

# ROTH'S THEOREM ON ARITHMETIC PROGRESSIONS

ALEX IOSEVICH

September 17, 2003

The purpose of this paper is to provide a simple and self-contained exposition of the celebrated Roth's theorem on arithmetic progressions of length three. The original result is proved in [Roth53], while the proof given below is very similar to the exposition of Roth's original argument given in [GRS1990].

**Definition.** We say that a subset of positive integers  $A$  has positive upper density if

$$(1) \quad \limsup_N \frac{|A \cap [1, N]|}{N} > 0.$$

**Roth's Theorem.** *If  $A$  is a subset of positive integers of positive upper density, then  $A$  contains a three term arithmetic progression.*

**Basic setup.** Let  $S(n)$  denote the largest number of integers in  $[1, n]$  that can be chosen so that no three term arithmetic progression is formed. Let

$$(2) \quad c = \lim_{n \rightarrow \infty} \frac{S(n)}{n}.$$

The existence of this limit exists follows from the fact that  $S : \mathbb{Z}^+ \rightarrow \mathbb{R}$  is a sub-additive function. The (easy) details are left to the reader.

Let

$$(3) \quad \epsilon = \frac{c^2}{10^6},$$

and let  $m$  be large enough so that

$$(4) \quad c \leq \frac{S(n)}{n} < c + \epsilon \text{ for } 2m + 1 \leq n.$$

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$

Let  $2N$  be sufficiently large in the sense that will become clear below. Let  $A \subset \{1, 2, \dots, 2N\}$  with  $|A| \geq 2Nc$  which contains no arithmetic progressions of length three. Let

$$(5) \quad A = \{u_1, u_2, \dots, u_r\}.$$

Let  $A_{\text{even}}$  denote the set of even elements of  $A$ ,

$$(6) \quad A_{\text{even}} = \{2v_1, 2v_2, \dots, 2v_s\}; \quad \frac{1}{2}A_{\text{even}} = \{v_1, v_2, \dots, v_s\}.$$

By assumption,

$$(7) \quad 2Nc \leq r \leq 2N(c + \epsilon),$$

and

$$(8) \quad N(c - \epsilon) \leq s \leq N(c + \epsilon).$$

**Fourier transform.** Let

$$(9) \quad \widehat{A}(\alpha) = \sum_{i=1}^r e(\alpha u_i),$$

and

$$(10) \quad \widehat{A_{\text{even}}}(\alpha) = \sum_{j=1}^s e(\alpha v_j),$$

where

$$(11) \quad e(t) = e^{2\pi i t}.$$

As we shall see below, the key to the proof of Roth's theorem is to show that away from  $\alpha = 0$ ,  $|\widehat{A}(\alpha)|$  is much smaller than  $N$ , the number of terms in the sum. The idea behind this is that the enemy of an exponential sum is presence of arithmetic progression. These progressions play the same role in the discrete Fourier transforms as that of lack of curvature in the decay properties of the Fourier transform of a surface carried measure.

**The basic idea.** Let  $\int$  denote the sum over  $\alpha = \frac{i}{2N}$ ,  $i = 0, 1, \dots, 2N - 1$ . Observe that

$$(12) \quad \int e(\alpha u) = 2N \text{ if } u = 0, \text{ and } 0 \text{ otherwise.}$$

The key observation is that

$$(13) \quad \int \widehat{A}(\alpha) (\widehat{A_{even}})^2(-\alpha) = 2N \#\{(i, j, k) : u_i - v_j - v_k = 0; u_i \in A, v_j, v_k \in \frac{1}{2}A_{even}\}.$$

Why is this important? If  $u_i - v_j - v_k = 0$ , then the set

$$(14) \quad \{2v_j, u_i, 2v_k\}$$

is an arithmetic progression of length three, except for the trivial cases when

$$(15) \quad 2v_j = u_i = 2v_k.$$

By assumption our  $A$  does not contain arithmetic progressions of length three, therefore the right hand side of (13) equals

$$(16) \quad 2Ns < 3cN^2,$$

where the inequality follows by (8).

We shall obtain a contradiction in the following manner. First,

$$(17) \quad \widehat{A}(0) (\widehat{A_{even}})^2(0) = rs^2 > c^3 N^3.$$

On the other hand,

$$(18) \quad \widehat{A}(0) (\widehat{A_{even}})^2(0) < \left| \int \widehat{A}(\alpha) (\widehat{A_{even}})^2(-\alpha) \right| + \left| \int_{\alpha \neq 0} \widehat{A}(\alpha) (\widehat{A_{even}})^2(-\alpha) \right| = I + II.$$

We already know that

$$(19) \quad I \leq 3cN^2.$$

We will see that

$$(20) \quad II \leq 18\epsilon cN^3.$$

This will be accomplished as follows. We will show that when  $\alpha \neq 0$ ,

$$(21) \quad |\widehat{A}(\alpha)| \leq 6\epsilon N.$$

This is the main estimate of the paper which we shall carry out shortly. With (21) in tow, we complete the proof in the following way. We observe that

$$(22) \quad II \leq \left( \max_{\alpha \neq 0} |\widehat{A}(\alpha)| \right) \int |(\widehat{A_{even}}(-\alpha))^2| \leq 6\epsilon N \int |(\widehat{A_{even}}(-\alpha))^2|,$$

so (20) would follow if we could show that

$$(23) \quad \int |\widehat{A_{even}}(-\alpha)|^2 \leq 3cN^2.$$

To establish (23) observe that the left hand side of (23) equals

$$(24) \quad \sum_{j=1}^s \sum_{k=1}^s \int e(\alpha(v_j - v_k)) = 2Ns \leq 3cN^2$$

by (8) and (12).

Using (17), (18), (19), and (20) we see that

$$(25) \quad c^3N^3 \leq 3cN^2 + 18\epsilon cN^3,$$

which is not possible if  $N$  is sufficiently large. Thus the proof of Roth's theorem is reduced to establishing (21).

**Estimate (21).** We need the following basic fact about diophantine approximation which can be found in any book on elementary number theory and/or deduced easily from the pigeon-hole principle. For  $\alpha$  arbitrary and  $M > 0$ , there exist integers  $p, q$  with

$$(26) \quad \alpha = \frac{p}{q} + \beta, \quad 1 \leq q \leq M \text{ and } q|\beta| \leq \frac{1}{M}.$$

We also need the following elementary estimate which we do not prove...

$$(27) \quad \left| \frac{1}{2}(e(x) + e(-x)) - 1 \right| = |\cos(x) - 1| \leq \frac{x^2}{2}.$$

The first step in establishing the estimate (21) is "smearing". More precisely, we show that

$$(28) \quad \left| \widehat{A}(\alpha) - \frac{1}{2m+1} \sum_A \sum_{|i| \leq m} e(\alpha(u + iq)) \right| \leq \frac{|A|m^2}{2M^2} \leq \frac{Nm^2}{2M^2}.$$

We shall then estimate the "smeared" part by showing that

$$(29) \quad \left| \frac{1}{2m+1} \sum_A \sum_{|i| \leq m} e(\alpha(u + iq)) \right| \leq 5N\epsilon.$$

Combining (28) and (29) yields (21).

We first establish (28), which is a bit easier. From (27) we deduce that

$$(30) \quad \left| \frac{1}{2m+1} \sum_{|i| \leq m} [e(\alpha + i\gamma) - e(\alpha)] \right| \leq \frac{(m\gamma)^2}{2}.$$

Let  $M$  denote the largest integer smaller than  $\sqrt{N}$ . Let  $\alpha \neq 0$  and let  $p, q, \beta$  be as in (26) above. Then

$$(31) \quad e(\alpha(u + iq)) = e(\alpha u + i(\beta q)).$$

It follows that

$$(32) \quad \left| \frac{1}{2m+1} \sum_{|i| \leq m} [e(\alpha(u + iq)) - e(\alpha u)] \right| = \left| e(\alpha u) - \frac{1}{2m+1} \sum_{|i| \leq m} e(\alpha(u + iq)) \right| \\ \leq \frac{(m\beta q)^2}{2} \leq \frac{m^2}{2M^2},$$

and (28) follows instantly.

We now turn our attention to (29). Let

$$(33) \quad W_s = \{s + iq : |i| \leq m\} \text{ calculated modulo } 2N.$$

It follows that

$$(34) \quad \frac{1}{2m+1} \sum_A \sum_{|i| \leq m} e(\alpha(u + iq)) = \sum_{s=0}^{2N-1} e(\alpha s) \frac{|W_s \cap A|}{2m+1}.$$

We want to show that

$$(35) \quad \left| \sum_{s=0}^{2N-1} e(\alpha s) \frac{|W_s \cap A|}{2m+1} \right| \leq 5N\epsilon$$

which will establish (29).

From (35), (34) and (28) it will then follow that

$$(36) \quad |\widehat{A}(\alpha)| \leq \frac{m^2 N}{2M^2} + 5N\epsilon \leq 6N\epsilon$$

for a sufficiently large  $N$  which will establish (21).

We now prove (35). Let

$$(37) \quad E_s = \frac{|W_s \cap A|}{2m+1} - c.$$

Observe that for  $mq \leq s \leq 2N - mq$ ,  $W_s$  forms an arithmetic progression of length  $2m+1$  in  $\{1, 2, \dots, 2N\}$ . It follows that

$$(38) \quad |W_s \cap A| \leq (2m+1)(c + \epsilon)$$

by (7). It follows that for these values of  $s$ ,  $E_s \leq \epsilon$ . For the other  $2mq$  values of  $s$  we use the trivial bound  $E_s \leq 1$ .

Our next observation is that the average value of  $E_s$  is positive. Indeed, since each  $a \in A$  appears in exactly  $2m+1$  sets  $W_s$ , we have

$$(39) \quad \frac{1}{2m+1} \sum_{s=0}^{2N-1} |W_s \cap A| = |A| \frac{2m+1}{2m+1} = |A|,$$

so

$$(40) \quad \frac{\sum_{s=0}^{2N-1} E_s}{2N} = \frac{|A|}{2N} - c,$$

which is a positive number.

Now, using (40) and the discussion following (38),

$$(41) \quad \sum_{s=0}^{2N-1} |E_s| \leq 2 \sum_{0 \leq s \leq 2N-1: E_s > 0} E_s \leq 2(2N\epsilon + 2mq) \leq 4\epsilon N + 4mM \leq 5N\epsilon$$

if  $N$  is sufficiently large.

For  $\alpha \neq 0$ ,  $\sum_{s=0}^{2N-1} e(\alpha s) = 0$ , so

$$(42) \quad \left| \sum_{s=0}^{2N-1} e(\alpha s) \frac{|W_s \cap A|}{2m+1} \right| = \left| \sum_{s=0}^{2N-1} e(\alpha s) E_s \right| \leq \sum_{s=0}^{2N-1} |E_s| \leq 5N\epsilon.$$

This establishes (35) and proof of Roth's theorem is complete.

#### REFERENCES

- [GRS1990] R. Graham, B. Rothschild, and J. Spencer, *Ramsey theory*, John Wiley and Sons, Inc. (1990).
- [Roth53] K. Roth, *On certain sets of integers*, J. London Math Soc. **28** (1953), 104-109.