The cardinality of the value sets modulo $n$ of $x^2 + x^{-2}$ and $x^2 + y^2$

Sara Hanrahan and Mizan Khan
The cardinality of the value sets modulo $n$ of $x^2 + x^{-2}$ and $x^2 + y^2$

Sara Hanrahan and Mizan Khan

(Communicated by Filip Saidak)

Consider the modular circle $\mathcal{C}_{a,n} = \{(x, y) : x^2 + y^2 \equiv a \pmod{n}, \ 0 \leq x, y \leq n-1\}$ and the modular hyperbola $\mathcal{H}_n = \{(x, y) : xy \equiv 1 \pmod{n}, \ 0 \leq x, y \leq n-1\}$.

We provide explicit formulas for the cardinality of the sets

\[
\{a \mod n : \mathcal{C}_{a,n} \cap \mathcal{H}_n \neq \emptyset\} \quad \text{and} \quad \{a \mod n : \mathcal{C}_{a,n} \neq \emptyset\}.
\]

**Introduction**

Let $\mathcal{H}_n$ denote the modular hyperbola

\[
\{(x, y) : xy \equiv 1 \pmod{n}, \ 0 \leq x, y \leq n-1\}.
\]

This simply defined discrete set of points has connections to a variety of other mathematical topics including Kloosterman sums, consecutive Farey fractions, and quasirandomness. These connections have inspired a closer look at the distribution of the points of $\mathcal{H}_n$, and many questions remain open. For a discussion of recent results and open problems on modular hyperbolae, see [Shparlinski 2007].

The propensity of the points on $\mathcal{H}_n$ to collect on lines of slope $\pm 1$ was investigated in [Eichhorn et al. 2009]. In the course of that investigation, formulas for the cardinalities of the sets

\[
\{(x - y) \mod n : (x, y) \in \mathcal{H}_n\} \quad \text{and} \quad \{(x + y) \mod n : (x, y) \in \mathcal{H}_n\},
\]

were derived. The techniques used to determine these formulas are elementary — within the grasp of an undergraduate mathematics major who has had a course in number theory or abstract algebra.

In this article we investigate the intersection of $\mathcal{H}_n$ with the modular circles

\[
\mathcal{C}_{a,n} = \{(x, y) : x^2 + y^2 \equiv a \pmod{n}, \ 0 \leq x, y \leq n-1\},
\]

Keywords: cardinality, value sets, modular circle, modular hyperbola.
This work was done as part of Hanrahan’s undergraduate honors thesis under Khan’s supervision.
and in particular we determine the cardinality of the set

\[ \{ a \mod n : \mathcal{E}_{a,n} \cap \mathcal{H}_n \neq \emptyset \} = \{ (x^2 + y^2) \mod n : (x, y) \in \mathcal{H}_n \}. \]

Figure 1 contrasts the modular circle \( \mathcal{C}_{1,997} \) with the modular hyperbola \( \mathcal{H}_{997} \). Figure 2 shows the two superimposed, and the intersection \( \mathcal{C}_{1,997} \cap \mathcal{H}_{997} \).

This short note is a concise version of SH’s honors thesis. It is also a natural addendum to [Eichhorn et al. 2009], as we used the formulas found there to prove our results.

**Figure 1.** Left: The modular hyperbola \( \mathcal{H}_{997} \). Right: The modular circle \( \mathcal{C}_{1,997} \).

**Figure 2.** Left: Superposition of the preceding two sets. Points of the modular circle are represented by crosses; those of the modular hyperbola by solid circles. Right: The intersection \( \mathcal{C}_{1,997} \cap \mathcal{H}_{997} = \{ (91, 252), (252, 91), (745, 906), (906, 745) \} \).
1. Preliminary results

Let \( f \in \mathbb{Z}[x_1, \ldots, x_k] \) and let \( S \subseteq \mathbb{Z}_n^k \) (where \( \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \) is the set of integers modulo \( n \)). Then \( I(f, S) \) will denote the set

\[
I(f, S) = \{ f(x_1, \ldots, x_k) \mod n : (x_1, \ldots, x_k) \in S \}.
\]

We also define two subsets of \( I(f, S) \):

\[
I'(f, S) = \{ a : a \in I(f, S), \gcd(a, n) = 1 \},
\]
\[
I''(f, S) = \{ a : a \in I(f, S), \gcd(a, n) \neq 1 \}.
\]

Our first result is that the quantity \( \#I(f, \mathbb{H}_n) \) is a multiplicative function of \( n \). Furthermore, by replacing each occurrence of \( \mathbb{H}_n \) with \( \mathbb{Z}_2^k \) in the statement and proof of the theorem, we get that \( \#I(f, \mathbb{Z}_2^k) \) is also a multiplicative function of \( n \).

**Proposition 1.** Let \( f \in \mathbb{Z}[x, y] \) and define \( f_n : \mathbb{H}_n \rightarrow \mathbb{Z}_n \) by

\[
f_n((x, y)) = f(x, y) \mod n.
\]

If \( n = a \cdot b \) with \( \gcd(a, b) = 1 \), then

\[
\#I(f, \mathbb{H}_n) = \#I(f, \mathbb{H}_a) \cdot \#I(f, \mathbb{H}_b).
\]

It follows that if \( n = \prod_{i=1}^m p_i^{e_i} \) is the canonical factorization of \( n \), then

\[
\#I(f, \mathbb{H}_n) = \prod_{i=1}^m \#I(f, \mathbb{H}_{p_i^{e_i}}).
\]

**Proof.** The Chinese remainder theorem says that the map \( r : \mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b \) given by

\[
r(x) = (x \mod a, x \mod b)
\]

is an isomorphism of rings. Hence the map \( R : \mathbb{H}_n \rightarrow \mathbb{H}_a \times \mathbb{H}_b \) defined by

\[
R((x, y)) = ((x \mod a, y \mod a), (x \mod b, y \mod b))
\]

is a bijection. The result now follows from the observation that the diagram

\[
\begin{array}{ccc}
\mathbb{H}_n & \xrightarrow{R} & \mathbb{H}_a \times \mathbb{H}_b \\
\downarrow f_n & & \downarrow f_a \times f_b \\
\mathbb{Z}_n & \xrightarrow{r} & \mathbb{Z}_a \times \mathbb{Z}_b.
\end{array}
\]

 Thus we have reduced the problem of determining formulas for \( \#I(x^2+y^2, \mathbb{H}_n) \) (or \( \#I(x^2+y^2, \mathbb{Z}_n^2) \)) to determining them for prime powers. From this point, we shall refer to the set \( I(x^2+y^2, \mathbb{H}_n) \) as \( I(x^2+x^{-2}, \mathbb{Z}_n) \). All of our formulas were
discovered through extensive numerical experimentation with Maple. Maple was the most valuable research tool at our disposal — only in discovering the formulas, but also in the proving stage. In the remainder of this section, we list the mathematical results we need to prove these formulas.

It is more convenient to work with the value set \( I((x + x^{-1})^2, \mathbb{Z}_n) \) than with \( I(x^2 + x^{-2}, \mathbb{Z}_n) \). The following lemma justifies the change.

**Lemma 2.** For any positive integer \( n \),

\[
\#I(x^2 + x^{-2}, \mathbb{Z}_n) = \#I((x + x^{-1})^2, \mathbb{Z}_n).
\] (2)

**Proof.** The map \( z \mapsto (z + 2) \mod n \) defines a bijection between \( I(x^2 + x^{-2}, \mathbb{Z}_n) \) and \( I((x + x^{-1})^2, \mathbb{Z}_n) \). \( \Box \)

We next state a basic criterion on the solvability of quadratic congruences modulo prime powers:

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

**Proposition 3** [Ireland and Rosen 1982, Propositions 4.2.3, 4.2.4, p. 46]. Let \( p \) be prime and let \( a \) be an integer such that \( \gcd(a, p) = 1 \).

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

**Proposition 4** [Stangl 1996]. Let \( p \) be an odd prime. Then

\[
\#I(x^2, \mathbb{Z}_{p^t}) = \frac{p^{t+1}}{2(p+1)} + \frac{(-1)^{t-1}}{4} \frac{p-1}{4(p+1)} + \frac{3}{4}. \] (3)

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

\[
\#I(x^2, \mathbb{Z}_{2^t}) = \frac{2^{t+1}}{3} + \frac{(-1)^{t-1}}{6} + \frac{3}{2}, \quad t \geq 2. \] (4)

**Proposition 5** [Eichhorn et al. 2009].

\[
\#I(x + x^{-1}, \mathbb{Z}_{p^t}) = \frac{(p-3)p^{t-1}}{2} + \frac{2p^{t-1} + (-1)^{t-1}(p-1)}{2(p+1)} + \frac{3}{2}. \] (5)

2. The formulas for \( \#I((x + x^{-1})^2, \mathbb{Z}_{p^t}) \)

The central result of this paper is as follows.
Theorem 6. For \( p = 2 \) and \( t \geq 7 \),
\[
\#I((x + x^{-1})^2, \mathbb{Z}_{2^t}) = \frac{2^{t-7}}{3} + \frac{(-1)^{t-1}}{6} + \frac{3}{2}. \tag{6}
\]
If \( p \equiv 1 \pmod{4} \) then
\[
\#I((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{(p - 5)p^{t-1}}{4} + \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{2(p + 1)} + \frac{3}{2}. \tag{7}
\]
If \( p \equiv 3 \pmod{4} \) then
\[
\#I((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{(p - 3)p^{t-1}}{4} + \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{4(p + 1)} + \frac{3}{4}. \tag{8}
\]
The proof occupies most of this section.

Proof of Theorem 6, case \( p > 2 \). We will use the squaring map modulo \( p^t \):
\[
Q : I(x + x^{-1}, \mathbb{Z}_{p^t}) \rightarrow I((x + x^{-1})^2, \mathbb{Z}_{p^t}), \quad Q(z) = z^2 \mod p^t.
\]
We note that it preserves coprimeness with \( p \):
\[
Q(I'(x + x^{-1}, \mathbb{Z}_{p^t})) = I'((x + x^{-1})^2, \mathbb{Z}_{p^t}),
\]
\[
Q(I''(x + x^{-1}, \mathbb{Z}_{p^t})) = I''((x + x^{-1})^2, \mathbb{Z}_{p^t}).
\]

Proposition 7. Let \( p \) be an odd prime. For any \( a \in I'((x + x^{-1})^2, \mathbb{Z}_{p^t}) \), we have \( \#Q^{-1}([a]) = 2 \), and consequently
\[
\#I'(x + x^{-1})^2, \mathbb{Z}_{p^t}) = \#I'(x + x^{-1}, \mathbb{Z}_{p^t})/2. \tag{9}
\]
Proof. Let \( a \) be an arbitrary element of \( I'((x + x^{-1})^2, \mathbb{Z}_{p^t}) \). There exists a point \((x_1, y_1) \in \mathcal{H}_{p^t}\) such that
\[
(x_1 + y_1)^2 \equiv a \pmod{p^t}.
\]
Since \( \gcd(x_1 + y_1, p) = 1 \),
\[
x_1 + y_1 \not\equiv -(x_1 + y_1) \pmod{p^t};
\]
hence the two distinct elements of \( I'((x + x^{-1})^2, \mathbb{Z}_{p^t}) \) that \( Q \) maps to \( a \) are
\[
(x_1 + y_1) \pmod{p^t} \quad \text{and} \quad -(x_1 + y_1) \pmod{p^t}.
\]
By Proposition 3, the congruence \( x^2 \equiv a \pmod{p^t} \) has at most two solutions and we conclude that \( \#Q^{-1}([a]) = 2 \). \( \square \)

Proposition 8.
\[
\#I''(x + x^{-1}, \mathbb{Z}_{p^t}) = \begin{cases} p^{t-1} & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{10}
\]
Consequently, when $p \equiv 1 \pmod{4}$,

$$I''(x + x^{-1}, \mathbb{Z}_{p^t}) = \{kp : k = 0, 1, \ldots, p^{t-1} - 1\}.$$

**Proof.** Define $s_{p^t} : \mathcal{E}_{p^t} \to \mathbb{Z}_{p^t}$ by $s_{p^t}((x, y)) = (x + y) \mod p^t$ and let

$$\mathcal{E}_{p^t}'' = \{(x, y) : (x, y) \in \mathcal{E}_{p^t} \text{ with } s_{p^t}((x, y)) \in I''(x + x^{-1}, \mathbb{Z}_{p^t})\}.$$

If $(x, y) \in \mathcal{E}_{p^t}''$, then $x + y \equiv 0 \pmod{p}$ and consequently $x^2 \equiv -1 \pmod{p}$. Since $-1$ is a quadratic residue modulo $p$ if and only if $p \equiv 1 \pmod{4}$, we obtain the second part of (10).

We now restrict our attention to primes $p$ that are congruent to 1 modulo 4. Since $s_{p^t}(\mathcal{E}_{p^t}''') = I''(x + x^{-1}, \mathbb{Z}_{p^t})$, we prove the first part of (10) by proving the following two assertions:

(i) $\#s_{p^t}^{-1}([a]) = 2$ for any $a \in I''(x + x^{-1}, \mathbb{Z}_{p^t})$.

(ii) $\#\mathcal{E}_{p^t}''' = 2p^{t-1}$.

The proof of (i) is as follows. Let $(r, s) \in s_{p^t}^{-1}([a])$. Then $(2r - a)$ and $(2s - a)$ are two distinct roots of the congruence

$$x^2 \equiv (a^2 - 4) \pmod{p^t}.$$

Since $p \mid a$, we have $\gcd(a^2 - 4, p) = 1$. Hence by Proposition 3

$$x^2 \equiv (a^2 - 4) \pmod{p^t}$$

cannot have more than two roots. Consequently $s_{p^t}^{-1}([a]) = \{(r, s), (s, r)\}$.

We now prove (ii). Let $(r, s)$ be an arbitrary element of $\mathcal{E}_{p^t}'''$ and let

$$r = d_0 + d_1 p + d_2 p^2 + \cdots + d_{t-1} p^{t-1}$$

be the expansion of $r$ in base $p$. There are only two possible choices for $d_0$, specifically, the two roots of $x^2 \equiv -1 \pmod{p}$, and for each of the other $d_i$’s there are $p$ possible choices: $0, 1, \ldots, p - 1$. So there are $2p^{t-1}$ possible $r$’s. Since $s$ is completely determined by the choice of $r$, we conclude that $\#\mathcal{E}_{p^t}''' = 2p^{t-1}$. \hfill $\square$

**Proposition 9.** If $p \equiv 1 \pmod{4}$ then

$$\#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{4(p + 1)} + \frac{3}{4}. \quad (11)$$

**Proof.** By Proposition 8

$$I''(x + x^{-1}, \mathbb{Z}_{p^t}) = \{kp : 0 \leq k \leq p^{t-1} - 1\}.$$
Consequently,
\[ I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = Q(I''((x + x^{-1})^2, \mathbb{Z}_{p^t})) = Q([kp : 0 \leq k \leq p^{t-1} - 1]) = \{j^2 \mod p^t : p \mid j\}. \]

Therefore,
\[ \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \#\{k^2 \mod p^t\} - \#\{k^2 \mod p^t : \gcd(k, p) = 1\}. \]

Combining Stangl’s formula (3) with the standard result that the number of quadratic residues modulo \( p^t \) is \( (p^t - p^{t-1})/2 \), we obtain
\[ \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{4(p + 1)} + \frac{3}{4}, \]
which proves Proposition 9.

We are now ready to prove formulas (7) and (8). We have
\[ \#I((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{\#I((x + x^{-1})^2, \mathbb{Z}_{p^t})}{2} + \frac{\#I''((x + x^{-1})^2, \mathbb{Z}_{p^t})}{2} = \frac{\#I((x + x^{-1})^2, \mathbb{Z}_{p^t})}{2} = \frac{\#I''((x + x^{-1})^2, \mathbb{Z}_{p^t})}{2} + \frac{\#I''((x + x^{-1})^2, \mathbb{Z}_{p^t})}{2}. \]

Formula (5) is
\[ \#I((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{(p - 3)p^{t-1}}{2} + \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{2(p + 1)} + \frac{3}{2}. \]

If \( p \equiv 3 \mod 4 \), then \( \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = 0 \) by (10). If \( p \equiv 1 \mod 4 \), then
\[ \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = p^{t-1} \]
and
\[ \#I''((x + x^{-1})^2, \mathbb{Z}_{p^t}) = \frac{2p^{t-1} + (-1)^{t-1}(p - 1)}{4(p + 1)} + \frac{3}{4}, \]
by (10) and (11). We complete the proof with simple algebraic computations.

\textbf{Proof of Theorem 6, case } p = 2. \textit{Interestingly this was the most difficult and time consuming part. It was only through experimenting with Maple that we discovered the map } f \textit{ (defined below) that allowed us to prove the formula for powers of 2.}

\textbf{Proposition 10.} \textit{Let } t \geq 3. \textit{The image of the map}
\[ f : I(x^2, \mathbb{Z}_{2^t}) \to \{0, 1, \ldots, 2^{t+6} - 1\} \]
given by

\[ f(k^2) = (64k^2 + 4) \mod 2^{t+6} \]

is \( I((x + x^{-1})^2, \mathbb{Z}_{2^{t+6}}) \). Since \( f \) is injective we conclude that

\[ \#I((x + x^{-1})^2, \mathbb{Z}_{2^{t+6}}) = \#I(x^2, \mathbb{Z}_{2^t}). \]  \hspace{1cm} (12)

\textbf{Proof.} First we show that \( I((x + x^{-1})^2, \mathbb{Z}_{2^{t+6}}) \subseteq \text{Image}(f) \). Let \((x, y) \in \mathcal{H}_{2^{t+6}} \). We can write

\[ x = 8x_1 + a \quad \text{and} \quad y = 8y_1 + a, \]

with \(0 \leq x_1, y_1 < 2^{t+3}\) and \(a = 1, 3, 5\) or 7. (We are using the fact that each element in \( \mathbb{Z}_8^* \) is its own inverse.) The following calculation now shows that \((x + y)^2 \mod 2^{t+6} \in \text{Image}(f) \).

\[
(x + y)^2 = (8x_1 + 8y_1 + 2a)^2 \\
= 64x_1^2 - 128x_1y_1 + 64y_1^2 + 256x_1y_1 + 32x_1a + 32y_1a + 4a^2 \\
= 64(x_1 - y_1)^2 + 4(64x_1y_1 + 8x_1a + 8y_1a + a^2) \\
= 64(x_1 - y_1)^2 + 4xy \\
\equiv (64(x_1 - y_1)^2 + 4) \pmod{2^{t+6}}.
\]

To show the reverse inclusion, let \( k^2 \in I(x^2, \mathbb{Z}_{2^t}) \). By Proposition 3 the congruence

\[ x^2 \equiv 16k^2 + 1 \pmod{2^n} \]

has a solution for all values of \( n \). Let \( l \) be any integer such that \( l^2 = 16k^2 + 1 \pmod{2^{t+6}} \), and let

\[ x = (l - 4k) \mod 2^{t+6}, \quad y = (l + 4k) \mod 2^{t+6}. \]

The immediate observations that \((x, y) \in \mathcal{H}_{2^{t+6}} \) and

\[ (x + y)^2 \equiv 4l^2 \equiv 64k^2 + 4 \pmod{2^{t+6}} \]

complete the proof. \hspace{1cm} \Box

Now the formula (6) for \( \#I((x + x^{-1})^2, \mathbb{Z}_{2^t}) \) is obtained by combining (2), (12) and (16). This concludes the proof of Theorem 6. \hspace{1cm} \Box

We can also derive the formula for \( \#I(x^2 + x^{-2}, \mathbb{Z}_p) \) as a special case of an old formula for pairs of quadratic residues.

\textbf{Theorem 11} [Berndt et al. 1998, Theorem 6.3.1, page 197]. \textit{Let} \( p \) \textit{be an odd prime and let} \( c \) \textit{be an integer relatively prime to} \( p \). \textit{Let} \( \epsilon_1 = \pm 1 \) \textit{and} \( \epsilon_2 = \pm 1 \). \textit{Then}

\[
\#\left\{ n : 0 \leq n < p, \ \left( \frac{n}{p} \right) = \epsilon_1, \ \left( \frac{n+c}{p} \right) = \epsilon_2 \right\} \\
= \frac{1}{4} \left\{ p - 2\epsilon_1 \left( \frac{-c}{p} \right) - \epsilon_2 \left( \frac{c}{p} \right) - \epsilon_1\epsilon_2 \right\}. \]  \hspace{1cm} (13)
The special case of this formula with \( \epsilon_1 = \epsilon_2 = c = 1 \) was first published by Aladov in 1896. The connection between (13) and \( \#I(x^2 + x^{-2}, \mathbb{Z}_p) \) is as follows.

**Theorem 12.** Let \( a \in \mathbb{Z} \) with \( \gcd(a^2 - 4, n) = 1 \). Then \( \mathcal{C}_{a,n} \cap \mathcal{H}_n \neq \emptyset \) if and only if for every prime, \( p \), in the canonical factorization of \( n \) we have

\[
\left( \frac{a-2}{p} \right) = \left( \frac{a+2}{p} \right) = 1. \tag{14}
\]

Consequently,

\[
\#I(x^2 + x^{-2}, \mathbb{Z}_p) = \# \left\{ a : 0 \leq a < p, \left( \frac{a-2}{p} \right) = \left( \frac{a+2}{p} \right) = 1 \right\} + 1.
\]

**Proof.** For the “only if” part, let \( (r, s) \in \mathcal{C}_{a,n} \cap \mathcal{H}_n \) and let \( p \) be an arbitrary prime divisor of \( n \). So, \( (r - s)^2 \equiv a - 2 \pmod{p} \) and \( (r + s)^2 \equiv a + 2 \pmod{p} \), which leads immediately to (14).

To prove the converse, let \( n = \prod_{i=1}^{t} p_i^{e_i} \) be the canonical factorization of \( n \). By Proposition 3, we can lift the square roots (modulo \( p \)) of \( (a - 2) \) and \( (a + 2) \) to the \( e_i \)th power, \( p_i^{e_i} \). Let \( s_i = \sqrt{a - 2} \pmod{p_i^{e_i}} \), and \( r_i = \sqrt{a + 2} \pmod{p_i^{e_i}} \). Then

\[
2^{-1} \cdot (r_i + s_i, r_i - s_i) \in \mathcal{C}_{p_i^{e_i}} \cap \mathcal{H}_{p_i^{e_i}},
\]

where \( 2^{-1} \) denotes the inverse of 2 modulo \( p_i^{e_i} \). Now invoke the Chinese remainder theorem to determine integers \( r \) and \( s \) such that

\[
r \equiv r_i \pmod{p_i^{e_i}} \quad \text{and} \quad s \equiv s_i \pmod{p_i^{e_i}} \quad \text{for} \quad i = 1, \ldots, t.
\]

Clearly \( (r, s) \in \mathcal{C}_n \cap \mathcal{H}_n \). \( \square \)

### 3. The formulas for \( \#I(x^2 + y^2, \mathbb{Z}_p^2) \)

We now determine the formulas for \( \#I(x^2 + y^2, \mathbb{Z}_p^2) \) to contrast them to \( \#I(x^2 + x^{-2}, \mathbb{Z}_p^2) \).

**Theorem 13.** Let \( p \) be an odd prime. Then

\[
\#I(x^2 + y^2, \mathbb{Z}_p^2) = \begin{cases} 
  p' & \text{if } p \equiv 1 \pmod{4}, \\
  p & \text{if } p \equiv 3 \pmod{4} \text{ and } t = 1, \\
  p' - \sum_{j=0}^{[t/2]-1} \varphi(p^{t-1-2j}) & \text{if } p \equiv 3 \pmod{4} \text{ and } t > 1,
\end{cases} \tag{15}
\]

When \( p = 2 \) we have

\[
\#I(x^2 + y^2, \mathbb{Z}_2^2) = \varphi(2') + 1. \tag{16}
\]

As is typically the case, the formula for powers of two, \( 2' \), will require a separate argument. We first prove (15).
Proof of formula (15). We treat each case separately.

- \( p \equiv 1 \pmod{4} \). Let \( a \in \{0, 1, \ldots, p' - 1\} \). The simultaneous congruences
  \[
  x - y \equiv 1 \pmod{p'} \quad \text{and} \quad x + y \equiv a \pmod{p'}
  \]
  have the solutions
  \[
  x = ((a + 1) \cdot (2^{-1} \pmod{p'})) \pmod{p'}, \\
  y = ((a - 1) \cdot (2^{-1} \pmod{p'})) \pmod{p'}.
  \]
  It immediately follows that \( x^2 + (i_{p'} y)^2 \equiv a \pmod{p'} \), where
  \[
i_{p'}^2 \equiv -1 \pmod{p'}.
  \]

- \( p \equiv 3 \pmod{4}, t = 1 \). Let \( a \in \{0, 1, \ldots, p - 1\} \). By (3), \( \#I(x^2, \mathbb{Z}_p) = (p + 1)/2 \) and therefore \( \#(a - I(x^2, \mathbb{Z}_p)) = (p + 1)/2 \). Since
  \[
  \#I(x^2, \mathbb{Z}_p) + \#(a - I(x^2, \mathbb{Z}_p)) = p + 1,
  \]
  it follows that there is an element \( (a - x_1^2) \in (a - I(x^2, \mathbb{Z}_p)) \) and an element \( x_2^2 \in I(x^2, \mathbb{Z}_p) \) such that \( (a - x_1^2) \equiv x_2^2 \pmod{p} \).

- \( p \equiv 3 \pmod{4}, t \geq 2 \). The key is to prove that an element \( a \in \{0, 1, 2, \ldots, p' - 1\} \)
  satisfies \( a \equiv x^2 + y^2 \pmod{p'} \) if and only if \( a = p^k b \), with \( \gcd(p, b) = 1 \) and \( k \) even.

  \( \Leftarrow \) Since \( p^k \) is a square in \( \mathbb{Z} \), it is sufficient to prove this for integers \( a \) that are relatively prime to \( p \). We argue by induction. The previous case shows that the result holds for \( t = 1 \). Let us assume it is true for \( t \). So
  \[
a \equiv (x^2 + y^2) \pmod{p'}.
  \]

  If \( p'^{t+1} \mid (a - x^2 - y^2) \), there is nothing to prove. So let us assume that \( (a - x^2 - y^2) = p'^t l \), with \( \gcd(l, p) = 1 \). Since \( \gcd(a, p) = 1 \) either \( \gcd(x, p) = 1 \) or \( \gcd(y, p) = 1 \).

  Without loss of generality we assume the former. We now define \( s \in \mathbb{Z} \), with\n  \[
  1 \leq s < p,
  \]
  to be the solution of the congruence
  \[
  2xs \equiv l \pmod{p}.
  \]

  An immediate calculation shows that
  \[
a \equiv (x + sp^t)^2 + y^2 \pmod{p'^{t+1}}.
  \]

  \( \Rightarrow \) We argue by contradiction. Suppose \( a = p^k b \), with \( a < p' \), \( \gcd(b, p) = 1 \), and \( k \) odd, be the sum of two squares modulo \( p' \). So there are integers \( x = p^{e_1} x_1 \), \( y = p^{e_2} y_1 \), with \( \gcd(x_1 y_1, p) = 1 \), such that
  \[
p^k b \equiv (x^2 + y^2) \pmod{p'},
  \]
that is,
\[
p^k b \equiv (p^{2e_1} x_1^2 + p^{2e_2} y_1^2) \pmod{p'}.
\]

Since \( b \not\equiv 0 \pmod{p} \) and \( k \) is odd we have \( \min\{2e_1, 2e_2\} < k \). Without loss of generality we may assume that \( e_1 \leq e_2 \). We can reduce the congruence
\[
p^k b \equiv (x^2 + y^2) \pmod{p'}
\]
to \( p^{k-2e_1} b \equiv x_1^2 + p^{2(e_2-e_1)} y_1^2 \pmod{p^{k-2e_1}} \), which in turns reduces to
\[
x_1^2 + p^{2(e_2-e_1)} y_1^2 \equiv 0 \pmod{p}.
\]

Since \( x_1 \not\equiv 0 \pmod{p} \) we must have \( p^{2(e_2-e_1)} y_1^2 \not\equiv 0 \pmod{p} \), that is \( e_2 = e_1 \), and consequently \( (x_1^2 + y_1^2) \equiv 0 \pmod{p} \), with \( \gcd(x_1 y_1, p) = 1 \). But this gives us the contradiction that \( x^2 \equiv -1 \pmod{p} \) is solvable for a prime \( p \) with \( p \equiv 3 \pmod{4} \). This concludes the proof of (15). \( \square \)

**Proposition 14.** Let \( t \geq 3 \) and \( 0 < m < 2^t \). Then \( m \in I(x^2 + y^2, \mathbb{Z}_{2^t}) \) if and only if \( m = 2^j \cdot a \), with \( j < t \) and \( a \equiv 1 \pmod{4} \).

**Proof.** \((\Leftarrow)\) Let \( a \equiv 1 \pmod{4} \). Since \( 2^j \) is a sum of squares (in \( \mathbb{Z} \)) we only need to show that \( a \) is a sum of two squares modulo \( 2^t \). If \( a \equiv 1 \pmod{8} \) then \( a \) is a square modulo \( 2^t \) by Proposition 3. If \( a \equiv 5 \pmod{8} \), then \( a - 4 \equiv 1 \pmod{8} \) and is therefore a square modulo \( 2^t \). Consequently \( a \) is a sum of two squares modulo \( 2^t \).

\((\Rightarrow)\) We now assume that \( a \equiv 3 \pmod{4} \) and argue by contradiction. Let
\[
x^2 + y^2 \equiv m \pmod{2^t}.
\]

We look at four possible cases.

1. \( j = 0 \): We obtain the contradiction that
\[
x^2 + y^2 \equiv 3 \pmod{4}.
\]

2. \( j = 1 \): We obtain the contradiction that
\[
x^2 + y^2 \equiv 6 \pmod{8}.
\]

3. \( j \geq 2, j \leq (t - 2) \): We have \( x = 2^{e_1} \cdot x_1 \) and \( y = 2^{e_2} \cdot y_1 \), with \( x_1, y_1 \) odd and \( j = \min\{2e_1, 2e_2\} \). Without loss of generality we may assume that \( e_1 \leq e_2 \). We now obtain the contradiction
\[
x_1^2 + 4^{e_2-e_1} y_1^2 \equiv a \equiv 3 \pmod{4}.
\]

4. \( j = t - 1 \): Then
\[
m = 2^{t-1} \cdot a \geq 2^{t-1} \cdot 3 > 2^t,
\]
contradicting the fact that the elements of \( I(x^2 + y^2, \mathbb{Z}_{2^t}) \) are less than \( 2^t \). \( \square \)
Proof of formula (16). Let $M_t$ denote the set

$$M_t = \{ m : 0 < m < 2^t, \ m = 2^j \cdot a, \ j < t, \ a \equiv 1 \pmod{4} \}.$$ 

In our previous proposition we proved that

$$I(x^2 + y^2, \mathbb{Z}_{2^t}^2) \setminus \{0\} = M_t.$$ 

We now make the following two observations about elements in $M_t$:

(i) If $m \in M_t$, then $(m + 2^t) \in M_{t+1}$ provided $m \neq 2^t - 1$.

(ii) If $m \in M_{t+1}$ with $m > 2^t$, then $(m - 2^t) \in M_t$.

From these two observations we conclude that

$$M_{t+1} \setminus \{2^t\} = M_t \cup \{m + 2^t : m \in M_t \setminus \{2^t - 1\}\},$$

and consequently \#$M_{t+1} = 2 \cdot \#M_t$. An inductive argument now proves that \#$M_t = \varphi(2^t)$ and therefore \#$I(x^2 + y^2, \mathbb{Z}_{2^t}^2) = \varphi(2^t) + 1$. \qed

References


Received: 2009-02-08 Accepted: 2010-06-21

hanrahans@stu.easternct.edu  Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, CT 06226, United States

khanm@easternct.edu  Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, CT 06226, United States
Recursive sequences and polynomial congruences
J. LARRY LEHMAN AND CHRISTOPHER TRIOLA

129

The Gram determinant for plane curves
JÓZEF H. PRZYTYCKI AND XIAOQI ZHU

149

The cardinality of the value sets modulo n of $x^2 + x^{-2}$ and $x^2 + y^2$
SARA HANRAHAN AND MIZAN KHAN

171

Minimal $k$-rankings for prism graphs
JUAN ORTIZ, ANDREW ZEMKE, HALA KING, DARREN NARAYAN AND MIRKO HORNÁK

183

An unresolved analogue of the Littlewood Conjecture
CLARICE FEROLITO

191

Mapping the discrete logarithm
DANIEL CLOUTIER AND JOSHUA HOLDEN

197

Linear dependency for the difference in exponential regression
INDIKA SÁTHISH AND DIAWARA NOROU

215

The probability of relatively prime polynomials in $\mathbb{Z}_p[x]$
THOMAS R. HAGEDORN AND JEFFREY HATLEY

223

G-planar abelian groups
ANDREA DÉWITT, JILLIAN HAMILTON, ALYS RODRIGUEZ AND JENNIFER DANIEL

233