Shortest Distance in Modular Hyperbola and Least Quadratic Nonresidue

Tsz Ho Chan

Abstract

In this paper, we study how small a box contains at least two points from a modular hyperbola \( xy \equiv c \pmod{p} \). There are two such points in a square of side length \( p^{1/4+\varepsilon} \). Furthermore, it turns out that either there are two such points in a square of side length \( p^{1/6+\varepsilon} \) or the least quadratic nonresidue is less than \( p^{1/(6\sqrt{e})+\varepsilon} \).

1 Introduction and Main results

Let \( p > 2 \) be a prime and \((c, p) = 1\). We consider the modular hyperbola

\[ H_c := \{(x, y) : xy \equiv c \pmod{p}\} \]

We are interested in the shortest distance between two points in \( H_c \). Rather than distances, we consider how small a box

\[ B(X, Y; H) := \{(x, y) : X + 1 \leq x \leq X + H \pmod{p}, Y + 1 \leq y \leq Y + H \pmod{p}\} \]

contains two points in \( H_c \) where \( X \) and \( Y \) run over \( 0, 1, \ldots, p - 1 \).

By Hölder’s inequality and Weil’s bound on character sum, we have

**Theorem 1** For all \((c, p) = 1\), there exist some \( 0 \leq X, Y \leq p - 1 \) so that

\[ |H_c \cap B(X, Y; H)| \geq 2 \]

if \( H \gg \varepsilon p^{1/4+\varepsilon} \).

Now let us switch to the subject of the least quadratic nonresidue modulo \( p \). Many people have been interested in the upper bound for \( n_p \). By Polya-Vinogradov bound on character sums, we have

\[ n_p \ll p^{1/2} \log p. \]

Vinogradov applied a trick and got

\[ n_p \ll_{\varepsilon} p^{1/(2\sqrt{e})+\varepsilon}. \]

Burgess proved a new bound on short character sum which together with Vinogradov’s trick yielded

\[ n_p \ll_{\varepsilon} p^{1/(4\sqrt{e})+\varepsilon}. \]

Recall a recent result of Heath-Brown and Shao on mean-value estimates of character sums:
Theorem 2 Given \( H \leq p \), a positive integer and any \( \epsilon > 0 \). Suppose that \( 0 \leq N_1 < N_2 < \ldots < N_J < p \) are integers satisfying \( N_{j+1} - N_j \geq H \) for \( 1 \leq j < J \). Then

\[
\sum_{j=1}^{J} \max_{\substack{h \leq H}} |S(N_j; h)|^{2r} \ll_{\epsilon, r} H^{2r-2} p^{1/2+1/(2r)+\epsilon}
\]

where

\[
S(N; H) := \sum_{N < n \leq N+H} \chi(n).
\]

and \( \chi \) is any non-principal character modulo \( p \).

Applying the above theorem, we can show that

Theorem 3 For any \( \epsilon > 0 \), we have either

\[
n_p \ll_{\epsilon} p^{1/(6\sqrt{\pi})+\epsilon}
\]

or, for any \( (c, p) = 1 \) and \( H \gg_{\epsilon} p^{1/6+\epsilon} \),

\[
|H_c \cap B(X, Y; H)| \geq 2
\]

for some \( 0 \leq X, Y \leq p - 1 \).

It is probably the case that the above two statements are true simultaneously. The paper is organized as follows. In section 2, we give a basic argument transforming the existence of two close points in the modular hyperbola to a certain equality in Legendre symbol. Then we prove Theorem 1 in section 3 and Theorem 3 in section 4.

Some Notations Throughout the paper, \( p \) stands for a prime. The symbol \( |S| \) denotes the number of elements in the set \( S \). We also use the Legendre symbol \( \left( \frac{a}{p} \right) \). The notation \( f(x) = o(g(x)) \) means that the ratio \( f(x)/g(x) \) is going to zero as \( x, p \to \infty \). The notations \( f(x) \ll g(x) \), \( g(x) \gg f(x) \) and \( f(x) = O(g(x)) \) are equivalent to \( |f(x)| \leq Cg(x) \) for some constant \( C > 0 \). Finally, \( f(x) \ll_{\lambda_1, \ldots, \lambda_k} g(x), g(x) \gg_{\lambda_1, \ldots, \lambda_k} f(x) \) and \( f(x) = O_{\lambda_1, \ldots, \lambda_k}(g(x)) \) mean that the implicit constant \( C \) may depend on \( \lambda_1, \ldots, \lambda_k \).

2 The Basic Argument

For \( (c, p) = 1 \), suppose \( |H_c \cap B(X, Y; H)| \geq 2 \) for some \( 0 \leq X, Y \leq p - 1 \). This means that

\[
xy \equiv c \pmod{p}, \text{ and } (x+a)(y+b) \equiv c \pmod{p}
\]

for some \( 1 \leq x, y \leq p - 1 \) and \( 1 \leq a, b \leq H \). After some algebra, one can show that (1) is equivalent to

\[
bx + ac\pi + ab \equiv 0 \pmod{p}
\]

where \( \pi \) stands for the multiplicative inverse of \( x \) modulo \( p \) (i.e. \( x\pi \equiv 1 \pmod{p} \)). This, in turn, is equivalent to

\[
(2bx + ab)^2 \equiv (ab)^2 - 4abc \pmod{p}.
\]

Therefore \( |H_c \cap B(X, Y; H)| \geq 2 \) if and only if

\[
\left( \frac{ab}{p} \right) = \left( \frac{ab - 4c}{p} \right) = 1
\]

for some \( 1 \leq a, b \leq H \). We are going to restrict our attention to even \( a = 2a' \) s and \( b = 2b' \) s. So we want

\[
\left( \frac{a'b'}{p} \right) = 1 \text{ for some } 1 \leq a', b' \leq H/2.
\]
3 Proof of Theorem 1

Throughout this section, we assume that \( H \gg p^{1/4+\epsilon} \). We want to show that

\[
\sum_{a' \leq H/2} \sum_{b' \leq H/2} \left( \frac{a'b'}{p} \right) \left( \frac{a'b' - c}{p} \right) = o(H^2).
\]

Then either we have two pairs with \( \left( \frac{a'_1 b'_1 - c}{p} \right) = 0 = \left( \frac{a'_2 b'_2 - c}{p} \right) \) which gives Theorem 1 automatically; or at most one such pair equal to 0 which would imply that \( \left( \frac{a'_1 b'_1 - c}{p} \right) = 1 \) and \( \left( \frac{a'_2 b'_2 - c}{p} \right) = -1 \) for some \( 1 \leq a'_1, b'_1, a'_2, b'_2 \leq H/2 \). However, we are going to restrict \( a' \) to a special form, namely \( a' = uv \) with \( 1 \leq u \leq U, 1 \leq v \leq V \) and \( UV = H/2 \). So let us consider

\[
S := \sum_{u \leq U} \sum_{v \leq V} \sum_{b' \leq H/2} \left( \frac{uvb'}{p} \right) \left( \frac{uvb' - c}{p} \right).
\]

Then

\[
S \leq \sum_{u \leq U} \sum_{v \leq V} \sum_{b' \leq H} \left| \sum_{u \leq U} \left( \frac{uvb' - c}{p} \right) \right| \leq \epsilon \sum_{n \leq VH} \sum_{u \leq U} \left| \sum_{u \leq U} \left( \frac{un - c}{p} \right) \right|
\]

as the number of divisors of \( n \) is \( O_\epsilon(n^\epsilon) \). Now apply Hölder’s inequality and get

\[
S \leq \epsilon \sum_{u \leq U} \sum_{v \leq V} \sum_{b' \leq H} \left( \frac{uvb'}{p} \right) \left( \frac{uvb' - c}{p} \right) \leq \epsilon \sum_{n \leq VH} \sum_{u \leq U} \left( \frac{un - c}{p} \right) \left( \frac{un - 4c}{p} \right) \left( \frac{un - 8c}{p} \right) \left( \frac{un - 16c}{p} \right)
\]

by Lemma 4 in [4] which follows from Weil’s bound on multiplicative character sums. Now we take \( U = p^{1/(2r)} \) and \( V = H/U \) with \( 1/r < \epsilon \). Then one can verify that \( S = o(H^2) \) which implies that there is some \( uv \leq H/2 \) and \( b' \leq H/2 \) such that \( \left( \frac{uvb'}{p} \right) \left( \frac{uvb' - c}{p} \right) = 1 \). This together with the argument in section 2 gives Theorem 1.

4 Proof of Theorem 3

Throughout this section, we assume that \( H \gg p^{1/6+\epsilon} \). Suppose, for all \( (c,p) = 1 \),

\[
\left( \frac{a'b'}{p} \right) \left( \frac{a'b' - c}{p} \right) = 1
\]

for some \( 1 \leq a', b' \leq H/2 \). This together with section 2 implies that

\[
|H_c \cap B(X,Y;H)| \geq 2
\]

for any \( (c,p) = 1 \) and \( H \gg p^{1/6+\epsilon} \).

Now, suppose this is not the case. Then, for some \( (c,p) = 1 \),

\[
\left( \frac{a'b'}{p} \right) \left( \frac{a'b' - c}{p} \right) = 0 \text{ or } -1
\]

for all \( 1 \leq a', b' \leq H/2 \). Suppose two such pairs give

\[
\left( \frac{a'_1 b'_1 - c}{p} \right) = 0 = \left( \frac{a'_2 b'_2 - c}{p} \right).
\]
This implies $|H_c \cap B(X,Y; H)| \geq 2$ automatically by section 2. Subsequently, we assume that
\[
\left( \frac{a'b'}{p} \right) \left( \frac{a'c' - b'}{p} \right) = -1
\]
for all but at most one pair of $1 \leq a', b' \leq H/2$. This implies that
\[
\left( \frac{a' - c'b'}{p} \right) = -\left( \frac{a'}{p} \right)
\]
for all but at most one pair of $1 \leq a', b' \leq H/2$. Consequently,
\[
\sum_{b' \leq H/2} \left| \sum_{a' \leq H/2} \left( \frac{a' - c'b'}{p} \right)^{2r} \right| \geq ([H/2] - 1) \sum_{a' \leq H} \left| \left( \frac{a'}{p} \right)^{2r} \right| =: ([H/2] - 1)|\Sigma|^{2r}.
\]
Now we apply Theorem 2 with $N_{b'} = -c'b'$. First we claim that $c'b_1 - c'b_2$ cannot be congruent to some $l \leq H$ modulo $p$ for $1 \leq b'_1 < b'_2 \leq H/2$. For otherwise
\[
c'b_1 - c'b_2 \equiv l \pmod{p}
\]
for some $1 \leq l \leq H$. Let $a'_1 \equiv c'b_1 \pmod{p}$ and $a'_2 \equiv c'b_2 \pmod{p}$. Then $(a'_1, b'_1)$ and $(a'_2, b'_2)$ would be two points of the modular hyperbola $H_c$ lying in a square of side length $H$ which contradicts our assumption that no such square contains two such points. Therefore, we can apply Theorem 2 and get
\[
([H/2] - 1)|\Sigma|^{2r} = \sum_{b' \leq H/2} \left| \sum_{a' \leq H/2} \left( \frac{a' - c'b'}{p} \right)^{2r} \right| \ll_{\epsilon,r} H^{2r-2} p^{1/2+1/(2r)+\epsilon}.
\]
This implies that
\[
\Sigma \ll_{\epsilon,r} H^{1-3/(2r)} p^{(r+1)/(4r^2)+\epsilon/(2r)} = o(H)
\]
if $r$ is sufficiently large. Hence we have that the character sum
\[
\sum_{a' \leq H/2} \left( \frac{a'}{p} \right) = o(H).
\]
Feeding this character sum estimate into the standard Vinogradov’s trick in obtaining upper bound for the least quadratic nonresidue, we have the first half of Theorem 3.

References
[1] D.A. Burgess, The distribution of quadratic residues and non-residues, Mathematika 4 (1957), 106–112.
[2] D.R. Heath-Brown, Burgess’s bounds for character sums, Number theory and related fields, 199-213, Springer Proc. Math. Stat., 43, Springer, New York, 2013.
[3] X. Shao, Character Sums over Unions of Intervals, ArXiv e-prints, arxiv.org/pdf/1302.0348.
[4] I. Shparlinski, Multiple Exponential and Character Sums with Monomials, Mathematika 60 (2014), no. 2, 363–373.
[5] I.M. Vinogradov, On a general theorem concerning the distribution of the residues and non-residues of powers, Trans. Amer. Math. Soc. 29 (1927), 209-217.
Tsz Ho Chan
Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152
U.S.A.
thchan6174@gmail.com