Sumset growth for multiplicative subgroups of a finite field

by

Albert Cochrane

A THESIS

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2021

Approved by:

Major Professor
Craig Spencer

Copyright

Abstract

For a given prime p, let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ denote the finite field of p elements and $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ the multiplicative group of units. For an integer k, we define A as the cyclic subgroup of k^{th} powers in $\mathbb{Z}_p^*$, $A = \{x^k : x \in \mathbb{Z}_p^*\}$. In this thesis, we analyze properties of the sumset $A + A$. In particular we will look at several conjectures and lemmas involving the size of $A + A$, as well as how the size of A relative to p affects the Waring Number modulo p. Throughout the research for this thesis, programs written in Python were used to generate computational data which in turn was used to formulate conjectures. Some of these conjectures have been proven and are presented as theorems, while others remain open.

Table of Contents

List of Figures

List of Tables

Chapter 1

Constructing a Multiplicative Subgroup of $\mathbb{Z}/p\mathbb{Z}$

For a given prime p, let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ denote the finite field of p elements and $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ the multiplicative group of units. For an integer k, we define A as the cyclic subgroup of k^{th} powers in $\mathbb{Z}_p^*$, $A = \{x^k : x \in \mathbb{Z}_p^*\}$. Setting $d = \gcd(k, p-1)$, we have $|A| = \frac{p-1}{d}$, so we can restrict our attention to the case that k is a positive divisor of $p-1$. Set $t := |A| = \frac{p-1}{k}$. Let g be a primitive element $\pmod p$. Then, g generates $\mathbb{Z}_p^*$, that is, $\mathbb{Z}_p^* = \langle g \rangle = \{1,\ g,\ g^2, ..., g^{p-2}\}$. It follows that $A = \langle \omega \rangle = \{1, \omega, \omega^2, ..., \omega^{t-1}\}$, where $\omega = g^k$.

1.1 A+A and Cosets of A

Recall the following concept from group theory. For a multiplicative subgroup A of $\mathbb{Z}_p^*$ and $x \in \mathbb{Z}_p^*$, a set of the form $xA = \{xa : a \in A\}$ is called a coset of A. We define

$$2A := A + A = \{a_1 + a_2 :\ a_1,\ a_2 \in A\}. \tag{1.1.1}$$

Because of the similarity in notation, it is important to note that the 2 in (1.1.1) denotes the number of times A is being added. Throughout this paper, $2A$ will always denote $A + A$

and not the coset $2A$ where 2 is viewed as an element of $\mathbb{Z}_p^*$.

Lemma 1.1.1. *For any multiplicative subgroup A of $\mathbb{Z}_p^*$, $A + A$ is a union of cosets of A together possibly with 0.*

Proof. Let x be a non-zero element of $A + A$. We can write $x = a_1 + a_2$ where $a_1,\ a_2 \in A$. Then, for any $a \in A$, $xa = (a_1 + a_2)a = a_1a + a_2a \in A + A$, because $a_1a,\ a_2a \in A$. Therefore, $xA \subseteq A + A$. Hence $\bigcup_{x \in A+A} xA \subseteq A + A$. Also note that $x = x1 \in xA$. Thus, $A + A = \bigcup_{x \in A+A} xA$. □

Lemma 1.1.2. *Let G be a finite cyclic group, A be a finite subgroup of G with order t, and x be an element of G. Then, $x \in A$ if and only if $x^t = 1$, the identity element of G.*

Proof. Let $G = \langle g \rangle$ with $|G| = n$. By Lagrange's theorem, $t|n$, that is, $tk = n$ for some positive integer k. Then

$$A = \langle g^k \rangle = \{1, g^k, g^{2k}, \ldots, g^{(t-1)k}\}.$$

Let $x \in G$, say $x = g^j$. Then $x \in A$ if and only if $k|j$. On the other hand, $x^t = 1$ if and only if $g^{jt} = 1$, that is, $n|jt$ (since $\mathrm{ord}(g) = n$), or equivalently, $\frac{n}{t}|j$, that is, $k|j$. □

Lemma 1.1.3. *For any multiplicative subgroup A of $\mathbb{Z}_p^*$, 0 is an element of $A + A$ if and only if $|A|$ is even.*

Proof. Suppose $t = |A|$ is even. Then, $(-1)^t = 1$. By Lemma 1.1.2, this means $-1 \in A$. 1 is trivially in A, so $-1 + 1 = 0 \in A + A$. Conversely, suppose $0 \in A + A$. Then, there exist $a_1,\ a_2 \in A$ such that $a_1 + a_2 = 0$, so $a_1 = -a_2$. It follows that $a_1a_2^{-1} = -1 \in A$, as A is closed under multiplication. Thus $(-1)^t = 1$, so t must be even. □

Putting together Lemmas 1.1.2 and 1.1.3, we immediately obtain the following:

Lemma 1.1.4. *Let λ be an integer denoting the number of distinct multiplicative cosets of A in $A+A$. Then, there exist $x_1, \ldots, x_\lambda \in \mathbb{Z}_p^*$ such that*

$$A+A = \begin{cases} \bigcup_{i=1}^{\lambda} x_i A \cup \{0\}, & \text{if } |A| \text{ is even,} \\ \bigcup_{i=1}^{\lambda} x_i A, & \text{if } |A| \text{ is odd.} \end{cases} \tag{1.1.2}$$

In particular,

$$|2A| = \begin{cases} \lambda t + 1, & \text{if } t \text{ is even,} \\ \lambda t, & \text{if } t \text{ is odd.} \end{cases} \tag{1.1.3}$$

Thus, in order to determine $|2A|$, it suffices to determine λ. To do this, we view the cosets as elements of the quotient group

$$G := \mathbb{Z}_p^*/A = \{g^i A : i = 0, 1, 2, \ldots, k-1\} = \{\overline{g}^i : i = 0, 1, \ldots, k-1\} = \langle \overline{g} \rangle. \tag{1.1.4}$$

Here, $\overline{g} := gA$. To justify the equalities in (1.1.4), let us recall that multiplication is defined on G by

$$\overline{g}^i * \overline{g}^j = \overline{g}^{i+j},$$

and that the identity element is $\overline{1} = A$. Since $g^k \in A$ we have $\overline{g}^k = \overline{1}$, and since g has order $p-1$ in $\mathbb{Z}_p^*$, k is the minimal exponent with this property. Therefore $\overline{g}$ has order k, that is, G is a cyclic group of order k.

Lemma 1.1.5. *Let G and H be multiplicative groups where e is the identity element of G and e' is the identity element of H. If $\eta : G \to H$ is a group homomorphism, then η is one-to-one if and only if $ker(\eta) = \{e\}$.*

Proof. Recall that $ker(\eta) = \{x \in G : \eta(x) = e'\}$. For any homomorphism η, $\eta(e) = \eta(ee) = \eta(e)\eta(e)$, and so by cancellation, $\eta(e) = e'$. Thus we always have $e \in ker(\eta)$. Suppose η

is one-to-one. Then e is the only element of $ker(\eta)$, implying $ker(\eta) = \{e\}$. Conversely, suppose $ker(\eta) = \{e\}$. For $x,\ y \in G$, suppose $\eta(x) = \eta(y)$. Then, $\eta(x)\eta(y^{-1}) = \eta(y)\eta(y^{-1})$. Thus, $\eta(xy^{-1}) = \eta(e) = e'$. Hence, $xy^{-1} \in ker(\eta)$, that is, $xy^{-1} = e$. It follows that $x = y$, and we conclude η is one-to-one. □

Lemma 1.1.6. *Let $G = \mathbb{Z}_p^*/A$, as in (1.1.4), and $\eta : G \to \mathbb{Z}_p^*$ be defined by $\eta(\overline{x}) = x^t$ for any $\overline{x} \in G$. Then η is a one-to-one homomorphism.*

Proof. First we observe that η is well defined. Suppose that $\overline{x} = \overline{y}$, that is, $xy^{-1} \in A$. Then $(xy^{-1})^t = 1$ and so $x^t = y^t$, that is, $\eta(\overline{x}) = \eta(\overline{y})$. Because multiplication is commutative in $\mathbb{Z}_p^*$, it is immediate that η is a homomorphism, i.e., $\eta(\overline{xy}) = \eta(\overline{x})\eta(\overline{y})$. To show that η is one-to-one it suffices to show that the kernel of η is just the identity element. Let $x \in \mathbb{Z}_p^*$. Then $\eta(\overline{x}) = 1$ if and only if $x^t = 1$, that is, $x \in A$, by Lemma 1.1.2. Note $x \in A$ is equivalent to saying $\overline{x} = \overline{1}$. □

Thus, if $\mathcal{S}$ is a collection of cosets of A, we can determine the number of distinct cosets in $\mathcal{S}$ by mapping $\mathcal{S}$ into $\mathbb{Z}_p^*$ using η and then counting the number of distinct points in $\eta(\mathcal{S})$. We saw earlier that $A + A$ can be expressed as a union of cosets of A together possibly with zero. To be precise, we claim the following:

Lemma 1.1.7. *If A is a multiplicative subgroup of $\mathbb{Z}_p^*$, then*

$$A + A = \begin{cases} \bigcup_{i=0}^{\frac{t}{2}-1} (1+\omega^i)A \cup \{0\}, & \text{if } |A| \text{ is even,} \\ \bigcup_{i=0}^{\frac{t-1}{2}} (1+\omega^i)A, & \text{if } |A| \text{ is odd.} \end{cases} \tag{1.1.5}$$

Proof. For any nonzero element $\omega^i + \omega^j$ in $A + A$, $\omega^i + \omega^j$ is in the coset $(\omega^i + \omega^j)A$ because 1 is trivially in A. Let $n = j - i$. Then, $(\omega^i + \omega^j)A = (1 + \omega^n)\omega^i A = (1 + \omega^n)A$. Thus, $A + A$ is a union of cosets of the form $(1 + \omega^i)A$ with $0 \le i < t$, together with 0 when t is even. We can further restrict i to the values indicated in (1.1.5) as follows. When t is even

and $i = \frac{t}{2}$, $1 + \omega^i = 0$ so $(1 + \omega^i)A = \{0\}$. Note that

$$(1 + \omega^i)A = (\omega^{-i} + 1)\omega^i A = (\omega^{t-i} + 1)A.$$

Thus for $\frac{t}{2} < i < t$, we can replace $(1 + \omega^i)A$ with $(1 + \omega^{t-i})A$, giving us the upper limits on the unions in (1.1.5). □

In general, the cosets listed in (1.1.5) need not be distinct. For the case of interest here, we take $\mathcal{S}$ to be the collection of these cosets.

$$\mathcal{S} := \begin{cases} \{(1 + \omega^i)A : 0 \leq i \leq \frac{t}{2} - 1\}, & \text{for even } t, \\ \{(1 + \omega^i)A : 0 \leq i \leq \frac{t-1}{2}\}, & \text{for odd } t. \end{cases} \tag{1.1.6}$$

Thus, to find $|2A|$, we must determine the cardinality of the following subset of $\mathbb{Z}_p^*$:

$$\eta(\mathcal{S}) = \begin{cases} \{(1 + \omega^i)^t : 0 \leq i \leq \frac{t}{2} - 1\}, & \text{for even } t, \\ \{(1 + \omega^i)^t : 0 \leq i \leq \frac{t-1}{2}\}, & \text{for odd } t. \end{cases} \tag{1.1.7}$$

1.2 Creating A Computationally

For the purposes of testing the conjectures in this paper, functions in Python were used to create the subgroup A. For a given prime p, we began by finding a primitive root of $\mathbb{Z}_p$. This was done via brute force by creating $\mathbb{Z}_p^*$ and an empty set G, and running the integers 2 to $p - 1$ in a 'for' loop, with the goal of finding a generator of $\mathbb{Z}_p^*$. To do this, G was filled by raising the current itinerant, a, to the powers 1 to $p - 1 \pmod p$. If this set did not equal $\mathbb{Z}_p^*$, G would be cleared to repeat the process for the next integer. The loop would run until $G = \mathbb{Z}_p^*$. When this equality was reached, we set $g = a$ and use this as the generator of $\mathbb{Z}_p^*$. Then, $\omega = g^k$ would be used as the generator for the cyclic subgroup of k^{th} powers in $\mathbb{Z}_p^*$.

```python
def generator(p):
    '''
    Arg: p - prime for which a generator g of Z_p^* will be found
    Returns: g
    '''
    ZPstar= set(range(1,p))
    G=set()

    for g in range(2,p):

        G=set(pow(g,x,p) for x in range(1,p))
        if G==ZPstar:
            return g
```

Figure 1.1: *Jupyter Notebook cell containing the generator function described above*

It should be noted that there are more efficient algorithms to find a generator; however this ran quickly enough for our purposes. With ω in hand, we can create $A = \{x^k : x \in \mathbb{Z}_p^*\}$, by raising $\omega = g^k$ to the powers $1,\ 2, ..., t$ and storing each value in a list.

1.3 Finding the size of $A + A$ directly

We used two distinct methods to calculate $|2A|$. The first involved constructing A as described above and then actually creating $A + A$ in Python. After having constructed A, nested for loops were used to add A to itself element-wise $\pmod p$. Once $2A$ was created, we simply found $|2A|$ using Python's length function, $len()$, which returns the number of elements in a given list. For a given prime, the same value g can be used to find generators $\omega = g^k$ for all subgroups of k^{th} powers, so we typically calculated $|2A|$ for all non-trivial positive divisors k of $p-1$ before moving on to the next prime. The code for this method is displayed in Figure 1.2 below.

```
for i in range(num):
    #fix a prime p
    p=primesList[i]

    #find primitive element of Zp*, g
    g=generator(p)

    n=p-1

    #initialize divisor list
    D=[]

    #brute force divisor finder
    for i in range(2,n//2+1):
        if (n % i==0):
            D.append(i)

    #creates A for each divisor k of p-1
    for k in D:

        #cardinality of A=(p-1)/k
        t=n//k

        A=[pow(g,i*k, p) for i in range(t)]

        #creates 2A and finds |2A|
        twoA=set((A[i]+A[j])%p for i in range(t) for j in range(t))

        size2A=len(twoA)
```

Figure 1.2: *Code used in constructive method of finding* $|2A|$

1.4 Finding the size of $A + A$ using cosets

As we saw in Section 1.1, we do not need to create the actual set $A+A$ to find its cardinality. In fact, we do not need to create the set A itself. Instead, we created the set $\eta(\mathcal{S})$ from (1.1.7) to find the number of distinct cosets of A in $A+A$, λ, and then calculated $|2A|$ using (1.1.3). The function in Python we used here followed the same principle of looping through all divisors k of $p-1$ before moving on to the next prime, again to save time by only needing to find the generator g once for each prime. The code for this method is displayed in Figure 1.3 below.

```
for i in range(num):
    p=primesList[i]
    g=generator(p)
    n=p-1
    D=[]

    for i in range(2,n//2+1):
        if (n % i==0):
            D.append(i)

    #creates set S for each divisor k of p-1
    for k in D:
        tempS=[]
        t=n//k

        #omega = g^k
        w=pow(g,k,p)

        #raises (1+w^i)^t for 0<=i<t/2
        for i in range(t//2+1):

            #finds potential element, s, of S
            s=pow((1+pow(w,i,p)),t,p)

            #if s is nonzero, it is added to S
            if s != 0:
                tempS.append(s)

        #remove redundacies
        S=list(set(tempS))

        #test parity of |A|
        if t%2==0:
            size2A= len(S)*t+1
        else:
            size2A= len(S)*t
```

Figure 1.3: *Code used to find* $|\eta(\mathcal{S})|$ *from (1.1.7)*

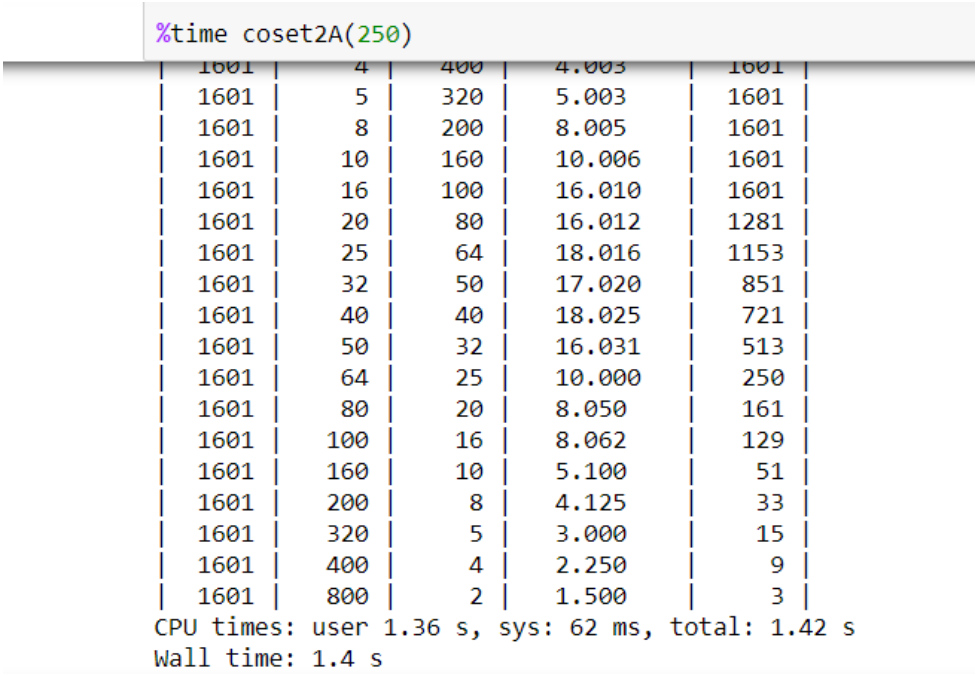
1.5 Relative efficiency of the two algorithms

The motivation for creating this second method of finding $|2A|$ was a desire to test conjectures for larger primes, which was excessively time-consuming using the constructive method. While the first method works well for relatively small primes, say $p < 15,000$, and has the benefit of being able to show the actual elements of $2A$, it becomes too slow at a certain point to effectively gather data for larger primes.

Looking at the two processes side by side, one can see they are essentially identical in their setups until the point where we begin looping through the divisors k of $p-1$ for a given prime p. Then, for a specific subgroup A of k^{th} powers, creating $A+A$ in the first method requires roughly t^2 iterations whereas creating $\eta(S)$ in the second method only requires roughly $t/2$ iterations. The trade off is that the latter requires an extra modular exponentiation in the process; however, Python's 'pow' function is able to take care of this quickly enough that the added time is negligible. Below we will compare the two algorithms' run times by looking at output generated while including the 'time' magic command which calculates how long a section of code takes to complete. The five columns in the data presented above the time printout represent p, k, t, the ratio $|2A|/|A|$, and $|2A|$, respectively. The ratio $|2A|/|A|$ is called the doubling constant, and it will be explored in much greater detail in the following chapter.

```
%time constructive2A(250)
|  1601 |     4 |   400 |   4.003   |  1601 |
|  1601 |     5 |   320 |   5.003   |  1601 |
|  1601 |     8 |   200 |   8.005   |  1601 |
|  1601 |    10 |   160 |  10.006   |  1601 |
|  1601 |    16 |   100 |  16.010   |  1601 |
|  1601 |    20 |    80 |  16.012   |  1281 |
|  1601 |    25 |    64 |  18.016   |  1153 |
|  1601 |    32 |    50 |  17.020   |   851 |
|  1601 |    40 |    40 |  18.025   |   721 |
|  1601 |    50 |    32 |  16.031   |   513 |
|  1601 |    64 |    25 |  10.000   |   250 |
|  1601 |    80 |    20 |   8.050   |   161 |
|  1601 |   100 |    16 |   8.062   |   129 |
|  1601 |   160 |    10 |   5.100   |    51 |
|  1601 |   200 |     8 |   4.125   |    33 |
|  1601 |   320 |     5 |   3.000   |    15 |
|  1601 |   400 |     4 |   2.250   |     9 |
|  1601 |   800 |     2 |   1.500   |     3 |
CPU times: user 11.3 s, sys: 1.48 s, total: 12.8 s
Wall time: 12.8 s
```

Figure 1.4: *Timing the constructive method for first 250 primes*



```
%time coset2A(250)
| 1601 |    4 |  400 |   4.003   | 1601 |
| 1601 |    5 |  320 |   5.003   | 1601 |
| 1601 |    8 |  200 |   8.005   | 1601 |
| 1601 |   10 |  160 |  10.006   | 1601 |
| 1601 |   16 |  100 |  16.010   | 1601 |
| 1601 |   20 |   80 |  16.012   | 1281 |
| 1601 |   25 |   64 |  18.016   | 1153 |
| 1601 |   32 |   50 |  17.020   |  851 |
| 1601 |   40 |   40 |  18.025   |  721 |
| 1601 |   50 |   32 |  16.031   |  513 |
| 1601 |   64 |   25 |  10.000   |  250 |
| 1601 |   80 |   20 |   8.050   |  161 |
| 1601 |  100 |   16 |   8.062   |  129 |
| 1601 |  160 |   10 |   5.100   |   51 |
| 1601 |  200 |    8 |   4.125   |   33 |
| 1601 |  320 |    5 |   3.000   |   15 |
| 1601 |  400 |    4 |   2.250   |    9 |
| 1601 |  800 |    2 |   1.500   |    3 |
CPU times: user 1.36 s, sys: 62 ms, total: 1.42 s
Wall time: 1.4 s
```

Figure 1.5: *Timing the coset method for first 250 primes*

We can see that for relatively small primes, the coset method of finding $|2A|$ is significantly quicker than the constructive method; however, the latter is still quite effective as 11 seconds is not a significant amount of time. Now we will look at their respective times for finding $|2A|$ for the first 1000 primes.

```
%time constructive2A(1000)
|  7919 |  3959 |     2 |   1.500    |     3 |

|  7927 |     2 |  3963 |   2.000    |  7926 |
|  7927 |     3 |  2642 |   3.000    |  7927 |
|  7927 |     6 |  1321 |   6.000    |  7926 |
|  7927 |  1321 |     6 |   3.167    |    19 |
|  7927 |  2642 |     3 |   2.000    |     6 |
|  7927 |  3963 |     2 |   1.500    |     3 |
|  7933 |     2 |  3966 |   2.000    |  7933 |
|  7933 |     3 |  2644 |   3.000    |  7933 |
|  7933 |     4 |  1983 |   4.000    |  7932 |
|  7933 |     6 |  1322 |   6.001    |  7933 |
|  7933 |    12 |   661 |  12.000    |  7932 |
|  7933 |   661 |    12 |   6.083    |    73 |
|  7933 |  1322 |     6 |   3.167    |    19 |
|  7933 |  1983 |     4 |   2.250    |     9 |
|  7933 |  2644 |     3 |   2.000    |     6 |
|  7933 |  3966 |     2 |   1.500    |     3 |
CPU times: user 16min 48s, sys: 609 ms, total: 16min 49s
Wall time: 16min 51s
```

Figure 1.6: *Timing the constructive method for first 1000 primes*

```
%time coset2A(1000)
|  7919 |  3959 |     2 |   1.500    |     3 |
|  7927 |     2 |  3963 |   2.000    |  7926 |
|  7927 |     3 |  2642 |   3.000    |  7927 |
|  7927 |     6 |  1321 |   6.000    |  7926 |
|  7927 |  1321 |     6 |   3.167    |    19 |
|  7927 |  2642 |     3 |   2.000    |     6 |
|  7927 |  3963 |     2 |   1.500    |     3 |
|  7933 |     2 |  3966 |   2.000    |  7933 |
|  7933 |     3 |  2644 |   3.000    |  7933 |
|  7933 |     4 |  1983 |   4.000    |  7932 |
|  7933 |     6 |  1322 |   6.001    |  7933 |
|  7933 |    12 |   661 |  12.000    |  7932 |
|  7933 |   661 |    12 |   6.083    |    73 |
|  7933 |  1322 |     6 |   3.167    |    19 |
|  7933 |  1983 |     4 |   2.250    |     9 |
|  7933 |  2644 |     3 |   2.000    |     6 |
|  7933 |  3966 |     2 |   1.500    |     3 |
CPU times: user 10.5 s, sys: 141 ms, total: 10.6 s
Wall time: 10.4 s
```

Figure 1.7: *Timing the coset method for first 1000 primes*

Here, we can see a significant difference, with the coset method only taking 10 seconds

compared to nearly 17 minutes for the other. This difference only becomes more significant as the values of p become larger, so for data involving $|2A|$ where $p > 15000$, the coset method was the algorithm we selected.

Chapter 2

The Doubling Constant

After finding the sizes of A and $A + A = 2A$, we define the doubling constant, denoted $\sigma(A)$, as the ratio $\sigma(A) = \frac{|2A|}{|A|}$. Here is an example looking at the group of fourth powers (mod 13). Note that 2 generates $\mathbb{Z}_{13}^*$ and 2^4 generates the subgroup of fourth powers.

$$A = \{x^4 : x \in \mathbb{Z}_{13}^*\} = \{2^4,\ 2^8,\ 2^{12}\} = \{3,\ 9,\ 1\}. \tag{2.0.1}$$

Thus, $A + A = \{2,\ 4,\ 5,\ 6,\ 10,\ 12\}$, and $\sigma(A) = \frac{6}{3} = 2$.

2.1 Background on Sumset Growth

2.1.1 Minimal Doubling of A

We begin by looking at the cases where the minimal amount of growth occurs when adding A to itself. If $|A| = 1$, then trivially, $|2A| = 1$. If $A = \mathbb{Z}_p^*$, $2A = \mathbb{Z}_p$ is also trivial. For $2 \leq |A| \leq p - 1$, we begin by considering the Cauchy-Davenport inequality [1, 2]. Here, we will roughly follow the proof in [3].

Theorem 2.1.1 (Cauchy-Davenport)**.** *For a prime p and non-empty sets $S, T \subseteq \mathbb{Z}_p$,*

$$|S+T| \geq \min(|S|+|T|-1,\ p).$$

Proof. We will proceed by induction on $|T|$. For $|T|=1$ the statement is trivial. The same is true when $|S|=p$. Suppose $|T| \geq 2,\ |S|<p$, and that the theorem holds for all sets $T' \subseteq \mathbb{Z}_p$ such that $|T'|<|T|$. By translation of T, we may assume $0 \in T$. Thus, $S+T \supseteq S$. We will show that $|S+T|>|S|$. For the sake of contradiction, assume $|S+T|=|S|$ which would mean $S+T=S$. Let t be a non-zero element of T. Then, $S+t \subseteq S,\ S+2t \subseteq S$, and in general, $S+nt \subseteq S$ for any natural number n. This implies $\mathbb{Z}_p \subseteq S$, that is, $\mathbb{Z}_p = S$, contrary to our assumption. Thus, $|S+T|>|S|$. Since $S+T \nsubseteq S$, there must exist an element s_0 of S such that $s_0+T \nsubseteq S$. Let $T_0 = \{t \in T : s_0+t \notin S\}$. Set $S' = S \cup (s_0+T_0)$ and $T' = T - T_0$. Thus, $|T'|<|T|$.

We claim that $S'+T' \subseteq S+T$. Indeed, $S'+T' = (S+T') \cup (s_0+T_0+T')$. It is trivial that $S+T' \subseteq S+T$. We need to show that $s_0+T_0+T' \subseteq S+T$. Let $t_0 \in T_0$ and $t' \in T'$. Because $t' \in T'$, there exists an $s_1 \in S$ with $s_0+t'=s_1$. Thus $s_0+t_0+t' = s_1+t_0 \in S+T$, and $s_0+T_0+T' \subseteq S+T$. Note that $(s_0+T_0) \cap S = \emptyset$. Thus, $|S'| = |S|+|s_0+T_0| = |S|+|T_0|$.

Thus, we have constructed two new sets $S',\ T'$ such that

$$|S'|+|T'| = (|S|+|T_0|)+(|T|-|T_0|) = |S|+|T|,$$

$|S+T| \geq |S'+T'|$, and $|T'|<|T|$. By applying the induction assumption to $S',\ T'$, we have that $|S'+T'| \geq |S'|+|T'|-1$. Thus,

$$|S+T| \geq |S'+T'| \geq |S'|+|T'|-1 = |S|+|T|-1$$

. □

The Cauchy-Davenport inequality is the best possible bound for arithmetic progressions with

the same difference.

Lemma 2.1.1. *If A, B are arithmetic progressions in $\mathbb{Z}_p$ with common difference d, then*

$$|A+B| = \min(|A|+|B|-1, p).$$

Proof. Let A be an arithmetic progression of length $k = |A|$, and B be of length $l = |B|$. Let $A = \{a_0 + dx : 1 \leq x \leq k\}$, and $B = \{b_0 + dy : 1 \leq y \leq l\}$, where $a_0, b_0, d \in \mathbb{Z}_p$ with $d \neq 0$. Then, $(a_0 + dx) + (b_0 + dy) = (a_0 + b_0) + d(x + y)$ is a typical element of $A + B$, and so,

$$A + B = \{(a_0 + b_0) + d(x + y) : 2 \leq x + y \leq k + l\}.$$

Thus, if $k + l - 1 \leq p$, $|A + B| = |A| + |B| - 1$; otherwise $|A + B| = p$. □

Note that when $|A| = 2$, we have $A = \{-1,\ 1\}$, an arithmetic progression, and $|2A| = 3 = 2|A| - 1$. For $|A| > 2$ we can say more.

Lemma 2.1.2. *Let A be the multiplicative subgroup of k^{th} powers in $\mathbb{Z}_p^*$. If $3 \leq |A| < p-1$, then*

$$|2A| \geq \begin{cases} 2|A|, & \text{if } t \text{ is odd,} \\ 2|A|+1, & \text{if } t \text{ is even.} \end{cases}$$

Proof. By the Cauchy-Davenport inequality (Theorem 2.1.1), we have that $2|A| \geq 2t - 1$. If t is odd, then by Lemma 1.1.4, $|2A| = \lambda t$. Thus, $\lambda t \geq 2t - 1$, implying that $\lambda \geq 2$. Similarly, if t is even, then $|2A| = \lambda t + 1$, and so $\lambda t + 1 \geq 2t - 1$, which implies that $\lambda \geq 2$. □

2.1.2 Maximal Doubling of A

We also consider the cases where the maximum amount of growth occurs when adding A to itself. Combinatorially, the number of distinct sums $a_1 + a_2$ with $a_1,\ a_2 \in A$ is at most

$\binom{t}{2} + t = \frac{t(t+1)}{2}$. For even t, there are $\frac{t}{2}$ sums with $a_1 + a_2 = 0$ since $-1 \in A$, and so the number of distinct sums is at most $\frac{t(t+1)}{2} - (\frac{t}{2} - 1) = \frac{t^2}{2} + 1$. The other situation we will consider an occurrence of maximal doubling is when $2A$ is simply $\mathbb{Z}_p$ or $\mathbb{Z}_p^*$. This will be looked at more thoroughly in Chapter 3.

Definition 2.1.1. *We say that a subgroup A has maximal doubling if*

$$|2A| = \begin{cases} \min\left(\dfrac{t(t+1)}{2},\ p-1\right), & \text{for odd } t, \\ \min\left(\dfrac{t^2}{2}+1,\ p\right), & \text{for even } t. \end{cases} \tag{2.1.1}$$

Maximal doubling is equivalent to saying that all the cosets listed in (1.1.5) are distinct, or that $2A \supseteq \mathbb{Z}_p^*$.

We begin our study of $\sigma(A)$ by looking at the case where A is the group of squares (mod p).

Lemma 2.1.3. *Let $p > 5$ be a prime and A be the multiplicative subgroup of squares in $\mathbb{Z}_p^*$. Then,*

$$|2A| = \begin{cases} p-1, & \text{for } p \equiv 3 \pmod 4, \\ p, & \text{for } p \equiv 1 \pmod 4. \end{cases}$$

Note that when $p = 5$, $A = \{-1, 1\}$, so $|2A| = 3$, as shown earlier.

Proof. Since $p > 5$, we have $|A| = \frac{p-1}{2} \geq 3$. Thus, by Lemma 2.1.2, $|2A| \geq 2|A| = p - 1$ if t is odd, and $|2A| \geq 2|A| + 1 = p$ if t is even. When t is odd, we get $|2A| = p - 1$ because $0 \notin 2A$. Note, t is even when $p \equiv 1 \pmod 4$, and t is odd when $p \equiv 3 \pmod 4$. □

Note that in the case where $k = 2$ and $p > 5$, we have both maximal doubling and minimal doubling in the sense of Lemma 2.1.2, that is, $|2A| = 2|A|$ or $|2A| = 2|A| + 1$.

2.2 Computational Data on $\sigma(A)$

To gain more insight into the relationship between the size of A and the doubling constant $\sigma(A)$, we used functions in Python to generate raw data and then test specific conjectures. Some of these have been proven and will be presented as lemmas, while others have been confirmed computationally for a significant number of primes, but remain under investigation. For each of these, we will comment on how many primes it has been tested for, list any exceptions that occurred, and show some samples of the data. In most cases, the tests could have been ran much further; however, for practical purposes we generally stopped after the first 2,500 to 10,000 primes if the result seemed clear.

If $|A| = 3$ we observed that $|2A| = 2|A|$ for all primes $p < 30,000$. Part of this data is seen in the table below.

Table 2.1: *First 30 rows of data*

p	k	t	$\sigma(A)$
7	2	3	2.000
13	4	3	2.000
19	6	3	2.000
31	10	3	2.000
37	12	3	2.000
43	14	3	2.000
61	20	3	2.000
67	22	3	2.000
73	24	3	2.000
79	26	3	2.000
97	32	3	2.000
103	34	3	2.000
109	36	3	2.000
127	42	3	2.000
139	46	3	2.000
151	50	3	2.000
157	52	3	2.000
163	54	3	2.000
181	60	3	2.000
193	64	3	2.000
199	66	3	2.000
211	70	3	2.000
223	74	3	2.000
229	76	3	2.000
241	80	3	2.000
271	90	3	2.000
277	92	3	2.000
283	94	3	2.000

This led us to the following result.

Lemma 2.2.1. *Suppose* $|A| = 3$. *Then,* $|2A| = 2|A|$.

Proof. For $|A| = 3$, we can write $A = \{1, \omega, \omega^2\}$, where $A = \langle\omega\rangle$. Then,

$$2A = \{2, 2\omega, 2\omega^2, 1+\omega, 1+\omega^2, \omega+\omega^2\}. \tag{2.2.1}$$

To show $|2A| = 2|A|$, it suffices to show all of the values listed in (2.2.1) are distinct. Working in $\mathbb{Z}_p$, we have that $\omega^3 = 1$. Thus, $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$, and since $\omega - 1 \neq 0$, we have $\omega^2 + \omega + 1 = 0$, yielding

$$\omega^2 = -1 - \omega. \tag{2.2.2}$$

We can easily show the elements in $2A$ are pairwise distinct through contradiction. Because $1,\ \omega$, and ω^2 are distinct, it follows that $2,\ 2\omega$, and $2\omega^2$ are distinct, and $1+\omega, 1+\omega^2$, and $\omega+\omega^2$ are distinct as well. Now suppose $2\omega = 1+\omega^2$. Then, by (2.2.2), $2\omega = 1+\omega^2 = -\omega$, so $3\omega = 0$. However, $\omega \neq 0$, $3 \neq 0$, and $\mathbb{Z}_p$ has no zero divisors, giving us a contradiction. Using similar methods, it is easy to check that $\{2, 2\omega, 2\omega^2\} \cap \{1+\omega, 1+\omega^2, \omega+\omega^2\} = \emptyset$. Thus, $|2A| = 6 = 2|A|$. □

If $|A| = 4$ we observed that $|2A| = 2|A| + 1$ for all primes $5 < p < 30,000$. We then generated the data again, this time including a test of this observation. The result of this test is indicated by a True or False in the leftmost column of the table.

Table 2.2: *First 30 rows of data including the mentioned test*

True/False	p	k	t	$\sigma(A)$
T	13	3	4	2.250
T	17	4	4	2.250
T	29	7	4	2.250
T	37	9	4	2.250
T	41	10	4	2.250
T	53	13	4	2.250
T	61	15	4	2.250
T	73	18	4	2.250
T	89	22	4	2.250
T	97	24	4	2.250
T	101	25	4	2.250
T	109	27	4	2.250
T	113	28	4	2.250
T	137	34	4	2.250
T	149	37	4	2.250
T	157	39	4	2.250
T	173	43	4	2.250
T	181	45	4	2.250
T	193	48	4	2.250
T	197	49	4	2.250
T	229	57	4	2.250
T	233	58	4	2.250
T	241	60	4	2.250
T	257	64	4	2.250
T	269	67	4	2.250
T	277	69	4	2.250
T	281	70	4	2.250
T	293	73	4	2.250
T	313	78	4	2.250

This led us to the following result. Note that if λ is the number of distinct cosets of A in $A + A$, we can write $\sigma(A) = \lambda$ when t is odd, and $\sigma(A) = \lambda + \frac{1}{t}$ when t is even, so $\lambda = \lfloor \sigma(A) \rfloor$. This explains the nonzero decimal part of $\sigma(A)$ which appears in several of the tables.

Lemma 2.2.2. *Suppose $A = \langle \omega \rangle$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ where $|A| = 4$ and $p > 5$. Then, $|2A| = 2|A| + 1$.*

Note that when $p = 5$, the only subgroup of order 4 is trivially $\mathbb{Z}_p^*$, and $2A$ is trivially $\mathbb{Z}_p$.

Proof. For $|A| = 4$, we have $A = \{1,\ \omega,\ \omega^2,\ \omega^3\}$. Working in $\mathbb{Z}_p$, we have that $\omega^4 = 1$. Thus, $0 = \omega^4 - 1 = (\omega^2 - 1)(\omega^2 + 1)$. By noting that $\omega^2 \neq 1$, we get that $\omega^2 + 1 = 0$, yielding $\omega^2 = -1$ and $\omega^3 = -\omega$.

We can now write $A = \{\pm 1, \pm\omega\}$, and we get that

$$2A = \{0, \pm 2, \pm 2\omega, \pm(1 + \omega), \pm(1 - \omega)\}.$$

Similar to the analysis in Lemma 2.2.1, one can show that these values are all distinct. Thus, $|2A| = 9 = 2|A| + 1$. □

We can now restrict our attention to the case where $5 \leq |A| \leq \frac{p-1}{3}$, that is, $t \geq 5$ and $k \geq 3$.

Table 2.3: *Testing if* $|2A| \geq 3|A|$ *for* $t \geq 5$ *and* $k \geq 3$

True/False	p	k	t	$\sigma(A)$
T	19	3	6	3.167
T	29	4	7	3.000
T	31	3	10	3.100
T	31	5	6	3.167
T	31	6	5	3.000
T	37	3	12	3.083
T	37	4	9	4.000
T	37	6	6	3.167
T	41	4	10	3.100
T	41	5	8	3.125
T	41	8	5	3.000
T	43	3	14	3.071
T	43	6	7	3.000
T	43	7	6	3.167
T	53	4	13	4.000
T	61	3	20	3.050
T	61	4	15	4.000
T	61	5	12	4.083
T	61	6	10	4.100
T	61	10	6	3.167
T	61	12	5	3.000
T	67	3	22	3.045
T	67	6	11	5.000
T	67	11	6	3.167
T	71	5	14	4.071
T	71	7	10	5.100
T	71	10	7	4.000
T	71	14	5	3.000
T	73	3	24	3.042
T	73	4	18	4.056
T	73	6	12	5.083

We observe that $\sigma(A) \geq 3$ uniformly in our data.

Conjecture 2.2.1. *If* $5 \leq |A| \leq \frac{p-1}{3}$*, then* $|2A| \geq 3|A|$.

This conjecture has been confirmed for primes $p < 30,000$. Part of the data can be seen

in the table above. It would follow from Conjecture 2.2.1 that for $p > 5$,

$$|2A| = 2|A| \text{ if and only if } t = 3, \text{ or } p \equiv 3 \pmod 4 \text{ and } t = \frac{p-1}{2}, \tag{2.2.3}$$

$$|2A| = 2|A| + 1 \text{ if and only if } t = 4, \text{ or } p \equiv 1 \bmod 4 \text{ and } t = \frac{p-1}{2}. \tag{2.2.4}$$

While proving Conjecture 2.2.1 for all cases remains under investigation, we can continue looking at doubling for specific values of t. Here, we will return to the notation in (1.1.5). Recall,

$$A + A = \begin{cases} \bigcup_{i=0}^{\frac{t}{2}-1} (1+\omega^i)A \cup \{0\}, & \text{if } |A| \text{ is even,} \\ \bigcup_{i=0}^{\frac{t-1}{2}} (1+\omega^i)A, & \text{if } |A| \text{ is odd.} \end{cases} \tag{2.2.5}$$

We will now look at the case where $|A| = 5$. In the following table the True/False column indicates whether $|2A| = 3|A|$.

Table 2.4: *First 30 rows of data for* $t = 5$

True/False	p	k	t	$\sigma(A)$
FAL	11	2	5	2.000
T	31	6	5	3.000
T	41	8	5	3.000
T	61	12	5	3.000
T	71	14	5	3.000
T	101	20	5	3.000
T	131	26	5	3.000
T	151	30	5	3.000
T	181	36	5	3.000
T	191	38	5	3.000
T	211	42	5	3.000
T	241	48	5	3.000
T	251	50	5	3.000
T	271	54	5	3.000
T	281	56	5	3.000
T	311	62	5	3.000
T	331	66	5	3.000
T	401	80	5	3.000
T	421	84	5	3.000
T	431	86	5	3.000
T	461	92	5	3.000
T	491	98	5	3.000
T	521	104	5	3.000
T	541	108	5	3.000
T	571	114	5	3.000
T	601	120	5	3.000
T	631	126	5	3.000
T	641	128	5	3.000
T	661	132	5	3.000
T	691	138	5	3.000
T	701	140	5	3.000

Based on the data, we conjectured and proved the following result.

Lemma 2.2.3. *Suppose* A *is a multiplicative subgroup of* $\mathbb{Z}_p^*$ *where* $|A| = 5$ *and* $p > 11$. *Then,* $|2A| = 3|A|$.

Proof. Let $A = \langle \omega \rangle = \{1, \omega, \omega^2, \omega^3, \omega^4\}$ be the group of order 5 in $\mathbb{Z}_p^*$. Using the notation in

(2.2.5), we know

$$A + A = (1 + 1)A \cup (1 + \omega)A \cup (1 + \omega^2)A.$$

We claim that for $p > 11$, the three cosets listed here are distinct, and therefore $|2A| = 3|A|$. If $(1 + 1)A \cap (1 + \omega)A \neq \emptyset$ then $1 + \omega = 2\omega^i$ for some $0 \leq i \leq 4$. Now, $1 + \omega = 2$ and $1 + \omega = 2\omega$ are plainly false. $1 + \omega = 2\omega^2$ gives $(2\omega + 1)(\omega - 1) = 0$, implying that $\omega = -2^{-1}$ and so $2^5 \equiv -1 \pmod{p}$, that is, $p|33$, in violation of the assumption that $p > 11$. Next, suppose $1 + \omega = 2\omega^3$. Squaring and using $\omega^6 = \omega$ gives $(\omega - 1)^2 = 0$, which cannot happen. Finally, suppose $1 + \omega = 2\omega^4$. Then $\omega + \omega^2 = 2$, that is, $(\omega + 2)(\omega - 1) = 0$, implying $\omega = -2$. Then $1 = \omega^5 = -32$, that is, $p|33$ which does not occur.

In a similar manner, one can show that $(1 + 1)A \cap (1 + \omega^2)A = \emptyset$ for $p > 11$. Indeed ω^2 is just another generator for A, and so it is the same proof. Consider now the intersection $(1 + \omega)A \cap (1 + \omega^2)A$. If it is nonempty then $1 + \omega^2 = \omega^i + \omega^{i+1}$ for some $0 \leq i \leq 4$. This is plainly impossible for $i = 0, 1, 2$ and 4. Suppose $1 + \omega^2 = \omega^3 + \omega^4$, that is, $\omega^2(1 - \omega^2) = \omega^3 - 1$. Then, dividing by $\omega - 1$ gives $-\omega^2(1 + \omega) = \omega^2 + \omega + 1$, so $\omega^3 + 2\omega^2 + \omega + 1 = 0$. Combining this with $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$, we have that $\omega^4 - \omega^2 = 0$ which is impossible. □

For the case where $|A| = 6$, we have the following result.

Lemma 2.2.4. *For any prime $p \neq 7, 13$ and subgroup A of $\mathbb{Z}_p^*$ of order $|A| = 6$, we have $|2A| = 3|A| + 1$.*

Proof. Let $A = \langle \omega \rangle$ be a group of order 6 in $\mathbb{Z}_p^*$. Then $\omega^6 = 1$, $\omega^3 = -1$ and $\omega^2 = \omega - 1$. By (2.2.5),

$$A + A = (1 + 1)A \cup (1 + \omega)A \cup (1 + \omega^2)A \cup \{0\}.$$

By using similar methods to those in the proof of Lemma 2.2.3, it is routine to check that for $p > 13$, the cosets listed here are distinct. Hence $|2A| = 3|A| + 1$. □

We now examine the cases where $7 \leq |A| \leq \frac{p-1}{4}$. Our data led to the following conjecture.

Conjecture 2.2.2. *For a multiplicative subgroup A of $\mathbb{Z}_p^*$, if $7 \leq |A| \leq \frac{p-1}{4}$ and $(k,t,p) \neq (4,7,29),(4,10,41),(5,8,41)$ or $(6,7,43)$, then $|2A| \geq 4|A|$.*

This conjecture was confirmed for primes $p < 30,000$.

Table 2.5: *Partial data testing Conjecture 2.2.2*

True/False	p	k	t	$\sigma(A)$
FAL	29	4	7	3.000
T	37	4	9	4.000
FAL	41	4	10	3.100
FAL	41	5	8	3.125
FAL	43	6	7	3.000
T	53	4	13	4.000
T	61	4	15	4.000
T	61	5	12	4.083
T	61	6	10	4.100
T	67	6	11	5.000
T	71	5	14	4.071
T	71	7	10	5.100
T	71	10	7	4.000
T	73	4	18	4.056
T	73	6	12	5.083
T	73	8	9	5.000
T	73	9	8	4.125
T	79	6	13	5.000
T	89	4	22	4.045
T	89	8	11	5.000
T	89	11	8	4.125
T	97	4	24	4.042
T	97	6	16	5.062
T	97	8	12	6.083
T	97	12	8	4.125
T	101	4	25	4.000
T	101	5	20	4.050
T	101	10	10	5.100
T	103	6	17	6.000
T	109	4	27	4.000
T	109	6	18	5.056

Assuming Conjectures 2.2.1 and 2.2.2, we would have the following results.

- $|2A| = 3|A|$ if and only if $t = 5$ and $k > 2$, $(k,t,p) = (4,7,29)$, or $(k,t,p) = (6,7,43)$.

- $|2A| = 3|A| + 1$ if and only if $k = 3$ and $t > 4$, $t = 6$ and $k > 2$, $(k, t, p) = (4, 10, 41)$, or $(k, t, p) = (5, 8, 41)$.

The final cases we will look at in this chapter are where where $9 \leq |A| \leq \frac{p-1}{5}$. Below is a slightly longer sample of the data than for the other cases, as the last exceptional case happens when $p = 127$.

Table 2.6: Data testing if $\sigma(A) \geq 5$ for $9 \leq t \leq \frac{p-1}{5}$

True/False	p	k	t	$\sigma(A)$
FAL	61	5	12	4.083
FAL	61	6	10	4.100
T	67	6	11	5.000
FAL	71	5	14	4.071
T	71	7	10	5.100
T	73	6	12	5.083
T	73	8	9	5.000
T	79	6	13	5.000
T	89	8	11	5.000
T	97	6	16	5.062
T	97	8	12	6.083
FAL	101	5	20	4.050
T	101	10	10	5.100
T	103	6	17	6.000
T	109	6	18	5.056
T	109	9	12	6.083
FAL	109	12	9	4.000
T	113	7	16	5.062
T	113	8	14	5.071
T	127	6	21	6.000
T	127	7	18	6.056

True/False	p	k	t	$\sigma(A)$
T	127	9	14	5.071
FAL	127	14	9	4.000
T	131	5	26	5.038
T	131	10	13	6.000
T	131	13	10	5.100
T	137	8	17	5.000
T	139	6	23	5.000
T	151	5	30	5.033
T	151	6	25	6.000
T	151	10	15	7.000
T	151	15	10	5.100
T	157	6	26	5.038
T	157	12	13	6.000
T	157	13	12	6.083
T	163	6	27	6.000
T	163	9	18	7.056
T	163	18	9	5.000
T	181	5	36	5.028
T	181	6	30	6.033
T	181	9	20	7.050
T	181	10	18	9.056
T	181	12	15	6.000
T	181	15	12	6.083
T	181	18	10	5.100
T	181	20	9	5.000
T	191	5	38	5.026
T	191	10	19	7.000
T	191	19	10	5.100

True/False	p	k	t	$\sigma(A)$
T	193	6	32	6.031
T	193	8	24	8.042
T	193	12	16	7.062
T	193	16	12	6.083
T	197	7	28	7.036
T	197	14	14	7.071
T	199	6	33	6.000
T	199	9	22	6.045
T	199	11	18	7.056
T	199	18	11	5.000
T	199	22	9	5.000

From our computational data, we believe the following conjecture, which has been confirmed for primes $127 < p < 30,000$.

Conjecture 2.2.3. *If* $9 \leq |A| \leq \frac{p-1}{5}$, *then* $|2A| \geq 5|A|$ *for* $p > 127$.

This is where we will stop examining specific cases for the size of A and consider the pattern that has emerged. Combining the earlier results, we make the following conjecture.

Conjecture 2.2.4. *Suppose* $A = \langle \omega \rangle$ *is a multiplicative subgroup of* k^{th} *powers in* $\mathbb{Z}_p^*$. *Then, for a positive integer* n, *if* $2n - 1 \leq |A| \leq \frac{p-1}{n}$, $|2A| \geq n|A|$ *for sufficiently large* p.

2.3 Relationship between Doubling and Energy

The Cauchy-Davenport theorem provides a uniform lower bound for the cardinality of $A+A$ for any subset A of $\mathbb{Z}_p$. Improvements on this can be obtained for certain sets by using the concept of additive energy.

Definition 2.3.1. *For any subset* A *of* $\mathbb{Z}_p$, *the additive energy of* A, *denoted* $E(A)$ *is defined*

by

$$E(A) := \#\{(a_1, a_2, a_3, a_4) : x_i \in A,\ 1 \leq i \leq 4,\ a_1 + a_2 = a_3 + a_4\}.$$

The additive energy of A measures the number of collisions when adding two elements of A together. Thus, if $E(A)$ is small, we expect $A + A$ to be large. This concept is quantified in the following lemma.

Lemma 2.3.1. *For any subset A of $\mathbb{Z}_p$, we have*

$$|2A| \geq \frac{|A|^4}{E(A)}. \tag{2.3.1}$$

Thus, any upper bound on $E(A)$ provides a lower bound for $|2A|$.

Proof. For any $y \in \mathbb{Z}_p$, define

$$S(y) := \{(a_1, a_2) \in A \times A : a_1 + a_2 = y\}$$

and $n(y) := |S(y)|$.

Note that $n(y) = 0$ if $y \notin 2A$. Thus

$$\sum_{y \in 2A} n(y) = |A|^2,$$

since every ordered pair $(a_1, a_2) \in A \times A$ belongs to exactly one of the sets $S(y)$ with $y \in 2A$. Also, for any $y \in \mathbb{Z}_p$,

$$n(y)^2 = \#\{(a_1, a_2, a_3, a_4) \in A^4 \ : a_1 + a_2 = y = a_3 + a_4\},$$

and so

$$\sum_{y \in 2A} n(y)^2 = \sum_{y \in \mathbb{Z}_p} n(y)^2 = \#\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\} = E(A).$$

Then, by the Cauchy-Schwarz inequality,

$$|A|^2 = \sum_{y \in 2A} n(y) \leq \left(\sum_{y \in 2A} 1 \right)^{1/2} \left(\sum_{y \in 2A} n(y)^2 \right)^{1/2} = |2A|^{1/2} E(A)^{1/2}.$$

The lemma follows upon squaring both sides and dividing by $E(A)$. □

Building from Lemma 2.3.1, we can obtain a lower bound on $|2A|$ by considering proven upper bounds on $E(A)$. From [4], we have that for $|A| < p^{2/3}$,

$$E(A) \leq \tfrac{16}{3}|A|^{5/2}. \tag{2.3.2}$$

Combining this with Lemma 2.3.1 yields

$$|2A| \geq \frac{|A|^4}{\frac{16}{3}|A|^{5/2}} = \frac{3}{16}|A|^{3/2}, \tag{2.3.3}$$

for groups of size $|A| < p^{2/3}$. Note that $\frac{3}{16}|A|^{3/2} > 2|A|$ when $|A| > 113$. Thus, in this range, (2.3.3) provides a stronger bound than the lower bound in Lemma 2.1.2, which was obtained using the Cauchy-Davenport inequality.

Chapter 3

The Waring Number

We will now examine how many times a multiplicative subgroup A of $\mathbb{Z}_p^*$ must be added to itself before the sum is either $\mathbb{Z}_p$ or $\mathbb{Z}_p^*$. Consider the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv c \pmod{p}. \tag{3.0.1}$$

We define the Waring number for A, $\Gamma(A)$, to be the smallest integer s such that this congruence is solvable with $p \nmid x_i$, $1 \leq i \leq s$, for all integers c in $\mathbb{Z}$. We will also consider $\Gamma^*(A)$, which we define as the smallest integer s such that the congruence is solvable for all integers c such that $p \nmid c$. For any positive integer n, we define

$$nA := A + A + \cdots + A = \{a_1 + \cdots + a_n : a_i \in A, 1 \leq i \leq n\}.$$

Then, our definitions of $\Gamma(A)$ and $\Gamma^*(A)$ can be restated as follows.

Definition 3.0.1. *Let A be a multiplicative subgroup of $\mathbb{Z}_p^*$. We write*

$$\Gamma(A) = \min\{n \in \mathbb{N} : nA = \mathbb{Z}_p\}, \tag{3.0.2}$$

$$\Gamma^*(A) = \min\{n \in \mathbb{N} : nA \supseteq \mathbb{Z}_p^*\}. \tag{3.0.3}$$

For $A_0 = A \cup \{0\}$, we also define $\Gamma(A_0) = \min\{n \in \mathbb{N} : nA_0 = \mathbb{Z}_p\}$. $\Gamma(A_0)$ is the smallest integer s such that (3.0.1) is solvable for all integers c in $\mathbb{Z}$. Here, we are allowing the x_i to be divisible by p.

Note that when $|A| = 1$, $\Gamma(A)$ and $\Gamma^*(A)$ are not defined since $|nA| = 1$ for any positive integer n. Thus we restrict our attention to $|A| \geq 2$, where by the Cauchy-Davenport inequality, Theorem 2.1.1, $\Gamma(A)$ and $\Gamma^*(A)$ both exist.

The primary focus in this chapter will be to examine how large $|A|$ must be to ensure that $\Gamma^*(A)= 2$.

3.1 Classical bounds on $\Gamma(A)$

Cauchy [1] established the following result.

Lemma 3.1.1. *For any subset A of $\mathbb{Z}_p^*$ and positive integer n,*

$$|nA_0| \geq \min(n|A| + 1, p).$$

Proof. We will proceed by induction on n. For $n = 1$, $|A_0| \geq |A| + 1$ is trivial. Now, suppose $|nA_0| \geq \min(n|A| + 1, p)$ is true for a given n. Then, for $n + 1$, either $(n + 1)A_0 = \mathbb{Z}_p$, or

$$|(n + 1)A_0| = |nA_0 + A_0| \geq |nA_0| + |A_0| - 1,$$

by the Cauchy-Davenport inequality, Theorem 2.1.1. Using the induction assumption,

$$|nA_0| + |A_0| - 1 \geq n|A| + 1 + |A_0| - 1 = n|A| + |A| + 1 = (n + 1)|A| + 1,$$

completing the proof. □

From this Cauchy [1] deduced the following result.

Corollary 3.1.1. *For the multiplicative subgroup A of k^{th} powers in $\mathbb{Z}_p^*$, we have $\Gamma(A_0) \leq k$.*

Proof. This follows directly from Lemma 3.1.1 by letting $n = k$. In this case we have

$$|kA_0| \geq \min\left(k\frac{p-1}{k} + 1, p\right) = p.$$

□

Analogues of these results can be used to look at the case where A is a multiplicative group of k^{th} powers and 0 is not included.

Lemma 3.1.2. *Let A be a multiplicative subgroup of $\mathbb{Z}_p^*$ with $t \geq 2$.*
i) If $t > 2$, then for any positive integer n,

$$|nA| \geq \min(n|A|, p).$$

ii) If $t = 2$, then for any positive integer n,

$$|nA| = \min(n + 1, p).$$

Proof. i) We will again proceed by induction on n. For $n = 1$, $|A| \geq |A|$ is trivial. Now assume $|nA| \geq \min(n|A|, p)$ is true for a given n. Then, for $n + 1$, either $(n + 1)A = \mathbb{Z}_p$, or by the Cauchy-Davenport inequality (Theorem 2.1.1),

$$|(n + 1)A| = |nA + A| \geq |nA| + |A| - 1.$$

By the induction assumption, $|nA| \geq n|A|$ (since we are assuming $(n + 1)A \neq \mathbb{Z}_p$), and so,

$$|(n + 1)A| \geq n|A| + |A| - 1 = (n + 1)|A| - 1.$$

We know $(n + 1)A$ is a union of cosets of A together possibly with 0 by a similar argument to the proof of Lemma 1.1.1. Thus for a positive integer λ, we have that $|(n + 1)A| = \lambda t$ or

$\lambda t + 1$, which implies $\lambda t + 1 \geq (n+1)t - 1$. Because $t \geq 3$, we conclude that $\lambda \geq n + 1$. Hence,

$$|(n+1)A| \geq \lambda t \geq (n+1)t = (n+1)|A|,$$

which completes the proof.

ii) First, we observe that the sum of any two arithmetic progressions with difference d is also an arithmetic progression with difference d. If $t = 2$, $A = \{-1, 1\}$, an arithmetic progression of length 2 and difference 2. $2A = \{-2, 0, 2\}$, an arithmetic progression of length 3 and difference 2. By Lemma 2.1.1, $|3A| = |2A| + |A| - 1 = 4$. Similarly, $|4A| = |3A| + |A| - 1 = 5$, and so on. One can see that for any $n \leq p - 1$, $|nA| = n + 1$. □

Building from these results, we have the following theorem.

Theorem 3.1.1. *Let A be a non-trivial multiplicative subgroup of k^{th} powers in $\mathbb{Z}_p^*$. Then,*

$$\Gamma^*(A) \leq k, \qquad \textit{for } |A| > 2,$$
$$\Gamma^*(A) = 2k - 1, \qquad \textit{for } |A| = 2.$$

Proof. Suppose $t > 2$. Letting $n = k$ in Lemma 3.1.2 *i*, we have

$$|kA| \geq \min(kt, p) = \min(p - 1, p) = p - 1.$$

Thus $|kA|$ is either $p - 1$ or p. Note that kA is a union of cosets of A together possibly with 0 by the same argument as Lemma 1.1.1. Thus, $\mathbb{Z}_p^* \subseteq kA$. In the case where $t = 2$, then from Lemma 3.1.2 we have that $|nA| = p - 1$ if $n = p - 2$. Again, because nA is a union of cosets of A together possibly with 0, we know 0 is the missing element. Hence $\Gamma^*(A) = p - 2 = 2k - 1$. □

Lemma 3.1.3. *For a non-trivial multiplicative subgroup A of $\mathbb{Z}_p^*$ and a positive integer m, if $\Gamma^*(A) = m$, then $\Gamma(A) \leq m + 1$.*

Proof. This follows directly from the Cauchy-Davenport inequality, Theorem 2.1.1. □

By combining Theorem 3.1.1 and Lemma 3.1.3, we get the following corollary.

Corollary 3.1.2. *Let A be a multiplicative subgroup of k^{th} powers in $\mathbb{Z}_p^*$. Then, $\Gamma(A) \leq k+1$ when $|A| > 2$, and $\Gamma(A) = 2k$ when $|A| = 2$.*

By Lemma 2.1.3, we also have that for the group of squares $\pmod p$ with $p > 5$, $\Gamma(A) = 2$ if t is even, and $\Gamma^*(A) = 2$ if t is odd. In our study of $\Gamma(A)$ and $\Gamma^*(A)$ we computationally calculated the two values for all non-trivial multiplicative subgroups A for the first 2500 primes p. Sections of the data are displayed in the following tables, and we can see that the results stated in Theorem 3.1.1 and Corollary 3.1.2 are reflected.

Table 3.1: $\Gamma(A)$ *for subgroups with* $k \geq 2$

p	k	t	$\Gamma(A)$
5	2	2	4
7	2	3	3
7	3	2	6
11	2	5	3
11	5	2	10
13	2	6	2
13	3	4	4
13	4	3	5
13	6	2	12
17	2	8	2
17	4	4	4
17	8	2	16
19	2	9	3
19	3	6	2
19	6	3	6
19	9	2	18
23	2	11	3
23	11	2	22
29	2	14	2
29	4	7	4
29	7	4	6
29	14	2	28
31	2	15	3
31	3	10	2
31	5	6	3
31	6	5	5
31	10	3	9
31	15	2	30
37	2	18	2
37	3	12	2
37	4	9	3

Table 3.2: $\Gamma^*(A)$ *for subgroups with* $k \geq 2$

p	k	t	$\Gamma^*(A)$
5	2	2	3
7	2	3	2
7	3	2	5
11	2	5	2
11	5	2	9
13	2	6	2
13	3	4	3
13	4	3	4
13	6	2	11
17	2	8	2
17	4	4	3
17	8	2	15
19	2	9	2
19	3	6	2
19	6	3	5
19	9	2	17
23	2	11	2
23	11	2	21
29	2	14	2
29	4	7	3
29	7	4	5
29	14	2	27
31	2	15	2
31	3	10	2
31	5	6	3
31	6	5	4
31	10	3	8
31	15	2	29
37	2	18	2
37	3	12	2

3.2 Existing bounds on t for $\Gamma^*(A)= 2$

We will now investigate how large $|A|$ must be relative to p to have $\Gamma^*(A)= 2$. Consider the following congruence:

$$x_1^k + x_2^k + \cdots + x_s^k \equiv c \pmod{p}.$$

By applying estimates from Hua and Vandiver [5], and Weil [6], one can obtain that $\Gamma(A_0) \leq s$ if $|A| \geq p^{\frac{1}{2}+\frac{1}{2s}}$. Then, by setting $s = 2$, we have $\Gamma(A_0) \leq 2$ if $t \geq p^{\frac{3}{4}}$. This result was explored further for the case of $\Gamma^*(A)$. By applying classical bounds on Gauss exponential sums, one can prove the following lemma; see [7].

Lemma 3.2.1. *Consider the congruence*

$$x_1^k + x_2^k + \cdots + x_s^k \equiv c \pmod{p}. \tag{3.2.1}$$

If $p \geq k^{\frac{2s}{s-1}}$, then for any nonzero c in $\mathbb{Z}_p$, there exists a solution in $\mathbb{Z}_p$ with $x_i \neq 0$ for $1 \leq i \leq s$.

Note that the minimum s for which congruence (3.2.1) holds for all nonzero c is equivalent to $\Gamma^*(A)$.

Corollary 3.2.1. *For the multiplicative subgroup A of k^{th} powers in $\mathbb{Z}_p^*$, if $t > p^{3/4}$, then $\Gamma^*(A)= 2$.*

Proof. Suppose $t > p^{3/4}$. By writing t as $\frac{p-1}{k}$, we have that $\frac{p-1}{k} > p^{3/4}$. Solving for k, we see that

$$\frac{(p-1)^4}{p^3} > k^4.$$

Thus, $p \geq k^4$, and by Lemma 3.2.1, we have that $\Gamma^*(A)= 2$. □

3.3 Improving the bound on t for $\Gamma^*(A)= 2$

It would be interesting to improve on the established $p^{3/4}$ bound in Corollary 3.2.1. From the data generated, it seems likely that there exists an $\alpha < 3/4$ where $\Gamma^*(A) = 2$ if $t > p^\alpha$ and p is sufficiently large. Two natural possibilities to consider here are $\frac{2}{3}$ and $\frac{1}{2}$, leading to the following conjectures.

Conjecture 3.3.1. *Let A be a multiplicative subgroup of k^{th} powers in $\mathbb{Z}_p^*$. If $|A| > p^{2/3}$, then $\Gamma^*(A)= 2$ for p sufficiently large.*

Conjecture 3.3.2. *Let A be a multiplicative subgroup of k^{th} powers in $\mathbb{Z}_p^*$. There exists some positive constant c such that if $|A| > cp^{1/2}$, then $\Gamma^*(A)= 2$.*

Suppose $|A| \leq \sqrt{p}$. For $p > 3$, by (2.1.1), we have

$$|2A| \leq \begin{cases} \min\left(\dfrac{p+\sqrt{p}}{2},\ p-1\right) < p-1, & \text{for odd } t, \\ \min\left(\dfrac{p}{2}+1,\ p\right) < p-1, & \text{for even } t. \end{cases} \tag{3.3.1}$$

Thus, if $|A| \leq \sqrt{p}$, then $\Gamma^*(A) \geq 3$.

We began our computational analysis of an improved bound by restricting our attention to subgroups A with $\sqrt{p} < |A| < p^{3/4}$. To gain a better visual perspective of conjectural bounds on $|A|$ that imply $\Gamma^*(A) = 2$, we made the following plots. For every prime p, we plotted the size of the largest multiplicative subgroup A of $\mathbb{Z}_p^*$ such that $\Gamma^*(A) > 2$. These appear as the red points on the figures below. Our goal was then to find a curve that dominated all of the points while remaining as close as possible to them.

In the first figure below, the blue curve is $t = p^{2/3}$, and the green curve is $t = 3\sqrt{2p}$, one of the first bounds we considered. Considering the maximal doubling bound in (2.1.1), we note that $\sqrt{2p}$ is close to the minimum threshold of $|A|$ required for $|2A|$ to reach $p-1$, so we began by choosing multiples of this for our tests.

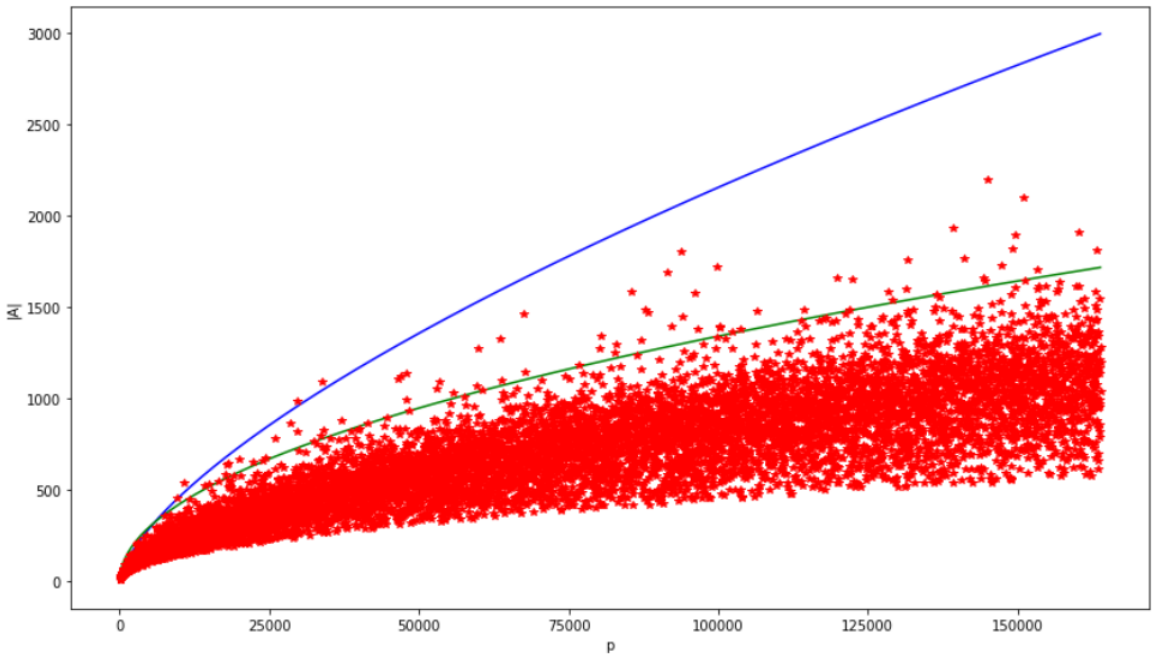


Figure 3.1: *Maximal* $|A|$ *with* $\Gamma^*(A) > 2$*, and curves* $|A| = p^{2/3}, |A| = 3\sqrt{2p}$

After running similar tests for primes up to $500,000$, we decided to move on from testing $p^{2/3}$ as a lower bound for t, as the data points progressively became further from that curve. The last case where $|A| > p^{2/3}$ and $\Gamma^*(A) > 2$ occurred when $p = 33791$, $k = 31$, and $t = 1090$, which can be seen in Figure 3.1 above. Thus, we strongly believe that for $p > 33791$ and $|A| > p^{2/3}$, we always have $\Gamma^*(A) = 2$.

As we tested for larger values of p, we observed that the most extreme cases still seemed to grow on the order of $\sqrt{p}$. When certain bounds looked promising for further testing, we would often generate a list of exceptions with their distances to the given curve. This would help make refinements to the constant in front of $\sqrt{p}$. Another practice we employed was printing a checkpoint every 1000 primes, as testing for primes up to 10^6 often involved leaving the program running for multiple days. This allowed us to begin making observations and potentially start another test while the original was still running. Here is an example of the output where we considered the bound $t > 3\sqrt{2p}$.

Exceptions Table

prime	k	|A|	bound	margin	% ratio m/b
checkpoint: 0 5 0					
checkpoint: 1000 7937 0					
9619	21	458	416.103	41.897	10.069
10781	20	539	440.520	98.480	22.355
14149	27	524	504.660	19.340	3.832
14897	28	532	517.828	14.172	2.737
16411	30	547	543.505	3.495	0.643
checkpoint: 2000 17417 0					
17581	30	586	562.546	23.454	4.169
17921	28	640	567.960	72.040	12.684
18089	28	646	570.615	75.385	13.211
20011	30	667	600.165	66.835	11.136
22271	34	655	633.149	21.851	3.451
23833	36	662	654.976	7.024	1.072
24337	36	676	661.866	14.134	2.136
25873	33	784	682.432	101.568	14.883
checkpoint: 3000 27481 0					
28579	33	866	717.232	148.768	20.742
29581	30	986	729.697	256.303	35.125
29629	36	823	730.289	92.711	12.695
32341	42	770	762.980	7.020	0.920

Here is the data plotted

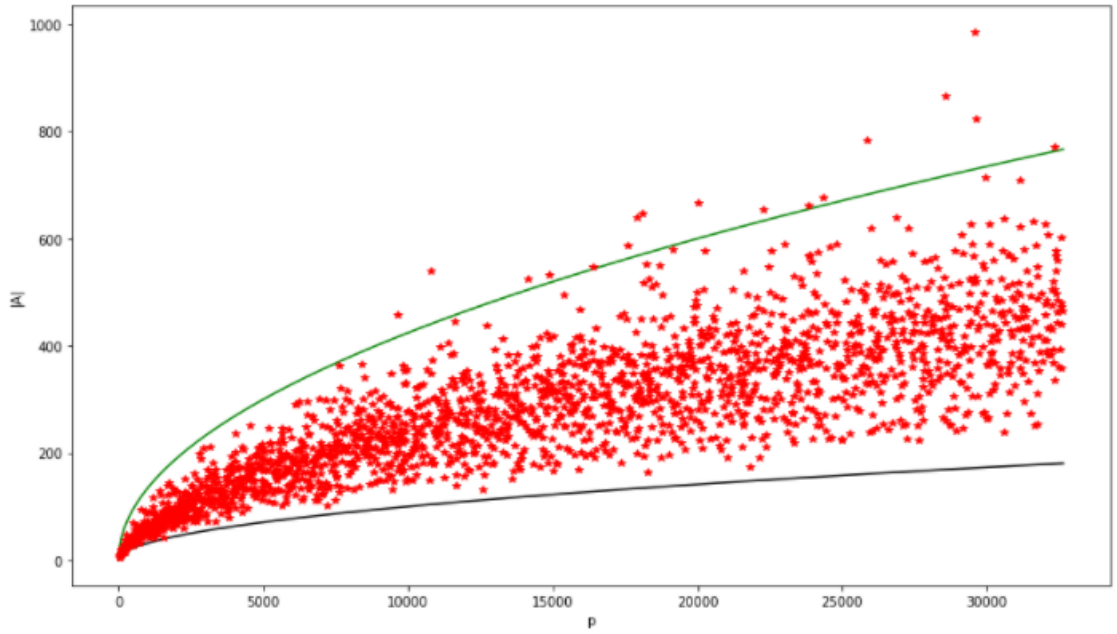


Figure 3.2: *Full output of a test for $t > 3\sqrt{2p}$ for the first 3500 primes*

By looking at the distance between an exception's size and the tested bound, we could get an idea of how to refine the constant in front of $\sqrt{p}$ for the next round of computations. Often, we would test several different estimates simultaneously, as can be seen in the following figure.

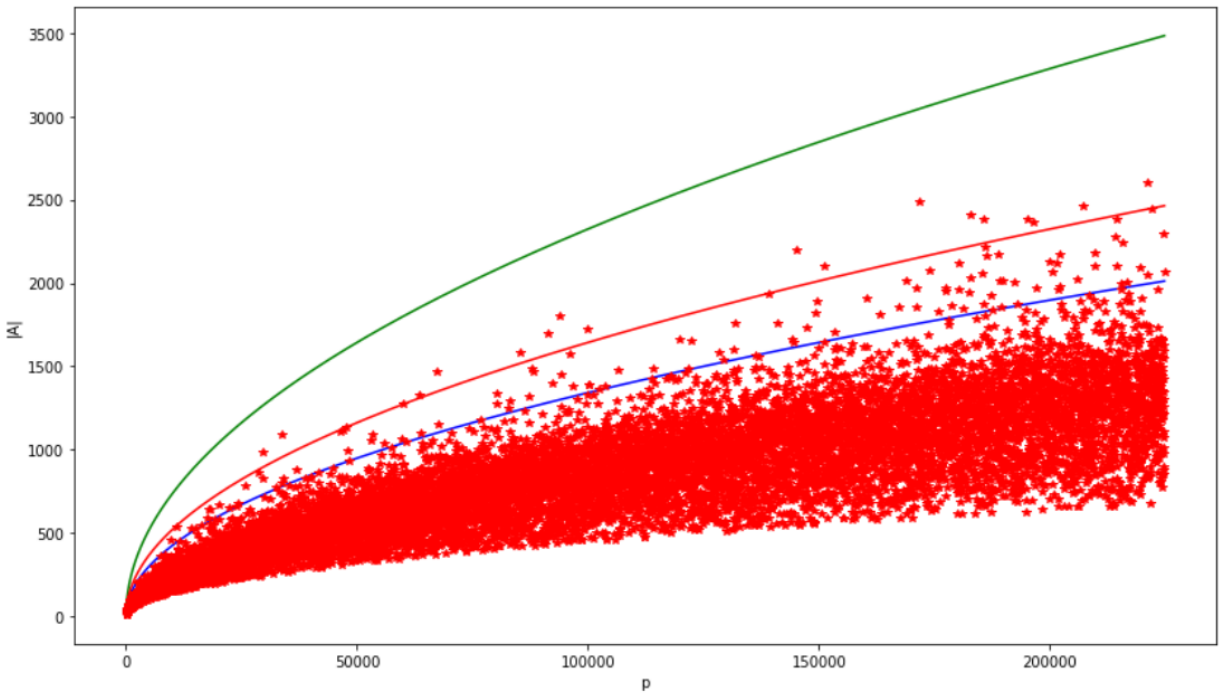


Figure 3.3: *Table generated plotting* $|A|$ *against the curves* $|A| = 3\sqrt{2p}$ *(blue),* $|A| = 3\sqrt{3p}$ *(red), and* $|A| = 3\sqrt{6p}$ *(green).*

After several rounds of testing constants and then refining them based on the most extreme exceptions, it seemed that getting an exact constant c to state in a conjecture would not be feasible through computational methods. The issue is that so far, we have been unable to determine when such exceptions will occur. For example, while testing primes $p < 500,000$, it appeared that if $|A| > 3\sqrt{6p}$, then $\Gamma^*(A) = 2$ in all cases. However, when running the program further, we found a single exception for primes $p < 10^6$, where $p = 751,181$, $k = 115$, $t = 6532$, and $\Gamma^*(A) \neq 2$. This can be seen in the final figure below, where 24 of the most extreme cases we found throughout our research are plotted along with the curves $t = 3\sqrt{3p}$, $t = 3\sqrt{6p}$, and $t = 6\sqrt{2p}$, in red, blue, and green, respectively.

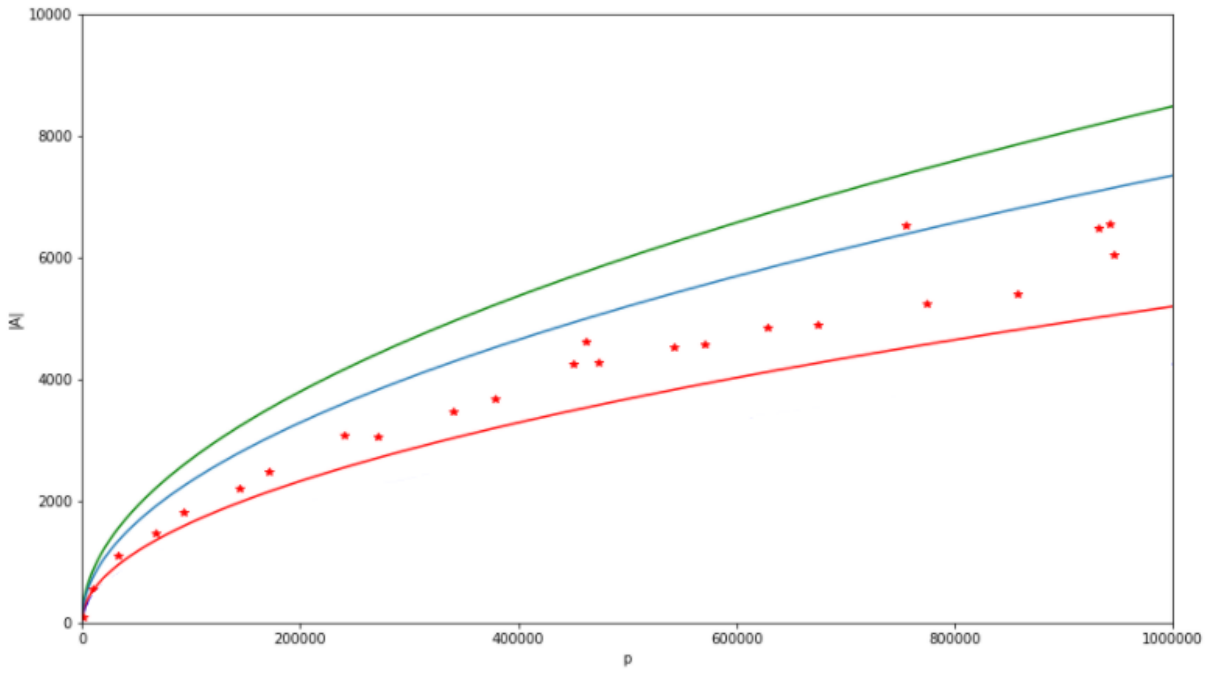


Figure 3.4: *Most extreme cases for* $p < 10^6$.

Regarding Conjecture 3.3.2, our investigation has shown that $\Gamma^*(A) = 2$ for all subgroups A with $|A| > 7.54\sqrt{p}$ and $p < 10^6$. However, we do not feel that enough data has been collected to claim that the constant 7.54 will continue to hold for larger p. Indeed, it is still too early to confidently say that any constant c exists for Conjecture 3.3.2.

Bibliography

[1] Augustin-Louis Cauchy. Recherches sur les nombres. *J. Ecole Polytechnique*, 9:99–116, 1813.

[2] Harold Davenport. On the addition of residue classes. *J. Lond. Math Soc.*, 10:30–32, 1935.

[3] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006. ISBN 978-0-521-85386-6; 0-521-85386-9. doi: 10.1017/CBO9780511755149. URL https://doi-org.er.lib.k-state.edu/10.1017/CBO9780511755149.

[4] Todd Cochrane and Chris Pinner. Explicit bounds on monomial and binomial exponential sums. *Q.J. Math.*, 62-2(4):323–349, 2011.

[5] L. K. Hua and H. S. Vandiver. On the nature of the solutions of certain equations in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, 35:481–487, 1949. ISSN 0027-8424. doi: 10.1073/pnas.35.8.481. URL https://doi-org.er.lib.k-state.edu/10.1073/pnas.35.8.481.

[6] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949. ISSN 0002-9904. doi: 10.1090/S0002-9904-1949-09219-4. URL https://doi-org.er.lib.k-state.edu/10.1090/S0002-9904-1949-09219-4.

[7] Todd Cochrane, Derrick Hart, Christopher Pinner, and Craig Spencer. Waring's number for large subgroups of $\mathbb{Z}_p^*$. *Acta Arith.*, 163(4):309–325, 2014. ISSN 0065-1036. doi: 10.4064/aa163-4-2. URL https://doi-org.er.lib.k-state.edu/10.4064/aa163-4-2.