The BS Paper

Brittany Brown, Tim Flowers, Kevin James, Amy Stout

The following paper is an investigation into the theory of binary quadratic forms and the related concept of the Hurwitz class number of a given discriminant. It also draws heavily on the theory of elliptic curves.

In our research, we looked at the splitting of the summation

$$\sum_{-D>0} H(-D) = \sum_{\substack{-D>0 \\ r\equiv 0 \bmod p}} H(-D) + \sum_{\substack{-D>0 \\ r\equiv 1 \bmod p}} H(-D) + \cdots + \sum_{\substack{-D>0 \\ r\equiv (p-1) \bmod p}} H(-D) = 2p$$

where $D = r^2 - 4p$.

We then attempted to discover what value each piece of the greater sum takes. For the cases in which the r values were split *mod* 2 and 3, we were able to find and subsequently prove all of these values, using the programs Maple and Pari, as well as the theory of quadratic residues *mod* p and elliptic curves over a finite field p.

For the case in which the r values were split *mod* 4 and *mod* 5, we were able to find all of the values, but not prove them. For the case in which the r values were split *mod* 7, we were able to find a majority of the values, but not all. We were able to find several values for *mod* 9. We did not prove these formulas.

We will present background information to help the reader understand our topic, the proofs we have, and the additional data we collected.

1 Introduction

As an introduction to our research topic, we will give a brief overview of several concepts related to binary quadratic forms. First, we will define quadratic forms.

A **binary quadratic form** f is a function

$$f(x,y) = ax^2 + bxy + cy^2$$

where $a, b, c \in \mathbb{Z}$. We say that f is **primitive** if

$$\gcd(a,b,c) = 1.$$

The **discriminant** D of f is $D = b^2 - 4ac$. [1]

1.1 Class Numbers

To enable us to define the class number of a given discriminant, we must first define several other terms.

A quadratic form is called **positive definite** if its discriminant D is less than zero and $a \geq 0$. [2]

And, we define

Definition 1.1 *A quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is **reduced** provided*

1. $|b| \leq a \leq c$
2. *If $|b| = a$ or $a = c$ then $b \geq 0$.* *[2]*

Now we are able to define the class number of a given discriminant D.

Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive, positive definite forms, the **class number**, of discriminant D is finite, and furthermore $h(D)$ is equal to the number of reduced forms of discriminant D. [2]

Here is an example of how to calculate the class number.

To calculate the class number, we must find the number of reduced forms of discriminant D. (Recall our definition of a reduced form above.)

Given a discriminant $D = -44$.

$$D = b^2 - 4ac$$

$$-D = 4ac - b^2$$

Since $a \leq c$ and $a \geq |b|$, we can say that

$$-D \geq 4a^2 - a^2 = 3a^2.$$

This implies that

$$a \leq \sqrt{\frac{-D}{3}}.$$

For our discriminant $D = -44$, this implies that $a \leq 3.83$.

Keep in mind our restriction $|b| \leq a$.

By a similar manipulation of the equation $D = b^2 - 4ac$, we can see that

$$c = \frac{b^2 - D}{4a}.$$

Now, we make a table of our a, b, c values.

a	b	c
1	0	11
1	1	$\frac{45}{4}$
2	-1	$\frac{45}{8}$
2	0	$\frac{44}{8}$
2	1	$\frac{45}{8}$
2	2	6
3	-2	4
3	-1	$\frac{45}{12}$
3	0	$\frac{44}{12}$
3	1	$\frac{45}{12}$
3	2	4
3	3	$\frac{53}{12}$

To count the reduced forms (and thus the class number of D), we are interested in those c's that are integers, those a, b, c such that $\gcd(a, b, c) = 1$ and those a, b, c which satisfy the conditions of being reduced.
By examining our table, we can see that there are three such triples, i.e. there are three reduced forms of discriminant D.

These are:

$$x^2 + 11y^2$$

$$3x^2 - 2xy + 4y^2$$

$$3x^2 + 2xy + 4y^2.$$

By our definition of class number, $h(-44) = 3$, the number of reduced forms of discriminant -44.

We are also interested in the similar concept of the Hurwitz class number of a discriminant D.

Definition 1.2 *Let N be a non-negative integer. The* ***Hurwitz class number*** $H(N)$ *is defined as follows.*

1. *If* $N \equiv 1$ *or* $2 \pmod 4$ *then* $H(N) = 0$.
2. *If* $N = 0$ *then* $H(0) = \frac{-1}{12}$.
3. *Otherwise (i.e if* $N \equiv 0$ *or* $3 \pmod 4$ *and* $N > 0$*) we define* $H(N)$ *as the class number of not necessarily primitive (positive definite) quadratic forms of discriminant* $-N$*, except that forms equivalent to* $a(x^2 + y^2)$ *should be counted with coefficient* $\frac{1}{2}$*, and those equivalent to* $a(x^2 + xy + y^2)$ *with coefficient* $\frac{1}{3}$. *[1]*

(Note that, since $H(N)$ is calculated with a positive integer, we must take our discriminant, which is always negative, and compute $H(-D)$.)

In short, when calculating the Hurwitz class number, we are interested in *any* integer triples a, b, c which give reduced forms, and not just those in which $\gcd(a, b, c) = 1$, keeping in mind the special weightings of two forms.

Going back to our previous example, $D = -44$, we can see that the Hurwitz class number $H(44) = 4$, one more than $h(-44)$ due to the case $(2, 2, 6)$.

Note that since none of our forms are of the form $a(x^2 + y^2)$ or $a(x^2 + xy + y^2)$, we do not need to worry about the weighting of our count.

1.2 Quadratic Residues and Legendre Symbols

Later on, we will use the idea of quadratic residues *mod p* to prove some of our results. Here, we will provide a basic introduction to the concept in order to make our proof easier to understand.

First, we will define a quadratic residue.

An element $a \in (\mathbb{Z}/m\mathbb{Z})$ is a **quadratic residue** *mod m* if $\gcd(a, m) = 1$ and $x^2 \equiv a \pmod m$ has a solution. If there is no solution, a is a **quadratic non-residue**. [3]

Now, we define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } \textit{mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue } \textit{mod } p \\ 0 & \text{if } p \text{ divides } a \qquad\qquad [1] \end{cases}$$

In essence, the Legendre symbol for some element $a \in (\mathbb{Z}/p\mathbb{Z})$ is 1 if a is the square of some number *mod* p and -1 if it is not.

For example, look at $\left(\frac{1}{p}\right)$. For any prime p, $1 = 1^2$. Therefore, the Legendre symbol $\left(\frac{1}{p}\right) = 1$. Now consider $\left(\frac{3}{7}\right)$. We must ask ourselves if 3 is the square of any number *mod* 7.

It is easy enough to simply calculate all the squares *mod* 7 and see.

a	a^2
1	1
2	4
3	2
4	2
5	4
6	1

Now we can note that 3 never appeared as an a^2 value, therefore it is a quadratic non-residue *mod* 7. Thus, $(\frac{3}{7}) = -1$.

There are two additional facts about Legendre symbols that we will need.

Lemma 1.1 *1.* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

2. There are $\frac{p-1}{2}$ *quadratic residues and* $\frac{p-1}{2}$ *quadratic non-residues* $\mathrm{mod}\, p$. *[3]*

2 Relevant Proofs

In our work, it was necessary to use several facts in order to come to our conclusions. We will first present an existing proof of a fact crucial to our topic, and then give proofs of several facts that we derived from our research.

2.1 Proof of the Total Sum

In order to check the accuracy of our data and prove several of our results, we needed to know the value of

$$\sum_{4p-r^2>0} H(4p - r^2).$$

The proof of this identity is combinatorial, meaning we find the value in two ways and then set the results equal to each other.

Kummer's Theorem 2.1

$$\sum_{4p-r^2>0} H(4p-r^2) = 2p.$$

To find this value the first way, we used a variation of Deuring's Theorem, which states:

Deuring's Theorem 2.1 *Let $p > 3$ be prime, and let $N = p+1-r$ be an integer, where $-2\sqrt{p} \leq r \leq 2\sqrt{p}$. Then the number of elliptic curves E over $\mathbb{F}_p$ which have $|E(\mathbb{F}_p)| = N = p+1-r$ is*

$$\frac{p-1}{2}H(4p-r^2). \qquad [2]$$

Our second method is to manually count the number of elliptic curves over $\mathbb{F}_p$.

It is a fact[4] that, as A and B vary independently from 0 to $p-1$,

$$E_{AB} : y^2 = x^3 + Ax + B$$

covers all elliptic curves mod p.

We now count all non-singluar curves (i.e. those curves with a non-zero discriminant).

To avoid curves with $\Delta = 0$, we set the discriminant Δ_E of E equal to zero and solve for B in terms of A.

$$\Delta_{E_{AB}} = 4A^3 - 27B^2$$

$$\Delta_{E_{AB}} = 0$$

$$\Rightarrow 4A^3 - 27B^2 = 0$$

$$\Rightarrow 4A^3 = 27B^2$$

$$\Rightarrow B^2 = \tfrac{4}{27}A^3 \bmod p$$

$$\Rightarrow B^2 = \left(\tfrac{2A}{3}\right)^2 \left(\tfrac{A}{3}\right) \bmod p$$

Therefore, we must avoid those curves for which

$$B^2 = \left(\frac{2A}{3}\right)^2 \left(\frac{A}{3}\right) \bmod p$$

because these values will give us a singular curve.

Now, we will count the curves. The number of elliptic curves is

$$\sum_{A=0}^{p-1} \sum_{\substack{B=0 \\ B^2 \neq (\frac{2A}{3})^2(\frac{A}{3})}}^{p-1} 1.$$

To evaluate this sum, we will split it into three parts.

First, we will consider the contribution when $A = 0$. Then

$$\sum_{B=1}^{p-1} 1 = p - 1.$$

Second, we will consider the contribution from those A for which $(\frac{A}{p}) = 1$. We have

$$\sum_{\substack{A=1 \\ (\frac{A}{p})=1}}^{p-1} \sum_{\substack{B=0 \\ B^2 \neq (\frac{2A}{3})^2(\frac{A}{3}) \bmod p}}^{p-1} 1.$$

$$= \sum_{\substack{A=1 \\ (\frac{A}{p})=1}}^{p-1} (p-2) = \left(\frac{p-1}{2}\right)(p-2).$$

Finally, we consider the contribution from A's with $(\frac{A}{p}) = -1$. We have,

$$\sum_{\substack{A=1 \\ (\frac{A}{p})=-1}}^{p-1} \sum_{\substack{B=0 \\ B^2 \neq (\frac{2A}{3})^2(\frac{A}{3}) \bmod p}}^{p-1} 1 = \sum_{\substack{A=1 \\ (\frac{A}{p})=-1}}^{p-1} \sum_{B=0}^{p-1} 1$$

$$= \sum_{\substack{A=1 \\ (\frac{A}{p})=-1}}^{p-1} p = \left(\frac{p-1}{2}\right)p.$$

Now we can put the three pieces of the sum back together.

$$\begin{aligned}\sum_{A=0}^{p-1}\sum_{\substack{B=0\\ \Delta(E_{AB})\neq 0}}^{p-1} 1 &= \sum_{\substack{B=1\\ (A=0)}}^{p-1} 1 + \sum_{\substack{A=1\\ (\frac{A}{p})=1}}^{p-1}\sum_{\substack{B=0\\ B^2\neq(\frac{2A}{3})^2(\frac{A}{3})}}^{p-1} 1 + \sum_{\substack{A=1\\ (\frac{A}{p})=-1}}^{p-1}\sum_{B=0}^{p-1} 1\\ &= (p-1) + \Big(\frac{p-1}{2}\Big)(p-2) + \Big(\frac{p-1}{2}\Big)(p)\\ &= (p-1)\Big[1+\frac{p-2}{2}+\frac{p}{2}\Big]\\ &= (p-1)p\end{aligned}$$

Thus, we have found that the number of elliptic curves over $\mathbb{F}_p$ is $(p-1)p$.

Now we set our two results equal to each other.

$$\Big(\frac{p-1}{2}\Big)\sum_{4p-r^2>0} H(4p-r^2) = (p-1)p$$

$$\implies \sum_{4p-r^2>0} H(4p-r^2) = \Big(\frac{2}{p-1}\Big)(p-1)p = 2p$$

2.2 Proof of Congruence

Flowers' Proposition 2.1 *For any $c\in\mathbb{Z}$ and for all primes p and q,*

$$\sum_{\substack{4p-r^2>0\\ r\equiv c \bmod q}} H(4p-r^2) = \sum_{\substack{4p-r^2>0\\ r\equiv -c \bmod q}} H(4p-r^2)$$

Proof:

Let $a_1, a_2, ..., a_n$ be all the $r \equiv c \pmod q$ such that

$$-2\sqrt{p} \leq r \leq 2\sqrt{p}.$$

Notice that for all i from 1 to n,

1. $-a_i \equiv -c \pmod q$ if and only if $a_i \equiv c \pmod q$
2. $-2\sqrt{p} \leq a_i \leq 2\sqrt{p} \;\;\Rightarrow (-a_i)^2 - 4p \leq 0.$

Because $(a_i)^2 = (-a_i)^2$, it follows that

$$\sum_{\substack{4p-r^2>0\\ r\equiv c \bmod q}} H(4p-r^2) = \sum_{\substack{4p-r^2>0\\ r\equiv -c \bmod q}} H(4p-r^2).$$

This shows that the sum of the Hurwitz class numbers of discriminant $(4p-r^2)$ where $-2\sqrt{p} \leq r \leq 2\sqrt{p}$ and $r \equiv c \pmod q$ will be equal to the sum of the Hurwitz class numbers of $(4p-r^2)$ where $-2\sqrt{p} \leq r \leq 2\sqrt{p}$ and r is congruent to $-c$ *mod* q.

2.3 Proof of Formulas for r values split *mod* 2

Here we wish to prove two of the formulas we derived from our computations. In this case, we split the r values *mod* 2 in order to see how the values were distributed where $r \equiv 0 \pmod 2$ and $r \equiv 1 \pmod 2$.

To begin, we returned to our previous statement of Deuring's Theorem: Let $p > 3$ be prime, and let $N = p + 1 - r$ be an integer, where $-2\sqrt{p} \leq r \leq 2\sqrt{p}$. Then the number of elliptic curves E over $\mathbb{F}_p$ which have $|E(\mathbb{F}_p)| = N = p + 1 - r$ is

$$\frac{p-1}{2} H(4p - r^2). \qquad [2]$$

In this specific case, we want to evaluate the expression

$$\sum_{\substack{-2\sqrt{p} \leq r \leq 2\sqrt{p} \\ 2|(p+1-r)}} H(4p - r^2).$$

Note that, in stating that $2|(p + 1 - r)$, we allow the sum to split the values *mod* 2. It also forces the order of the elliptic curves to be divisible by 2, thus forcing two-torsion.

Rearranging the restriction $2|p + 1 - r$ we can see that $p + 1 - r \equiv 0 \pmod 2$, or $r \equiv p + 1 \pmod 2$. We exclude the case $p = 2$ so that we can say all primes are 1 (mod 2). Thus, we are finding the formula for $r \equiv 0 \pmod 2$.

In order to evaluate this expression, we must simply count the number of elliptic curves with a point of order 2.

It is a fact that any curve with two-torsion can be written in the form

$$E_{bc} : y^2 = x^3 + bx^2 + cx. \qquad [4]$$

We want to count all of the non-singluar curves, so we must avoid those curves which have a discriminant of 0. Therefore, we must solve for the discriminant of E. Using the program Maple, we find that

$$\Delta_{E_{bc}} = 16c^2(b^2 - 4c).$$

Thus, we know that the values we need to avoid in order to prevent singular curves are $c = 0$ and $b^2 - 4c = 0$.

Now we can count our elliptic curves. We let b and c vary over all values from 0 to $p - 1$ and count 1 for each curve, keeping in mind our restriction that $\Delta_{E_{bc}} \neq 0$.

$$\sum_{b=0}^{p-1} \sum_{\substack{c=0 \\ \Delta_{E_{bc}} \neq 0}}^{p-1} 1 = \sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ b^2-4c \neq 0}}^{p-1} 1$$

We note that $y^2 = x^3 + bx^2 + cx = x(x^2 + bx + c)$ factors when the discriminant of $x^2 + bx + c$ factors (i.e. when $b^2 - 4c$ is a square). When this happens we get three solutions instead of one; thus, we see that when $b^2 - 4c$ is a square we get three isomorphic curves so we introduce a $\frac{1}{3}$ here to count these curves only once. We also note that in the case where $(\frac{b^2-4c}{p}) = -1$, this polynomial does not factor so we do not have isomorphic curves.

$$\sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ b^2-4c \neq 0}}^{p-1} 1 = \frac{1}{3} \sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1 + \sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=-1}}^{p-1} 1.$$

To evaluate this sum, we will work through each part individually. We will start with

$$\sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1.$$

First, by splitting off the case in which $b = 0$, we can say that

$$\sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1 = \sum_{\substack{c=1 \\ (\frac{-4c}{p})=1}}^{p-1} 1 + \sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1$$

$$= \sum_{\substack{c=1 \\ (\frac{-c}{p})=1}}^{p-1} 1 + \sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1$$

since we can split $(\frac{-4c}{p})$ into $(\frac{-c}{p})(\frac{4}{p})$ and we know that 4 is always a square mod p.

Looking at this part of our sum,

$$\sum_{\substack{c=1 \\ (\frac{-c}{p})=1}}^{p-1} 1,$$

we can see that this is equal to $\frac{p-1}{2}$ since half of the integers from 1 to $p - 1$ for any p will be quadratic residues *mod p*.

Therefore, the expression we wish to evaluate becomes

$$\frac{p-1}{2} + \sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1$$

Now, let $b^2 - 4c = bd$. This implies that $d = b - 4cb^{-1}$. Therefore,

$$c = \frac{b^2 - bd}{4}.$$

Here, we will make a variable change in our sum.

$$\sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1 = \sum_{b=1}^{p-1} \sum_{\substack{d=1 \\ d\neq b \\ (\frac{b}{d})=(\frac{d}{p})}}^{p-1} 1$$

Note that $d \neq 0$ because, since we defined $b^2 - 4c = bd$, that would make the discriminant equal to 0, which we excluded.

Also, $d \neq b$ since $c \neq 0$ (i.e. $d = b \Rightarrow c = \frac{b^2-b^2}{4}$, thus making $c = 0$).

Note also that we are able to say that $(\frac{b}{d}) = (\frac{d}{p})$ due to our definition of $b^2 - 4c$ as bd. We can then change $(\frac{b^2-4c}{p})$ to $(\frac{bd}{p})$. Splitting the Legendre symbol, we can thus say that $(\frac{b}{d})(\frac{d}{p}) = 1$. We know that, for this to be true, the Legendre symbols must either both be equal to 1 or both equal to -1, so they must be equal to each other.

We can now say that

$$\frac{p-1}{2} + \sum_{b=1}^{p-1} \sum_{\substack{d=1 \\ d\neq b \\ (\frac{b}{d})=(\frac{d}{p})}}^{p-1} 1 = \frac{p-1}{2} + \sum_{b=1}^{p-1} \Big(\frac{p-1}{2} - 1\Big)$$

since, from 1 to $p-1$, for every d in $\mathbb{F}_p$ there are $\frac{p-1}{2}$ different b values for which $(\frac{b}{p}) = (\frac{d}{p})$. We subtract 1 from this because we have stated that $d \neq b$, which eliminates one such case.

Now, we can reduce the last sum to

$$(p-1)\Big(\frac{p-3}{2}\Big)$$

since there are $p - 1$ possible b values.

Thus,

$$\sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=1}}^{p-1} 1\Big(\frac{p-1}{2}\Big) + (p-1)\Big(\frac{p-3}{2}\Big) = \frac{(p-1)(p-2)}{2}.$$

Now, we will reduce the second expression,

$$\sum_{b=0}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=-1}}^{p-1} 1.$$

Again, splitting off the case $b = 0$, we have

$$\sum_{\substack{c=1 \\ (\frac{-4c}{p})=-1}}^{p-1} 1 + \sum_{b=1}^{p-1} \sum_{\substack{c=1 \\ (\frac{b^2-4c}{p})=-1}}^{p-1} 1.$$

Using our previous arguements and again letting $d = b - 4cb^{-1}$, the last sum becomes

$$\Big(\frac{p-1}{2}\Big) + \sum_{b=1}^{p-1} \sum_{\substack{d=1 \\ d\neq b \\ (\frac{b}{p})=-(\frac{d}{p})}}^{p-1} 1$$

This can be reduced to

$$\Big(\frac{p-1}{2}\Big) + \sum_{b=1}^{p-1} \Big(\frac{p-1}{2}\Big)$$

since there are $(\frac{p-1}{2})$ values from 1 to $p-1$ that d can take.

(Notice that this time we do not need to remove a case since the restriction $(\frac{b}{p}) = -(\frac{d}{p})$ automatically excludes the case $d = b$.)

It is easy to see now that this expression equals

$$\Big(\frac{p-1}{2}\Big) + (p-1)\Big(\frac{p-1}{2}\Big) = \frac{p(p-1)}{2}.$$

We can now say that our original sum,

$$\sum_{b=0}^{p-1} \sum_{\substack{c=0 \\ \Delta_{E_{bc}}\neq 0}}^{p-1} 1 = \frac{1}{3}\Big[\frac{(p-1)(p-2)}{2}\Big] + \Big(\frac{p(p-1)}{2}\Big).$$

Since we know that the number of elliptic curves with two-torsion is equal to

$$\frac{p-1}{2} H(4p - r^2)$$

we can set the results equal to each other.

Therefore,

$$\frac{p-1}{2}\sum_{\substack{4p-r^2>0\\ r\equiv 0 \bmod 2}} H(4p-r^2) = \frac{1}{3}\Big(\frac{p-1}{2}\Big)(p-2)+\Big(\frac{p-1}{2}\Big)(p)$$

Multiplying through by $\frac{2}{p-1}$ we have

$$\sum_{\substack{4p-r^2>0\\ r\equiv 0 \bmod 2}} H(4p-r^2) = \frac{1}{3}(p-2)+p$$

$$= \frac{4p-2}{3}$$

when $r \equiv 0 \pmod 2$.

Corollary 2.1 *Now, since we know that the total sum is equal to* $2p$*, we have*

$$\sum_{r\equiv 1 \bmod 2} H(4p-r^2) = 2p - \Big(\frac{4p-2}{3}\Big) = \frac{(2p+2)}{3}.$$

We can display these results in a table, where $p \equiv i \pmod 2$.

MOD 2	$r = 0$	$r = 1$
$i = 1$	$\frac{\mathbf{(4p-2)}}{\mathbf{3}}$	$\frac{(2p+2)}{3}$

2.4 Proof of Case in Which r Values Are Split *mod* 3 and Primes Are Equal to $1 \pmod 3$

Theorem 2.1

$$\sum_{\substack{4p-r^2>0\\ p\equiv 1 \bmod 3\\ r\equiv 2 \bmod 3}} H(4p-r^2) = \frac{3p-1}{4}.$$

Proof:
It is a fact that all elliptic curves with three-torsion can be written in the form

$$E : y^2 + a_1xy + a_3y = x^3. \qquad [4]$$

Therefore, to count all such elliptic curves, we must vary a_1 and a_3 over all values from 0 to $p-1$. We must, however, avoid all singular curves, so we must ensure that our discriminant is non-zero.

Using Maple, we find that our discriminant is

$$\Delta_{E_{a_1a_3}} = a_3^3(a_1^3 - 27a_3).$$

Therefore, $\Delta_{E_{a_1a_3}} = 0$ when $a_3 = 0$ or $a_3 = (\frac{a_1}{3})^3$. Thus,

$$\sum_{a_1=0}^{p-1} \sum_{\substack{a_3=0 \\ \Delta_{E_{a_1a_3}} \neq 0}}^{p-1} 1 = \sum_{a_1=0}^{p-1} \sum_{\substack{a_3=1 \\ a_3 \neq (\frac{a_1}{3})^3}}^{p-1} 1.$$

Here, we must begin to think of the problem in terms of the elliptic curves it involves. We will denote our curves of the form $E : y^2 + a_1xy + a_3y = x^3$ as (a_1, a_3).

By specializing the general formula given by Silverman [5] to suit our specific set of curves, we can see that any curve of the form (a_1, a_3) is isomorphic to a curve of the form (ua_1, u^3a_3).

It is easy to see that we can choose our u value to be $u = a_1^{-1}$. Note that we must be careful here because 0 has no multiplicative inverse. Thus, we must separate the case in which $a_1 = 0$. The rest of our curves become $(1, u^3A_3)$. Now, we have

$$\sum_{a_3=1}^{p-1} 1 + \sum_{a_1=1}^{p-1} \sum_{\substack{a_3=1 \\ a_3 \neq (\frac{a_1}{3})^3}}^{p-1} 1.$$

At this point, we must consider which values of a_3 will result in a unique case. The two cases we must watch out for are those in which the A and B values of the general elliptic curve formula

$$E : y^2 = x^3 + Ax + B$$

are zero. Using Maple computations, we can see that the coefficient A is zero when $a_3 = \frac{1}{24}$ and B is zero when $a_3 = \frac{1}{12} \pm \frac{\sqrt{3}}{36}$. So, we must treat these cases separately.

Therefore, we have

$$(p-1) + \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36}}}^{p-1} (p-1) + (p-1) + 2(p-1).$$

The first $(p-1)$ comes from the fact that

$$\sum_{a_3=1}^{p-1} 1 = p-1.$$

We changed

$$\sum_{a_1=1}^{p-1} \sum_{\substack{a_3=1 \\ a_3 \neq (\frac{a_1}{3})^3}}^{p-1} 1$$

to

$$\sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36}}}^{p-1} (p-1) + (p-1) + 2(p-1)$$

since

$$\sum_{u=1}^{p-1} 1 = p-1.$$

Note that here we have changed our a_1 value to a u value, recognizing that as we vary u from 1 to $p-1$, we see the inverse of each of our a_1 values and thus fix $ua_1 = 1$ in our curve $(ua_1, u^3 a_3)$.

The second $p-1$ comes from the fact that we are evaluating the case $(1, \frac{1}{24})$, which is isomorphic to $(u, \frac{u^3}{24})$. We simply vary u from 1 to $p-1$, which gives us $p-1$.

The $2(p-1)$ comes from the fact that we are evaluating the case $(1, \frac{1}{12} \pm \frac{\sqrt{3}}{36})$, which is isomorphic to $(u, u^3(\frac{1}{12} \pm \frac{\sqrt{3}}{36}))$. We simply vary u from 1 to $p-1$, which gives us $(p-1)$. However, we must realize that we have two distinct cases, $(u, u^3(\frac{1}{12} + \frac{\sqrt{3}}{36}))$ and $(u, u^3(\frac{1}{12} - \frac{\sqrt{3}}{36}))$, which gives us $2(p-1)$. It is also important to realize that this last case only occurs when $p \equiv 1 \pmod{12}$ because the $\sqrt{3}$ does not exist for our other cases. Further note that $(u, u^3(\frac{1}{12} + \frac{\sqrt{3}}{36})) \cong (u, u^3(\frac{1}{12} - \frac{\sqrt{3}}{36}))$.

So, now we have

$$(p-1) + (p-1) + \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36} \\ \text{special}}}^{p-1} (p-1) + \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36} \\ \text{ordinary}}}^{p-1} (p-1) + 2(p-1)$$

The first $p-1$ is simply carried down from the above equation. It is important to realize, however, that it represents the case $(0, a_3)$ which is isomorphic to $(0, u^3)$. This represents three separate isomorphism classes.

The second $p-1$ is our case $(1, \frac{1}{24})$ and is carried down from the previous expression as well.

We have split the sum into two cases, special and ordinary. In the special case, the curve $(1, a_3)$ is isomorphic to three other curves of the form $(1, A_3)$. In the ordinary case, $(1, a_3)$ is not isomorphic to any other curves of the form $(1, A_3)$.

Now we will examine this expression and reduce it to the number of isomorphism classes of elliptic curves, rather than the number of elliptic curves. This becomes

$$2 + 1 + \frac{1}{4} \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36} \\ \text{special}}}^{p-1} 1 + \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}, \frac{1}{24} \\ a_3 \neq \frac{1}{12} \pm \frac{\sqrt{3}}{36} \\ \text{ordinary}}}^{p-1} 1 + 1^*.$$

The first number is 2 because we realize that one of the three isomorphism classes $(0, a_3)$ is isomorphic to $(u, \frac{u^3}{24})$ so we split off that case and only count it once, in the following 1. We introduce a $\frac{1}{4}$ coefficient to the special sum in order to account for the fact that each of the special curves is isomorphic to three other curves. And finally, we put a star by the final 1 to indicate that it represents the isomorphism class of the curves $(1, \frac{1}{12} \pm \frac{\sqrt{3}}{36})$, which is only counted when $p \equiv 1 \pmod{12}$.

If $p \equiv 1 \pmod{12}$, this becomes

$$2 + 1 + 1 + \frac{1}{4}\Big(\frac{p-7}{3} - 2\Big) + \left(p - 5 - \Big(\frac{p-13}{3}\Big)\right)$$

$$= \frac{3p+9}{4}.$$

We have $\frac{p-7}{3} - 2$ because there are seven u values that give us either a zero discriminant or a trivial isomorphism and these $(p-7)$ u values yield only $\frac{p-7}{3}$ distinct a_3 values. We then remember to substract off the cases $a_3 = \frac{1}{12} \pm \frac{\sqrt{3}}{36}$ because they will be counted later.

We have $(p - 5 - \left(\frac{p-13}{3}\right)$ because there are 5 illegitimate a_3 values in this case and we have already counted $\frac{p-7}{3} - 2 = \frac{p-13}{3}$ of the legitimate a_3 values in the other sum.

If $p \equiv 7 \pmod{12}$, this becomes

$$2+1+\frac{1}{4}\Big(\frac{p-7}{3}\Big)+\left(p-3-\Big(\frac{p-7}{3}\Big)\right)$$

$$=\frac{3p+7}{4}.$$

Note that here we have $\frac{p-7}{3}$ because we can ignore the case $a_3 = \frac{1}{12} \pm \frac{\sqrt{3}}{36}$ as it does not exist when $p \equiv 7 \pmod{12}$. This also accounts for the $p-3$ in the second expression instead of the $p-5$ in the other case.

We will now use an alternate form of Deuring's Theorem. This version states that the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ is equal to the number of reduced but not necessarily primitive forms of discriminant (r^2-4p). This value is

$$\sum_{\substack{4p-r^2>0 \\ r\equiv p+1 \pmod 3}} H(4p-r^2)+c$$

where c is the constant value that accounts for the fact that $H(4p-r^2)$ is a weighted count.

We must find the value of c, taking into account both weighted forms.

The first weighted form is $a(x^2+y^2)$. The discriminant of this form is $-4a^2$.

So, we can say that

$$r^2-4p=-4a^2.$$

Rearranging our variables, we have

$$r^2+4a^2=4p.$$

This implies that r^2 is divisible by 4 (or r is divisible by 2), so we write $r=2r_1$.

Thus,

$$r_1^2+a^2=p.$$

If $p \equiv 1 \pmod 4$, we can factor this equation into

$$p=(r_1+ia)(r_1-ia).$$

Thus, this only occurs here for $p \equiv 1 \pmod{12}$.

We must now consider how many different times this can happen within the case $p \equiv 1 \pmod{12}$.

If $r \equiv p+1 \pmod 3 \equiv 2 \pmod 3$, then $r_1 \equiv 1 \pmod 3$. Knowing that $p \equiv 1 \pmod 3$ and $r_1^2 + a^2 = p$, we can see that $a \equiv 0 \pmod 3$. Therefore, this only occurs once.

So, we see that, if $p \equiv 7 \pmod{12}$ (i.e. $3 \pmod 4$), we cannot factor $r_1^2 + a^2 = p$ and the case $a(x^2+y^2)$ does not occur. If $p \equiv 1 \pmod{12}$ (i.e. $1 \pmod 4$), we can factor $r_1^2 + a^2 = p$, leading to the conclusion that $a(x^2+y^2)$ occurs once. Thus, when $p \equiv 1 \pmod{12}$, we must add 1/2 back into our sum, since we counted one form with a weight of one half instead of one.

Now we will consider the other weighted form, $a(x^2+xy+y^2)$. The discriminant of this form is $-3a^2$.

We say then that

$$r^2 - 4p = -3a^2.$$

Rearranging our variables, we have

$$r^2 + 3a^2 = 4p.$$

Since $p \equiv 1 \pmod 3$, we can factor this into

$$p = \Big(\frac{r + a\sqrt{-3}}{2}\Big)\Big(\frac{r - a\sqrt{-3}}{2}\Big).$$

This gives us six possible values. However, since we know $r \equiv p+1 \equiv 2 \pmod 3$, we know that there are just three possible values.

So, for $p \equiv 1, 7 \pmod{12}$, there are three $a(x^2+xy+y^2)$ forms, each counted as a 1/3 in the sum. Thus, the three forms summed to 1 in the sum and we must add back 2 to make the sum equal to the actual count.

Thus,

$$c = \begin{cases} \frac{5}{2} & \text{if } p \equiv 1 \pmod{12} \\ 2 & \text{if } p \equiv 7 \pmod{12} \end{cases}$$

Now, we can find the value of

$$\sum_{\substack{4p - r^2 > 0 \\ r \equiv (p+1) \bmod 3}} H(4p - r^2).$$

When $p \equiv 1 \pmod{12}$ we have, from the alternate form of Deuring's Theorem, that

$$\frac{3p+9}{4} = \sum_{\substack{4p-r^2>0 \\ r\equiv(p+1) \bmod 3}} H(4p-r^2) + \frac{5}{2}.$$

This implies that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv(p+1) \bmod 3}} H(4p-r^2) = \frac{3p-1}{4}.$$

When $p \equiv 7 \pmod{12}$ we have

$$\frac{3p+7}{4} = \sum_{\substack{4p-r^2>0 \\ r\equiv(p+1) \bmod 3}} H(4p-r^2) + 2.$$

This implies that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv(p+1) \bmod 3}} H(4p-r^2) = \frac{3p-1}{4}.$$

Thus we see that, for all relevant $p \equiv 1 \pmod 3$ values,

$$\sum_{\substack{4p-r^2>0 \\ r\equiv(p+1) \bmod 3}} H(4p-r^2) + c = \frac{3p-1}{4}.$$

¿From our congruence theorem, we know that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 2 \bmod q}} H(4p-r^2) = \sum_{\substack{4p-r^2>0 \\ r\equiv -2 \bmod q}} H(4p-r^2),$$

thus

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 1 \bmod q}} H(4p-r^2) = \frac{3p-1}{4}.$$

Using the fact that

$$\sum_{4p-r^2>0} H(4p-r^2) = 2p$$

we can now say that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 0 \bmod q}} H(4p-r^2) = 2p - 2\Big(\frac{3p-1}{4}\Big) = \frac{p+1}{2}.$$

2.5 Proof of Case in Which r Values Are Split *mod* 3 and Primes Are Equal to $2 \pmod 3$

This proof is directly related to the proof of the case in which r values are split *mod* 3 and $p \equiv 1 \pmod 3$. The first difference between the proofs comes at the step when we have

$$\sum_{a_3=1}^{p-1} 1 + \sum_{a_1=1}^{p-1} \sum_{\substack{a_3=1 \\ a_3 \neq (\frac{a_1}{3})^3}}^{p-1} 1.$$

When $p \equiv 2 \pmod 3$, this equals

$$(p-1) + \sum_{\substack{a_3=1 \\ a_3 \neq \frac{1}{27}}}^{p-1} (p-1).$$

Note that we have omitted the special cases $a_3 = \frac{1}{12} \pm \frac{\sqrt{3}}{36}$ because the $\sqrt{3}$ does not exist when $p \equiv 2 \pmod 3$ as well as the case $a_3 = \frac{1}{24}$ because this is only relevant when $p \equiv 1 \pmod 3$.

The $p-1$ value comes again from the case in which we set $a_1 = 0$. We let a_3 vary from 1 to $p-1$, thus getting $p-1$ values.

The main difference in this case is that, when we use this to count isomorphism classes of elliptic curves, there are fewer oddities occuring.

The first thing we notice is that in the case that $p \equiv 2 \pmod 3$, every element from 1 to $p-1$ is a cube. Thus, when we count how many curves $(0, a_3)$ are isomorphic to $(0, u^3 A_3)$, we see that every curve is isomorphic to all the other curves (i.e. if we let u vary, we see $p-1$ distinct values, but only one isomorphism class.

It is also crucial to see that, when $p \equiv 2 \pmod 3$, the curve $(1, a_3)$ is not isomorphic to any other curve of the form $(1, u^3 A_3)$ because we would need the $\sqrt{3}$ to exist. Since it does not when $p \equiv 2 \pmod 3$, we know this does not happen. Therefore, we can let u vary from 1 to $p-1$, excluding our case in which the discriminant is zero, and we get $p-2$ distinct isomorphism classes of size $p-1$.

Thus, our count of isomorphism classes becomes

$$1 + (p-2).$$

Clearly, this means that the number of isomorphism classes we have when $p \equiv 2 \pmod 3$ is $(p-1)$.

We will now use the alternate form of Deuring's Theorem again. This version states that the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ is equal to the number of reduced but not necessarily primitive forms of discriminant $(r^2 - 4p)$. This value is

$$\sum_{\substack{4p-r^2>0 \\ r\equiv p+1 \pmod 3}} H(4p - r^2) + c$$

where c is the constant value that accounts for the fact that $H(4p - r^2)$ is a weighted count.

We must find the value of c, taking into account both weighted forms.

The first weighted form is $a(x^2 + y^2)$. The discriminant of this form is $-4a^2$.

So, we can say that

$$r^2 - 4p = -4a^2.$$

Rearranging our variables, we have

$$r^2 + 4a^2 = 4p.$$

This implies that r^2 is divisible by 4 (or r is divisible by 2), so we write $r = 2r_1$.

Thus,

$$r_1^2 + a^2 = p.$$

If $p \equiv 1 \pmod 4$, we can factor this equation into

$$p = (r_1 + ia)(r_1 - ia).$$

Thus, this only occurs here for $p \equiv 5 \pmod{12}$.

We must now consider how many different times this can happen within the case $p \equiv 5 \pmod{12}$.

If $r \equiv p + 1 \pmod 3 \equiv 0 \pmod 3$, then $r_1 \equiv 0 \pmod 3$. Knowing that $p \equiv 2 \pmod 3$ and $r_1^2 + a^2 = p$, we can see that $a^2 \equiv 2 \pmod 3$. But 2 is not a square *mod* 3, so this can never happen. Thus, we do not need to add any value back into our class number in order to account for the weighted form $a(x^2 + y^2)$.

Now we will consider the other weighted form, $a(x^2 + xy + y^2)$. The discriminant of this form is $-3a^2$.

We say then that

$$r^2 - 4p = -3a^2.$$

Rearranging our variables, we have

$$r^2 + 3a^2 = 4p.$$

Since $p \equiv 2 \pmod 3$, we can no longer factor it any further. Thus, this does not occur when $p \equiv 2 \pmod 3$ and we do not need to add back value to our class number to account for the weighted forms $a(x^2 + xy + y^2)$.

Thus, we can see in this instance that our c value is simply 0.

So, we conclude that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 0 \bmod 3}} H(4p - r^2) = p - 1,$$

the number of isomorphism classes.

Using our proof that

$$\sum_{4p-r^2>0} H(4p - r^2) = 2p$$

we can now say that

$$2p = (p-1) + \sum_{\substack{4p-r^2>0 \\ r\equiv 1 \bmod 3}} H(4p - r^2) + \sum_{\substack{4p-r^2>0 \\ r\equiv 2 \bmod 3}} H(4p - r^2).$$

Now, we note that 1 and 2 are inverses *mod* 3, so we can apply our congruence theorem. Thus

$$2p = (p-1) + 2 \sum_{\substack{4p-r^2>0 \\ r\equiv 1 \bmod 3}} H(4p - r^2).$$

Now we can conclude that

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 1 \bmod 3}} H(4p - r^2) = \frac{p+1}{2}$$

and

$$\sum_{\substack{4p-r^2>0 \\ r\equiv 2 \bmod 3}} H(4p - r^2) = \frac{p+1}{2}.$$

So, we make a table of our proven values, where $p \equiv i \pmod 3$.

MOD 3	$r = 0$	$r = 1$	$r = 2$
$i = 1$	$\frac{(p+1)}{2}$	$\frac{\mathbf{(3p-1)}}{\mathbf{4}}$	$\frac{\mathbf{(3p-1)}}{\mathbf{4}}$
$i = 2$	$\mathbf{p-1}$	$\frac{(p+1)}{2}$	$\frac{(p+1)}{2}$

3 Conjectures

In order to produce computations to study in our research, we used a Pari program to compute

$$\sum_{\substack{4p-r^2>0 \\ r\equiv i \bmod q}} H(r^2-4p)$$

where $q = 4, 5, 7, 9$ and i varied from 0 to $q-1$.

Using a similar Pari program, we were able to check our patterns for both *mod* 5 and *mod* 7 out to one million. While we have no proof for these patterns, we feel confident that the patterns will hold.

In this table, our primes are congruent to $i \pmod 4$.

MOD 4	$R = 0$	$R = 1$	$R = 2$	$R = 3$
i = 1	$\frac{(p+1)}{2}$	$\frac{(p+1)}{3}$	$\frac{(5p-7)}{6}$	$\frac{(p+1)}{3}$
i = 3	$\frac{(5p-7)}{6}$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{2}$	$\frac{(p+1}{3}$

In this table, our primes are congruent to $i \pmod 5$.

MOD 5	$R = 0$	$R = 1$	$R = 2$	$R = 3$	$R = 4$
$i = 1$	$\frac{\mathbf{(p+1)}}{\mathbf{2}}$	$\frac{(p+1)}{3}$	$\frac{(5p-7)}{12}$	$\frac{(5p-7)}{12}$	$\frac{(p+1)}{3}$
$i = 2$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{3}$	$\frac{\mathbf{(p-1)}}{\mathbf{2}}$	$\frac{\mathbf{(p-1)}}{\mathbf{2}}$	$\frac{(p+1)}{3}$
$i = 3$	$\frac{(p+1)}{3}$	$\frac{\mathbf{(p-1)}}{\mathbf{2}}$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{3}$	$\frac{\mathbf{(p-1)}}{\mathbf{2}}$
$i = 4$	$\frac{\mathbf{(p-3)}}{\mathbf{2}}$	$\frac{(5p+5)}{12}$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{3}$	$\frac{(5p+5)}{12}$

In this table, our primes are congruent to $i \pmod 7$.

MOD 7	$R=0$	$R=1$	$R=2$	$R=3$	$R=4$	$R=5$	$R=6$
$i=1$		$\frac{\mathbf{(p+1)}}{\mathbf{3}}$					$\frac{\mathbf{(p+1)}}{\mathbf{3}}$
$i=2$				$\frac{\mathbf{(p-2)}}{\mathbf{3}}$	$\frac{\mathbf{(p-2)}}{\mathbf{3}}$		
$i=3$	$\frac{\mathbf{(p+1)}}{\mathbf{3}}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$\frac{(p-2)}{3}$	$\frac{(p-2)}{3}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$
$i=4$			$\frac{\mathbf{(p-2)}}{\mathbf{3}}$			$\frac{\mathbf{(p-2)}}{\mathbf{3}}$	
$i=5$	$\frac{\mathbf{(p+1)}}{\mathbf{2}}$	$\frac{(p-2)}{3}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$\frac{(p-2)}{3}$
$i=6$	$\frac{(p-5)}{3}$	$\frac{(p+1)}{4}$	$\frac{\mathbf{(p+1)}}{\mathbf{3}}$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$\frac{\mathbf{(p+1)}}{\mathbf{3}}$	$\frac{(p+1)}{4}$

Conjecture 3.1 *The (i, j)th entry in the table MOD q is the conjectured value of* $\sum$

In this table, our primes are congruent to $i \pmod 9$.

MOD 9	$r=0$	$r=1$	$r=2$	$r=3$	$r=4$	$r=5$	$r=6$	$r=7$	$r=8$
i = 1									
i = 2	$\frac{\mathbf{(p+1)}}{\mathbf{3}}$								
i = 4									
i = 5									
i = 7									
i = 8	$\frac{(p-5)}{3}$			$\frac{\mathbf{(p+1)}}{\mathbf{3}}$	$\frac{(p+1)}{6}$	$\frac{(p+1)}{6}$	$\frac{\mathbf{(p+1)}}{\mathbf{3}}$		

During our research, we computed the Hurwitz class numbers $H(-D)$ for primes split *mod* 11 and *mod* 13. We were able to find a general rule for the largest column *mod* 11, but we were unable to find any patterns for *mod* 13; we could not even find a method to identify which column would be the largest number. We were also unsuccessful in finding proofs for any of the columns for *mod* 4, *mod* 5, *mod* 7, *mod* 9 or *mod* 11; however, we are confident that proofs exist. We feel that the pattern chart for *mod* 9 could be fully completed with additional computations. It would also be relevant to find a method of predicting which h and k case we have in the special *mod* 7 cases.

4 *mod* 7

Our table for *mod* 7 is not complete. In an effort to find the remaining patterns, we split up our primes *mod* 168, hoping we would see more clearly what was happening. What we noticed is the following pattern.

Banana Split Conjecture 4.1 *For primes that are 1,2, or 4* mod *7, we can identify the largest column. If* $p \equiv 1 \pmod 7$*, then*

$$max\{\sum_{\substack{4p-r^2>0\\ r\equiv j \bmod q\\ 0\leq j\leq q-1}} H(4p-r^2)\}$$

has the formula $\frac{p+1}{3}$*. If* $p \equiv 2, 4 \pmod 7$*, then*

$$max\{\sum_{\substack{4p-r^2>0\\ r\equiv j \bmod q\\ 0\leq j\leq q-1}} H(4p-r^2)\}$$

has the formula $\frac{p-2}{3}$*.*

For these values of p, we can construct a table as follows.

MOD 7	$r=0$	$r=1$	$r=2$	$r=3$	$r=4$	$r=5$	$r=6$
$p \equiv 1 \bmod 7$	$\frac{p+h+1}{4}$	$\frac{p+1}{3}$	$\frac{7p+k}{24}$	$\frac{p-h+1}{4}$	$\frac{p-h+1}{4}$	$\frac{7p+k}{24}$	$\frac{p+1}{3}$
$p \equiv 2 \bmod 7$	$\frac{p+h+1}{4}$	$\frac{7p+k}{24}$	$\frac{p-h+1}{4}$	$\frac{p-2}{3}$	$\frac{p-2}{3}$	$\frac{p-h+1}{4}$	$\frac{7p+k}{24}$
$p \equiv 4 \bmod 7$	$\frac{p+h+1}{4}$	$\frac{p-h+1}{4}$	$\frac{p-2}{3}$	$\frac{7p+k}{24}$	$\frac{7p+k}{24}$	$\frac{p-2}{3}$	$\frac{p-h+1}{4}$

There are two different cases for h and k. If $h = (8)(7)(x) + m$ *then* $k = (24)(7)(x) + n$*, where* m, n *are some integers. If* $h = (4)(7)(x) + m$ *then* $k = (12)(7)(x) + n$*, where* m, n *are some integers. We have no way, at this point, of describing which case of h and k happens for which primes.*

5 *mod* 11

Although we were not successful in finding specific patterns for the *mod* 11 case, we did notice a general pattern that we will present here. Note that we believe that, in the following conjecture, $b + s \equiv 0 \bmod 10$ because 10=11-1 (i.e. the number by which we are splitting our r values less one).

Brown-Stout Conjecture 5.1 *Define*

$$M(p) \ = max\{ \sum_{\substack{4p-r^2>0 \\ r\equiv j \bmod 11 \\ 0\leq j\leq 10}} H(4p - r^2)\}$$

for some prime p.

Let b and s be two primes and let $i \in \mathbb{Z}$*. If* $M(b) = \frac{b-i}{(\frac{10}{2})}$ *and* $M(l) = \frac{s+i}{(\frac{10}{2})}$*, then* $b + s \equiv 0 \bmod 10$*.*

References

[1] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 1993.

[2] David A. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989.

[3] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1990.

[4] Anthony Knapp, *Elliptic Curves*, Princeton University Press, New Jersey, 1992.

[5] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.