

# Roth's Theorem on Arithmetic Progressions

Ernie Croot

April 23, 2004

## 1 Introduction

Here we give a proof of the following classical theorem of K. F. Roth:

**Theorem 1** *There exists a constant  $c > 0$  so that for all  $x$  sufficiently large, if  $S$  is a subset of the integers in  $[1, x]$  having at least  $cx/\log \log x$  elements, then  $S$  must contain a three-term arithmetic progression.*

Throughout the next section we will make use of the discrete Fourier transform, which is defined as follows: If  $f$  is a mapping from  $\mathbb{Z}/N\mathbb{Z}$  to the complex numbers, then we define the Fourier transform of  $f$  to be

$$\hat{f}(a) = \sum_{n=0}^{N-1} f(n)\omega^{an},$$

where  $\omega = e^{2\pi i/N}$ . We will also make use of Parseval's identity, which says that

$$\sum_{a=0}^{N-1} |\hat{f}(a)|^2 = N \sum_{n=0}^{N-1} |f(n)|^2.$$

## 2 The Proof

Suppose  $|S| = \epsilon x$ , and let  $N = 2x$ . Then, we have that the set of 3APs of  $S$  in the integers coincides with the set of 3APs in  $S$  modulo  $N$ . Now, to count

the number of 3APs of  $S$  modulo  $N$ , if we think of  $S$  as a subset of residue classes modulo  $N$ , we can associate to it the indicator function

$$S(n) = \begin{cases} 1, & \text{if } n \in S; \\ 0, & \text{if } n \notin S. \end{cases}$$

Then, we define  $\hat{S}(a)$  to be the Fourier transform of this indicator function as in the Introduction.

Next, we define the function  $f(n)$  to be  $\epsilon$  if  $1 \leq n \leq x$ , and to be 0 if  $x < n \leq N - 1$  or  $n = 0$ . One can think of this function as a “smoothed-out” version of  $S(n)$ , since the sum of the values of  $f(n)$  and  $S(n)$  are both equal to  $\epsilon x$ , and since  $f(n)$  and  $S(n)$  are both 0 for  $x < n \leq N - 1$ .

We now define the balanced function  $T(n) = S(n) - f(n)$ , which has Fourier transform  $\hat{T}(a) = \hat{S}(a) - \hat{f}(a)$ .

It is easy to verify the identity

$$\begin{aligned} \frac{1}{N} \sum_{a=0}^{N-1} \hat{S}(a)^2 \hat{T}(-2a) &= \frac{1}{N} \sum_{a=0}^{N-1} \hat{S}(a)^2 \hat{S}(-2a) - \frac{1}{N} \sum_{a=0}^{N-1} \hat{S}(a)^2 \hat{f}(-2a) \\ &= \#(\text{3AP's in } S) - \epsilon(O^2 + E^2) \\ &\leq \#(\text{3AP's in } S) - \epsilon \frac{|S|^2}{2}, \end{aligned} \tag{1}$$

where  $O$  is the number of odd integers in  $S$ , and where  $E$  is the number of even integers in  $S$ . Note that  $O^2 + E^2$  counts the number of ordered pairs  $(u, v) \in S \times S$  such that  $u$  and  $v$  both have the same parity. Here, a 3AP means a triple  $(u, v, w) \in S \times S \times S$  satisfying  $u + v = 2w$ . Note that this counts both trivial and non-trivial triples, where by “trivial” we mean those where  $u = v = w$ .

Suppose we were lucky and had that for all  $a = 0, \dots, N - 1$ ,

$$|\hat{T}(a)| < \delta |S|. \tag{2}$$

Then, by Parseval’s identity, we have that

$$\frac{1}{N} \left| \sum_{a=0}^{N-1} \hat{S}(a)^2 \hat{T}(-2a) \right| < \frac{\delta |S|}{N} \sum_{a=0}^{N-1} |\hat{S}(a)|^2 = \delta |S|^3.$$

Combining this with (1) gives that

$$\#(\text{3AP's in } S) \geq \frac{\epsilon |S|^2}{2} - \delta |S|^3.$$

So, for  $\delta < \epsilon/3$ , say, this would give that  $S$  has “lots” of 3AP’s; in fact, since  $S$  contains only  $|S|$  trivial triples, this would give that  $S$  must contain at least  $\epsilon|S|^2/3 - |S|$  non-trivial 3AP’s, which is just what we wanted to show.

The idea is to now show that if (2) doesn’t hold, then there is an arithmetic progression

$$P = \{b, b + d, b + 2d, \dots, b + hd\} \subset [1, x], \quad \text{where } |P| > \sqrt{x}/\log x, \quad (3)$$

such that  $S$  has “increased density on  $P$ ”, in the sense that

$$\frac{|S \cap P|}{|P|} > \epsilon \left(1 + \frac{\delta}{2}\right). \quad (4)$$

Then, by translating and rescaling  $S \cap P$ , we can produce a new set of integers  $S_2$  lying in  $[1, y]$ , where  $y = \sqrt{x}/\log x$ , such that  $S_2$  has a 3AP implies  $S$  has a 3AP. By iterating the above argument (of showing that if  $\hat{T}(a)$  is “large” for some  $a$ , then there is an AP on which  $S$  has increased density), at some point we either get a set  $S_j$  having “lots” of 3AP’s, or else we get a sequence of sets of integers

$$S_1 = S, S_2, S_3, \dots, S_k, \quad \text{where } S_i \subset [1, y_i],$$

where

$$k > \alpha(\log \log x), \quad \text{for some } \alpha > 0,$$

such that for  $i = 2, \dots, k$ ,

$$\frac{|S_i|}{y_i} > \left(1 + \frac{\delta}{2}\right) \frac{|S_{i-1}|}{y_{i-1}}, \quad \text{where } y_i = \sqrt{y_{i-1}}/\log y_{i-1}.$$

This obviously cannot hold for a fixed  $\epsilon \in (0, 1]$  and for  $x$  sufficiently large, since for  $\delta = \epsilon/3$  we would have

$$\frac{|S_k|}{y_k} > \left(1 + \frac{\delta}{2}\right)^{k-1} \epsilon > \epsilon \exp(\kappa \epsilon \log \log x) > 1,$$

where  $\kappa > 0$  is some constant. Thus,  $S$  would have to contain a 3AP, as claimed.

If one refines this argument, one can show that if  $|S| > cx/\log \log x$ , then  $S$  must contain a 3AP, as claimed by the Theorem in the Introduction.

Let us now see that if (2) fails to hold for some  $a$ , then there exists  $P$  as in (3) such that (4) holds. First, we claim that there exists an integer  $1 \leq d \leq \sqrt{x}$  such that  $da/N \equiv \gamma \pmod{1}$ , where  $|\gamma| < 1/\sqrt{x}$ : To see this, consider the set  $\{ja/N \pmod{1} : 0 \leq j \leq \sqrt{x}\}$ . Since the set contains  $> \sqrt{x}$  elements, there must exist a pair  $0 \leq j_1 < j_2 \leq \sqrt{x}$  such that  $j_1a/N \equiv j_2a/N + \gamma \pmod{1}$ , where  $|\gamma| < 1/\sqrt{x}$ . Setting  $d = j_2 - j_1$  then gives the result.

Now, we have for  $0 \leq j \leq \sqrt{x}/\log x$  that

$$\omega^{(b+jd)a} = \omega^b \omega^{jda} = \omega^b (1 + O(j/\sqrt{x})) = \omega^b + O(1/\log x),$$

since the fractional part of  $jda/N$  is of size at most  $j/\sqrt{x}$ . Now consider the sum

$$F = \sum_{1 \leq b \leq x(1-1/\log x)} \left| \sum_{0 \leq j \leq \sqrt{x}/\log x} S(b+jd) - f(b+jd) \right|.$$

We will relate this sum to  $\hat{T}(a)$  as follows: We have that

$$\begin{aligned} F &= \sum_{1 \leq b \leq x(1-1/\log x)} \left| \sum_{0 \leq j \leq \sqrt{x}/\log x} (S(b+jd) - f(b+jd)) \omega^{(b+jd)a} \right| + O(x\sqrt{x}/\log^2 x) \\ &\geq \left| \sum_{1 \leq b \leq x(1-1/\log x)} \sum_{0 \leq j \leq \sqrt{x}/\log x} T(b+jd) \omega^{(b+jd)a} \right| + O(x\sqrt{x}/\log^2 x) \\ &= \left| \sum_{n \leq x} r(n) T(n) \omega^{an} \right| + O(x\sqrt{x}/\log^2 x), \end{aligned}$$

where  $r(n)$  is the number of pairs of integers  $(b, j)$ ,  $0 \leq j \leq \sqrt{x}/\log x$ , and  $1 \leq b \leq x(1-1/\log x)$ , such that  $b+jd = n$ . Now, for  $n \in [x/\log x, (1-1/\log x)x]$  we have that  $r(n) = \lfloor \sqrt{x}/\log x \rfloor + 1$ . Thus,

$$\begin{aligned} F &> (\sqrt{x}/\log x) \left| \sum_{1 \leq n \leq x} T(n) \omega^{an} \right| + O(x\sqrt{x}/\log^2 x) \\ &= (\sqrt{x}/\log x) |\hat{T}(a)| + O(x\sqrt{x}/\log^2 x) \\ &> \frac{\delta |S| \sqrt{x}}{\log x} + O(x\sqrt{x}/\log^2 x) \\ &= \frac{\delta \epsilon x \sqrt{x}}{\log x} + O(x\sqrt{x}/\log^2 x), \end{aligned}$$

Thus, with a little work, one can show for one of the integers  $1 \leq b \leq x(1 - 1/\log x)$  that

$$\sum_{0 \leq j \leq \sqrt{x}/\log x} S(b + jd) - f(b + jd) > \frac{\delta \epsilon \sqrt{x}}{\log x} + O(\sqrt{x}/\log^2 x).$$

Thus, since  $f(b + jd) = \epsilon$  for these values of  $j$ , we deduce that

$$\sum_{0 \leq j \leq \sqrt{x}/\log x} S(b + jd) > \frac{\epsilon \sqrt{x}}{\log x} \left(1 + \frac{\delta}{2}\right),$$

for  $x$  sufficiently large. Thus,  $S$  has density at least  $\epsilon(1 + \delta/2)$  on the progression  $P = \{b + jd : 0 \leq j \leq \sqrt{x}/\log x\}$ , as claimed.