Chin. Ann. Math. Ser. B
47(5), 2026, 899–910
DOI: 10.1007/s11401-026-0026-7

Chinese Annals of Mathematics, Series B

On a Conjecture of Sun Involving Powers of Three*

Quan-Hui YANG[1] Lilu ZHAO[2]

Abstract Given a positive integer $n \geq 2$, let $D(n)$ denote the smallest positive integer m such that $a^3 + a\,(a = 1, \cdots, n)$ are pairwise distinct modulo m^2. A conjecture of Sun states that $D(n) = 3^k$, where 3^k is the least power of 3 no less than $\sqrt{n}$. The purpose of this paper is to confirm this conjecture.

Keywords Congruence, Gauss sum, Quadratic residue, Kloosterman sum
2020 MR Subject Classification 11A07, 11L05

1 Introduction

Let $\mathbb{N} = \{0, 1, 2, \cdots\}$ be the set of natural numbers and let $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ be the set of positive integers. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with all $f(a)\,(a \in \mathbb{Z}^+)$ pairwise distinct. Define the discriminator $\Delta_f(n)$ to be the smallest positive integer m such that $f(a)\,(a = 1, \cdots, n)$ are pairwise distinct modulo m.

In 1985, Arnold, Benkoski and McCabe [1] studied $\Delta_f(n)$ with $f(x) = x^2$, and it was shown in [1] that for $n > 4$, $\Delta_f(n)$ is the smallest positive integer $m \geq 2n$ such that m is p or $2p$ with p an odd prime. Sun [8] determined $\Delta_f(n)$ for $f(x) = 2x(x-1)$ and $f(x) = x(x-1)$, respectively. For example, Sun [8] proved that if $f(x) = 2x(x-1)$, then $\Delta_f(n)$ is the least prime number greater than $2n-2$, and if $f(x) = x(x-1)$, then $\Delta_f(n)$ is the smallest $m \geq 2n-1$ such that m is a prime number or a positive power of 2. For the study of $\Delta_f(n)$ with higher degree polynomials f, one may refer to [2, 6–7, 10]. Sun proposed many interesting conjectures related to discriminators, and one may refer to [8] (see also Section 4 of Chapter 6 in [9]) for details.

In this paper, we consider $D(n)$, which denotes the smallest positive integer m such that $a^3 + a\,(1 \leq a \leq n)$ are pairwise distinct modulo m^2. In 2013, Sun made the following conjecture (see [9, Conjecture 6.76]).

Conjecture 1.1 For all $n \geq 2$, one has $D(n) = 3^k$, where

$$k = \min\{j \in \mathbb{Z}^+ :\ 3^j \geq \sqrt{n}\}. \tag{1.1}$$

Manuscript received November 26, 2021. Revised August 21, 2024.
[1]Ministry of Education Key Laboratory for NSLSCS, School of Mathematical Sciences, Nanjing Normal University, Nanjing 210023, China. E-mail: yangquanhui01@163.com
[2]Corresponding author. School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China. E-mail: zhaolilu@sdu.edu.cn
*This work was supported by the National Key Research and Development Program of China (No. 2021YFA1000701) and the National Natural Science Foundation of China (Nos. 12371005, 12471008).

The main result in this paper is to confirm the above conjecture.

Theorem 1.1 *Conjecture* 1.1 *is true.*

We prove Theorem 1.1 by combining methods from elementary number theory and analytic number theory. In particular, we make use of the explicit formulae of quadratic Gauss sums and the well-known upper bound on Kloosterman sums.

2 Preparations

We first point out that $\sqrt{n} \le D(n) \le 3^k$, where k is given in (1.1) throughout this paper. In fact, we have the following lemma.

Lemma 2.1 *Let $n \ge 2$. Then $a^3 + a\,(1 \le a \le n)$ are pairwise distinct modulo 3^{2k}.*

Proof Suppose that $1 \le a < b \le n$. Note that $b^3 + b - a^3 - a = (b-a)(a^2 + ab + b^2 + 1)$. Since $3 \nmid (a^2 + ab + b^2 + 1)$ and $1 \le b - a < n \le 3^{2k}$, one has $b^3 + b \not\equiv a^3 + a \pmod{3^{2k}}$. This completes the proof.

By Lemma 2.1, in order to establish Theorem 1.1, it suffices to prove the following result.

Proposition 2.1 *Let $n \ge 2$. Suppose that $m > 0$ and $k > 0$ are integers satisfying*

$$\sqrt{n} \le m < 3^k < 3\sqrt{n}. \tag{2.1}$$

Then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.

In order to prove Proposition 2.1, we shall consider the following six cases.

(i) $m = \delta p^r$, where $1 \le \delta \le 3$, $p \ge 5$ is a prime, $r \in \mathbb{Z}^+$ and $p^r \ge 11$.

(ii) $m = 2^r$, where $r \in \mathbb{Z}^+$.

(iii) $m = 2^r 3^s$, where $r, s \in \mathbb{Z}^+$.

(iv) $m = 2^r 3^s 5$, where $r, s \in \mathbb{N} = \mathbb{Z}^+ \cup \{0\}$.

(v) $m = 2^r 3^s 7$ or $m = 2^r \cdot 3^s \cdot 5 \cdot 7$, where $r, s \in \mathbb{N}$.

(vi) $m = \delta p^r$, where $\delta \ge 4$, $p \ge 5$ is a prime, $r \in \mathbb{Z}^+$, $p \nmid \delta$ and $p^r \ge 11$.

The letter δ always denotes a positive integer. It is clear that m in (2.1) must satisfy one of the above six cases.

3 The Cases (ii)–(vi)

The purpose of this section is to deal with cases (ii)–(vi). From now on, we assume that (2.1) holds.

Lemma 3.1 *Suppose that $m = \delta p^r$, where $\delta \in \mathbb{Z}^+$, $p \ge 5$ is a prime, $r \in \mathbb{Z}^+$ and $p \nmid \delta$. If $p^{2r} + \delta^2 \frac{p-1}{2} \le n$, then there exist $1 \leqslant a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof We consider $1 \le a \le p^{2r}$ and $b = a + \delta^2 c$ with $1 \le c \le \frac{p-1}{2}$. Note that

$$b \le p^{2r} + \delta^2 \frac{p-1}{2} \le n.$$

It suffices to find a, c such that

$$a^2 + a(a + \delta^2 c) + (a + \delta^2 c)^2 + 1 \equiv 0 \pmod{p^{2r}}.$$

This is equivalent to

$$(6a + 3\delta^2 c)^2 \equiv -3\delta^4 c^2 - 12 \pmod{p^{2r}}.$$

It is well known (see [3, Chapter 7]) that for any odd prime p and $a, b, c \in \mathbb{Z}$ with $p \nmid a$, we have

$$\Big(\frac{a}{p}\Big) \sum_{x=0}^{p-1} \Big(\frac{ax^2 + bx + c}{p}\Big) = \begin{cases} p-1, & \text{if } p \mid b^2 - 4ac, \\ -1, & \text{otherwise,} \end{cases}$$

where $\big(\frac{\cdot}{p}\big)$ denotes the Legendre symbol. In particular, we have

$$\Big| \sum_{-\frac{p-1}{2} \le j \le \frac{p-1}{2}} \Big(\frac{-3\delta^4 j^2 - 12}{p}\Big) \Big| = 1.$$

Note that $3 \nmid p$, and we conclude that there exists $1 \le c \le \frac{p-1}{2}$ such that $-3\delta^4 c^2 - 12$ is a quadratic residue modulo p. By [4, Proposition 4.2.3], for any odd prime p, if $x^2 \equiv s \pmod{p}$ is solvable, then so is $x^2 \equiv s \pmod{p^h}$, where h is any positive integer. Therefore, there exists $1 \le a \le p^{2r}$ such that $(6a + 3\delta^2 c)^2 \equiv -3\delta^4 c^2 - 12 \pmod{p^{2r}}$. This completes the proof.

Lemma 3.2 (Case (vi)) *Suppose that $m = \delta p^r$, where $\delta \ge 4$, $p \ge 5$ is a prime, $r \in \mathbb{Z}^+$, $p \nmid \delta$ and $p^r \ge 11$. Then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof In view of Lemma 3.1, we need to verify $p^{2r} + \delta^2 \frac{p-1}{2} \le n$. By (2.1), $n > \frac{\delta^2 p^{2r}}{9}$. It suffices to prove that $p^{2r} + \frac{1}{2}\delta^2 p \le \frac{\delta^2 p^{2r}}{9}$. Since $\delta^2 - 9 \ge 7$ and $p^{2r-1} \ge p^r \ge 11$, we have $(\delta^2 - 9)\big(p^{2r-1} - \frac{9}{2}\big) \ge \frac{81}{2}$, which is equivalent to $p^{2r} + \frac{1}{2}\delta^2 p \le \frac{\delta^2 p^{2r}}{9}$. This completes the proof.

Lemma 3.3 (Case (v)) *Suppose that $m = 2^r 3^s 7$ or $m = 2^r \cdot 3^s \cdot 5 \cdot 7$, where $r, s \in \mathbb{N}$. Then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof We first consider the case $r \ge 1$. We write $m^2 = 14t$. Note that $14 \mid t$. We choose $a = 3$, $b = 3 + t$ and it is easy to verify $b^3 + b \equiv a^3 + a \pmod{m^2}$. For $m \ge 14$, by (2.1), we have $n > 20$ and $3 + t = 3 + \frac{m^2}{14} < 3 + \frac{9}{14} n \le n$.

Now we assume that $r = 0$. Thus $m = 3^s 7$ or $m = 3^s \cdot 5 \cdot 7$. We write $m^2 = 7t$ and choose $a = 3$, $b = 3 + t$. Then again it is easy to verify $b^3 + b \equiv a^3 + a \pmod{m^2}$. We need to confirm $3 + t \le n$. If $m = 3^s 7$, then by (2.1) we have $s = k - 2$, $n > 3^{2s+2}$ and $3 + t = 3 + 3^{2s} 7 \le 3^{2s+2} + 1 \le n$. If $m = 3^s \cdot 5 \cdot 7$, then by (2.1) we have $s = k - 4$, $n > 3^{2s+6}$ and $3 + t = 3 + 3^{2s} 5^2 7 < 3^{2s+6} < n$. This completes the proof.

Lemma 3.4 *Suppose that $m = 2^r t$, where $r \in \mathbb{Z}^+$, t is an odd number. If $2^{2r} + t^2 \le n$, then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof We consider $1 \le a \le 2^{2r}$ and $b = a + t^2$. Note that $b \le 2^{2r} + t^2 \le n$. It suffices to find a such that

$$a^2 + a(a + t^2) + (a + t^2)^2 + 1 \equiv 0 \pmod{2^{2r}}.$$

This is equivalent to

$$3a^2 + 3at^2 + t^4 + 1 \equiv 0 \pmod{2^{2r}}.$$

In fact, we can prove by induction that for any $j \in \mathbb{Z}^+$, there exists $1 \le a \le 2^j$ such that

$$3a^2 + 3at^2 + t^4 + 1 \equiv 0 \pmod{2^j}. \tag{3.1}$$

When $j = 1$, we choose $a = 1$. Suppose that (3.1) holds. We consider $a' = a + 2^j c$. Then

$$3a'^2 + 3a't^2 + t^4 + 1 \equiv 3a^2 + 3at^2 + t^4 + 1 + 3t^2 \cdot 2^j c \pmod{2^{j+1}}. \tag{3.2}$$

We can find $c \in \{0, 1\}$ such that $3a'^2 + 3a't^2 + t^4 + 1 \equiv 0 \pmod{2^{j+1}}$. This completes the proof.

Lemma 3.5 (Case (iv)) *Suppose that $m = 2^r 3^s 5$, where $r, s \in \mathbb{N}$. Then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof We first consider the case $r \ge 2$. In view of Lemma 3.4, we only need to verify $2^{2r} + t^2 \le n$, where $t = 3^s 5$. This follows from $2^{2r} + t^2 \le \frac{2^{2r} t^2}{9}$, because $n > \frac{m^2}{9} = \frac{2^{2r} t^2}{9}$. The inequality $2^{2r} + t^2 \le \frac{2^{2r} t^2}{9}$ holds due to $2^{2r} \ge 16$ and $t^2 \ge 25$.

Now we assume that $r = 0$ or $r = 1$. Then $m = 3^s 5$ or $m = 2 \cdot 3^s \cdot 5$. We write $m = \delta p$ with $p = 5$. In view of Lemma 3.1, we only need to verify $25 + 2\delta^2 \le n$. If $m = 3^s 5$, then by (2.1), we have $s = k - 2$, $n > 3^{2k-2} = 3^{2s+2}$ and $25 + 2\delta^2 = 25 + 2 \cdot 3^{2s} < 3^{2s+2} \le n$ provided that $s \ge 1$. In the case $m = 5$, by (2.1), we have $n > 9$ and we can obtain $b^3 + b \equiv a^3 + a \pmod{m^2}$ by choosing $a = 2$ and $b = 10$. If $m = 2 \cdot 3^s \cdot 5$, then by (2.1), we have $s = k - 3$, $n > 3^{2k-2} = 3^{2s+4}$ and $25 + 2\delta^2 = 25 + 8 \cdot 3^{2s} \le 3^{2s+4} < n$. This completes the proof.

Lemma 3.6 (Case (iii)) *Suppose that $m = 2^r 3^s$, where $r, s \in \mathbb{Z}^+$. Then there exist $1 \le a < b \le n$ such that $b^3 + b \equiv a^3 + a \pmod{m^2}$.*

Proof It is easy to deduce from (2.1) and $m \ge 6$ that $n \ge 10$. We first consider the case $r \ge 2$ and $s \ge 2$. It is easy to verify $2^{2r} + 3^{2s} \le n$ since $2^{2r} + 3^{2s} \le \frac{2^{2r} 3^{2s}}{9}$, and the desired conclusion follows from Lemma 3.4.

Next we consider the case $r = 1$ and $s \ge 2$. By (2.1), we have $s = k - 1$ and $n > 3^{2k-2}$. Then we have $1 + 3^{2s} = 1 + 3^{2k-2} \le n$. The desired conclusion follows by choosing $a = 1$ and $b = 1 + 3^{2s}$, since $a^2 + ab + b^2 + 1 \equiv 0 \pmod 4$.

Now we assume that $s = 1$. Then $m = 2^r 3$. Note that $a^2 + a(a + 9) + (a + 9)^2 + 1$ is equal to $112 = 2^4 \cdot 7$ if $a = 1$. If $r \le 2$, then the desired conclusion follows by choosing $a = 1$ and $b = 10$. Next we assume $r \ge 3$. Similar to (3.1)–(3.2), we can prove that for any $j \ge 4$, there exists $1 \le a \le 2^j - 15$ such that

$$a^2 + a(a + 9) + (a + 9)^2 + 1 \equiv 0 \pmod{2^j}.$$

In particular, there exists $1 \le a \le 2^{2r}-15$ such that $a^2+a(a+9)+(a+9)^2+1 \equiv 0 \pmod{2^{2r}}$. The desired congruence follows by choosing $b = a+9$. Note that $b \le 2^{2r}-6 < n$. This completes the proof.

Lemma 3.7 (Case (ii)) *Suppose that $m = 2^r$, where $r \in \mathbb{Z}^+$. Then there exist $1 \le a < b \le n$ such that $b^3+b \equiv a^3+a \pmod{m^2}$.*

Proof For $n \le 4$, by (2.1), we have $m = 2$ and it suffices to choose $a = 1$ and $b = 2$. Next we assume $n \ge 5$. If $r \le 3$, the desired conclusion follows by choosing $a = 1$ and $b = 5$. Now we assume that $r \ge 4$.

Since $(a+4)^3+(a+4)-a^3-a = 4(3(a+2)^2+5)$, it suffices to find $1 \le a \le 2^{2r-4}-3$ such that $3(a+2)^2+5 \equiv 0 \pmod{2^{2r-2}}$.

Note that $3 \cdot 1^2+5 \equiv 0 \pmod 8$. We can prove by induction that for any $j \ge 3$, there exists x such that

$$3x^2+5 \equiv 0 \pmod{2^j}. \tag{3.3}$$

From (3.3), for $j \ge 3$, we can deduce that $3(x+2^{j-1}c)^2+5 \equiv 3x^2+5+3x \cdot 2^j c \pmod{2^{j+1}}$. Thus, there exists x' such that $3x'^2+5 \equiv 0 \pmod{2^{j+1}}$. In particular, there exists x such that $3x^2+5 \equiv 0 \pmod{2^{2r-2}}$. Since x is odd, we can assume that $1 \le x \le 2^{2r-3}-1$.

Let $y = 2^{2r-3}-x$. Then we deduce that $3y^2+5 = 3(2^{2r-3}-x)^2+5 \equiv 3x^2+5 \equiv 0 \pmod{2^{2r-2}}$. Therefore, we can further assume that $1 \le x \le 2^{2r-4}-1$. Since $r \ge 4$, we have $3 \le x \le 2^{2r-4}-1$. On choosing $a = x-2$, we obtain $3(a+2)^2+5 \equiv 0 \pmod{2^{2r-2}}$. Note that

$$a+4 \le 2^{2r-4}+1 < \frac{9}{16}n+1 \le n.$$

This completes the proof.

4 Case (i)

In this section, we deal with the case (i). The first result is the following.

Lemma 4.1 *Suppose that $m = \delta p^r$, where $1 \le \delta \le 3$, $p \equiv 1 \pmod 3$ is a prime, $r \in \mathbb{Z}^+$ and $p^r \ge 11$. Then there exist $1 \le a < b \le n$ such that $b^3+b \equiv a^3+a \pmod{m^2}$.*

Proof We consider $1 \le a \le \frac{p^r-1}{2}$ and $b = a+\delta^2 p^r$. We claim that there exists $1 \le a \le \frac{p^r-1}{2}$ such that

$$a^2+a(a+\delta^2 p^r)+(a+\delta^2 p^r)^2+1 \equiv 0 \pmod{p^r},$$

which is equivalent to

$$3a^2+1 \equiv 0 \pmod{p^r}.$$

The claim is true due to the condition $p \equiv 1 \pmod 3$.

We need to verify $\frac{p^r-1}{2}+\delta^2 p^r \le n$. By (2.1), it suffices to prove $\frac{p^r}{2}+\delta^2 p^r \le \frac{\delta^2 p^{2r}}{9}$, which is equivalent to

$$p^r \ge 9+\frac{9}{2\delta^2}.$$

Since $p^r \geq 11$ and $p \equiv 1 \pmod 3$, the above inequality holds except $m = 13$.

For $m = 13$, by (2.1), we have $k = 3$ and $n > 81$. By choosing $a = 2$ and $b = 2 + 13 = 15$, we have $b^3 + b \equiv a^3 + a \pmod{m^2}$. This completes the proof.

From now on, we assume throughout this section that $m = \delta p^r$, where $1 \leq \delta \leq 3$, $p \equiv 2 \pmod 3$ is an odd prime, $r \in \mathbb{Z}^+$. Note that $p \equiv 2 \pmod 3$ is equivalent to $\left(\frac{-3}{p}\right) = -1$.

We shall deal with the remaining case by using analytic number theory method. Throughout this section, we use the notation

$$e(\alpha) = \mathrm{e}^{2\pi \mathrm{i}\alpha}.$$

We introduce

$$X := X_p = \begin{cases} \left\lfloor \dfrac{p^2}{9} \right\rfloor p^{2r-2}, & \text{if } p = 5, \\ \left\lfloor \dfrac{p}{9} \right\rfloor p^{2r-1}, & \text{if } p \geq 11, \end{cases} \tag{4.1}$$

where $\lfloor x \rfloor$ denotes the greatest integer no more than x. We write

$$\rho := \rho_p = \begin{cases} 2r-2, & \text{if } p = 5, \\ 2r-1, & \text{if } p \geq 11. \end{cases} \tag{4.2}$$

We aim to find $1 \leq a \neq b \leq \frac{n}{\delta^2}$ such that $\delta^4(a^2 + ab + b^2) + 1 \equiv 0 \pmod{p^{2r}}$. Then on choosing $a_* = \delta^2 a$, $b_* = \delta^2 b$, we obtain $a_*^3 + a_* \equiv b_*^3 + b_* \pmod{m^2}$. By (2.1), we have $X < \frac{n}{\delta^2}$.

Let

$$f(a, b) = \delta^4(a^2 + ab + b^2). \tag{4.3}$$

Now we introduce

$$\mathcal{N} = \sum_{\substack{1 \leq a, b \leq X \\ f(a,b)+1 \equiv 0 \pmod{p^{2r}}}} 1. \tag{4.4}$$

Since $p \equiv 2 \pmod 3$ is an odd prime, one has $f(a, a) + 1 \not\equiv 0 \pmod{p^{2r}}$. In particular,

$$\mathcal{N} = \sum_{\substack{1 \leq a \neq b \leq X \\ f(a,b)+1 \equiv 0 \pmod{p^{2r}}}} 1.$$

Therefore, the main objective is to prove $\mathcal{N} > 0$.

For $j \geq 1$, we define

$$T_j = \sum_{\substack{1 \leq c \leq p^j \\ (c,p)=1}} \sum_{1 \leq a, b \leq X} e\Big(\frac{cf(a, b) + c}{p^j}\Big). \tag{4.5}$$

Lemma 4.2 *Let $\mathcal{N}$ and T_j be given in* (4.4) *and* (4.5)*, respectively. We have*

$$\mathcal{N} = \frac{X^2}{p^{2r}} + \frac{1}{p^{2r}} \sum_{j=1}^{2r} T_j. \tag{4.6}$$

Proof We make use of the identity ($q \in \mathbb{Z}^+, t \in \mathbb{Z}$),

$$\frac{1}{q}\sum_{c=1}^{q} e\Big(\frac{ct}{q}\Big) = \begin{cases} 1, & \text{if } q \mid t, \\ 0, & \text{if } q \nmid t \end{cases} \tag{4.7}$$

to obtain

$$\mathcal{N} = \frac{1}{p^{2r}} \sum_{1\le c\le p^{2r}} \sum_{1\le a,b\le X} e\Big(\frac{cf(a,b)+c}{p^{2r}}\Big).$$

We change variables by taking $c = p^{2r-j}c'$ with $0 \le j \le 2r$, $1 \le c' \le p^j$ and $(c', p) = 1$ to deduce that

$$\mathcal{N} = \frac{1}{p^{2r}} \sum_{j=0}^{2r} \sum_{\substack{1\le c'\le p^j \\ (c',p)=1}} \sum_{1\le a,b\le X} e\Big(\frac{c'f(a,b)+c'}{p^j}\Big) = \frac{X^2}{p^{2r}} + \frac{1}{p^{2r}}\sum_{j=1}^{2r} T_j.$$

We are done.

We define

$$S_j := S_j(x,y) = \sum_{\substack{1\le c\le p^j \\ (c,p)=1}} \sum_{1\le a,b\le p^j} e\Big(\frac{cf(a,b)+ax+by+c}{p^j}\Big). \tag{4.8}$$

Lemma 4.3 *Let S_j be given in* (4.8)*. We have*

$$S_j = p^j\Big(\frac{-3}{p^j}\Big) \sum_{\substack{1\le c\le p^j \\ (c,p)=1}} e\Big(\frac{\overline{3c\delta^4}(-x^2+xy-y^2)+c}{p^j}\Big), \tag{4.9}$$

where the notation $\overline{d}$ in (4.9) *denotes the least $x \in \mathbb{N}$ with $dx \equiv 1 \pmod{p^j}$.*

Proof Write

$$R_j = \sum_{1\le a,b\le p^j} e\Big(\frac{cf(a,b)+ax+by}{p^j}\Big).$$

The desired conclusion follows from

$$R_j = p^j\Big(\frac{-3}{p^j}\Big)e\Big(\frac{\overline{3c\delta^4}(-x^2+xy-y^2)}{p^j}\Big). \tag{4.10}$$

It is not hard to verify that (by transforming the quadratic form to its normal form)

$$\begin{aligned} &c\delta^4(a^2+ab+b^2)+ax+by \\ &\equiv c\delta^4(a+\overline{2}b+\overline{2c\delta^4}x)^2 + 3c\delta^4(\overline{2}b+\overline{3c\delta^4}(y-\overline{2}x))^2 + \overline{3c\delta^4}(-x^2+xy-y^2) \pmod{p^j}. \end{aligned}$$

We conclude from the above that

$$R_j = \Big(\sum_{1\le a\le p^j} e\Big(\frac{ca^2}{p^j}\Big)\Big)\Big(\sum_{1\le b\le p^j} e\Big(\frac{3cb^2}{p^j}\Big)\Big)e\Big(\frac{\overline{3c\delta^4}(-x^2+xy-y^2)}{p^j}\Big).$$

For the Gauss sum, it is well known that (see [3, Chapter 7])

$$\sum_{1\le a\le p^j} e\Big(\frac{ca^2}{p^j}\Big) = p^{\frac{j}{2}}\Big(\frac{c}{p^j}\Big)\varepsilon_{p^j},$$

where ε_{p^j} satisfies $\varepsilon_{p^j}^2 = \big(\frac{-1}{p^j}\big)$. This proves (4.10) and we are done.

Lemma 4.4 *Let ρ be given in* (4.2). *For $1 \le j \le \rho$, we have*

$$T_j = X^2 p^{-j}\Big(\frac{-3}{p^j}\Big)\mu(p^j), \tag{4.11}$$

where $\mu(\cdot)$ is the Möbius function.

Proof If $1 \le j \le \rho$, then $p^j \mid X$ and we have

$$T_j = X^2 p^{-2j} \sum_{\substack{1\le c\le p^j\\(c,p)=1}} \sum_{1\le a,b\le p^j} e\Big(\frac{cf(a,b)+c}{p^j}\Big) = X^2 p^{-2j} S_j(0,0).$$

By Lemma 4.3, we have

$$S_j(0,0) = p^j\Big(\frac{-3}{p^j}\Big)\mu(p^j)$$

and this yields (4.11). We are done.

Lemma 4.5 *Let ρ be given in* (4.2). *We have*

$$\mathcal{N} = \frac{X^2}{p^{2r}}\Big(1+\frac{1}{p}\Big) + \frac{1}{p^{2r}}\sum_{j=\rho+1}^{2r} T_j.$$

Proof The desired conclusion follows from Lemma 4.2 and Lemma 4.4.

Note that for $\rho+1 \le j \le 2r$, the summations over a and b in (4.5) are incomplete summations (modulo p^j).

Lemma 4.6 *For $\rho+1 \le j \le 2r$, we have*

$$T_j = \frac{1}{p^{2j}} \sum_{1\le x,y\le p^j} S_j(x,y) \sum_{1\le a',b'\le X} e\Big(-\frac{a'x+b'y}{p^j}\Big). \tag{4.12}$$

Proof This follows from (4.7) by considering the summations over x and y in (4.12).

Lemma 4.7 *Let $u \in \mathbb{Z}$. We have*

$$\Big|\sum_{\substack{1\le c\le p^j\\(c,p)=1}} e\Big(\frac{\overline{c}u+c}{p^j}\Big)\Big| \le 2p^{\frac{j}{2}}. \tag{4.13}$$

In particular, we have

$$|S_j| \le 2p^{\frac{3j}{2}}. \tag{4.14}$$

Proof Write

$$K(p^j;u)=\sum_{\substack{1\le c\le p^j\\(c,p)=1}} e\Big(\frac{\overline{c}u+c}{p^j}\Big).$$

If $p^j|u$, then $K(p^j;u)$ is a Ramanujan sum and $K(p^j;u)=\mu(p^j)$. If $p\nmid u$, then $K(p^j;u)$ is a Kloosterman sum and by [5, Corollary 4.4] we have $|K(p^j;u)|\le 2p^{\frac{j}{2}}$.

Now we assume that $p^t\|u$ (i.e., $p^t\mid u$ but $p^{t+1}\nmid u$) with $1\le t\le j-1$. By changing the variables $c=xp^{j-1}+y$, we obtain

$$K(p^j;u)=\sum_{\substack{1\le y\le p^{j-1}\\(y,p)=1}}\sum_{1\le x\le p} e\Big(\frac{\overline{y}u+xp^{j-1}+y}{p^j}\Big)=0.$$

The proof of (4.13) is complete. Note that (4.14) follows from Lemma 4.3 and (4.13) immediately. We are done.

Lemma 4.8 *For $\rho+1\le j\le 2r$, we have*

$$\sum_{1\le x\le p^j}\Big|\sum_{1\le a\le X} e\Big(\frac{ax}{p^j}\Big)\Big|\le p^j(2+\log p^j).$$

Proof On writing $Y=\frac{p^j-1}{2}$, we have

$$\begin{aligned}\sum_{1\le x\le p^j}\Big|\sum_{1\le a\le X} e\Big(\frac{ax}{p^j}\Big)\Big| &= X+2\sum_{1\le x\le Y}\Big|\sum_{1\le a\le X} e\Big(\frac{ax}{p^j}\Big)\Big|\\ &= X+2\sum_{1\le x\le Y}\Big|\frac{1-e\Big(\frac{xX}{p^j}\Big)}{1-e\Big(\frac{x}{p^j}\Big)}\Big|\\ &\le X+4\sum_{1\le x\le Y}\Big|\frac{1}{1-e\Big(\frac{x}{p^j}\Big)}\Big|.\end{aligned}$$

For $0<\theta<\frac{1}{2}$, we have $|1-e(\theta)|=2\sin(\pi\theta)>4\theta$. Therefore,

$$\sum_{1\le x\le p^j}\Big|\sum_{1\le a\le X} e\Big(\frac{ax}{p^j}\Big)\Big|\le X+\sum_{1\le x\le Y}\frac{p^j}{x}\le X+p^j(1+\log Y)\le p^j(2+\log p^j).$$

We are done.

Lemma 4.9 *For $\rho+1\le j\le 2r$, we have*

$$|T_j|\le 2p^{\frac{3j}{2}}(2+\log p^j)^2.$$

Proof By Lemmas 4.6–4.8, we deduce that

$$|T_j|\le\frac{1}{p^{2j}}\sum_{1\le x,y\le p^j}|S_j(x,y)|\cdot\Big|\sum_{1\le a',b'\le X} e\Big(-\frac{a'x+b'y}{p^j}\Big)\Big|$$

$$\begin{aligned}
&\le 2p^{\frac{3j}{2}}\cdot\frac{1}{p^{2j}}\sum_{1\le x,y\le p^j}\Big|\sum_{1\le a',b'\le X}e\Big(-\frac{a'x+b'y}{p^j}\Big)\Big|\\
&=2p^{\frac{3j}{2}}\cdot\frac{1}{p^{2j}}\Big(\sum_{1\le x\le p^j}\Big|\sum_{1\le a\le X}e\Big(\frac{ax}{p^j}\Big)\Big|\Big)^2\\
&\le 2p^{\frac{3j}{2}}(2+\log p^j)^2.
\end{aligned}$$

We are done.

Lemma 4.10 *We have*

$$\Big|\mathcal{N}-\frac{X^2}{p^{2r}}\Big(1+\frac{1}{p}\Big)\Big|\le\begin{cases}2p^r(2+\log p^{2r})^2\Big(1+\dfrac{1}{p\sqrt{p}}\Big), & \text{if } p=5,\\ 2p^r(2+\log p^{2r})^2, & \text{if } p\ge 11.\end{cases}\tag{4.15}$$

Proof The desired conclusion follows from Lemma 4.5 and Lemma 4.9.

Lemma 4.11 *Suppose that $m=\delta p^r$, where $1\le\delta\le 3$, $p\ge 5$ is a prime, $p\equiv 2\pmod 3$, $r\in\mathbb{Z}^+$. Suppose further more that $p^r\ge 675^2$. Then we have*

$$\mathcal{N}>0.$$

Proof For $p=5$, by (4.15), we need to prove

$$\frac{\Big\lfloor\dfrac{p^2}{9}\Big\rfloor^2 p^{4r-4}\Big(1+\dfrac{1}{p}\Big)}{p^{2r}}>8p^r(1+\log p^r)^2\Big(1+\frac{1}{p\sqrt{p}}\Big),$$

and this follows from

$$p^r>2\cdot 5^4(1+\log p^r)^2.\tag{4.16}$$

For $p\ge 23$, we have

$$\lfloor\frac{p}{9}\rfloor>\frac{p}{9}-1\ge\frac{1}{17}p,$$

and thus

$$\Big\lfloor\frac{p}{9}\Big\rfloor^2 p^{-2}\ge 17^{-2}.\tag{4.17}$$

One can check that (4.17) holds for $11\le p\le 19$ as well.

For $p\ge 11$, by (4.15), we need to prove

$$\frac{\Big\lfloor\dfrac{p}{9}\Big\rfloor^2 p^{4r-2}}{p^{2r}}>8p^r(1+\log p^r)^2,$$

and by (4.17), this follows from

$$p^r>8\cdot 17^2(1+\log p^r)^2.\tag{4.18}$$

On writing $q=\sqrt{p^r}$, our task is to prove

$$q>34\sqrt{2}(1+2\log q).$$

Let $g(x)=x-34\sqrt{2}(1+2\log x)$. Then $g'(x)=1-68\sqrt{2}\cdot\frac{1}{x}$ and g is increasing when $x>68\sqrt{2}$. Note that $g(675)>0$. This establishes both (4.16) and (4.18) since $p^r\geq 675^2$. The proof is complete.

Suppose that

$$3^{k-1}<\delta p^r<3^k,$$

and we define

$$\mathcal{N}^*=\sum_{\substack{1\leq a<b\leq 3^{2k-2}\\ a^3+a\equiv b^3+b\,(\mathrm{mod}\,\delta^2p^{2r})}}1. \tag{4.19}$$

We verify $\mathcal{N}^*>0$ for $11\leq p^r<675^2$ with the help of a computer.

Lemma 4.12 *Let $\mathcal{N}^*$ be given in* (4.19). *Suppose that $m=\delta p^r$, where $1\leq\delta\leq 3$, $p\geq 5$ is a prime, $p\equiv 2\pmod 3$, $r\in\mathbb{Z}^+$. Suppose further more that $11\leq p^r<675^2$. Then we have*

$$\mathcal{N}^*>0.$$

Proof This is checked by C++ taking about one and a half hours. We give some remarks here. For $5\leq p\leq 97$, the computer needs only a moment to complete the calculation (in no more than two seconds, say).

For $p>97$, the inequality (4.17) can be improved to $\lfloor\frac{p}{9}\rfloor^2p^{-2}\geq 10^{-2}$ and the proof in Lemma 4.11 implies $\mathcal{N}>0$ for $p^r\geq 362^2$. To complete the calculation subject to the conditions $p>97$, $p\equiv 2\pmod 3$ and $p^r<362^2$, it takes the computer about six minutes. The inequality in Lemma 4.8 can also be improved due to the loss in the inequality $\big|1-e\big(\frac{xX}{p^j}\big)\big|\leq 2$, and it is possible to prove $\mathcal{N}>0$ for $p^r\geq 250^2$ (and $p>97$). Then the computer can complete the calculation in two minutes.

Lemma 4.13 (Case (i)) *Suppose that $m=\delta p^r$, where $1\leq\delta\leq 3$, $p\geq 5$ is a prime, $r\in\mathbb{Z}^+$ and $p^r\geq 11$. Then there exist $1\leq a<b\leq n$ such that $b^3+b\equiv a^3+a\pmod{m^2}$.*

Proof The desired conclusion follows from Lemmas 4.1 and 4.11–4.12.

Proof of Proposition 2.1 Proposition 2.1 follows from Lemmas 3.2–3.3, 3.5–3.7 and 4.13. According to the remark between Lemma 2.1 and Proposition 2.1, we thus complete the proof of Theorem 1.1.

Acknowledgement The authors would like to thank the referee for the helpful suggestions.

Declarations

Conflicts of interest The authors declare no conflicts of interest.

References

[1] Arnold, L. K., Benkoski, S. J. and McCabe, B. J., The discriminator (a simple application of Bertrand's postulate), *Amer. Math. Monthly*, **92**, 1985, 275–277.

[2] Bremser, P. S., Schumer, P. D. and Washinyton, L. C., A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory*, **35**, 1990, 105–108.

[3] Hua, L. K., Introduction to Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[4] Ireland, K. and Rosen, M., A Classical Introduction to Mordern Number Theory (3rd ed.), Grad. Texts in Math., **84**, Springer-Verlag, New York, 1990.

[5] Iwaniec, H., Topic in Classical Automorphic Forms, Amer. Math. Soc., Providence, RI, 1997.

[6] Moree, P., The incongruence of consecutive values of polynomials, *Finite Fields Appl.*, **2**, 1996, 321–335.

[7] Moree, P. and Mullen, G. L., Dickson polynomial discriminators, *J. Number Theory*, **59**, 1996, 88–105.

[8] Sun, Z.-W., On functions taking only prime values, *J. Number Theory*, **133**, 2013, 2794–2812.

[9] Sun, Z.-W., New Conjectures in Number Theory and Combinatorics, Harbin Institute of Technology Press, Harbin, 2021.

[10] Zieve, M., A note on discriminator, *J. Number Theory*, **73**, 1998, 122–138.