The Erdős-Heilbronn Conjecture
Math 21 – 801 (Additive Combinatorics)
Carnegie Mellon University - Spring 2009

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 $\mathbb{P} = \{p \in \mathbb{Z} \mid p$ 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 Cauchy[1] 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 $A \dot{+} B := \{a+b \bmod p \mid a \in A, b \in B \text{ and } a \neq b\}$.

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

[1] Cauchy used this theorem to prove that $Ax^2+By^2+C \equiv 0 (\text{mod } p)$ 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 $i = 0, \ldots, k-1$. 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 $A = \{a_1, \ldots, a_k\}$. Our goal is to construct the appropriate polynomial $C(x)$ of degree at most $k-1$. Put $C(x) = c_0 + c_1 x + \cdots + c_{k-1}x^{k-1}$. Thus we need

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

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

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

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 $A = \{a_1, \ldots, a_k\}$. 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 $A\dot{+}B := \{a + b \ mod \ p \ \mid a \in A, \ b \in B \ and \ a \neq b \ \}$.

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

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

As well define

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

Then

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

and

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

Lastly we form the polynomial

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

Note that

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

and that

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

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

$$\begin{aligned}
\binom{k+l-3}{k-2} - \binom{k+l-3}{l-2} &= \binom{k+l-3}{k-2} - \binom{k+l-3}{k-1} \\
&= \frac{(k+l-3)!}{(k-2)!(l-1)!} - \frac{(k+l-3)!}{(k-1)!(l-2)!} \qquad (14) \\
&= \frac{(k-1)(k+l-3)!}{(k-1)!(l-1)!} - \frac{(l-1)(k+l-3)!}{(k-1)!(l-1)!} \qquad (15) \\
&= \frac{(k-l)(k+l-3)!}{(k-1)!(l-1)!} \qquad (16) \\
&\neq 0 \pmod{p}.
\end{aligned}$$

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

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

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 $|C| \geq k + l - 2$. □

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 $B = A \backslash \{a\}$. The result follows from Theorem 4.1. □

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. □

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 $A = \{1, 1 + d, 1 + 2d, \ldots, 1 + (k - 1)d\}$ and $B = \{1, 1 + d, 1 + 2d, \ldots, 1+(l-1)d\}$. Defining C as in Theorem 5.2 we get $C = \{2+id \mid i = 1, \ldots, k + l - 3\}$, 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.

The Erdős-Heilbronn Problem for Finite Groups

Paul Balister

Department of Mathematical Sciences, University of Memphis

Memphis, TN 38152, USA

pbalistr@memphis.edu

Jeffrey Paul Wheeler

Duquesne University / The University of Pittsburgh

Pittsburgh PA, USA

wheelerj@duq.edu / jpw41@pitt.edu

1 Background

Additive Number Theory can be best described as the study of sums of sets of integers. A simple example is given two subsets A and B of a set of integers, what facts can we determine about $A+B$ where $A+B := \{a+b \mid a \in A \text{ and } b \in B\}$? We will state a result regarding this example shortly. We note that a very familiar problem 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 S be the set of all integers that are perfect squares, then Lagrange's Theorem has the form

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

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

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

A classic problem in Additive Number Theory was the conjecture of Paul Erdős and Hans Heilbronn [11] which stood as an open problem for over 30 years until proved in 1994. We seek to extend this result. This conjecture

has its roots in a theorem proved by Cauchy [6] in 1813 and independently by Davenport [8] in 1935 (Davenport discovered in 1947 [9] that Cauchy had previously proved the theorem). The theorem in its original form is

Theorem 1.1 (Original Cauchy-Davenport)**.** *If A and B are 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.

The structures over which the Cauchy-Davenport Theorem holds have been extended beyond $\mathbb{Z}/p\mathbb{Z}$. Before stating the extended versions, the following definition is needed.

Definition 1.2 (Minimal Torsion Element)**.** *Let G be a group. We define $p(G)$ to be the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$ (or, if multiplicative notation is used, $g^p = 1$). If no such p exists, we write $p(G) = \infty$.*

Before we continue an observation.

Remark 1.3. If G is finite, then $p(G)$ is the smallest prime factor of $|G|$.

Equipped with this we can state that the Cauchy-Davenport Theorem has been extended to abelian groups by Károlyi [16], [17] and then to all finite groups by Károlyi [18] and Balister and Wheeler [5], namely:

Theorem 1.4 (Cauchy-Davenport Theorem for Finite Groups)**.** *If A and B are non-empty subsets of a finite group G, then $|A \cdot B| \geq \min\{p(G), |A| + |B| - 1\}$, where $A \cdot B := \{a \cdot b \mid a \in A \text{ and } b \in B\}$.*

Naturally, induction further gives us

Theorem 1.5. *Let $h \geq 2$. Then for $A_1, A_2, \ldots, A_h$, nonempty subsets of a finite group G,*

$$|A_1 \cdot A_2 \cdots A_h| \geq \min\left\{p(G), \textstyle\sum_{i=1}^{h} |A_i| - h + 1\right\}.$$

Over 40 years ago, Paul Erdős and Hans Heilbronn conjectured that if the addition in the Cauchy-Davenport Theorem is restricted to distinct elements, the lower bound changes only slightly. 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 [21], 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 1.6 (Erdős-Heilbronn Problem)**.** *If A and B are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime, then $|A\dot{+}B| \geq \min\{p, |A| + |B| - 3\}$, where $A\dot{+}B := \{a + b \bmod p \mid a \in A,\ b \in B \text{ and } a \neq b\}$.*

The conjecture was first proved for the case $A = B$ by Dias da Silva and Hamidounne in 1994 [10] with the more general case established by Alon, Nathanson, and Ruzsa using the polynomial method in 1995 [2]. Károlyi extended this result to abelian groups for the case $A = B$ in 2004 [17] and to cyclic groups of prime powered order in 2005 [19].

Our aim is to establish this result for all finite groups. We in fact prove a more general result, for which it will be useful to introduce the following notation.

Definition 1.7. *For a group G let $\mathrm{Aut}(G)$ be the group of automorphisms of G. Suppose $\theta \in \mathrm{Aut}(G)$ and $A, B \subseteq G$. Write*

$$A \overset{\theta}{\cdot} B := \{a \cdot \theta(b) \mid a \in A,\ b \in B,\ \text{and } a \neq b\}.$$

Given this definition, we can clearly state our objective, namely to extend the theorem to finite groups; in particular we seek to prove

Theorem 1.8 (Generalized Erdős-Heilbronn for Finite Groups)**.** *If A and B are non-empty subsets of a finite group G, and $\theta \in \mathrm{Aut}(G)$, then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, |A| + |B| - 3\}$, where $\delta = 0$ if θ has odd order in $\mathrm{Aut}(G)$ and $\delta = 1$ otherwise.*

As well we can state

Corollary 1.9. *If A and B are non-empty subsets of a finite group G, and $\theta \in \mathrm{Aut}(G)$, then*

$$|\{ab \mid a \neq \theta(b),\ a \in A,\ b \in B\}| \geq \min\{p(G) - \delta, |A| + |B| - 3\},$$

where $\delta = 0$ if θ has odd order in $\mathrm{Aut}(G)$ and $\delta = 1$ otherwise.

Proof.

$$\{ab \mid a \neq \theta(b),\, a \in A,\, b \in B\} = \{a\theta^{-1}(u) \mid a \neq u,\, a \in A,\, u \in \theta(B)\}$$
$$= A \overset{\theta^{-1}}{\cdot} \theta(B).$$

We then use Theorem 1.8 noting that $\theta^{-1} \in \mathrm{Aut}(G)$ has the same order as θ and that $|\theta(B)| = |B|$. □

We note that Lev [20] has shown that the results of Theorem 1.8 and Corollary 1.9 are not true for an arbitrary bijection θ.

An additional outcome is

Theorem 1.10 (Erdős-Heilbronn Conjecture for Finite Groups)**.** *If A and B are non-empty subsets of a finite group G, then*

$$|\{ab \mid a \in A,\, b \in B,\, a \neq b\}| \geq \min\{p(G), |A| + |B| - 3\}.$$

Proof. Follows from Theorem 1.8 by putting $\theta = 1$. □

2 The Polynomial Method

Before stating our objective in this section, we establish the following:

Definition 2.1. *Let $\mathbb{F}_{p^n}$ be the field of order p^n (which is unique up to isomorphism) and let $\mathbb{F}_{p^n}^{\times}$ be the collection of all nonzero elements in $\mathbb{F}_{p^n}$.*

Lemma 2.2. *Suppose A and B are finite subsets of a field F with $|A| = a$ and $|B| = b$. If $f(x, y) \in F[x, y]$ is a polynomial with coefficients in F of homogeneous degree at most $a + b - 2$ and the coefficient of $x^{a-1}y^{b-1}$ is not zero, then there exists $u \in A$ and $v \in B$ such that $f(u, v) \neq 0$.*

Proof. This is a result of the Combinatorial Nullstellensatz [1]. □

With this we seek to adapt the polynomial method in the following manner:

Theorem 2.3 (The Polynomial Method)**.** *Suppose A and B are nonempty subsets of $\mathbb{F}_{p^n}$. Fix $\gamma \in \mathbb{F}_{p^n}^{\times}$. Then $|A \overset{\gamma}{+} B| \geq \min\{p - \delta, |A| + |B| - 3\}$, where $A \overset{\gamma}{+} B := \{a + \gamma b \mid a \in A,\, b \in B,\, a \neq b\}$ and where $\delta = 1$ if $\gamma = -1$ and $\delta = 0$ otherwise.*

Before we begin the proof, we note that if $\gamma = 1$ we have the result by Theorem 1.6 in [2]. As well, if $p = 2$, a little work will show that in this case the lower bound can be strengthened to $\min\{3, |A| + |B| - 3\}$. Moreover if p is a prime greater than 2 let a be any nonzero element in (the additive group) $\mathbb{F}_{p^n}$. Putting $A = B = \{0, a, 2a, \ldots, (p-1)a\}$ and $\gamma = 1$ gives us $|A \overset{\gamma}{+} B| = p \leq 2p - 3$, and with the same A and B but $\gamma = -1$ yields $|A \overset{\gamma}{+} B| = p - 1 < 2p - 3$. Hence the term $p - \delta$ is required in $\min\{p - \delta, |A| + |B| - 3\}$.

Proof. Write $a = |A|$ and $b = |B|$. We form the set C_γ by setting $C_\gamma = A \overset{\gamma}{+} B$. We first prove the result in three special cases. Indeed for these special cases we prove a stronger lower bound of $\min\{p - \delta, a + b - 2\}$.

Special Case 1: $|A|$ or $|B| = 1$.
Without loss of generality, suppose $|A| = 1$. Then

$$|A \overset{\gamma}{+} B| \geq |B| - 1 = a + b - 2.$$

Special Case 2: $\gamma = -1$.
If $\gamma = -1$, then by Theorem 1.4

$$\begin{aligned} |A \overset{\gamma}{+} B| &= |\{u - v \mid u \in A,\, v \in B, \text{ and } u \neq v\}| \\ &= |(A + (-B)) \setminus \{0\}| \\ &\geq \min\{p, a + b - 1\} - 1 \\ &= \min\{p - 1, a + b - 2\}. \end{aligned}$$

Special Case 3: $\gamma(a-1) \neq (b-1)$ and $p \geq a + b - 2$.
We shall prove in this case that $|C_\gamma| \geq a + b - 2$. We begin the proof by assuming for contradiction that

$$|C_\gamma| \leq a + b - 3. \tag{1}$$

Choose a set C containing C_γ of size $a + b - 3$. We form a polynomial in $\mathbb{F}_{p^n}[x, y]$ by defining

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

Hence

$$\deg(f) = 1 + |C| = a + b - 2$$

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

$$f(u,v) = 0 \text{ for all } u \in A,\ v \in B$$

since either $u - v = 0$ or $u + \gamma v - c = 0$ for some c in C. Since

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

we have

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

By assumption, $p \geq a+b-2$, and $a, b > 0$. Therefore the coefficient $f_{a-1,b-1}$ of the term $x^{a-1}y^{b-1}$ is

$$\begin{aligned} &\gamma^{b-1}\binom{a+b-3}{b-1} - \gamma^{b-2}\binom{a+b-3}{b-2} = \\ &= \gamma^{b-1}\frac{(a+b-3)!}{(a-2)!(b-1)!} - \gamma^{b-2}\frac{(a+b-3)!}{(a-1)!(b-2)!} \\ &= \gamma^{b-2}[\gamma(a-1)-(b-1)]\frac{(a+b-3)!}{(a-1)!(b-1)!} \\ &\neq 0 \bmod p. \end{aligned}$$

This contradicts Lemma 2.2 and therefore our assumption in (1). Hence we have $|C_\gamma| \geq a+b-2$.

Now we prove the general case. First suppose $p-\delta \geq a+b-3$ where $\delta = 1$ if $\gamma = -1$ and $\delta = 0$ otherwise. By Special Case 1 we may assume $a, b \geq 2$. By Special Case 2 we may assume $\gamma \neq -1$. Hence either $\gamma(a-2) \neq b-1$ or $\gamma(a-1) \neq b-2$. Assume $\gamma(a-2) \neq b-1$. Let $A^* = A \setminus \{u\}$ where $u \in A$. Then by Special Case 3 applied to A^* and B

$$|A \overset{\gamma}{+} B| \geq |A^* \overset{\gamma}{+} B| \geq \min\{p, (a-1)+b-2\} = \min\{p, a+b-3\}.$$

Similarly we can remove one element from B if $\gamma(a-1) \neq b-2$.

Now suppose $p - \delta < a+b-3$. Pick nonempty subsets $A^* \subseteq A$ and $B^* \subseteq B$ such that $|A^*| + |B^*| - 3 = p - \delta$. Then by the first part of the general case applied to A^* and B^*

$$|A \overset{\gamma}{+} B| \geq |A^* \overset{\gamma}{+} B^*| \geq |A^*| + |B^*| - 3 = p - \delta.$$

□

We note that the result of Theorem 2.3 is not new. This is an immediate consequence of Corollary 3 in Hao Pan and Zhi-Wei Sun's 2002 paper [22]. However, we feel the proof of the theorem is instructive and as such choose to present it.

3 A Structure Theorem for Finite Solvable Groups

Our approach to establishing the Erdős-Heilbronn Problem in the case of finite groups will involve solvable groups. We begin by reminding the reader of some basic definitions.

Definition 3.1. *Let G be a group. The* commutator *of x and y in G is defined to be $[x, y] = xyx^{-1}y^{-1}$. The* commutator *of two subgroups H and K of G is $[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle$. We define inductively*

$$G^{(0)} = G,\ G^{(1)} = [G, G],\ \ldots,\ G^{(i+1)} = [G^{(i)}, G^{(i)}] \text{ for } i \geq 1.$$

And though several equivalent definitions exist, we choose the following definition for solvable group: G is solvable *if there exists an $n \geq 0$ such that $G^{(n)} = \{1\}$.*

Given these definitions we state some useful facts.

1. $G^{(1)} \trianglelefteq G$;
2. $G/G^{(1)}$ is abelian;
3. if $G \neq \{1\}$ is solvable then $G \neq G^{(1)}$; and
4. subgroups of solvable groups are solvable.

We are now ready to establish the following important theorem.

Theorem 3.2 (The Associated Field Structure Theorem)**.** *Let G be a non-trivial finite solvable group and let $\theta \in \mathrm{Aut}(G)$. Then there exists a $K \trianglelefteq G$, $K \neq G$, such that*

(1) $\theta(K) = K$,

(2) $G/K \cong (\mathbb{F}_{p^n}, +)$ *for some prime* p *and* $n \geq 1$, *and*

(3) $\overline{\theta}(x) = \gamma x$ *where* $\gamma \in \mathbb{F}_{p^n}^{\times}$, $x \in G/K$, *and* $\overline{\theta}$ *is the map induced by* θ *on* G/K *which we identify with* $\mathbb{F}_{p^n}$ *by* (2).

Proof. Easy matters first. Suppose $\theta \in \mathrm{Aut}(G)$ and $K \trianglelefteq G$ with $\theta(K) = K$. The map $\overline{\theta}$ is defined by $\overline{\theta}(gK) = \theta(g)K$ and this is well defined since if $g_1K = g_2K$, then

$$\theta({g_2}^{-1}g_1) \in \theta(K) = K,$$

so

$$\theta(g_1) \in \theta(g_2)K$$

and thus

$$\theta(g_1)K = \theta(g_2)K.$$

With well-definedness established, we continue by noting that there is at least one proper normal subgroup with an abelian quotient, namely $G^{(1)}$. Note that $\theta(xyx^{-1}y^{-1}) = \theta(x)\theta(y)\theta(x)^{-1}\theta(y)^{-1}$ and thus $G^{(1)}$ is fixed by θ. Thus if $K = G^{(1)}$ we have the following:

1. K is a proper normal subgroup of G;
2. $\theta(K) = K$; and
3. G/K is abelian.

Of all subgroups meeting these three conditions, choose a subgroup K which is maximal in the sense that there is no K', $K \subsetneq K'$ with K' meeting each of the three conditions. We claim that this is the desired subgroup; i.e., that G/K can be given a field structure and $\overline{\theta}(gK) = \theta(g)K$ is multiplication by a nonzero element from G/K.

Before proceeding with the proof, a helpful observation:

Observation 3.3. *G/K has no proper, non-trivial $\overline{\theta}$-invariant subgroup.*

Proof of observation. Suppose that G/K has a proper, nontrivial $\overline{\theta}$-invariant subgroup, in other words there exists a subgroup H, $K \leq H \leq G$, such that $\{1\} \lneq H/K \lneq G/K$ and $\overline{\theta}(H/K) \subseteq H/K$. But G/K is abelian, so $\{1\} \lhd H/K \lhd G/K$ thus $K \lhd H \lhd G$ and $\theta(H) \subseteq H$. But $|\theta(H)| = |H|$, so $\theta(H) = H$. Also $G/H \cong (G/K)/(K/H)$ is abelian. These contradict the maximality of K. Hence G/K has no proper, nontrivial $\overline{\theta}$-invariant subgroup. □

Now we continue with the proof of Theorem 3.2.

Since G/K is abelian, $G/K \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, a product of cyclic groups. Let p be a prime factor of d_1. Put $P = \{x \mid x^p = 1\}$, the set of all elements in G/K of order dividing p. Since G/K is abelian, P is a subgroup of G/K. Also, since $x^p = 1$, $\overline{\theta}(x)^p = 1$, thus $\overline{\theta}(P) \subseteq P$ and so P is $\overline{\theta}$-invariant. But $P \neq \{1\}$, so $P = G/K$. Hence $d_i = p$ for $1 \leq i \leq r$, i.e., $G/K \cong (\mathbb{Z}/p\mathbb{Z})^n \cong (\mathbb{F}_p)^n$. We must be careful in that this isomorphism is an additive group isomorphism; there is work yet to do to establish a field structure.

Given this, we now show that G/K meets the remaining conditions of the lemma, namely that G/K can be given the structure of a finite field and that $\overline{\theta}(x) = \gamma x$ for $\gamma \in \mathbb{F}_{p^n}^{\times}$ where $x = gK$, $g \in G$.

First, since $G/K \cong (\mathbb{F}_p)^n$, G/K is a $\mathbb{F}_p$-vector space. Moreover, since $\overline{\theta}$ is an additive group homomorphism, for any scalar $k \in \{0, 1, \ldots, p-1\} = \mathbb{F}_p$,

$$\overline{\theta}(kx) = \overline{\theta}(\underbrace{x + \cdots + x}_{k \text{ terms}}) = \underbrace{\overline{\theta}(x) + \cdots + \overline{\theta}(x)}_{k \text{ terms}} = k\overline{\theta}(x),$$

i.e., $\overline{\theta}$ is an $\mathbb{F}_p$-linear map. Now we pick a nonzero $e_1 \in G/K$ and define a map

$$\chi \colon \mathbb{F}_p[x] \to G/K$$

by

$$\chi(\sum a_i x^i) = \sum a_i \overline{\theta}^i(e_1) \qquad (G/K \text{ written additively}).$$

This map is $\mathbb{F}_p$-linear. Also, if $f(x) = \sum a_i x^i$ then

$$\begin{aligned} \chi(xf(x)) &= \chi(\sum a_i x^{i+1}) \\ &= \sum a_i \overline{\theta}^{i+1}(e_1) \\ &= \overline{\theta}(\sum a_i \overline{\theta}^i(e_1)) \qquad \text{(by linearity)} \\ &= \overline{\theta}(\chi(f(x))). \end{aligned} \tag{2}$$

The image $V \subseteq G/K$ of χ is a linear subspace of G/K, and hence a subgroup of G/K, and by (2), $\overline{\theta}(V) \subseteq V$. But $\overline{\theta}$ has no non-trivial proper invariant subgroup. As $0 \neq e_1 \in V$, we must have $V = G/K$, and so χ is surjective. Thus, by the First Isomorphism Theorem (for groups),

$$\mathbb{F}_p[x]/\ker(\chi) \cong G/K \qquad \text{(as groups)}. \tag{3}$$

Claim: $\ker(\chi)$ is a maximal ideal of the ring $\mathbb{F}_p[x]$.

Proof of claim. Suppose $f(x) \in \ker(\chi)$, so that $\chi(f(x)) = 0$. Then we have $\chi(xf(x)) = \overline{\theta}(\chi(f(x))) = 0$. Therefore an induction argument gives us that $\chi(g(x)f(x)) = 0$ for any polynomial $g(x) \in \mathbb{F}_p[x]$. Since $\ker(\chi)$ is a subgroup under $+$, we have shown that $\ker(\chi)$ is an ideal.

Suppose $\ker(\chi)$ is not a maximal ideal, namely, that there exists an ideal I of $\mathbb{F}_p[x]$ such that

$$\ker(\chi) \subsetneq I \subsetneq \mathbb{F}_p[x].$$

Considering the image of each of these under χ, we get

$$(0) \subsetneq \chi(I) \subsetneq G/K.$$

The inclusions here are strict since we know that χ induces the isomorphism (3). But since I is an ideal of $\mathbb{F}_p[x]$, $xI \subseteq I$, and so by (2), $\overline{\theta}(\chi(I)) = \chi(xI) \subseteq \chi(I)$, i.e., $\chi(I)$ is $\overline{\theta}$-invariant. This is a contradiction, hence $\ker(\chi)$ is maximal. □

As a result, $\mathbb{F}_p[x]/\ker(\chi)$ is a field, in particular

$$\mathbb{F}_p[x]/\ker(\chi) \cong \mathbb{F}_{p^n} \qquad \text{(as rings)}$$

for some $n \geq 1$.

Hence we have condition (2) of the theorem (namely, the field structure). But again, we have more. We have shown in (2) that $\overline{\theta}$ acting on G/K is the same in $\mathbb{F}_p[x]/\ker(\chi)$ as multiplication by x, which is the same in $\mathbb{F}_{p^n}$ as multiplication by a nonzero element element, i.e., we have met condition (3) of the theorem. □

4 The Erdős-Heilbronn Problem for Finite Solvable Groups

Let G be a finite solvable group. By Theorem 3.2, for any $\theta \in \mathrm{Aut}(G)$ there is some $K \trianglelefteq G$ such that

1. $\theta(K) = K$,
2. $G/K \cong (\mathbb{F}_{p^n}, +)$, and

3. $\overline{\theta}(x) = \gamma x$ where $\gamma \in \mathbb{F}_{p^n}^{\times}$ and $\overline{\theta}$ is the map induced by θ on G/K.

For each $h \in (\mathbb{F}_{p^n}, +) \cong G/K$ pick a representative $\tilde{h} \in G$ of h, in particular choose $\tilde{0} = 1$. Define $\psi\colon K \times (\mathbb{F}_{p^n}, +) \to G$ by $\psi(k, h) = k\tilde{h}$. We have that ψ is a bijection and

$$\begin{aligned}\psi(k_1, h_1) \cdot \psi(k_2, h_2) &= k_1\tilde{h}_1 \cdot k_2\tilde{h}_2 \\ &= k_1\phi_{h_1}(k_2)\tilde{h}_1\tilde{h}_2 \\ &= (k_1\phi_{h_1}(k_2)\eta_{h_1,h_2})(\widetilde{h_1 + h_2}) \\ &= \psi(k_1\phi_{h_1}(k_2)\eta_{h_1,h_2}, h_1 + h_2) \end{aligned} \tag{4}$$

where $\phi_h(k) = \tilde{h}k\tilde{h}^{-1}$ (so, in particular $\phi_h \in \mathrm{Aut}(K)$) and $\eta_{h_i,h_j} = \tilde{h}_i \cdot \tilde{h}_j \cdot (\widetilde{h_i + h_j})^{-1} \in K$ with $\tilde{h}$ the coset representative of h in G. Hence ψ can be considered an isomorphism if we put the following non-standard multiplication on $K \times (\mathbb{F}_{p^n}, +)$:

$$(k_1, h_1) \star (k_2, h_2) = (k_1\phi_{h_1}(k_2)\eta_{h_1,h_2}, h_1 + h_2).$$

In summary, for $A \subseteq G$, we can consider $A \subseteq K \times (\mathbb{F}_{p^n}, +)$, in particular, $A = \{(k_1, h_1), (k_2, h_2), \ldots, (k_t, h_t)\}$ for some $k_1, k_2, \ldots, k_t \in K$ and $h_1, h_2, \ldots h_t \in (\mathbb{F}_{p^n}, +)$.

Remark 4.1. *Let (k_1, h_1) and (k_2, h_2) be elements in G, let $\theta \in \mathrm{Aut}(G)$, and let $\gamma \in \mathbb{F}_{p^n}^{\times}$ be as in condition* (3)*. Then*

$$\begin{aligned}\theta(k_2, h_2) &= \theta((k_2, 0) \star (1, h_2)) \\ &= \theta(k_2, 0) \star \theta(1, h_2) \\ &= (\theta(k_2), 0) \star (c_{h_2}, \overline{\theta}(h_2)) \\ &= (\theta(k_2)c_{h_2}, \gamma h_2) \end{aligned} \tag{5}$$

where $c_{h_2} \in K$ depends only on h_2. Thus

$$\begin{aligned}(k_1, h_1) \star \theta(k_2, h_2) &= (k_1, h_1) \star (\theta(k_2)c_{h_2}, \gamma h_2) \\ &= (k_1 \cdot \phi_{h_1}[\theta(k_2)c_{h_2}]\eta_{h_1,h_2}, h_1 + \gamma h_2) \\ &= (k_1 \cdot \phi_{h_1}[\theta(k_2)] \cdot \phi_{h_1}[c_{h_2}] \cdot \eta_{h_1,h_2}, h_1 + \gamma h_2) \\ &= (k_1 \cdot \theta'(k_2) \cdot f_{h_1,h_2}, h_1 + \gamma h_2) \end{aligned} \tag{6}$$

where $\theta' := \phi_{h_1} \circ \theta \in \mathrm{Aut}(K)$, and f_{h_1,h_2} depends only on h_1, h_2.

Definition 4.2. *For any $A \subseteq G$, consider A as a subset of $K \times \mathbb{F}_{p^n}$. Define*

$$A^1 := \{k \in K \mid \text{there exists } h \in \mathbb{F}_{p^n} \text{ such that } (k,h) \in A\} \text{ and}$$
$$A^2 := \{h \in \mathbb{F}_{p^n} \mid \text{there exists } k \in K \text{ such that } (k,h) \in A\}.$$

In other words, A^1 is the collection of first coordinates of A and A^2 is the collection of second coordinates of A when A is written as a subset of $K \times \mathbb{F}_{p^n}$.

Definition 4.3. *Put $a = |A|$ and $b = |B|$. Let $A^2 = \{h_1, \ldots, h_\alpha\}$ and $B^2 = \{h'_1, \ldots, h'_\beta\}$. Then define $A_i = \{(k,h) \in A \mid h = h_i\}$, $1 \leq i \leq \alpha$ and write $a_i = |A_i|$. Order the h_i's so that $a_1 \geq a_2 \geq \cdots \geq a_\alpha$. Construct $B_1, B_2, \ldots, B_\beta$ in a similar manner so that $B_j = \{(k,h) \in B \mid h = h'_j\}$, $b_j = |B_j|$, and $b_1 \geq b_2 \geq \cdots \geq b_\beta$.*

Note that $A = A_1 \cup A_2 \cup \cdots \cup A_\alpha$ and $B = B_1 \cup B_2 \cup \cdots \cup B_\beta$, hence $|A| = a = a_1 + a_2 + \cdots + a_\alpha$ and $|B| = b = b_1 + b_2 + \cdots + b_\beta$.

The following lemma and remarks will be the last pieces in equipping us in establishing the desired theorem.

Lemma 4.4. *If $h_i \neq h'_j$, then*

$$|A_i \overset{\theta}{\cdot} B_j| = |(A_i)^1 \cdot \theta'((B_j)^1)|.$$

If $h_i = h'_j$, then

$$|A_i \overset{\theta}{\cdot} B_j| = |(A_i)^1 \overset{\theta'}{\cdot} (B_j)^1|,$$

where $\theta' = \phi_{h_i} \circ \theta$.

Proof. Regarding the first equality, by Definition 1.7, Remark 4.1, and noting that $h_i \neq h'_j$, we have

$$\begin{aligned} |A_i \overset{\theta}{\cdot} B_j| &= |\{a_i \cdot \theta(b_j) \mid a_i \in A_i,\, b_j \in B_j,\, a_i \neq b_j\}| \\ &= |\{(k_i, h_i) \star \theta(k_j, h'_j) \mid k_i \in A_i^1,\, k_j \in B_j^1\}| \\ &= |\{k_i \cdot \theta'(k_j) \cdot f_{h_i, h'_j}, h_i + \gamma h'_j\}|. \end{aligned}$$

Since h_i and h'_j are fixed elements, $f_{h_i,h_j} \in K$ is fixed. But multiplication by an element of K is a bijection on K. Likewise, since ϕ_{h_i} is conjugation by h_i, $\theta' = \phi_{h_i} \circ \theta$ is a fixed automorphism of K. Hence

$$\begin{aligned} |A_i \overset{\theta}{\cdot} B_j| &= |\{k_i \cdot \theta'(k_j) \mid k_i \in A_i^1,\, k_j \in B_j^1\}| \\ &= |(A_i)^1 \cdot \theta'(B_j^1)|. \end{aligned}$$

As for the second equality, again by Definition 1.7, Remark 4.1, and our observation regarding θ' we have

$$\begin{aligned}
|A_i \overset{\theta}{\cdot} B_j| &= |\{a_i \cdot \theta(b_j) \mid a_i \in A_i,\, b_j \in B_j,\, a_i \neq b_j\}| \\
&= |\{(k_i, h_i) \star \theta(k_j, h_i) \mid k_i \in A_i^1,\, k_j \in B_j^1,\, k_i \neq k_j\}| \\
&= |\{(k_i \cdot \theta'(k_j) \cdot f_{h_i,h_i}, h_i + \gamma h_i) \mid k_i \neq k_j\}| \\
&= |\{k_i \cdot \theta'(k_j) \mid k_i \neq k_j\}| \\
&= |A_i^1 \overset{\theta'}{\cdot} B_j^1|.
\end{aligned}$$

□

Since we have introduced $\theta' = \phi_h \circ \theta$ we address the following:

Lemma 4.5. *For G a group of odd order, if θ has odd order in $\mathrm{Aut}(G)$ then θ' has odd order in $\mathrm{Aut}(K)$.*

Proof. We first establish $\theta' \in \mathrm{Aut}(K)$. By Theorem 3.2, $\theta(K) = K$ and θ is an isomorphism, therefore $\theta \in \mathrm{Aut}(K)$. Moreover it is well known that for K a normal subgroup of G, conjugation by any $h \in G$ is an automorphism of K; i.e., $\phi_h \in \mathrm{Aut}(K)$. Thus $\theta' = \phi_h \circ \theta \in \mathrm{Aut}(K)$. As well we establish that since $\mathrm{Inn}(G) := \{\phi_h \mid h \in G\} \cong G/Z(G)$ and since $|G|$ is odd, $|\mathrm{Inn}(G)|$ must be odd.

Suppose $\theta^r = 1$ in $\mathrm{Aut}(G)$ where r is odd. Then $\theta^r = 1$ in $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. But θ and θ' give rise to the same element of $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, so $\theta'^r = 1$ in $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. Thus $\theta'^r \in \mathrm{Inn}(G)$ and so by Lagrange's Theorem, $\theta'^{rs} = 1$ in $\mathrm{Aut}(G)$ where $s = |\mathrm{Inn}(G)|$. But then $\theta'^{rs} = 1$ as an element of $\mathrm{Aut}(K)$ and rs is odd, so θ' has odd order in $\mathrm{Aut}(K)$. □

Remark 4.6. Assume $p - \delta_\gamma \geq \alpha + \beta - 3$ where $\delta_\gamma = 1$ if $\gamma = -1$ and $\delta_\gamma = 0$ otherwise.

Case 1: Suppose that there does not exist an j such that $h'_j = h_1$, i.e., the second coordinates of the B_j's will be distinct from A_1^2.

The set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$ will have β elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Theorem 2.3 and Theorem 3.2, $|A^2 \overset{\gamma}{+} B^2| \geq \alpha + \beta - 3$. Thus there are at least $\alpha - 3$ elements of the form $h_i + \gamma h'_j$, $h_i \neq \gamma h'_j$, that are not in the set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$.

Case 2: Now suppose that there does exist an r such that $h'_r = h_1$, i.e., some second coordinate of the B_j's will be the same as A_1^2.

Hence the set $\{h_1 + \gamma h'_j \mid h_1 \neq h'_j\}$ will have $\beta - 1$ elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Theorem 2.3 and Theorem 3.2 $|A^2 \overset{\gamma}{+} B^2| \geq \alpha+\beta-3$. Thus, since $\alpha + \beta - 3 = (\beta - 1) + (\alpha - 2)$, there are at least $\alpha - 2$ elements of the form $h_i + \gamma h'_j$, $h_i \neq h'_j$ not in the set $\{h_1 + \gamma h'_j \mid h_1 \neq h'_j\}$.

Remark 4.7. Assume that $p - \delta_\gamma \geq \alpha + \beta - 1$ where $\delta_\gamma = 1$ if $\gamma = -1$ and $\delta_\gamma = 0$ otherwise. The set $\{(A_1 \cdot \theta(B_j))^2 \mid 1 \leq j \leq \beta\} = \{h_1 + \gamma h_j \mid 1 \leq j \leq \beta\}$ will have β elements. But $A^2, B^2 \subseteq \mathbb{F}_{p^n}$, hence by Theorem 1.4 $|A^2 + \gamma B^2| \geq \alpha + \beta - 1$. Thus, since $\alpha + \beta - 1 = \beta + (\alpha - 1)$, there are at least $\alpha - 1$ elements $h_i + \gamma h'_j$ that are not in the set $\{h_1 + \gamma h'_j \mid 1 \leq j \leq \beta\}$.

And lastly,

Remark 4.8. For G a finite solvable group with a normal subgroup K we have $p(K) \geq p(G)$ and $p \geq p(G)$ where the p is the characteristic of the field in Theorem 3.2.

Proof. By Remark 1.3, $p(G)$ is the smallest prime factor of $|G|$. Since $K \leq G$, by Lagrange's Theorem, $|K| \mid |G|$, thus $p(K) \geq p(G)$. Likewise, G/K is of order p^n, thus $p \geq p(G)$. □

Before continuing, we define the following generalizations of the δ_γ from the Polynomial Method.

Definition 4.9 (δ_θ and $\delta_{\theta'}$)**.** *For $\theta \in \mathrm{Aut}(G)$, put*

$$\delta_\theta = \begin{cases} 1, & \text{if } \theta \text{ has even order in } \mathrm{Aut}(G); \text{and} \\ 0, & \text{if } \theta \text{ has odd order in } \mathrm{Aut}(G). \end{cases}$$

Likewise, put

$$\delta_{\theta'} = \begin{cases} 1, & \text{if } \theta' \text{ has even order in } \mathrm{Aut}(K); \text{and} \\ 0, & \text{if } \theta' \text{ has odd order in } \mathrm{Aut}(K). \end{cases}$$

where $\theta' = \phi_{h_i} \circ \theta$ with ϕ_{h_i} representing conjugation by h_i.

Hence by Lemma 4.5, $\delta_{\theta'} \leq \delta_\theta$, we have

Corollary 4.10.

$$p(G) - \delta_\theta \leq p(K) - \delta_{\theta'}.$$

□

Now we may state and prove the main result of this section.

Theorem 4.11 (Solvable Erdős-Hielbronn)**.** *Suppose $A, B \subseteq G$, G solvable of order n, with $|A| = a$, $|B| = b$, $a, b > 0$, and $\theta \in \mathrm{Aut}(G)$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta_\theta, a + b - 3\}$ where $\delta_\theta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta_\theta = 0$ otherwise.*

Proof. We will proceed by induction on n, namely we will assume the theorem holds for solvable groups of order less then n (note that the base case is trivial in that if $|G| = 1$, $A = B = G$ and thus $a + b - 3 < 0$ whereas $A \overset{\theta}{\cdot} B$ is empty). We have that there exists a $K \trianglelefteq G$ such that $G/K \cong \mathbb{F}_{p^n}$. We may assume that $p - \delta_\theta \geq a + b - 3$, otherwise we may replace A and B by an $A^* \subseteq A$ and a $B^* \subseteq B$ such that this holds. We will express A and B as in Definition 4.3 and since $|A \overset{\theta}{\cdot} B| = |B^{-1} \overset{\theta^{-1}}{\cdot} A^{-1}|$ and θ and θ^{-1} give rise to the same K and δ_θ, without loss of generality we choose A and B such that $\beta \geq \alpha$.

We further note that $\delta_\gamma = 1$ implies that $\delta_\theta = 1$ (if $\overline{\theta}$ is multiplication by $\gamma = -1$, then $\overline{\theta}$ has order 2, so θ has even order). As such, we have that $\alpha + \beta - 3 \leq |A| + |B| - 3 \leq p(G) - \delta_\theta \leq p - \delta_\gamma$ where the last inequality follows from Remark 4.8.

Case 1: There does not exist a j, $1 \leq j \leq \beta$, such that $A_1^2 = B_j^2$, i.e., the second coordinates of the B_j's are distinct from the second coordinate of A_1.

Together with Remark 4.6 we get (since there are at least $\alpha - 3$ non-empty disjoint sets $A_i \overset{\theta}{\cdot} B_j$, $1 < i \leq \alpha$, $1 \leq j \leq \beta$ disjoint from all $A_1 \overset{\theta}{\cdot} B_j$, i.e., there are $\alpha - 3$ second coordinates that come from these sets.)

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + |A_1 \overset{\theta}{\cdot} B_2| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \alpha - 3.$$

By Case 1 of Lemma 4.4, we have

$$|A \overset{\theta}{\cdot} B| \geq |A_1^1 \cdot \theta'(B_1^1)| + |A_1^1 \cdot \theta'(B_2^1)| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| + \alpha - 3.$$

Thus by Theorem 1.4,

$$\begin{aligned} |A \overset{\theta}{\cdot} B| &\geq (a_1 + b_1 - 1) + (a_1 + b_2 - 1) + \cdots + (a_1 + b_\beta - 1) + \alpha - 3 \\ &\geq \beta a_1 + b_1 + b_2 + \cdots + b_\beta - \beta + \alpha - 3 \\ &= \alpha a_1 + b + (\beta - \alpha)(a_1 - 1) - 3 \\ &\geq a + b - 3, \end{aligned}$$

since $\alpha a_1 = a_1 + \cdots + a_1 \geq a_1 + a_2 + \cdots + a_\alpha = a$, $\beta \geq \alpha$, and $a_1 \geq 1$.

Note that the above holds as long as each $a_1 + b_i - 1 \leq p(K) - \delta_{\theta'}$. If this is not true for some i, then

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_i| &\geq p(K) - \delta_{\theta'} \\ &\geq p(G) - \delta_\theta \qquad \text{(by Corollary 4.10)} \\ &\geq a + b - 3 \qquad \text{(by assumption).} \end{aligned}$$

Case 2: There exists a j, $1 \leq j \leq \beta$, such that $A_1^2 = B_j^2$, i.e., some B_j has a second coordinate that agrees with the second coordinate of A_1.

First we note that by Remark 4.7 there exists a set I of pairs (i, m) with $h_i + \gamma h'_m$ distinct and not equal to any $h_1 + \gamma h'_j$. Note well that if $\alpha + \beta - 1 \leq p - \delta_\gamma$ that $|I| = \alpha - 1$. Hence

Subcase A: $a_1 > 1$.

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_j| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in I} |A_i \overset{\theta}{\cdot} B_m|.$$

By Lemma 4.4, we have

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq &|A_1^1 \cdot \theta'(B_1^1)| + \cdots + |A_1^1 \overset{\theta'}{\cdot} B_j^1| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| + \\ &+ (|I| - |\{A_i \overset{\theta}{\cdot} B_m = \varnothing \mid (i,m) \in I\}|). \end{aligned}$$

But $A_i \overset{\theta}{\cdot} B_m = \varnothing$ if and only if $A_i = B_m = \{(k, h)\}$, i.e., each is a singleton. In particular, for each i this can only occur with at most one value of m. Thus if $r = |\{|A_i| = 1\}|$, then $|\{A_i \overset{\theta}{\cdot} B_m = \varnothing\}| \leq r$. Recall that if $\alpha+\beta-1 \leq p-\delta_\gamma$ that $|I| = \alpha - 1$. Hence by the induction hypothesis on K, which is solvable and of order less than n, we get

$$\begin{aligned} |A \overset{\theta}{\cdot} B| &\geq (a_1 + b_1 - 1) + \cdots + (a_1 + b_j - 3) + \cdots + (a_1 + b_\beta - 1) + \\ &\qquad + (\alpha - 1 - r) \\ &\geq \beta a_1 + b_1 + \cdots + b_\beta - \beta + \alpha - 3 - r \\ &= \alpha a_1 + b + (\beta - \alpha)(a_1 - 1) - 3 - r \end{aligned}$$

Since $\beta \geq \alpha$, $a_1 \geq 2$, and $\alpha a_1 - a = \sum_{i=1}^{\alpha} (a_1 - a_i) \geq r$,

$$|A \overset{\theta}{\cdot} B| \geq a + r + b - 3 - r = a + b - 3.$$

Now by assumption $a+b-3 \leq p(G)-\delta_\theta \leq p-\delta_\gamma$, so if $\alpha+\beta-1 > p-\delta_\gamma$, we must have that $a_1 = 2$ and $a_i = 1$ for all $i > 1$, and also each $b_j = 1$. In particular, this means that

$$|A_1^1 \overset{\theta'}{\cdot} B_j^1| \geq 1 = a_1 + b_j - 2$$

and that $|I| = \alpha - 2$. Hence, following the same work as above we still have that

$$|A \overset{\theta}{\cdot} B| \geq a+b-3.$$

Subcase B: $a_1 = \cdots = a_\alpha = 1$ and no $A_i = B_m$.

$$|A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_j| + \cdots + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in I} |A_i \overset{\theta}{\cdot} B_m|.$$

By Lemma 4.4, we have

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq |A_1^1 \cdot \theta'(B_1^1)| + \cdots + |A_1^1 \overset{\theta'}{\cdot} B_j^1| + \cdots + |A_1^1 \cdot \theta'(B_\beta^1)| + \\ + |I| - |\{A_i = B_m\}| = (*). \end{aligned} \tag{7}$$

Since $|A_1| = 1$,

$$\begin{aligned} (*) &= b_1 + \cdots + (b_j - 1) + \cdots + b_\beta + |I| \\ &= b + |I| - 1. \end{aligned} \tag{8}$$

We may have that $\alpha+\beta-1 \geq |A|+|B|-3$. Unfortunately this means that we have three further subcases.

Subcase B.1, $\alpha+\beta-1 \leq |A|+|B|-3$:
From our observation in Subcase A, we have that $|I| = \alpha - 1$. But $a = \sum_{i=1}^{\alpha} a_i = \alpha$, so

$$|A \overset{\theta}{\cdot} B| \geq b + |I| - 1 = a + b - 2$$

Subcase B.2, $\alpha+\beta-1 = |A|+|B|-2$:
Here we have that $|I| \geq \alpha - 2 = a - 2$. Hence

$$|A \overset{\theta}{\cdot} B| \geq b + |I| - 1 \geq a + b - 3$$

Subcase B.3, $\alpha+\beta-1 = |A|+|B|-1$:
In this situation we have that $b_j = 1$ for every j. Also we have $|I| \geq \alpha - 3 =$

$a-3$. Moreover, we have that $|A_1^1 \overset{\theta'}{\cdot} B_j^1| \geq 1 = b_j$ since $A_i^1 \neq B_j^1$. Hence continuing line 7:

$$|A \overset{\theta}{\cdot} B| \geq b_1 + \cdots + b_j + \cdots + b_\beta + |I| \geq a + b - 3.$$

Subcase C: $a_1 = \cdots = a_\alpha = 1$ and there exist i and m such that $A_i = B_m$.

Without loss of generality, let A_1 be one such A_i, namely $A_1 = B_s$. As well we note that by Remark 4.6, Case 2, we have a set J of pairs (i, m) with $h_i + \gamma h'_m$ distinct, $h_i \neq h'_m$ and $h_i + \gamma h'_m$ not equal to any $h_1 + \gamma h'_s$ and $|J| = \alpha - 2$. Hence

$$\begin{aligned} |A \overset{\theta}{\cdot} B| \geq |A_1 \overset{\theta}{\cdot} B_1| + \cdots + |A_1 \overset{\theta}{\cdot} B_{s-1}| + |A_1 \overset{\theta}{\cdot} B_{s+1}| + \cdots \\ + |A_1 \overset{\theta}{\cdot} B_\beta| + \sum_{(i,m)\in J} |A_i \overset{\theta}{\cdot} B_m|. \end{aligned}$$

By Remark 4.6, Case 2,

$$\begin{aligned} |A \overset{\theta}{\cdot} B| &\geq b_1 + \cdots + b_{s-1} + b_{s+1} + \cdots + b_\beta + \alpha - 2 \\ &= b - 1 + \alpha - 2 \\ &= a + b - 3. \end{aligned}$$

□

5 The Erdős-Heilbronn Conjecture for Finite Groups

We now extend Theorem 4.11 to all finite groups. Before we continue,

Theorem 5.1 (Feit-Thompson [15])**.** *Every group of odd order is solvable.*

Theorem 5.2 (Generalized Erdős-Heilbronn for Finite Groups)**.**
Let G be a finite group, $\theta \in \mathrm{Aut}(G)$, and let $A, B \subseteq G$ with $|A| = a$ and $|B| = b$, $a, b > 0$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, a + b - 3\}$ where $\delta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta = 0$ otherwise.

Proof. We first consider the case when G is of even order, hence $p(G) = 2$. If $a = 1$ or 2, then $|A \overset{\theta}{\cdot} B| \geq |B| - 1 > a + b - 3$. For $a \geq 3$, $|A \overset{\theta}{\cdot} B| \geq |A| - 1 \geq 2 = p(G)$. Lastly, if G is of odd order, then by Theorem 5.1, G is solvable. The result then follows from Theorem 4.11. □

6 Closing Remarks

Of course, Alon, Nathanson, and Ruzsa's work [2] established the Erdős-Heilbronn Problem for elementary abelian groups. As noted earlier Gyula Károlyi used different techniques to extend the Erdős-Heilbronn Problem to abelian groups for the case $A = B$ in 2004 [17] and to cyclic groups of prime powered order in 2005 [19]. Our result completes these results in establishing the general case of the Erdős-Heilbronn Problem for any finite abelian group. Moreover we note the extent of the comprehensiveness of the result; in particular establishing this theorem required using the techniques of Károlyi together with the Polynomial Method of Alon, Nathanson, and Ruzsa.

Acknowledgements

The authors wish to thank Gyula Károlyi for introducing us to this problem. As well we wish to thank Zhi-Wei Sun for alerting us to a significant oversight in the original version of one of our proofs. We especially wish to thank the referee for a helpful recommendation which shortened a proof, for providing us with a list of inaccuracies, and, in particular, for a very careful reading of our paper.

References

[1] Alon, Noga, Combinatorial nullstellensatz, *Combinatorics, Probability and Computing* **8** (1999) 7–29.

[2] Alon, Noga, Nathanson, Melvyn B. and Ruzsa, Imre, Adding distinct congruence classes modulo a prime, *American Mathematical Monthly* **102** (1995) 250–255.

[3] 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.

[4] Alon, N. and Tarsi, M., Colorings and orientations of graphs, *Combinatorica* **12** (1992) 125–134.

[5] Balister, Paul and Wheeler, Jeffrey Paul, The Cauchy-Davenport theorem for finite groups, *Preprint,* `http://jeffreypaulwheeler.com/` (2006).

[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** (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] **28** *Université de Genève L'Enseignement Mathématique,* 1980, 128pp.

[14] Erdős, P. and Heilbronn, H., On the addition of residue classes (mod p), *Acta Arithmetica* **9** (1964) 149–159.

[15] Feit, Walter and Thompson, John G. Solvability of groups of odd order, *Pacific Journal of Mathematics* **13** (1963) 775–1029.

[16] Károlyi, Gyula, On restricted set addition in abelian groups, *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Mathematica*, **46** (2003) 47–54.

[17] Károlyi, Gyula, The Erdős-Heilbronn problem in abelian groups, *Israel Journal of Mathematics* **139** (2004) 349–359.

[18] Károlyi, Gyula, The Cauchy-Davenport theorem in group extensions, *L' Enseignement Mathematique* **51** (2005) 239–254.

[19] Károlyi, Gyula, A compactness argument in the additive theory and the polynomial method, *Discrete Mathematics* **302** (2005) 124–144.

[20] Lev, Vsevolod F., Restricted set addition in groups II, a generalization of the Erdős-Heilbronn conjecture, *The Electric Journal of Combinatorics* **7** (2000) Research paper R4, 10 pages (electronic).

[21] Nathanson, Melvyn B., *Additive number theory, inverse problems and the geometry of subsets*, Springer-Verlag, 1996.

[22] 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 A* **100** (2002) 387–393.

The Cauchy-Davenport Theorem for Finite Groups

Paul Balister
Department of Mathematical Sciences, University of Memphis
Memphis, TN, USA
pbalistr@memphis.edu

Jeffrey Paul Wheeler
Department of Mathematics, University of Pittsburgh
Pittsburgh, PA, USA
jeffreypaulwheeler@hotmail.com

Abstract

The Cauchy-Davenport theorem states that for any two nonempty subsets A and B of $\mathbb{Z}/p\mathbb{Z}$ we have $|A+B| \geq \min\{p, |A|+|B|-1\}$, where $A+B := \{a+b \bmod p \mid a \in A, b \in B\}$. We generalize this result from $\mathbb{Z}/p\mathbb{Z}$ to arbitrary finite (including non-abelian) groups. This result from early in 2006 is independent of Gyula Károlyi's[1] 2005 result in [13] and uses different methods.

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 subsets A and B of a group G, define

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

where $+$ is the group operation[2]*.*

We note that originally $G = \mathbb{Z}/p\mathbb{Z}$ but much work (including this one) has been done and is being done in arbitrary groups.

[1]The authors wish to thank Gyula for introducing them to this problem and encouraging work on it. Regrettably we did not let Gyula know that we were making progress, hence the independent results. We discovered Gyula had a result the day before this work was presented to the Combinatorics seminar at Memphis.

[2]We are not suggesting that G is abelian, but rather being consistent with the notation for the sumset in cases where G is $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}$, or an abelian group. Later we will introduce the more appropriate notation.

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 $A + B$? We will state a result regarding this example shortly. Note that a very familiar problem 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,

Theorem 1.2. *[Lagrange's Four Square Theorem]*
Let $\mathbb{N}_0 = \{x \in \mathbb{Z} \mid x \geq 0\}$ *and let* $\mathbb{S} = \{x^2 \mid x \in \mathbb{Z}\}$. *Then*

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

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

Theorem 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 is greater than 2 is conjecture to be the sum of two primes. Notice that we do not have set equality in equation (1) because $2 \in \mathbb{P}$.

2. Background

The theorem we wish to extend was first proved by Augustin Cauchy in 1813[3] [3] and later independently reproved by Harold Davenport in 1935 [5] (Davenport discovered in 1947 [6] that Cauchy had previously proved the theorem). In particular,

Theorem 2.1. *[Cauchy-Davenport]*
Let k, l *be positive integers. If* $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, p *prime, with* $|A| = k \leq p$ *and* $|B| = l \leq p$, *then* $|A + B| \geq min\{p, k + l - 1\}$ *where* $A + B := \{a + b \mid a \in A \text{ and } b \in B\}$.

We note that in 1935 Inder Chowla [4] extended the result to composite moduli m when $0 \in B$ and the other members of B are relatively prime to m. As well it is worth noting that in 1996 Alon, Nathanson, and Ruzsa provided a simple proof of this theorem using the Polynomial Method[1].

Of interest to this work is Gyula Károlyi's extension of the theorem to abelian groups[9],[10]. Before we state the theorem, though, a useful definition:

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

Definition 2.2 (Minimal Torsion Element)**.**
Let G be a group. We define $p(G)$ to be the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$ (or, if multiplicative notation is used, $g^p = 1$). If no such p exists, we write $p(G) = \infty$.

Lemma 2.3.
The p in Definition 2.2 is the smallest prime factor of $|G|$ provided G is finite.

Proof.
Suppose $|G| = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \cdots \cdot {p_n}^{e_n}$ where $p_1 < p_2 < \cdots < p_n$ are primes end the e_i are positive integers. By Cauchy's Theorem there is an element $g \in G$ such that $g^{p_1} = 1$. Suppose there were a smaller prime q such that there were a $g_c \in G$ where $g_c^q = 1$. Then $| \langle g_c \rangle | = q$ and by Lagrange's Theorem $q||G|$. This is a contradiction.

□

Equipped with Definition 2.2 we state

Theorem 2.4. (*Károlyi*[9],[10])
If A and B are nonempty subsets of an abelian group G, then $|A + B| \geq \min\{p(G), |A| + |B| - 1\}$ where $A + B := \{a + b | a \in A, b \in B\}$.

Again, our goal is to extend this result to arbitrary finite groups. A necessary tool will be the famous and very useful result:

Theorem 2.5 (Feit-Thompson[8])**.**
Every group of odd order is solvable.

3. A Basic Structure of Finite Solvable Groups

Throughout this section G will be a finite solvable group, i.e. there exists a chain of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_i/G_{i-1} is abelian for $i = 1, 2, 3, \ldots, n$.

By definition, there is some $K = G_{n-1} \trianglelefteq G$ such that $G/K = H$ where H is abelian. Pick a representative $\widetilde{h}_i \in G$ for each coset $h_i = K\widetilde{h}_i \in H$. So for each $g \in G$, there is a $k_i \in K$ and there is an $h_i \in H$ (in particular, the coset representative) such that $g = k_i\widetilde{h}_i$. Given this, we build a useful structure for finite solvable groups. First, define

$$\psi_H : G \to K \times G/K = K \times H \text{ by } \psi(g) = (k_i, \tilde{h}_i). \tag{2}$$

(Note well that the second coordinate is the coset representative.) As well, define an operation $\star$ on $K \times H$ by

$$(k_1, \tilde{h_1}) \star (k_2, \tilde{h_2}) := (k_1 \phi_{\tilde{h_1}}(k_2) \eta_{\tilde{h_1}, \tilde{h_2}}, \tilde{h_1 h_2}). \tag{3}$$

where

$$\phi_{\tilde{h}} : K \to Aut(K) \tag{4}$$

in particular, $\phi_{\tilde{h}}(k) = \tilde{h} k \tilde{h}^{-1}$, and

$$\eta_{\tilde{h_1}, \tilde{h_2}} = \tilde{h_1} \cdot \tilde{h_2} \cdot (\widetilde{h_1 h_2})^{-1} \in K \tag{5}$$

with $\tilde{h}$ the coset representative of h in G/K [4]. Notice that $\eta : H \times H \to K$ (think cosets instead of coset representatives). Later examples will illustrate that this η plays an analogous role to "carrying the 1" in addition of real numbers.

Lemma 3.1 (A Basic Structure of Solvable Groups)**.**
Let G be a solvable group with $K \trianglelefteq G$. Upon fixing the coset representatives in $H = G/K$, ψ_H in (2) is an isomorphism from G to the group $(K \times H, \star)$.

Proof.
Since we have fixed the coset representatives $h = \tilde{h}$ for H, for every $g \in G$ there exists a unique $k \in K$ such that $g = kh$; i.e. ψ_H is one-to-one and onto. Suppose $g_1 = k_1 h_1$ and $g_2 = k_2 h_2$. Then

$$\psi_H(g_1) \star \psi_H(g_2) = (k_1, h_1) \star (k_2, h_2) \tag{6}$$

$$= (k_1 \phi_{h_1}(k_2) \eta_{h_1, h_2}, h_1 h_2) \tag{7}$$

$$= (k_1 \tilde{h_1} k_2 \tilde{h_1}^{-1} \tilde{h_1} \tilde{h_2} (\widetilde{h_1 h_2})^{-1}, h_1 h_2) \tag{8}$$

$$= \psi_H(k_1 \tilde{h_1} k_2 (\tilde{h_1}^{-1} \tilde{h_1}) \tilde{h_2} (\widetilde{h_1 h_2})^{-1} \widetilde{h_1 h_2}) \tag{9}$$

$$= \psi_H(k_1 \tilde{h_1} k_2 \tilde{h_2}) \tag{10}$$

$$= \psi_H(k_1 h_1 k_2 h_2) \tag{11}$$

$$= \psi_H(g_1 g_2)$$

□

In summary, for $A \subseteq G$, we have an isomorphism $A \to K \times H$, in particular, $A \cong \{(k_1, h_1), (k_2, h_2), \ldots, (k_t, h_t)\}$ for some $k_1, k_2, \ldots, k_t \in K$ and (fixed) $h_1, h_2, \ldots h_t \in H$. We note that it is certainly not the case that the k_i's nor the h_j's are distinct.

It is worth noting that the construction of $\star$ on $K \times H$ is more general than the semi-direct product. Indeed, G may not be a semi-direct product of K and H.

[4] i.e. for each $h \in H = G/K$ there exists $\tilde{h} \in G$ such that $h = K\tilde{h}$.

Before we continue, two illustrative examples.

Example 3.2.
Let Q be the quaternion group, namely $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ with Q's multiplication table stated for easy reference in Table 1 (Note: multiplication is row $\cdot$ column). Put $K = \{\pm 1, \pm k\}$ and since $|Q/K| = 2$,

$$\{1\} \trianglelefteq K \trianglelefteq Q;$$

i.e. Q is a solvable group.

TABLE 1. Multiplication Table for the Quaternion Group Q

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

So $Q/K = \{K, Kj\}$ and we choose 1 as our coset representative of K and j as the coset representative of Kj (see Table 2).

TABLE 2. Cosets of Q and Their Representatives

Cosets of Q/K	*Representative*
$K = \{\pm 1, \pm k\}$	1
$Kj = \{\pm j, \pm i\}$	j

Hence the order of Kj in Q/K is 2 however the order of j in Q is 4. This means

$$\begin{aligned} \eta_{j,j} &:= \tilde{j} \cdot \tilde{j} \cdot (\widetilde{j \cdot j})^{-1} \\ &= \tilde{j} \cdot \tilde{j} \cdot \tilde{1}^{-1} \text{ (note that the coset representative of } -1 \text{ is } 1) \\ &= j \cdot j \cdot 1 \text{ (now we multiply as in } G) \\ &= -1. \end{aligned} \tag{12}$$

As well

$$\begin{aligned} \eta_{j,1} &= \eta_{1,j} \\ &:= \tilde{1} \cdot \tilde{j} \cdot (\widetilde{1 \cdot j})^{-1} \\ &= \tilde{1} \cdot \tilde{j} \cdot \tilde{j}^{-1} \\ &= 1 \cdot j \cdot j^{-1} \\ &= 1 \cdot j \cdot -j \\ &= 1. \end{aligned} \tag{13}$$

And clearly

$$\eta_{1,1} = 1. \tag{14}$$

Before continuing with the example, we list the elements of Q as written using the structure of Lemma 3.1 with $K = \{\pm 1, \pm k\}$ in Table 3. Note that the first component is in K and the second is either of the selected coset representatives 1 or j.

TABLE 3. Elements of Q Written as in the Basic Structure with Coset Representatives as in Table 2

$q \in Q$	1	-1	i	$-i$	j	$-j$	k	$-k$
(k,h)	$(1,1)$	$(-1,1)$	$(-k,j)$	(k,j)	$(1,j)$	$(-1,j)$	$(k,1)$	$(-k,1)$

Thus, since $i = -k \cdot j$,

$$\begin{aligned}
i \cdot i &\cong \psi_H(i) \star \psi_H(i) && (15)\\
&= (-k, j) \star (-k, j) \qquad \textit{(see table 3)} && (16)\\
&= (-k\{j(-k)j^{-1} \cdot \eta_{j,j}\}, jj) && (17)\\
&= (-k\{-i(-j)(-1)\}, j^2) && (18)\\
&= (-k \cdot -k, 1) && (19)\\
&\quad (\textit{the multiplication in the second slot is as coset multiplication})\\
&= (-1, 1) && (20)\\
&\cong -1.
\end{aligned}$$

Which is what we hoped for since $i \cdot i = -1$.

To show we were not just lucky,

$$\begin{aligned}
i \cdot k &\cong \psi_H(i) \star \psi_H(k) && (21)\\
&= (-k, j) \star (k, 1) \qquad \textit{(see table 3)} && (22)\\
&= (-k\{j(k)j^{-1} \cdot \eta_{j,1}\}, j1) && (23)\\
&= (-kjk(-j)1, j) && (24)\\
&= ([kj]^2, j) && (25)\\
&= (-1, j) && (26)\\
&\cong -j.
\end{aligned}$$

and

$$
\begin{aligned}
(27)\qquad & j \cdot i \cong \psi_H(j) \cdot \psi_H(i) \\
(28)\qquad & = (1, j)(-k, -j) \qquad \textit{(see table 3)} \\
(29)\qquad & = (1j(-k)j^{-1} \cdot \eta_{j,-j}\}, j(-j) \\
(30)\qquad & = (j(-k)(-j)(-1), j(j)) \\
(31)\qquad & = (-jkj, 1) \\
& \big(\textit{the multiplication in the second slot is as coset multiplication}\big) \\
(32)\qquad & = (-k, 1) \\
& \cong -k.
\end{aligned}
$$

□

Example 3.3.
Let p be a prime. Then

$$\mathbb{Z}/p^2\mathbb{Z} \cong \big(p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \star\big)$$

where $H = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\} \cong \mathbb{Z}/p\mathbb{Z}$ which we will write as $\{0, 1, \ldots, p-1\}$ and $K = \{\overline{0}, \overline{p}, \ldots, \overline{(p-1)p}\} \cong p\mathbb{Z}/p^2\mathbb{Z}$ which we will write as $\{0, p, \ldots, (p-1)p\}$.

Hence

$$\mathbb{Z}/p^2\mathbb{Z} \cong \{(0,0), (0,1), \ldots, (0,p-1), (p,0), \ldots, (p,p-1), \ldots, ([p-1]p, p-1)\}$$

.

TABLE 4. Elements of $\mathbb{Z}/p^2\mathbb{Z}$ Written as in the Basic Structure

$\mathbb{Z}/p^2\mathbb{Z}$	0	1	$\cdots$	$p-1$	p	$p+1$	$\cdots$	p^2-1
$(p\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$	$(0,0)$	$(0,1)$	$\cdots$	$(0,p-1)$	$(p,0)$	$(p,1)$	$\cdots$	$([p-1]p, p-1)$

Hence

$$
\begin{aligned}
(33)\qquad & \\
& 3 + [p^2 - 2] \cong (0,3) + ([p-1]p, [p-2]) \\
(34)\qquad & = (0 + \phi_3([p-1]p) + \eta_{3,[p-2]}, 3 + [p-2]) \\
(35)\qquad & = (\{3 + [p-1]p + [p^2-3]\} + \{3 + [p-2] + [\overline{3+p-2}]^{-1}\}, p+1) \\
(36)\qquad & = (-p + 3 + [p-2] + 1^{-1}, 1) \\
(37)\qquad & = (1 + 1^{-1}, 1) \\
(38)\qquad & = (0,1) \\
& \cong 1
\end{aligned}
$$

□

Before leaving this section, we note that (as stated earlier) neither $\mathbb{Z}/p^2\mathbb{Z}$ nor the quaternion group is the semidirect product of its respective K and H.

Before proceeding, developing some notation will be helpful.

Definition 3.4.
For G a finite solvable group, we have $K = G_{n-1} \trianglelefteq G$. Putting $H = G/K$ and for $S \subseteq G$,

$$S \cong \{(k_i, h_i) \text{ where } k_i \in K \text{ and } h_i \in H\}. \tag{39}$$

We will define

$$S^1 := \{k_i \in K | \exists h_i \in H \text{ such that } (k_i, h_i) \in S\} \text{ and}$$
$$S^2 := \{h_i \in G \backslash K | \exists k_i \in K \text{ where } (k_i, h_i) \in S\}.$$

In other words, S^1 is the collection of first coordinates of S and S^2 is the collection of second coordinates of S when S is written as in (39).

4. The Cauchy-Davenport Theorem for Finite Solvable Groups

Let G be a solvable group and let S and T be subsets of G. Put $s = |S|$ and $t = |T|$. As previously stated, there exists a $K \trianglelefteq G$ so that $H = G/K$ with $|H| = \sigma$. Thus

$S \cong \{(k_u, h_i)\}$ for some $i \in \{1, \ldots, \sigma\}$ where $k_u \in K$ for $u \in \{1, \ldots, s\}$

$T \cong \{(k_v, h_j)\}$ for some $j \in \{1, \ldots, \sigma\}$ where $k_v \in K$ for $v \in \{1, \ldots, t\}$.

Hence

Definition 4.1.
Define $S_1 = \{(k_{j_1}, h_1)\}, S_2 = \{(k_{j_2}, h_2)\}, \ldots, S_\alpha = \{(k_{j_\alpha}, h_\alpha)\}$ where $|S_1| = s_1 \geq |S_2| = s_2 \geq \cdots \geq |S_\alpha| = s_\alpha$ (thus $1 \leq j_1 \leq s_1$, $1 \leq j_2 \leq s_2$, etc.). Construct $T_1, T_2, \ldots, T_\beta$ in a similar manner.

Following Definition 4.1,

Remark 4.2.
We have $S = S_1 \cup S_2 \cup \cdots \cup S_\alpha$ and $T = T_1 \cup T_2 \cup \cdots \cup T_\beta$, hence $|S| = s = s_1 + s_2 + \cdots + s_\alpha$ and $|T| = t = t_1 + t_2 + \cdots + t_\beta$.

Since we will be concerned with non-abelian groups,

Definition 4.3.
For an arbitrary group G with $S, T \subseteq G$,

$$S \cdot T := \{st | s \in S \text{ and } t \in T\}.$$

Since the second coordinates will be distinct, the set $\{(S_1 \cdot T_j)^2 | 1 \leq j \leq \beta\}$ will have β elements. But $S^2, T^2 \subseteq H$, hence by Theorem 2.4 $|S^2 \cdot T^2| \geq \alpha + \beta - 1$. Thus

Remark 4.4.
Since $\alpha + \beta - 1 = (\beta) + (\alpha - 1)$, there are at least $\alpha - 1$ elements in the set $\{(S_i \cdot T_j)^2 | 1 < i \leq \alpha, 1 \leq j \leq \beta\}$.

Lemma 4.5.
For each $i \in \{1, \ldots, \alpha\}$ and each $j \in \{1, \ldots, \beta\}$,

$$|S_i \cdot T_j| = |(S_i \cdot T_j)^1| = |{S_i}^1 \phi_{h_i}(T_j^1) \eta_{h_i, h_j}| = |(S_i)^1 \cdot (T_j)^1|$$

Proof.
Noting that the second coordinate is the same establishes the first equality. The second equality is just the definition of the product. The final equality holds since conjugation is an isomorphism as is multiplying by η_{h_i, h_j}, which is some fixed element in K (h_i and h_j are fixed).

□

Theorem 4.6.
Suppose $S, T \subseteq G$, G solvable of order n with $|S| = s, |T| = t$ and $s + t - 1 < p(G)$. Then $|S \cdot T| \geq s + t - 1$.

Proof.
We will proceed by induction on n, namely we will assume the theorem holds for solvable groups of order less then n. We have that there exists a $K \trianglelefteq G$ such that $H = G/K$. We will express S and T as in Definition 4.1 and we choose S and T such that $\beta \geq \alpha$. Together with Remark 4.4 we get (since there are at least $\alpha - 1$ non-empty sets $(S_i \cdot T_j)$, $1 < i \leq \alpha$, $1 \leq j \leq \beta$)[5]

(40)
$$|S \cdot T| \geq |S_1 \cdot T_1| + |S_1 \cdot T_2| + \cdots + |S_1 \cdot T_\beta| + \alpha - 1$$

By Lemma 4.5, we have

(41) $$= |S_1^1 \cdot T_1^1| + |S_1^1 \cdot T_2^1| + \cdots + |S_1^1 \cdot T_\beta^1| + \alpha - 1$$

By the induction hypothesis on K which is solvable and of order $< n$, we get

(42) $$\geq s_1 + t_1 - 1 + s_1 + t_2 - 1 + \cdots + s_1 + t_\beta - 1 + \alpha - 1$$

(43) $$\geq \beta s_1 + t_1 + t_2 + \cdots + t_\beta - \beta + \alpha - 1$$

(44) $$= \alpha s_1 + t + (\beta - \alpha) s_1 - (\beta - \alpha) - 1 \text{ (since } \beta \geq \alpha)$$

(45) $$\geq s + t + 0 - 1 \text{ (since } s_1 \geq 1)$$

(46) $$= s + t - 1.$$

[5]By Remark 4.4, there are $\alpha - 1$ second coordinates that come from these sets.

□

5. The Cauchy-Davenport Theorem for Finite Groups

We now extend Theorem 4.6 to all finite groups.

Theorem 5.1.
Let G be a finite group and let $S, T \subseteq G$ with $|S| = s$ and $|T| = t$. Then $|S \cdot T| \geq \min\{p(G), s + t - 1\}$.

Proof.
The case $|S| = |T| = 1$ is trivial. If G is of even order, then $p(G) = 2$. If G is of odd order, then by Theorem 2.5, G is solvable. The result then follows from Theorem 4.6.

□

6. A Related Problem

Very related to the Cauchy-Davenport Theorem is a conjecture of Paul Erdős and Hans Heilbronn. In the early 1960's they conjectured that if the sumset addition in the theorem is restricted to distinct elements then the lower bound changes slightly. In particular,

Theorem 6.1. *[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 $A \dot{+} B := \{a + b \pmod p \mid a \in A,\ b \in B$ and $a \neq b\ \}$.

The conjecture was first proved for the case $A = B$ by J.A. Dias da Silva and Y.O. Hamidounne in 1994 [7] using methods from linear algebra with the more general case established by Noga Alon, Melvin B. Nathanson, and Imre Z. Ruzsa using the polynomial method in 1995 [1]. Gyula Károlyi extended this result to abelian groups for the case $A = B$ in 2004 [10] and to cyclic groups of prime powered order in 2005 [13].

What is interesting to note is how much more difficult the restricted addition makes the problem. The Cauchy-Davenport Theorem was proven immediately but the Erdős-Heilbronn Conjecture was open for more than 30 years. The authors of this paper have as well extended the conjecture of Erdős and Heilbronn to Finite Groups [2] using similar techniques as in this paper. The increased difficulty of the problem is represented well by requiring a much stronger structure on finite solvable groups than what was used here. Curious readers are encouraged to read J. Wheeler's Ph.D. thesis [14].

References

[1] Alon, Noga and Nathanson, Melvyn B. and Ruzsa, Imre *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory, Volume 56, 1996, pgs. 404-417.

[2] Balister, Paul N. and Wheeler, Jeffrey Paul, *The Erdős-Heilbronn problem for finite groups*, to appear in Acta Arithmetica.

[3] Cauchy, A. *Recherches sur les nombres*, J. École Polytech, Volume 9, 1813, pgs. 99-116.

[4] 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.

[5] Davenport, H. *On the addition of residue classes*, Journal of the London Mathematical Society, Volume 10, 1935, pgs. 30-32.

[6] Davenport, H., *A historical note*, Journal of the London Mathematical Society, **22**, (1947) 100–101.

[7] 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.

[8] Feit, Walter and Thompson, John G. *Solvability of groups of odd order*, Pacific Journal of Mathematics, Volume 13, 1963, pgs. 775-1029, Reviewer: M. Suzuki.

[9] Károlyi, Gyula *On restricted set addition in abelian groups*, Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Mathematica, **46** (2003) 47–53.

[10] Károlyi, Gyula *The Erdős-Heilbronn problem in abelian groups*, Israel Journal of Mathematics, **139** (2004) 349–359.

[11] Károlyi, Gyula *The Cauchy-Davenport theorem in group extensions*, L' Enseignement Mathematique, **51** (2005) 239–254.

[12] Károlyi, Gyula *An inverse theorem for the restricted set addition in abelain groups*, Journal of Algebra, **290** (2005) 557–593.

[13] Károlyi, Gyula *A compactness argument in the additive theory and the polynomial method*, Discrete Mathematics, **302** (2005) 124–144.

[14] Wheeler, Jeffrey Paul *The Cauchy-Davenport theorem and the Erdős-Heilbronn problem for finite groups*, Ph.D. Thesis, *http://jeffreypaulwheeler.com/*, 2008.