8, 1 by 0 and 2, 2 by 1 and 3, 3 by 1 and 5, 5 by 2 and 8, and finally 8 is balanced by 0 and 3 as well as by 1 and 2.*

Notice that if N is even (say $N = 2k$), then $\{0, k\}$ is a balanced set as $2(k) = 0 + 0 \bmod N$ and $2(0) = k + k \bmod N$ (it is not required that the y and z in the definition of balanced set be distinct). Accordingly, we have $\alpha(N) = 2$ for N even. In the case that N is odd and y and z agree, then one can see that there are no solutions to (1). Thus in the odd case which is the only interesting case by the above observation, the x, y and z appearing in (1) will all be distinct.

[*] Univ. of Victoria, znedev@gmail.com.

[†] Univ. of Victoria, aquas@uvic.ca.

Similarly, if $N = 3k$ where k is odd, it is not hard to see that $\alpha(N) = 3$ by considering the set $\{0, k, 2k\}$. More generally, if $N = mn$, one can see that $\alpha(N) \leq \alpha(m)$ since if S is a balanced set modulo m, then nS, the set of all elements of S multiplied by n may be checked to be a balanced set modulo $nm = N$. We will show below that $\alpha(mn) = \min(\alpha(m), \alpha(n))$.

2 Application for small Balanced Sets

We first establish a connection to the following two-player game that we call the minimal variant of the *Vector Game*. The game is played at a circular table with N seats consecutively labelled 0 to $N-1$. The two players are called Magnus and Derek. If the current position is i, a round consists of Magnus calling a magnitude ℓ with $0 < \ell \leq N/2$ and after which Derek calling a direction ($+$ or $-$). The position is then updated to $i + \ell \bmod N$ or $i - \ell \bmod N$ according to whether Derek called $+$ or $-$. Magnus's aim in the game is to minimize the cardinality of the set of all positions occupied in the course of the game (while Derek's is to maximize it).

The maximal variant of the game has been studied in [2] (where it was called the Magnus-Derek game). In this variant, instead of minimizing the eventual set of occupied positions, Magnus's goal was to maximize the set of occupied positions. In [2], a simple formula was given (in terms of the prime factorization of N) for the size of such a set if both players play optimally.

Returning to the minimal variant, we claim that

Proposition 1. *$\alpha(N)$ is precisely the eventual size of the occupied set if both players play optimally.*

Proof. To see this, note that given any balanced set S, if a round starts with the current position x belonging to S, then since S is balanced, there exist y and z also belonging to S such that $2x = y + z$. Equivalently, y and z may be expressed as $x \pm \ell \pmod N$. Accordingly Magnus calls ℓ for the magnitude and whichever direction Derek chooses, the play remains in the set S. Since a balanced set may be translated to contain the initial position, it follows that Magnus has a strategy to ensure that no more than $\alpha(N)$ positions are occupied, irrespective of Derek's strategy.

Conversely, consider the following strategy for Derek. At each turn he is presented with a pair (x, ℓ) consisting of the current position x and the magnitude ℓ selected by Magnus. The strategy for Derek is to alternate: the first time a given pair arises, he chooses $x + \ell$ or $x - \ell$ according to which position has not yet been occupied, or arbitrarily if neither or both have been occupied. On subsequent occasions when he is presented with (x, ℓ) he simply makes the opposite choice to his previous choice. We consider the set A of pairs (x, ℓ) that arise infinitely often in the sequence of plays. Since there are finitely many pairs, the set A is non-empty. Letting S be the projection of A onto the first coordinate, we claim that S is balanced. To see this, note that given $x \in S$, there is a pair (x, ℓ) that is called infinitely often, so that the current position is infinitely often $x + \ell$ and infinitely often $x - \ell$. Since there are only finitely many magnitudes, there must by a pair $(x + \ell, \ell')$ that arises infinitely often in the sequence of plays. Similarly, there must be an $(x - \ell, \ell'')$ that arises infinitely often. Accordingly $x \pm \ell \in S$ and we see that S is balanced, so that the set of positions visited infinitely often has cardinality at least $\alpha(N)$. In fact, using the results below, one can prove that there exists a strategy for Derek forcing visits to at least $\alpha(N)$ sites within $O((\log N)^2)$ steps. □

Our next aim is to establish that for a prime p, a smallest balanced set has $\Theta(\log p)$ elements. We give an upper bound using an algorithmic construction of a balanced set and a lower bound using finite fields.

3 Lower Bound

In [1], Browkin, Diviš, and Schinzel proved (among other things) that for any subset S of a field L of characteristic p with size $|S| < \log_2 p + 1$, there exists a $z \in L$ represented uniquely as $z = x + y$, $x, y \in S$. Since they work with ordered representations, only sums of the form $x + x$, $x \in S$ can be unique. In fact, Browkin et al. prove that every S with $|S| < \log_2 p + 1$ is unbalanced. It follows then from their paper that $\alpha(p) \geq \log_2 p + 1$.

Without knowing about their paper, we proved that $\alpha(p) \geq \frac{1}{\log_2 \sqrt{6}} \log_2 p + 1$. Our proof rediscovers the techniques used in [1]. Initially, we used Hadamard's inequality instead of the determinant inequality from [3] that Browkin et al. use. We offer here our original proof, modified to use the more powerful inequality from [3]. This proof is more specific (for the field $\mathbb{Z}_p$) and much shorter than the proof in [1].

Proposition 2. *Let $p > 2$ be a prime number. Then $\alpha(p) \geq \log_2 p + 1$.*

Proof. Let $\alpha(p) = m$ so that there exists at least one balanced set S modulo p of cardinality m. We label the elements of S in increasing order so that $0 \leq e_1 < e_2 < \ldots < e_m \leq p - 1$.

Since p is odd, as remarked earlier, each e_n is balanced by two *distinct* elements of $S \setminus \{e_n\}$, e_{i_n} and e_{j_n}, say. Accordingly, we have that $e = (e_1, \ldots, e_m)^T$ is a solution to the following system of equations:

$$\begin{aligned} 2e_1 - e_{i_1} - e_{j_1} &= 0 \bmod p \\ 2e_2 - e_{i_2} - e_{j_2} &= 0 \bmod p \\ &\cdots \\ 2e_m - e_{i_m} - e_{j_m} &= 0 \bmod p \end{aligned}$$

This can be written in matrix form as $\mathbf{C}e = 0 \bmod p$, where e has all different components and $\mathbf{C}$ is an $m \times m$ matrix with the following two properties.

1) In each row the coefficient on the main diagonal is $+2$, two other coefficients are -1 and the remaining coefficients are zero.

2) Given any partition $E \cup F$ of $\{1, \ldots, m\}$ into two nonempty sets, there exist $i \in E$ and $j \in F$ such that $C_{i,j} = -1$ (We use $C_{i,j}$ to denote the (i, j) entry of the matrix $\mathbf{C}$).

The first condition is immediate and the second condition is a consequence of the minimality of the set S as we now show. Supposing that there were a partition $E \cup F$ such that for all $i \in E$ and $j \in F$, $C_{i,j} = 0$. In this case, each element e_i for $i \in E$ would be the average of two further (distinct) elements of $S_E = \{e_k \colon k \in E\}$ and S_E would be a smaller balanced set.

We call the class of $m \times m$ matrices satisfying the above conditions $\mathcal{A}(m)$. We call the matrix $\mathbf{C}$ a *balancing matrix* of S modulo p.

Example. *For our first example with $S = \{0, 1, 2, 3, 5, 8\}$ as a smallest balanced set modulo 13 we can derive two balancing matrices. The first is:*

$$\begin{pmatrix} 2 & 0 & 0 & 0 & -1 & -1 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 0 & 2 & -1 & 0 \\ 0 & 0 & -1 & 0 & 2 & -1 \\ -1 & 0 & 0 & -1 & 0 & 2 \end{pmatrix}$$

Since $e_6 = 8$ is balanced also by $e_2 = 1$ and $e_3 = 2$, we can replace the last row with the row $(0 \; -1 \; -1 \quad 0 \quad 0 \quad 2)$ to get the second balancing matrix.

Example. *The following matrix does not belong to $\mathcal{A}(5)$:*

$$\begin{pmatrix} 2 & 0 & -1 & 0 & -1 \\ -1 & 2 & 0 & -1 & 0 \\ -1 & 0 & 2 & 0 & -1 \\ 0 & -1 & -1 & 2 & 0 \\ -1 & 0 & -1 & 0 & 2 \end{pmatrix}$$

This is because setting $E = \{1, 3, 5\}$ and $F = \{2, 4\}$, the second condition fails.

Lemma 3. *Let the matrix $\mathbf{C}$ belong to $\mathcal{A}(m)$. Then the rank of $\mathbf{C}$ over $\mathbb{Q}$ is $m - 1$.*

Proof. Consider the null space of $\mathbf{C}$, $\mathrm{Null}(\mathbf{C}) = \{x \in \mathbb{Q}^m : \mathbf{C}x = 0\}$. Since the vector $(1, 1, 1, \ldots, 1)^T$ belongs to $\mathrm{Null}(\mathbf{C})$, it follows that $\mathrm{Null}(\mathbf{C})$ has dimension at least 1.

Now let $x \in \mathbb{Q}^m$ be such that $\mathbf{C}x = 0$. We want to prove that $x_1 = x_2 = \ldots = x_m$. Suppose that the x_i are not all the same, let $E = \{i \colon x_i = \min_j x_j\}$ and $F = \{1, \ldots, m\} \setminus E$. By assumption, this is a non-trivial partition, so since $\mathbf{C} \in \mathcal{A}(m)$, there exist $i \in E$ and $j \in F$ such that $C_{i,j} = -1$, so that we have $2x_i = x_j + x_k$ (where k is position of the other -1 in the ith row of $\mathbf{C}$) and $2 \min_\ell x_\ell = x_j + x_k$. Since $x_k \geq \min_\ell x_\ell$ and $x_j > \min_\ell x_\ell$, this gives a contradiction.

It follows that $\mathrm{Null}(\mathbf{C})$ consists of multiples of $(1, \ldots, 1)^T$ so that $\dim(\mathrm{Null}(\mathbf{C})) = 1$.

Considering the linear transformation $L : Q^m \to Q^m$ defined by $L(x) = \mathbf{C}x$, the rank–nullity theorem of Linear Algebra gives $\mathrm{rank}(\mathbf{C}) + \dim(\mathrm{Null}(\mathbf{C})) = \dim(\mathbb{Q}^m) = m$ so that $\mathrm{rank}_{\mathbb{Q}}(\mathbf{C}) = m - 1$. □

Now consider the linear transformation $L^* : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$, defined by $L^*(x) = \mathbf{C}x \bmod p$.

Lemma 4. *If S is a balanced set modulo p and $\mathbf{C}$ is the balancing matrix of S, then rank$(\mathbf{C}) \leq m-2$ over $\mathbb{Z}_p$.*

Proof. By our observations above, $\mathbf{C}$ belongs to the class $\mathcal{A}(m)$ and $x = (1, 1, 1, \ldots, 1)^T$ is a trivial solution to $\mathbf{C}x = 0$. By construction of the matrix $\mathbf{C}$, we have also $\mathbf{C}e = 0 \bmod p$, where e is the vector representation of the balanced set S. It follows that $\mathrm{Null}(\mathbf{C})$ has dimension at least 2. Appealing to the rank–nullity theorem again, the lemma follows.

□

Combining Lemmas 3 and 4, we see that the balancing matrix of S satisfies:

1) $\operatorname{rank}_{\mathbb{Q}}(\mathbf{C}) = m - 1$

2) $\operatorname{rank}_{\mathbb{Z}_p}(\mathbf{C}) \leq m - 2$

From linear algebra, we have that over any field the determinant rank of $\mathbf{C}$ equals the row (column) rank of $\mathbf{C}$, where the determinant rank of $\mathbf{C}$ is the largest positive integer r such that there exists an $r \times r$ submatrix of $\mathbf{C}$ with non-zero determinant.

Accordingly, the matrix $\mathbf{C}$ has an $(m-1) \times (m-1)$ submatrix $\mathbf{C}'$ with non-zero determinant over $\mathbb{Q}$. On the other hand, it also follows that $\mathbf{C}'$ has a zero determinant over $\mathbb{Z}_p$. Since the matrix $\mathbf{C}'$ is an integer matrix, the determinant over $\mathbb{Z}_p$ is just the residue of the determinant over $\mathbb{Q}$ reduced modulo p. It follows that $p|\det(\mathbf{C}')$ and in particular, $|\det(\mathbf{C}')| \geq p$.

We consider the row vectors in $\mathbf{C}'$, and note that for each row we have $|\text{row}_i| \leq \sqrt{6}$. We then apply Hadamard's inequality:

$$p \leq \left|\det(\mathbf{C}')\right| \leq \prod_{i=1}^{m-1} |\text{row}_i| \leq (\sqrt{6})^{m-1} \quad \text{implying that} \quad \alpha(p) = m \geq \frac{1}{\log_2 \sqrt{6}} \log_2 p + 1.$$

Now let us denote the elements of $\mathbf{C}'$ by $(a_{ij})_{1 \leq i,j \leq m-1}$. To obtain a stronger lower bound, we apply the inequality from [3]:

$$p \leq \left|\det(\mathbf{C}')\right| \leq \prod_{i=1}^{m-1} \max\{\sum_{j=1,a_{ij}>0}^{m-1} a_{ij}, -\sum_{j=1,a_{ij}<0}^{m-1} a_{ij}\} = 2^{m-1}$$

yielding the desired conclusion: $\alpha(p) = m \geq \log_2 p + 1$. □

4 Upper Bound

We first establish a simple upper bound. Let $k = \lfloor \log_2 N \rfloor$ and $\Delta = N - 2^k$. Clearly $0 < \Delta < 2^k$. Initially, let S be the set consisting of the five residues $\{0, \pm 2^{k-1}, \pm[2^{k-1} - \Delta]\}$. These elements are balanced for $N = 7$, so assume that $N > 7$. Then in S, only $\pm[2^{k-1} - \Delta]$ are unbalanced. We will proceed algorithmically to add elements to S until all elements in S are balanced. Of our two initially unbalanced elements $\pm[2^{k-1} - \Delta]$, exactly one of these, say T, is in $[0, 2^{k-1}]$. Let $[L, R]$ denote the *current interval*, with $L = 0$ and $R = 2^{k-1}$ initially. For these initial values we have $L, R \in S$. We now repeat the following step:

Let $M = \frac{L+R}{2}$, and add $\pm M$ to S. Note that M is balanced by $\{L, R\}$, and $-M$ is balanced by $\{-R, -L\}$. Of the two subintervals $[L, M]$ and $[M, R]$, choose the one that contains T and let it be the new *current interval*, again denoted $[L, R]$. Repeat until $R - L = 1$.

On each step, the new elements $\pm M$ are balanced, and on the last step, M coincides with T. Therefore, when the algorithm stops, $\pm T$ are balanced, and we have obtained a balanced set S with $|S| = 2k + 1$. Thus $\alpha(N) \leq 2\lfloor \log_2 N \rfloor + 1$.

Next we will use the following trivial observation. *Every subset S of $\mathbb{Z}_p$ which is symmetric about a point, say 0, is balanced iff no difference of elements from S occurs exactly once, i.e. if $a, b \in S$, then there must exist $x, y \in S$, not the same as a, b, such that $a - b = x - y$.*

The observation follows from three properties of such sets: First, in a set S symmetric about 0, for any $a, b \in S$ with $b \neq -a$, their difference $a - b$ occurs also as $(-b) - (-a)$. Second, if 0 is in S, it has many balancing pairs of the form $\{x, -x\}$. Third, $\forall x \in S, x - (-x) = 2x$ and $-x \in S$, so $x - (-x)$ is non-unique iff $2x = y - z = y + (-z)$ with $y, (-z) \in S \setminus \{x\}$.

In [4], Straus studies sets of residues mod p with unique differences and for the upper bound he presents two constructions of small size subsets of $\mathbb{Z}_p$ with non-unique differences. Although he does not deal with (un)balanced sets, both of his constructions are symmetric about zero, and due to the above observation provide examples of balanced sets. His first construction has size $2\lfloor \log_2 N \rfloor + 1$; his second construction gives a better upper bound. He proves the following theorem.

Theorem 5. *For any $\epsilon > 0$ and sufficiently large p there exist a symmetric about 0 set of residues $(\mathrm{mod}\ p)$ with fewer than $(2 + \epsilon)\log_3 p$ elements so that no difference occurs exactly once.*

By combining theorem 5 and proposition 2, we obtain the following theorem.

Theorem 6. *For p prime, we have*

$$\log_2 p + 1 \leq \alpha(p) \leq (2 + o(1)) \log_3 p.$$

5 $\alpha(N)$ for N composite

Theorem 7. *Let $N > 1$. We have $\alpha(N) = \min_{p|N} \alpha(p)$, where the minimum is taken over all primes p dividing N.*

Lemma 8. *If $M|N$ where $M > 1$ then $\alpha(N) \leq \alpha(M)$.*

Proof. If S is a balanced set modulo M then $(N/M)S$ is a balanced set modulo N. □

Lemma 9. *Let $M|N$ and let S be a balanced set modulo N that is minimal under inclusion. Then $S \bmod M$ is balanced or consists of a single point.*

Proof. Let the elements of S be $s_1, \ldots, s_\ell$. Since S is balanced modulo N, for each $i \in \{1, \ldots, \ell\}$, there are a_i, b_i distinct from i such that $2s_i = s_{a_i} + s_{b_i} \pmod{N}$. We then define a directed graph on the vertex set $\{1, \ldots, \ell\}$ with constant out-degree 2. Each vertex i is connected to vertices a_i and b_i. Note that this directed graph may not be unique as there may be more than one choice of the a_i and b_i. We claim that this graph is strongly connected. If not, then there is a proper subset U of $\{1, \ldots, \ell\}$ such that all edges leaving vertices in U go to vertices in U. In this case, the set $\{s_i \colon i \in U\}$ is a proper subset of S, which can easily be seen to be balanced contradicting the minimality of S under inclusion.

Now consider the set $T = S \bmod M$ and suppose that T is not a singleton. Let $x \in T$ and let $U = \{i \leq \ell \colon s_i \equiv x \pmod{M}\}$. Since the digraph above is strongly connected, there exists a vertex $i \in U$ and a vertex $j \notin U$ such that $i \to j$ (so that $j = a_i$ or $j = b_i$). It follows that at least one of (and hence by the balance condition both of) a_i and b_i do not belong to U. Now $2s_i = s_{a_i} + s_{b_i} \pmod{N}$, so reducing modulo M we see that $2x = (s_{a_i} \bmod M) + (s_{b_i} \bmod M) \pmod{M}$. Since a_i and b_i do not belong to U, this shows that x is balanced in T as required. □

Proof of Theorem 7. From Lemma 8, we see that $\alpha(N) \leq \min_{p|N} \alpha(p)$. It remains to prove that given N, there is a $p|n$ with $\alpha(p) \leq \alpha(N)$.

Let S be a balanced set modulo N of minimum cardinality and let $N = p_1^{\beta_1} \dots p_k^{\beta_k}$. We consider the reductions $S \bmod p_i^{\beta_i}$ (for $i = 1, \dots, k$) and note that from the Chinese Remainder Theorem, there is an i for which $S \bmod p_i^{\beta_i}$ is not a singleton.

Now let $j \geq 1$ be the smallest integer such that $S \bmod p_i^j$ is not a singleton (in particular $j \leq \beta_i$). Since S was of minimum cardinality, it is certainly a minimal balanced set modulo N by inclusion and hence by Lemma 9, we see that $S \bmod p_i^j$ is balanced. By the choice of j, $S \bmod p_i^{j-1}$ is a singleton, $\{r\}$ say. It then follows that $S - r \bmod p_i^j$ is balanced and consists of multiples of p_i^{j-1}. Hence $(S - r)/p_i^{j-1} \bmod p_i$ is a balanced set modulo p_i so that $\alpha(p_i) \leq \alpha(N)$. □

6 Numerical Data

Using a simple exhaustive search algorithm, we calculated $\alpha(p)$ for all primes up to 650. This data turned out to be astonishingly regular. Defining m_k to be the smallest p for which $\alpha(p) = k$, the function essentially takes the value 2 for p in a range $[m_2, m_3)$, 3 for p in a range $[m_3, m_4)$, and in general k for p in a range $[m_k, m_{k+1})$, so that the function appears to be essentially non-decreasing (any decrease is rare, it is always isolated and its value is one). The first decrease occurs for $p = 43$: $\alpha(41) = 8$, $\alpha(43) = 7$ and $\alpha(47) = 8$ again. The next decreases only occur between $\alpha(571) = 12$ and $\alpha(577) = 11$; $\alpha(593) = 12$ and $\alpha(599) = 11$. These are the only decreases for $p < 650$. In addition, the m_k at which the function jumps also appear to increase in a very regular exponential manner. We have $m_2 = 2$, $m_3 = 3$, $m_4 = 5$, $m_5 = 7$, $m_6 = 13$, $m_7 = 23$, $m_8 = 41$, $m_9 = 79$, $m_{10} = 157$, $m_{11} = 283$, $m_{12} = 569$. It is striking how close they are to doubling at each step.

Fitting least squares data to these jump points, the best approximation is $\alpha(p) \approx \lfloor 2.52 + 1.04 \log_2 p \rfloor$, so that $1.52 + 1.04 \log_2 p \lesssim \alpha(p) \lesssim 2.52 + 1.04 \log_2 p$ (here the symbol $\lesssim$ means approximately less than or equal). The graphs of $\alpha(p)$, $1.52 + 1.04 \log_2 p$ and $2.52 + 1.04 \log_2 p$ are shown (in a log-linear scale) in Figure 1.

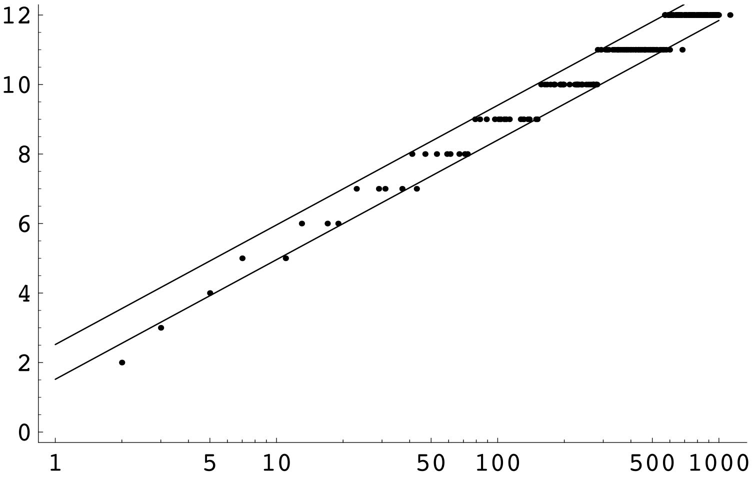

Figure 1: Log-Linear Relationship between p and $\alpha(p)$

7 Conclusions and Open Problems

If S is a balanced set modulo N, then obviously the translation by $a \in \mathbb{Z}$ and the scaling by d, $(d, N) = 1$, lead to balanced sets $a + S$ and dS. Thus if N is prime, without loss of generality we can assume that a balanced set satisfies $0 \in S$ and $\pm 1 \in S$.

Problem 2. *Is a minimal (or at least a smallest) balanced set unique up to translations and scalings? At least in the case of prime N?*

The following two related open problems are of interest only for integers N without a trivially small factor.

Problem 3. *Is the problem of finding a smallest balanced set easier or more difficult than integer factorization?*

Problem 4. *Is it possible to compute $\alpha(N)$ without knowing the factorization of N?*

The new problem is remarkably different in one respect from factorization: it admits approximate solutions. Any balanced subset of $\mathbb{Z}_N$ of small size can be considered as an approximate solution to it. Accordingly the following question arises: Is there an algorithm for finding an approximate value/solution of our new problem?

8 Acknowledgments

In connection to this paper, we are very grateful to the following people and places for their advice, discussions and support: Jeffrey O. Shallit; Valerie King; Uriel Feige; Noam Sturmwind; S. Muthu Muthukrishnan; Mario Szegedy; the School of Computer Science at University of Waterloo and the DIMACS Center.

References

[1] J. Browkin, B. Diviš, and A. Schinzel. Addition of sequences in general fields. 1976. Monatshefte für Mathematik **82**, pp. 261-268.

[2] Z. Nedev and S. Muthukrishnan. The Magnus-Derek game. 2008. Theoretical Computer Science.

[3] A. Schinzel. An inequality for determinants with real entries. Colloq. Math. 38 (1977), 319-321.

[4] E. G. Straus. Differences of residues (mod p). 1976. J. Number Theory **8**, pp. 40-42.