NNTDM 17 (2011), 1, 30-36

A note on diagonalization of integral quadratic forms modulo p^m

Ali H. Hakami
Department of Mathematics, King Khalid University,
P.O.Box 9004, Abha, Postal Code: 61431, Saudi Arabia,
E-mail: *aalhakami@kku.edu.sa*

Abstract: Let m be a positive integer, p be an odd prime, and $\mathbb{Z}_{p^m} = \mathbb{Z} / (p^m)$ be the ring of integers modulo p^m. Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n)$ be a nonsingular quadratic form with integer coefficients. In this paper we shall prove that any nonsingular quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$, $Q(\mathbf{x})$ is equivalent to a diagonal quadratic form (modulo p^m).
Keywords: Integral quadratic form, Nonsingular quadratic form, Diagonalization quadratic form modulo prime.
AMS Classification: 11E08

1. Introduction

In this section we simply mention the basic concepts of quadratic forms which we shall need throughout. For details the reader is referred to [1], [2], and [3].

A quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$ is a polynomial of the type

$$Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j ,$$

with $a_{ij} \in \mathbb{Z}$, $1 \le i \le j \le n$. We associate with $Q(\mathbf{x})$ a symmetric n×n matrix $A = A_Q$ given by

$$A_Q = \begin{bmatrix} a_{11} & \frac{1}{2}a_{12} & \frac{1}{2}a_{13} & \cdots & \frac{1}{2}a_{1n} \\ \frac{1}{2}a_{21} & a_{22} & \frac{1}{2}a_{23} & \cdots & \frac{1}{2}a_{2n} \\ \frac{1}{2}a_{31} & \frac{1}{2}a_{32} & a_{33} & \cdots & \frac{1}{2}a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2}a_{n1} & \frac{1}{2}a_{n2} & \frac{1}{2}a_{n3} & \cdots & a_{nn} \end{bmatrix}.$$

That is

$$A = [a_{ij}^*]_{n \times n}, \qquad a_{ij}^* = \begin{cases} \frac{1}{2}a_{ij} & for \quad i < j \\ \frac{1}{2}a_{ji} & for \quad i > j \\ a_{ii} & for \quad i = j \end{cases}$$

Observe that

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x}$$

where

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \ \mathbf{x}^t = [x_1 \quad x_2 \quad \ldots \quad x_n].$$

Here $\mathbf{x}^t$ denotes the transpose of the matrix $\mathbf{x}$. On the other hand, note that if the matrix A is diagonal (An $n \times n$ matrix A is diagonal if $a_{ij} = 0$ whenever $i \neq j$), then the corresponding quadratic form Q has the diagonal representation

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x} = a_{11}x_1^2 + \ldots + a_{nn}x_n^2,$$

i.e., the quadratic form will contain no "cross product" terms. In the same way we call Q a diagonal quadratic form (mod p^m) for any prime power p^m if Q contains no "cross product" terms when read (mod p^m). The determinant of Q, abbreviated $\det Q$, is defined to be the determinant of the matrix A_Q. We say that $Q(\mathbf{x})$ is nonsingular over $\mathbb{Z}$ if $\det Q \neq 0$. Similarly for any odd prime power p^m we say $Q(\mathbf{x})$ is nonsingular mod p^m if $p \nmid \det Q$.

Again let p^m be an odd prime power. Let $Q(\mathbf{x})$ and $\widetilde{Q}(\mathbf{x})$ be two quadratic forms over $\mathbb{Z}$ with associated matrices $A_Q, A_{\widetilde{Q}}$, respectively. We now view the entries of these matrices as elements of $\mathbb{Z}/(p^m)$, and regard 1/2 as the multiplicative inverse of 2 (mod p^m). (Alternatively we can replace 1/2 with $(p^m + 1) / 2$ and regard A_Q as having integer entries). We say that $Q(\mathbf{x})$ is equivalent to $\widetilde{Q}(\mathbf{x}) \pmod{p^m}$, written $Q(\mathbf{x}) \sim \widetilde{Q}(\mathbf{x}) \pmod{p^m}$, if there is an invertible $n \times n$ matrix T over $\mathbb{Z}/(p^m)$, such that $\widetilde{Q}(\mathbf{x}) = Q(T\mathbf{x}) \pmod{p^m}$, that is

$$A_{\widetilde{Q}} \equiv T^t A_Q T \pmod{p^m}.$$

It is clear that "$\sim$" is an equivalence relation. Note that

$$\det \widetilde{Q} = \det Q \cdot (\det T)^2 \pmod{p^m}.$$

***Example*:** Let p^m be any odd prime power and $Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2$. Then

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x},$$

where

$$A = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}.$$

That is

$$Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2 = \underbrace{[x_1 \quad x_2]}_{\mathbf{x}^t} \underbrace{\begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}}_{A_Q} \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{\mathbf{x}}.$$

By making the simple observation that

$$Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2 \equiv x_1^2 + \underbrace{(p^m + 1)}_{even} x_1x_2 + x_2^2 \pmod{p^m},$$

we can write

$$Q(\mathbf{x}) \equiv \mathbf{x}^t A' \mathbf{x} \pmod{p^m},$$

with

$$A' = \begin{bmatrix} 1 & \frac{p^m+1}{2} \\ \frac{p^m+1}{2} & 1 \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}).$$

Note that since p is odd, the entries of A' are all integers. Thus we may assume that $A_Q \in M_{2\times 2}(\mathbb{Z})$ when working with congruences modulo odd primes.

2. Diagonalization of quadratic forms modulo p^m

Theorem 1. *For any odd prime power p^m, and nonsingular quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$, $Q(\mathbf{x})$ is equivalent to a diagonal quadratic form (modulo p^m).*

Proof. We proceed by induction on m. When $m = 1$, it is well known (see [4]) that Q can be diagonalized over the finite field $\mathbb{F}_p$. Say

$$T^t A_Q T \equiv D \pmod{p^m},$$

for some $T, D \in M_{n\times n}(\mathbb{Z})$ with T nonsingular (mod p) and D a diagonal matrix. Let us lift this to a solution (mod p^2). Let

$$U = T + pX,$$

where $X = [x_{ij}]$ is a matrix of variables. We wish to solve

$$U^t A_Q U \equiv D \pmod{p^2}$$

This is equivalent to

$$\begin{aligned} & (T+pX)^t A_Q (T+pX) \equiv D \pmod{p^2} \\ \Leftrightarrow \quad & T^t A T + T^t A_Q pX + pX^t A_Q T \equiv D \pmod{p^2} \\ \Leftrightarrow \quad & \frac{T^t A_Q T - D}{p} + \underbrace{T^t A_Q X}_{Y} + X^t A_Q T \equiv 0 \pmod{p} \\ \Leftrightarrow \quad & Y + Y^t \equiv \underbrace{\frac{D - T^t A_Q T}{p}}_{B} \pmod{p} \end{aligned}$$

where $Y = T^t A_Q X$ and $B = (D - T^t A_Q T)/p$. Note that B is a symmetric matrix with integer entries. Let

$$Y \equiv \begin{bmatrix} \frac{1}{2}b_{11} & & & & \\ b_{21} & \frac{1}{2}b_{22} & & & \\ b_{31} & b_{32} & \frac{1}{2}b_{33} & & \\ \vdots & \vdots & \vdots & \ddots & \\ b_{n1} & b_{n2} & b_{n3} & \cdots & \frac{1}{2}b_{nn} \end{bmatrix} \pmod{p^2}.$$

Then $Y + Y^t = B$. Thus, we are left with solving the congruence

$$T^t A_Q X \equiv Y \pmod{p}.$$

Since T and A_Q are nonsingular (mod p), this equation has a unique solution

$$X \equiv A_Q^{-1}(T^t)^{-1}Y \pmod{p}.$$

In the same manner one can lift a solution (mod p^m), to (mod p^{m+1}) for any m. Indeed, proceeding as above, suppose that

$$T^t AT \equiv D \pmod{p^m},$$

for some $T, D \in M_{n\times n}(\mathbb{Z})$ with T nonsingular (mod p) and D a diagonal matrix. Let

$$U = T + p^m X,$$

where X is a matrix of variables and solve

$$U^t A_Q U \equiv D \pmod{p^{m+1}}.$$

This is equivalent to

$$\begin{aligned}
&(T + p^m X)^t A_Q (T + p^m X) \equiv D \pmod{p^{m+1}} \\
\Leftrightarrow\ & T^t A_Q T + T^t A_Q p^m X + p^m X^t A_Q T \equiv D \pmod{p^{m+1}} \\
\Leftrightarrow\ & \frac{T^t A_Q T - D}{p^m} + \underbrace{T^t A_Q X}_{Y} + X^t A_Q T \equiv 0 \pmod{p} \\
\Leftrightarrow\ & Y + Y^t \equiv \underbrace{\frac{D - T^t A_Q T}{p^m}}_{B} \pmod{p}
\end{aligned}$$

where $Y = T^t AX$ and $B = (D - T^t AT)/p^m$ is a symmetric matrix with integer entries. Let

$$Y \equiv \begin{bmatrix}
\frac{1}{2}\beta_{11} & & & & \\
\beta_{21} & \frac{1}{2}\beta_{22} & & \mathbf{0} & \\
\beta_{31} & \beta_{32} & \frac{1}{2}\beta_{33} & & \\
\vdots & \vdots & \vdots & \ddots & \\
\beta_{n1} & \beta_{n2} & \beta_{n3} & \cdots & \frac{1}{2}\beta_{nn}
\end{bmatrix} \pmod{p^m}.$$

Then $Y + Y^t = B$ (We note that the choice of Y is not unique). Hence, we are left with solving the congruence

$$T^t AX \equiv Y \pmod{p}.$$

As T and A are nonsingular (mod p), this equation has a unique solution

$$X \equiv A^{-1}(T^t)^{-1}Y \pmod{p^m}.$$

This completes the induction step. □

***Examples*: 1.** Let

$$Q(x,y) = \begin{bmatrix} x & y \end{bmatrix} \overbrace{\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}}^{A} \begin{bmatrix} x \\ y \end{bmatrix} = x^2 + pxy + y^2.$$

Note that $Q(x,y)$ is already a diagonal form when read (mod p). We proceed to diagonalize $Q(x,y)$ (mod p^2).

$$T = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$B = \frac{D - T^t AT}{p} = \frac{1}{p}\left[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\right] = \begin{bmatrix} 0 & -\frac{1}{2} \\ -\frac{1}{2} & 0 \end{bmatrix} = -\frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y = \begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix}.$$

Solve $AX \equiv Y \pmod{p}$,

$$\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\begin{bmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix} \pmod{p}$$

$$\Leftrightarrow \quad \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \end{bmatrix} \equiv -\frac{1}{2}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \pmod{p}$$

$$\Leftrightarrow \quad \begin{bmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix} \pmod{p}$$

***Check* :**

$$U = T + pX = -\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + p\begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ -\frac{p}{2} & 1 \end{bmatrix}$$

$$U^t AU = \begin{bmatrix} 1 & -\frac{p}{2} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\begin{bmatrix} -\frac{p}{2} & 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & -\frac{p}{2} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{p}{2} \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{p^2}.$$

Thus $Q(\mathbf{x}) \sim x^2 + y^2 \pmod{p^2}$.

2. Let

$$Q(x, y) = \begin{bmatrix} x & y \end{bmatrix}\overbrace{\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 0 \end{bmatrix}}^{A}\begin{bmatrix} x \\ y \end{bmatrix} = x^2 + pxy \equiv x^2 \pmod{p}.$$

What happens if A singular?
Here A is not invertible, so we cannot directly follow the method given in our proof. Let us try to solve

$$T^t AX \equiv Y \pmod{p}.$$

First, we see that $T = I_2$ since A is already diagonal (mod p) . Let $\frac{1}{2} \mapsto \frac{(p^2+1)}{2}$. Then

$$A = \begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p^2},$$

and the latter matrix has integer entries.

$$B = \frac{D-A}{p} = \frac{1}{p}\left[\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 1 \end{bmatrix}\right] = \begin{bmatrix} 0 & -\frac{p^2+1}{2} \\ -\frac{p^2+1}{2} & 0 \end{bmatrix}.$$

If we proceed as in the proof we would let

$$Y = \begin{bmatrix} 0 & 0 \\ -\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p^2}.$$

Now solve

$$\begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} X \equiv \begin{bmatrix} 0 & 0 \\ -\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p}.$$

This is equivalent to

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix} \pmod{p}$$

$$\Leftrightarrow \begin{bmatrix} x_{11} & x_{12} \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ -\frac{1}{2} & 0 \end{bmatrix} \pmod{p},$$

which give us a contradiction $(0 = -\frac{1}{2})$ and hence there is no solution of this system.

Next, let us try the choice

$$Y = \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} \pmod{p^2}.$$

Then

$$Y + Y^t = \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} + \begin{bmatrix} 0 & -\frac{p^2+1}{2} - \alpha \\ \alpha & 0 \end{bmatrix} = B \pmod{p^2}.$$

Solve

$$\begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} X \equiv \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} \pmod{p},$$

or, equivalently

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0+\alpha \\ -\frac{1}{2} - \alpha & 0 \end{bmatrix} \pmod{p}.$$

Let $\alpha = -\frac{1}{2}$. Then obviously

$$\begin{bmatrix} x_{11} & x_{12} \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & -\frac{1}{2} \\ 0 & 0 \end{bmatrix} \pmod{p},$$

so that

$$X = \begin{bmatrix} 0 & -\frac{1}{2} \\ 0 & 0 \end{bmatrix}.$$

Hence, it follows one can make the change of variable

$$x \mapsto x + p\frac{p-1}{2}y, \quad y \mapsto y$$

to diagonalize the quadratic form $Q(x, y) \pmod{p^2}$. Indeed,

$$\begin{aligned} x^2 + pxy &\sim \left(x + \frac{p-1}{2}py\right)^2 + p\left(x + \frac{p-1}{2}py\right)y \\ &\equiv (p-1)pxy + x^2 + pxy \pmod{p^2} \\ &\equiv x^2 \pmod{p^2} \end{aligned}$$

Our proof of Theorem 1 actually yields the stronger result.

Corollary 1. *If p is an odd prime, $Q(\mathbf{x})$ is a quadratic form over $\mathbb{Z}$, nonsingular (*mod p*) and equivalent to diagonal form $\sum_{i=1}^{n} a_i x_i^2 \pmod{p}$, then $Q(\mathbf{x})$ is equivalent to the same diagonal form $\sum_{i=1}^{n} a_i x_i^2 \pmod{p^m}$ for any m.*

***Note*:** This fails for nonsingular forms.
Indeed, $x^2 + py^2 \sim x^2 \pmod{p}$, but $x^2 + py^2 \not\sim x^2 \pmod{p^2}$.

References

[1] Larry J. Gerstein, *Basic Quadratic Forms*, American Mathematical Society, 2008.

[2] G. L. Watson, *Integral Quadratic Forms*, Cambridge University Press, 1960.

[3] Michel Artin, *Algebra*, Prentice-Hall, New Jersey, 1991.

[4] R. Lidl and H. Niederreiter, *Encyclopedia of Mathematics and its Applications, Finite Fields*, Addison-Wesley Publishing Company, 1983.