MODULAR HYPERBOLAS AND THE COEFFICIENTS OF 
\((X^{-1} + 6 + X)^K\)

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

Received: 11/5/09, Accepted: 4/2/10, Published: 3/9/11

Abstract
Let \(F_q^*\) be the multiplicative group of a finite field, \(F_q\), of cardinality \(q\), with \(q\) odd; and let \(P(F_q^*)\) denote its power set. We define the arithmetical function \(D : P(F_q^*) \rightarrow \mathbb{Z}\) via

\[
D(S) = \#I(x + x^{-1}, S) - \#I(x - x^{-1}, S),
\]

where for \(S \subseteq F_q^*\),

\[
I(x \pm x^{-1}, S) = \{ x \pm x^{-1} : x \in S \}.
\]

Furthermore, let

\[
t_q = \begin{cases} 
    k - 1, & \text{if } q = 4k + 1 \\
    k, & \text{if } q = 4k + 3,
\end{cases}
\]

and let \(F(k, l)\) be the coefficient of \(x^l\) in \((x^{-1} + 6 + x)^k\). Then

\[
\#D^{-1}(\{l\}) = \begin{cases} 
    2^{q}(3F(t_q, l - 1) + 10F(t_q, l) + 3F(t_q, l + 1)), & q \equiv 1 \pmod{4} \\
    2^{q}(F(t_q, l - 1) + 3F(t_q, l)), & q \equiv 3 \pmod{4}.
\end{cases}
\]

1. Introduction
Let \(A\) be a nonempty subset of \(\mathbb{Z}\). We define the sumset \(A + A\) and difference set \(A - A\) via

\[
A + A = \{a + b : a, b \in A\} \text{ and } A - A = \{a - b : a, b \in A\}.
\]

Given that \(x + y = y + x\), but for \(x \neq y, x - y \neq y - x\), it seems intuitively obvious that for an arbitrary finite subset \(A\) of \(\mathbb{Z}\) the cardinality \(#(A - A)\) should be approximately twice the cardinality \(#(A + A)\). However, there are some recent
papers [3, 4] where the authors show quite ingeniously how to construct sets with more sums than differences.

In this paper we look at an easier problem. Let $R$ be a finite ring with the group of multiplicative units $R^*$. (The fundamental example is of course $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$.) Let $P(R^*)$ be the power set of $R^*$. For each $S \in P(R^*)$, in place of the sets $S + S$ and $S - S$, we define the sets $I(x + x^{-1}, S)$ and $I(x - x^{-1}, S)$ via

$$I(x \pm x^{-1}, S) = \{ x \pm x^{-1} : x \in S \}.$$  

We would like to compare the cardinalities of $I(x + x^{-1}, S)$ and $I(x - x^{-1}, S)$, and so we define the arithmetical function

$$D : P(R^*) \to \mathbb{Z} \text{ via } D(S) = \# I(x + x^{-1}, S) - \# I(x - x^{-1}, S).$$

In this paper we explore some of the properties of $D$ with $R$ being the finite field $\mathbb{F}_q$, and $q$ odd. The essence of our main result is as follows. Let $l \in D(P(\mathbb{F}_q^*))$, and let $d(q, l)$ be defined as

$$d(q, l) = \# D^{-1}(\{l\}).$$

Then, in nearly all cases, $d(q, -l) = d(q, l)$, that is, in almost all cases, the number of sets with $D$ value $l$ equals the number of sets with $D$ value $-l$. The solitary exception is when $q \equiv 3 \pmod{4}$ and $l = \max(D(P(\mathbb{F}_q^*)))$. In this case we have that

$$d(q, \max(D(P(\mathbb{F}_q^*)))) > 0 = d(q, -\max(D(P(\mathbb{F}_q^*))))).$$

Even though the results and proofs in this paper are completely algebraic, the motivation is geometric. Specifically it arises from studying the graphs of the modular hyperbolas $H_n$, where

$$H_n = \{(x, y) : xy \equiv 1 \pmod{n}, 1 \leq x, y \leq n - 1, n \in \mathbb{Z}^+\}.$$  

Visually a favorite example is $H_{555}$:

![Figure 1. The graph $H_{555}$](image)
The cardinalities
\[ \#\{x + y : (x, y) \in \mathcal{H}_n\} \] and \[ \#\{x - y : (x, y) \in \mathcal{H}_n\} \]
count the number of lines of slope −1 and +1 that intersect \( \mathcal{H}_n \) respectively. In [1] these two cardinalities are compared by first developing formulas for the cardinalities \( \#\{x + x^{-1} : x \in \mathbb{Z}_n^*\} \) and \( \#\{x - x^{-1} : x \in \mathbb{Z}_n^*\} \), and then applying these formulas to prove \( \lim \inf s_n = 0 \) and \( \lim \sup s_n = \infty \), where \( s_n \) is the sequence
\[ s_n = \frac{\#\{x + y : (x, y) \in \mathcal{H}_n\}}{\#\{x - y : (x, y) \in \mathcal{H}_n\}}. \]

The most interesting consequence of the formulas is that \( D(\mathbb{Z}_n^*) > 0 \) for at least 84% of \( n \in \mathbb{N}^+ \). (The initial belief of the authors of [1] that \( D(\mathbb{Z}_n^*) \) would be nonnegative for about 50 percent of the natural numbers and nonpositive for the remaining 50 percent was completely incorrect!) Furthermore it is conceivable that this 84% figure maybe as high as 100% since it is an open question whether or not the set \( \{ n : D(\mathbb{Z}_n^*) \leq 0 \} \) has positive density.

Shparlinski suggestion to extend the work to subsets of \( \mathbb{Z}_n^* \) led to the present paper. We restrict our moduli to primes as the combinatorics are quite straightforward. Let us elaborate. The starting point is to define a very simple equivalence relation on \( \mathbb{Z}_p^* \) such that if \( E_a \) and \( E_b \) are two distinct equivalence classes, then
\[ I(x + x^{-1}, E_a) \cap I(x + x^{-1}, E_b) = \emptyset, I(x - x^{-1}, E_a) \cap I(x - x^{-1}, E_b) = \emptyset. \] (2)

This is an immediate consequence of the result that a quadratic polynomial over a field has no more than 2 roots. We also get that with the exception of one (or two) cases, the cardinality of the equivalence classes is 4. We then proceed to a counting argument to obtain our main result. The reason our method does not extend to the composite case is that if we define the same equivalence relation on \( \mathbb{Z}_p^* \), then (2) need not hold. The results (and proofs) for \( S \subseteq \mathbb{Z}_p^* \) generalize to working with subsets over finite fields of odd characteristic and so we work in this slightly more general setting.

We first take care of the trivial case, that is, when the field has characteristic 2.

**Proposition 1.** If \( \mathbb{F} \) is a finite field of characteristic 2, then \( D(S) = 0 \) for any \( S \subseteq \mathbb{F}^* \).

**Proof.** For any \( x \in \mathbb{F}^* \), \( x + x^{-1} = x - x^{-1} \), and therefore \( D(S) = 0 \). \( \square \)

From hereupon our finite fields, \( \mathbb{F}_q \) will have odd characteristic, with \( q \) denoting the cardinality of the field. We now state our main result. We remind the reader that \( d(q, l) = \#D^{-1}(\{l\}) \).
Theorem 2. Let
\[ t_q = \begin{cases} 
  k - 1, & \text{if } q = 4k + 1 \\
  k, & \text{if } q = 4k + 3,
\end{cases} \] (3)
and \( d(k, l) \) as in (1). Then
\[ F(k, l) = \text{coefficient of } x^i \text{ in } (x^{-1} + 6 + x)^k \] (4)

In conclusion, the author views this work as an ongoing study of modular hyperbolas and we refer the reader to the survey article [5] for many other interesting questions on this topic.

2. Preliminaries

We start by defining an equivalence relation on \( \mathbb{F}_q^* \) via
\[ x \sim y \iff y \in E_x := \{ x, -x, x^{-1}, -x^{-1} \}. \]

Lemma 3. The equivalence classes \( E_x \) have the following properties:
1. \( E_1 = \{ 1, -1 \} \) and \( \#I(x + x^{-1}, E_1) = 2, \#I(x - x^{-1}, E_1) = 1. \)
2. If \( q \equiv 1 \pmod{4} \) then there is an element \( i_q \in \mathbb{F}_q^* \) such that \( i_q^2 = -1 \). In this case
   \[ E_{i_q} = \{ i_q, -i_q \} \text{ and } \#I(x + x^{-1}, E_{i_q}) = 1, \#I(x - x^{-1}, E_{i_q}) = 2. \]
3. In all other cases, that is, \( x \in \mathbb{F}^*, x^2 \neq \pm 1, \)
   \[ E_x = \{ x, -x, x^{-1}, -x^{-1} \} \text{ and } \#I(x + x^{-1}, E_x) = \#I(x - x^{-1}, E_x) = 2. \]
4. If \( E_a \neq E_b, \) then
   \[ I(x + x^{-1}, E_a) \cap I(x + x^{-1}, E_b) = \emptyset \text{ and } I(x - x^{-1}, E_a) \cap I(x - x^{-1}, E_b) = \emptyset. \]

The proof of each statement in Lemma 3 is routine. From the lemma we immediately conclude the following.

Corollary 4. Let \( \lambda \) range over an index for the equivalence classes of \( \sim \). Then, any set \( S \subseteq \mathbb{F}_q^* \) can be written as the disjoint union
\[ S = \bigcup_{\lambda} (S \cap E_\lambda), \] (6)
and consequently
\[ D(S) = \sum_{\lambda} D(S \cap E_\lambda). \] (7)
Our next lemma shows that \( D(S \cap E_\lambda) = 0 \) most of the time.

**Lemma 5.**

1. \( D(S \cap E_1) = 1 \iff E_1 \subseteq S. \) Otherwise \( D(S \cap E_1) = 0. \)
2. \( D(S \cap E_{1q}) = -1 \iff E_{1q} \subseteq S. \) Otherwise \( D(S \cap E_{1q}) = 0. \)
3. Let \( x \in \mathbb{F}_q^* \) with \( x^2 \neq \pm 1. \) Then
   \[
   D(S \cap E_x) = 1 \iff S \cap E_x = \{x, -x^{-1}\} \text{ or } S \cap E_x = \{-x, x^{-1}\}
   \]
   and
   \[
   D(S \cap E_x) = -1 \iff S \cap E_x = \{x, x^{-1}\} \text{ or } S \cap E_x = \{-x, -x^{-1}\}
   \]
   Otherwise \( D(S \cap E_x) = 0. \)

We are now in a position to determine the range of the map \( D. \)

**Proposition 6.** Let \( q = 4k + a \) where \( a = 1 \) or \( 3 \) depending on whether \( q \) is congruent to \( 1 \) or \( 3 \) modulo \( 4. \) We have the following.

1. If \( q \equiv 1 \mod 4, \) then
   \[
   D\left( \mathbf{P}\left( \mathbb{F}_q^* \right) \right) = \{-k, -k + 1, \ldots, k - 1, k\}.
   \]
2. If \( q \equiv 3 \mod 4, \) then
   \[
   D\left( \mathbf{P}\left( \mathbb{F}_q^* \right) \right) = \{-k, -k + 1, \ldots, k, k + 1\}.
   \]

**Proof.** (Sketch) A simple computation shows that the number of equivalence classes for \( \sim \) is \( k + 1. \) We discuss the specific case of how to show that \( D^{-1}(\{k - 1\}) \neq \emptyset \) when \( q \equiv 1 \mod 4. \) Let

\[
E_1, E_{1q}, E_{x_3}, E_{kx}, \ldots, E_{x_k}, E_{x_{k+1}}
\]

denote the distinct equivalence classes of \( \sim, \) and let \( S \) be the set

\[
S = \{1, -1, x_3, -x_3^{-1}, \ldots, x_k, -x_k^{-1}\}.
\]

Combining (7) with Lemma 5, we conclude that \( D(S) = k - 1. \) All other cases are handled similarly.

\( \square \)

3. **Proof of Theorem 2**

**Proposition 7.** Let

\[
S = \{S : S \subseteq \mathbb{F}_q^*; \text{ and for any } x \in S, x^2 \neq \pm 1\},
\]

\( t_q \) as in (3), and \( F(t_q, l) \) as in (4). Then

\[
\# \{S \in S : D(S) = l\} = 2^{t_q} \cdot F(t_q, l).
\]
Proof. We count the cardinality of \( \{ S : D(S) = l, S \in \mathcal{S} \} \) by utilizing the decomposition described in (6), where in addition \( \lambda^2 \neq \pm 1 \) for any \( E_\lambda \). Thus each of the \( E_\lambda \)'s has cardinality 4 and \( D(S \cap E_\lambda) = -1,0 \) or 1. Consequently

\[
l = D(S) = \sum D(S \cap E_\lambda) = m_1 \cdot 1 + m_2 \cdot (-1) + (t_q - m_1 - m_2) \cdot 0,
\]

(10)

that is, there are \( m_1 \) sets \( E_\lambda \) with \( D(S \cap E_\lambda) = 1; m_2 \) sets \( E_\lambda \) with \( D(S \cap E_\lambda) = -1; \) and for the remaining \( E_\lambda \)'s, \( D(S \cap E_\lambda) = 0. \)

Let us fix the values \( m_1 \) and \( m_2 \). We have \( \binom{t_q}{m_1} \cdot 2^{m_1} \) many ways to choose the \( E_\lambda \)'s to obtain the \( m_1 \) term in (10); we have \( \binom{t_q - m_1}{m_2} \cdot 2^{m_2} \) many ways to choose the \( E_\lambda \)'s to obtain the \( m_2 \) term in (10); and we have \( 12^{t_q - m_1 - m_2} \) many ways to choose the \( E_\lambda \)'s to obtain the \( (t_q - m_1 - m_2) \) term in (10). It now follows that

\[
\# \{ S : D(S) = l, S \in \mathcal{S} \}
= \sum_{m_1 - m_2 = l} \frac{t_q!}{m_1!m_2!(t_q - m_1 - m_2)!} 2^{m_1} 2^{m_2} 12^{t_q - m_1 - m_2}
= 2^{t_q} \sum_{m_1 - m_2 = l} \frac{t_q!}{m_1!m_2!(t_q - m_1 - m_2)!} 6^{t_q - m_1 - m_2}
= 2^{t_q} F(t_q, l),
\]

which is what we wanted to prove. \( \square \)

Proof of Theorem 2. Let \( q \equiv 1 \pmod{4} \) and denote by \( i_q \) one of the two square roots of \(-1\) in \( \mathbb{F}_q^* \). Let \( \mathcal{S} \) be the set defined in (8) and let

\[
\mathbf{A} = \{ \{1, -1\}, \{1, -1, i_q\}, \{1, -1, -i_q\} \},
\]

\[
\mathbf{C} = \{ \{i_q, -i_q\}, \{1, i_q, -i_q\}, \{-1, i_q, -i_q\} \}
\]

and

\[
\mathbf{B} = \mathbf{P}(\{1, -1, i_q, -i_q\}) - (\mathbf{A} \cup \mathbf{C}).
\]

We note that \( D(A) = 1 \) if \( A \in \mathbf{A}, D(B) = 0 \) if \( B \in \mathbf{B} \) and \( D(C) = -1 \) if \( C \in \mathbf{C}. \)

Using Corollary 4 we infer that if \( S' \in \mathcal{S} \) and \( S'' \in \mathbf{A} \cup \mathbf{B} \cup \mathbf{C} \), then

\[
D(S' \cup S'') = D(S') + D(S'').
\]

Let \( S \) be an arbitrary element of the set \( D^{-1}(\{l\}) \). Then \( S \) can be decomposed in exactly one of the following three ways.

1. \( S = S' \cup A \) with \( S' \in \mathcal{S}, D(S') = l - 1, \) and \( A \in \mathbf{A}. \)
2. \( S = S' \cup B \) with \( S' \in \mathcal{S}, D(S') = l, \) and \( B \in \mathbf{B}. \)
3. \( S = S' \cup C \) with \( S' \in \mathcal{S}, D(S') = l + 1, \) and \( C \in \mathbf{C}. \)
Combining (9) with the cardinalities of \( A, B \) and \( C \) we get that
\[
\# \{ S' \cup A : D(S') = l - 1, S' \in S, A \in A \} = 2^{t_q} \cdot 3 \cdot F(t_q, l - 1),
\]
\[
\# \{ S' \cup B : D(S') = l, S' \in S, B \in B \} = 2^{t_q} \cdot 10 \cdot F(t_q, l),
\]
and
\[
\# \{ S' \cup C : D(S') = l + 1, S' \in S, C \in C \} = 2^{t_q} \cdot 3 \cdot F(t_q, l + 1).
\]
Consequently, \( d(q, l) = 2^{t_q}(3F(t_q, l - 1) + 10F(t_q, l) + 3F(t_q, l + 1). \)

We obtain the formula for the case \( q \equiv 3 \pmod{4} \) in a similar manner. \( \square \)

One of our goals was to discover a closed form for \( d(q, l) \). However, from the excellent offices of Ekhad and Zeilberger [2], we learnt that the multinomial coefficient \( F(n, a) \) does NOT have a closed form but it does satisfy the recurrences
\[
32(n + 2)(n + 1)F(n, a) - 6(n + 2)(2n + 3)F(n + 1, a) \\
- (n + a + 2)(-n + a - 2)F(n + 2, a) = 0
\]
(11)
and
\[
(n - a)F(n, a) - 6(a + 1)F(n, a + 1) - (n + a + 2)F(n, a + 2) = 0.
\]
(12)

**Acknowledgements.** I would like to thank my colleague P. Zhao for his helpful comments and careful reading of this article.

**References**


