THE DISTRIBUTION OF SOLUTIONS TO QUADRATIC POLYNOMIALS OVER FINITE RINGS

ALI H. HAKAMI

Department of Mathematics
Faculty of Science
Jazan University
P. O. Box 277, Jazan
Postal Code 45142
Saudi Arabia
e-mail: aalhakami@jazanu.edu.sa

Abstract

Let $m$ be a positive integer. Denote to the ring $\mathbb{Z}/(m)$ by $R_m$, and a Cartesian product of $n$ copies of $\mathbb{Z}/(m)$ by $R^m_n$. Let $f(x)$ be a quadratic polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$. Write $f(x) = Q(x) + a \cdot x + c$, where $a \in \mathbb{Z}^n$, $c \in \mathbb{Z}$, and $Q(x)$ is a quadratic form given by $Q(x) = \frac{1}{2} x A x^T$, where $A$ is a symmetric $n \times n$ matrix with integer entries. Assume $\gcd(\det A, m) = 1$, unless we mention else. Let $V$ be the set of points in $R^m_n$ satisfying the congruence $f(x) \equiv 0 \pmod{m}$. If $d|m$ and $x, y \in R^m_n$, we shall say $x \equiv y \pmod{d}$ if $x$ is congruent to $y$ modulo the ideal $dR_m$. For any subset $S$ of $R^m_n$ and divisor $d$ of $m$, let $\gamma(S, d) = |\{ (s_1, s_2) \in S \times S : s_1 \equiv s_2 \pmod{d} \}|$, where $|$ denote to the cardinality. Let $\phi$ denote the Euler phi-function, $\tau(m)$ denote the number of distinct positive divisors of $m$, and for positive integers $m, n$ set 2010 Mathematics Subject Classification: 11D79, 11E08, 11H50, 11H55.

Keywords and phrases: quadratic polynomials, congruences.

Received September 12, 2012

© 2012 Scientific Advances Publishers
In this paper, we shall prove that for any subsets $S$ and $T$ of $R^m_n$, with $|S| \leq |T|$, we have

$$|(S + T) \cap V| \geq m^{-1}|T| - m^{-1}|S|^{-1} \sum_{d \mid m, d \neq m} \phi(d)d^{n/2} \eta(S, d)^{1/2} \eta(T, d)^{1/2}. $$

We also show that the above result can be made more precise when $S + T$ is a box of points in $R^m_n$.

1. Introduction

Let $R_m = \mathbb{Z}_m$ be a finite ring. Let $f(x)$ be a quadratic polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$. We can write

$$f(x) = Q(x) + a \cdot x + c, \tag{1}$$

where $a \in \mathbb{Z}^n$, $c \in \mathbb{Z}$, and $Q(x)$ is a quadratic form given by

$$Q(x) = \frac{1}{2} x A x^T, \tag{2}$$

where $A$ is a symmetric $n \times n$ matrix with integer entries. Throughout this paper (with the exception of Lemma 2), we shall assume that $\gcd(\det A, m) = 1$. Let $V$ be the algebraic subset of $R^m_n$ defined by

$$f(x) \equiv 0 \pmod{m}.$$

If $d \mid m$ and $x, y \in R^m_n$, we shall say that $x \equiv y \pmod{d}$ if $x$ is congruent to $y$ modulo the ideal $dR_m$. For any subset $S$ of $R^m_n$ and divisor $d$ of $m$, let

$$\eta(S, d) = |\{(s_1, s_2) \in S \times S : s_1 = s_2 \pmod{d}\}|.$$

Let $\phi$ denote the Euler phi-function, $\tau(m)$ denote the number of distinct positive divisors of $m$, and for positive integers $m, n$ set
Our main result is

**Theorem 1.** For any subsets $S$ and $T$ of $R^n_1$, with $|S| \leq |T|$, we have

$$|(S + T) \cap V| \geq m^{-1}|T| - m^{-1}|S|^{-1} \sum_{d \geq m} \phi(d)^{n/2} \eta(S, d)^{1/2} \eta(T, d)^{1/2}.$$  

The proof of the theorem will be given latter in Section 3. The result can be made more precise when $S + T$ is a box of points in $R^n_m$, that is, the image $\overline{B}$ of a box $B$ in $Z^n$ under the canonical mapping of $Z^n$ onto $R^n_m$, where

$$B = \{x \in Z^n : a_i \leq x_i < a_i + m_i\}, \quad (3)$$

for some $a_i, m_i \in Z$ with $0 < m_i \leq m, 1 \leq i \leq n$. In this case, we obtain

**Corollary 1.** Suppose that $n \geq 4$. Let $\overline{B}$ be a box in $R^n_m$, whose sides are all of the same length $M < m$, that is, let $\overline{B}$ be the image of a box $B$ as given in (3), where $m_i = M, 1 \leq i \leq n$. Put $c = [(M + 1) / 2]$. Then

$$|\overline{B} \cap V| \geq \frac{c^n}{m} \left(1 - \Phi_n(m) - 2^n \frac{\tau(m)}{c} - \frac{m^{(m/2)+1}}{c^n} \left(2^n \frac{c}{m} + 1\right)\right).$$

In particular, if $n \geq 6$ and $M >> m^{1/2+1/n}$, then $\overline{B} \cap V$ is nonempty.

The second part of the corollary follows immediately from Lemma 1 of next section. The first part of the corollary will be proven after the proof of Theorem 1.
2. Lemmas

Lemma 1. If \( n \geq 4 \), then for any integer \( m > 1 \),

\[
\Phi_n(m) \leq \prod_{p|m} \left( 1 + p^{1-(n/2)} \right) - 1,
\]

where the product is over all primes \( p \) dividing \( m \). In particular, if \( n \geq 6 \), then for all \( m > 1 \), \( \Phi_n(m) \leq 2^{2-(n/2)} \).

Proof. Let \( s = n / 2 \) and set \( g(m) = \sum_{d|m} \phi(d)d^{-s} \), so that \( \Phi_n(m) = g(m) - 1 \). Since \( \phi(d) \) and \( d^{-s} \) are both multiplicative, \( g(m) \) is multiplicative. If \( p \) is a prime and \( e \geq 1 \), then

\[
g(p^e) = 1 + \sum_{i=1}^{e} \left( p^i - p^{i-1} \right)p^{-si}
\]

\[
= 1 + \left( 1 - p^{-1} \right) \sum_{i=1}^{e} p^{(1-s)i}
\]

\[
< 1 + \left( 1 - p^{-1} \right)p^{1-s} \sum_{i=0}^{\infty} p^{(1-s)i}
\]

\[
= 1 + p^{1-s} \frac{1 - p^{-1}}{1 - p^{1-s}}
\]

\[
\leq 1 + p^{1-s},
\]

the last inequality follows since \( s \geq 2 \). The first part of the lemma now follows from the multiplicative property of \( g(m) \).

Now suppose that \( n \geq 6 \). Again, letting \( s = n / 2 \), we can say that

\[
\Phi_n(m) \leq \sum_{d=2}^{\infty} \phi(d)d^{-s} \leq \frac{1}{2^s} + \frac{2}{3^s} + \frac{2}{4^s} + \sum_{d=5}^{\infty} d^{1-s},
\]

since \( \phi(d) < d \). But
\[
\sum_{d=5}^{\infty} d^{1-s} < \int_{4}^{\infty} x^{1-s} dx = (s - 2)^{-1} 4^{2-s}.
\]

Thus,
\[
\Phi_n(m) < \frac{1}{2^s} \left( 1 + 2 \left( \frac{2}{3} \right)^s + \frac{1}{2^{s-1}} + \frac{1}{2^{s-4}(s - 2)} \right)
\]
\[
\leq \frac{1}{2^s} \cdot 4, \quad \text{for} \quad s \geq 3.
\]

To prove Theorem 1, we make use of exponential sums. Let
\[e_m(x) = e^{\frac{2\pi i x}{m}}.\]

We shall abbreviate complete sums \(\sum_{x \in R_m^n} (\cdot)\) by simply \(\sum_x (\cdot)\). Also, we shall need to use the following fundamental identity:

For any \(y \in R_m^n\),
\[
\sum_x e_m(x \cdot y) = \begin{cases} m^n, & \text{if } y = 0, \\ 0, & \text{if } y \neq 0. \end{cases} \tag{5}
\]

Let \(f(x)\) and \(Q(x)\) be as defined by (1) and (2). By viewing \(R_m^n\) as a \(\mathbb{Z}\)-module, the Gauss sums
\[
G_m(Q, y) = \sum_{x \in R_m^n} e_m(Q(x) + y \cdot x),
\]
and
\[
G_m(f, y) = \sum_{x \in R_m^n} e_m(f(x) + y \cdot x),
\]
are well defined whether we take \(y \in \mathbb{Z}^n\) or \(y \in R_m^n\).

For any \(n \times n\) matrix \(A\) with integer entries, we define \(\ker_m(A)\) by
\[
\ker_m(A) = \{x \in R_m^n : Ax^T = 0^T (\text{mod } m)\}.
\]
We need the following lemmas:

**Lemma 2** ([5, Equation (13)]). Let \( Q(x) \) be a quadratic form given by (2), where now we allow \( A \) to be any symmetric integral matrix with even diagonal entries. Then given \( y \in R^n_m \), the Gauss sum \( G_m(Q, y) \) is zero unless \( Q(x) + y \cdot x \equiv 0 \pmod{m} \) for all \( x \in \ker_m(A) \), in which case \[ |G_m(Q, y)|^2 = m^n|\ker_m(A)|. \]

**Lemma 3.** Let \( f(x) \) be a quadratic polynomial as given by (1) with \( \gcd(\det A, m) = 1 \). Let \( y \in \mathbb{Z}^n, \lambda \in \mathbb{Z}, \lambda \neq 0 \pmod{m} \), and set \( d = (\lambda, m) \). Then

\[
|G_m(\lambda f, y)| = \begin{cases}
(md)^{n/2}, & \text{if } y \equiv 0 \pmod{d}, \\
0, & \text{if } y \not\equiv 0 \pmod{d}.
\end{cases}
\]

**Proof.** By (1), we have

\[
|G_m(\lambda f, y)| = \sum_x e_m(\lambda f(x) + y \cdot x) = \sum_x e_m(\lambda Q(x) + (\lambda a + y) \cdot x + \lambda c) = \sum_x e_m(\lambda Q(x) + (\lambda a + y) \cdot x).
\]

Now \( \lambda Q(x) = \frac{1}{2}x(\lambda A)x^T \), so that by Lemma 2, \( G_m(\lambda f, y) = 0 \) unless \( y \) satisfies the following condition:

For all \( x \in \ker_m(\lambda A), \ (\lambda a + y) \cdot x + \lambda Q(x) \equiv 0 \pmod{m}. \) \hfill (6)

Now

\[
\ker_m(\lambda A) = \{x \in R^n_m : \lambda Ax^T \equiv 0 \pmod{m}\}
\]

\[
= \{x \in R^n_m : Ax^T \equiv 0 \pmod{m/d}\},
\]

but as \( \gcd(\det A, m) = 1 \), we conclude that
\[
\ker_m(\lambda A) = \{ x \in R^m_m : x \equiv 0 \pmod{m/d} \}. \tag{7}
\]
Thus, setting \( x = (m/d)t \pmod{m} \), we see that (6) is equivalent to saying that for all \( t \in \mathbb{Z}^n \),
\[
\lambda \left( \frac{m}{d} \right) a \cdot t + \left( \frac{m}{d} \right) y \cdot t + \lambda \left( \frac{m}{d} \right)^2 Q(t) \equiv 0 \pmod{m}. \tag{8}
\]
But \( \lambda \left( \frac{m}{d} \right) = m \left( \frac{\lambda}{d} \right) \equiv 0 \pmod{m} \) and similarly \( \lambda \left( \frac{m}{d} \right)^2 = m \left( \frac{\lambda}{d} \right)^2 \equiv 0 \pmod{m} \) so that (8) simplifies to the congruence \( \left( \frac{m}{d} \right) y \cdot t \equiv 0 \pmod{m} \), that is, \( y \cdot t \equiv 0 \pmod{d} \). Hence \( y \) satisfies (6), if and only if for all \( t \in \mathbb{Z}^n \), \( y \cdot t = 0 \pmod{d} \), that is, \( y = 0 \pmod{d} \). If \( y = 0 \pmod{d} \), then by Lemma 2 and (7), we have
\[
|G_m(\lambda f, y)|^2 = m^2 |\ker_m(\lambda A)| = m^n d^n. \quad \square
\]

3. Proof of Theorem 1

Let \( S, T \) be subsets of \( R^n_m \), and \( V \) be the set of points in \( R^n_m \) satisfying \( f(x) = 0 \pmod{m} \). Let \( N \) be the number of triples \( (s, t, v) \in S \times T \times V \) such that \( s + t = v \pmod{m} \). By the fundamental identity (5),
\[
N = m^{-n} \sum_{x \in V} \sum_{s \in S} \sum_{t \in T} \sum_{y} e_m(y \cdot (s + t - x))
\]
\[
= m^{-n-1} \sum_{x \in R^n_m} \left[ \sum_{\lambda \in R_m} e_m(\lambda f(x)) \right] \sum_{s \in S} \sum_{t \in T} \sum_{y} e_m(y \cdot (s + t - x))
\]
\[
= m^{-n-1} \sum_{\lambda} \sum_{y} \Psi(y) \sum_{x} e_m(\lambda f(x) - x)),
\]
where

\[ \Psi(y) = \sum_{s \in S} \sum_{t \in T} e_m(y \cdot (s + t)). \]

Peeling off the \( \lambda = 0 \) term yields

\[ N = m^{-1} |S| \cdot |T| + m^{-n-1} \sum_{\lambda \neq 0} \sum_{y} \Psi(y) \sum_{x} e_m(\lambda f(x) - y \cdot x). \quad (9) \]

Thus (from (9)),

\[ N - m^{-1} |S| \cdot |T| = m^{-n-1} \sum_{1 \leq \lambda < m} \sum_{y} \Psi(y) \sum_{x} e_m(\lambda f(x) - y \cdot x), \]

so that by Lemma 3,

\[ |N - m^{-1} |S| \cdot |T|| \leq m^{-n-1} \sum_{d \mid m} \sum_{\lambda \leq m \leq \lambda d = d} m^{n/2} d^{n/2} \sum_{y}^{*} |\Psi(y)|, \]

where the sum on \( y \) is over all \( y \equiv 0 \) (mod \( d \)). On replacing \( d \) by \( m/d \) and \( \sum_{y}^{*} \) by \( \sum_{y}^{**} \), the sum over all \( y \equiv 0 \) (mod(\( m/d \))), we obtain

\[ |N - m^{-1} |S| \cdot |T|| \leq m^{-n/2-1} \sum_{d \mid m} \phi \left( \frac{m}{d} \right) d^{n/2} \sum_{y}^{**} |\Psi(y)| \]

\[ = m^{-1} \sum_{d \geq 1} \sum_{d \mid m} \phi(d) d^{-n/2} \sum_{y}^{**} |\Psi(y)|. \quad (10) \]

Now,

\[ \sum_{y}^{**} |\Psi(y)||\Psi(y)| = \sum_{y} \sum_{s \in S} \sum_{t \in T} e_m(y \cdot s) \sum_{t \in T} e_m(y \cdot t) \]

\[ \leq \left[ \sum_{y} \sum_{s \in S} e_m(y \cdot s) \right]^{2^{-1/2}} \left[ \sum_{y} \sum_{t \in T} e_m(y \cdot t) \right]^{2^{-1/2}}. \quad (11) \]
Setting $y = (m/d)u(\text{mod } m)$, and letting $u$ run through a complete set of representatives for $R^n_d$, we can say

$$\sum_{y}^{**} \left| \sum_{t \in T} e_m(y \cdot t) \right|^2 = \sum_{y}^{**} \sum_{s_1 \in S} \sum_{s_2 \in S} e_m(y \cdot (s_1 - s_2))$$

$$= \sum_{s_1 \in S} \sum_{s_2 \in S} \sum_{y}^{**} e_m(y \cdot (s_1 - s_2))$$

$$= \sum_{s_1 \in S} \sum_{s_2 \in S} \sum_{u \in R^n_d} e_m\left(\frac{m}{d} u \cdot (s_1 - s_2)\right)$$

$$= \sum_{s_1 \in S} \sum_{s_2 \in S} \sum_{u} e_d(u \cdot (s_1 - s_2))$$

$$= d^n \eta(S, d).$$

Thus, by (11),

$$\sum_{y}^{**} |\Psi(y)| \leq d^n \eta(S, d)^{1/2} \eta(T, d)^{1/2},$$

and therefore by (10),

$$|N - m^{-1} |S||T| \leq m^{-1} \sum_{d \mid m} \phi(d) d^{-n/2} d^n \eta(S, d)^{1/2} \eta(T, d)^{1/2}.$$  \hspace{1cm} (12)

Theorem 1 now follows on observing that $|(S + T) \cap V| \geq N/|S|^{-1}$. This inequality holds for there are at most $|S|$ ways of representing any point $x$ as a sum $s + t$ with $s \in S$ and $t \in T$.

**4. Proof of Corollary 1**

Let

$$B = \{ x \in \mathbb{Z}^n : a_i \leq x_i < a_i + M, 1 \leq i \leq n \},$$
\[ S = \{ x \in \mathbb{Z}^n : 0 \leq x_i < c \}, \]
\[ T = S + (a_1, a_2, \ldots, a_n), \]
for some \( a_i \in \mathbb{Z}, 1 \leq i \leq n \), where \( c = \left\lceil \frac{M+1}{c} \right\rceil \). Let \( \overline{B}, \overline{S}, \overline{T} \) be the images of \( B, S, \) and \( T \) in \( R_m^n \) under the canonical mapping of \( \mathbb{Z}^n \) onto \( R_m^n \). Then \( \overline{S} + \overline{T} \subset \overline{B} \) and \( |\overline{S}| = |\overline{T}| = \left\lceil \frac{M+1}{c} \right\rceil^n \geq 2^{-n}|B| \). We claim that for any divisor \( d \) of \( m \),
\[ \eta(\overline{S}, d) \leq c^n \left( \frac{c}{d} + 1 \right)^n, \quad (13) \]
and that the same inequality holds for \( \eta(\overline{T}, d) \). Let \( s = (s_1, \ldots, s_n) \) be a fixed point in \( S \). If \( u = (u_1, \ldots, u_n) \) is a point in \( S \) such that \( u \equiv s \pmod{d} \), then \( u_i = s_i + dk_i \), for some \( k_i \in \mathbb{Z}, 1 \leq i \leq n \). Since \( 0 \leq u_i < c \), there are at most \( \left\lceil \frac{c}{d} \right\rceil + 1 \) choices for each \( u_i \), and thus at most \( \left( \frac{c}{d} + 1 \right)^n \) choices for \( u \). Since \( |S| = c^n \), we obtain (13). It is clear that \( \eta(\overline{S}, d) = \eta(\overline{T}, d) \) so that (13) holds also for \( \eta(\overline{T}, d) \).

We now apply Theorem 1 with \( S \) and \( T \) replaced by the sets \( \overline{S} \) and \( \overline{T} \) just defined. We shall abbreviate the sum \( \sum_{d \mid m} \) by simple \( \sum^* \). From (12) and (13), we have
\[ |N - m^{-1}|S||T| \leq m^{-1} \sum^* \phi(d)d^n/2^nc^n([c/d] + 1)^n \]
\[ \leq m^{-1} \sum^* \phi(d)d^n/2^nc^nd^{-n}(c + d)^n \]
\[ = m^{-1}c^n \sum^* \phi(d)d^{-n/2}c^n(c + d)^n. \]
Now, since \((c + d)^n \leq c^n + 2^n(c^{n-1}d + cd^{n-1}) + d^n\), we have
\[
|N - m^{-1}|S||T|| \leq m^{-1}c^{2n} \sum d^{-n/2} + m^{-1}2^n c^{2n-1} \sum d^{1-n/2} \\
+ m^{-1}2^n c^{n+1} \sum d^{(n/2)-1} + m^{-1}c^n \sum d^{n/2}. \tag{14}
\]
The first sum on the right-hand side of (14) is just \(\Phi_n(m)\). We make crude estimates for the remaining sums. For \(n \geq 4\), we have
\[
\sum d^{-n/2} \leq \sum d^{-1} \leq \sum d^{-1} < \tau(m), \tag{15}
\]
\[
\sum d^{(n/2)-1} \leq m^{n/2-1} \sum d \leq m^{n/2-1} \cdot m = m^{n/2},
\]
\[
\sum d^{n/2} \leq m^{n/2} \sum d \leq m^{n/2+1}.
\]
Thus by (14), we see that
\[
N \geq m^{-1}c^{2n} - m^{-1}c^{2n} \Phi_n(m) - m^{-1}2^n c^{2n-1} \tau(m) \\
- m^{-1}2^n c^{n+1} m^{n/2} - m^{-1}c^n m^{(n/2)-1} \\
= m^{-1}c^{2n} (1 - \Phi_n(m) - 2^n c^{-1} \tau(m) \\
- c^{-n} m^{(n/2)-1} (2^n c^{-1} + 1)).
\]
The corollary now follows from the observation that
\[
|\overline{B} \cap V| \geq |(\overline{S} \cap \overline{T}) \cap V| \geq N|S|^{-1} = Nc^{-n}.
\]

5. Remarks

(1) It is clear from (15) and Lemma 1 that if \(n \geq 8\), then in the statement of Corollary 1, we can replace \(\tau(m)\) by \(2^{3-(n/2)}\).
(2) Let \( f(x) \) be given by (1), \( V \) be the set of zeros of \( f(x) \) in \( R^n_m \) and again suppose that \( \gcd(\det A, m) = 1 \). Lemma 3 provides us with an easy means of estimating \( |V| \). For \( n \geq 4 \), we obtain

\[
|V| = m^{n-1} \prod_{p|m} \left( 1 + \theta_p p^{1-(n/2)} \right),
\]

where the product is over all primes \( p \) dividing \( m \), and for each such \( p \), \( \theta_p \) is a real number of absolute value \( \leq 1 \). Equation (16) follows from the observation that

\[
|V| = m^{-1} \sum_{x \in R^n_m} \sum_{\lambda=0}^{m-1} e(\lambda f(x))
\]

\[
= m^{n-1} + m^{-1} \sum_{\lambda=1}^{m-1} \sum_{x} e(\lambda f(x)).
\]

By Lemma 3, we then have

\[
|V| = m^{n-1} + \theta_m m^{n/2-1} \sum_{1 \leq d < m \atop d|m} \phi\left(\frac{m}{d}\right) d^{n/2},
\]

for some \( \theta_m \in \mathbb{R} \), with \( |\theta_m| \leq 1 \). Since

\[
\Phi_n(m) = \sum_{d>1 \atop d|m} \phi(d) d^{-n/2} = \sum_{1 \leq d < m \atop d|m} \phi\left(\frac{m}{d}\right) \left(\frac{d}{m}\right)^{n/2},
\]

we obtain

\[
|V| = m^{n-1} [1 + \theta_m \Phi_n(m)].
\]

To obtain (16), we apply (17) in turn to each prime power dividing \( m \) and use the Chinese remainder theorem to compute \( |V| \). That is, for each divisor \( d \) of \( m \), we let \( v(d) \) be the number of points in \( R^n_d \) satisfying the
congruence \( f(x) = 0 \) (mod \( d \)). Consequently, if \( m = \prod_{i=1}^s p_i^{e_i} \), then
\[
v(m) = \prod_{i=1}^s v(p_i^{e_i}).\]
Thus, by (17), we have
\[
|V| = v(m) = \prod_{i=1}^s p_i^{e_i(n-1)}(1 + \theta_i \Phi_n(p_i^{e_i})),
\]
for some \( \theta_i \in \mathbb{R} \) with \( |\theta_i| \leq 1 \), \( 1 \leq i \leq s \), and by Lemma 1, we have
\[
\Phi_n(p^e) \leq p^{1-(n/2)},
\]
for any prime power \( p^e \), when \( n \geq 4 \). Equation (16) is now immediate.

Equation (16) indicates that we obtain roughly the expected quota of zeros for \( f(x) \), namely, \( m^{n-1} \), when \( \text{gcd}(\det A, m) = 1 \). When \( \text{gcd}(\det A, m) \neq 1 \), this is no longer the case. For example, suppose that \( m = pq \), where \( p \) and \( q \) are distinct primes. Let \( \alpha \) be a quadratic non-residue (mod \( p \)), \( \beta \) be a quadratic non-residue (mod \( q \)), and \( f(x) = f(x_1, x_2, x_3, x_4) \) be defined by
\[
f(x) = p(x_1^2 - \beta x_2^2) + q(x_3^2 - \alpha x_4^2).
\]
If \( x \) is an integral solution of the congruence \( f(x) = 0 \) (mod \( m \)), then \( x_1^2 - \beta x_2^2 \equiv 0 \) (mod \( q \)) and \( x_3^2 - \alpha x_4^2 \equiv 0 \) (mod \( p \)), so that \( x_1 = x_2 = 0 \) (mod \( q \)) and \( x_3 = x_4 = 0 \) (mod \( p \)). Thus, if \( V \) is the set of points in \( \mathbb{F}_m^4 \) satisfying \( f(x) \equiv 0 \) (mod \( m \)), then \( |V| = p^2q^2 = m^2 \), rather than expected quota of \( m^3 \). This example indicates that Corollary 1 does not hold when \( \text{gcd}(\det A, m) \neq 1 \).

We have not been able to obtain an analogue of Theorem 1 when \( \text{gcd}(\det A, m) \neq 1 \). The main difficulty is that \( \text{ker}_m(\lambda A) \) no longer leads to such a simple description as in the case when \( \text{gcd}(\det A, m) = 1 \); see Equation (7). To overcome this difficulty, one may be able to use the
description of $\ker_m(\lambda A)$ given in Section 4 of [4], which involved the invariant factors of $A$. Another possibility is to use the explicit evaluations of the Gauss sums $G_m(Q, y)$ given by [6, Theorem 2]. But as a warning to the reader, the expression he gives for $G_m(Q, y)$ is a product of terms 8 lines long in very fine print, involving a number of invariant factors associated with $Q$.

(3) If we replace $R_m = \mathbb{Z}/(m)$ by a finite field $\mathbb{F}_q$, then the work of this paper has been investigated before by [1-3, 7-11], for any polynomial.

References


