COMMUNICATIONS

DE LA FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ D'ANKARA

Série A: Mathématîques, Physique et Astronomie

TOME 22 A ANNÉE 1973

A Matrix Representation Of The Quadratic Residue And Quadratic Non-Residue Classes.

by

E. KAYA

4

Faculté des Sciences de l'Université d'Ankara
Ankara, Turquie

Communications de la Faculté des Sciences de l'Université d'Ankara

---

La Revue "Communications de la Faculté des Sciences de l'Université d'Ankara" est un organe de publication englobant toutes les disciplines scientifiques représentées à la Faculté: Mathématiques pures et appliquées, Astronomie, Physique et Chimie théorique, expérimentale et technique, Géologie, Botanique et Zoologie.

La Revue, à l'exception des tomes I, II, III, comprend trois séries

Série A : Mathématiques, Physique et Astronomie.
Série B : Chimie.
Série C : Sciences naturelles.

En principe, la Revue est réservée aux mémoires originaux des membres de la Faculté. Elle accepte cependant, dans la mesure de la place disponible, les communications des auteurs étrangers. Les langues allemande, anglaise et française sont admises indifféremment. Les articles devront être accompagnés d'un bref sommaire en langue turque.

Adresse: Fen Fakültesi Tebliğler Dergisi, Fen Fakültesi' Ankara, Turquie.

A Matrix Representation Of The Quadratic Residue And Quadratic Non-Residue Classes.

E. KAYA*

SUMMARY

In this article, we obtain a matrix representation of residue classes (mod p) using Mahler's Matrices and extended this to quadratic and non-quadratic residue classes of an odd prime p.

Some properties of Mahler's Matrices have been obtained by D. H. Lehmer [1] and J. L. Brenner [2].

I. INTRODUCTION

Let p be an odd prime and m a positive integer so that $(m,p) = 1$, $m \equiv 1 \pmod{p}$.

Definition 1.1. Let Q be a square matrix of order p of the form.

$$Q = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ w & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

where w is a primitive p-th root of unity.

Lemma 1.1. $w^m = w$

1.2. $Q^p = wE$ (E is the unit matrix of order p).

1.3. $Q^{mp} = w^m E = wE$.

* Department of Mathematics, Ankara University, Ankara, Turkey.

Definition 2.1. Set $v = \frac{1}{1 - w}(1,1, \ldots 1)$

2.2. Let B (m) be a square matrix of order p of the form.

$$B(m) = \begin{bmatrix} v\,E \\ v\,Q^{m} \\ \cdot \\ \cdot \\ \cdot \\ v\,Q^{(p-1)m} \end{bmatrix}$$

First, we investigate some properties of the matrices B(m).

Lemma 2.1. $Q\,B(m) = B(m)\,Q^{m}$

2.2. $Q^{k}\,B(m) = B(m)\,Q^{km}$
where k is any positive integer.

2.3. $(E\text{-}Q)\,B(m) = B(m)\,(E\text{-}Q^{m})$

2.4. $v\,B(m)\,(E\text{-}Q^{m}) = v$

2.5. $(E\text{-}Q)\,B(m)\,(E\text{-}Q)\,(B(m')) = (E\text{-}Q)\,B(mm')$

Proof. (2.1) We can write Q B(m) and B(m) Q^m as follows

$$Q\,B(m) = \begin{bmatrix} v\,Q^{m} \\ \cdot \\ \cdot \\ \cdot \\ v\,Q^{(p-1)m} \\ w\,v\,E \end{bmatrix}, \quad B(m)\,Q^{m} = \begin{bmatrix} vQ^{m} \\ \cdot \\ \cdot \\ \cdot \\ v\,Q^{(p-1)m} \\ v\,Q^{pm} \end{bmatrix}$$

By lemma (1.3), the last row of B(m) Q^m is $vQ^{pm} = wvE$. This completes the proof of (2.1).

(2.2) This can be proved by induction.

(2.3) By (2.1) and (2.2), we have

$$\begin{aligned} B(m)\,(E\text{-}Q^{m}) &= B(m) - B(m)\,Q^{m}, \\ &= B(m) - Q\,B(m) \\ &= (E\text{-}Q)\,B(m). \end{aligned}$$

(2.4) Let us consider the following equality

$$(E\text{-}Q^{pm}) = (E\text{-}Q^{m})\ (E+Q^{m}+\dots+Q^{(p-1)m}).$$

Multiplying on the left by v both sides of the relation,

$$(E+Q^{m}+\dots+Q^{(p-1)m})\quad (E\text{-}Q^{m}) = (E\text{-}Q^{pm})$$

and using (1.3), (2.1), (2.2), (2.3), we have

$$v(E+Q^{m}+\dots+Q^{(p-1)m})\quad (E\text{-}Q^{m}) = v\ (E\text{-}Q^{pm}),$$

$$(vE+vQ^{m}+\dots+vQ^{(p-1)m})\quad (E\text{-}Q^{m}) = v(E\text{-}wE),$$

$$(1,1,\dots,1)\ B(m)\quad (E\text{-}Q^{m}) = (1\text{-}w)v,$$

$$v\ B(m)\ (E\text{-}Q^{m}) = v, \quad \text{or}$$

$$v(E\text{-}Q)\ B(m) = v.$$

(2.5) The left hand side of (2.5) is

$$(E\text{-}Q)\ B(m)\ (E\text{-}Q)\ B(m') \quad \text{or}$$

$$B(m)\ (E\text{-}Q^{m})\ B(m')\ (E\text{-}Q^{m'}).$$

By (2.1), (2.2), (2.3), (2.4); the r-th row of this is

$$v\ Q^{(r-1)m}\ (E\text{-}Q^{m})\ B(m')\ (E\text{-}Q^{m'}),$$

$$v\ B(m')\ Q^{(r-1)mm'}\ (E\text{-}Q^{mm'})\ (E\text{-}Q^{m'}),$$

$$v\ B(m')\ (E\text{-}Q^{m'})\ Q^{(r-1)mm'}\ (E\text{-}Q^{mm'});$$

$$v\ Q^{(r-1)mm'}\ (E\text{-}Q^{mm'}).$$

But the relation is the r-th row of

$$B(mm')\ (E\text{-}Q^{mm'}).$$

Thus (2.5) is proved.

Definition 3.1. Set $A(m) = \left(\frac{m}{p}\right) (E\text{-}Q)\ B(m)$

where $\left(\frac{m}{p}\right)$ is the Legendre's symbol.

Now, we investigate some properties of the matrices A(m).

Lemma 3.1. $A(1) = E$.

3.2. $A(m)\ A(m') = A(mm')$.

3.3. $A(m)\ A(m') = E$, if m' is the solution of the linear congruence

$$mx \equiv 1 \pmod{p^2}.$$

3.4. $A(m) = A(m')$ if $m \equiv m' \pmod{p^2}$

Proof. (3.1) and (3.2) are easily obtained using the above results.

If $(m, p) = 1$ then the linear congruence

$$mx \equiv 1 \pmod{p^2}$$

has exactly one solution $m' \pmod{p^2}$, [3]. Then the solution m' satisfies the relation $m\ m' \equiv 1 \pmod{p^2}$. From this, we have, since

$$A(m)\ A(m') = A(mm'),$$

$$A(mm') = A(1+qp^2) = A(1) = E.$$

where q is any integer.

Hence, we see that each matrix $A(m)$ has an inverse.

2. Suppose that $(\alpha, p) = 1$. If the conguence

$$x^2 \equiv \alpha \pmod{p}$$

has a solution, then the integer α is said to be a quadratic residue of p. If this congruence has no solution, α is said to be a quadratic non-residue of p.

We write α R p or α N p according as α is a quaratic residue or α is a quadratic non-residue of p.

Lemma 4.1. If α R p and α' R p, then

$$A(\alpha)\ A(\alpha') = A(\alpha\alpha').$$

4.2. If α N p, α' N p then,

$$A(\alpha)\ A(\alpha') = A(\alpha\alpha').$$

4.3. If α Rp and α' N p then

$$A(\alpha)\ A(\alpha') = -A(\alpha\alpha').$$

Proof. (4.1). If α Rp and α' Rp then $\left(\frac{\alpha}{p}\right) = +1$, $\left(\frac{\alpha'}{p}\right) = +1$.

Hence,

$$A(\alpha)\ A(\alpha') = A(\alpha\alpha').$$

(4.2). $\left(\frac{\alpha}{p}\right) = -1, \left(\frac{\alpha'}{p}\right) = -1.$ From these we have

$$A(\alpha)\ A(\alpha') = A(\alpha\alpha').$$

(4.3). $\left(\frac{\alpha}{p}\right) = +1, \left(\frac{\alpha'}{p}\right) = -1.$ Then

$$A(\alpha)\ A(\alpha') = -A\ (\alpha\alpha').$$

Thus we have proved the following theorem.

Theorem. Let p be an odd prime. If m is a quadratic residue of p, then the set $\{A(m)\}$ forms a finite Abelian group, isomorphic to the multiplicative group of quadratic residues of (mod p^2) [3, 4].

REFERENCES

[1] **D. H. Lehmer,** *Mahler's Matrices,* Australian Journal of Mathematics, Vol 1, pp. 385–395 (1960).

[2] **J. L. Brenner,** *Mahler Matrices and the equation QA = AQ^m*, Duke Mathematical Journal, vol. 29, pp. B-28 (1962).

[3] **G. H. Hardy and E. M. Wright,** *An Introduction to the Theory of Numbers,* Oxford at the Clarendon Press, Fourth Edition (1960).

[4] **J. Hunter,** *Number Theory*, Oliver and Boyd (1964).

ÖZET

Bu çalışmada (mod p) kalanlar sınıflarının Mahler Matrisleri ile gösterimi, kuadratik ve kuadratik olmıyan kalanlar sınıflarına bir teşmili yapılmıştır.

Prix de l'abonnement annuel

Turquie : 15 TL; Étranger: 30 TL.

Prix de ce numéro : 5 TL (pour la vente en Turquie).

Prière de s'adressei pour l'abonnement à : Fen Fakültesi Dekanlığı Ankara, Turquie.

Ankara Üniversitesi Basımevi–1973