1992

Tournaments and Ideal Class Groups.

Robert John Kingan

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation

Kingan, Robert John, "Tournaments and Ideal Class Groups." (1992). *LSU Historical Dissertations and Theses*. 5323.

https://digitalcommons.lsu.edu/gradschool_disstheses/5323

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600

Order Number 9301071

Tournaments and ideal class groups

Kingan, Robert John, Ph.D.

The Louisiana State University and Agricultural and Mechanical Col., 1992

Copyright ©1993 by Kingan, Robert John. All rights reserved.

U·M·I

**300 N. Zeeb Rd.
Ann Arbor, MI 48106**

TOURNAMENTS AND IDEAL CLASS GROUPS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Robert John Kingan

B.S., The University of Central Arkansas, 1987

M.S., Louisiana State University, 1989

May, 1992

ACKNOWLEDGEMENTS

The author wishes to thank his advisor, Dr. Jurgen Hurrelbrink, for his guidance and enormous patience during the preparation of this dissertation. Thanks are also due to Dr. P. E. Conner, Dr. Robert Perlis, and Dr. Antone Costa for their support and help, and to Dr. Neal Stoltzfus for his technical assistance with the NeXT computer.

The author especially wishes to thank his wife, Sandra, for her constant support and inspiration. Without her, this might never have been done.

TABLE OF CONTENTS

	<u>page</u>
ACKNOWLEDGEMENTS	ii
ABSTRACT	iv
CHAPTER	
I PRELIMINARIES	1
1. Introduction	1
2. The Narrow Ideal Class Group	6
II PREVIOUS RELATED RESULTS	9
1. Classical Results; the Method of Rédei and Reichardt	9
2. The Method of Conner and Hurrelbrink	11
3. The Equivalence of the Two Methods	18
4. A Useful Result of Gerth's	22
III RESULTS USING ADJUSTED TOURNAMENT MATRICES	24
1. Realization of All Possible Values for $r_4(m)$, $r_4(-m)$	24
2. Minimal Rank Adjusted Tournament Matrices	32
3. A Condition for $r_4(-m) = r_4(m)$	37
4. Circulant Tournaments	44
BIBLIOGRAPHY	56
APPENDIX: Tournaments of Size Six and Smaller	61
VITA	69

ABSTRACT

In a series of papers published in the 1930's, L. Rédei and H. Reichardt established a method for determining the 4-rank of the narrow ideal class group of a quadratic number field, essentially by finding the rank over $\mathbb{F}_2$ of a $\{0, 1\}$ -matrix determined by applying the Kronecker symbol to the prime divisors of the field discriminant. When this field is of the form $\mathbb{Q}(m^{\frac{1}{2}})$, with $m = \pm p_1 \cdots p_n$, each $p_i \equiv 3 \pmod{4}$ prime, this matrix takes a form similar to that of the adjacency matrix for a tournament graph. Also, in this case we can find the 4-rank of the ideal class group in the ordinary sense.

In Chapter 1, we introduce this method. In Chapter 2, we explain in detail the equivalence of Rédei's method to a more modern one, and give some useful results concerning the ranks of anti-symmetric matrices over $\mathbb{F}_2$. In Chapter 3, we use matrices to give precise ranges for the 4-rank of the ideal class group in our situation, establish conditions for maximal 4-rank, and give a partial verification of a previous result relating the 4-rank of a real and corresponding imaginary quadratic extension. We conclude with some results concerning circulant tournaments and their matrices.

CHAPTER I

PRELIMINARIES

1. Introduction

In the late nineteenth century, E. E. Kummer was working on a proof for Fermat's Last Theorem, which of course remains an open problem to this day. It was pointed out by Dirichlet that one cannot rely on unique prime factorization of elements in the ring of integers of an algebraic number field, since this does not hold in general. This led Kummer to the study of what he called "ideal elements", known to us today as ideals. R. Dedekind's study of ideal theory led him to a proof that, in the ring of integers of an algebraic number field, any ideal can be factored uniquely as a product of prime ideals. This was also proved by L. Kronecker and D. Hilbert.

Kummer's study of cyclotomic fields led to the proof that the classes of fractional ideals of a field E , under the equivalence relation $I \sim J$ if and only if $I = xJ$ for some $x \in E^*$, form a group whose identity is the class of principal fractional ideals. This group, which exists for any number field, is known as the **ideal class group** of E , and is denoted $C(E)$. It can be shown that $C(E)$ is a finite abelian group; its size, called the **class number** of E , gives a rough measure of how close the ring of integers of E is to being a unique factorization domain, as $C(E)$ is trivial if and only if the ring of integers of E is a principal ideal domain.

The structure and size of the ideal class group are, in general, difficult to compute. Gauss conjectured that for $m < 0$, the only fields $F = \mathbb{Q}(m^{\frac{1}{2}})$ with class number one are those with $m = -1, -2, -3, -7, -11, -19, -43, -67$, and -163 , and that for $m > 0$, there are infinitely many fields F with class number one.

The former result has been proved by Stark; the latter remains an open question. It is not known whether every finite abelian group is an ideal class group, although it has been shown in [C] that the answer is no if we restrict ourselves to imaginary quadratic number fields.

Dirichlet devised a formula which, in the real quadratic case, gives the class number in terms of the “fundamental unit” of the field (which is itself difficult to compute) and the Jacobi symbol applied to the units in $\mathbf{Z}/D\mathbf{Z}$, where D is the discriminant of the extension.

Among other important results in this area are those of Carlitz, characterizing all fields with class number 2, and Czogala, characterizing all fields with ideal class group C_2 , C_3 , or $C_2 \times C_2$, where C_i denotes the cyclic group of order i , in terms of factorizations of irreducible elements in the ring of integers.

As a first step toward understanding the structure of the ideal class group in a quadratic extension, an important goal of research in this area has been to determine the structure of the 2-Sylow subgroup of the ideal class group of a quadratic number field.

Definition: The sum of the values a_i in the decomposition:

$$C_2^{a_1} \times C_4^{a_2} \times \cdots \times C_{2^k}^{a_k}, \quad (1)$$

of the 2-Sylow subgroup of $C(E)$ is called the **2-rank** of $C(E)$. The sum of the values a_i with $i \geq 2$ is called the **4-rank**, and other higher 2-power ranks are defined accordingly. We will denote the 4-rank of $C(\mathbf{Q}(m^{\frac{1}{2}}))$ by $r_4(m)$.

Let n be the number of distinct prime divisors of the field discriminant $\text{Dis}(E/\mathbf{Q})$. It is a result of Gauss [G] that the 2-rank of $C(E)$ is given by $n - 2$ if E is real quadratic and -1 is not a norm from E , and $n - 1$ otherwise. Of

course, the 2-rank cannot be negative; the fact that -1 is a norm from a real quadratic extension E if and only if no primes congruent to 3 (mod 4) divide the discriminant insures that $n \geq 2$ in the appropriate case.

Thus, among complex quadratic number fields, the only fields with odd class number are those in which only one prime divides the discriminant. Among real quadratic number fields, the only fields with odd class number are those in which either -1 is a norm and the discriminant is prime, or -1 is not a norm and the discriminant has exactly 2 prime divisors. We summarize this information in the following lemma:

Lemma 1.1: The class number of a quadratic extension $E/\mathbb{Q}$ is odd if and only if $E = \mathbb{Q}(m^{\frac{1}{2}})$ for:

- (i) $m = -1, -2, -p$ where p is a prime congruent to 3 (mod 4)
- (ii) $m = 2, q$ where q is a prime congruent to 1 (mod 4)
- (iii) $m = p, 2p, p_1p_2$ where $p, p_1, p_2 \equiv 3 \pmod{4}$ are prime. ■

This dissertation deals specifically with fields of the form $E = \mathbb{Q}(d^{\frac{1}{2}})$ and $L = \mathbb{Q}((-d)^{\frac{1}{2}})$, where $d = p_1 \cdots p_n$ with each $p_i \equiv 3 \pmod{4}$ prime. We are interested in the 4-rank of the ideal class group of these fields.

Suppose $d = p_1 \cdots p_n$, with each $p_i \equiv 3 \pmod{4}$ prime. Define an $n \times n$ matrix $A = (a_{ij})$ over the field $\mathbb{F}_2$ by:

$$(-1)^{a_{ij}} = \begin{cases} \left(\frac{p_j}{p_i}\right) & \text{if } i \neq j \\ (-1)^{n+1} \left(\frac{\frac{d}{p_i}}{p_i}\right) & \text{if } i = j, \end{cases}$$

where $\left(\frac{a}{p}\right)$ denotes the Jacobi symbol. Then, as a consequence of a 1934 result of Rédei, we have the following formulas:

- (i) If n is even, then $r_4(d) = n - 1 - \text{rank}_{\mathbf{F}_2}(A)$, and $r_4(-d) = n - \text{rank}_{\mathbf{F}_2}(A)$ or $n - 1 - \text{rank}_{\mathbf{F}_2}(A)$.
- (ii) If n is odd, then $r_4(d) = n - 1 - \text{rank}_{\mathbf{F}_2}(A)$ or $n - 2 - \text{rank}_{\mathbf{F}_2}(A)$, and $r_4(-d) = n - 1 - \text{rank}_{\mathbf{F}_2}(A)$.

Since d is a product of n primes congruent to 3 (mod 4), we will have a factor of 2 in the discriminant in the real case when n is odd, and in the complex case when n is even. In the other two cases, the discriminant will simply be d or $-d$. Note that the ambiguity in the above formulas occurs in the two cases where the discriminant is even. Later, we will find that the value can be made precise, using the congruence of the primes dividing d modulo 8 and properties of the matrix A .

Thus, we see that we can find information about $r_4(d)$ and $r_4(-d)$ by studying properties of the matrix A . We can immediately see that A is anti-symmetric, since $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ when $p, q \equiv 3 \pmod{4}$, by quadratic reciprocity. Furthermore, the choice of diagonal entries insures that the sum of the entries of each column of A is even. This immediately tells us that A cannot be invertible. Later, we will find more restrictive bounds on $\text{rank}_{\mathbf{F}_2}(A)$.

The fact that A is anti-symmetric leads us to a graph-theoretic interpretation. A **tournament** is a directed graph T with a vertex set V and edge set E such that, for any distinct $x, y \in V$, either $(x, y) \in E$ or $(y, x) \in E$, but not both. In other words, the vertices can be thought of as “teams”, and each team either defeats, or is defeated by, each other team.

The **tournament matrix** for a tournament T on n vertices with edge set E is a square $\{0, 1\}$ -matrix (a_{ij}) of size n such that:

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } (i, j) \in E \\ 0 & \text{otherwise.} \end{cases}$$

In particular, the diagonal entries of the tournament matrix are all zero. To suit our situation, we make the following definition:

Definition: Let T be a tournament on n vertices with edge set E . Then the **adjusted tournament matrix** $A = (a_{ij})$ for T is a square $\{0, 1\}$ -matrix of size n given as follows:

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } (i, j) \in E \\ 0 & \text{if } i \neq j \text{ and } (i, j) \notin E \\ \sum_{k \neq i} a_{ki} \pmod{2} & \text{if } i = j. \end{cases}$$

Then each column of the adjusted tournament matrix A of T will have even **weight**; that is, an even number of ones. If n is even, then each row of A will have odd weight; otherwise, each row of A will have even weight. Also, thought of as a matrix over the field $\mathbb{F}_2$, A satisfies the equation:

$$A + A^T = I + J,$$

where I and J denote (and hereafter will always denote) the $n \times n$ identity matrix and matrix whose entries are all ones, respectively.

Note: Given a field $\mathbb{Q}(m^{\frac{1}{2}})$, where $|m|$ is a product of primes congruent to 1 (mod 4), we can use the results of Rédei to define a similar $\{0, 1\}$ -matrix which also yields information about the 4-rank of the ideal class group, as well as the sign of the fundamental unit. In this case, quadratic reciprocity will insure that the matrix is symmetric, yielding an interpretation in terms of graphs.

Example 1.1: Let $p_1 = 11$, $p_2 = 7$, and $p_3 = 3$. Then we have the following adjusted tournament matrix and tournament graph:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Fig. 1.1.1

(In the tournament graph, we assume a downward arrow whenever two vertices are not connected.) We see that $\text{rank}_{\mathbb{F}_2}(A) = 2$, so that $\tau_4(11 \cdot 7 \cdot 3) = 0$. In this case, the discriminant of $\mathbb{Q}((11 \cdot 7 \cdot 3)^{\frac{1}{2}})$ is $4 \cdot 11 \cdot 7 \cdot 3$, so the 2-rank of the ideal class group is 2. Therefore, we can conclude that the 2-Sylow subgroup of the ideal class group is of the form $C_2 \times C_2$.

Example 1.2: Let $p_1 = 3$, $p_2 = 11$, $p_3 = 83$, and $p_4 = 239$. Then we have the following adjusted tournament matrix and tournament graph:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Fig. 1.1.2

This tournament, distinguished by its lack of “cycles”, is called **transitive**. In this case, we still have $\text{rank}_{\mathbb{F}_2}(A) = 2$, so that $\tau_4(3 \cdot 11 \cdot 83 \cdot 239) = 1$, by the formulae. This time, the 2-rank of the ideal class group is 2, so the 2-Sylow subgroup of the ideal class group is of the form $C_2 \times C_{2^k}$ for some $k \geq 2$. It is an indication of the power of this method that the value 654,621 is already much larger than the discriminant values that can be found in most published tables of 4-ranks.

2. The Narrow Ideal Class Group

The original work of Rédei, like most research in this area, was actually concerned with the **narrow ideal class group**. In this section, we will define the

narrow ideal class group and indicate why, in our case, the 4-ranks of the two groups are the same.

Suppose F is an algebraic number field. An element $x \in F^*$ is called **totally positive** if, for each embedding σ of F into $\mathbf{R}$, $\sigma x > 0$. We denote the set of totally positive elements of F by F^+ . It is easily seen that F^+ is a multiplicative subgroup of F^* . We can define an equivalence relation $\approx$ on the fractional ideals of F by $I \approx J$ if and only if $I = xJ$ for some $x \in F^+$. Then, once again, the equivalence classes form a group, called the narrow ideal class group of F , denoted $C_+(F)$. If $F = \mathbf{Q}(m^{\frac{1}{2}})$, we denote the 4-rank of $C_+(F)$ by $r_4^+(m)$. Actually, using quadratic forms, Gauss proved that the 2-rank of $C_+(F)$ is one less than the number of prime divisors of the discriminant of F . The result mentioned earlier is a consequence of this.

Lemma 2.1: Let $d = p_1 \cdots p_n$, where each $p_i \equiv 3 \pmod{4}$ is prime. Then $r_4(d) = r_4^+(d)$ and $r_4(-d) = r_4^+(-d)$.

Proof. In the complex case the result is obvious, and indeed holds for any 2-power rank; since there are no real embeddings of $\mathbf{Q}((-d)^{\frac{1}{2}})$, every nonzero element is totally positive. Thus, $C(\mathbf{Q}((-d)^{\frac{1}{2}})) = C_+(\mathbf{Q}((-d)^{\frac{1}{2}}))$.

In the real case, let $E = \mathbf{Q}(d^{\frac{1}{2}})$. We make use of the natural surjection:

$$\nu : C_+(E) \longrightarrow C(E) \longrightarrow 1.$$

First, we wish to examine $\ker(\nu)$. We can easily see that $\ker(\nu)$ is an elementary abelian 2-group, since the square of any element of E^* is totally positive. Furthermore, by [C-H] page 46, we find that:

$$\ker(\nu) \cong E^*/E^+O_E^*,$$

where by O_E we mean the ring of integers of E .

Now, when any prime congruent to 3 (mod 4) divides the discriminant of a quadratic number field, we know that there can be no elements of O_E^* with negative norm, since $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod{4}$. Therefore, each element of $E^+O_E^*$ is either totally positive or totally negative, so $E^*/E^+O_E^*$ consists merely of the two classes $\{\pm 1\}$. Thus, we have a short exact sequence:

$$1 \longrightarrow C_2 \longrightarrow C_+(E) \longrightarrow C(E) \longrightarrow 1.$$

As mentioned above, in this case $2\text{-rank}(C(E))$ is two less than the number of primes dividing $\text{Dis}(E/\mathbb{Q})$; thus, $2\text{-rank}(C(E))$ is $n - 2$ if n is even, and $n - 1$ if n is odd. Also, $2\text{-rank}(C_+(E))$ is one less than the number of primes dividing $\text{Dis}(E/\mathbb{Q})$. In other words, $2\text{-rank}(C_+(E)) = 2\text{-rank}(C(E)) + 1$. This, together with the short exact sequence above, tells us that the 2-Sylow subgroup of $C_+(E)$ is isomorphic to the product of C_2 and the 2-Sylow subgroup of $C(E)$. In particular, $r_4^+(d) = r_4(d)$. ■

CHAPTER II

PREVIOUS RELATED RESULTS

1. Classical Results; the Method of Rédei and Reichardt

The study of the 4-rank of the narrow ideal class group dates back to Gauss and Dirichlet, who proved that $r_4^+(p) = 1$ when $p \equiv 1 \pmod{4}$ is prime. In the late 1920's and early 1930's Rédei and Reichardt proved several significant results, which appear in [R-R], [R1], [R2], [R4], [R5], and [Re2]. Of particular interest is [R1], in which Rédei explains how $r_4^+(m)$ can be determined by counting the **Einheitsmengen**, or sets of columns whose product (element-wise) is the column consisting of ones, of the following matrix:

$$M_D = \begin{bmatrix} \left(\frac{D}{p_1}\right) & \left(\frac{p_2}{p_1}\right) & \left(\frac{p_3}{p_1}\right) & \cdots & \left(\frac{p_{t-1}}{p_1}\right) \\ \left(\frac{p_1}{p_2}\right) & \left(\frac{D}{p_2}\right) & \left(\frac{p_3}{p_2}\right) & \cdots & \left(\frac{p_{t-1}}{p_2}\right) \\ \left(\frac{p_1}{p_3}\right) & \left(\frac{p_2}{p_3}\right) & \left(\frac{D}{p_3}\right) & \cdots & \left(\frac{p_{t-1}}{p_3}\right) \\ \vdots & & & \ddots & \vdots \\ \left(\frac{p_1}{p_{t-1}}\right) & \left(\frac{p_2}{p_{t-1}}\right) & \left(\frac{p_3}{p_{t-1}}\right) & \cdots & \left(\frac{D}{p_{t-1}}\right) \\ \left(\frac{p_1}{p_t}\right) & \left(\frac{p_2}{p_t}\right) & \left(\frac{p_3}{p_t}\right) & \cdots & \left(\frac{p_{t-1}}{p_t}\right) \end{bmatrix},$$

where $D = \text{Dis}(\mathbb{Q}(m^{\frac{1}{2}})/\mathbb{Q})$, and $p_1, \dots, p_t$ are the prime divisors of D , set as follows: If D is even, we set $p_t = 2$, and the signs of all odd p_i are adjusted so that $p_i \equiv 1 \pmod{4}$. (We use the formula $\left(\frac{p}{2}\right) = (-1)^{\frac{p-1}{4}}$.) We have the following result:

Theorem 1.1 (Rédei): Let n_1 be the number of *Einheitsmengen* of M_D . Then $2^{r_4^+(d)} = n_1$.

Example 1.1: Let $d = 3 \cdot 7 \cdot 11 = 231$, and let $E = \mathbf{Q}(d^{\frac{1}{2}})$. Then $D = 4 \cdot 3 \cdot 7 \cdot 11$, so the matrix M_D looks like:

$$M_D = \begin{bmatrix} +1 & -1 & +1 \\ +1 & +1 & -1 \\ -1 & +1 & +1 \\ -1 & +1 & -1 \end{bmatrix}.$$

There is only one way (the empty product) to multiply rows element-wise to get a column consisting completely of ones, so $n_1 = 1$, and $r_4^+(231) = 0$.

Example 1.2: Let $d = 3 \cdot 11 \cdot 83 \cdot 239 = 654,621$, and let $L = \mathbf{Q}((-d)^{\frac{1}{2}})$. Then $D = -4 \cdot 3 \cdot 11 \cdot 83 \cdot 239$, so M_D looks like:

$$M_D = \begin{bmatrix} -1 & +1 & +1 & +1 \\ -1 & +1 & +1 & +1 \\ -1 & -1 & -1 & +1 \\ -1 & -1 & -1 & +1 \\ -1 & -1 & -1 & +1 \end{bmatrix}.$$

In this case, there are four ways to multiply columns together to get a column of ones: the empty product; the second and third columns; the second, third, and fourth columns; and the fourth column. Thus $n_1 = 4$, so $r_4^+(-654,621) = 2$.

Some similarity between M_D and the adjusted tournament matrix determined by d (when d is a product of primes congruent to 3 (mod 4)) is already apparent. We will see later that our formulas for $r_4^+(d)$ can be obtained from Rédei and Reichardt's results.

Another method for computing $r_4^+(d)$ developed by Rédei and Reichardt is that of D -splittings. We say that an integer is a **discriminant** if it is either 1, or the discriminant of some quadratic number field.

Definition: If D is the discriminant of a quadratic number field, a **D -splitting** $\{d_1, d_2\}$ is an unordered factorization $D = d_1 \cdot d_2$, where d_1 and d_2 are discriminants. Then necessarily $(d_1, d_2) = 1$. We say that a D -splitting $\{d_1, d_2\}$ is of the

second type if: $\left(\frac{d_1}{p}\right) = +1$ for all primes p dividing d_2 , and $\left(\frac{d_2}{p}\right) = +1$ for all primes p dividing d_1 .

It can be seen that, under the operation:

$$\{d_1, d_2\} \circ \{d'_1, d'_2\} = \left\{ \frac{d_1 \cdot d'_1}{(d_1, d'_1)^2}, \frac{d_1 \cdot d'_2}{(d_1, d'_2)^2} \right\},$$

the set of D -splittings of the second type is an elementary abelian 2-group, with identity element $\{1, D\}$. The following result appears in [R-R]:

Theorem 1.2: $2^{r_4^+(m)}$ is the number of D -splittings of the second type, where $D = \text{Dis}(\mathbb{Q}(m^{\frac{1}{2}})/\mathbb{Q})$.

Example 1.3: Let $m = 3 \cdot 11 \cdot 83 \cdot 239 = 654,621$, and let $E = \mathbb{Q}(m^{\frac{1}{2}})$. Then $D = m$, and we have the following D -splittings:

$$\begin{aligned} &\{1, 3 \cdot 11 \cdot 83 \cdot 239\}, \{3 \cdot 11, 83 \cdot 239\}, \{3 \cdot 83, 11 \cdot 239\}, \{3 \cdot 239, 11 \cdot 83\}, \\ &\{-3, -11 \cdot 83 \cdot 239\}, \{-11, -3 \cdot 83 \cdot 239\}, \{-83, -3 \cdot 11 \cdot 239\}, \{-239, -3 \cdot 11 \cdot 83\} \end{aligned}$$

Of these, only the identity $\{1, 3 \cdot 11 \cdot 83 \cdot 239\}$ and $\{3 \cdot 11, 83 \cdot 239\}$ are of the second type, so $r_4^+(654,621) = 1$.

In [U], Uehara uses this method to determine conditions under which $r_4^+(m) = r_4^+(-m)$. In Chapter III, Section 3, we will rephrase this result (in the appropriate case) in terms of adjusted tournament matrices, and give a partial verification.

2. The Method of Conner and Hurrelbrink

Let $m = \pm d$ and $E = \mathbb{Q}(m^{\frac{1}{2}})$, where $d = p_1 \cdots p_n$, and each $p_i \equiv 3 \pmod{4}$ is prime. Let

$$U = \{x \in \mathbb{Q}^* \mid \text{ord}_p x = 0 \text{ for all primes } p \text{ such that } p \nmid \text{Dis}(E/\mathbb{Q})\}.$$

Then U is the group of units of the ring $S^{-1}\mathbf{Z}$, where S is the multiplicative set generated by the primes of $\mathbf{Z}$ which ramify in E . Thus, U/U^2 is an elementary abelian 2-group, and the set of divisors of $\text{Dis}(E/\mathbf{Q})$ is a set of representatives. Furthermore, there is a natural map:

$$\rho : U/U^2 \longrightarrow \mathbf{Q}^*/NE^*,$$

induced by the inclusion $U \hookrightarrow \mathbf{Q}^*$, where NE^* denotes the image of the norm map from E^* to $\mathbf{Q}^*$. For our purposes, this corresponds to the map:

$$\rho : U/U^2 \longrightarrow R^0(E/\mathbf{Q})$$

defined in [C-H], section 19, as $R^0(E/\mathbf{Q}) \hookrightarrow \mathbf{Q}^*/NE^*$, by Lemma 1.4 of [C-H].

We know that $-1 \notin NE^*$, since all our primes are congruent to 3 (mod 4). This tells us that the map i_0 mentioned in Theorem 19.3 of [C-H] is injective, so we obtain from that theorem the following result:

Theorem 2.1: Let E, ρ be defined as above. Then $r_4(m) = 0$ if and only if:

$$\text{2-rank ker } (\rho) = \begin{cases} 2 & \text{if } m > 0; \\ 1 & \text{if } m < 0. \end{cases}$$

This result was later extended by Brauckmann in [Br] to the following:

Theorem 2.2: Let E be as defined above, and let $\rho^+ : U_+/U_+^2 \longrightarrow \mathbb{Q}/NE^+$ be defined similarly to ρ , with U^+ the set of positive elements of U . Then:

$$r_4(m) = 2\text{-rank ker } (\rho^+) - 1$$

Of course, when $m < 0$, $2\text{-rank ker}(\rho^+) = 2\text{-rank ker}(\rho)$, since there are no negative norms. When $m > 0$, $2\text{-rank ker}(\rho^+) = 2\text{-rank ker}(\rho) - 1$, since there are negative norms, such as $-m$.

Therefore, to calculate $r_4(m)$, we want to find out which divisors of $\text{Dis}(E/\mathbb{Q})$ are norms. For the moment, let us restrict ourselves to asking which odd divisors of $\text{Dis}(E/\mathbb{Q})$ are norms. Since U_+/U_+^2 and $\mathbb{Q}^*/NE^+$ are elementary abelian 2-groups, we can think of the map ρ as a linear transformation on a vector space over $\mathbb{F}_2$, so that a divisor $p_1^{b_1} \cdots p_n^{b_n}$ of d , with each $b_i = 1$ or 0 , can be represented by the column vector:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Let $A = (a_{ij})$ be the adjusted tournament matrix for $p_1, \dots, p_n$ as defined before.

Recall that:

$$(-1)^{a_{ij}} = \begin{cases} \left(\frac{p_i}{p_j} \right) & \text{if } i \neq j, \\ (-1)^{n+1} \left(\frac{p_i}{p_i} \right) & \text{if } i = j, \end{cases}$$

where $P_i = p_1 \cdots \hat{p}_i \cdots p_n$. We will see that either A or $A + I$ is the matrix representing ρ^+ with respect to the basis $\{p_1, \dots, p_n\}$, depending on n , and whether E is a real or complex extension. In other words, we must consider the following four cases:

Case 1: Suppose n is even, and $E = \mathbb{Q}(d^{\frac{1}{2}})$. Then 2 does not divide $\text{Dis}(E/\mathbb{Q}) = d$. Let $p_1^{b_1} \cdots p_n^{b_n}$ be a divisor of $\text{Dis}(E/\mathbb{Q})$, and let:

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = A \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Then:

$$\begin{aligned} (-1)^{c_i} &= (-1)^{\sum a_{ik} b_k} = \left(\frac{p_1}{p_i} \right)^{b_1} \cdots \left(\frac{-P_i}{p_i} \right)^{b_i} \cdots \left(\frac{p_n}{p_i} \right)^{b_n} \\ &= (p_1, p_i)_{p_i}^{b_1} \cdots (p_i, d)_{p_i}^{b_i} \cdots (p_n, p_i)_{p_i}^{b_n}, \\ &= (p_1^{b_1} \cdots p_n^{b_n}, d)_{p_i} \end{aligned}$$

where by $(a, b)_p$ we mean the Hilbert symbol, given by $(a, b)_p = +1$ if there exist $x, y \in \mathbb{Q}_p$ such that $ax^2 + by^2 = 1$, and $(a, b)_p = -1$ otherwise. The second equality above, follows from the following:

$$\begin{aligned} (p_i, d)_{p_i} &= (p_i, p_1)_{p_i} \cdots (p_i, p_i)_{p_i} \cdots (p_i, p_n)_{p_i} \\ &= \left(\frac{p_1}{p_i} \right) \cdots \left(\frac{-1}{p_i} \right) \cdots \left(\frac{p_n}{p_i} \right) \\ &= \left(\frac{-1}{p_i} \right) \left(\frac{P_i}{p_i} \right) \\ &= \left(\frac{-P_i}{p_i} \right). \end{aligned}$$

Now, $x \in NE^*$ if and only if $(x, d)_p = +1$ for all primes p . Since $(x, d)_p = +1$ for any finite prime p not dividing x or d , and since $(x, d)_\infty = +1$ for $x > 0$, we can say that, for $x > 0$ dividing d , $x \in NE^+$ if and only if $(x, d)_{p_i} = +1$ for $1 \leq i \leq n$. Therefore, $p_1^{b_1} \cdots p_n^{b_n} \in NE^+$ if and only if:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \ker(A),$$

so $r_4(d) = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$.

Case 2: Suppose n is odd, and $L = \mathbf{Q}((-d)^{\frac{1}{2}})$. Then once again, $\text{Dis}(L/\mathbf{Q}) = -d$ is odd. If we define our vectors as above, we find that:

$$\begin{aligned}
 (-1)^{c_i} &= \left(\frac{p_1}{p_i}\right)^{b_1} \cdots \left(\frac{p_i}{p_i}\right)^{b_i} \cdots \left(\frac{p_n}{p_i}\right)^{b_n} \\
 &= \left(\frac{-1}{p_i}\right)^{b_i} \cdot \left(\frac{p_1}{p_i}\right)^{b_1} \cdots \left(\frac{-p_i}{p_i}\right)^{b_i} \cdots \left(\frac{p_n}{p_i}\right)^{b_n} \\
 &= (p_1^{b_1} \cdots p_n^{b_n}, -1)_{p_i} \cdot (p_1^{b_1} \cdots p_n^{b_n}, d)_{p_i} \\
 &= (p_1^{b_1} \cdots p_n^{b_n}, -d)_{p_i},
 \end{aligned}$$

where the third equality stems from the fact that:

$$(p_1^{b_1} \cdots p_n^{b_n}, -1)_{p_i} = (p_i^{b_i}, -1)_{p_i} = \left(\frac{-1}{p_i}\right)^{b_i}.$$

Therefore, $p_1^{b_1} \cdots p_n^{b_n} \in NL^*$ if and only if:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \ker(A),$$

so $r_4(-d) = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$.

In the remaining two cases, 2 ramifies. Our approach will still only calculate the 2-rank of the kernel of the map ρ^+ restricted to odd divisors of $\text{Dis}(E/\mathbf{Q})$ or $\text{Dis}(L/\mathbf{Q})$. This is what produces the ambiguity in our formulas for $r_4(d)$ and $r_4(-d)$ in terms of $\text{rank}(A)$, since the presence of norms divisible by 2 in U_+/U_+^2 may increase $2\text{-rank } \ker(\rho^+)$ by one. However, we will see at the end of this section that it is possible to determine which of the two values given by the formula is accurate, based on the congruences of the primes dividing d modulo 8.

We will also need the following fact, proved in [M], about adjusted tournament matrices:

Fact: Let A be an adjusted tournament matrix of size n . Then:

$$\text{rank}(A + I) = \begin{cases} \text{rank}(A) & \text{if } n \text{ is even} \\ \text{rank}(A) + 1 & \text{if } n \text{ is odd} \end{cases}.$$

Case 3: Suppose that n is odd, and $E = \mathbf{Q}(d^{\frac{1}{2}})$. Then $\text{Dis}(E/\mathbf{Q}) = 4d$. Let $A_1 = A + I = (a_{ij})$, where A is the adjusted tournament matrix for $p_1, \dots, p_n$.

Then $\text{rank}(A_1) = \text{rank}(A) + 1$, and $(-1)^{a_{ii}} = \left(\frac{-P_i}{p_i}\right)$. Therefore:

$$\begin{aligned} (p_1^{b_1} \cdots p_n^{b_n}, d)_{p_i} &= \left(\frac{p_1}{p_i}\right)^{b_1} \cdots \left(\frac{-P_i}{p_i}\right)^{b_i} \cdots \left(\frac{p_n}{p_i}\right)^{b_n} \\ &= (-1)^{\sum a_{ik} b_k}, \end{aligned}$$

so $p_1^{b_1} \cdots p_n^{b_n} \in NE^+$ if and only if:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \ker(A_1).$$

If there are no norms with a factor of 2 in U_+/U_+^2 , then this yields the formula:

$$\begin{aligned} r_4(d) &= 2\text{-rank } \ker(\rho^+) - 1 \\ &= \text{corank}(A_1) - 1 \\ &= \text{corank}(A) - 2 \\ &= n - 2 - \text{rank}(A). \end{aligned}$$

Otherwise, $2\text{-rank } \ker(\rho^+) = \text{corank}(A_1) + 1$, so $r_4(d) = n - 1 - \text{rank}(A)$.

Case 4: Finally, suppose that n is even, and $L = \mathbf{Q}((-d)^{\frac{1}{2}})$. Then $\text{Dis}(L/\mathbf{Q}) = -4d$. Define A_1 as in Case 3. Then $\text{rank}(A_1) = \text{rank}(A)$, since n is even, and $(-1)^{a_{ii}} = \left(\frac{P_i}{p_i}\right)$. In this case:

$$\begin{aligned} (p_1^{b_1} \cdots p_n^{b_n}, -d)_{p_i} &= \left(\frac{-1}{p_i}\right) \cdot \left(\frac{p_1}{p_i}\right)^{b_1} \cdots \left(\frac{-P_i}{p_i}\right)^{b_i} \cdots \left(\frac{p_n}{p_i}\right)^{b_n} \\ &= \left(\frac{p_1}{p_i}\right)^{b_1} \cdots \left(\frac{P_i}{p_i}\right)^{b_i} \cdots \left(\frac{p_n}{p_i}\right)^{b_n} \\ &= (-1)^{\sum a_{ik} b_k}, \end{aligned}$$

so $p_1^{b_1} \cdots p_n^{b_n} \in NE^+$ if and only if:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \ker(A_1).$$

Therefore, if there are no norms with a factor of 2 in U_+/U_+^2 , then:

$$\begin{aligned} r_4(-d) &= 2\text{-rank } \ker(\rho^+) - 1 \\ &= \text{corank } (A_1) - 1 \\ &= \text{corank } (A) - 1 \\ &= n - 1 - \text{rank}(A). \end{aligned}$$

Otherwise, $2\text{-rank } \ker(\rho^+) = \text{corank } (A_1) + 1$, so $r_4(-d) = n - \text{rank}(A)$.

In cases 3 and 4, we would like to be able to resolve the ambiguity that arises from the fact that 2 ramifies in E or L . Consider the real case. We have $2p_1^{b_1} \cdots p_n^{b_n} \in NE^+$ if and only if $(2p_1^{b_1} \cdots p_n^{b_n}, d)_{p_i} = +1$ for $1 \leq i \leq n$. However, this just means that $(2, d)_{p_i} \cdot (p_1^{b_1} \cdots p_n^{b_n}, d)_{p_i} = +1$ for each i ; and:

$$(2, d)_{p_i} = \left(\frac{2}{p_i} \right) = \begin{cases} +1 & \text{if } p_i \equiv 7 \pmod{8} \\ -1 & \text{if } p_i \equiv 3 \pmod{8}, \end{cases}$$

since each $p_i \equiv 3 \pmod{4}$. In terms of the matrix A_1 , this means that:

$$A_1 \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix},$$

where $(-1)^{c_i} = \left(\frac{2}{p_i} \right)$. The same criterion holds for Case 4.

The above information can be summarized as follows:

Theorem 2.3: Let $d = p_1 \cdots p_n$, where each $p_i \equiv 3 \pmod{4}$ is prime. Let A be the adjusted tournament matrix determined by $p_1, \dots, p_n$. Then:

- (i) If n is even, then $r_4(d) = n - 1 - \text{rank}(A)$, and $r_4(-d) = n - \text{rank}(A)$ or $n - 1 - \text{rank}(A)$.
- (ii) If n is odd, then $r_4(d) = n - 1 - \text{rank}(A)$ or $n - 2 - \text{rank}(A)$, and $r_4(-d) = n - 1 - \text{rank}(A)$.

Define the column vector $\vec{v}_2$ as follows:

$$\vec{v}_2 = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix},$$

where $(-1)^{c_i} = \left(\frac{2}{p_i}\right)$. Then in the cases where the formula is ambiguous, the greater value is taken when $\vec{v}_2 \in \text{Im}(A + I)$. ■

Example 2.1: Let $d = 3 \cdot 7 \cdot 11 = 231$, and let $E = \mathbf{Q}(d^{\frac{1}{2}})$. Then our adjusted tournament matrix A and vector $\vec{v}_2$ look like:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad \vec{v}_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix},$$

so $\text{rank}(A) = 2$, and $\vec{v}_2 \in \text{Im}(A + I)$. Therefore, $r_4(231) = 2 - \text{rank}(A) = 0$.

For an example of an extension where $\vec{v}_2 \notin \text{Im}(A + I)$, see the end of the first section of Chapter 3.

3. The Equivalence of the Two Methods

We have seen how $r_4(d)$ and $r_4(-d)$ can be computed for a product d of primes congruent to 3 (mod 4) using Rédei matrices and adjusted tournament matrices. In this section, we will show that both of these methods are, in fact, equivalent. We will consider the same four cases as in the last section, given by choosing a real or imaginary extension, with an even or odd number of primes dividing d . Of

course, in all cases we have $d = q_1 \cdots q_n$, with each $q_i \equiv 3 \pmod{4}$ prime, so in Rédei's matrix M_D , we will have $p_i = -q_i$ for $1 \leq i \leq n$, and possibly $p_{n+1} = 2$. In each case, let the entries of M_D be denoted by (m_{ij}) .

Case 1: Suppose n is even and $E = \mathbb{Q}(d^{\frac{1}{2}})$. Then $D = \text{Dis}(E/\mathbb{Q}) = d$, so we have the following M_D :

$$M_D = \begin{bmatrix} -\left(\frac{d}{q_1}\right) & -\left(\frac{q_2}{q_1}\right) & -\left(\frac{q_3}{q_1}\right) & \cdots & -\left(\frac{q_{n-1}}{q_1}\right) \\ -\left(\frac{q_1}{q_2}\right) & -\left(\frac{d}{q_2}\right) & -\left(\frac{q_3}{q_2}\right) & \cdots & -\left(\frac{q_{n-1}}{q_2}\right) \\ -\left(\frac{q_1}{q_3}\right) & -\left(\frac{q_2}{q_3}\right) & -\left(\frac{d}{q_3}\right) & \cdots & -\left(\frac{q_{n-1}}{q_3}\right) \\ \vdots & & & \ddots & \vdots \\ -\left(\frac{q_1}{q_{n-1}}\right) & -\left(\frac{q_2}{q_{n-1}}\right) & -\left(\frac{q_3}{q_{n-1}}\right) & \cdots & -\left(\frac{d}{q_{n-1}}\right) \\ -\left(\frac{q_1}{q_n}\right) & -\left(\frac{q_2}{q_n}\right) & -\left(\frac{q_3}{q_n}\right) & \cdots & -\left(\frac{q_{n-1}}{q_n}\right) \end{bmatrix}.$$

Define $B_D = (b_{ij}) \in M_{n \times (n-1)}(\mathbb{F}_2)$ in such a way so that $(-1)^{b_{ij}} = m_{ij}$. Then by Theorem 1.1, $r_4(d) = \text{corank}(B_D)$. Let A_D be obtained from B_D by adding a column on the right such that:

$$(-1)^{b_{in}} = \begin{cases} -\left(\frac{q_n}{q_i}\right) & \text{if } i \neq n \\ -\left(\frac{d}{q_n}\right) & \text{if } i = n. \end{cases}$$

Then it is easily seen that this new right-hand column is the sum of the remaining columns, so $\text{rank}(A_D) = \text{rank}(B_D)$. Since $\text{corank}(B_D) + \text{rank}(B_D) = n - 1$, $\text{corank}(B_D) = \text{corank}(A_D) - 1$. Furthermore, A_D^T is the adjusted tournament matrix A determined by $q_1, \dots, q_n$, so $\text{corank}(A_D) = \text{corank}(A)$. Thus, using Theorem 1.1, we have $r_4(d) = \text{corank}(B_D) = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$, which is exactly the value given by Theorem 2.3.

Case 2: Suppose n is odd, and $L = \mathbf{Q}((-d)^{\frac{1}{2}})$. Then $D = \text{Dis}(L/\mathbf{Q}) = -d$, so the matrix M_D looks like:

$$M_D = \begin{bmatrix} \left(\frac{\frac{d}{q_1}}{q_1}\right) & -\left(\frac{q_2}{q_1}\right) & -\left(\frac{q_3}{q_1}\right) & \dots & -\left(\frac{q_{n-1}}{q_1}\right) \\ -\left(\frac{q_1}{q_2}\right) & \left(\frac{\frac{d}{q_2}}{q_2}\right) & -\left(\frac{q_3}{q_2}\right) & \dots & -\left(\frac{q_{n-1}}{q_2}\right) \\ -\left(\frac{q_1}{q_3}\right) & -\left(\frac{q_2}{q_3}\right) & \left(\frac{\frac{d}{q_3}}{q_3}\right) & \dots & -\left(\frac{q_{n-1}}{q_3}\right) \\ \vdots & & & \ddots & \vdots \\ -\left(\frac{q_1}{q_{n-1}}\right) & -\left(\frac{q_2}{q_{n-1}}\right) & -\left(\frac{q_3}{q_{n-1}}\right) & \dots & \left(\frac{\frac{d}{q_{n-1}}}{q_{n-1}}\right) \\ -\left(\frac{q_1}{q_n}\right) & -\left(\frac{q_2}{q_n}\right) & -\left(\frac{q_3}{q_n}\right) & \dots & -\left(\frac{q_{n-1}}{q_n}\right) \end{bmatrix}.$$

Define B_D , A_D , and A as in Case 1. Then we find once again that $\text{corank}(B_D) = \text{corank}(A_D) - 1$, and $A_D^T = A$, so we have $r_4(d) = \text{corank}(B_D) = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$, which agrees once again with Theorem 2.3 .

Case 3: Suppose n is odd and E and D are as above. Then $D = 4d$, so we have the following matrix M_D :

$$M_D = \begin{bmatrix} -\left(\frac{\frac{d}{q_1}}{q_1}\right) & -\left(\frac{q_2}{q_1}\right) & -\left(\frac{q_3}{q_1}\right) & \dots & -\left(\frac{q_n}{q_1}\right) \\ -\left(\frac{q_1}{q_2}\right) & -\left(\frac{\frac{d}{q_2}}{q_2}\right) & -\left(\frac{q_3}{q_2}\right) & \dots & -\left(\frac{q_n}{q_2}\right) \\ -\left(\frac{q_1}{q_3}\right) & -\left(\frac{q_2}{q_3}\right) & -\left(\frac{\frac{d}{q_3}}{q_3}\right) & \dots & -\left(\frac{q_n}{q_3}\right) \\ \vdots & & & \ddots & \vdots \\ -\left(\frac{q_1}{q_n}\right) & -\left(\frac{q_2}{q_n}\right) & -\left(\frac{q_3}{q_n}\right) & \dots & -\left(\frac{\frac{d}{q_n}}{q_n}\right) \\ \left(\frac{2}{q_1}\right) & \left(\frac{2}{q_2}\right) & \left(\frac{2}{q_3}\right) & \dots & \left(\frac{2}{q_n}\right) \end{bmatrix},$$

since $\left(\frac{-q_i}{2}\right) = (-1)^{\frac{-q_i-1}{4}} = \left(\frac{2}{q_i}\right)$. Let B_D be defined as above. Let A_D be obtained from B_D by removing the last row, and let $\vec{v}_2 \in \mathbf{F}_2^n$ be the column vector such that $\vec{v}_2^T$ is the last row of B_D . Then we have the following:

$$\text{corank}(A_D) = \begin{cases} \text{corank}(B_D) & \text{if } \vec{v}_2 \in c(A_D^T) \\ \text{corank}(B_D) + 1 & \text{otherwise} \end{cases}.$$

In this case $A_D^T = A + I$, where A is the adjusted tournament matrix determined by $q_1, \dots, q_n$, so $\text{corank}(A_D) = \text{corank}(A + I) = \text{corank}(A) - 1$, since n is odd. Therefore, if $\vec{v}_2 \in c(A + I)$, then $r_4(d) = \text{corank}(B_D) = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$; otherwise, $r_4(d) = \text{corank}(B_D) = \text{corank}(A) - 2 = n - 2 - \text{rank}(A)$. In both cases, Theorem 1.1 agrees with Theorem 2.3 .

Case 4: Suppose n is even and $L = \mathbf{Q}((-d)^{\frac{1}{2}})$. Then $D = \text{Dis}(L/\mathbf{Q}) = -4d$, so we have the following matrix M_D :

$$M_D = \begin{bmatrix} \left(\frac{d}{q_1}\right) & -\left(\frac{q_2}{q_1}\right) & -\left(\frac{q_3}{q_1}\right) & \dots & -\left(\frac{q_n}{q_1}\right) \\ -\left(\frac{q_1}{q_2}\right) & \left(\frac{d}{q_2}\right) & -\left(\frac{q_3}{q_2}\right) & \dots & -\left(\frac{q_n}{q_2}\right) \\ -\left(\frac{q_1}{q_3}\right) & -\left(\frac{q_2}{q_3}\right) & \left(\frac{d}{q_3}\right) & \dots & -\left(\frac{q_n}{q_3}\right) \\ \vdots & & & \ddots & \vdots \\ -\left(\frac{q_1}{q_n}\right) & -\left(\frac{q_2}{q_n}\right) & -\left(\frac{q_3}{q_n}\right) & \dots & \left(\frac{d}{q_n}\right) \\ \left(\frac{q_1}{2}\right) & \left(\frac{q_2}{2}\right) & \left(\frac{q_3}{2}\right) & \dots & \left(\frac{q_n}{2}\right) \end{bmatrix}.$$

Define B_D , A_D , and $\vec{v}_2$ as in the previous case. Then, again, we have:

$$\text{corank}(A_D) = \begin{cases} \text{corank}(B_D) & \text{if } \vec{v}_2 \in c(A_D^T) \\ \text{corank}(B_D) + 1 & \text{otherwise} \end{cases}.$$

In this case, $A_D = A + J$, where A is the adjusted tournament matrix determined by $q_1, \dots, q_n$. Thus $A_D = A^T + I$, so $A_D^T = A + I$. Therefore, if $\vec{v}_2 \in c(A + I)$, then $r_4(-d) = \text{corank}(B_D) = \text{corank}(A + I) = \text{corank}(A) = n - \text{rank}(A)$, since n is even. If $\vec{v}_2 \notin c(A + I)$, then $r_4(-d) = \text{corank}(B_D) = \text{corank}(A + I) - 1 = \text{corank}(A) - 1 = n - 1 - \text{rank}(A)$. Once again, in both cases Theorem 1.1 agrees with Theorem 2.3 .

4. A Useful Result of Gerth's

In a 1984 paper [Ge4], Gerth uses Rédei matrices to establish various density results for the possible values of $r_4^+(d)$ and $r_4^+(-d)$. These calculations, using Markov processes, involve finding the probabilities for an increase of 1 or 2 in these values when one or two prime factors are added to d . In this paper, Gerth proved a result concerning anti-symmetric matrices over $\mathbb{F}_2$ which we will use often in the following chapter:

Theorem 4.1: Let $A \in M_{n \times n}(\mathbb{F}_2)$ be an antisymmetric matrix. Let $r = \text{rank}(A)$ (over $\mathbb{F}_2$). Let $c(A)$ denote the column space of A . If n is even, then:

$$\dim[c(A) + c(A^T)] = n \text{ and } \dim[c(A) \cap c(A^T)] = 2r - n.$$

If n is odd, then:

$$\dim[c(A) + c(A^T)] \geq n - 1 \text{ and } \dim[c(A) \cap c(A^T)] \leq 2r - n + 1.$$

Proof. We make use of the fact that:

$$\text{rank}(I + J) = \begin{cases} n & \text{if } n \text{ is even} \\ n - 1 & \text{if } n \text{ is odd,} \end{cases}$$

where I and J denote the $n \times n$ identity matrix and matrix with all entries one, as mentioned earlier.

Suppose $\vec{v} \in c(I + J)$, say $\vec{v} = (I + J)\vec{w}$. Then since $A + A^T = I + J$:

$$\vec{v} = (I + J)\vec{w} = A\vec{w} + (A + I + J)\vec{w} = A\vec{w} + A^T\vec{w}.$$

Thus $c(I + J) \subseteq [c(A) + c(A^T)]$, so if n is even, $\dim[c(A) + c(A^T)] = n$. Therefore:

$$\dim[c(A) \cap c(A^T)] = \dim[c(A)] + \dim[c(A^T)] - \dim[c(A) + c(A^T)] = 2r - n.$$

If n is odd, the result follows using the same formulae. ■

Corollary 4.1: Let A , n , and r be as defined above. If n is even, then the result above insures that $2r - n \geq 0$, so $r \geq \frac{n}{2}$. If n is odd, then $2r - n + 1 \geq 0$, so $r \geq \frac{n+1}{2}$. ■

Suppose $d = p_1 \cdots p_n$, with each $p_i \equiv 3 \pmod{4}$ prime. We immediately obtain the following bounds for $r_4(d)$:

<u>n even</u>	<u>n odd</u>
$0 \leq r_4(-d) \leq \frac{n}{2}$	$0 \leq r_4(-d) \leq \frac{n-1}{2}$
$0 \leq r_4(d) \leq \frac{n}{2} - 1$	$0 \leq r_4(d) \leq \frac{n-1}{2}$

In the first section of the next chapter, we will see that any value for $r_4(d)$ or $r_4(-d)$ within these ranges can occur, for any n .

CHAPTER III

RESULTS USING ADJUSTED TOURNAMENT MATRICES

1. Realization of All Possible Values for $r_4(m)$, $r_4(-m)$

We have seen that, for any integer m that is a product of primes congruent to 3 (mod 4), $r_4(m)$ and $r_4(-m)$ can be determined by finding the rank of the adjusted tournament matrix associated to the prime divisors of m . Before continuing, we need to determine which adjusted tournament matrices arise in this manner. The following lemma demonstrates, as a consequence of Dirichlet's theorem on primes in arithmetic progressions, that any given adjusted tournament matrix can be realized in infinitely many ways by appropriate choice of primes.

Lemma 1.1: Let A be an adjusted tournament matrix of size n . Then there are primes $p_1, \dots, p_n$, each $p_i \equiv 3 \pmod{4}$, whose associated adjusted tournament matrix is A .

Proof. By induction on n . If $n = 2$ the result is trivial.

Suppose the result is known for all values smaller than n . Let $A = (a_{ij})$ be an $n \times n$ adjusted tournament matrix. Then we may choose $p_1, \dots, p_{n-1}$ prime, each $p_i \equiv 3 \pmod{4}$, such that $\left(\frac{p_i}{p_j}\right) = (-1)^{a_{ji}}$ for $1 \leq i, j \leq n-1$, $i \neq j$. Choose integers $b_1, \dots, b_{n-1}$ such that $\left(\frac{b_i}{p_i}\right) = (-1)^{a_{in}}$ for each i . Let $b = \sum_{i=1}^{n-1} b_i p_1^2 \cdots \hat{p}_i^2 \cdots p_{n-1}^2$. Then, if $1 \leq k \leq n-1$:

$$\begin{aligned}
\left(\frac{b}{p_k}\right) &= \left(\frac{\sum_{i=1}^{n-1} b_i p_1^2 \cdots \hat{p}_i^2 \cdots p_{n-1}^2}{p_k}\right) \\
&= \left(\frac{b_k p_1^2 \cdots \hat{p}_k^2 \cdots p_{n-1}^2}{p_k}\right) \\
&= \left(\frac{b_k}{p_k}\right) \\
&= (-1)^{a_{kn}}.
\end{aligned}$$

Furthermore, b is relatively prime to each p_i . Adding $p_1 \cdots p_n$ to b changes none of these properties, so we may assume that b is odd.

Define c as follows:

$$c = \begin{cases} b, & \text{if } b \equiv 3 \pmod{4} \\ b + 2p_1 \cdots p_n, & \text{if } b \equiv 1 \pmod{4} \end{cases}.$$

Let $d = 4p_1 \cdots p_n$. Then c and d are relatively prime. For any $k \geq 0$, $c + kd \equiv 3 \pmod{4}$, and $\left(\frac{c+kd}{p_i}\right) = \left(\frac{b}{p_i}\right) = (-1)^{a_{in}}$ for $1 \leq i \leq n-1$. By Dirichlet's theorem, we can find infinitely many primes in the sequence $\{c + kd\}_{k=0}^{\infty}$. Choose p_n to be any one of these primes. This completes the proof. $\blacksquare$

The lemma above tells us that any information we can obtain concerning ranks of adjusted tournament matrices will yield information concerning possible values for $r_4(d)$.

So far, the only restriction on $r_4(d)$ imposed by our formulas is that arising from the result of Gerth mentioned in the last section of Chapter 1. In the remainder of this section, we will see that, for any n , there are adjusted tournament matrices of size n with any rank in the range of possible values. Thus, if we choose primes carefully enough to resolve the ambiguities in our formulas due to the possibility of norms congruent to 2 (mod 4), it is possible to find values for m with any value of $r_4(m)$ in the range given in Chapter 1. Before proceeding, it is necessary to make the following observations.

Given an adjusted tournament matrix A of size $n > 1$, define A' to be the $(n - 1) \times (n - 1)$ matrix obtained from A by deleting the rightmost column and the bottom row. Then A' is anti-symmetric. The bottom row of A , being the sum of the remaining rows, is completely determined by them. Likewise, the rightmost column of A , being either the sum of the remaining columns, or distinct from that sum in every position, is determined by the remaining columns. Using this information, we obtain the following lemma:

Lemma 1.2: The map $A \mapsto A'$, defined above, produces a 1-1 correspondence between adjusted tournament matrices of size n and anti-symmetric, square $\{0, 1\}$ -matrices of size $n - 1$. If n is odd, then $\text{rank}(A') = \text{rank}(A)$. If n is even, then $\text{rank}(A') = \text{rank}(A)$ if and only if $\text{Im}(A')$ contains the column vector consisting completely of ones. Otherwise, $\text{rank}(A') = \text{rank}(A) - 1$.

Proof. It remains only to prove the statements concerning rank. Suppose A is an adjusted tournament matrix of size n . Then the last row of A is the sum of the remaining rows, so removing it does not change the rank of the matrix. This immediately tells us that moving from A to A' decreases the rank by no more than one. If n is odd, the rightmost column of A is the sum of the remaining columns, so its removal does not change the rank of the matrix. However, when n is even, each row has odd weight, so each entry of the rightmost column of A can be obtained by adding 1 to the sum of the remaining entries in its row. If $\text{Im}(A')$ contains the column vector made up of $n - 1$ ones, then the column vector made up of n ones lies within the span of the left $n - 1$ columns of A itself (since each column of A has even weight). Thus, the rightmost column of A lies within the span of the remaining columns, so removing the rightmost column does not change

the rank. Conversely, if moving from A to A' does not change the rank, then the last column of A must lie within the span of the remaining columns. Thus, since the last column is the sum of the remaining columns, plus the column vector of n ones, that column vector must lie within the span of the remaining columns, and thus the column vector of $n - 1$ ones lies within the span of the columns of A' . ■

It follows that, to find an adjusted tournament matrix of a given rank and size n , we need only find an anti-symmetric matrix of size $n - 1$ of the same rank, with the column vector of $n - 1$ ones within its column space if n is even.

Lemma 1.3: Let $n > 1$, and suppose $\lfloor \frac{n}{2} \rfloor \leq k \leq n - 1$. Let $j = n - 1 - k$. Then there is an adjusted tournament matrix A with rank k .

Proof. Define A' as follows:

$$A' = \begin{bmatrix} M_1 & J \\ 0 & M_2 \end{bmatrix},$$

where J is a $2j \times (n - 1 - 2j)$ matrix consisting completely of ones; M_1 is square of size $2j$, with one zero followed by $2j - 1$ ones in the first two rows, three zeroes followed by $2j - 3$ ones in the second two rows, ..., $2j - 1$ zeroes followed by a single one in the last two rows; and M_2 is square of size $n - 1 - 2j$, with ones on and above the diagonal and zeroes below it:

$$M_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & \dots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & \dots & 1 & 1 & 1 & 1 \\ \vdots & & & & \ddots & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 & 1 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix}.$$

Then it is clear that $\text{rank}(M_1) = j$, and $\text{rank}(M_2) = n - 1 - 2j$. Furthermore, it can be seen that the only row vector within the span of the first $2j$ rows of A' with zeroes in each of the first $2j$ positions is the zero vector; thus, none of the remaining $n - 1 - 2j$ rows lie within the span of the first $2j$ rows. Therefore:

$$\begin{aligned}\text{rank}(A') &= \text{rank}(M_1) + \text{rank}(M_2) \\ &= j + n - 1 - 2j \\ &= k.\end{aligned}$$

It is also apparent that A' is anti-symmetric; all entries above its diagonal are ones, and all entries below are zeroes. Let A be the adjusted tournament matrix of size n corresponding to A' . Since the rightmost column of A' is made up completely of ones, $\text{rank}(A) = \text{rank}(A') = k$ whether n is even or odd. ■

Thus, given n , we can find adjusted tournament matrices with any rank k in the range $\lfloor \frac{n}{2} \rfloor \leq k \leq n - 1$.

Example 1.1: Let $n = 8$, $k = 5$. Then:

$$M_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ and } M_2 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

The resulting matrix A , with rank 5, and its associated tournament graph look like:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Fig. 3.1.1

Example 1.2: If $n = 8$ and $k = 6$, we obtain the following rank 6 matrix and tournament graph:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Fig. 3.1.2

As before, assume that d is a product of n distinct primes, each congruent to 3 (mod 4). We have just shown that, if n is even, $r_4(d)$ may take on any value in the range $0 \leq r_4(d) \leq \frac{n}{2} - 1$, and that if n is odd, $r_4(-d)$ may take on any value in the range $0 \leq r_4(-d) \leq \frac{n-1}{2}$. In the cases where 2 ramifies, however, it is a bit more difficult to establish the range of possible values.

Suppose n is even, and let A be an adjusted tournament matrix associated to d . Then $r_4(-d) = n - \text{rank}(A)$ if there are norms congruent to 2 (mod 4) from $\mathbb{Q}((-d)^{\frac{1}{2}})$ dividing $-4d$; otherwise, $r_4(-d) = n - 1 - \text{rank}(A)$. Examining the proof of the first lemma, one finds that it can easily be restricted to insure that any given adjusted tournament matrix can be realized with primes congruent to 7 (mod 8). Choose d to be a product of such primes, in such a way that A has rank $\frac{n}{2}$. Then, since the Kronecker symbol $\left(\frac{2}{p}\right) = +1$ for all prime divisors p of d , there must be norms congruent to 2 (mod 4) dividing $-4d$, since the vector $\vec{v}_2$ mentioned in Theorem 2.3 of Chapter 1 is the zero vector. Therefore, $r_4(-d) = \frac{n}{2}$.

We may also choose $p_1, \dots, p_{n-1} \equiv 3 \pmod{8}$ and $p_n \equiv 7 \pmod{8}$ in such a way that the adjusted tournament matrix A resulting is the rank $n - 1$ matrix

constructed above (A' has ones above and on the diagonal):

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 0 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 & 0 \\ & \vdots & & \ddots & & \vdots & \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 1 & 0 & 1 & \dots & 1 & 0 & 1 \end{bmatrix}.$$

In this case, by Theorem 2.3 of Chapter 1, there are norms congruent to 2 (mod 4) dividing $-4d$ if and only if the column vector with one zero, in the bottom position, lies within $\text{Im}(A + I)$. However, it is apparent from the construction of A that the $(n - 1)^{\text{st}}$ row of $A + I$ consists completely of zeroes; thus, the column vector in question cannot lie within $\text{Im}(A + I)$. Therefore, in this case, $r_4(-d) = 0$, so when n is even, $r_4(-d)$ may take on any value in the range $0 \leq r_4(-d) \leq \frac{n}{2}$. Similarly, when n is odd, $r_4(d)$ may take on any value in the range $0 \leq r_4(d) \leq \frac{n-1}{2}$. These results are summarized in the following theorem:

Theorem 1.1: Let $n > 0$. If n is even, and $0 \leq k \leq \frac{n}{2}$, $0 \leq j \leq \frac{n}{2} - 1$, then there exist primes $p_1, \dots, p_n, q_1, \dots, q_n \equiv 3 \pmod{4}$ such that $r_4(p_1 \cdots p_n) = j$ and $r_4(-q_1 \cdots q_n) = k$. If n is odd, and $0 \leq k \leq \frac{n-1}{2}$, then there exist primes $p_1, \dots, p_n, q_1, \dots, q_n \equiv 3 \pmod{4}$ such that $r_4(p_1 \cdots p_n) = r_4(-q_1 \cdots q_n) = k$. In both cases, $p_1, \dots, p_n$ and $q_1, \dots, q_n$ can be chosen in infinitely many ways. ■

The following two examples illustrate this result for $n = 3$ and 4:

Example 1.3: Suppose $n = 3$. Then $0 \leq r_4(d), r_4(-d) \leq 1$. When $d = 3 \cdot 11 \cdot 19$, we obtain the following matrix:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \text{ and } A + I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Thus $\text{rank}(A) = 2$. Since $3, 11, 19 \equiv 3 \pmod{8}$, and $A + I$ is invertible, $2 \cdot 3 \cdot 11 \cdot 19$ is a norm from $\mathbb{Q}(\sqrt{627})$, so $r_4(627) = 2 - \text{rank}(A) = 0$. $r_4(-627) = 2 - \text{rank}(A) = 0$ also.

When $d = 3 \cdot 11 \cdot 83$, we obtain the rank 1 matrix:

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \text{ and } A + I = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

The right-hand column of $A + I$ is all ones, and $3, 11, 83 \equiv 3 \pmod{8}$, so $2 \cdot 3 \cdot 11 \cdot 83$ is a norm from $\mathbb{Q}(\sqrt{2739})$, so $r_4(2739) = 2 - \text{rank}(A) = 1$. $r_4(-2739) = 2 - \text{rank}(A) = 1$ also.

Example 1.4: Suppose $n = 4$. Then $0 \leq r_4(d) \leq 1$ and $0 \leq r_4(-d) \leq 2$. When $d = 3 \cdot 11 \cdot 83 \cdot 127$, we obtain the matrix:

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}, \text{ with } A + I = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Thus $\text{rank}(A)=3$, so $r_4(347,853) = 3 - \text{rank}(A) = 0$. Since $3, 11, 83 \equiv 3 \pmod{8}$ and $127 \equiv 7 \pmod{8}$, we can see from $A + I$ that there are no norms dividing the discriminant that are congruent to $2 \pmod{4}$. Thus $r_4(-347,853) = 3 - \text{rank}(A) = 0$.

When $d = 3 \cdot 11 \cdot 83 \cdot 239$, we obtain the matrix:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ with } A + I = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus $\text{rank}(A)=2$, so $r_4(654,621) = 3 - \text{rank}(A) = 1$. Since $3, 11, 83 \equiv 3 \pmod{8}$ and $239 \equiv 7 \pmod{8}$, we see from the third column of $A + I$ that $2 \cdot 3 \cdot 11 \cdot 83$ is a norm. Therefore, $r_4(-654,621) = 4 - \text{rank}(A) = 2$.

Finally, when $d = 3 \cdot 11 \cdot 167 \cdot 127$, we obtain the same matrix A , with rank 3, as in the case when $d = 3 \cdot 11 \cdot 83 \cdot 127$. However, since $3, 11 \equiv 3 \pmod{8}$ and $167, 127 \equiv 7 \pmod{8}$, and since the sum of the first and third columns of $A + I$

has two ones, in the top two positions, we find that $2 \cdot 3 \cdot 11$ is a norm; therefore, $r_4(699, 897) = 4 - \text{rank}(A) = 1$.

2. Minimal Rank Adjusted Tournament Matrices

As we have seen, the smallest rank possible for an adjusted tournament matrix of size n is either $\frac{n}{2}$ or $\frac{n-1}{2}$, according to whether n is even or odd. In this section, we will be concerned with when these ranks take on their minimal values. We have two main results; one holds only for matrices of even size, and the other holds in general.

When $n \leq 5$, we find that the only adjusted tournament matrix of size n with minimal rank is the matrix for the **transitive** tournament; that is, the unique tournament of size n with no 3-cycles. It is easily shown that for any n , the adjusted tournament matrix for the transitive tournament of size n has minimal rank. However, when $n = 6$, we find a nontransitive tournament with minimal rank:

Example 2.1: Consider the adjusted tournament matrix and corresponding tournament shown below:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Fig. 3.2.1

This is the only example, up to graph isomorphism, of a nontransitive tournament of size 6 with minimal rank; however, it is possible to construct an infinite number of nontransitive tournaments of greater size with minimal rank; in particular, there are such tournaments of any size p , where p is any prime congruent to 7 (mod 8).

Example 2.2: When $n = 7$, we have the following nontransitive adjusted tournament matrix with minimal rank:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

In a later section, we will put this second example in a more general setting.

Our first result concerns tournaments of even size. It turns out that, while minimal rank tournaments of even size may not be transitive, they are easily distinguished.

Proposition 2.1: Let n be a positive even integer. Then an adjusted tournament matrix A of size n has minimal rank if and only if each row of A is identical to exactly one other row.

Proof. If the latter statement is true of A , the former statement is immediate. Suppose, however, that A has minimal rank. Furthermore, suppose that one of its row vectors, say $\vec{r}$, is distinct from all the other rows of A . Denote these other row vectors by $\vec{s}_1, \dots, \vec{s}_{n-1}$. Now, since each column of A has even weight, $\vec{s}_1 + \dots + \vec{s}_{n-1} = \vec{r}$, so $\text{Span}((\vec{s}_1 + \vec{r})^T, \dots, (\vec{s}_{n-1} + \vec{r})^T) = \text{Im}(A^T)$, the “row space” of A . Furthermore, each column vector $(\vec{s}_1 + \vec{r})^T, \dots, (\vec{s}_{n-1} + \vec{r})^T$ has even weight, since each row of A has odd weight, and the sum of two vectors of the same weight (mod 2) has even weight. Therefore, we may find a basis $\{\vec{t}_1, \dots, \vec{t}_{\frac{n}{2}}\}$ for $\text{Im}(A^T)$, where each $\vec{t}_i$ has even weight. Also, since each column of A has even weight, we can find a basis $\{\vec{v}_1, \dots, \vec{v}_{\frac{n}{2}}\}$ of vectors with even weight for $\text{Im}(A)$. Now, by Gerth’s result in [Ge4], we know that $\text{Im}(A) \cap \text{Im}(A^T) = \{0\}$, since

$\text{rank}_{\mathbb{F}_2}(A) = \frac{n}{2}$. Thus, the set $\{\vec{t}_1, \dots, \vec{t}_{\frac{n}{2}}, \vec{v}_1, \dots, \vec{v}_{\frac{n}{2}}\}$ is linearly independent; that is, it is a basis for $\mathbb{F}_2^n$. However, each of these vectors has even weight, and the subspace of vectors of even weight in $\mathbb{F}_2^n$ has dimension $n - 1$, a contradiction. Thus, each row of A has another row identical to it. Finally, it follows that since A has minimal rank and even size, it is impossible for three rows to be identical. Otherwise, since each row has been shown to be identical to at least one other row, we would have $\text{rank}(A) < \frac{n}{2}$, a contradiction. (In fact, it can easily be shown that no anti-symmetric $\{0, 1\}$ -matrix can have three identical rows.) ■

The main result of this section gives a necessary and sufficient condition for any adjusted tournament matrix to have minimal rank.

Theorem 2.1: An adjusted tournament matrix A , of given size n , has minimal rank if and only if it is idempotent.

Proof. We will make extensive use of the equation:

$$A = A^T + I + J, \tag{1}$$

where I and J are as mentioned in the introduction.

Suppose, first, that A is idempotent. We consider A as a linear transformation on the (column) vector space of $\mathbb{F}_2^n$. Then $A|_{\text{Im}(A)} = I|_{\text{Im}(A)}$. Since each column of A has even weight, and each vector in $\text{Im}(A)$ is a sum of columns of A , each member of $\text{Im}(A)$ has even weight. Therefore, $J|_{\text{Im}(A)} = 0$. Thus, restricting each map in equation (1) to $\text{Im}(A)$, we find that $A|_{\text{Im}(A)} = A|_{\text{Im}(A)} + A^T|_{\text{Im}(A)}$; in other words, $A^T|_{\text{Im}(A)} = 0$. Therefore, $\text{Im}(A) \subseteq \ker(A^T)$, so $\text{rank}(A^T) \leq n - \text{rank}(A)$. But $\text{rank}(A) = \text{rank}(A^T)$, so $2 \cdot \text{rank}(A) \leq n$. Thus A has minimal rank.

Suppose conversely that A has minimal rank; i.e., that $2 \cdot \text{rank}(A) \leq n$. Then by Gerth's result in [Ge3], $\text{Im}(A) \cap \text{Im}(A^T) = \{0\}$. Once again, restrict equation

(1) to $\text{Im}(A)$. Then again $J|_{\text{Im}(A)} = 0$, so $A|_{\text{Im}(A)} + I|_{\text{Im}(A)} = A^T|_{\text{Im}(A)}$. The image of the map on the left is contained within $\text{Im}(A)$, and certainly $\text{Im}(A^T|_{\text{Im}(A)}) \subseteq \text{Im}(A^T)$, so $\text{Im}(A^T|_{\text{Im}(A)}) \subseteq \text{Im}(A) \cap \text{Im}(A^T) = \{0\}$. Thus $A|_{\text{Im}(A)} = I|_{\text{Im}(A)}$, but this implies that A is idempotent. ■

The following corollary details the implications of this theorem for the values $r_4(d)$ and $r_4(-d)$:

Corollary 2.1: Suppose $d = p_1 \cdots p_n$, with each $p_i \equiv 3 \pmod{4}$ prime. Let A be the adjusted tournament matrix associated with $p_1, \dots, p_n$, and let the column vector $\vec{v}_2$ be defined as in Theorem 2.3 of Chapter 1. Then:

- (i) If n is even, then $r_4(d) = \frac{n}{2} - 1$ if and only if A is idempotent. $r_4(-d) = \frac{n}{2}$ if and only if A is idempotent and $\vec{v}_2 \in \text{Im}(A + I)$.
- (ii) If n is odd, then $r_4(d) = \frac{n-1}{2}$ if and only if A is idempotent and $\vec{v}_2 \in \text{Im}(A + I)$. $r_4(-d) = \frac{n-1}{2}$ if and only if A is idempotent. ■

The theorem above raises further questions concerning powers of adjusted tournament matrices. One wonders whether there is a more general relationship between the minimal polynomial of an adjusted tournament matrix, over $\mathbf{F}_2$, and the rank of the matrix. However, it seems unlikely, in view of the minimal polynomials for the adjusted tournament matrices for the 12 nonisomorphic tournaments of size 5, that a more general relationship exists. For example, the following three adjusted tournament matrices:

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

have minimal polynomials $x^4 + x$, $x(x^4 + x + 1)$, and $x(x^2 + x + 1)$, and ranks 3, 4, and 4, respectively.

We can obtain another interpretation of the adjusted tournament matrix if we modify our original tournament graph, adding “loops” at vertices to insure that each vertex has an even indegree, then the associated adjusted tournament matrix is the adjacency matrix for this digraph. For example, the following tournament (here shown with its adjusted tournament matrix):

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

can be modified as follows:

It is a well-known result in graph theory that, if $A = (a_{ij})$ is the adjacency matrix for a digraph D , then the number of paths of length k from vertex i to vertex j is given by c_{ij} , where $A^k = (c_{ij})$, with all multiplication in $\mathbb{Z}$. When A^k is calculated mod 2, the resulting entries yield the number of paths from one vertex to another, modulo 2. Perhaps this approach will yield further information concerning the rank of the adjusted tournament matrix.

3. A Condition for $r_4(-m) = r_4(m)$

Uehara proved the following result in a 1989 paper [U]:

Theorem 3.1: Let $m > 1$ be a square-free rational integer.

- (i) In the case $m \equiv 1 \pmod{4}$, $r_4^+(m) = r_4^+(-m)$ if there exists a $(-4m)$ -splitting $\{d_1, d_2\}$ with $d_1 \equiv 5 \pmod{8}$ for which the equation $x^2 = d_1y^2 + d_2z^2$ has a nontrivial integral solution, and $r_4^+(-m) = r_4^+(m) + 1$ otherwise.
- (ii) In the case $m \equiv 2 \pmod{4}$, $r_4^+(-m) = r_4^+(m) + 1$ if there exists a $(-4m)$ -splitting $\{d_1, d_2\}$ with $d_1 \equiv 1 \pmod{4}$ for which the equation $x^2 = -d_1y^2 + d_2z^2$ has a nontrivial integral solution, and $r_4^+(-m) = r_4^+(m)$ otherwise.
- (iii) In the case $m \equiv 3 \pmod{4}$, $r_4^+(-m) = r_4^+(m) + 1$ if there exists a $4m$ -splitting $\{d_1, d_2\}$ with $d_1 \equiv 5 \pmod{8}$ for which the equation $x^2 = d_1y^2 + d_2z^2$ has a nontrivial integral solution, and $r_4^+(-m) = r_4^+(m)$ otherwise.

Recall that a D -splitting is an unordered factorization $\{d_1, d_2\}$ of a discriminant D into two discriminants d_1 and d_2 . In this section, we will rephrase this result, in the case where m is a product of primes each congruent to 3 (mod 4), in terms of adjusted tournament matrices. We will then prove part of this result for this special case, using matrices.

Let us first recall our formulas for $r_4(m)$ when $m = p_1 \cdots p_n$, each $p_i \equiv 3 \pmod{4}$. Let A be the adjusted tournament matrix associated with $p_1, \dots, p_n$. Then if n is even, $r_4(-m) + \text{rank}(A) = n$ or $n - 1$, and $r_4(m) + \text{rank}(A) = n - 1$. If n is odd, then $r_4(-m) + \text{rank}(A) = n - 1$, and $r_4(m) + \text{rank}(A) = n - 1$ or $n - 2$.

In both cases where an ambiguity exists, the smaller value is taken on when no norms congruent to 2 (mod 4) divide $\text{Dis}(\mathbf{Q}(m^{\frac{1}{2}})/\mathbf{Q})$ or $\text{Dis}(\mathbf{Q}((-m)^{\frac{1}{2}})/\mathbf{Q})$, whichever is appropriate. Thus, when n is even, $r_4(m) = r_4(-m)$ if and only if

there are no norms congruent to 2 (mod 4) dividing $\text{Dis}(\mathbb{Q}((-m)^{\frac{1}{2}})/\mathbb{Q})$, and when n is odd, $r_4(m) = r_4(-m)$ if and only if there are norms congruent to 2 (mod 4) dividing $\text{Dis}(\mathbb{Q}(m^{\frac{1}{2}})/\mathbb{Q})$.

Furthermore, we have seen already that the existence of an even norm as described above depends on the presence of a certain vector in $\text{Im}(A + I)$. Suppose $p_1, \dots, p_l \equiv 3 \pmod{8}$ and $p_{l+1}, \dots, p_n \equiv 7 \pmod{8}$. Then the vector $\vec{v}_2$ mentioned in Theorem 2.3 of Chapter 1 has ones in positions 1 through l , and zeroes in positions $l + 1$ through n , so $2p_1^{b_1} \cdots p_n^{b_n}$ is a norm if and only if:

$$(A + I) \begin{bmatrix} b_1 \\ \vdots \\ b_l \\ b_{l+1} \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

This is true since the Legendre symbol $\left(\frac{2}{p_i}\right) = +1$ if and only if $p_i \equiv 7 \pmod{8}$.

Returning to Uehara's theorem, we note that, by the Minkowski-Hasse Theorem, $x^2 = d_1 y^2 + d_2 z^2$ has a nontrivial integral solution if and only if the Hilbert symbol $(d_1, d_2)_p = +1$ for all primes p , both finite and infinite. To check the latter condition, we need only check those finite primes dividing $d_1 d_2$. As a matter of fact, we need only check odd primes, since we always have $d_2 \equiv 4 \pmod{8}$ in cases (i) and (iii) of the theorem.

Suppose $d_1 = p_1^{b_1} \cdots p_n^{b_n}$, and let $1 \leq i \leq n$. When n is even, $d_1 d_2 = -4m$ and $(d_1, -m) = (-1)^{\sum a_{ik} b_k}$, where $(a_{ij}) = A + I$. Therefore:

$$\begin{aligned} (d_1, d_2)_{p_i} &= (d_1, d_1)_{p_i} (d_1, d_1 d_2)_{p_i} \\ &= (d_1, d_1)_{p_i} (d_1, -4m)_{p_i} \\ &= (d_1, d_1)_{p_i} (d_1, -m)_{p_i} \\ &= (d_1, d_1)_{p_i} (-1)^{\sum a_{ik} b_k}. \end{aligned}$$

Thus, $(d_1, d_2)_{p_i} = +1$ for all i if and only if $(d_1, d_1)_{p_i} = (-1)^{\sum a_{ik} b_k}$ for all i . Now if $b_i = 1$, then p_i divides d_1 , so $(d_1, d_1)_{p_i} = (p_i, p_i)_{p_i} = \left(\frac{-1}{p_i}\right) = -1$. If $b_i = 0$, then p_i does not divide d_1 , so $(d_1, d_1)_{p_i} = +1$. Thus, $(d_1, d_2)_{p_i} = +1$ for all i if and only if $\sum a_{ik} b_k \equiv b_i \pmod{2}$ for all i ; in other words, if and only if:

$$(A + I) \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

When n is odd, $d_1 d_2 = 4m$, and $(d_1, m)_{p_i} = (-1)^{\sum a_{ik} b_k}$. These two changes lead to the same result: $(d_1, d_2)_{p_i} = +1$ for all i if and only if the column vector made up of entries $b_1, \dots, b_n$ is fixed by the matrix $A + I$.

When n is even, so that $d_1 d_2 = -4m$, it is possible that $d_1 < 0$. Suppose $d_1 = -p_1^{b_1} \cdots p_n^{b_n}$, and let $1 \leq i \leq n$. Then:

$$\begin{aligned} (d_1, d_2)_{p_i} &= (-1, d_2)_{p_i} (-d_1, d_2)_{p_i} \\ &= (-1, d_2)_{p_i} (-d_1, d_1)_{p_i} (-d_1, d_1 d_2)_{p_i} \\ &= (-1, d_2)_{p_i} (-d_1, -4m)_{p_i} \\ &= (-1, d_2)_{p_i} (-d_1, m)_{p_i} \\ &= (-1, d_2)_{p_i} (-1)^{\sum a_{ik} b_k}, \end{aligned}$$

where, once again, $(a_{ij}) = A + I$. Thus, $(d_1, d_2)_{p_i} = +1$ for all i if and only if $(-1, d_2)_{p_i} = (-1)^{\sum a_{ik} b_k}$ for all i . Now if $b_i = 0$, $(-1, d_2)_{p_i} = \left(\frac{-1}{p_i}\right) = -1$; if $b_i = 1$, $(-1, d_2)_{p_i} = +1$. Thus, $(d_1, d_2)_{p_i} = +1$ for all i if and only if $\sum a_{ik} b_k \equiv b_i + 1 \pmod{2}$; that is, if and only if:

$$(A + I) \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} b_1 + 1 \\ \vdots \\ b_n + 1 \end{bmatrix}.$$

Before proceeding, it should be noted that, since $p_1, \dots, p_l \equiv 3 \pmod{8}$ and $p_{l+1}, \dots, p_n \equiv 7 \pmod{8}$, saying that $d_1 = p_1^{b_1} \cdots p_n^{b_n} \equiv 5 \pmod{8}$ is the same as

saying that the column vector made up of $b_1, \dots, b_n$ has an odd number of ones in positions 1 through l , and an odd number of ones in positions $l + 1$ through n . Saying that $d_1 = -p_1^{b_1} \cdots p_n^{b_n} \equiv 5 \pmod{8}$ is the same as saying that the column vector made up of $b_1, \dots, b_n$ has an odd number of ones in positions 1 through l and an even number of ones in positions $l + 1$ through n .

We are now ready to state Uehara's theorem, in the case where m is a product of primes congruent to 3 (mod 4), in terms of matrices. Let $\vec{u}$ denote the column vector in $\mathbb{F}_2^n$ consisting completely of ones. Let A be an adjusted tournament matrix of size n , let $1 \leq l \leq n$, and let $m = p_1 \cdots p_n$ with each $p_i \equiv 3 \pmod{4}$, in such a way that A is the adjusted tournament matrix for $p_1, \dots, p_n$, and $p_1, \dots, p_l \equiv 3 \pmod{8}$, $p_{l+1}, \dots, p_n \equiv 7 \pmod{8}$.

If n is even, then the column vector:

$$\vec{v}_l = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

with ones in positions 1 through l and zeroes in positions $l + 1$ through n , does **not** lie within $\text{Im}(A + I)$ (that is, $r_4(m) = r_4(-m)$) if and only if one of the following is true:

- (a) There is a vector $\vec{y} \in \mathbb{F}_2^n$ with an odd number of ones in positions 1 through l and an odd number of ones in positions $l + 1$ through n , such that $(A + I)\vec{y} = \vec{y}$. (This vector corresponds to a positive $d_1 \equiv 5 \pmod{8}$.)
- (b) There is a vector $\vec{z} \in \mathbb{F}_2^n$ with an odd number of ones in positions 1 through l and an even number of ones in positions $l + 1$ through n , such that $(A + I)\vec{z} = \vec{z} + \vec{u}$. (This vector corresponds to a negative $d_1 \equiv 5 \pmod{8}$.)

If n is odd, then $\vec{v}_l \in \text{Im}(A + I)$ (that is, $r_4(-m) = r_4(m)$) if and only if the condition (a) above fails to hold, so $\vec{v}_l \notin \text{Im}(A + I)$ if and only if (a) holds. The following gives a partial verification of this matrix result.

Proposition 3.1: If either of the conditions (a) or (b) hold, then $\vec{v}_l \notin \text{Im}(A + I)$, whether n is even or odd.

Proof. Suppose that (a) is true. We may permute entries 1 through l and $l + 1$ through n of $\vec{y}$ (and the corresponding rows and columns of $A + I$), so that all of the ones of $\vec{y}$ lie in a group, say between positions k and m . Then $l - k + 1$ is odd, as is $m - l + 1$, so $m - k + 1$ is even. Partition $A + I$ as follows:

$$A + I = \begin{bmatrix} B_1 & B_2 & B_3 \\ B_2^T + J_2 & B_4 & B_5 \\ B_3^T + J_3 & B_5^T + J_5 & B_6 \end{bmatrix}$$

where the matrices B_i have the following dimensions:

$$\begin{array}{ll} B_1: (k - 1) \times (k - 1) & B_4: (m - k + 1) \times (m - k + 1) \\ B_2: (k - 1) \times (m - k + 1) & B_5: (m - k + 1) \times (n - m) \\ B_3: (k - 1) \times (n - m) & B_6: (n - m) \times (n - m) \end{array}$$

and each matrix J_i is the matrix of appropriate dimensions consisting completely of ones.

Now, since $(A + I)\vec{y} = \vec{y}$, the sum of columns k through m of $A + I$ must yield $\vec{y}$, so the weight of each row of B_2 must be even. Since $m - k + 1$ is even, the weight of each column $B_2^T + J_2$ must be even. Similarly, the weight of each column of B_5 is even, since each row of $B_5^T + J_5$ has even weight. Since B_4 is an anti-symmetric, square matrix of even size, each of whose rows has odd weight, B_4 is an adjusted tournament matrix, and thus has even column weights. Therefore, the weight of each column in the middle “band” of $A + I$ consisting of $B_2^T + J_2$, B_4 , and B_5 is

even. If $\vec{v}_l$ were within $\text{Im}(A + I)$, it would be possible to add columns of $A + I$ to obtain $\vec{v}_l$. The sum of the corresponding columns of the middle band of $A + I$ would then yield the middle band of $\vec{v}_l$, which has odd weight since $\vec{v}_l$ has ones in positions k through l . This contradicts the fact that the weight of each column in the middle band of $A + I$ is even. Thus, $\vec{v}_l \notin \text{Im}(A + I)$.

Now, suppose (b) is true. Again, we may assume that all of the ones in $\vec{z}$ are grouped between two positions k and m . In this case, however, while $l - k + 1$ is still odd, $m - k + 1$ is also odd, since $m - l + 1$ is even.

Partition $A + I$ in a similar fashion to that above. Since $(A + I)\vec{z} = \vec{z} + \vec{u}$, each row weight of B_2 must be odd. Thus, since $m - k + 1$ is odd, each column weight of $B_2^T + J_2$ is even. Similarly, each column weight of B_5 is even. Each row weight of B_4 is even, and B_4 is an anti-symmetric, odd-sized square matrix, so B_4 is once again an adjusted tournament matrix, and thus has columns of even weight. Thus, once again, each column weight of the middle “band” of $A + I$ is even, so $\vec{v}_l$, which has ones in positions k through l and zeroes in positions $l + 1$ through m , cannot be obtained by adding columns of $A + I$. ■

To prove the opposite implication of Uehara’s theorem using matrices, it would be necessary to show that, for an adjusted tournament matrix A of size n and $1 \leq l \leq n$, if the vector $\vec{v}_l$ mentioned earlier does not lie within $\text{Im}(A + I)$, then either (a) or (b) is true. Such a proof would certainly be more involved than that given for preceding proposition.

Example 3.1: Let $p_1 = 3$, $p_2 = 11$, $p_3 = 7$, and $p_4 = 23$, so that $m = 5313$. Let A be the adjusted tournament matrix associated to p_1, p_2, p_3, p_4 . Then:

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \text{ and } A + I = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

and $\text{rank}(A)=3$. Furthermore,

$$\text{Im}(A + I) = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}.$$

Thus, since $p_1, p_2 \equiv 3 \pmod{8}$ and $p_3, p_4 \equiv 7 \pmod{8}$, and since the column vector:

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

does not lie in $\text{Im}(A + I)$, $r_4(5313) = r_4(-5313) = 3 - \text{rank}(A) = 0$. Also, we know from Uehara's theorem that either $(A + I)\vec{y} = \vec{y}$ for some column vector $\vec{y}$ with odd weight in both the upper two positions and the lower two positions, or $(A + I)\vec{z} = \vec{z} + \vec{u}$ for some column vector $\vec{z}$ with odd weight in the upper two positions and even weight in the lower two positions. As it turns out,

$$(A + I) \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Interpreted in terms of Uehara's result, this means that there should be a nontrivial integral solution to the equation $x^2 = 11 \cdot 23y^2 - 4 \cdot 3 \cdot 7z^2$. Indeed, the values $x = 13$, $y = 1$, and $z = 1$ satisfy this equation.

Example 3.2: Let $p_1 = 3$, $p_2 = 11$, $p_3 = 31$, $p_4 = 167$, and $p_5 = 239$, so that $m = 40,830,999$. Let A be the adjusted tournament matrix associated to p_1, p_2, p_3, p_4, p_5 . Then:

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \text{ and } A + I = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

and $\text{rank}(A)=2$. In this case,

$$(A + I) \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Therefore, $r_4(-40, 830, 999) = r_4(40, 830, 999) + 1$. Since $r_4(-40, 830, 999) = 4 - \text{rank}(A) = 2$, $r_4(40, 830, 999) = 1$.

4. Circulant Tournaments

Let $n > 0$ be an odd integer. Then it is possible to define a tournament in which each vertex defeats exactly $\frac{n-1}{2}$ vertices. Such a tournament is called a **regular** tournament. It is also possible when n is odd to find subsets $R \subseteq (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ such that $R \cup (-R) = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ and $R \cap (-R) = \emptyset$. The set $R = \{1, 2, \dots, \frac{n-1}{2}\}$ is one such set.

Definition: Suppose $R \subseteq (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ has the two properties mentioned above. We may then define a tournament on the vertices $\{0, 1, \dots, n-1\}$ by the rule a defeats b if and only if $a - b \in R$. Such a tournament is called a **circulant tournament**. It will necessarily be a regular tournament, as its adjusted tournament matrix has the property that any row below the first row can be obtained from the row above by “shifting” it one position to the right (mod n). (Similarly, if $S \subseteq (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ such that $-S = S$, we can define a graph on the vertices $\{0, 1, \dots, n-1\}$ by connecting a to b if and only if $a - b \in S$; such a graph is also called circulant.)

In this section, we will present a few examples of circulant tournaments, and prove three results regarding their ranks.

Let n be odd, and consider the following three subsets $R \subseteq (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$:

$$\{1, 2, \dots, \frac{n-1}{2}\}, \{2, 4, \dots, n-1\}, \text{ and } \{1, 3, \dots, n-2\}.$$

Clearly, each of these sets satisfies the requirements above. The tournaments defined by these choices of R are called the **fundamental**, **even**, and **odd** tournaments on n vertices, respectively.

Theorem 4.1: Let $n > 0$ be odd. Then the fundamental tournament on n vertices has a maximal rank adjusted tournament matrix.

Proof. We consider two cases: $n \equiv 3$ and $n \equiv 1 \pmod{4}$.

If $n = 3$, then we can easily check the result by examining the matrix:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Suppose $n > 3$ and $n \equiv 3 \pmod{4}$. Let A be the adjusted tournament matrix for the fundamental tournament on n vertices, and let A' be obtained from A by deleting the bottom row and the rightmost column, as mentioned in Section 1. Then, since n is odd, we have seen that $\text{rank}(A) = \text{rank}(A')$, so to show that A has maximal rank, it suffices to show that A' is invertible.

Partition A' as follows:

$$A' = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix},$$

where each matrix A_i is square of size $\frac{n-1}{2}$. Then we find that A_1 and A_4 both have ones on and above the diagonal, and zeroes below. A_2 has ones on and below the diagonal, and zeroes above, and A_3 has ones below the diagonal, and zeroes on and above it. (The bottom $\frac{n-1}{2}$ rows have weight $\frac{n-1}{2}$; the top $\frac{n-1}{2}$ rows have

weight $\frac{n+1}{2}$.) For example, when $n = 7$, we have the following matrix A' :

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Now the matrices A_1 , A_2 , and A_4 are invertible so, in particular, the top $\frac{n-1}{2}$ rows of A' and the bottom $\frac{n-1}{2}$ rows of A' are independent. To show that A' is invertible, then, it suffices to show that none of the bottom $\frac{n-1}{2}$ rows can be written as a combination of the top $\frac{n-1}{2}$ rows. It is important to note the following fact: Row $\frac{n-1}{2} + k$ of A' is the sum of a subset of the first $\frac{n-1}{2}$ rows if and only if row k of A_3 is the sum of the corresponding rows of A_1 and row k of A_4 is the sum of the corresponding rows of A_2 . We proceed by writing each row of A_3 as a sum of rows of A_1 , and each row of A_4 as a sum of rows of A_2 .

Now row 1 of A_1 consists completely of ones; if $1 < k \leq \frac{n-1}{2}$, then row k of A_1 has k ones in the rightmost positions, and zeroes elsewhere. Row k of A_3 , therefore, is the sum of rows 1 and k of A_1 .

Row $\frac{n-1}{2}$ of A_2 consists completely of ones, and row k has k ones, followed by zeroes. Thus, row 1 of A_4 is equal to row $\frac{n-1}{2}$ of A_2 , and if $k > 1$, then row k of A_4 is the sum of rows $\frac{n-1}{2}$ and $k-1$ of A_2 .

Therefore, if row $\frac{n-1}{2} + k$ of A' is the sum of some of the upper rows of A' , then either $k = 1$, so that row $\frac{n-1}{2} + 1$ is equal to row $\frac{n-1}{2}$, an obvious contradiction, or $k > 1$ and we have the set equality $\{1, k\} = \{\frac{n-1}{2}, k-1\}$. Thus, either $\frac{n-1}{2} = 1$, so $n = 3$, a contradiction, or $k-1 = 1$ and $k = \frac{n-1}{2}$, so $k = 2$ and $n = 5$, contradicting $n \equiv 3 \pmod{4}$. Thus A' is invertible.

Now suppose that $n \equiv 1 \pmod{4}$, and let A , A' , A_1 , A_2 , A_3 , and A_4 be defined as above. In this case, the diagonal entries of A are zero, so A_1 and A_4

have ones above the diagonal and zeroes on and below it. A_2 has ones on and below the diagonal, and zeroes above it; A_3 has ones below the diagonal and zeroes on and above it. For example, when $n = 9$ we get the following matrix A' :

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Once again, it is easily seen that the top $\frac{n-1}{2}$ rows are independent, as are the bottom $\frac{n-1}{2}$ rows. Furthermore, since each of the top $\frac{n-1}{2}$ rows has a zero in the leftmost position, and every one of the bottom $\frac{n-1}{2}$ rows has a one in the leftmost position, except row $\frac{n-1}{2} + 1$, none of these rows can be a combination of the top rows.

It remains only to see that row $\frac{n-1}{2} + 1$ does not lie in the span of the first $\frac{n-1}{2}$ rows. Now, row 1 of A_4 , with one zero in the leftmost position and ones everywhere else, is the sum of rows $\frac{n-1}{2}$ and 1 of A_2 . Since the rows of A_2 are independent, this expression is unique. However, the sum of rows 1 and $\frac{n-1}{2}$ of A_1 is not equal to row 1 of A_3 (row $\frac{n-1}{2}$ of A_1 and row 1 of A_3 are all zeroes; row 1 of A_1 is not). Thus, row $\frac{n-1}{2} + 1$ of A' does not lie in the span of the upper rows, so A' is invertible. ■

Theorem 4.2: The odd and even tournaments of size n have maximal rank adjusted tournament matrices, for any $n > 0$ odd.

Proof. It suffices to show that the adjusted tournament matrix A for the odd tournament on n vertices has maximal rank for, if B is the adjusted tournament matrix for the even tournament on n vertices, then B can be obtained from A by

changing each entry of A , except for the diagonal entries; that is $B = A + I + J$, where I and J are as defined earlier. However, we already know that $A^T = A + I + J$, so $\text{rank}(B) = \text{rank}(A^T) = \text{rank}(A)$.

To prove our result for the odd tournament, recall the following from Section 2.4:

Fact: Let I_n and J_n denote the $n \times n$ identity matrix and matrix consisting completely of ones, respectively. Then:

$$\text{rank}(I_n + J_n) = \begin{cases} n - 1 & \text{if } n \text{ is odd} \\ n & \text{if } n \text{ is even} \end{cases}.$$

Let A be the adjusted tournament matrix for the odd tournament on n vertices. First, suppose that $n \equiv 1 \pmod{4}$. Then the set R mentioned above has even size, so each diagonal entry of A is zero. In this case, the bottom row of A looks like:

$$0 \ 1 \ 0 \ \dots \ 1 \ 0$$

and each row above the bottom row can be found by “shifting” the row below it one position to the left, modulo n . For example, when $n = 9$, we get the following matrix:

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Note that, if $1 \leq k < n$, then row k differs from row $k + 1$ in every position except $k + 1$. Let $\hat{A}$ be obtained from A by replacing row k , for $1 \leq k < n$, by the sum

of rows k and $k + 1$. Then $\hat{A}$ has the form:

$$\hat{A} = \begin{bmatrix} \vec{u} & I_{n-1} + J_{n-1} \\ 0 & \vec{v} \end{bmatrix},$$

where $\vec{u}$ is the column vector of size $n - 1$ made up completely of ones and $\vec{v} = [1 \ 0 \ 1 \ \dots 1 \ 0]$ has size $n - 1$. Since the bottom row of A is the sum of the remaining rows, the bottom row of $\hat{A}$ is the sum of the remaining odd-numbered rows. Therefore, its deletion will not change the rank of $\hat{A}$. Furthermore, the leftmost column of the remaining matrix is the sum of the remaining columns, so its removal will also not affect $\text{rank}(\hat{A})$. Thus, $\text{rank}(\hat{A}) = \text{rank}(I_{n-1} + J_{n-1}) = n - 1$, since $n - 1$ is even. Therefore, A has maximal rank.

Example 4.1: When $n = 9$, the matrix $\hat{A}$ looks like:

$$\hat{A} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

We now return to our proof. Suppose that $n \equiv 3 \pmod{4}$. Then R has odd size, so each diagonal entry of A is one. Now, the first row of A looks like:

$$1 \ 0 \ 1 \ \dots \ 0 \ 1$$

and each row below the top row can be found by “shifting” the row above it one position to the right, modulo n . Thus, each row k , for $1 \leq k < n$, differs from row $k + 1$ in each position except position k . For example, when $n = 7$, we get the

following matrix:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Let $\hat{A}$ be obtained from A by replacing row k , for $1 \leq k < n$, by the sum of rows k and $k + 1$. Then $\hat{A}$ has the form:

$$\hat{A} = \begin{bmatrix} I_{n-1} + J_{n-1} & \vec{u} \\ \vec{v} & 1 \end{bmatrix},$$

where $\vec{u}$ is as defined above, and $\vec{v} = [0 \ 1 \ 0 \ \dots \ 0 \ 1]$ has size $n - 1$. Once again, the bottom row of $\hat{A}$ is within the span of the remaining rows, so its removal will not affect the rank of the matrix. Also, since $n - 1$ is even, each row of $I_{n-1} + J_{n-1}$ has odd weight, so the right-hand column of the remaining matrix is the sum of the other columns. Therefore, $\text{rank}(\hat{A}) = \text{rank}(I_{n-1} + J_{n-1}) = n - 1$. Thus, A has maximal rank. $\blacksquare$

Example 4.2: When $n = 7$, the matrix $\hat{A}$ looks like:

$$\hat{A} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Definition: Let $p \equiv 3 \pmod{4}$ be prime, and let $R = (\mathbb{Z}/p\mathbb{Z})^{*2}$, the nonzero squares of $(\mathbb{Z}/p\mathbb{Z})$. Then, since the Kronecker symbol $\left(\frac{-1}{p}\right) = -1$, $R \cap (-R) = \phi$. Since $\#R = \frac{p-1}{2}$, $R \cup (-R) = (\mathbb{Z}/p\mathbb{Z})^*$. Thus, we may define a tournament on p vertices using the set R . This tournament is called the **Paley tournament** on

p vertices. (When $p \equiv 1 \pmod{4}$, $\left(\frac{-1}{p}\right) = +1$, so we obtain a graph, called the Paley graph on p vertices.)

These tournaments and graphs arise in the study of random graphs. We have the following result concerning the ranks of the adjusted tournament matrices for these tournaments:

Theorem 4.3: Let $p \equiv 3 \pmod{4}$ be prime, and let A denote the adjusted tournament matrix for the Paley tournament on p vertices. Then A has minimal rank if and only if $p \equiv 7 \pmod{8}$.

Proof. We will use the theorem from Section 2 of this chapter which states that an adjusted tournament matrix has minimal rank if and only if it is idempotent. In order to decide whether the adjusted tournament matrix for a circulant tournament of size p is idempotent, it is necessary only to check that the product of the matrix with its first column yields the first column. This is true because each succeeding column of the adjusted tournament matrix can be found by shifting the column to the left down one position $\pmod{p}$, and because each row can be found by shifting the row above it one position to the right $\pmod{p}$.

Denote the first column of A by $\vec{x}$. Then for any $1 \leq k \leq p$, $\vec{x}$ has a 1 in position k if and only if $k - 1 \in (\mathbb{Z}/p\mathbb{Z})^2$. Also, row 1 of A has ones in positions corresponding to $((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) \cup \{0\}$, so row k of A has ones in positions corresponding to $[(\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2] \cup \{0\} + (k - 1)$. Therefore, the column vector $A\vec{x}$ has a 1 in position k if and only if the cardinality of:

$$(\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) \cup \{0\} + (k - 1)]$$

is odd. Therefore, $A\vec{x} = \vec{x}$ if and only if, for $1 \leq k \leq p$:

$$\#(\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) \cup \{0\} + (k-1)] \equiv \begin{cases} 1 \pmod{2} & k-1 \in (\mathbb{Z}/p\mathbb{Z})^2 \\ 0 \pmod{2} & k-1 \notin (\mathbb{Z}/p\mathbb{Z})^2 \end{cases}$$

This condition can be simplified somewhat. If $j \in (\mathbb{Z}/p\mathbb{Z})^2$, then $0 \notin [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) + j]$, so:

$$\begin{aligned} & \# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) \cup \{0\} + j] \} \\ &= \# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) + j] \} + 1. \end{aligned}$$

If $j \notin (\mathbb{Z}/p\mathbb{Z})^2$, then:

$$(\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) \cup \{0\} + j] = (\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) + j].$$

Also, since $\#(\mathbb{Z}/p\mathbb{Z})^2$ is even (0 is included, and $\frac{p-1}{2}$ is odd),

$$\# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [((\mathbb{Z}/p\mathbb{Z}) \setminus (\mathbb{Z}/p\mathbb{Z})^2) + j] \} \equiv \# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j] \} \pmod{2}.$$

Therefore, $A\vec{x} = \vec{x}$ if and only if, for each $0 \leq j \leq p-1$:

$$\# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j] \} \equiv 0 \pmod{2}.$$

It is apparent that $\# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j] \} = \# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 - j] \}$, so we may assume that $j \in (\mathbb{Z}/p\mathbb{Z})^2$, say $j \equiv m^2 \pmod{2}$.

Claim 1: Let $j \in (\mathbb{Z}/p\mathbb{Z})^2$, and let k be the number of solutions $(x, y) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ to the equation $y^2 - x^2 = j$. Then:

$$\# \{ (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j] \} = \frac{k-2}{4} + 1.$$

Proof. Suppose that (x, y) is a solution to $y^2 - x^2 = j$. Then $y^2 \in (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j]$. We have the two solutions $(0, m)$ or $(0, -m)$, which yield the same

element $j \in (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j]$. Furthermore, if (x, y) is a solution such that $x, y \neq 0$, then the four distinct solutions (x, y) , $(-x, y)$, $(x, -y)$, and $(-x, -y)$ all yield the same element $y^2 \in (\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j]$. Therefore, $\# \{(\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j]\}$ has one element contributed by the solutions $(0, m)$ and $(0, -m)$, and one element contributed by each set of four solutions (x, y) , $(-x, y)$, $(x, -y)$, and $(-x, -y)$, with $x, y \neq 0$. This confirms our result.

Claim 2: Let $j_1, j_2 \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{0\}$. Then the number of solutions to the equations $y^2 - x^2 = j_1$ and $y^2 - x^2 = j_2$ are the same for, if $a^2 j_1 = j_2$, then $(y+x)(y-x) = j_1$ if and only if $(ay+ax)(ay-ax) = j_2$.

Thus, for all $j \in (\mathbb{Z}/p\mathbb{Z})^*$, the number of solutions to $y^2 - x^2 = j$ is constant.

Let n denote this value.

Claim 3: $n = p - 1$.

Proof. We can write the set $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ as the following disjoint union:

$$(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) = \{(x, y) | y^2 = x^2\} \cup \bigcup_{j=1}^{p-1} \{(x, y) | y^2 - x^2 = j\}.$$

Now, $\# \{(x, y) | y^2 = x^2\} = 2p - 1$, since

$$\{(x, y) | y^2 = x^2\} = \{(x, x) | x \in (\mathbb{Z}/p\mathbb{Z})^*\} \cup \{(x, -x) | x \in (\mathbb{Z}/p\mathbb{Z})\}$$

is a disjoint union. Therefore, by Claim 2,

$$n = \frac{p^2 - 2p + 1}{p - 1} = p - 1.$$

This tells us that, for any $1 \leq j \leq p - 1$:

$$\# \{(\mathbb{Z}/p\mathbb{Z})^2 \cap [(\mathbb{Z}/p\mathbb{Z})^2 + j]\} = \frac{p+1}{4}.$$

As a result of the above computations, we find that, when $p \equiv 7 \pmod{8}$, $\frac{p+1}{4}$ is even, so A has minimal rank. Furthermore, when $p \equiv 3 \pmod{8}$, $\frac{p+1}{4}$ is odd, so A does not have minimal rank. ■

It is possible to be more specific about the rank of the adjusted tournament matrix for the circulant tournament of size p when $p \equiv 3 \pmod{8}$. For any $R \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ which satisfies the requirements for determining a circulant tournament, we have the subgroup $G(R)$ of $(\mathbb{Z}/p\mathbb{Z})^*$ made up of all elements a of $(\mathbb{Z}/p\mathbb{Z})^*$ such that $aR = R$. Let m be the least positive integer such that $2^m \in G(R)$, and let A be the adjusted tournament matrix for the tournament on p vertices defined by R . Then it has been shown by Conner that:

$$m \cdot \#G(R) | (\dim(\ker(A)) - 1).$$

Let $R = (\mathbb{Z}/p\mathbb{Z})^{*2}$. Then $G(R) = R$, since R is itself a group, so $\#G(R) = \frac{p-1}{2}$. Furthermore, $m = 2$ whenever $p \equiv 3 \pmod{8}$, since $\left(\frac{2}{p}\right) = -1$. Thus, when $p \equiv 3 \pmod{8}$, $p - 1 | (\dim(\ker(A)) - 1)$. However, since $\text{rank}(A) \geq \frac{p-1}{2}$, $\dim(\ker(A)) \leq \frac{p-1}{2}$. Thus, $\dim(\ker(A)) - 1 = 0$, so A has maximal rank.

The following two examples illustrate both of the possible cases:

Example 4.3: When $p = 7$, we have the following matrix A for the Paley tournament:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

which has minimal rank 3.

Example 4.4: When $p = 11$, we have the following A :

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix},$$

which has maximal rank 10.

BIBLIOGRAPHY

- [B-C] P. BARRACUND and H. COHN, Primes of type $x^2 + 32y^2$, class number and residuacity, *J. reine angew. Math.* **238** (1969), 67–70.
- [B1] H. BAUER, Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *J. reine angew. Math.* **248** (1971), 42–46.
- [B2] H. BAUER, Die 2-Klassenzahl spezieller quadratischer Zahlkörper, *J. reine angew. Math.* **252** (1972), 79–81.
- [Be] E. T. BELL, *The Development of Mathematics*, 2nd ed. McGraw-Hill Book Co., 1945.
- [Bo] L. BOUVIER, Tables des 2-rang, 4-rang, et 8-rang du 2-group des classes d'idéaux au sens restreint de $\mathbb{Q}(\sqrt{m})$, preprint.
- [Br] B. BRAUCKMANN, 4-ranks of S -ideal class groups, preprint.
- [B-P] E. BROWN and C. J. PARRY, Class numbers of imaginary quadratic number fields having exactly three discriminantal divisors, *J. reine angew. Math.* **260** (1973), 31–34.
- [Bro1] E. BROWN, The power of 2 dividing the class number of a binary quadratic discriminant, *J. Number Theory* **5** (1973), 413–419.
- [Bro2] E. BROWN, Class numbers of real quadratic fields, *Trans. of the AMS* **190** (1974), 99–107.
- [C-F] J. W. S. CASSELS and A. FRÖHLICH, *Algebraic Number Theory*. Acad. Press (1987).
- [C-L] G. CHARTRAND and L. LESNIAK, *Graphs and Digraphs*, 2nd ed. Wadsworth and Brooks/Cole (1986).
- [C] S. CHOWLA, An extension of Heilbronn's class-number theorem, *Quart. J. Math., Oxford Ser.* **5** (1934), 304–307.
- [Co-L] H. COHEN and H. LENSTRA, Heuristics on class groups of number fields, in *Lecture Notes in Mathematics* Vol. 1068. Springer-Verlag (1984), 33–62.
- [C-M] H. COHEN and J. MARTINET, Class groups of number fields: numerical heuristics, *Math. Comp.* **48** (1987), 123–137.
- [C-H] P. E. CONNER and J. HURRELBRINK, *Class Number Parity*. Ser. in Pure Math. Vol. 8, World Sci. Publ. (1988).
- [Co] A. COSTA, A generalization of a result of Kaplan on class number congruences, preprint.
- [deC] D. DE CAEN, The ranks of tournament matrices, *The American Mathematical Monthly* **98** (1991), 829–831.

- [D] R. DEDEKIND, Über die Theorie der ganzen algebraischen Zahlen, XI Suppl. to Dirichlet's *Vorlesungen über Zahlentheorie*, 2nd ed. (1871), 3rd ed. (1879), 4th ed. (1894).
- [F] A. FRÖHLICH, The generalization of a theorem of Rédei's, *Quart. J. Math., Oxford Ser. (2)* 5 (1954), 130–140.
- [G] C. F. GAUSS, *Disquisitiones Arithmeticae*. Göttingen (1801).
- [Ge1] F. GERTH, An application of matrices over finite fields to algebraic number theory, *Math. of Comp.* 41 (1983), 229–234.
- [Ge2] F. GERTH, The 4-class ranks of quadratic extensions of certain imaginary quadratic fields, *Ill. J. of Math.* 33 (1989), 132–142.
- [Ge3] F. GERTH, The 4-class ranks of quadratic extensions of certain real quadratic fields, *J. Number Theory* 33 (1989), 18–31.
- [Ge4] F. GERTH, The 4-class ranks of quadratic fields, *Inventiones mathematicae* 77 (1984), 489–515.
- [Gr] G. GRAS, Relations congruentielles linéaires entre nombres de classes de corps quadratiques, *Acta Arith.* 52 (1989), 219–227.
- [H-K] F. HALTER-KOCH, Über den 4-Rang der Klassengruppe quadratischer Zahlkörper, *J. Number Theory* 19 (1984), 219–227.
- [H1] H. HASSE, Bericht über neuere Untersuchungen und Probleme der Theorie der algebraischen Zahlkörper, Teil 1, *Jahresber. dt. Math. verein.* 35 (1926).
- [H2] H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag, 1952; new edition: Springer-Verlag 1985.
- [H3] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \pmod{2^3}$, *Aequationes Math.* 3 (1969), 165–169.
- [H4] H. HASSE, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, *J. Number Theory* 1 (1969), 231–234.
- [H5] H. HASSE, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *J. reine angew. Math.* 241 (1970), 1–6.
- [H6] H. HASSE, Über Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *Math. Nachr.* 46 (1970), 61–70.
- [Hi] M. HIKITA, On the congruences for the class numbers of the quadratic fields whose discriminants are divisible by 8, *J. Number Theory* 23 (1986), 86–101.
- [Hil1] D. HILBERT, Über die Theorie des relativ-quadratischen Zahlkörpers, *Math. Annalen* 51 (1899), 1–127.

- [Hil2] D. HILBERT, Über die Zerlegung der Ideale eines Zahlkörpers in Primideale, *Math. Annalen* **44** (1894), 1–8.
- [Hu] J. HURRELBRINK, On the 4-rank of the ideal class group, preprint.
- [I] E. INABA, Über die Struktur der l -Klassengruppe zyklischer Zahlkörper vom Primzahlgrad l , *J. Fac. Sci. Univ. Tokyo (II)* **4** (1940), 61–115.
- [K1] P. KAPLAN, Divisibilité par 8 du nombre des classes des corps quadratiques réels dont le 2-sous-groupe des classes est cyclique, *Comptes Rendus Hebdomadaires, Académie des Sciences, Paris* **275** (1972), 887–890.
- [K2] P. KAPLAN, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocity biquadratique, *J. Math. Soc. Japan* **25** (1973), 596–608.
- [K3] P. KAPLAN, 2-groupe des classes et facteurs principaux de $\mathbb{Q}(\sqrt{pq})$ ou $p \equiv -q \equiv 1 \pmod{4}$, *Comptes Rendus Hebdomadaires, Académie des Sciences, Paris* **276** (1973), 89–92.
- [K4] P. KAPLAN, Comparaison des 2-groupes des classes d'idéaux au sens large et au sens étroit d'un corps quadratique réel, *Proc. of the Japan Acad.* **50** (1974), 688–693.
- [K5] P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques, *J. reine angew. Math.* **283/284** (1976), 313–363.
- [K6] P. KAPLAN, Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certain corps quadratiques, *Bull. Soc. Math. France, Mém.* **49/50** (1977), 113–124.
- [K-W] P. KAPLAN and K. S. WILLIAMS, On the class number of $\mathbb{Q}(\sqrt{\pm 2p})$ modulo 16 for $p \equiv 1 \pmod{8}$ a prime, *Acta Arithmetica* **40.3** (1982), 289–296.
- [K-Z] H. KOCH and W. ZINK, Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern, *Math. Nachr.* **54** (1972), 309–333.
- [Kr] L. KRONECKER, Grundzüge einer arithmetischen Theorie der algebraischen Größen, *J. reine angew. Math.* **92** (1882), 1–122.
- [L1] J. C. LAGARIAS, On determining the 4-rank of the ideal class group of a quadratic field, *J. Number Theory* **12** (1980), 191–196.
- [L2] J. C. LAGARIAS, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, *Trans. of the AMS* **260** (1980), 485–508.
- [La] J. L. LAGRANGE, Recherches d'arithmétique, *N. Mém. Acad. Roy. Sci. Bel. Lettr. de Berlin* (1773, 1775).
- [Le] H. LEOPOLDT, Zur Struktur der l -Klassengruppe galoisscher Zahlkörper, *J. reine angew. Math.* **199** (1958), 165–174.

- [M] T. S. MICHAEL, private communication.
- [Moi] J. M. MOINE, Quelques problèmes concernant les classes ambiges des corps quadratiques, *Ann. Univ. Besançon* 4 (1972), 1–63.
- [Mo] J. W. MOON, *Topics on Tournaments*. Holt, Rinehart, and Winston (1968).
- [Mor1] P. MORTON, Density results for the 2-classgroups of imaginary quadratic fields, *J. reine angew. Math.* 332 (1982), 156–187.
- [Mor2] P. MORTON, The quadratic number fields with cyclic 2-class groups, *Pac. J. Math.* 108 (1983), 165–175.
- [N] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publ. (1990).
- [O1] B. ORIAT, Relation entre le 2-groupe des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, *Ann. Inst. Fourier* 27/2 (1977) 37–59.
- [O2] B. ORIAT, Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$, *J. Math. Soc. Japan* 30 (1978), 279–285.
- [P] A. PFIZER, On the 2-part of the class number of imaginary quadratic number fields, *J. Number Theory* 8 (1976), 184–192.
- [R-R] L. RÉDEI and H. REICHARDT, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.* 170 (1933), 69–74.
- [R1] L. RÉDEI, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.* 171 (1934), 55–60.
- [R2] L. RÉDEI, Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.* 171 (1934), 61–64.
- [R3] L. RÉDEI, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, *J. reine angew. Math.* 180 (1939), 1–43.
- [R4] L. RÉDEI, Über die Klassenzahl des imaginären quadratischen Zahlkörpers, *J. reine angew. Math.* 159 (1928), 210–219.
- [R5] L. RÉDEI, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörpern, *J. reine angew. Math.* 171 (1934), 131–148.
- [R6] L. RÉDEI, Über einige Mittelwertfragen im quadratischen Zahlkörper, *J. reine angew. Math.* 174 (1936), 131–148.

- [Re1] H. REICHARDT, Über die 2-Klassengruppe gewisser quadratischer Zahlkörper, *Math. Nachr.* **46** (1970), 71–80.
- [Re2] H. REICHARDT, Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.* **170** (1934), 75–82 .
- [St1] P. STEVENHAGEN, *Class Groups and Governing Fields*, thesis, U. C. Berkeley (1988).
- [St2] P. STEVENHAGEN, On the 2-power divisibility of certain quadratic class numbers, preprint.
- [St3] P. STEVENHAGEN, Rédei matrices and the structure of quadratic 2-class groups, preprint.
- [U] T. UEHARA, On the 4-rank of the narrow ideal class group of a quadratic field, *J. Number Theory* **31** (1989), 167–173.
- [W] W. C. WATERHOUSE, Pieces of eight in class groups of quadratic fields, *J. Number Theory* **5** (1973), 95–97.

APPENDIX

TOURNAMENTS OF SIZE SIX AND SMALLER

The following pages contain the graphs, adjusted tournament matrices and ranks of the non-isomorphic tournaments of size n , for $2 \leq n \leq 6$. The list of non-isomorphic tournaments is taken from [Mo]. Again, note that when two vertices are not connected by an arrow, it is understood that the upper vertex “defeats” the lower one.

Tournaments of Size Smaller than 5

$\succ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad 1$	
$\begin{matrix} \bullet \\ \bullet \\ \bullet \end{matrix} \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad 1$	$\begin{matrix} \bullet \\ \bullet \\ \bullet \end{matrix} \succ \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad 2$
$\begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad 2$	$\begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} \succ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad 3$
$\begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} \succ \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad 3$	$\begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} \succ \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad 3$

VITA

Robert J. Kingan was born in Bloomington, Illinois on December 9, 1965. He graduated from the University of Central Arkansas in May, 1987 with a Bachelor of Science degree in mathematics and computer science, and began graduate study at Louisiana State University that fall. He received a Master of Science degree in mathematics from LSU in May, 1989, and is presently a candidate for the doctoral degree in mathematics at LSU.

DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Robert John Kingan

Major Field: Mathematics

Title of Dissertation: TOURNAMENTS AND IDEAL CLASS GROUPS

Approved:

J. Hurrelbrink
Major Professor and Chairman

Daniel Fogel
Dean of the Graduate School

EXAMINING COMMITTEE:

Luke Weis

Robert V. Perlis

P. E. Conner

John A. Hildebrand

David H. Frey

Date of Examination:

3/16/92