SHORTEST DISTANCE IN MODULAR CUBIC POLYNOMIALS

Tsz Ho Chan
Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, U.S.A.
thchan6174@gmail.com

Received: 6/6/16, Accepted: 6/23/17, Published: 7/17/17

Abstract

In this paper, we study how small a box contains at least two points from a modular cubic polynomial $y \equiv ax^3 + cx + d \pmod p$ with $(a, p) = 1$. We prove that some square of side length $p^{1/6+\epsilon}$ contains two such points.

1. Introduction and Main Results

In the x-y plane, the most common way to define distance between two points is

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

We say that two points are close to one another if d is small. However, if we are working with curves $\pmod p$, we may not be able to take the square root. So, instead of using distance, we say that two points are close to each other if they are both inside a box

$$B(X, Y; H) := \{(x, y) : X+1 \le x \le X+H \pmod p, Y+1 \le y \le Y+H \pmod p\}$$

for some X and Y with H small. We may say, in some sense, that the smallest such H is the "distance" between the two points. Here and throughout the paper, p stands for a prime number.

Recently, the author [1] studied the apparently new question of shortest "distance" in a modular hyperbola $xy \equiv c \pmod p$ and its relation with the least quadratic nonresidue modulo p. Inspired by this, we try to study the shortest "distance" for other kinds of curves.

For linear polynomials, the shortest distance can have order of magnitude $\sqrt{p}$ which is optimal. For example, take $H = [\sqrt{p}]$ and $m = H + 1$. Then the numbers mh for $1 \le h \le H - 1$ are all greater than H and less than p. Thus, when we look at the linear equation $y \equiv mx \pmod p$, it cannot have two points in the box $B(X, Y, H)$. For if (x_1, y_1) and (x_2, y_2) are two such points with $1 \le x_1 < x_2 < p$, say $x_2 = x_1 + h$ for some $1 \le h < H$. Then $y_2 - y_1 = mx_2 - mx_1 = mh$ cannot be any number between 1 and $H - 1 \pmod{p}$. Hence there can be no such two points from the line in the box. As for why $\sqrt{p}$ is optimal, by any $1 \le a \le p$, two of $ak_1 \pmod{p}$ and $ak_2 \pmod{p}$ must be within $H + 1$ from one another for some $1 \le k_1 < k_2 \le H + 1$ by pigeonhole principle. So the two points (k_1, ak_1) and (k_2, ak_2) on the line $y \equiv ax \pmod{p}$ are in a box of length $H + 1$.

Meanwhile the shortest distance can be as small as $O(1)$ for quadratic polynomials. Suppose $p > 3$. Starting from any quadratic polynomial $y \equiv ax^2 + bx + c \pmod{p}$, we can turn it to the form $y \equiv ax^2 \pmod{p}$ after completing the square as shifting does not affect distance. Now, consider the two points (x_1, ax_1^2) and (x_2, ax_2^2) with $a(2x_1 + 1) \equiv 1 \pmod{p}$ and $x_2 = x_1 + 1$. One can verify that they are both in the box $B(x_1 - 1, ax_1^2 - 1; 2)$.

Next, we study the shortest distance for the next type of curves, namely cubic polynomials. It turns out that this can be studied perfectly with the method of [1].

Let $p > 3$ be a prime, $(a, p) = 1$, and c any integer. We consider the reduced modular cubic polynomial

$$C_{a,c} := \{(x, y) : y \equiv ax^3 + cx \pmod{p}\}.$$

The restriction to such reduced cubic polynomials is not restrictive at all as one can transform a general cubic to such form through change of variables in x and y which does not affect the distance between points on the cubic polynomial. We consider how small a box $B(X, Y; H)$ contains at least two points in $C_{a,c}$ where X and Y run through 0, 1, ..., $p - 1$. To study this, we need a recent result of Heath-Brown [2] and Shao [3] on mean-value estimates of character sums:

Theorem 1. *Given $H \le p$, a positive integer and any $\epsilon > 0$. Suppose that $0 \le N_1 < N_2 < ... < N_J < p$ are integers satisfying $N_{j+1} - N_j \ge H$ for $1 \le j < J$. Then*

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

where

$$S(N; H) := \sum_{N < n \le N+H} \chi(n)$$

and χ is any non-principal character modulo p.

Applying the above theorem, we can show that

Theorem 2. *For any $\epsilon > 0$, for any $(a, p) = 1$, integer c and $H \gg_\epsilon p^{1/6+\epsilon}$, we have*

$$|C_{a,c} \cap B(X, Y; H)| \ge 2$$

for some $0 \le X, Y \le p - 1$.

As a consequence, we also have the following curious new results.

Corollary 1. *For any $\epsilon > 0$ and integer c, there exist $1 \leq u_1, v_1, u_2, v_2 \ll_\epsilon p^{1/6+\epsilon}$ such that*

$$\Big(\frac{u_1}{p}\Big)\Big(\frac{u_1^3 + cu_1 - v_1}{p}\Big) = 1$$

and

$$\Big(\frac{u_2}{p}\Big)\Big(\frac{u_2^3 + cu_2 - v_2}{p}\Big) = -1.$$

In particular, by setting $c = 0$, we have

$$\Big(\frac{u_3}{p}\Big)\Big(\frac{u_3^3 - v_3}{p}\Big) = 1$$

and

$$\Big(\frac{u_4}{p}\Big)\Big(\frac{u_4^3 - v_4}{p}\Big) = -1$$

for some $1 \leq u_3, v_3, u_4, v_4 \ll_\epsilon p^{1/6+\epsilon}$.

Finally, we finish with the following

Conjecture 1. For any $\epsilon > 0$, for any $(a, p) = 1$, integer c and $H \gg_\epsilon p^\epsilon$, we have

$$|C_{a,c} \cap B(X, Y; H)| \geq 2$$

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

Some Notation. 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 $(\frac{\cdot}{p})$. 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, $f(x) \ll_{\lambda_1,\dots,\lambda_k} g(x)$, $g(x) \gg_{\lambda_1,\dots,\lambda_k} f(x)$ and $f(x) = O_{\lambda_1,\dots,\lambda_k}(g(x))$ mean that the implicit constant C may depend on λ_1, ..., λ_k.

2. The Basic Argument

Without loss of generality, we assume that $p > 3$. For $(a, p) = 1$ and any integer c, suppose $|C_{a,c} \cap B(X, Y; H)| \geq 2$ for some $0 \leq X, Y \leq p - 1$. This means that

$$y \equiv ax^3 + cx \pmod{p}, \text{ and } y + v \equiv a(x + u)^3 + c(x + u) \pmod{p} \qquad (1)$$

for some $1 \leq x, y \leq p$ and $1 \leq u, v \leq H$. Subtracting, we get

$$v \equiv 3au(x^2 + ux + \overline{3}u^2) + cu \pmod{p}$$

where $\overline{y}$ denotes the multiplicative inverse of y modulo p (i.e. $y\overline{y} \equiv 1 \pmod{p}$.) After some algebra and completing the square, we have

$$(2x+u)^2 \equiv 4\overline{3}v\overline{au} - \overline{3}u^2 - 4\overline{3}\overline{a}c \pmod{p}.$$

The above process is reversible. So $|C_{a,c} \cap B(X,Y;H)| \geq 2$ for some $0 \leq X, Y \leq p-1$ is equivalent to

$$\Big(\frac{-3}{p}\Big)\Big(\frac{a}{p}\Big)\Big(\frac{u}{p}\Big)\Big(\frac{au^3+4cu-4v}{p}\Big) = 1.$$

We are going to restrict our attention to even $u = 2u'$'s and $v = 2v'$'s. So we want

$$\Big(\frac{-3}{p}\Big)\Big(\frac{a}{p}\Big)\Big(\frac{u'}{p}\Big)\Big(\frac{au'^3+cu'-v'}{p}\Big) = 1 \text{ for some } 1 \leq u', v' \leq H/2. \tag{2}$$

3. Proofs of Theorem 2 and Corollary 1

Proof. Suppose (2) is not true. Then either

$$\Big(\frac{-3}{p}\Big)\Big(\frac{a}{p}\Big)\Big(\frac{u'}{p}\Big)\Big(\frac{au'^3+cu'-v'}{p}\Big) = 0;$$

or

$$\Big(\frac{-3}{p}\Big)\Big(\frac{a}{p}\Big)\Big(\frac{u'}{p}\Big)\Big(\frac{au'^3+cu'-v'}{p}\Big) = -1$$

for all $1 \leq u', v' \leq H/2$. If the former is true for two pairs of $1 \leq u', v' \leq H/2$, we have

$$au'^3 + cu' \equiv v' \pmod{p} \text{ and } au''^3 + cu'' \equiv v'' \pmod{p} \tag{3}$$

which gives Theorem 2. Henceforth we suppose the latter is true for all but at most one pair of $1 \leq u', v' \leq H/2$. Hence

$$\begin{aligned} H^2 \ll & \Big| \sum_{u' \leq H/2} \sum_{v' \leq H/2} \Big(\frac{u'}{p}\Big)\Big(\frac{au'^3+cu'-v'}{p}\Big) \Big| \leq \sum_{u' \leq H/2} \Big| \sum_{v' \leq H/2} \Big(\frac{au'^3+cu'-v'}{p}\Big) \Big| \\ \leq & \Big(\sum_{u' \leq H/2} 1 \Big)^{(2r-1)/(2r)} \Big(\sum_{u' \leq H/2} \Big| \sum_{v' \leq H/2} \Big(\frac{au'^3+cu'-v'}{p}\Big) \Big|^{2r} \Big)^{1/(2r)}. \end{aligned}$$

Suppose $|C_{a,c} \cap B(X,Y;H)| \leq 1$ for all $0 \leq X, Y \leq p-1$. Then the points $au'^3 + cu'$ are spaced more than H apart. So we can apply Theorem 1 and get

$$H^2 \ll_{\epsilon,r} H^{(2r-1)/(2r)} (H^{2r-2} p^{1/2+1/(2r)+\epsilon})^{1/(2r)}$$

which gives $H \ll_{\epsilon,r} p^{(r+1)/(6r)+\epsilon/2}$. This contradicts $H \gg_\epsilon p^{1/6+\epsilon}$ if r is sufficiently large. This final contradiction together with (3) gives Theorem 2. $\square$

Proof. By setting $a = 1$, the above proof gives some $1 \le u', v' \ll_\epsilon p^{1/6+\epsilon}$ such that

$$\Big(\frac{-3}{p}\Big)\Big(\frac{u'}{p}\Big)\Big(\frac{u'^3 + cu' - v'}{p}\Big) = 1.$$

A similar argument also gives some $1 \le u'', v'' \ll_\epsilon p^{1/6+\epsilon}$ such that

$$\Big(\frac{-3}{p}\Big)\Big(\frac{u''}{p}\Big)\Big(\frac{u''^3 + cu'' - v''}{p}\Big) = -1.$$

It follows that Corollary 1 is true. □

Acknowledgement. Then author would like to thank the referee for helpful suggestions that improves the presentation of the paper.

References

[1] T.H. Chan, Shortest distance in modular hyperbola and least quadratic nonresidue, *Mathematika* **62** (2016), 860–865.

[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, *Forum Math.* **27** (5) (2015), 3017–3026.