Can. J. Math. Vol. **46** (1), 1994 pp. 169–183

CIRCULANT GRAPHS AND 4-RANKS OF IDEAL CLASS GROUPS

JURGEN HURRELBRINK

ABSTRACT. This is about results on certain regular graphs that yield information about the structure of the ideal class group of quadratic number fields associated with these graphs. Some of the results can be formulated in terms of the quadratic forms $x^2 + 27y^2$, $x^2 + 32y^2$, $x^2 + 64y^2$.

1. **Introduction.** For a real quadratic field $E = \mathbb{Q}(\sqrt{d})$, d being a product of t distinct prime numbers incongruent to 3 mod 4, the 4-rank of the narrow ideal class group of E can be computed via Eulerian vertex decompositions (EVD's) of the graph Γ_E attached to E. We study the situation $t = p$, p an odd prime number, and Γ_E a circulant graph on p vertices, where the relevant data can be obtained from the arithmetic of the cyclotomic field $\mathbb{Q}(\xi_p)$.

Section 2 presents the reformulation of the Rédei-Reichardt Theorem on the 4-rank of the narrow ideal class group of E in terms of the number of EVD's of the graph Γ_E as it can be found in [12].

Section 3 studies circulant graphs and introduces P. E. Conner's Theorem about their number of EVD's in arithmetic terms.

Section 4 makes the results explicit *e.g.* for Paley graphs and Cayley graphs corresponding to the subgroups of cubes and fourth powers of $(\mathbb{Z}/p\mathbb{Z})^*$.

These connections between combinatorics and arithmetic provide us with number fields E whose graph Γ_E is connected, regular, and has an arbitrarily large number of EVD's, which in particular implies that the 4-rank of the ideal class group of E is arbitrarily large. It should be noted—compare (2.9)—that those graphs are extremely rare among all graphs.

An extension of the results for more general circulant graphs on t vertices by using the arithmetic of $\mathbb{Q}(\xi_t)$ would be interesting and will encounter new obstacles. One might wish to investigate the case of t being a prime power.

2. **Rédei-Reichardt revisited.** We will consider real quadratic number fields $E = \mathbb{Q}(\sqrt{d})$ with $d = p_1 \cdot \cdots \cdot p_t$, a product of $t \geq 1$ distinct prime numbers $p_i \not\equiv 3 \bmod 4$. These are the quadratic number fields E for which -1 is a field norm from E over $\mathbb{Q}$. Let $C(E)$ be the *narrow* ideal class group of E and let 2-rank $C(E)$ *and* 4-rank $C(E)$ denote the number of cyclic factors of $C(E)$ of order divisible by 2 and 4, respectively.

Received by the editors April 30, 1992.
AMS subject classification: 05C90, 11R11, 11R29.

By Gauss' genus theory we have the well known 2-rank formula

$$\text{2-rank } C(E) = t - 1. \tag{2.1}$$

With $E = \mathbb{Q}(\sqrt{p_1 \cdot \cdots \cdot p_t})$ as above we associate the $t \times t$ matrix $M_E = (a_{ij})$ over $\mathbb{F}_2$ given by

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } (\frac{p_i}{p_j}) = -1 \\ 0 & \text{if } i \neq j \text{ and } (\frac{p_i}{p_j}) = +1 \end{cases} \tag{2.2}$$

$$a_{ii} = \sum_{\substack{j=1 \\ j \neq i}}^{t} a_{ij}.$$

Here, for $p_i = 2$ and $p_j \equiv 1 \bmod 4$, it is understood that $(\frac{2}{p_j}) = (\frac{p_j}{2}) = +1$ if and only if $p_j \equiv 1 \bmod 8$.

We call M_E the *Rédei matrix* of E and notice that M_E is a symmetric matrix over $\mathbb{F}_2$ whose rows sum up to the zero row. In particular, the rank of M_E over $\mathbb{F}_2$ is at most $t-1$. What Rédei and Reichardt have set up in terms of "d-splittings of the second type" amounts to the 4-rank formula

$$\text{4-rank } C(E) = t - 1 - \operatorname{rank}_{\mathbb{F}_2} M_E; \tag{2.3}$$

compare [5], [7] through [16], and [18], [20].

With the Rédei matrix M_E we now associate a *graph* Γ_E given by

(2.4) set of vertices $V = \{1, 2, \ldots, t\}$; two distinct vertices i and j are adjacent if and only if $a_{ij} = 1$.

In other words, vertices i and j are linked by an edge if and only if $(\frac{p_i}{p_j}) = -1$. In this way we have obtained from E a graph Γ_E having a finite set of vertices, no loops, and no multiple edges. Moreover, by Dirichlet's theorem on primes in arithmetic progressions, *every* such graph Γ is a graph Γ_E for some quadratic number field E (in fact, for infinitely many quadratic number fields E).

An *Eulerian vertex decomposition* (EVD) of a graph Γ with set of vertices V is an unordered pair

$$\{V_1, V_2\} \text{ such that } V = V_1 \cup V_2, \quad V_1 \cap V_2 = \emptyset \tag{2.5}$$

and every vertex in V is adjacent to an *even* number of vertices in the subset V_1 or V_2 to which it does not belong.

By this definition, for an EVD $\{V_1, V_2\}$, the subgraph of Γ consisting of all edges between V_1 and V_2 is an Eulerian graph. We refer to $\{\emptyset, V\}$ as the trivial EVD.

The 4-rank formula (2.3) for $C(E)$ in terms of the Rédei matrix M_E becomes in terms of the corresponding graph Γ_E a formula on the number of EVD's of Γ_E. Namely:

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

THEOREM 2.6 (RÉDEI-REICHARDT). *For a quadratic number field E as above with associated graph Γ_E, the 4-rank of the narrow class group $C(E)$ is given by*

$$2^{4\text{-rank}(E)} = \#\text{ of Eulerian vertex decompositions of } \Gamma_E.$$

See [12] for this formulation of the Rédei-Reichardt theorem. In particular we have by Theorem 2.6: 4-rank $C(E) = 0$; that is, the 2-Sylow subgroup of $C(E)$ is elementary abelian if and only if Γ_E does not admit a non-trivial EVD.

Consider a graph Γ on t vertices and any quadratic number field $E = \mathbb{Q}(\sqrt{p_1 \cdot \cdots \cdot p_t})$ such that $\Gamma = \Gamma_E$. We then say, for $0 \leq c \leq t-1$,

(2.7)
$$\begin{aligned} &\Gamma \text{ has property } P_c \text{ if and only if } \Gamma \text{ has } 2^c \text{ EVD's; that is,} \\ &\qquad\qquad \text{if and only if 4-rank } C(E) = c \text{; that is,} \\ &\qquad\qquad \text{if and only if co-rank}_{\mathbb{F}_2} M_E = c+1. \end{aligned}$$

Extreme cases: Γ has property P_0 if and only if 2-Sylow $C(E)$ is elementary abelian, and Γ has property P_{t-1} if and only if M_E is the zero-matrix; that is, if and only if Γ is totally disconnected. Property P_0 is what is called property (P) in [11].

ILLUSTRATION 2.8.

E	$\mathbb{Q}(\sqrt{5\cdot 13\cdot 37})$	$\mathbb{Q}(\sqrt{5\cdot 13\cdot 17\cdot 41})$	$\mathbb{Q}(\sqrt{13\cdot 17\cdot 101})$
2-rank $C(E)$	2	3	2
Rédei matrix M_E	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
$\text{rank}_{\mathbb{F}_2} M_E$	2	2	0
$\text{co-rank}_{\mathbb{F}_2} M_E$	1	2	3
graph Γ_E			
# of EVD's	2^0	2^1	2^2
4-rank $C(E)$	0	1	2

It follows from [16] that the graphs with property P_c for c large are extremely rare among all graphs (having finitely many vertices, no loops, and no multiple edges). For example:

(2.9) More than 41.94% of all graphs have property P_0, the same percentage of graphs have property P_1, and more than 99.85% of all graphs have property P_c for some $c \leq 3$.

We will exhibit families of connected, regular graphs having property P_c with c arbitrarily large.

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

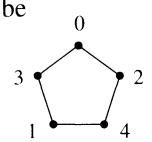
3. **Circulant graphs.** A *circulant graph* is a graph whose adjacency matrix, for some ordering of the vertices, is a circulant matrix; compare [2]. In this paper we consider only circulant graphs on p vertices, where p is an odd prime number.

By a *graph set* we mean a subset S of the group of units $(\mathbb{Z}/p\mathbb{Z})^* = \{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ of $\mathbb{Z}/p\mathbb{Z}$ satisfying $(-1)S = S$. In particular, a graph set has an even number of elements.

DEFINITION 3.1. For an odd prime p and a graph set $S \subset (\mathbb{Z}/p\mathbb{Z})^*$, the circulant graph $\Gamma(S)$ is given by:

$$\text{set of vertices } \mathbb{Z}/p\mathbb{Z} = \{0\} \cup (\mathbb{Z}/p\mathbb{Z})^*;$$
$$\text{two vertices } i, j \in \mathbb{Z}/p\mathbb{Z} \text{ are adjacent if and only if } i - j \in S.$$

These are the graphs on p vertices with a circulant adjacency matrix. In Illustration 2.8 we have seen two circulant graphs on $p = 3$ vertices. For $p = 5$, $S = \{\pm 2\}$ we obtain $\Gamma(S)$ to be



with circulant matrix $\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$.

In general, a circulant graph $\Gamma(S)$ is *regular* of degree $\# S$. So, for $S = \emptyset$ we obtain the totally disconnected graph, for $S = \{\pm i\}$ the *p-cycle*, for $S = (\mathbb{Z}/p\mathbb{Z})^*$ the *complete graph* on p vertices.

The totally disconnected graph on p vertices has property P_{p-1}, the p-cycle and the complete graph on p vertices both have property P_0. For $S \neq \emptyset$ the graphs $\Gamma(S)$ are connected. In fact, they are *Cayley graphs*, defined in terms of the additive group $\mathbb{Z}/p\mathbb{Z}$; compare [3], [4].

REMARK 3.2. The adjacency matrix of a circulant graph $\Gamma(S) = \Gamma_E$ is the Rédei matrix M_E as defined in (2.2).

Reason: since $\Gamma(S)$ is regular of *even* degree, all diagonal entries of the Rédei matrix of E are 0.

Thus, in view of (2.3), (2.7), in order to determine property P_c in case of circulant graphs, it suffices to know the rank over $\mathbb{F}_2$ of their adjacency matrices. In turn, this will yield information about the 4-rank of ideal class groups.

For a graph set $S \subset (\mathbb{Z}/p\mathbb{Z})^*$ we put

$$G = G(S) = \{u \in (\mathbb{Z}/p\mathbb{Z})^* : uS = S\}.$$

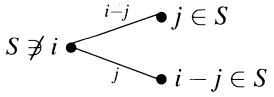
In particular, $G(\phi) = G\big((\mathbb{Z}/p\mathbb{Z})^*\big) = (\mathbb{Z}/p\mathbb{Z})^*$. Clearly, G is a group of even order dividing $p - 1$ that contains $\{\pm 1\}$. The reader will notice that G can be viewed as a subgroup of the group of automorphisms of the graph $\Gamma(S)$.

The complete graph on p vertices turns out to be the only circulant graph on p vertices with $2 \in G$ that has property P_0. Namely we prove in terms of Eulerian vertex decompositions:

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

THEOREM 3.3. *Let $\Gamma(S)$ be a circulant graph that is not complete. If $2 \in G(S)$, then $\Gamma(S)$ does not have property P_0.*

PROOF. Assume $2 \in G(S)$; consider a vertex $i \notin S$. Let $j \in S$ be a vertex that is adjacent to i; that is, $i - j \in S$. Then $i - j$ is also adjacent to i.



Now, $j \neq i - j$ since $2j \neq i$ in view of $2 \in G(S)$, $j \in S$ and $i \notin S$. Thus, the vertices in S that are adjacent to a vertex not in S come in pairs. Since the vertex 0 is adjacent to exactly the vertices in S we can state:

Every vertex $i \notin S \cup \{0\}$ is adjacent to an *even* number of vertices in $S \cup \{0\}$.

We continue to assume $2 \in G(S)$; consider a vertex $i \in S$. Let $j \in S$ be a vertex that is adjacent to i. Then, as above, j and $i - j \in S$ are adjacent to i. This time, $j \neq i - j$ if and only if $j \neq 2^{-1}i \in S$. So, every vertex $i \in S$ is adjacent to an *odd* number of vertices in S. In view of $\Gamma(S)$ being regular of even degree we can state:

Every vertex $i \in S \cup \{0\}$ is adjacent to an *even* number of vertices *not* in $S \cup \{0\}$.

Put $V_1 = S \cup \{0\}$, $V_2 = (\mathbb{Z}/p\mathbb{Z}) \setminus V_1$. We have proved: every vertex in V_2 is adjacent to an even number of vertices in V_1 and every vertex in V_1 is adjacent to an even number of vertices in V_2. Thus, $\{V_1, V_2\}$ is an EVD of $\Gamma(S)$; see (2.5). Since $\Gamma(S)$ is not complete; that is, $S \neq (\mathbb{Z}/p\mathbb{Z})^*$, we have found a non-trivial EVD. Consequently, by (2.7), $\Gamma(S)$ has property P_c with $c \geq 1$. ∎

The converse of Theorem 3.3 does not hold in general as will follow from results like Theorem 4.8 in the next section.

Let $\xi = \xi_p$ be a primitive p-th root of unity. It is natural to associate with a graph set $S \subset (\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$ an element γ_S in the ring of integers $\mathbb{Z}[\xi]$ of the p-th cyclotomic field $\mathbb{Q}(\xi)$. We put

$$\gamma_S = \sum_{j=1}^{p-1} a_j \xi^j \text{ where } a_j = \begin{cases} 1 & \text{if } j \in S \\ 0 & \text{otherwise.} \end{cases}$$

Let F be the fixed field of the subgroup $G = G(S)$ of $\mathrm{Gal}\big(\mathbb{Q}(\xi)/\mathbb{Q}\big)$. Clearly, γ_S lies in the ring O_F of integers of F. We define:

$a = a(S) \geq 0$ is the number of distinct dyadic primes of O_F that divide (γ_S).

$b = b(S) \geq 1$ is the smallest natural number satisfying $2^b \in G(S)$.

f is the order of 2 modulo p.

Then $(2^b)^{\#G} \equiv 1 \bmod p$ and $\frac{p-1}{b \cdot \#G}$ is the total number of dyadic primes of F. Thus we can say

$$f \mid b \cdot \#G \mid p - 1. \tag{3.4}$$

It might be a bit of a surprise that, for a circulant graph $\Gamma(S)$, our problem of determining its property P_c essentially amounts to being able to compute $a = a(S)$; namely:

THEOREM 3.5 (P. E. CONNER). *Let $\Gamma(S)$ be a circulant graph. Then $\Gamma(s)$ has property P_c with*

$$c = a \cdot b \cdot \#G.$$

ADDENDUM. If $S = (\mathbb{Z}/p\mathbb{Z})^{*n}$ and $2 \in S$, then $a \equiv n - 1 \bmod 2$.

For the proofs we refer to the appendix.

COROLLARY 3.6. *If 2 is a primitive root modulo p, then every circulant graph $\Gamma(S)$ with $S \neq \emptyset$ on p vertices has property P_0.*

PROOF. The totally disconnected graph has been excluded. So, by (2.7) with $t = p$, $\Gamma(S)$ has property P_c for some c satisfying

$$0 \leq c < p - 1.$$

The assumption of 2 being a primitive root modulo p means $f = p - 1$. By (3.4) we obtain $b \cdot \#G = p - 1$ and conclude by Theorem 3.5 that

$$p - 1 \mid c;$$

so $c = 0$. ∎

A *Sophie-Germain prime* is a prime number p for which $\frac{p-1}{2}$ is also a prime. It is still open if there are infinitely many such primes.

COROLLARY 3.7. *If p is a Sophie-Germain prime, then every circulant graph $\Gamma(S)$ with $S \neq \emptyset$ on p vertices has property P_0.*

PROOF. For a Sophie-Germain prime p, the only possibilities for f are $\frac{p-1}{2}$ and $p-1$. As in the proof of Corollary 3.6 we conclude that c is a multiple of f and c is even, so $p - 1 \mid c$, implying $c = 0$. ∎

4. **Applications.** We are going to exhibit infinite families of connected, regular graphs whose property P_c can be determined effectively in number theoretic terms. These graphs will be circulant graphs on p vertices where p denotes an odd prime number.

For any odd n satisfying $1 \leq n \leq p - 2$ we consider the graph set

$$S_n = \left\{ j \in (\mathbb{Z}/p\mathbb{Z})^* : \frac{n+1}{2} \leq j \leq p - \frac{n+1}{2} \right\};$$

so

$$S_1 = (\mathbb{Z}/p\mathbb{Z})^*, \quad \#S_n = p - n, \quad S_{p-2} = \left\{ \pm \frac{p+1}{2} \right\}.$$

PROPOSITION 4.1. *Let p be an odd prime. Then every circulant graph $\Gamma(S_n)$ with a graph set $S_n \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ as above has property P_0.*

PROOF. The integer $\gamma_{S_n} \in \mathbb{Z}[\xi]$ associated with S_n is given by

$$\gamma_{S_n} = \eta_{\frac{n+1}{2}} + \eta_{\frac{n+3}{2}} + \cdots + \eta_{\frac{p-3}{2}} + \eta_{\frac{p-1}{2}}$$

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

where

$$\eta_i = \xi^i + \xi^{-i}.$$

Thus

$$\begin{aligned}\gamma_{S_n} &= -(1 + \eta_1 + \eta_2 + \cdots + \eta_{\frac{n-1}{2}}) \\ &= -\xi^{\frac{n-1}{2}} \cdot \frac{\xi^n - 1}{\xi - 1},\end{aligned}$$

a cyclotomic unit. Consequently the norm of γ_{S_n} from $\mathbb{Q}(\xi)$ to $\mathbb{Q}$ is ± 1, hence odd. So, $a = a(S)$ is 0 in Theorem 3.5 and $\Gamma(S_n)$ has property P_0. ∎

We have seen how to obtain in a systematic way circulant graphs having property P_0. Now our main concern is to determine connected graphs having property P_c with c large; recall (2.9).

Let us consider *Paley graphs*, the "quintessential example of concrete random graphs on $p \equiv 1 \bmod 4$ vertices for which the edges are chosen independently and with probability $\frac{1}{2}$"; compare [4]. They are defined, for primes $p \equiv 1 \bmod 4$, as the circulant graphs $\Gamma(S)$ with

$$S = (\mathbb{Z}/p\mathbb{Z})^{*2} = \left\{ j \in (\mathbb{Z}/p\mathbb{Z})^* : \left(\frac{j}{p}\right) = +1 \right\}.$$

We notice that S is a graph set since we have arranged for $(\frac{-1}{p}) = +1$. Since S is the group of quadratic residues modulo p, we have $G(S) = S$, $\Gamma(S)$ is regular of degree $\frac{p-1}{2}$ and

$$2 \in G(S) \text{ if and only if } \left(\frac{2}{p}\right) = +1.$$

So, by Theorem 3.3 we know already: If $p \equiv 1 \bmod 8$, then the Paley graph on p vertices does *not* have property P_0. Specifically:

THEOREM 4.2. *Let p be a prime, $p \equiv 1 \bmod 4$, $S = (\mathbb{Z}/p\mathbb{Z})^{*2}$. Then we have for the Paley graph:*

$\Gamma(S)$ has property P_0 if and only if $p \equiv 5 \bmod 8$

$\Gamma(S)$ has property $P_{\frac{p-1}{2}}$ if and only if $p \equiv 1 \bmod 8$.

PROOF. The group $G(S)$ has $\frac{p-1}{2}$ elements, so $\Gamma(S)$ has property P_c for some multiple c of $\frac{p-1}{2}$, by Theorem 3.5; thus $c = \frac{p-1}{2}$ or $c = 0$ since $0 \le c < p - 1$. For $p \equiv 1 \bmod 8$ we have already concluded by Theorem 3.3 that $\Gamma(S)$ does not have property P_0, so $\Gamma(S)$ has property $P_{\frac{p-1}{2}}$. For $p \equiv 5 \bmod 8$ we obtain $b = 2$ in Theorem 3.5 since $2 \notin G(S)$; consequently c is a multiple of $2 \cdot \frac{p-1}{2} = p - 1$, so $c = 0$. ∎

We can rephrase the above result as follows:

COROLLARY 4.3. *The Paley graph does not have property P_0 if and only if 2 is a square modulo p.*

It will pay off later to reprove this in terms of *Gaussian sums*. For $S = (\mathbb{Z}/p\mathbb{Z})^{*2}$, γ_S is given by

$$\gamma_S = \sum_{j=1}^{p-1} \frac{1 + (\frac{j}{p})}{2} \xi^j = \frac{-1}{2} + \frac{1}{2} \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \xi^j,$$

an integer in $\mathbb{Q}(\sqrt{p})$. Namely:

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\xi^j = \sqrt{p}. \tag{4.4}$$

and hence $\gamma_S = \frac{-1+\sqrt{p}}{2}$. The norm of γ_S from $\mathbb{Q}(\sqrt{p})$ over $\mathbb{Q}$ is $\frac{1-p}{4}$ which is odd if and only if $p \equiv 5 \bmod 8$. So, we have $a = 0$ with $c = 0$ in Theorem 3.5 if and only if $p \equiv 5 \bmod 8$ and $a = 1$ with $c = \frac{p-1}{2}$ if and only if $p \equiv 1 \bmod 8$. ∎

It seems to be natural to look at the following generalization of Paley graphs. Choose an odd prime q and consider

$$S = (\mathbb{Z}/p\mathbb{Z})^{*q}.$$

Clearly, S is a graph set since -1 is a q-th power and $G(S) = S$. If $p \not\equiv 1 \bmod q$, then $S = (\mathbb{Z}/p\mathbb{Z})^*$. Thus $\Gamma(S)$ is the complete graph on p vertices and has property P_0. We exclude this easy case and assume $p \equiv 1 \bmod q$. Then Theorem 4.2 and Corollary 4.3 generalize to:

THEOREM 4.5. *Let p be a prime, $p \equiv 1 \bmod q$ with an odd prime q; $S = (\mathbb{Z}/p\mathbb{Z})^{*q}$. Then $\Gamma(S)$ does not have property P_0 if and only if 2 is a q-th power modulo p.*

PROOF. If 2 is a q-th power mod p, then $\Gamma(S)$ does not have property P_0, by Theorem 3.3. If 2 is not a q-th power mod p, then $b \cdot \#G = q \cdot \frac{p-1}{q} = p - 1$ and hence $c = 0$ in Theorem 3.5. ∎

For $q = 3$ this result can be made specific in terms of p being represented by a positive definite binary quadratic form over $\mathbb{Z}$. Namely for primes $p \equiv 1 \bmod 3$, even Gauss observed

(4.6) 2 is a cube modulo p if and only if $p = x^2 + 27y^2$ for some $x, y \in \mathbb{Z}$;

compare for example [20]. Thus

COROLLARY 4.7. *Let p be a prime, $p \equiv 1 \bmod 3$, $S = (\mathbb{Z}/p\mathbb{Z})^{*3}$. Then $\Gamma(S)$ does not have property P_0 if and only if $p = x^2 + 27y^2$ for some $x, y \in \mathbb{Z}$.*

This tells us that for $p = 31, 43, 109, \ldots$ the circulant graphs $\Gamma(S)$ with $S = (\mathbb{Z}/p\mathbb{Z})^{*3}$ have property P_c with $c = \frac{p-1}{3}$ or $c = 2 \cdot \frac{p-1}{3}$. One can be even more specific. By the addendum to Theorem 3.5 with $n = 3$ we conclude that $a \equiv 0 \bmod 2$, so $a = 2$. Hence, for all primes $p = x^2 + 27y^2$, the graph $\Gamma(S)$ has property P_c with $c = 2 \cdot \frac{p-1}{3}$.

Here we would like to express our thanks to the referee for the natural question whether it is always possible to give the precise value of c in the situation of Theorem 4.5. We can announce that the answer will be yes for $q = 5$ and $q = 7$ also. Namely, with $p \equiv 1 \bmod q$ and $2 \in S$, we have in Theorem 4.5:

If $S = (\mathbb{Z}/p\mathbb{Z})^{*5}$, then $\Gamma(S)$ has property P_c with $c = 4 \cdot \frac{p-1}{5}$.
If $S = (\mathbb{Z}/p\mathbb{Z})^{*7}$, then $\Gamma(S)$ has property P_c with $c = 6 \cdot \frac{p-1}{7}$.

Thus, for $q = 3, 5, 7$, we obtain $c = (q-1) \cdot \frac{p-1}{q}$, a result which one however is not allowed to expect for all p if $q > 7$. Already for $q = 11$, the circulant graph on

$p = 331$ vertices given by $S = (\mathbb{Z}/p\mathbb{Z})^{*11}$ has 2^{180} EVD's; that is, it has property P_c with $c = 6 \cdot \frac{p-1}{11}$.

We turn to another analogue of Paley graphs, namely circulant graphs on p vertices defined in terms of fourth powers modulo p.

Let p be a prime, $p \equiv 1 \bmod 8$, and denote by $[\frac{\cdot}{p}]_4$ the fourth power symbol modulo p. Put

$$S = (\mathbb{Z}/p\mathbb{Z})^{*4} = \left\{ j \in (\mathbb{Z}/p\mathbb{Z})^* : \left[\frac{j}{p}\right]_4 = +1 \right\}.$$

Because of $p \equiv 1 \bmod 8$, -1 is a fourth power modulo p and S is a graph set. Clearly, $G(S) = S$ and $\#G(S) = \frac{p-1}{4}$. Moreover, 2 is a square modulo p; if 2 is a fourth power modulo p, then $2 \in G(S)$ and the circulant graph $\Gamma(S)$ does not have property P_0, by Theorem 3.3. Hence, if $\Gamma(S)$ has property P_0, then $[\frac{2}{p}]_4 = -1$, and we prove:

THEOREM 4.8. *Let p be a prime, $p \equiv 1 \bmod 8$; $S = (\mathbb{Z}/p\mathbb{Z})^{*4}$. If $[\frac{2}{p}]_4 = -1$, then:*
$\Gamma(S)$ has property P_0 if and only if $p \equiv 1 \bmod 16$.
$\Gamma(S)$ has property $P_{\frac{p-1}{2}}$ if and only if $p \equiv 9 \bmod 16$.

PROOF. The group $G(S) = S$ has $\frac{p-1}{4}$ elements, 2 is a square modulo p, but not a fourth power, so $b = 2$ and c is a multiple of $\frac{p-1}{2}$, by Theorem 3.5. Thus, $\Gamma(S)$ has property P_c with

$$c = 0 \quad \text{or} \quad c = \frac{p-1}{2},$$

in which case $a = 0$ or $a = 1$ in Theorem 3.5, respectively.

The fixed field F of $G \subseteq \mathrm{Gal}\big(\mathbb{Q}(\xi)/\mathbb{Q}\big)$ is of degree 4 over $\mathbb{Q}$, and we have a tower of cyclic subfields of the p-th cyclotomic field $\mathbb{Q}(\xi)$ with relative degrees as indicated:

$$\mathbb{Q} \overset{2}{\hookleftarrow} \mathbb{Q}(\sqrt{p}) \overset{2}{\hookleftarrow} F \overset{\frac{p-1}{8}}{\hookleftarrow} \mathbb{Q}(\xi + \xi^{-1}) \overset{2}{\hookleftarrow} \mathbb{Q}(\xi).$$

Consider the integer $\gamma_S \in F$ that is associated with the graph set $S = (\mathbb{Z}/p\mathbb{Z})^{*4}$. It is given by

$$\gamma_S = \sum_{\substack{j=1 \\ j \text{ fourth power mod } p}}^{p-1} \xi^j = \sum_{\substack{j=1 \\ j \text{ fourth power mod } p}}^{\frac{p-1}{2}} \eta_j$$

where $\eta_j = \xi^j + \xi^{-j}$. Let us determine the norm of γ_S from F to $\mathbb{Q}(\sqrt{p})$. The Galois group of F over $\mathbb{Q}(\sqrt{p})$ is generated by the automorphism δ_2 induced by $\xi \longrightarrow \xi^2$. Here we use $\left[\frac{2}{p}\right]_4 = -1$ again. The η's multiply according to $\eta_i \eta_j = \eta_{i+j} + \eta_{i-j}$, so $\eta_{x^4} \cdot \eta_{2y^4} = \eta_{x^4+2y^4} + \eta_{x^4-2y^4}$.

Since -1 is a fourth power modulo p, this identity yields:

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S = \gamma_S \cdot \delta_2(\gamma_S) = s \cdot \Sigma^+ + n \cdot \Sigma^-$$

with

$$\Sigma^+ = \sum_{\substack{j=1 \\ j \text{ square mod } p}}^{p-1} \xi^j, \quad \Sigma^- = \sum_{\substack{j=1 \\ j \text{ non-square mod } p}}^{p-1} \xi_j,$$

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

$$s = \#\{(X^4, Y^4) \in S \times S : v = X^4 + 2Y^4\}$$
$$n = \#\{(X^4, Y^4) \in S \times S : w = X^4 + 2Y^4\},$$

where v denotes any quadratic residue and w denotes any quadratic non-residue modulo p.

We stress again that the values of s and n do not depend on the particular choice of the non-zero square v and the non-square w, respectively.

In particular,

$$s = \#\{(X^4, Y^4) \in S \times S : 1 = X^4 + 2Y^4\}$$
$$= \#\{(X^4, Y^4) \in S \times S : 2 = X^4 + Y^4\},$$

and we conclude that s is odd.

There are $\frac{p-1}{2}$ summands in Σ^+ and Σ^- each, thus

$$s \cdot \frac{p-1}{2} + n \cdot \frac{p-1}{2} = \left(\frac{p-1}{4}\right)^2;$$

so,

$$s + n = \frac{p-1}{8}.$$

Once again we can use the Gaussian sum (4.4) in order to find Σ^+ and Σ^-. From

$$\Sigma^+ + \Sigma^- = -1 \quad \text{and} \quad \Sigma^+ - \Sigma^- = \sqrt{p}$$

we obtain

$$\Sigma^+ = \frac{-1 + \sqrt{p}}{2}, \quad \Sigma^- = \frac{-1 - \sqrt{p}}{2}.$$

Hence,

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S = s \cdot \frac{-1 + \sqrt{p}}{2} + n \cdot \frac{-1 - \sqrt{p}}{2};$$

that is,

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S = -s + (s - n)\frac{1 + \sqrt{p}}{2}.$$

This norm computation will make explicit the circulant graph's property P_c. Namely:

If $p \equiv 1 \bmod 16$, then $\frac{p-1}{8}$ is even and thus $s - n \equiv 0 \bmod 2$. Since s is odd, we obtain

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \in 1 + 2\mathbb{Z}\left[\frac{1 + \sqrt{p}}{2}\right],$$

so $N_{F/\mathbb{Q}}\gamma_S$ odd, so $a = 0$ in Theorem 3.5 and hence $c = 0$.

Similarly, if $p \equiv 9 \bmod 16$, then $\frac{p-1}{8}$ is odd and thus $s - n \equiv 1 \bmod 2$. Since s is odd we obtain

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \in 2\mathbb{Z}\left[\frac{1 + \sqrt{p}}{2}\right],$$

so $N_{F/\mathbb{Q}}\gamma_S$ even, so $a \neq 0$ in Theorem 3.5 and hence $c = \frac{p-1}{2}$. ∎

We notice from Theorem 4.8 that the converse of Theorem 3.3 does not hold. The analogue of Theorem 4.2 for $2 \in G(S)$ is given by:

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

THEOREM 4.9. *Let p be a prime, $p \equiv 1 \bmod 8$; $S = (\mathbb{Z}/p\mathbb{Z})^{*4}$. If $[\frac{2}{p}]_4 = +1$, then:*

$\Gamma(S)$ has property $P_{\frac{p-1}{4}}$ if and only if $p \equiv 9 \bmod 16$.

$\Gamma(S)$ has property $P_{3\cdot\frac{p-1}{4}}$ if and only if $p \equiv 1 \bmod 16$.

PROOF. We try to follow the proof of Theorem 4.8 and point out the different features. This time, 2 is a fourth power modulo p, so $b = 1$ and c is a non-zero multiple of $\frac{p-1}{4}$ by Theorems 3.3 and 3.5. Thus $\Gamma(S)$ has property P_c with

$$c = \frac{p-1}{4} \quad \text{or} \quad c = \frac{p-1}{2} \quad \text{or} \quad c = 3 \cdot \frac{p-1}{4}$$

in which case $a = 1$ or $a = 2$ or $a = 3$, respectively.

The Galois group of F over $\mathbb{Q}(\sqrt{p})$ is generated by an automorphism δ_g induced by $\xi \longrightarrow \xi^g$, where g denotes any square modulo p that is not a fourth power. Again we obtain

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S = s\Sigma^+ + n\Sigma^-,$$

this time with

$$s = \#\{(X^4, Y^4) \in S \times S : v = X^4 + gY^4\}$$

and

$$n = \#\{(X^4, Y^4) \in S \times S : w = X^4 + gY^4\}.$$

with v and w as before. In particular,

$$\begin{aligned} s &= \#\{(X^4, Y^4) \in S \times S : 1 = X^4 + gY^4\} \\ &= \#\{(X^4, Y^4) \in S \times S : g = X^4 + Y^4\}. \end{aligned}$$

Since g does not differ from 2 by a fourth power, we conclude that—differently from Theorem 4.8—s is even.

As before, we have $s + n = \frac{p-1}{8}$ and

$$N_{F/\mathbb{Q}(\sqrt{p})}\gamma_s = -s + (s-n)\frac{1+\sqrt{p}}{2}.$$

which now yields:

if $p \equiv 1 \bmod 16$, then $N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \in 2\mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$;

if $p \equiv 9 \bmod 16$, then $N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \in 1 + 2\mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$.

The fixed field F has four dyadic primes. By the addendum to Theorem 3.5 we can eliminate the possibility of $a = 2$. Namely with $n = 4$ we have $a \equiv 1 \bmod 2$, so $a = 1$ or $a = 3$.

Hence

if $N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \in 2\mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$, then $a = 3$;

if $N_{F/\mathbb{Q}(\sqrt{p})}\gamma_S \notin 2\mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$, then $a = 1$.

Thus, $p \equiv 1 \bmod 16$ implies $c = 3 \cdot \frac{p-1}{4}$ and $p \equiv 9 \bmod 16$ implies $c = \frac{p-1}{4}$. ∎

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

As before for cubes, we can characterize the property of 2 being a fourth power modulo p in terms of p being represented by a positive definite binary quadratic form over $\mathbb{Z}$. For primes $p \equiv 1 \bmod 8$, the result we can attribute to Dirichlet is:

$$\left[\frac{2}{p}\right]_4 = +1 \text{ if and only if } p = x^2 + 64y^2 \text{ for some } x, y \in \mathbb{Z}; \tag{4.10}$$

compare for example the exercise in [17, p. 70].

Thus, given any fourth power circulant graph on $p \equiv 1 \bmod 8$ vertices, one can readily determine its property P_c by:

COROLLARY 4.11. *Let p be a prime, $p \equiv 1 \bmod 8$; $S = (\mathbb{Z}/p\mathbb{Z})^{*4}$. Then:*

$\Gamma(S)$ has property P_0 if and only if $p \equiv 1 \bmod 16$ and $p \neq x^2 + 64y^2$ for all $x, y \in \mathbb{Z}$

$\Gamma(S)$ has property $P_{\frac{p-1}{4}}$ if and only if $p \equiv 9 \bmod 16$ and $p = x^2 + 64y^2$ for some $x, y \in \mathbb{Z}$

$\Gamma(S)$ has property $P_{\frac{p-1}{2}}$ if and only if $p \equiv 9 \bmod 16$ and $p \neq x^2 + 64y^2$ for all $x, y \in \mathbb{Z}$

$\Gamma(S)$ has property $P_{3\cdot\frac{p-1}{4}}$ if and only if $p \equiv 1 \bmod 16$ and $p = x^2 + 64y^2$ for some $x, y \in \mathbb{Z}$.

PROOF. Combine Theorem 4.8, Theorem 4.9 and statement (4.10). ∎

Each of the four classes of primes listed in Corollary 4.11 has a density $\frac{1}{4}$ in the set of all primes $p \equiv 1 \bmod 8$. We see that for $p \equiv 17, 73, 41$, and 113 the fourth power circulant graphs have property P_0, $P_{\frac{p-1}{4}} = P_{18}$, $P_{\frac{p-1}{2}} = P_{20}$, and $P_{3\cdot\frac{p-1}{4}} = P_{84}$, respectively.

Concerning the fourth power symbol $\left[\frac{2}{p}\right]_4$, we would like to point out the following analogy. For a prime $p \equiv 1 \bmod 8$, the 2-Sylow subgroup of the ideal class group of both imaginary quadratic number fields

$$\mathbb{Q}(\sqrt{-p}) \text{ and } \mathbb{Q}(\sqrt{-2p})$$

is known to be cyclic of order divisible by 4, see *e.g.* [6, (18.6) and (19.2)]. So, both class numbers $h\big(\mathbb{Q}(\sqrt{-p})\big)$ and $h\big(\mathbb{Q}(\sqrt{-2p})\big)$ are multiples of 4.

It has been proved in [1] that

$$h\big(\mathbb{Q}(\sqrt{-p})\big) \equiv 0 \bmod 8 \text{ if and only if } p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z}. \tag{4.12}$$

Now it is known that $h\big(\mathbb{Q}(\sqrt{-2p})\big)$ is a multiple of 8 if and only if $\left[\frac{2}{p}\right]_4 = +1$. Hence, by (4.10), we have analogously to (4.12):

$$h\big(\mathbb{Q}(\sqrt{-2p})\big) \equiv 0 \bmod 8 \text{ if and only if } p = x^2 + 64y^2 \text{ for some } x, y \in \mathbb{Z}. \tag{4.13}$$

There is a vast literature on the divisibility of $h\big(\mathbb{Q}(\sqrt{-p})\big)$ and $h\big(\mathbb{Q}(\sqrt{-2p})\big)$ by 8. For some further references we just point out the recent paper [19]. For a reformulation of (4.13) in terms of the quadratic form $x^2 + 32y^2$ we refer to [6; 24.6]. Thus also Corollary 4.11 can be expressed in terms of $x^2 + 32y^2$.

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

A final remark on 4-ranks of narrow ideal class groups: we can choose primes $p_i \equiv 1 \bmod 4$ for $i = 1, \ldots, 257$ such that the graph Γ_E associated with the real quadratic field

$$E = \mathbb{Q}(\sqrt{p_1 p_2 \cdot \cdots \cdot p_{257}})$$

is the circulant graph $\Gamma(S)$ with $S = (\mathbb{Z}/257\mathbb{Z})^{*4}$. Then we have obtained a *connected* graph with 2^{192} Eulerian vertex decompositions and can conclude that

2-rank $C(E) = 256$

4-rank $C(E) = 192$.

This is the result of Corollary 4.11 for the prime $p = 257 = 1 \bmod 16$, $257 \equiv 1^2 + 64 \cdot 2^2$, about property $P_{3 \cdot \frac{p-1}{4}} = P_{192}$.

5. **Appendix.** Here is a proof of Theorem 3.5. As before, p is an odd prime number, $\xi = \xi_p$, and $\Gamma(S)$ denotes the circulant graph associated with a graph set $S \subset (\mathbb{Z}/p\mathbb{Z})^*$. We want to deduce that $\Gamma(S)$ has property P_c where

$$c = a \cdot b \cdot \#G$$

with $a = a(S)$, $b = b(S)$, $G = G(S)$ defined as before in Theorem 3.5.

Let C_p be a cyclic group of order p with generator t and consider the group ring $\mathbb{F}_2[C_p]$. There is a 1 : 1 correspondence between the set of subsets L of $(\mathbb{Z}/p\mathbb{Z})^*$ and

$$\left\{ \sum_{j=0}^{p-1} \gamma_j t^j \in \mathbb{F}_2[C_p] : \gamma_0 = 0 \right\}$$

given by $L \longrightarrow \gamma_L = \sum_{j=0}^{p-1} X_L(j) t^j$ with characteristic function $X_L(j) = 1$ if $j \in L$ and $X_L(j) = 0$ otherwise.

Every EVD of $\Gamma(S)$ is an unordered pair $\{L, (\mathbb{Z}/p\mathbb{Z}) \setminus L\}$ for some $L \subseteq (\mathbb{Z}/p\mathbb{Z})^*$. In $\mathbb{F}_2[C_p]$ we have

$$\begin{aligned} \gamma_S \cdot \gamma_L &= \sum_{s=0}^{p-1} X_s(s) t^s \cdot \sum_{j=0}^{p-1} X_L(j) t^j \\ &= \sum_{i=0}^{p-1} \Big(\sum_{s+j \equiv i(p)} X_S(s) X_L(j) \Big) t^i \\ &= \sum_{i=0}^{p-1} \Big(\sum_{j=0}^{p-1} X_S(i-j) X_L(j) \Big) t^i. \end{aligned}$$

Since $\Gamma(S)$ is Eulerian, a subset L of $(\mathbb{Z}/p\mathbb{Z})^*$ yields an EVD if and only if every vertex $i = 0, 1, \ldots, p-1$ of $\Gamma(S)$ is adjacent to an even number of vertices in L; that is, if and only if $\sum_{j=0}^{p-1} X_S(i-j) X_L(j)$ is even for all i, $0 \le i \le p-1$. The last condition means $\gamma_L \cdot \gamma_S = 0$ in $\mathbb{F}_2[C_p]$. So: the number of EVD's of $\Gamma(S)$ is equal to the number of elements in

$$\left\{ \sum_{j=0}^{p-1} \gamma_j t^j \in \mathbb{F}_2[C_p] : \gamma_0 = 0 \text{ and } \gamma \cdot \gamma_S = 0 \right\}.$$

https://doi.org/10.4153/CJM-1994-005-2 Published online by Cambridge University Press

We map $\mathbb{F}_2[C_p]$ onto $\mathbb{Z}[\xi]/(2)$ by $t \longrightarrow \xi$. Every element of $\mathbb{Z}[\xi]/(2)$ can be written uniquely as $\sum_{j=0}^{p-1} \gamma_j \xi^j$ with $\gamma_j \in \{0,1\}$ and $\gamma_0 = 0$. The only relation between $1, \xi, \xi^2, \ldots, \xi^{p-1}$ to consider is $1 + \xi + \cdots + \xi^{p-1} = 0$. For all $\gamma \in \mathbb{F}_2[C_p]$ we have $\gamma \cdot \gamma_S \neq 1 + t + \cdots + t^{p-1}$ since the augmentation of γ_S is even and p is odd. Thus we obtain: the number of EVD's of $\Gamma(S)$ is equal to the number of elements in

$$\{\gamma \in \mathbb{Z}[\xi]/(2) : \gamma \cdot \gamma_S = 0\},$$

where γ_S now stands for $\sum_{s=0}^{p-1} X_S(s)\xi^s \in \mathbb{Z}[\xi]/(2)$, of course. What is the number of elements in the annihilating ideal of γ_S in $\mathbb{Z}[\xi]/(2)$? The ideal (2) is a product of distinct prime ideals in $\mathbb{Z}[\xi]$, so the ring $\mathbb{Z}[\xi]/(2)$ is a direct sum of fields, with one direct summand each for every dyadic prime of $\mathbb{Q}(\xi)$. Hence: the number of EVD's of $\Gamma(S)$ is equal to the number of elements in

$$\mathbb{Z}[\xi]/(2, \gamma_S).$$

In other words, by (2.7), we have concluded that $\Gamma(S)$ has property P_c if and only if the ideal norm from $\mathbb{Q}(\xi)$ to $\mathbb{Q}$ of the greatest common divisor of (γ_S) and (2) is $2^c\mathbb{Z}$; *i.e.*

$$N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\gamma_S, 2) = 2^c\mathbb{Z}.$$

Each dyadic ideal of $\mathbb{Q}(\xi)$ has absolute norm $2^f\mathbb{Z}$, where f is the order of 2 modulo p. Thus $\Gamma(S)$ has property P_c means:

$$c = f \cdot \#\text{ of distinct dyadic primes of } \mathbb{Q}(\xi) \text{ that divide } (\gamma_S).$$

The total number of dyadic primes of $\mathbb{Q}(\xi)$ is $\frac{p-1}{f}$. The degree of the fixed field F of $G(S)$ over $\mathbb{Q}$ is $\frac{p-1}{\#G}$; each dyadic prime of F has inertial degree b, so, the total number of dyadic primes of F is $\frac{p-1}{b\cdot\#G}$.

This tells us that each dyadic prime of F splits in $\mathbb{Q}(\xi)$ into a product of $\frac{p-1}{f} \cdot \frac{b\cdot\#G}{p-1} = \frac{b\cdot\#G}{f}$ distinct dyadic primes. Thus, if a is the number of distinct dyadic primes of F dividing (γ_S), then $a \cdot \frac{b\cdot\#G}{f}$ is the number of distinct dyadic primes of $\mathbb{Q}(\xi)$ that divide (γ_S). So, $c = a \cdot b \cdot \#G$. ∎

Here is a proof of the addendum to Theorem 3.5. We may assume $S = G(S)$ with $\#S = \frac{p-1}{n}$ and $2 \in S$. The fixed field F of S has degree n over $\mathbb{Q}$. As an element of the ring O_F of integers F, we have $\gamma_S = \text{trace}_{\mathbb{Q}(\xi)/F}(\xi)$ and hence

$$\text{trace}_{F/\mathbb{Q}}\, \gamma_S = -1.$$

Since $2 \in G(S)$, we conclude that F is contained in the fixed field of the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by 2. Therefore the rational prime 2 splits completely in F. So, F has n dyadic primes, $D_1, \ldots, D_n$, say. Consider the n residue homomorphisms

$$r_i : O_F \longrightarrow O_F/Di \cong \mathbb{F}_2.$$

We have $r_i(\gamma_S) = 1$ if and only if D_i does not divide (γ_S), and $r_i(\gamma_S) = 0$ for each of the a distinct dyadic primes of F that divide (γ_S). Thus: $-1 = \text{trace}_{F/\mathbb{Q}}\, \gamma_S = \sum_{i=1}^{n} r_i(\gamma_S) = n - a$ in $\mathbb{Z}/2\mathbb{Z}$; so $n - a$ is odd; that is, $a \equiv n - 1 \bmod 2$. ∎

REFERENCES

1. P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. reine angew. Math. **238**(1969), 67–70.
2. N. L. Biggs, *Algebraic Graph Theory*, Cambridge Tracts in Math. **67**, Cambridge Univ. Press, 1974.
3. N. L. Biggs and A. T. White, *Permutation Groups and Combinatorical Structures*, London Math. Soc. Lecture Note Ser. **33**, Cambridge Univ. Press, 1979.
4. B. Bollobás, *Random Graphs*, Academic Press, London, 1985.
5. B. Brauckmann, *4-ranks of S-ideal class groups*, preprint, (1990).
6. P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. **8**, World Scientific, Singapore, 1988.
7. F. Gerth III, *The 4-class ranks of quadratic fields*, Invent. Math. **77**(1984), 489–515.
8. ———, *The 4-class ranks of quadratic extensions of certain real quadratic fields*, J. Number Theory **33**(1989), 18–31.
9. G. Gras, *Sur la norme du groupe des unites d'extensions quadratiques relatives*, preprint, (1990).
10. F. Halter-Koch, *Über den 4-Rang der Klassengruppe quadratischer Zahlkorper*, J. Number Theory, (1984), 219–227.
11. J. Hurrelbrink, *On the norm of the fundamental unit*, preprint, (1990).
12. J. C. Lagarias, *On determining the 4-rank of the ideal class group of a quadratic field*, J. Number Theory **12**(1980), 191–196.
13. P. Morton, *Density results for the 2-class groups of imaginary quadratic fields*, J. reine angew. Math. **332**(1982), 156–187.
14. L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppen eines beliebigen quadratischen Zahlkorpers*, J. reine angew. Math. **170**(1934), 69–74.
15. L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkorper*, J. reine angew. Math. **171**(1935), 55–60.
16. ———, *Über einige Mittelwertfragen im quadratischen Zahlkorper*, J. reine angew. Math. **174**(1936), 131–148.
17. H. E. Rose, *A Course in Number Theory*, Oxford Science Publ., Clarendon Press, Oxford, 1988.
18. P. Stevenhagen, *Rédei-matrices and the structure of quadratic 2-class groups*, preprint, (1991).
19. ———, *On the 2-power divisibility of certain quadratic class numbers*, preprint, (1991).
20. T. Y. Uehara, *On the 4-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31**(1989), 167–173.

Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana 70803
U.S.A.