SUMS AND DIFFERENCES OF THE COORDINATES OF POINTS ON MODULAR HYPERBOLAS

Dennis Eichhorn  
Department of Mathematics, University of California, Irvine, CA 92697  
deichert@math.uci.edu

Mizan R. Khan  
Department of Math and Computer Science, Eastern Connecticut State  
University, Willimantic, CT 06226  
khanm@easternct.edu

Alan H. Stein  
Department of Mathematics, University of Connecticut, Waterbury, CT 06702  
stein@math.uconn.edu

Christian L. Yankov  
Department of Math and Computer Science, Eastern Connecticut State  
University, Willimantic, CT 06226  
yankovc@easternct.edu

Received: 1/18/08, Accepted: 9/8/08, Published: 10/13/09

Abstract  
The modular hyperbola $\mathcal{H}_n$ is $\{(x, y) : xy \equiv 1 \mod n, 1 \leq x, y \leq n-1\}$. This simply defined set of points has connections to a variety of other mathematical topics including Kloosterman sums, quasirandomness, and consecutive Farey fractions. These connections have inspired a closer look at the distribution of the points of $\mathcal{H}_n$, and many questions remain open. In this paper, we examine the propensity of these points to collect on lines of slope $\pm 1$.

1. Introduction

Let $\mathcal{H}_n$ denote the modular hyperbola $\mathcal{H}_n = \{(x, y) : xy \equiv 1 \mod n, 1 \leq x, y \leq n - 1\}$. An important property of these sets is that the sequence $\{n^{-1}\mathcal{H}_n\}$ is uniformly distributed in the unit square. More precisely, if $\Omega \subseteq [0,1]^2$ has piecewise smooth boundary then

$$
\lim_{n \to \infty} \frac{\#(\Omega \cap n^{-1}\mathcal{H}_n)}{\varphi(n)} = \text{area}(\Omega).
$$

(1)
We note that the cardinality of $\mathcal{H}_n$ is $\varphi(n)$, where $\varphi$ denotes the Euler phi function. To prove (1) it suffices to only consider rectangles $R \subseteq [0,1]^2$. We can express $\#(R \cap n^{-1}\mathcal{H}_n)$ as an exponential sum and then invoke bounds for Kloosterman sums to obtain that
\[
\#(R \cap n^{-1}\mathcal{H}_n) = \text{area}(R)\varphi(n) + O(\tau^2(n) \log^2(n) \sqrt{n}),
\]
where $\tau(n)$ is the number of positive divisors of $n$. The limit (1) is an immediate consequence of this asymptotic formula. The details of this calculation are elegantly presented in [2, Lemma 1.7].

Using a computer algebra package, such as MAPLE, we can easily generate graphs of $\mathcal{H}_n$. A typical example is shown in Figure 1. Such pictures provide convincing visual evidence of the validity of (1) and we encourage the reader to generate other examples. The relevant MAPLE code is given in the appendix.

\[\text{Figure 1. The graph } \mathcal{H}_{5001}\]

In recent years quantitative forms of (1) have been given in a number of papers, see [3, 5, 15, 17, 18] and references therein. For example, it follows from general results of [5] that for primes $p$,
\[
\text{area}(\Omega) - \frac{\#(\Omega \cap p^{-1}\mathcal{H}_p)}{p-1} = O\left(p^{-1/4} \log p\right),
\]
where the implied constant depends only on $\Omega$.

On a whimsical note we observe that from a visual perspective the graphs of $\mathcal{H}_n$ are particularly interesting when $n$ is small. For such integers, the cardinality of $\mathcal{H}_n$, $\varphi(n)$, is small and so one can try to identify patterns in the graphs in the same vein as one looks at clouds in the sky and identifies fanciful shapes! (Once $\varphi(n)$
takes on values in the thousands you simply see a mass of points illustrating the uniform distribution of \( \{n^{-1} \mathcal{H}_n\} \). We give a few of our favorite examples below.
Figure 2. The graph $H_{47}$

Figure 3. The graph $H_{88}$
INTEGERS: 9 Supplement (2009)

In displaying these images, we are delighted to reveal that a butterfly, a dragonfly, and a scholar all lie hidden in the arithmetic structure of the integers!

Returning to matters mathematical, let $D(n)$, $S(n)$, $\bar{D}(n)$ and $\bar{S}(n)$ be the following sets:

$$D(n) = \{(x-y) : (x,y) \in \mathcal{H}_n\}, \quad S(n) = \{(x+y) : (x,y) \in \mathcal{H}_n\},$$

$$\bar{D}(n) = \{(x-y) \mod n : (x,y) \in \mathcal{H}_n\}, \quad \bar{S}(n) = \{(x+y) \mod n : (x,y) \in \mathcal{H}_n\}.$$  

The quantities $\#D(n)$ and $\#S(n)$ count the number of lines, of slope 1 and $-1$ respectively, that have nonempty intersection with $\mathcal{H}_n$. The central results of this paper are precise formulas for $\#D(n)$ and $\#S(n)$.

Since $\{n^{-1}\mathcal{H}_n\}$ is uniformly distributed in the unit square, it is natural to believe that the ratio $\#D(n)/\#S(n)$ should be close to 1 when $n$ is large. Furthermore, it is easy to show that for primes $p$,

$$\frac{\#D(p)}{\#S(p)} = 1 - \frac{1 - (-1/p)}{p+1},$$

where $(a/p)$ is the Legendre symbol. (We prove this assertion at the end of this section.) However whilst looking at some graphs of $\mathcal{H}_n$ (typically with $n$ having several factors of 2), we were quite surprised to see that there seemed to be many more lines of slope 1 intersecting the graph than lines of slope $-1$. Two such “unusual” examples are $\mathcal{H}_{1024}$ and $\mathcal{H}_{1728}$. 

**Figure 4.** The graph $\mathcal{H}_{249}$
We then used Maple to generate some data. In particular we noticed that for powers of 2, the ratio $#D(2^k)/#S(2^k)$, with $k \geq 10$, seemed to lie between 4 and 5 (see Table 1). Our numerical work at this juncture suggested the asymptotic

$$\frac{#D(n)}{#S(n)} \approx 1;$$

but we eventually proved that

$$\liminf_{n \to \infty} \frac{#D(n)}{#S(n)} = 0 \quad \text{and} \quad \limsup_{n \to \infty} \frac{#D(n)}{#S(n)} = \infty,$$

a result completely contrary to our initial intuition and belief!

In the course of our work we realized that we could apply the Chinese Remainder Theorem to the sets $D(n)$ and $S(n)$ and consequently determine formulas for $#D(n)$ and $#S(n)$. This is not the case for the sets $D(n)$ and $S(n)$; but our formulae for
\[ \#D(n) \text{ and } \#S(n), \text{ in conjunction with the inequalities} \]
\[ \#D(n) \leq \#D(n) \leq 2\#D(n) \text{ and } \#S(n) \leq \#S(n) \leq 2\#S(n), \] (3)
give us upper and lower bounds for \#D(n), \#S(n) and related ratios. For example they allow us to prove that \( 3 \leq \#D(2^t)/\#S(2^t) \leq 12 , \) for \( t \) large. Two interesting consequences of the formulas are that the mean-value of \( c(n) \), where \( c(n) = \#S(n)/\#D(n) \), is approximately 1.3; and for more than 80\% of all integers \( c(n) > 1 \).

We end this section by proving our earlier assertion that for primes
\[ \frac{\#D(p)}{\#S(p)} = 1 - \frac{1 - (-1/p)}{p + 1}. \]

**Proposition 1.** For primes \( p > 2 \),
\[ \#S(p) = \frac{p + 1}{2} \] (4)
and
\[ \#D(p) = \frac{p + (-1/p)}{2}, \] (5)
where \((a/p)\) denotes the Legendre symbol.

**Proof.** Let \( k \in S(p) \) and let \((a, b) \in l_k \cap \mathcal{H}_p \), where \( l_k \) denotes the line \( x + y = k \). It is easy to check that \( a \) is a root of \( x^2 - kx + 1 = 0 \) (mod \( p \)). Since any quadratic congruence modulo a prime has at most two roots, we conclude that \( 1 \leq \#(l_k \cap \mathcal{H}_p) \leq 2 \). Now \( x = y \) is a line of symmetry of \( \mathcal{H}_p \) and therefore \((b, a) \in l_k \cap \mathcal{H}_p \). If \( a = b \) then \( l_k \cap \mathcal{H}_p = \{(a, a)\} \), and if \( a \neq b \) then \( l_k \cap \mathcal{H}_p = \{(a, b), (b, a)\} \).

There are two of the former, \( \{(1, 1)\} \) and \( \{(p - 1, p - 1)\} \), and \( (p - 3)/2 \) of the latter, so \( \#S(p) = (p + 1)/2 \).

The proof of (5) is similar. We look at lines \( x - y = k \), and since \( x + y = p \) is a line of symmetry of \( \mathcal{H}_p \) the points again come in pairs, \((a, b) \) and \((p - b, p - a) \). If \(-1 \) is a quadratic residue, the counting is exactly the same and \( \#D(p) = (p + 1)/2 \). If \(-1 \) is not a quadratic residue, there are no singleton sets and \( \#D(p) = (p - 1)/2 \). \( \Box \)

The set \( \{|x - y| \ (x, y) \in \mathcal{H}_p \} \) has been studied in [12] and each result in [12] has an analogous result for \( D(p) \) and \( S(p) \). In particular, the above result and proof is essentially [12, Theorem 1]. As mentioned in the abstract, there are many interesting questions that one can ask about modular hyperbolas. For a discussion of recent results and open problems on modular hyperbolas we refer the reader to the survey article [11].

<table>
<thead>
<tr>
<th>( m )</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
<th>512</th>
<th>1024</th>
<th>2048</th>
<th>4096</th>
<th>8192</th>
<th>16384</th>
</tr>
</thead>
<tbody>
<tr>
<td>( #D(m) )</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>13</td>
<td>21</td>
<td>53</td>
<td>97</td>
<td>205</td>
<td>393</td>
<td>797</td>
<td>1549</td>
<td>3089</td>
</tr>
<tr>
<td>( #S(m) )</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>28</td>
<td>44</td>
<td>84</td>
<td>162</td>
<td>328</td>
<td>652</td>
</tr>
</tbody>
</table>
2. General Strategy

From this point on, \( p \) will always denote a prime. In this section, we will apply the Chinese Remainder Theorem to prove that the quantities \( \#\bar{D}(n) \) and \( \#\bar{S}(n) \) are multiplicative. We will then translate the problem of counting \( \#\bar{D}(p^k) \) and \( \#\bar{S}(p^k) \) to one of counting squares.

**Proposition 2.** Let \( n = \prod_{i=1}^{m} p_i^{e_i} \) be the canonical factorization of \( n \). Then

\[
\#\bar{D}(n) = \prod_{i=1}^{m} \#\bar{D}(p_i^{e_i}) \tag{6}
\]

and

\[
\#\bar{S}(n) = \prod_{i=1}^{m} \#\bar{S}(p_i^{e_i}). \tag{7}
\]

**Proof.** Since the proofs (6) and (7) are identical we only prove the former. The Chinese Remainder Theorem states that the map

\[ f : \mathbb{Z}_n \rightarrow \prod_{i=1}^{m} \mathbb{Z}_{p_i^{e_i}} \]

via

\[ f(x) = (x \mod p_1^{e_1}, \ldots, x \mod p_m^{e_m}) \]

is an isomorphism of rings. Consequently, when we restrict \( f \) to \( \bar{D}(n) \) we obtain a map \( g : \bar{D}(n) \rightarrow \prod_{i=1}^{m} \bar{D}(p_i^{e_i}) \). We now show that \( g \) is a bijection.

The injectivity of \( g \) is clear, so we need to only worry about the surjectivity. Let \((k_1, \ldots, k_m) \in \prod_{i=1}^{m} \bar{D}(p_i^{e_i})\). So there exist \((a_i, b_i) \in \bar{H}_{p_i^{e_i}}\), with \( i = 1, \ldots, m \), such that \((a_i - b_i) \mod p_i^{e_i} = k_i\). By the Chinese Remainder Theorem, the two systems of congruences

\[ x \equiv a_i \mod p_i^{e_i}, \ y \equiv b_i \mod p_i^{e_i}, \ i = 1, \ldots, m, \]

have a unique solution \( x = a, y = b \) modulo \( n \). Since \( a_i b_i \equiv 1 \mod p_i^{e_i} \) for \( i = 1, \ldots, m \), we have that \( ab \equiv 1 \mod n \). Clearly \( g((a - b) \mod n) = (k_1, \ldots, k_m) \). \( \square \)

We now translate the problem of counting \( \#\bar{D}(p^k) \) and \( \#\bar{S}(p^k) \) to one of counting squares. We start with a minor observation.

**Lemma 3.** Let \((a, b) \in \mathcal{H}_{p^r}\). Then \( a - b \equiv 2k_1 \mod p^r \) and \( a + b \equiv 2k_2 \mod p^r \) for some \( k_1, k_2 \in \mathbb{Z} \).

**Proof.** If \( p = 2 \) then \( a, b \) are both odd. If \( p \neq 2 \), then 2 is invertible modulo \( p^r \). \( \square \)

**Theorem 4.** Let \((a, b) \in \mathcal{H}_{p^r}\). Then
1. \((2k \mod p^t) \in \bar{D}(p^t) \iff (k^2 + 1)\) is a square modulo \(p^t\).

Furthermore, the map \(d_{p^t}(k) = 2k \mod p^t\) defines a bijection

\[
d_{p^t} : \{k : k^2 + 1 \text{ is a square modulo } p^t, 0 \leq k < p^t\} \to \bar{D}(p^t),
\]

when \(p \neq 2\).

For the special case \(p = 2\), the map \(d_{2^t}(k) = 2k \mod 2^t\) defines a bijection

\[
d_{2^t} : \{k : k^2 + 1 \text{ is a square modulo } 2^t, 0 \leq k < 2^{t-1}\} \to \bar{D}(2^t),
\]

(that is, we restrict the elements of the domain to lie between 0 and \(2^{t-1}-1\)).

2. \((2k \mod p^t) \in \bar{S}(p^t) \iff (k^2 - 1)\) is a square modulo \(p^t\).

Furthermore, the map \(s_{p^t}(k) = 2k \mod p^t\) defines a bijection

\[
s_{p^t} : \{k : k^2 - 1 \text{ is a square modulo } p^t, 0 \leq k < p^t\} \to \bar{S}(p^t),
\]

when \(p \neq 2\).

For the special case \(p = 2\), the map \(s_{2^t}(k) = 2k \mod 2^t\) defines a bijection

\[
s_{2^t} : \{k : k^2 - 1 \text{ is a square modulo } 2^t, 0 \leq k < 2^{t-1}\} \to \bar{S}(2^t),
\]

(that is, we restrict the elements of the domain to lie between 0 and \(2^{t-1}-1\)).

Proof. Since the proofs of the two parts are identical, we only prove the result for \(\bar{D}(p^t)\).

Let \((a, b) \in \mathcal{H}_{p^t}\). By Lemma 3, \(a - b \equiv 2k \pmod{p^t}\) for some \(k \in \mathbb{Z}\). Upon completing the square, we obtain \(k^2 + 1 \equiv (a - k)^2 \pmod{p^t}\). Conversely, if \(k^2 + 1\) is a square, then there exists \(c \in \mathbb{Z}\) such that \(c^2 - k^2 \equiv 1 \pmod{p^t}\). It follows that

\[(a, b) = ((c + k) \mod p^t, (c - k) \mod p^t) \in \mathcal{H}_{p^t},\]

and \(a - b \equiv 2k \pmod{p^t}\).

If \(p \neq 2\), then 2 is invertible modulo \(p^t\), and consequently

\[d_{p^t}^{-1}(x) = 2^{-1}x \mod p^t.\]

The case when \(p = 2\) is slightly more involved. Let \(k\) be an integer, with \(0 \leq k < 2^t, \) such that \(k^2 + 1\) is a square modulo \(2^t\). It follows immediately that for the integer \(k_1 = (k - 2^{t-1}) \mod 2^t, k_1^2 + 1\) is also a square modulo \(2^t\). The congruence \(2x \equiv 2k \pmod{2^t}\) has precisely two distinct solutions, which must be \(k\) and \(k_1\). Since either \(k\) or \(k_1\) is less than \(2^{t-1}\), we conclude that \(d_{2^t}\) is a bijection.

From this we see that counting \(#\bar{D}(p^t)\) or \(#\bar{S}(p^t)\) is equivalent to counting the \(k\)'s such that \(k^2 + 1\) and \(k^2 - 1\) are squares. In this context, we will on two separate occasions invoke the following formulas of Stangl [13].
Theorem 5 (Stangl). Let \( p \) be an odd prime. Then

\[
\#\{k^2 \mod p^t\} = \frac{p^{t+1}}{2(p+1)} + (-1)^{t-1} \frac{p-1}{4(p+1)} + \frac{3}{4}.
\] (8)

For the special case \( p = 2 \) we have that

\[
\#\{k^2 \mod 2^t\} = \frac{2^{t-1}}{3} + \frac{(-1)^{t-1}}{6} + \frac{3}{2}, \quad t \geq 2.
\] (9)

Finally, we will need the following criteria concerning the solvability of quadratic congruences. (See [8, Propositions 4.2.3, 4.2.4, page 46].)

Proposition 6. For the congruence

\[ x^2 \equiv a \pmod{p^t} \]

where \( p \) is prime and \( a \) is an integer such that \( p \nmid a \), we have the following:

1. \( p \neq 2 \) : If the congruence \( x^2 \equiv a \pmod{p} \) is solvable, then for every \( t \geq 2 \) the congruence \( x^2 \equiv a \pmod{p^t} \) is solvable with precisely 2 distinct solutions.

2. \( p = 2 \) : If the congruence \( x^2 \equiv a \pmod{2^t} \) is solvable, then for every \( t \geq 3 \) the congruence \( x^2 \equiv a \pmod{2^t} \) is solvable with precisely 4 distinct solutions.

3. The Formulas for \( \#\tilde{S}(p^t) \) and \( \#\tilde{D}(p^t) \)

3.1. Case \( n = 2^t \)

In this section we determine the cardinality of \( \tilde{D}(2^t) \) and \( \tilde{S}(2^t) \).

Theorem 7. The cardinality of the set \( D(2^t) \) is

\[
\#D(2^t) = \begin{cases} 
1, & 1 \leq t \leq 3 \\
2^{t-3}, & t \geq 4.
\end{cases}
\] (10)

Proof. Direct computations show that the result is true for \( t \leq 4 \). So we assume that \( t \geq 5 \). By Theorem 4,

\[
\#\tilde{D}(2^t) = \#\{k : k^2 + 1 \text{ is a square modulo } 2^t, 0 \leq k < 2^{t-1}\}.
\]

We claim that

\[ k^2 + 1 \text{ is a square modulo } 2^t \iff k = 4l \text{ for some } l \in \mathbb{Z}. \]

We obtain the \((\Rightarrow)\) direction by reducing modulo 8 and observing that \( k^2 + 1 \) is a square modulo 8 if and only if \( k \equiv 0 \pmod{8} \) or \( k \equiv 4 \pmod{8} \). To obtain the \((\Leftarrow)\) direction we note that \( x^2 \equiv 16l^2 + 1 \pmod{8} \) is solvable for any \( l \), and therefore by
Therefore since and assume \(Pr\) the set \(S\) of \(k\) such that \(k^2 + 1\) is a square modulo \(2^l\), \(0 \leq k < 2^{l-1}\) is \(\{4l : 0 \leq l < 2^{l-3}\}\), and therefore \(\#D(2^l) = 2^{l-3}\).

**Theorem 8.** The cardinality of the set \(\tilde{S}(2^t)\) is

\[
\#\tilde{S}(2^t) = \begin{cases} 
1, & t = 1, 2 \\
2, & t = 3, 4 \\
\frac{2^{t-4}}{3} + \frac{(-1)^{t-1}}{3} + 3, & t \geq 5.
\end{cases}
\]  

(11)

**Proof.** Direct computations show that the result is true for \(t \leq 6\) and so we may assume that \(t \geq 7\). We will prove that

\[
\#\{k : k^2 - 1\ is\ a\ square\ modulo\ 2^l, 0 \leq k < 2^{l-1}\} = 2 \cdot \#\{k^2 \ mod\ 2^{t-4}\}
\]

and conclude by applying (9).

Let \(j \in \{k : k^2 - 1\ is\ a\ square\ modulo\ 2^l, 0 \leq k < 2^{l-1}\}\). Since \(j^2 - 1\ is\ a\ square\ modulo\ 2^l\), we have that \(j = 2l + 1\ for\ some\ l, 0 \leq l < 2^{t-2}\). (Otherwise we would have that \(-1\ is\ a\ square\ modulo\ 4\).) It follows that \((l^2 + l)\ is\ a\ square\ modulo\ 2^{t-2}\) and so we can conclude that

\[
\#\{k : k^2 - 1\ is\ a\ square\ modulo\ 2^l, 0 \leq k < 2^{l-1}\} = \#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}\}.
\]

The set \(\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}\}\) is the union of

\(\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ odd\}\)

and

\(\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ even\}\).

Since \(l^2 + l \equiv (2^{t-2} - 1 - l)^2 + (2^{t-2} - 1 - l) \mod 2^{t-2}\),

\[
\#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ odd\} = \#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ even\}.
\]

Therefore,

\[
\#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}\} = 2\#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ odd\}.
\]

Now

\[
\#\{l : l^2 + l\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ odd\} = \#\{l^{-1} + 1 : l^{-1} + 1\ is\ a\ square\ modulo\ 2^{l-2}, 0 \leq l < 2^{l-2}, l\ odd\}.
\]
If $l^{-1} + 1$ is square modulo $2^{t-2}$, then it is a multiple of 4 and consequently
\[ l^{-1} + 1 \equiv 4m^2 \pmod{2^{t-2}} \]
for some $m, 0 \leq m < 2^{t-4}$. Consequently,
\[ \# \{ l^{-1} + 1 : l^{-1} + 1 \text{ is a square modulo } 2^{t-2}, 0 \leq l < 2^{t-2} \} = \# \{ k^2 \pmod{2^{t-4}} \}, \]
which ends the proof. \qed

### 3.2. Case $n = p^t$, $p$ an Odd Prime

**Proposition 9.** If $p \equiv 1 \pmod{4}$, then for all $t$,
\[ \# \hat{D}(p^t) = \# \hat{S}(p^t). \]  
(12)

**Proof.** If $p \equiv 1 \pmod{4}$, then for any value of $t$ the congruence $x^2 \equiv -1 \pmod{p^t}$ has a solution, $i_{p^t}$. The map $I_{p^t} : \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ via $I_{p^t}(x) = i_{p^t}x$ is a bijection.

Let $k \in \{ k \pmod{p^t} : k^2 - 1 \text{ is a square modulo } p^t \}$. Then $k^2 - 1 \equiv m^2 \pmod{p^t}$ for some $m$, and consequently
\[ i_{p^t}^2 k^2 + 1 \equiv -(k^2 - 1) \equiv -m^2 \equiv (i_{p^t}m)^2 \pmod{p^t}. \]

The above calculation shows that
\[ I_{p^t} ( \{ k \pmod{p^t} : k^2 - 1 \text{ is a square modulo } p^t \} ) = \{ k \pmod{p^t} : k^2 + 1 \text{ is a square modulo } p^t \}, \]
and therefore by Theorem 4, $\# \hat{D}(p^t) = \# \hat{S}(p^t)$. \qed

For the rest of this section we will use the following notation: Let
\[ S'(p^t) = \{ k \pmod{p^t} : k^2 - 1 \text{ is a square modulo } p^t, p \not| (k^2 - 1) \}, \]
\[ S''(p^t) = \{ k \pmod{p^t} : k^2 - 1 \text{ is a square modulo } p^t, p| (k^2 - 1) \}, \]
\[ D'(p^t) = \{ k \pmod{p^t} : k^2 + 1 \text{ is a square modulo } p^t, p \not| (k^2 + 1) \}, \]
and
\[ D''(p^t) = \{ k \pmod{p^t} : k^2 + 1 \text{ is a square modulo } p^t, p| (k^2 + 1) \}. \]

We note that the bijections from Theorem 4 imply
\[ \# \hat{S}(p^t) = \# S'(p^t) + \# S''(p^t) \]
and
\[ \# \hat{D}(p^t) = \# D'(p^t) + \# D''(p^t), \]
which explains our notation. In our next theorem we determine $\# D'(p^t)$ and $\# S'(p^t)$ by calculating a sum of Legendre symbols. We then determine $\# D''(p^t)$ and $\# S''(p^t)$ by applying Stangl’s formula (8).
Theorem 10. Let \( p \) be an odd prime, and let \((a/p)\) denote the Legendre symbol. Then
\[
\# \mathcal{S}'(p^t) = \frac{(p - 3)p^{t-1}}{2}.
\] (13)
and
\[
\# \mathcal{D}'(p^t) = \begin{cases} 
(p - 3)p^{t-1}/2, & p \equiv 1 \pmod{4} \\
(p - 1)p^{t-1}/2, & p \equiv 3 \pmod{4}.
\end{cases}
\] (14)

Proof. The proofs of (13) and (14) are identical and so we will only do the second one. If \( l \in \mathcal{D}'(p^t) \), then the Legendre symbol \(((l^2 + 1)/p) = 1\). Therefore,
\[
\# \mathcal{D}'(p^t) = \frac{1}{2} \sum_{l=0, \gcd(l^2+1,p)=1}^{p^t-1} \left( \left( \frac{l^2 + 1}{p} \right) + 1 \right)
\]
\[
= \frac{1}{2} \sum_{k=0}^{p^t-1} \sum_{l=0, l^2 \neq -1 \pmod{p}}^{p-1} \left( \left( \frac{(l+k)^2 + 1}{p} \right) + 1 \right)
\]
\[
= \left( \sum_{l=0, l^2 \neq -1 \pmod{p}}^{p-1} \left( \left( \frac{l^2 + 1}{p} \right) + 1 \right) \right) \frac{p^t-1}{2}
\]
\[
= \left( -1 + \sum_{l=0, l^2 \neq -1 \pmod{p}}^{p-1} 1 \right) \frac{p^t-1}{2},
\]
where the \(-1\) term in the last expression arises by invoking
\[
\sum_{a=0}^{p-1} \left( \frac{a^2 + 1}{p} \right) = -1,
\]
(see [1, Theorem 2.1.2, page 58]). We complete our proof by noting that
\[
\sum_{l=0, l^2 \neq -1 \pmod{p}}^{p-1} 1 = \begin{cases} 
0, & p \equiv 1 \pmod{4} \\
-1, & p \equiv 3 \pmod{4}.
\end{cases}
\]
\[
\square
\]

Lemma 11. If \( p \equiv 3 \pmod{4} \), then
\[
\# \mathcal{D}''(p^t) = 0,
\]
and consequently
\[
\# \mathcal{D}(p^t) = \# \mathcal{D}'(p^t) = \frac{\varphi(p^t)}{2}.
\] (15)

Proof. If \( p \equiv 3 \pmod{4} \) then the congruence \( x^2 + 1 = 0 \pmod{p} \) has no solutions and consequently
\[
\# \mathcal{D}''(p^t) = 0.
\]
\[
\square
Proposition 12. The cardinality of the set $S''(p^t)$ is

$$
\#S''(p^t) = \begin{cases} 
\frac{(p^t-1)2}{p+1} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)} & \text{if } p \equiv 1 \pmod{4}, t \leq 2 \\
\frac{(p^t-1)2}{p+1} + \frac{p-1}{2} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)} & \text{if } p \equiv 1 \pmod{4}, t \geq 3
\end{cases}
$$

(16)

Proof. Let $k \in S''(p^t)$. Then $k^2 - 1 \equiv p^2m^2 \pmod{p^t}$ for some $m, 0 \leq m < p^{t-2}$. We have two cases to consider.

1. $t \leq 2$: In this case we have $m = 0$, and since the congruence $x^2 \equiv 1 \pmod{p^t}$ has exactly 2 solutions, we conclude that $\#S''(p^t) = 2$.

2. $t \geq 3$: In this case we define a map

$$S''(p^t) \rightarrow \{m^2 \mod p^{t-2}\}

$$

via $k \mapsto m^2$. By Proposition 6, for each $m^2 \in \{m^2 \mod p^{t-2}\}$, the congruence $x^2 \equiv p^2m^2 + 1 \pmod{p^t}$ is solvable with precisely two solutions. Hence, the map is surjective with each element in the image having exactly two elements in its preimage. Consequently, we can infer that $\#S''(p^t) = 2 \#\{m^2 \mod p^{t-2}\}$, and we conclude by invoking (8).

\[ \square \]

On combining all of the pieces we obtain the following formulas for $\#\bar{D}(p^t)$ and $\#\bar{S}(p^t)$.

Theorem 13. The cardinalities of the sets $\bar{D}(p^t)$ and $\bar{S}(p^t)$ are

$$
\#\bar{D}(p^t) = \begin{cases} 
\left(\frac{(p-1)p^{t-1}}{2}\right) + \frac{2}{2} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)}, & p \equiv 1 \pmod{4}, t \leq 2 \\
\left(\frac{(p-1)p^{t-1}}{2}\right) + \frac{p-1}{2} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)}, & p \equiv 1 \pmod{4}, t \geq 3
\end{cases}
$$

(17)

and

$$
\#\bar{S}(p^t) = \begin{cases} 
\left(\frac{(p-3)p^{t-1}}{2}\right) + \frac{2}{2} + \frac{p-1}{2} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)}, & t \leq 2 \\
\left(\frac{(p-3)p^{t-1}}{2}\right) + \frac{p-1}{2} + \frac{3}{2} + (-1)^{t-3} \frac{p-1}{2(p+1)}, & t \geq 3
\end{cases}
$$

(18)

4. Some Properties of $c(n) = \#\bar{S}(n)/\#\bar{D}(n)$

To simplify notational matters, let $c(n) = \#\bar{S}(n)/\#\bar{D}(n)$. We use our formulas for $\#\bar{S}(n)$ and $\#\bar{D}(n)$ to determine some properties of $c(n)$. We begin with some elementary, but useful remarks about $c(p^k)$.

Lemma 14. $c(p^k)$ has the following properties.

1. For $p \equiv 1 \pmod{4}$,

$$c(p^k) = 1.
$$

(19)
2. For \( p \equiv 3 \pmod{4} \),
\[
c(p) = \left( 1 + \frac{2}{p-1} \right).
\] (20)

3. For \( p \equiv 3 \pmod{4} \) and \( k \geq 2 \),
\[
c(p^k) - c(p^{k-1}) = \begin{cases} 
-\frac{4}{p^k - 1}, & k \text{ even} \\
-\frac{2}{p^k - 1}, & k \text{ odd}.
\end{cases}
\] (21)

4. For \( k \geq 6 \),
\[
c(2^k) - c(2^{k-1}) = \begin{cases} 
-\frac{1}{2^k - 1}, & k \text{ even} \\
-\frac{1}{2^k - 1}, & k \text{ odd}.
\end{cases}
\] (22)

5. For \( k \geq 1 \),
\[
1/6 \leq c(2^k) \leq 2.
\] (23)

6. For \( k \geq 2 \),
\[
\frac{1}{4} \leq c(3^k) \leq \frac{2}{3}.
\] (24)

7. For \( p \geq 5, p \equiv 3 \pmod{4} \) and \( k \geq 2 \),
\[
\left( 1 - \frac{2}{p-1} \right) \leq c(p^k) \leq \left( 1 - \frac{2}{p-1} + \frac{4}{p^2 - p} \right) < 1.
\] (25)

Proof. These are immediate consequences of formulas (17) and (18). We make a few remarks: the maximum value of \( c(2^k) \) is \( c(8) = 2 \); in (25) the upper bound is achieved when \( k = 2 \); if \( p \equiv 3 \pmod{4} \) then for any \( k \geq 2 \), \( c(p^k) < c(p) \). Finally, the reason we treated the case of \( 3^k \) separately is that the LHS of (25) equals 0 when \( p = 3 \). We could have merged (24) and (25) by replacing the LHS of (25) with
\[
\left( 1 - \frac{2}{p-1} + \frac{2}{p^2 - 1} \right)
\]

\( \Box \)

We now prove that the maximal and minimal order of \( c(n) \) is \( \log \log n \) and \( 1/\log \log n \) respectively.

Theorem 15. Let \( N_k = \prod_{i=1}^{k} p_i \), where \( p_i \) is the \( i \)-th prime that is congruent to 3 modulo 4.

(1) We have
\[
c(N_k) \asymp \log \log N_k;
\] (26)

and for any \( t \geq 2 \),
\[
c(N_k^t) \asymp (\log \log N_k)^{-1}.
\] (27)
Consequently,
\[ \limsup_{n \to \infty} c(n) = \infty, \]  
and
\[ \liminf_{n \to \infty} c(n) = 0. \]

(2) Furthermore,
\[ c(n) \ll \log \log n \]  
and
\[ c(n) \gg \frac{1}{\log \log n}. \]

Proof. For (1), we only prove (26) as the proof of (27) is similar. Since
\[ c(N_k) = \prod_{i=1}^{k} \left( 1 + \frac{2}{p_i - 1} \right), \]
we have by the Taylor series of \( \log(1 + x) \) that
\[ \log c(N_k) = 2 \sum_{i=1}^{k} \frac{1}{p_i - 1} + \sum_{i=1}^{k} \sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} \left( \frac{2}{p_i - 1} \right)^m. \]  
(32)

For \( p \geq 5 \),
\[ \left| \frac{4}{(p-1)^2} \sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} \left( \frac{2}{p-1} \right)^{m-2} \right| \leq \frac{4}{(p-1)^2} \sum_{m=0}^{\infty} 2^{-m} = \frac{8}{(p-1)^2}, \]
and therefore the double series
\[ C = \sum_{i=1}^{\infty} \sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} \left( \frac{2}{p_i - 1} \right)^m \]
converges since the \( i = 1 \) term is a convergent alternating series and the remaining terms are bounded in magnitude by \( \sum_{i=2}^{\infty} 8i^{-2} \).

Since \( C < 0 \), we obtain from (32) the inequality
\[ 2 \sum_{i=1}^{k} \frac{1}{p_i} + C \leq \log c(N_k) \leq 1 + 2 \sum_{i=1}^{k} \frac{1}{p_i}. \]  
(33)

We now apply to (33) Mertens’s formula (see [4, Section 2.2]) for primes \( p \equiv 3 \) (mod 4),
\[ \lim_{k \to \infty} \left( \sum_{i=1}^{k} \frac{1}{p_i} - \frac{1}{2} \log \log p_k \right) = 0.048239 \ldots, \]
and obtain
\[ \log(c(N_k)) - \log \log(p_k) = O(1). \]  
(34)
The prime number theorem for arithmetic progressions for primes \( p \equiv 3 \pmod{4} \) implies
\[
\lim_{k \to \infty} \frac{\log N_k}{p_k} = \frac{1}{2}.
\]
Consequently \( \log \log N_k - \log \log p_k = o(1) \) and so we can replace \( \log \log p_k \) with \( \log \log \log N_k \) in (34) and obtain the desired conclusion that \( \log(c(N_k)) - \log \log N_k = O(1) \).

The proof of (27) is nearly identical. The main difference is that we start with the inequality
\[
\frac{1}{4} \prod_{i=2}^{k} \left( 1 - \frac{2}{p_i - 1} \right) \leq c(N_k) \leq \prod_{i=1}^{k} \left( 1 - \frac{2}{p_i - 1} + \frac{4}{p^2 - p} \right),
\]
that we obtain by applying the inequalities (24) and (25).

We next prove item (2). If \( n \) has no prime factors congruent to 3 modulo 4, then we have the inequality \( 1/6 \leq c(n) \leq 2 \). So without loss of generality we may assume that \( q_1, \ldots, q_k \) are the distinct prime factors of \( n \) that are congruent to 3 modulo 4. Clearly \( n \geq q_1 \ldots q_k \geq N_k \). From (20) and (26) we get that \( c(n) \leq 2c(N_k) \approx \log \log N_k \leq \log \log n \).

We now prove (31). An immediate consequence of the asymptotic
\[
2 \sum_{i=1}^{k} \frac{1}{p_i} - \log \log N_k = O(1)
\]
is that
\[
\frac{1}{4} \prod_{i=2}^{k} \left( 1 - \frac{2}{p_i - 1} \right) \asymp \frac{1}{\log \log N_k}.
\]
We combine this with the inequality
\[
c(n) \geq \frac{1}{24} \prod_{i=2}^{k} \left( 1 - \frac{2}{q_i - 1} \right) \geq \frac{1}{24} \prod_{i=2}^{k} \left( 1 - \frac{2}{p_i - 1} \right)
\]
to obtain (31).

\(\square\)

**Corollary 16.** For the sequence \( \frac{\#S(n)}{\#D(n)} \) we have
\[
\liminf \frac{\#S(n)}{\#D(n)} = 0 \text{ and } \limsup \frac{\#S(n)}{\#D(n)} = \infty.
\]

**Proof.** Since \( \#D(n) \leq \#S(n) \leq 2\#D(n) \) and \( \#S(n) \leq \#D(n) \leq 2\#S(n) \), we obtain the inequality
\[
0.5c(n) \leq \frac{\#S(n)}{\#D(n)} \leq 2c(n).
\]
We now apply (29), (28) to obtain (35). \(\square\)
Corollary 17. The Dirichlet series \( \sum_{n=1}^{\infty} c(n)n^{-s} \) converges absolutely in the half-plane \( \Re(s) > 1 \).

Proof. This is an immediate consequence of (30).

We preface our calculation of the mean value of \( c(n) \) with the following observation about mean values of arithmetical functions. Let

\[
M(g) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} g(n)
\]
denote the mean value of \( g \). If \( M(g) \) exists, then, via partial summation, we have that

\[
M(g) = \lim_{s \to 1^+} \frac{1}{\zeta(s)} \sum_{n=1}^{\infty} g(n)n^{-s}.
\]

Thus if \( g \) is multiplicative then we can represent \( M(g) \) by the infinite product

\[
M(g) = \prod_{p \text{ prime}} \left( 1 - \frac{1}{p} \right) \left( \sum_{k=0}^{\infty} \frac{g(p^k)}{p^k} \right) = \prod_{p \text{ prime}} \left( 1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^k} \right).
\]

Since we have explicit formulas for \( c(p^k) \) we can easily compute \( M(c) \) provided we first show that this mean value exists. Arguably the simplest proof of the existence of \( M(c) \) is to invoke Wintner’s mean-value theorem for multiplicative functions.

Theorem 18 (Wintner). If \( g \) is a multiplicative function satisfying the conditions

\[
\sum_{p \text{ prime}} \frac{|g(p) - 1|}{p} < \infty \quad \text{and} \quad \sum_{p \text{ prime}} \sum_{k=2}^{\infty} \frac{|g(p^k) - g(p^{k-1})|}{p^k} < \infty,
\]

then \( M(g) \) exists.

This was first proved in [16] — a monograph that is very difficult to find. For a more recent and accessible reference see [10, II.2, Corollary 2.3]. The proof is a straightforward convolution argument.

Theorem 19. The mean-value of \( c(n) \), \( M(c) \), is given by the infinite product

\[
M(c) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} c(n) = \frac{337}{320} \prod_{p \equiv 3 \pmod{4}} \left( 1 + \frac{2(p^2 - p + 1)}{p^4 - 1} \right) \approx 1.32. \quad (36)
\]

Proof. From the properties of \( c(p^k) \) listed in Lemma 14 the series

\[
\sum_{p \text{ prime}} \frac{|c(p) - 1|}{p} \quad \text{and} \quad \sum_{p \text{ prime}} \sum_{k=2}^{\infty} \frac{|c(p^k) - c(p^{k-1})|}{p^k}
\]

are both convergent and therefore by Wintner’s theorem we conclude that \( M(c) \) exists. We now use (10), (11), (19), (20), (21) and (22) to obtain \( M(c) \). \( \Box \)
Our final result shows that \( c(n) > 1 \) for over 80% of all integers. We prove it by applying Wirsing's mean-value theorem for multiplicative functions \([14, \text{III.4, Theorem } 5]\).

**Theorem 20 (Wirsing).** If \( g \) is a real multiplicative function with \( |g(n)| \leq 1 \) for all \( n \in \mathbb{Z}^+ \), then \( M(g) \) exists.

Wirsing's theorem is a deep theorem. For example, it contains the Prime Number Theorem in its equivalent form \( M(\mu) = 0 \), where \( \mu \) is the Möbius function, see [7, Section 3]. We would have preferred to have used a simpler result such as Wintner's theorem; however, the condition that \( \sum_{p \text{ prime}} |g(p) - 1|p^{-1} \) is convergent is not satisfied in one part of our argument. We will need the following lemma to justify the use of Wirsing's theorem.

**Lemma 21.** For each prime \( p \), let \( v_p(n) \) denote the exponent of the prime \( p \) in the canonical factorization of \( n \) and let \( A_p \) denote a non-empty subset of \( \mathbb{Z}^+ \cup \{0\} \). Then the characteristic function of the set \( \{ n : v_p(n) \in A_p \} \cup \{1\} \) is multiplicative.

**Proof.** We construct a function \( \chi : \mathbb{Z}^+ \to \{0, 1\} \) in the following way. Let \( \chi(1) = 1 \) and, for \( k \geq 1 \), let

\[
\chi(p^k) = \begin{cases} 1 & k \in A_p \\ 0 & k \notin A_p; \end{cases}
\]

and

\[
\chi(n) = \prod_i \chi(p_i^{v_i}),
\]

where \( \prod p_i^{v_i} \) is the canonical factorization of \( n \). Clearly, \( \chi \) is both multiplicative and also the characteristic function of \( \{ n : v_p(n) \in A_p \} \cup \{1\} \).

**Theorem 22.** Let \( \mathcal{C} = \{ n : c(n) > 1 \} \) and let \( \chi \) denote the characteristic function of \( \mathcal{C} \). Then the lower density of \( \mathcal{C} \), \( \liminf_{x \to \infty} x^{-1} \sum_{n \leq x} \chi(n) \), satisfies the inequality

\[
\liminf_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \chi(n) \geq \frac{63}{64} \prod_{p \equiv 3 \mod 4} \left( 1 - \frac{1}{p^2} \right) \approx 0.84.
\]

Furthermore, for any positive constant \( L \), the set \( \{ n : c(n) \geq L \} \) has positive lower density.

**Proof.** Let \( \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \) be the sets

\[
\mathcal{C}_1 = \{ n : v_2(n) \leq 5, \text{ and } v_p(n) \leq 1 \text{ if } p \equiv 3 \mod 4 \},
\]

\[
\mathcal{C}_2 = \{ n : n \in \mathcal{C}_1, v_2(n) \neq 3, \text{ and } v_p(n) = 0 \text{ if } p \equiv 3 \mod 4 \},
\]

and \( \mathcal{C}_3 = \mathcal{C}_1 \setminus \mathcal{C}_2 \); and let \( \chi_1 \) and \( \chi_2 \) be the characteristic functions of \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) respectively. The conditions on \( \mathcal{C}_1 \) ensure that for any \( n \in \mathcal{C}_1 \) and for any prime \( p \),
$c(p^v(n)) \geq 1$. Therefore for any $n \in C_1$ we have $c(n) \geq 1$ with equality precisely when $n \in C_2$, showing that $C_3 \subseteq C$.

By Lemma 21, $\chi_1$ and $\chi_2$ are multiplicative functions and so we can apply Wirsing’s theorem to obtain that

$$\text{density}(C_3) = M(\chi_1 - \chi_2) = M(\chi_1) - M(\chi_2)$$

$$= \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right) \left(1 + \sum_{i=1}^{k} \frac{\chi_1(p^i)}{p^i}\right) - \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right) \left(1 + \sum_{i=1}^{k} \frac{\chi_2(p^i)}{p^i}\right)$$

$$= \frac{63}{64} \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{1}{p^2}\right) - 0 = \frac{63}{64} \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{1}{p^2}\right).$$

(We cannot invoke Wintner’s theorem here as the series $\sum_p |\chi_2(p) - 1|p^{-1}$ is divergent.) By our formulas for $\#D(n)$ and $\#S(n)$ we have the inclusion $C_3 \subseteq C$, and so we can conclude that the lower density of $C$ is greater or equal to the density of $C_3$.

A slight variation of the above proof gives the second assertion. Recalling the notation in Theorem 15, let $p_i$ denote the $i$-th prime congruent to 3 modulo 4 and let $N_k = \prod_{i=1}^{k} p_i$. Since $c(N_k) \asymp \log \log N_k$ (see asymptotic (26)), we can find an integer $l$ such that $c(N_k) \geq L$ for $k \geq l$. Let

$$L_1 = \{ n : v_2(n) = 0 \text{ and } v_{p_i}(n) \leq 1 \text{ for } i = 1, 2, \ldots \},$$

$$L_2 = \{ n : n \in L_1 \text{ and } v_{p_i}(n) = 0 \text{ for } i = 1, \ldots, l \},$$

and $L_3 = L_1 \setminus L_2$. A slight modification of our earlier calculation of density$(C_3)$ gives that

$$\text{density}(L_3) = \frac{1}{2} \left(1 - \prod_{i=1}^{l} \frac{1}{1 + \frac{1}{p_i}}\right) \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{1}{p^2}\right).$$

We conclude by observing that for any $n \in L_3$, $c(n) \geq c(N_l) \geq L$. \qed

### 4.1. Unanswered Questions and Ongoing Work

We have not resolved the following 3 questions.

1. Does the density of $A = \{ n \in \mathbb{Z}^+ : c(n) = 1 \}$ equal 0? This would follow if we could prove that for any $n \in A$, the odd prime factors of $n$ are all congruent to 1 mod 4.

2. What is the density of $\{ n \in \mathbb{Z}^+ : c(n) < 1 \}$? Is it non-zero?

3. What is the normal order of $c(n)$?
It is easy to generalize Proposition 2 to arbitrary polynomials in \( \mathbb{Z}[x,y] \). Specifically, if \( f \in \mathbb{Z}[x,y] \) and we define the map \( f_n : \mathcal{H}_n \rightarrow \mathbb{Z}_n \) via \( f_n((x,y)) = f(x,y) \) mod \( n \), then the quantity \( \#\text{Image}(f_n) \) is a multiplicative function of \( n \). One possible extension of our work is to determine formulas for \( \#\text{Image}(f_p) \) for some other polynomials \( f \in \mathbb{Z}[x,y] \), especially for cases where one can apply the formulas in [13] and this paper. S. Hanrahan, under the supervision of M. Khan, is currently writing an undergraduate honors thesis on this topic for the quadratic forms \( x^2 + y^2 \) and \( x^2 - y^2 \).

5. Appendix
This is the MAPLE code that generated the graph of \( \mathcal{H}_{5001} \).

```maple
n:=5001:
a:=array(1..numtheory[phi](n)):
b:=array(1..numtheory[phi](n)):
count:=1:
for i from 1 to n-1 do;
  if gcd(i,n)=1 then
    a[count]:=i: b[count]:=(i^(-1)mod n):
    count := count+1;
  end if;
end do:
printf("n=\%d, no. of points on graph=\%d \n",n,count-1):
points := zip((x,y) -> [x,y],a,b):
p1:=plot(points,style=POINT,symbol=CROSS):
plots[display](p1);
```

References


