

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 $A + B := \{a + b \pmod p \mid a \in A, b \in B\}$. 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's¹ 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 operation².

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.

¹The 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.

²We 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

$$(1) \quad \mathbb{E} \subseteq \mathbb{P} + \mathbb{P}.$$

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 1813³ [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:

³Cauchy 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.

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 $|G| = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_n^{e_n}$ where $p_1 < p_2 < \dots < p_n$ are primes and 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 $q \mid |G|$. 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 $A + B := \{a + b \mid a \in A, b \in B\}$.

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

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

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

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

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

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

$$(3) \quad (k_1, \tilde{h}_1) \star (k_2, \tilde{h}_2) := (k_1 \phi_{\tilde{h}_1}(k_2) \eta_{\tilde{h}_1, \tilde{h}_2}, \tilde{h}_1 \tilde{h}_2).$$

where

$$(4) \quad \phi_{\tilde{h}} : K \rightarrow \text{Aut}(K)$$

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

$$(5) \quad \eta_{\tilde{h}_1, \tilde{h}_2} = \tilde{h}_1 \cdot \tilde{h}_2 \cdot (\widetilde{h_1 h_2})^{-1} \in K$$

with \tilde{h} the coset representative of h in G/K ⁴. Notice that $\eta : H \times H \rightarrow K$ (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

$$\begin{aligned} (6) \quad \psi_H(g_1) \star \psi_H(g_2) &= (k_1, h_1) \star (k_2, h_2) \\ (7) \quad &= (k_1 \phi_{h_1}(k_2) \eta_{h_1, h_2}, h_1 h_2) \\ (8) \quad &= (k_1 \tilde{h}_1 k_2 \tilde{h}_1^{-1} \tilde{h}_1 \tilde{h}_2 (\widetilde{h_1 h_2})^{-1}, h_1 h_2) \\ (9) \quad &= \psi_H(k_1 \tilde{h}_1 k_2 (\tilde{h}_1^{-1} \tilde{h}_1) \tilde{h}_2 (\widetilde{h_1 h_2})^{-1} \widetilde{h_1 h_2}) \\ (10) \quad &= \psi_H(k_1 \tilde{h}_1 k_2 \tilde{h}_2) \\ (11) \quad &= \psi_H(k_1 h_1 k_2 h_2) \\ &= \psi_H(g_1 g_2) \end{aligned}$$

□

In summary, for $A \subseteq G$, we have an isomorphism $A \rightarrow K \times H$, in particular, $A \cong \{(k_1, h_1), (k_2, h_2), \dots, (k_t, h_t)\}$ for some $k_1, k_2, \dots, k_t \in K$ and (fixed) $h_1, h_2, \dots, h_t \in H$. 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 .

⁴i.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

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

As well

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

And clearly

$$(14) \quad \eta_{1,1} = 1.$$

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 $i = -k \cdot j$,

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

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

To show we were not just lucky,

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

and

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

□

Example 3.3.

Let p be a prime. Then

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

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

Hence

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

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

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

Hence

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

□

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 $S \subseteq G$,

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

We will define

$$S^1 := \{k_i \in K \mid \exists h_i \in H \text{ such that } (k_i, h_i) \in S\} \text{ and}$$

$$S^2 := \{h_i \in G \setminus K \mid \exists k_i \in K \text{ where } (k_i, h_i) \in S\}.$$

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

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

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

Hence

Definition 4.1.

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

Following Definition 4.1,

Remark 4.2.

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

Since we will be concerned with non-abelian groups,

Definition 4.3.

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

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

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 $i \in \{1, \dots, \alpha\}$ and each $j \in \{1, \dots, \beta\}$,

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

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 than 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)

$$|S \cdot T| \geq |S_1 \cdot T_1| + |S_1 \cdot T_2| + \dots + |S_1 \cdot T_\beta| + \alpha - 1$$

By Lemma 4.5, we have

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

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

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

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

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

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

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

⁵By 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 $A \dot{+} B := \{a + b \pmod{p} \mid a \in A, b \in B \text{ and } a \neq b\}$.

The conjecture was first proved for the case $A = B$ by J.A. Dias da Silva and Y.O. Hamidoune in 1994 [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 Mathématique, **51** (2005) 239–254.
- [12] Károlyi, Gyula *An inverse theorem for the restricted set addition in abelian 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.