Large Family of Sequences from Elliptic Curves over Residue Class Rings*

Shengqiang Li†, Member, Zhixiong Chen†‖, and Liang Zhou†, Nonmembers

SUMMARY An upper bound is established for certain exponential sums on the rational points of an elliptic curve over a residue class ring \( \mathbb{Z}_N \) for two distinct odd primes \( p \) and \( q \). The result is a generalization of an estimate of exponential sums on rational point groups of elliptic curves over finite fields. The bound is applied to showing the pseudorandomness of a large family of binary sequences constructed by using elliptic curves over \( \mathbb{Z}_N \).

Key words: elliptic curves, exponential sums, binary sequences, well-distribution measure, correlation measure

1. Introduction

Elliptic curves over a residue class ring \( \mathbb{Z}_k \) (\( k \) composite number) were firstly employed by Lenstra [17] for factoring integers. Such curves have also been proposed for cryptography. The first public key cryptosystem on such curves was developed by Koyama et al. [15]. Since then a lot of public key schemes based on such curves have been introduced in a series of papers, see [7], [11], [14], [16], [23] and references therein. The security of these cryptosystems is based on the factorization problem for \( k \).

For any positive integer \( K > 1 \), we identify \( \mathbb{Z}_K \), the residue class ring modulo \( K \), with the set \( \{0, 1, \ldots, K-1\} \). An elliptic curve \( E \) defined over \( \mathbb{Z}_K \) is given by an affine Weierstrass equation of the standard form:

\[
E : y^2 = x^3 + Ax^2 + B \quad \text{(mod } K\text{)}
\]

with coefficients \( A, B \in \mathbb{Z}_K \) and nonzero discriminant, see [6]. We denote by \( E(\mathbb{Z}_K) \) the set of \( \mathbb{Z}_K \)-rational points of \( E \) including the point at infinity \( O \).

Throughout this paper, let \( N = pq \), where \( p \) and \( q \) are two distinct odd primes satisfying “RSA type” with

\[2 < p < q < 2p.\]

It is known that the set \( E(\mathbb{Z}_N) \) of \( \mathbb{Z}_p \)-rational points of \( E \) forms an Abelian group under an appropriate composition rule denoted by \( \oplus \) and with the point at infinity \( O \) as the neutral element. We recall that

\[
|\#E(\mathbb{Z}_p) - p - 1| \leq 2p^{1/2},
\]

where \( \#E(\mathbb{Z}_p) \) is the number of \( \mathbb{Z}_p \)-rational points, including the point at infinity \( O \). Similarly, \( E(\mathbb{Z}_q) \) is an Abelian group with the point at infinity \( O \) as the neutral element. One can define an addition operation on \( E(\mathbb{Z}_N) \) in a natural way. That is, the addition operation on \( E(\mathbb{Z}_N) \) is the same addition on \( E(\mathbb{Z}_p) \) except replacing all operations modulo \( p \) by operations modulo \( N \). But unfortunately, \( E(\mathbb{Z}_N) \) does not form a group since division is not always possible modulo \( N \), i.e., the addition on \( E(\mathbb{Z}_N) \) will not always be defined.

By the Chinese Remainder Theorem (CRT), any \( x \in \mathbb{Z}_N \) can be uniquely denoted by a pair of integers \( [x_p, x_q] \) with \( x_p \in \mathbb{Z}_p \) and \( x_q \in \mathbb{Z}_q \). Hence, every point \( Q \in E(\mathbb{Z}_N) \) can be uniquely represented by a pair of points \( [Q_p, Q_q] = [(x_p, y_p), (x_q, y_q)] \) such that \( Q_p \in E(\mathbb{Z}_p) \) and \( Q_q \in E(\mathbb{Z}_q) \). The neutral element \( O \in E(\mathbb{Z}_N) \) is denoted by \([O_p, O_q]\).

Now let \( \overline{E}(\mathbb{Z}_N) = E(\mathbb{Z}_N) \times E(\mathbb{Z}_N) \) be the direct product of groups \( E(\mathbb{Z}_p) \) and \( E(\mathbb{Z}_q) \). Then \( \overline{E}(\mathbb{Z}_N) \) forms a group with neutral element \( O = [O_p, O_q] \). For any \( Q_p \in E(\mathbb{Z}_p) \setminus \{O_p\} \) and \( Q_q \in E(\mathbb{Z}_q) \setminus \{O_q\} \), the points \([Q_p, O_q] \) and \([O_p, Q_q] \) in \( \overline{E}(\mathbb{Z}_N) \) are called semi-zero points. In fact, the group \( \overline{E}(\mathbb{Z}_N) \) consists of \( \#E(\mathbb{Z}_N) - 1 \) points belonging to \( E(\mathbb{Z}_N) \) and \#\( E(\mathbb{Z}_p) \) + \#\( E(\mathbb{Z}_q) \) - 2 semi-zero points.

From the addition rule, it is easy to see that if \( Q = [Q_p, Q_q] \) and \( P = [P_p, P_q] \) are defined in \( E(\mathbb{Z}_N) \) for \( P = [P_p, P_q] \in E(\mathbb{Z}_N) \) then \( Q_p \neq O_p \) and \( Q_q \neq O_q \). Hence \( Q = lP \) is not defined if either \( lP_p \neq O_p \) or \( lP_q \neq O_q \).

The remainder of this correspondence is organized as follows. In Sect. 2, an upper bound is established for certain exponential sums on the rational points of an elliptic curve over \( \mathbb{Z}_N \). In Sect. 3, we describe a construction of bit generators from elliptic curves over \( \mathbb{Z}_N \) and prove that such generator can produce sequences with strong pseudorandomness. A conclusion is made in Sect. 4.

Throughout this paper, the implied constant in the symbol ‘\( c \)’ is absolute. We recall that the notation \( U \ll V \) is equivalent to the assertion that the inequality \( |U| \leq cV \) holds for some constant \( c > 0 \).

*a) E-mail: shqli@uestc.edu.cn
b) E-mail: ptczx@126.com (Corresponding author)

DOI: 10.1587/transfun.E93.A.1827

Copyright © 2010 The Institute of Electronics, Information and Communication Engineers
2. **Exponential Sums on Elliptic Curves over \( \mathbb{Z}_N \)**

Let \( f(x, y) \) be a rational function of \( E \) over \( \mathbb{Z}_N \). Assume \( f_p(x, y) \equiv f(x, y) \pmod{p} \) and \( f_q(x, y) \equiv f(x, y) \pmod{q} \). It is easy to see that \( f_p(x, y) \) (resp. \( f_q(x, y) \)) is a rational function of \( E \) over \( \mathbb{Z}_p \) (resp. \( \mathbb{Z}_q \)). Here we present the notion of degree of \( f_p(x, y) \) (and similarly of \( f_q(x, y) \)), which is needed in our proof. Let \( R \in \mathcal{E}(\overline{\mathbb{Z}_p}) \), where \( \overline{\mathbb{Z}_p} \) is the closure of \( \mathbb{Z}_p \), \( R \) is called a zero (resp. a pole) of \( f_p(x, y) \) if \( f_p(R) = 0 \) (resp. \( f_p(R) = \infty \)). Let \( \text{ord}_R(f_p) \) be the order of \( f_p(x, y) \) at \( R \). Obviously, \( \text{ord}_R(f_p) = 0 \) for all but finitely many \( R \in \mathcal{E}(\overline{\mathbb{Z}_p}) \) and \( \text{ord}_R(f_p) > 0 \) if \( R \) is a zero of \( f_p \) while \( \text{ord}_R(f_p) < 0 \) if \( R \) is a pole of \( f_p \). The degree of \( f_p \) is \( \text{deg}(f_p) = \sum_{\text{ord}_R(f_p) > 0} \text{ord}_R(f_p) = \sum_{\lambda \in \mathbb{Z}_p^*} |\text{ord}_R(f_p)| \). For example, \( \text{deg}(X) = 2 \) and \( \text{deg}(Y) = 3 \).

An upper bound for certain exponential sums defined on the points of elliptic curves over finite fields has been established in [13]. For integer \( m > 1 \), let

\[
\mathbf{e}(z) = \exp(2\pi i z) \quad \text{and} \quad \mathbf{e}_m(z) = \mathbf{e}\left(\frac{z}{m}\right).
\]

The following statement is a special case of [13, Corollary 1].

**Lemma 1:** Let \( f_p(x, y) \) be a nonconstant rational function and \( G \in \mathcal{E}(\mathbb{Z}_p) \) a rational point of order \( t \). Then the bound

\[
\left| \sum_{\substack{z \in \mathbb{Z}_p \setminus \{0\} \atop f_p(zG) \neq 0}} e_p(\alpha f_p(zG))e_\beta(z) \right| \leq 2 \text{deg}(f_p) p^{t/2}
\]

holds for all \( \alpha \in \mathbb{Z}_p \setminus \{0\} \) and any \( \beta \in \mathbb{Z}_p \).

In this section, we extend the bound in Lemma 1 to the case of elliptic curves defined over \( \mathbb{Z}_N \). Let \( Q_p \in \mathcal{E}(\mathbb{Z}_p) \) be a point of order \( M_p \) and \( Q_q \in \mathcal{E}(\mathbb{Z}_q) \) a point of order \( M_q \) with \( \gcd(M_p, M_q) = 1 \). Let \( \mathcal{Q} = \langle Q_p, Q_q \rangle \in \mathcal{E}(\mathbb{Z}_N) \). It is easy to see that the cyclic group \( \langle \mathcal{Q} \rangle = \langle Q_p \rangle \times \langle Q_q \rangle \) with order \( M = M_p M_q \). We note that there are \( M_p + M_q - 1 \) semi-zeros in \( \langle \mathcal{Q} \rangle \). Let

\[
I = \{ i : 0 \leq i \leq M - 1, iQ \text{ is a semi-zero} \}.
\]

**Theorem 1:** With notations as above. Let \( f \) be a rational function of \( E \) over \( \mathbb{Z}_N \) such that \( f_p \) and \( f_q \) are nonconstant rational functions of \( E \) over \( \mathbb{Z}_p \) and \( \mathbb{Z}_q \), respectively. For any \( \lambda \in \mathbb{Z}_N \setminus \{0\} \) and \( \beta \in \mathbb{Z}_M \), the following bound holds:

\[
\left| \sum_{\substack{z \in \mathbb{Z}_N \setminus \{0\} \atop f \circ (iq)(z) \neq 0}} e_T(\alpha f(iq)(z))e_M(i\beta) \right| \ll \begin{cases} \text{deg}(f_p) \text{deg}(f_q) N^\frac{t}{2}, & \text{if } \lambda \in \mathbb{Z}_N^*, \\ \text{deg}(f_q) q^\frac{t}{2} M_p, & \text{if } p | \lambda, \\ \text{deg}(f_p) p^\frac{t}{2} M_q, & \text{if } q | \lambda, \end{cases}
\]

Proof. See Appendix A.

**Corollary 1:** With assumptions as in Theorem 1 and \( L \leq M \), the bound of incomplete sums holds for fixed integers \( a \geq 0 \) and \( 1 \leq b \leq M - 1 \):

\[
\sum_{\substack{0 \leq i \leq L-1 \atop f \circ (ia+ib)(z) \neq 0}} e_T(\alpha f((ia+ib)Q)) \ll \begin{cases} \text{deg}(f_p) \text{deg}(f_q) N^\frac{t}{2} \log M, & \text{if } \lambda \in \mathbb{Z}_N^*, \\ \text{deg}(f_q) q^\frac{t}{2} M_p \log M, & \text{if } p | \lambda, \\ \text{deg}(f_p) p^\frac{t}{2} M_q \log M, & \text{if } q | \lambda. \end{cases}
\]

Proof. See Appendix A. The proof will be based on the following basic statements on exponential sums.

**Lemma 2** [21]: For any integer \( \lambda \),

\[
\sum_{z=0}^{m-1} e_m(z\lambda) = \begin{cases} m, & \text{if } \lambda \equiv 0 \pmod{m}; \\ 0, & \text{otherwise}. \end{cases}
\]

**Lemma 3** [21]: For any integer \( h \) and \( 1 \leq l \leq m \), the following bound holds

\[
\sum_{j=0}^{m-1} \sum_{\substack{z=0 \atop z \equiv h \pmod{l}}}^{m-1} e_m(z\lambda) \leq m(1 + \log m).
\]

3. **Application: Elliptic Curve Bit Generators**

Recent developments point towards an attractive interest in the elliptic curve analogues of pseudo-random number generators over finite fields (abbr. EC-generators). Sequences generated from these EC-generators might possess ‘good’ cryptographic properties and hence provide strong potential applications, see the recent survey [22].

In particular, elliptic curves over finite fields have also been used to generate binary sequences in the last decades. To the best of our knowledge, Kaliski first applied elliptic curves to constructing binary sequences by using the elliptic curve discrete logarithm [12]. Gong, Berson and Stinson constructed a class of binary sequences by applying trace functions to elliptic curves over finite fields of characteristic 2 [8]. Goubin, Mauduit and Sárközy presented five constructions of binary sequences in [9] and conjectured that such sequences possess strong pseudorandomness, which has been proved by Xiao and the second author in [4]. Other elliptic curve binary sequences are presented in [2], [3], [5], [18].

In this section, we will apply elliptic curves over residue class ring \( \mathbb{Z}_N \) to constructing a large family of binary sequences with strong pseudorandomness in terms of the well-distribution measure and the correlation measure, introduced by Mauduit and Sárközy [19].

For a finite binary sequence \( S_T = \{s_1, \ldots, s_T\} \in [0, 1]^T \), the well-distribution measure of \( S_T \) is defined by

\[
W(S_T) = \max_{a,b,t} \left| \sum_{j=0}^{T-1} (-1)^{s_{j+a} s_{j+b}} \right|.
\]
where the maximum is taken over all \(a, b, t \in \mathbb{N}\) such that \(1 \leq a \leq a + (t - 1)b \leq T\), and the correlation measure of order \(\ell\) of \(S_T\) is defined as

\[
C_\ell(S_T) = \max_{D_L} \left| \sum_{i=1}^{L} (-1)^{y_{d_1} + \cdots + y_{d_L}} \right|
\]

where the maximum is taken over all \(D = (d_1, \ldots, d_L)\) and \(L\) such that \(0 \leq d_1 < \cdots < d_L \leq T - L\). One would expect that both measures are “small” in terms of \(T\) (in particular, both are \(o(T)\) as \(T \to \infty\)). In this case, \(S_T\) can be considered as a “good” pseudorandom sequence.

As defined in Sect. 2, \(Q = (Q_p, Q_q) \in E(\mathbb{Z}_N)\) is a rational point of order \(M = M_p M_q\), where \(Q_p \in E(\mathbb{Z}_p)\) is a point of order \(M_p\) and \(Q_q \in E(\mathbb{Z}_q)\) is a point of order \(M_q\) such that \(\gcd(M_p, M_q) = 1\).

From now on, we suppose that \(f = X\) or \(f = Y\) and \(X(G)\) (resp. \(Y(G)\)) denotes the \(X\)-coordinate (resp. \(Y\)-coordinate) of \(G\) for any finite rational point \(G \in E(\mathbb{Z}_N)\).

Since \(iQ\) is a semi-zero point if \(M_p|ii\) or \(M_q|ii\), we suppose \(f(iQ) = f_p(iQ_p)\) if \(M_p|i\) and \(f(iQ) = f_q(iQ_q)\) if \(M_q|i\). We remark again that there are \(M_p + M_q - 1\) semi-zeros in \((Q)\). Let \(f(O) = 0\).

**Construction.** For any \(1 \leq i \leq M\), we define a binary sequence \(S_M = \{s_1, \ldots, s_M\}\) of length \(M = M_p M_q\) as follows:

\[
s_i = \begin{cases} 
0, & \text{if } f(iQ) \text{ is even;} \\
1, & \text{otherwise.}
\end{cases}
\]

(2)

Now for any finite point \(iQ\) (except semi-zeros and \(O\)), by Eq. (2), we have

\[
\frac{1}{N} \sum_{r=0}^{(N-1)/2} \sum_{i=1}^{N-1} e_N(\lambda f(iQ) - 2r) = \begin{cases} 
1, & \text{if } f(iQ) \text{ is even,} \\
0, & \text{otherwise.}
\end{cases}
\]

(3)

and

\[
\frac{1}{N} \sum_{r=1}^{(N-1)/2} \sum_{i=0}^{N-1} e_N(\lambda f(iQ) + 2r) = \begin{cases} 
0, & \text{if } f(iQ) \text{ is even,} \\
1, & \text{otherwise.}
\end{cases}
\]

(4)

Then (3) minus (4), we get

\[
\frac{1}{N} \sum_{r=0}^{(N-1)/2} \sum_{i=1}^{N-1} e_N(\lambda f(iQ)) V(\lambda) = \begin{cases} 
1, & \text{if } f(iQ) \text{ is even,} \\
-1, & \text{otherwise.}
\end{cases}
\]

where

\[
V(\lambda) = \sum_{r=0}^{(N-1)/2} e_N(-2\lambda r) - \sum_{r=1}^{(N-1)/2} e_N(2\lambda r).
\]

(5)

So for any finite point \(iQ\), we have

\[
(-1)^{h} = \frac{1}{N} \sum_{r=0}^{N-1} e_N(\lambda f(iQ)) V(\lambda).
\]

(6)

We will consider the well-distribution measure and the correlation measure of order 2 of \(S_M\), which is the most interesting case for pseudorandom sequences. We also need the following statements.

**Lemma 4:** Let \(V(\lambda)\) be defined as in Eq. (5). Then the following bounds hold:

\[
\sum_{\lambda \in \mathbb{Z}_N} |V(\lambda)| \ll N \log N; \quad \sum_{\lambda \in \mathbb{Z}_N} |V(\lambda)| \ll q \log q;
\]

\[
\sum_{\lambda \in \mathbb{Z}_N} |V(\lambda)| \ll p \log p.
\]

Proof. Since

\[
|V(\lambda)| \leq \left| \sum_{r=0}^{(N-1)/2} e_N(-2\lambda r) \right| + \left| \sum_{r=1}^{(N-1)/2} e_N(2\lambda r) \right|
\]

by Lemma 3, we have

\[
\sum_{\lambda \in \mathbb{Z}_N} |V(\lambda)| < \sum_{\lambda \in \mathbb{Z}_N} \left| \sum_{r=0}^{(N-1)/2} e_N(-2\lambda r) \right| + \sum_{\lambda \in \mathbb{Z}_N} \left| \sum_{r=1}^{(N-1)/2} e_N(2\lambda r) \right|
\]

\[
\ll N \log N.
\]

On the other hand,

\[
\sum_{\lambda \in \mathbb{Z}_N} |V(\lambda)| = \sum_{\lambda \in \mathbb{Z}_N} |V(p\lambda_1)|
\]

\[
< \sum_{\lambda_1} \sum_{r=0}^{(N-1)/2} \left| e_N(-2p\lambda_1 r) \right| + \sum_{\lambda_1} \sum_{r=1}^{(N-1)/2} \left| e_N(2p\lambda_1 r) \right|
\]

\[
= \sum_{\lambda_1} \sum_{r=0}^{(N-1)/2} \left| e_N(-2\lambda_1 r) \right| + \sum_{\lambda_1} \sum_{r=1}^{(N-1)/2} \left| e_N(2\lambda_1 r) \right|
\]

Using Lemma 2 for the inner sums and Lemma 3, we get the desired result. The third desired result follows similarly. □

Now we present upper bounds on the well-distribution measure and the correlation measure of order 2 of \(S_M\). The proofs will be based on the exponential sums in Sect. 2.

**Theorem 2:** Let \(S_M\) be the binary sequence defined as in Eq. (2). Then the bound of the well-distribution measure of \(S_M\) holds:

\[
W(S_M) \ll N^{1/2} \log N \log M.
\]

Proof. See Appendix B. □

**Theorem 3:** Let \(S_M\) be the binary sequence defined as in Eq. (2). Then the bound of the correlation measure of order 2 of \(S_M\) holds:

\[
C_2(S_M) \ll N^{3/4}(\log N)^2 \log M.
\]

Proof. See Appendix C. □

For estimates on the correlation measure of higher order, we would meet a complicated mathematical problem. However, it seems that the idea of [20] might be helpful.

4. **Conclusion**

We present an estimate of certain exponential sums on the
points of elliptic curves over $\mathbb{Z}_{pq}$ and use it to analyze the pseudorandomness of a family of binary sequences. One can construct other family binary sequences $s'_M = \{s'_1, \ldots, s'_M\}$ by defining

$$s'_i = \begin{cases} 
0, & \text{if } 0 \leq f(i(Q)) < N/2; \\
1, & \text{otherwise.}
\end{cases}$$

The pseudorandomness can be studied in a similar way. It would be interesting to study other cryptographic properties, such as linear complexity.

**Acknowledgements**

The authors wish to thank the editor and the reviewer for their valuable comments.

**References**


**Appendix A**

**Proof of Theorem 1.** We note that there are at most $\deg(f_q) + \deg(f_p) + \deg(e) + \deg(f)$ rational points $iQ \in \mathbb{Q}$ such that $f(iQ) = \infty$, since $f(iQ) = \infty$ if and only if $f_q(iQ) = \infty$ or $f_p(iQ) = \infty$. It is easy to see that

$$f(iQ) \equiv q^{-1}f_p(iQ) + p^{-1}f_q(iQ) \pmod{N}$$

by the Chinese Remainder Theorem (CRT), where $qq^{-1} \equiv 1 \pmod{p}$ and $pp^{-1} \equiv 1 \pmod{q}$ with integers $p^{-1}$ and $q^{-1}$.

If $\ell \in \mathbb{Z}^*$, there exist integers $\lambda_1 \in \mathbb{Z}_p$ and $\lambda_2 \in \mathbb{Z}_q$ such that $\ell = \lambda_1 + \lambda_2$ by the CRT. Similarly, for any $i \in \mathbb{Z}_M$ there exist unique $u \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_q$ such that $i = uM_q + vM_p$ since gcd$(M_p, M_q) = 1$. By Lemma 1, we have the following Eq. (A·1). The last inequality of Eq. (A·1) holds by Eq. (1) and $2 < p < q < 2p$. If $p|\lambda$, let $\lambda = p\lambda_1$ with $(\lambda, q) = 1$, then we have

$$\sum_{\substack{0 \leq |\ell| < M_p, \\ f(iQ) \neq \infty}} \mathbf{e}_N(\lambda f(iQ)) = \sum_{\substack{0 \leq |\ell| < M_p, \\ f(iQ) \neq \infty}} \mathbf{e}_N(\lambda f(iQ)) \mathbf{e}_M(i\beta) \leq M_p \sum_{\substack{0 \leq |\ell| < M_p, \\ f(iQ) \neq \infty}} \mathbf{e}_N(\lambda f(iQ)) = \sum_{\substack{0 \leq |\ell| < M_p, \\ f(iQ) \neq \infty}} \mathbf{e}_N(\lambda f(iQ)) \mathbf{e}_M(i\beta) + M_p$$

$$\ll \deg(f_q)q^{1/2}M_p.$$
\[ \sum_{j=0}^{L-1} \sum_{j=0}^{M-1} e_N(\lambda f(iQ)) \cdot \frac{1}{M} \sum_{j=0}^{M-1} e_M(\mu(i - (a + jb))) = \frac{1}{N} \sum_{j=0}^{N-1} V(\lambda) \sum_{j=0}^{t-1} e_N(\lambda f((a + jb)Q)) + M_p + M_q \]

\[ \leq \frac{t}{N} \sum_{j=0}^{N-1} |V(\lambda)| \cdot \sum_{j=0}^{t-1} e_N(\lambda f((a + jb)Q)) + M_p + M_q \]

Suppose \( d = \gcd(b, M) \). Using Lemma 3 we have

\[ \sum_{\mu=0}^{M-1} e_M(\mu) \cdot \sum_{j=0}^{L-1} e_N(\lambda f(iQ)) \cdot e_M(\mu) = M \sum_{\mu=0}^{M-1} e_M(\mu) \cdot e_M(\mu) = d \sum_{\mu=0}^{M/d-1} e_M(\mu) \cdot e_M(\mu/d) \]

\[ \ll dM/d \log M/d \ll M \log M. \]

We note that in the inner sums above, we will use Lemma 2 if \( L \geq M/d \). Now the desired result follows by Theorem 1. \( \Box \)

**Appendix B**

**Proof of Theorem 2.** For any \( a, b, t \in \mathbb{N} \) with \( 1 \leq a \leq a + (t - 1)b \leq M \), from Eq. (6) we have

\[ \sum_{j=0}^{t-1} (-1)^{j+a+b} \ll \frac{t}{N} + N^{1/2} \log N \log M \]

By Lemma 4 and Corollary 1, after simple calculations we have

\[ \frac{M_p}{p} \cdot q^{1/2} \log q \log M + \frac{M_q}{q} \cdot p^{1/2} \log p \log M + M_p + M_q. \]
We note that \( \deg(f_{p}) = \deg(f_{q}) \leq 3 \) since \( f = X \) or \( f = Y \). From Eq. (1), we see that \( \frac{p}{q} < 2 \) and \( \frac{q}{p} < 2 \). Then the desired result follows. \( \square \)

Appendix C

Proof of Theorem 3. For \( D = (d_1, d_2) \) and \( L \) with \( 0 \leq d_1 < d_2 \leq M - L \), we have

\[
\sum_{i=1}^{L} (-1)^{\sum_{j=1}^{i} d_j + s_i + d_2} \leq \left| \sum_{i=1}^{L} \sum_{\substack{j=1, j \neq i \mod q \mod \mathbb{N} \neq 0}}^{N-1} \frac{N-1}{N} V(\lambda_i)V(\lambda_j) \sum_{k=1}^{L} \epsilon_N(\lambda_k f((i + d_1)Q)) \right| + 2(M_p + M_q).
\]

We note that \( V(0) = 1 \). If \( \lambda_1 = \lambda_2 = 0 \), the inner sums above is at most \( L \). It suffices to compute for \( k = 1 \) and \( k = 2 \)

\[
T_1 := \left| \sum_{\lambda_1=1}^{N-1} V(\lambda_1) \sum_{\substack{i=1, i \neq j \mod q \mod \mathbb{N} \neq 0}}^{N-1} \frac{N-1}{N} V(\lambda_j) \epsilon_N(\lambda_k f((i + d_1)Q)) \right|
\]

and

\[
T_2 := \left| \sum_{\lambda_1, \lambda_2=1}^{N-1} V(\lambda_1)V(\lambda_2) \sum_{\substack{i=1, i \neq j \mod q \mod \mathbb{N} \neq 0}}^{N-1} \frac{N-1}{N} V(\lambda_j) \epsilon_N(\lambda_k f((i + d_1)Q)) \right|.
\]

For computing \( T_1 \), we need to consider three cases:

\( \lambda_k \in \mathbb{Z}_N^* \), \( p|\lambda_k \) and \( q|\lambda_k \). By Lemma 4 and Corollary 1, we get

\[
T_1 \ll N^{3/2} \log N \log M + q^{3/2} M_p \log q \log M
\]

\[
+ p^{3/2} M_q \log p \log M \ll N^{3/2} \log N \log M.
\]

Similarly, for computing \( T_2 \), we need to consider three cases: \( \gcd(\lambda_1, \lambda_2, N) = 1 \), \( p|\gcd(\lambda_1, \lambda_2) \) and \( q|\gcd(\lambda_1, \lambda_2) \). On the other hand, we should take into account the restrictions on \( d_1, d_2 \) as follows:

Case (1). If \( d_1 \neq d_2 \) (mod \( M_p \)) and \( d_1 \neq d_2 \) (mod \( M_q \)), then \( F := \lambda_1 f \circ \tau_{d_1} + \lambda_2 f \circ \tau_{d_2} \) is not constant over \( \mathbb{Z}_N \) (and \( \mathbb{Z}_{M_p}, \mathbb{Z}_{M_q} \)) since \( \equiv d_1 Q, \equiv d_2 Q \) are poles of \( F \). Then by Lemma 4 and Corollary 1, we get

\[
T_2 \ll N^{3/2} (\log N)^2 \log M + q^{5/2} M_p (\log q)^2 \log M
\]

\[
+ p^{5/2} M_q (\log p)^2 \log M \ll N^{3/2} (\log N)^2 \log M.
\]

Case (2). If \( d_1 \equiv d_2 \) (mod \( M_p \)), in which case we have \( d_1 \neq d_2 \) (mod \( M_q \)) since \( \gcd(M_p, M_q) = 1 \), then using the proof of Theorem 1, and by Lemma 4 and Corollary 1 again, we get

\[
T_2 \ll N^{3/2} (\log N)^2 q^{1/2} M_p \log M + q^{5/2} M_p (\log q)^2 \log M
\]

\[
+ p^2 (\log p)^2 L \ll N^{11/4} (\log N)^2 \log M.
\]

We also get the same bound for the case \( d_1 \equiv d_2 \) (mod \( M_q \)).

Putting everything together, for any \( D = (d_1, d_2) \) we obtain

\[
\sum_{i=1}^{L} (-1)^{\sum_{j=1}^{i} d_j + s_i + d_2} \ll \frac{1}{N^2} \left( L + 2N^{3/2} \log N \log M + N^{11/4} (\log N)^2 \log M \right)
\]

\[
+ 2(M_p + M_q) \ll N^{3/2} (\log N)^2 \log M. \square
\]