The set of $a^2 + b$ is Large

February 18, 2011

1 Introduction

Here we prove the following theorem:

Theorem 1 *Suppose that $A \subseteq \mathbb{F}_p$, and suppose that $2 \leq |A| < p^{1/2}$. Then,*

$$|\{a^2 + b \ : \ a, b \in A\}| \ > \ |A|^{1+c},$$

for some constant $c > 0$.

2 Theorems and Lemmas We Will Need

First, we will require a few basic results on the theory of set addition:

Theorem 2 (Plunnecke-Ruzsa Theorem) *Suppose that U is a finite subset of an abelian group G, and suppose that*

$$|U + U| \ < \ K|U|.$$

Then,

$$|hU - kU| \ < \ K^{h+k}|U|.$$

Theorem 3 (Gowers-Balog-Szemeredi) *Suppose that A is a subset of an additive group for which we have the energy condition $E(A, A) \geq \gamma m^3$, where $m = |A|$. Then, there exists $A' \subseteq A$ with $|A'| \geq \gamma^{10} m$ such that $|A' + A'| \leq \gamma^{-10}|A'|$.*

Lemma 1 (Ruzsa's Triangle Inequality) *Suppose that U, V, W are finite subsets of an abelian group G. Then,*

$$|U||V-W| \ \leq \ |U-V||U-W|.$$

An almost immediate corollary of this lemma and Plunnecke-Ruzsa is the following:

Corollary 1 *Suppose that $|U| \leq H|V|$ and that $|U+V| \leq K|U|$. Then,*

$$|U+U| \lesssim |U|, \ |U-U| \lesssim |U|,$$

where the notation $|A| \lesssim |B|$ means "up to a factor of the form $H^{O(1)}K^{O(1)}$" (e.g. $|A| \leq H^5 K^{10}|B|$).

Theorem 4 (Bourgain-Katz-Tao-Konyagin Sum-Product Inequality) *There exists $\epsilon > 0$ so that if $U \subseteq \mathbb{F}_p$, and $2 \leq |U| < p^{1/2}$, then*

$$\max(|U+U|, |U \cdot U|) \ \geq \ |U|^{1+\epsilon}.$$

3 Proof of Theorem 1

Suppose that $A \subseteq \mathbb{F}_p$, $A_0 \leq |A| = m < p^{1/2}$ (A_0 is a constant that comes out of the proof), such that

$$|\{a^2 + b \ : \ a, b \in A\}| \ < \ |A|^{1+c} \ = \ m^{1+c}. \tag{1}$$

We will show that this is impossible for $c > 0$ sufficiently small.

To make the exposition easy to follow I will use the $\lesssim$ notation appearing in the above corollary, but here when I write $|A| \lesssim m$ I will always mean that $|A| \leq \kappa_1 m^{1+\kappa_2 c}$, where κ_1, κ_2 are constants (κ_2 may even be negative, but κ_1 will also be positive).

From (1) and Corollary 1, we deduce that

$$|A-A| \ \lesssim \ m, \text{ and } |A+A| \ \lesssim \ m. \tag{2}$$

From this it easily follows that

$$E(A,A) \gtrsim m^3.$$

Now we use an averaging argument to show that there are a lot of pairs $(a,a') \in A \times A$ such that $a - a'$ lies in a single translate $A - b$ of A: We have that

$$\begin{aligned} \frac{1}{m} \sum_{b \in A} |\{a, a' \in A \ : \ a - a' \in A - b\}| \ &= \ \frac{1}{m} \sum_{a,a' \in A} |\{b \in A \ : \ a - a' \in A - b\}| \\ &= \ \frac{E(A,A)}{m} \ \gtrsim \ m^2. \end{aligned}$$

Thus, there exists $b \in A$ such that there are $\gtrsim m^2$ pairs $(a,a') \in A \times A$ such that $a - a' \in A - b$. Call this set of pairs P; so,

$$|P| \ \gtrsim \ m^2. \tag{3}$$

Then, for every pair $(a,a') \in P$ we have that $a - a' + b \in A$.

Now, from Corollary 1 with

$$B \ = \ \{a^2 \ : \ a \in A\},$$

we deduce that since

$$|B + A| \ \lesssim \ m, \text{ and } |A| = H|B|, \ 1 \leq H \leq 2,$$

then

$$|B - B| \ \lesssim \ m.$$

Then, from Theorem 2 (see remarks following the statement of the theorem) we deduce that

$$|B + B - B - B| \ \lesssim \ m.$$

However, since for every $(a,a') \in P$ we have that $a - a' + b \in A$, then $(a - a' + b)^2 \in B$, which means that $B + B - B - B$ contains

$$(a - a' + b)^2 - a^2 - (a')^2 + b^2 \ = \ -2aa' + 2ab - 2a'b + 2b^2 \ = \ -2(a+b)(a'-b).$$

Thus,

$$|\{(a+b)(a'-b) \ : \ (a,a') \in P\}| \ \lesssim \ m; \tag{4}$$

and, from (2),

$$|\{(a-b)+(a'-b)\ :\ (a,a')\in A\times A\}|\ \lesssim\ m. \tag{5}$$

We now consider the the set

$$U=\{a-b\ :\ a\in A\}\cup\{a+b\ :\ a\in A\}$$

under multiplication. From (4) and (3) we deduce that the set U has lots of multiplicative quadruples; in fact,

$$|\{u_1,u_2,u_3,u_4\in U\ :\ u_1u_2=u_3u_4\}|\ \gtrsim\ m^3.$$

Applying the Gowers-Balog-Szemeredi theorem (multiplicative version) to the set U, we have that there exists a subset

$$U'\ \subseteq\ U,$$

such that

$$|U'|\ \gtrsim\ m; \tag{6}$$

and

$$|U'\cdot U'|\ \lesssim\ m. \tag{7}$$

From (5) we can also dedcue that

$$|U'+U'|\ \lesssim\ |A+A|\ \lesssim\ m \tag{8}$$

However, if $c>0$ is sufficiently small, then (6), (7) and (8) contradict the Bourgain-Katz-Tao-Konyagin theorem provided $|U|$ is sufficiently large.

We conclude then that for some sufficiently small $c>0$,

$$|\{a^2+b\ :\ a,b\in A\}|\ \geq\ |A|^{1+c},$$

when $|A|>A_0$. But then we must also get the same result just under the condition $|A|\geq 2$ (by choosing $c>0$ even smaller to make the inequality work for $2\leq|A|\leq A_0$).