UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

ON SOLUTIONS IN ARITHMETIC PROGRESSIONS TO HOMOGENOUS SYSTEMS OF LINEAR EQUATIONS

by Jonas Lindstrøm Jensen

Preprint Series No.: 2
February 2009
2009/02/26

Ny Munkegade, Bldg. 1530
DK-8000 Aarhus C, Denmark
http://www.imf.au.dk
institut@imf.au.dk

On solutions in arithmetic progressions to homogenous systems of linear equations

Jonas Lindstrøm Jensen*

Abstract

We consider subsets of the natural numbers that contains infinitely many aritmetic progressions (APs) of any given length – such sets will be called AP-sets and we know due to the Green-Tao Theorem that the primes is an AP-set. We prove that the equation

$$M\underline{x} = 0,$$

where M is an integer matrix whose null space has dimension at least 2, has infinitely many solutions in any AP-set such that the coordinates of each solution are elements in the same AP, if and only if $(1, 1, \ldots, 1)$ is a solution.

We will furthermore prove that AP-sets are exactly the sets that has infinitely many solutions to a homogeneous system of linear equations, whenever the sum of the columns is zero.

1 Introduction

The existence of different kinds of additive structures in the primes is a field of research that has drawn much attention. Recently Ben Green and Terrence Tao [1] has proved the existence of arbitrarily long arithmetic progressions in the primes and Granville [3] has considered several additive structures that can be found using the results of Green and Tao. Inspired by this we are looking for solutions in any subset of the integers that contains arbitrarily long aritmethic progressions to homogeneous systems of linear equations – in particular solutions consisting of primes.

Balog [4] gave a lower bound on the number of prime solutions to a homogeneous system of linear equations $M\underline{x} = 0$ if the matrix M has a certain admissible structure, the null space contains a vector with positive coordinates and $M\underline{x} \equiv 0 \pmod{p}^{\alpha}$ has integer solutions coprime to p for all prime powers p^{α}. In particular he proved that if M is admissible and $(1, 1, \ldots, 1)$ is

*Email: jonas@imf.au.dk

a solution, then $M\underline{x} = 0$ has prime solutions. Choi, Liu and Tsang [5] has considered upper bounds for prime solutions to ternary linear equations.

In this paper we will prove that we have infinitely many solutions to a system of linear equations in a set with arbitrarily long arithmetic progressions if the null space of the matrix has dimension at least 2 and contains $(1, 1, \dots, 1)$. Due to the Green-Tao Theorem the primes is such a set and due to Szemeredi's Theorem [2] all subsets of the integers with positive density are such sets.

The main result in this paper is that the method here also gives us that for each of the solutions the coordinates are in the same arithmetic progression, and that the sets that contain arithmetic progressions of any length are exactly the sets that have infinitely many solutions to a homogeneous system of linear equations whenever the sum of the columns is zero. This gives us a new arithmetic structure on such sets and a new formulation of the Erdős-Turan Conjecture.

The results in this paper have been found while working on my master thesis and I would like to thank my supervisors Jørgen Brandt and Simon Kristensen for their help. I would furthermore like to thank Andrew Granville for reading and commenting on the results.

2 APs and GAPs

As we are considering arithmetic progressions the following notation will come in handy.

Definition 1 (Arithmetic progressions)**.** Let $k, d \geq 1$ and $a \geq 0$ be integers. Then an *arithmetic progression* (AP) of length k, base a and step d is the set

$$\mathrm{AP}(k, a, d) = \{a + \lambda d \mid 0 \leq \lambda < k\}.$$

We consider subsets of N that contains arbitrarily large arithmetic progressions. We will call these sets AP-sets and define them as follows.

Definition 2 (AP-set)**.** Let $A \subseteq \mathbb{N}$. We will call A an *AP-set* if there for any $k \geq 1$ exists a pair $(a, d) \in \mathbb{N}^2$ such that

$$\mathrm{AP}(k, a, d) \subseteq A.$$

Remark 3. Notice that an AP-set contains infinitely many APs of any length.

We will now consider generalizes arithmetic progressions which we define as follows.

Definition 4 (Generalized arithmetic progressions)**.** Let $d \geq 1$, $a \geq 0$, $b_1, \dots, b_d \geq 1$ and $N_1, \dots, N_d \geq 1$ be integers. Then a *generalized arithmetic progression* (GAP) of dimension d, base a, step $(b_1, \dots, b_d)$ and volume $(N_1, \dots, N_d)$ is the set

$$\{a + n_1 b_1 + \dots + n_d b_d \mid 0 \leq n_i < N_i \text{ for all } i\}.$$

Remark 5. Notice that a GAP of dimension d, base a, step $(b_1, \ldots, b_d)$ and volume $(2N_1 - 1, \ldots, 2N_d - 1)$ can be written as

$$\{a' + n_1 b_1 + \cdots + n_d b_d \mid -N_i < n_i < N_i \text{ for all } i\} \tag{1}$$

where $a' = a + (N_1 - 1)b_1 + \cdots + (N_d - 1)b_d$.

We can construct a GAP of any dimension and volume from a sufficiently long AP, so in particular an AP-set contains infinitely many GAPs of any given dimension and volume. The following lemma is taken from [3] and gives us a little more than just GAPs in AP-sets.

Lemma 6. *Any AP-set containts infitely many GAPs of any given dimension and volume such that each GAP is contained in an AP.*

3 Finding solutions in an AP-set

Using the existence of GAPs in AP-sets we can now find infinitely many solutions to systems of linear equations in any AP-set.

Theorem 7. *Let $n \geq 3$ and $m \geq 1$ and let $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Assume that the solution space of*

$$M\underline{x} = 0 \tag{2}$$

has dimension $d \geq 2$ and contains $(1, 1, \ldots, 1)$. Then (2) has infinitely many solutions in any given AP-set with the coordinates of a solution being elements in the same AP and not all equal.

Proof. The solution space of (2) can be written as

$$m_1\underline{r}_1 + m_2\underline{r}_2 + \cdots + m_d\underline{r}_d, \quad m_i \in \mathbb{R}$$

where $\underline{r}_1 = (1, 1, \ldots, 1)$, $\underline{r}_i = (r_{i1}, \ldots, r_{in}) \in \mathbb{Z}^n$ for $2 \leq i \leq d$ and $\underline{r}_1, \ldots, \underline{r}_d$ are linearly independent over $\mathbb{R}$. Now let $N = \max_{i,j} |r_{ij}| + 1$ and take a GAP of dimension $d - 1$ and volume $(2N - 1, \ldots, 2N - 1)$. According to Lemma 6 we can construct GAPs of any given size such that it is contained in an AP. Now take such a GAP, and as we did in (1) we write it as

$$\{a + n_1 b_1 + \cdots + n_{d-1} b_{d-1} \mid -N < n_i < N \text{ for all } i\}. \tag{3}$$

Now

$$a\underline{r}_1 + b_1\underline{r}_2 + \cdots + b_{d-1}\underline{r}_d$$

is a solution to (2) and each coordinate is an element in the GAP given in (3). Now assume that the solution we have found has all coordinates equal. Then it is equal to $c\underline{r}_1$ for some $c \in \mathbb{N}$ so

$$(a - c)\underline{r}_1 + b_1\underline{r}_2 + \cdots + b_{d-1}\underline{r}_d = 0.$$

This is not possible since $\underline{r}_1, \ldots, \underline{r}_d$ are linearly independent. $\square$

4 Prime-like sets

Theorem 7 on the previous page gives us a sufficient condition to be able to find infinitely many solutions in an AP-set. Let us now examine in what way it also is a nescessary condition. To examine this we need to require a bit more from our AP-set.

Definition 8 (Prime-like sets)**.** A set $A \subseteq \mathbb{N}$ is called *prime-like* if for each $\mathrm{AP}(k,a,d) \subseteq A$ with $k \geq 3$ we have $\gcd(a,d) = 1$.

Notice that the primes is prime-like because if we have a progression $\mathrm{AP}(k,a,d)$ in the primes, then a is prime and d is even.

Theorem 9. *Let A be a prime-like AP-set, $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and $k \geq 3$. Assume that*

$$M\underline{x} = 0 \tag{4}$$

has infinitely many solutions such that for each solution $(x_1, \ldots, x_n)$ there is $(a,d) \in \mathbb{N}^2$ such that

$$\{x_1, \ldots, x_n\} \subseteq AP(k,a,d) \subseteq A.$$

Then $(1,1,\ldots,1)$ is a solution to (4).

Proof. Let $1 \leq i \leq m$ be given. Assume for contradiction that $a_{i1} + \cdots + a_{in} \neq 0$. Let $\{(x_1^{(j)}, \ldots, x_n^{(j)}) \mid j \in \mathbb{N}\}$ be the infinitely many solutions given in the lemma. For each $j \in \mathbb{N}$ there exist b_j and d_j such that $x_l^{(j)} = b_j + \lambda_l^{(j)} d_j$ with $0 \leq \lambda_l^{(j)} < k$ for all $l = 1, \ldots, n$ since each $x_l^{(j)}$ is an element of $\mathrm{AP}(k, b_j, d_j)$. Inserting this in (4) we get that we for each $j \in \mathbb{N}$ have

$$b_j(a_{i1} + \cdots + a_{in}) = -d_j(a_{i1}\lambda_1^{(j)} + \cdots + a_{in}\lambda_n^{(j)}).$$

Since $\gcd(b_j, d_j) = 1$, b_j must divide $a_1\lambda_1^{(j)} + \cdots + a_n\lambda_n^{(j)}$ so if we let $C = |a_{i1}| + \cdots + |a_{in}|$ we have $b_j \leq Ck$. Now

$$|d_j| = \left| b_j \frac{a_1 + \cdots + a_n}{a_1\lambda_1^{(j)} + \cdots + a_n\lambda_n^{(j)}} \right| \leq Ck$$

so the set $\{d_j \mid j \in \mathbb{N}\}$ is also finite. The solutions $\{(x_1^{(j)}, \ldots, x_n^{(j)}) \mid j \in \mathbb{N}\}$ are therefore taken from only finitely many APs of length k, and there can hence be only finitely many of them. This is a contradiction against the assumption, and this finishes the proof. $\square$

Combining this with Theorem 7 on the preceding page we get the following.

Theorem 10. *Let A be a prime-like AP-set and let $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ such that the null space of M has dimension at least 2. Then there is a $k \in \mathbb{N}$ such that the equation*

$$M\underline{x} = 0$$

has infinitely many solutions where for each solution, all coordinates are elements of the same AP of length k if and only if $(1, 1, \ldots, 1)$ is a solution.

We now give an example of an application of Theorem 7 on page 3. This is a known result, see for instance [3].

Corollary 11. *Let an AP-set A and $n \geq 1$ be given. Then there exists infinitely many n-tuples in $x_1, \ldots, x_n \in A$ with $x_i \neq x_j$ for some i, j such that*

$$\frac{x_1 + \cdots + x_n}{n} \in A.$$

Proof. When $n = 1$ it is trivial so let $n \geq 2$ be given. Consider the linear equation

$$x_1 + \cdots + x_n - nx_{n+1} = 0.$$

From Theorem 7 on page 3 we know that this equation has infinitely many solutions $x_1, \ldots, x_n, x_{n+1} \in A$ with $x_i \neq x_j$ for some i, j. Now for each of these we have

$$\frac{x_1 + \cdots + x_n}{n} = x_{n+1} \in A,$$

which finishes the proof. □

5 Zero-solution sets

We have proven that in any AP-set we can find infinitely many solutions to any system of linear equation, as long as the sum of the columns of the matrix is zero. This motivates the following definition.

Definition 12 (Zero-solution sets)**.** Let $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ such that the sum of the columns is zero and the null space of M has dimension at least 2. A set $A \subseteq \mathbb{N}$ is a *zero-solution set* if

$$M\underline{x} = 0$$

has infinitely many solutions $\underline{x} = (x_1, \ldots, x_n)$ with $x_1, \ldots, x_n \in A$ and $x_i \neq x_j$ for some i, j.

Now Theorem 7 on page 3 can be formulated as follows: If A is an AP-set then A is a zero-solution set. We now want to prove that zero-solution sets and AP-sets are the same.

Theorem 13. *Let $A \subseteq \mathbb{N}$. Then A is a zero-solution set if and only if A is an AP-set.*

Proof. The 'if' part we get from Theorem 7 on page 3. Let $n \geq 3$ be an integer and let $M \in \mathrm{Mat}_{n-2,n}(\mathbb{Z})$ be given such that the solution space of $M\underline{x} = 0$ is given by

$$m_1(1, 1, \ldots, 1) + m_2(0, 1, 2, \ldots, n-1), \quad m_1, m_2 \in \mathbb{R}.$$

Since A is a zero-solution set there are infinitely many solutions in A with $m_2 \neq 0$. We also see that such a solution is in A so it is integer and both m_1 and m_2 are hence integer. Each of these solutions gives us an AP of length n. $\square$

This result gives us a new formulation of the Erdős-Turan conjecture [6],

$$\sum_{a \in A} \frac{1}{a} = \infty \;\Rightarrow\; A \text{ is a zero-solution set.}$$

References

[1] Ben Green & Terence Tao (2008), The Primes Contain Arbitrarily Long Arithmetic Progressions, *Ann. of Math. (2) vol. 167 no. 2*, pp. 481–547.

[2] Endre Szemerédi (1975), On sets of integers containing no k elements in arithemetic progression, *Acta Arith. 27*, pp. 299–345.

[3] Andrew Granville (2008), Prime Number Patterns, *American Mathematical Monthly, vol. 115*, pp. 279–296.

[4] Antal Balog (1992), Linear Equations in Primes, *Mathematika, vol. 39*, pp. 367–378.

[5] Choi, Lui and Tsang (1992), Conditional bounds for small prime solutions of linear equations, *Manuscripta math. col 74*, pp. 321–340.

[6] Paul Erdős and P. Turán (1936), On Some Sequences of Integers, *J. London Math. Soc. 11*, pp. 261–264.