

1. MOTIVATION

The problems we will be considering lie in the area of Additive Number Theory. This relatively young area of Mathematics is part of Combinatorial Number Theory and can best be described as the study of sums of sets of integers. As such, we begin by stating the following definition:

Definition 1.1. [*Sumset*]

For sets A and B (usually subsets of $\mathbb{Z}/p\mathbb{Z}$), define

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

A simple example of a problem in Additive Number Theory is given two subsets A and B of a set of integers, what facts can we determine about $A + B$? Note that a very familiar result in Number Theory, namely Lagrange's theorem that every nonnegative integer can be written as the sum of four squares, can be expressed in terms of sumsets. In particular, if we let \mathbb{N}_0 be the set of nonnegative integers and if we let \mathbb{S} be the set of all integers that are perfect squares, then Lagrange's Four Square Theorem has the form

Theorem 1.2. [*Lagrange's Four Square Theorem*]

$$\mathbb{N}_0 = \mathbb{S} + \mathbb{S} + \mathbb{S} + \mathbb{S}$$

where $\mathbb{N}_0 = \{x \in \mathbb{Z} \mid x \geq 0\}$ and $\mathbb{S} = \{x^2 \mid x \in \mathbb{Z}\}$.

As well the binary version of Goldbach's Conjecture can be restated in terms of sumsets. In particular,

Conjecture 1.3. [*Goldbach's Conjecture*]

Let $\mathbb{E} = \{2x \mid x \in \mathbb{Z}, x \geq 2\}$ and let $\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ is prime}\}$. Then

$$\mathbb{E} \subseteq \mathbb{P} + \mathbb{P}. \tag{1}$$

In other words, every even integer that is greater than 2 is the sum of two primes. Notice that we do not have set equality in equation (1) because $2 \in \mathbb{P}$. Once again, 2 is the "odd" prime.

2. THE PROBLEMS WE CONSIDER

2.1. The Cauchy-Davenport Theorem.

The first result we will be concerned with is a theorem proved by Cauchy¹ in 1813 [6] and independently by Davenport in 1935 [8] (Davenport discovered in 1947 [9] that Cauchy had previously proved the theorem). In particular,

Theorem 2.1. *[Cauchy-Davenport]*

Let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime. Then $|A + B| \geq \min\{p, |A| + |B| - 1\}$ where $A + B := \{a + b \mid a \in A \text{ and } b \in B\}$.

We note that in 1935 Inder Cholwa [7] extended the result to composite moduli m when $0 \in B$ and the other members of B are relatively prime to m .

2.2. The Erdős-Heilbronn Conjecture.

The second result we consider is a slightly different version of the first. In the early 1960's, Paul Erdős and Hans Heilbronn conjectured that if the addition in the Cauchy-Davenport Theorem is restricted to distinct elements the lower bound slightly changes. Erdős stated this conjecture in 1963 during a number theory conference at the University of Colorado [11]. Interestingly, Erdős and Heilbronn did not mention the conjecture in their 1964 paper on sums of sets of congruence classes [14] though Erdős mentioned it often in his lectures (see [15], page 106). Eventually the conjecture was formally stated in Erdős' contribution to a 1971 text [12] as well as in a book by Erdős and Graham in 1980 [13]. In particular,

Theorem 2.2. *[Erdős-Heilbronn Conjecture]*

Let p be a prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A \neq \emptyset$ and $B \neq \emptyset$. Then $|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}$, where $A \dot{+} B := \{a + b \text{ mod } p \mid a \in A, b \in B \text{ and } a \neq b\}$.

The conjecture was first proved for the case $A = B$ by J.A. Dias da Silva and Y.O. Hamidoune in 1994 [10] using methods from linear

¹Cauchy used this theorem to prove that $Ax^2 + By^2 + C \equiv 0 \pmod{p}$ has solutions provided that $ABC \not\equiv 0$. This is interesting in that Lagrange used this result to establish his four squares theorem.

algebra with the more general case established by Noga Alon, Melvin B. Nathanson, and Imre Z. Ruzsa using the polynomial method in 1995 [1].

3. PRELIMINARY MATTER

The following fact from field theory is essential to our work.

Theorem 3.1.

Let \mathbb{F} be a field and suppose $p(x) \in \mathbb{F}[x]$ where degree $p(x) = d$. If $p(x)$ is not the zero polynomial, then $p(x)$ can have at most d distinct roots in \mathbb{F} .

We use this to establish the following Lemma which is fundamental to the Polynomial Method.

Lemma 3.2 (Alon-Tarsi [3]).

Let $f(x, y)$ be a polynomial with coefficients in an arbitrary field \mathbb{F} and of degree at most $k - 1$ in x and degree at most $l - 1$ in y . Let A and B be subsets of \mathbb{F} with $|A| = k$ and $|B| = l$. If $f(a, b) = 0$ for all $a \in A$ and for all $b \in B$, then $f(x, y) \equiv 0$.

Proof.

We have

$$f(x, y) = \sum_{i=0}^{k-1} \sum_{j=0}^{l-1} f_{i,j} x^i y^j.$$

Grouping together terms of degree x^i and factoring enable us to write

$$f(x, y) = \sum_{i=0}^{k-1} g_i(y) x^i$$

where $g_i(y) = \sum_{j=0}^{l-1} f_{i,j} y^j$ for each $i = 0, \dots, k - 1$. As well, fix $b \in B$ and put

$$h(x) = \sum_{i=0}^{k-1} g_i(b) x^i.$$

Then for all $a \in A$, $h(a) = f(a, b) = 0$. But $|A| = k$ while degree $h(x) \leq k - 1$. Hence by Theorem 3.1, $h(x) \equiv 0$ giving us $g_i(b) = 0$ for all i . This is true for each $b \in B$. Thus, since $|B| = l$ and degree $g_i(y) = l - 1$, Theorem 3.1 again gives $g_i(y) \equiv 0$ for each i . Hence we have $f(x, y) \equiv 0$. □

We will also need

Lemma 3.3 (Alon-Nathanson-Ruzsa [1]).

Let A be a finite subset of an arbitrary field \mathbb{F} with $|A| = k$. Then for every $r \geq k$ there exists a polynomial $g_r(x) \in \mathbb{F}[x]$ of degree at most $k - 1$ such that $g_r(a) = a^r$ for all $a \in A$.

Proof.

Fix $r \geq k$ and let $A = \{a_1, \dots, a_k\}$. Our goal is to construct the appropriate polynomial $C(x)$ of degree at most $k - 1$. Put $C(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$. Thus we need

$$\begin{aligned} C(a_1) &= c_0 + c_1 \cdot a_1 + \dots + c_{k-1}a_1^{k-1} = a_1^r \\ C(a_2) &= c_0 + c_1 \cdot a_2 + \dots + c_{k-1}a_2^{k-1} = a_2^r \\ &\vdots \\ C(a_k) &= c_0 + c_1 \cdot a_k + \dots + c_{k-1}a_k^{k-1} = a_k^r. \end{aligned}$$

Note that this gives rise to a k by k matrix and, by Cramer's Rule, this matrix has a solution if the determinant of the coefficient matrix is nonzero. But this matrix is just

$$V(a_1, \dots, a_n) = \prod_{1 \leq i < j \leq n} (a_j - a_i)$$

which is not 0. □

This proof is the one provided by Alon, Nathanson, and Ruzsa. A much simpler means of establishing the result is by making use of Lagrange Interpolation:

Lagrange Interpolation.

Fix $r \geq k$ and let $A = \{a_1, \dots, a_k\}$. Put

$$g_r(x) := \sum_{a_i \in A} \left(a_i^r \prod_{\substack{a_j \in A \\ j \neq i}} \frac{x - a_j}{a_i - a_j} \right).$$

Then $g_r(a_i) = a_i^r$ for all i , $1 \leq i \leq k$. □

We note that Lemma 3.2 was originally stated in [3] for a polynomial with coefficients in \mathbb{Z} where A and B are subsets of \mathbb{Z} . The result was proven for arbitrary fields in [1].

4. THE METHOD EMPLOYED

We first prove

Theorem 4.1.

Suppose A and B are nonempty subsets of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime. Further suppose that $|A| = k$, $|B| = l$, and that $k \neq l$. Then

$$|A \dot{+} B| \geq \min\{p, k + l - 2\}$$

where $A \dot{+} B := \{a + b \text{ mod } p \mid a \in A, b \in B \text{ and } a \neq b\}$.

Proof.

Without loss of generality we may assume that

$$1 \leq l = |B| < k = |A| \leq p.$$

Now if $k + l - 2 > p$, let $l' = p - k + 2$. Then

$$2 \leq l' \leq l < k$$

and

$$k + l' - 2 = p.$$

Choose $B' \subseteq B$ such that $|B'| = l'$. Hence, if the theorem holds for the sets A and B' , then

$$|A \dot{+} B| \geq |A \dot{+} B'| \geq k + l' - 2 = p = \min\{p, k + l - 2\}.$$

Therefore we may assume that

$$k + l - 2 \leq p. \tag{2}$$

We form the set $C = A \dot{+} B$ and assume for contradiction that

$$|C| \leq k + l - 3 \tag{3}$$

and we will put

$$m = k + l - 3 - |C|. \tag{4}$$

Thus, by (3), m is nonnegative.

We form a polynomial in $\mathbb{F}_p[x, y]$ by defining

$$f_0(x, y) := \prod_{c \in C} (x + y - c). \tag{5}$$

Hence

$$\deg(f_0) = |C| \leq k + l - 3 \tag{6}$$

where $\deg(f_0)$ is the homogeneous degree of f_0 . Also

$$f_0(a, b) = 0 \text{ for all } a \in A, b \in B, a \neq b. \quad (7)$$

As well define

$$f_1(x, y) = (x - y)f_0(x, y) = (x - y) \prod_{c \in C} (x + y - c). \quad (8)$$

Then

$$\deg(f_1) = 1 + |C| \leq k + l - 2 \quad (9)$$

and

$$f_1(a, b) = 0 \text{ for all } a \in A, b \in B. \quad (10)$$

Lastly we form the polynomial

$$f(x, y) = (x + y)^m f_1(x, y) = (x + y)^m (x - y) \prod_{c \in C} (x + y - c). \quad (11)$$

Note that

$$\deg(f) = m + 1 + |C| = k + l - 2 \quad (12)$$

and that

$$f(a, b) = 0 \text{ for all } a \in A, b \in B. \quad (13)$$

Since

$$\begin{aligned} f(x, y) &= (x - y)(x + y)^m \prod_{c \in C} ((x + y) - c) \\ &= (x - y)(x + y)^{m+|C|} + \text{lower order terms,} \end{aligned}$$

we have

$$f(x, y) = \sum_{\substack{i, j \geq 0 \\ i+j \leq k+l-2}} f_{i,j} x^i y^j = (x - y)(x + y)^{k+l-3} + \text{lower order terms.}$$

By assumption, $p \geq k + l - 2$, and we have $k, l \neq 0$. Therefore the coefficient $f_{k-1, l-1}$ of the term $x^{k-1}y^{l-1}$ is

$$\begin{aligned} \binom{k+l-3}{k-2} - \binom{k+l-3}{l-2} &= \binom{k+l-3}{k-2} - \binom{k+l-3}{k-1} \\ &= \frac{(k+l-3)!}{(k-2)!(l-1)!} - \frac{(k+l-3)!}{(k-1)!(l-2)!} \end{aligned} \quad (14)$$

$$= \frac{(k-1)(k+l-3)!}{(k-1)!(l-1)!} - \frac{(l-1)(k+l-3)!}{(k-1)!(l-1)!} \quad (15)$$

$$= \frac{(k-l)(k+l-3)!}{(k-1)!(l-1)!} \quad (16)$$

$$\neq 0 \pmod{p}.$$

But by Lemma 3.3, for $r \geq k$, there is a $g_r(x)$ of degree at most $k-1$ such that $g_r(a) = a^r$ for all $a \in A$. Likewise for each $s \geq l$, there is a $h_s(y)$ of degree at most $l-1$ such that $h_s(b) = (b)^s$ for all $b \in B$.

Given the existence of these polynomials we employ the following algorithms:

Algorithm 4.2.

If $x^m y^n$ is a term in $f(x, y)$ with $m \geq k$, then replace $x^m y^n$ with $[g_m(x)]y^n$.

Note that if the term $x^m y^n$ occurs in $f(x, y)$ with $m \geq k$ then $m + n \leq \deg(f) = k + l - 2$, so

$$n \leq l - 2. \quad (17)$$

Note also that for each $m \geq k$

$$[g_m(x)]y^n = \sum_{i \leq k-1} f_{m,i}^* x^i y^n.$$

As well

Algorithm 4.3.

If $x^m y^n$ is a term in $f(x, y)$ with $n \geq l$, then replace $x^m y^n$ with $x^m [h_n(y)]$.

So for each $n \geq l$

$$x^m [h_n(y)] = \sum_{j \leq l-1} f_{n,j}^{**} x^m y^j.$$

Let $f^\#(x, y)$ be the polynomial formed by following both Algorithm 4.2 and Algorithm 4.3. In forming the polynomial $f^\#(x, y)$, by (17) and the corresponding statement with Algorithm 4.3, the coefficient $f_{k-1, l-1}$ is unaffected (i.e. $f_{k-1, l-1}^\# = f_{k-1, l-1}$). But

$$f^\#(a, b) = f(a, b) = 0$$

for all $a \in A$ and each $b \in B$. Hence by Lemma 3.2,

$$f^\#(x, y) \equiv 0,$$

in particular, $f_{k-1, l-1} = 0$. This contradicts (12) and therefore our assumption in (3). Hence we have $|C| \geq k + l - 2$. \square

With Theorem 4.1 in hand, we may establish

Theorem 4.4 (Dias da Silva-Hamidoune [10]).

Let p be a prime and $A \subseteq F = \mathbb{Z}/p\mathbb{Z}$ with $|A| = k \geq 2$. Then

$$|2^{\wedge} A| := |A \dot{+} A| \geq \min\{p, 2|A| - 3\}.$$

Proof. Choose $a \in A$ and put $B = A \setminus \{a\}$. The result follows from Theorem 4.1. \square

5. FURTHER APPLICATIONS OF THE METHOD

Theorem 5.1 (Cauchy-Davenport).

Let p be a prime and nonempty $A, B \subseteq F = \mathbb{Z}/p\mathbb{Z}$. Then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof.

Put $|A| = k$ and $|B| = l$. We may assume that $k + l - 1 \leq p$. If $|C| \leq k + l - 2$, let $m = k + l - 2 - |C|$. Now consider the polynomial

$$f(x, y) = (x + y)^m \prod_{c \in C} (x + y - c).$$

Then $f(a, b) = 0$ for all $a \in A$ and $b \in B$ and $\deg(f) = k + l - 2$. Moreover the coefficient of the $x^{k-1}y^{l-1}$ is

$$\binom{k + l - 2}{k - 1} \neq 0 \pmod{p}.$$

The rest of the proof proceeds exactly as in Theorem 4.1. \square

The Polynomial Method also establishes:

Theorem 5.2.

Let p be a prime and nonempty $A, B \subseteq F = \mathbb{Z}/p\mathbb{Z}$. Put $C = \{a + b \mid a \in A, b \in B, ab \neq 1\}$. Then

$$|C| \geq \min\{p, |A| + |B| - 3\}.$$

Proof.

Put $|A| = k$ and $|B| = l$. If $k + l - 3 > p$, let $l' = p - k + 3$. Then $3 \leq l' < l$. Choose $B' \subseteq B$ such that $|B'| = l'$ and let

$$C' = \{a + b' \mid a \in A, b' \in B', ab' \neq 1\}.$$

Since $C' \subseteq C$, it suffices to prove that $|C'| \geq k + l - 3$. Equivalently, we can assume that $k + l - 3 \leq p$ and attempt to prove that $|C| \geq k + l - 3$.

As such, assume for contradiction that $|C| \leq k + l - 4$. Again we choose m such that $|C| + m = k + l - 4$. Next we consider the polynomial

$$f(x, y) = (xy - 1)(x + y)^m \prod_{c \in C} (x + y - c).$$

Then $f(a, b) = 0$ for all $a \in A$ and $b \in B$. The polynomial has degree $k + l - 2$ and the coefficient of the monomial $x^{k-1}y^{l-1}$ is

$$\binom{k + l - 4}{k - 2} \neq 0 \pmod{p}.$$

The rest of the proof proceeds exactly as in Theorem 4.1. □

Regarding the bound in the above theorem let $k + l - 3 \leq p$ where $k, l > 1$. Choose $d \in \mathbb{Z}/p\mathbb{Z}, d \neq 0$ such that

$$1 + (k - 1)d(1 + (l - 1)d) = 1.$$

Put $A = \{1, 1 + d, 1 + 2d, \dots, 1 + (k - 1)d\}$ and $B = \{1, 1 + d, 1 + 2d, \dots, 1 + (l - 1)d\}$. Defining C as in Theorem 5.2 we get $C = \{2 + id \mid i = 1, \dots, k + l - 3\}$, i.e. the lower bound is sharp. Note that if $k = 1$, the lower bound is $|B| - 1 = k + l - 2$.

In closing we note that in 2002, Hao Pan and Zhi-Wei Sun [16] established the following more general result of the Erdős-Heilbronn Problem:

Theorem 5.3 (Pan and Sun [16]).

Let \mathbb{F} be a field of characteristic p and let A and B be finite nonempty subsets of \mathbb{F} . Moreover let $\emptyset \neq S \subseteq \mathbb{F}^\times \times \mathbb{F}$ with $|S| < \infty$. Then

$$|\{a + b \mid a \in A, b \in B \text{ and } a + ub \neq v \text{ if } \langle u, v \rangle \in S\}| \geq \min\{p - |\{v \in \mathbb{F} \mid \langle 1, v \rangle \in S\}|, |A| + |B| - 2|S| - 1\}.$$

REFERENCES

- [1] Alon, Noga, Nathanson, Melvyn B. and Ruzsa, Imre *Adding distinct congruence classes modulo a prime*, American Mathematical Monthly, **102** (1995) 250-255.
- [2] Alon, Noga, Nathanson, Melvyn B. and Ruzsa, Imre *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory, **56** (1996) 404-417.
- [3] Alon, N. and Tarsi, M., *Colorings and orientations of graphs*, Combinatorica. An International Journal on Combinatorics and the Theory of Computing, **12** No.2 (1992) 125-134.
- [4] Balister, Paul N., Wheeler, Jeffrey Paul *The Cauchy-Davenport theorem for finite groups*, Preprint, <http://jeffreypaulwheeler.com/>, 2006.
- [5] Balister, Paul N. and Wheeler, Jeffrey Paul, *The Erdős-Heilbronn problem for finite groups*, to appear in Acta Arithmetica.
- [6] Cauchy, A.L., *Recherches sur les nombres*, J. École polytech., **9**, (1813) 99-116.
- [7] Chowla, Inder, *A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring's problem.*, Proceedings of the Indian Academy of Sciences, Section A, **1**, (1935) 242-243.
- [8] Davenport, H., *On the addition of residue classes*, Journal of the London Mathematical Society, **10**, (1935) 30-32.
- [9] Davenport, H., *A historical note*, Journal of the London Mathematical Society, **22**, (1947) 100-101.
- [10] Dias da Silva, J. A. and Hamidoune, Y. O., *Cyclic spaces for Grassmann derivatives and additive theory*, The Bulletin of the London Mathematical Society, **26** No.2, (1994) 140-146.
- [11] Erdős, P., *On the addition of residue classes (mod p)*, Proceedings of the 1963 Number Theory Conference at the University of Colorado, Univeristy of Colorado Press, (1963) 16-17.
- [12] Erdős, P., *Some problems in number theory*, in *Computers in Number Theory*, edited by A.O.L. Atkin and B.J. Birch, Academic Press, (1971) 405-414.
- [13] Erdős, P. and Graham, R. L., *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], volume 28, Université de Genève L'Enseignement Mathématique, 1980.
- [14] Erdős, P. and Heilbronn, H., *On the addition of residue classes (mod p)*, Acta Arithmetica, **9** (1964) 149-159.
- [15] Nathanson, Melvyn B., *Additive Number Theory, Inverse Problems and the Geometry of Subsets*, Springer-Verlag, 1996.
- [16] Pan, Hao and Sun, Zhi-Wei, *A lower bound for $|\{a+b : a \in A, b \in B, P(a, b) \neq 0\}|$* , Journal of Combinatorial Theory, Series A, **100** (2002) 387-393.
- [17] Tao, Terence and Vu, Van H., *Additive Combinatorics*, Cambridge University Press, 2006.