Characterizations of Mersenne and 2-rooted primes

Sunil K. Chebolu a,*, Keir Lockridge b, Gaywalee Yamskulna a

a Department of Mathematics, Illinois State University, Normal, IL 61790, USA
b Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, USA

ARTICLE INFO

Article history:
Received 18 June 2014
Received in revised form 11 June 2015
Accepted 12 June 2015
Available online 22 June 2015
Communicated by Neal Koblitz

MSC:
primary 11A41, 11A07
secondary 15B99, 05C90

Keywords:
Mersenne primes
Group algebras
Circulant matrices
Primitive roots
Bipartite graphs

ABSTRACT

We give several characterizations of Mersenne primes (Theorem 1.1) and of primes for which 2 is a primitive root (Theorem 1.2). These characterizations involve group algebras, circulant matrices, binomial coefficients, and bipartite graphs.

© 2015 Elsevier Inc. All rights reserved.
1. Introduction

A Mersenne prime is a prime number of the form $2^n - 1$ for some positive integer $n$. (It is easy to see that if $n$ is composite, then so is $2^n - 1$. Therefore we may assume that $n$ is prime in the definition of a Mersenne prime.) These primes were named after the French monk Marin Mersenne who studied them in the early 17th century, but they appeared much earlier. In the 4th century BC, Euclid showed that if $2^p - 1$ is prime for a prime $p$, then $2^{p-1}(2^p - 1)$ is a perfect number. (Recall that a positive integer is perfect if it equals the sum of its proper divisors.) Euler studied these primes in the 17th century when he proved the converse of Euclid’s theorem. We refer the reader to [3] for a historical survey on Mersenne primes. In the late 1990s, the GIMPS (Great Internet Mersenne Prime Search) project rejuvenated interest in these primes. Although there has been much theoretical and computational research on Mersenne primes, basic questions about them remain open. For instance, it is not known whether there are infinitely many such primes.

In this paper we obtain several characterizations of Mersenne primes (Theorem 1.1) and also of primes for which 2 is a primitive root (Theorem 1.2). Some of these characterizations are obtained by studying groups of units in group algebras; others are based on binomial coefficients, circulant matrices, and bipartite graphs. Our characterizations will therefore translate theorems, unsolved problems, and conjectures about these primes into other areas of mathematics including commutative algebra, linear algebra and graph theory.

Our results on Mersenne primes are summarized in the following theorem. Let $C_p$ denote the (multiplicative) cyclic group of order $p$.

**Theorem 1.1 (Mersenne Primes).** Let $p > 3$ be a prime. Then the following statements are equivalent.

1. The prime $p$ is a Mersenne prime.
2. There is a non-trivial abelian group $G$ and a field $k$ such that every non-trivial unit in $kG$ has order $p$. 
(3) There is a non-trivial group $G$ and a field $k$ such that every non-trivial unit in $kG$ has order $p$.

(4) Every non-trivial unit in $\mathbb{F}_2 C_p$ has order $p$.

(5) $(1 + x + x^2)^p = 1$ in $\mathbb{F}_2 C_p$, where $x$ is a generator of $C_p$.

(6) $(1 + x)^p = (1 + x^3)^p$ in $\mathbb{F}_2 C_p$, where $x$ is a generator of $C_p$.

(7) $(\binom{p}{r}) \equiv (3r \mod p) \mod 2$ for all $1 \leq r \leq p - 1$.

(8) The group of $p \times p$ invertible circulant matrices over $\mathbb{F}_2$ is an elementary abelian $p$-group.

(9) The circulant matrix $\text{circ}(1,1,0,0,\cdots,0)$ is of order $p$ in the ring of $p \times p$ matrices over $\mathbb{F}_2$. (See Section 6 for definitions.)

(10) $[\text{circ}(1,1,0,0,\cdots,0)]^p = [\text{circ}(1,0,0,1,0,\cdots,0)]^p$ in the ring of $p \times p$ matrices over $\mathbb{F}_2$.

(11) Every circulant $(p,p)$ bipartite graph with an odd number of perfect matchings has $s_{ij}(p) \mod 2 = \delta_{ij}$, where $s_{ij}(p)$ is the number of pseudopaths between vertex $a_i$ and vertex $b_j$, and $\delta_{ij}$ is the Kronecker delta symbol. (See Section 7 for definitions.)

(12) The $(p,p)$ bipartite graph corresponding to the $p \times p$ circulant matrix $\text{circ}(1,1,1,0,0,\cdots,0)$ has $s_{ij}(p) \mod 2 = \delta_{ij}$.

Note that when $p = 3$, which is a Mersenne prime, the element $1 + x + x^2$ is a zero divisor in the ring $\mathbb{F}_2 C_3$ because $(1 + x + x^2)(1 + x) = 1 + x^3 = 1 + 1 = 0$. Therefore the above theorem breaks down partially when $p = 3$. However, it will be clear from our analysis that even in this case, statements 1, 2, 3, 4, 8, and 11 are equivalent.

Several characterizations of Mersenne primes in connection to binomial coefficients, number-theoretic functions, and units in a ring can be found in the literature. Here we state a few characterizations. An odd prime $p$ is Mersenne if and only if all the binomial coefficients $\binom{p}{r}$ $(0 \leq r \leq p)$ are odd numbers; see [10, Theorem 8.14]. The $n$th Catalan number is defined to be the quantity

$$\frac{1}{n+1} \binom{2n}{n}.$$ 

The $p$th Catalan number is odd if and only if $p$ is a Mersenne prime; see [10, Theorem 8.15]. Let $\sigma(n)$ denote the sum of the positive divisors of a positive integer $n$. The quantity $\sigma(n)$ is a power of 2 if and only if $n$ is a product of distinct Mersenne primes; see [10, Example 8.22]. There is a ring $R$ with exactly $p$ units if and only if $p$ is a Mersenne prime; see [6]. Our Theorem 1.1 adds several items to this list.

We now turn our attention to primes for which 2 is a primitive root (primes $p$ for which 2 generates the multiplicative group of the field with $p$ elements). It is well known that every odd prime $p$ has a primitive root. Since the multiplicative group of the field with $p$ elements is a cyclic group of order $p - 1$, we know that in fact there are $\phi(p - 1)$ primitive roots mod $p$, where $\phi$ is Euler’s totient function. However, there is no known formula or even a polynomial-time algorithm for finding a primitive root. So one looks
at the inverse primitive root problem. That is, we fix an integer $a$ and ask: for which odd primes $p$ will $a$ be a primitive root? For $a$ to be a primitive root mod $p$, there are some obvious necessary conditions on $a$. For instance, $a$ cannot be $-1$, because $(-1)^2 = 1$. Similarly, it is easy to see that $a$ cannot be a perfect square because a primitive root has to be a quadratic non-residue mod $p$. A deep conjecture of Artin says that these two conditions on $a$ are sufficient to guarantee the existence of infinitely many primes $p$ for which $a$ will be a primitive root.

**Artin’s Conjecture:** Let $a$ be an integer which is not a perfect square and not equal to $-1$. Then $a$ is a primitive root mod $p$ for infinitely many primes $p$.

There is no single specific value of $a$ for which Artin’s conjecture is resolved. However, it is known that the Generalized Riemann Hypothesis implies Artin’s Conjecture. We refer the reader to [9,11] for more details. The smallest positive integer $a$ that satisfies the conditions of Artin’s conjecture is $a = 2$. The corresponding special case of Artin’s Conjecture is the statement that there are infinitely many primes $p$ for which 2 is a primitive root. We will call such primes 2-rooted. In this paper we offer several characterizations of these primes, summarized in the next theorem.

**Theorem 1.2 (2-Rooted primes).** Let $p$ be an odd prime. Then the following are equivalent.

1. The prime 2 is a primitive root mod $p$.
2. $|\mathbb{F}_2 C_p^*| = 2^{p-1} - 1$.
3. The only units in $\mathbb{F}_2 C_p$ which have order $p$ are the non-identity elements of $C_p$.
4. If $\theta$ is an element of $\mathbb{F}_2 C_p$ which is not the norm element (the sum of all the group elements) and which is not in the kernel of the augmentation map, then $\theta$ is a unit.
5. There are $2^{p-1} - 1$ invertible circulant matrices of size $p \times p$ over $\mathbb{F}_2$.
6. The only invertible circulant matrices over $\mathbb{F}_2$ that have order dividing $p$ are the circulant permutation matrices. (See Section 6 for definitions.)
7. If $A$ is a $p \times p$ circulant matrix over $\mathbb{F}_2$ which is not $J$ (the $p \times p$ matrix with all 1’s) and the vector of all 1’s is not in the null space of $A$, then $A$ is invertible over $\mathbb{F}_2$.
8. There are $2^{p-1} - 1$ circulant $(p,p)$ bipartite graphs on labeled vertices with an odd number of perfect matchings. (See Section 7 for definitions.)
9. If $G$ is a circulant $(p,p)$ bipartite graph on labeled vertices with odd degree and if $G$ is not a complete bipartite graph, then $G$ has an odd number of perfect matchings.
10. If $G$ is a circulant $(p,p)$ bipartite graph on labeled vertices with an odd number of perfect matchings and $s_{ij}(p) \mod 2 = \delta_{ij}$ for all $1 \leq i, j \leq p$, then the degree of $G$ is 1. (See Section 7 for definitions.)

Moreover, if any of these statements hold, then $p \equiv 3$ or $5 \mod 8$.

There is another interesting characterization of these primes which occurs in connection to the Josephus problem [1]. Let $p$ be an odd prime expressed as $2m + 1$ for some positive integer $m$. Then the permutation
is transitive (which simply means that it is a single cycle containing all of 1, 2, \cdots, m) if and only if \( p \) is 2-rooted; see [1].

By combining Theorem 1.1 and Theorem 1.2 we recover the following result in number theory.

**Corollary 1.3.** The prime 3 is the only prime which is both Mersenne and 2-rooted.

This result is often obtained as an immediate consequence of the quadratic reciprocity law. Our proof is different and is relatively more elementary than the one which uses the reciprocity law; see Proposition 4.6.

We now explain how we arrived at these characterizations. It is interesting to note that the original problem which led to these characterizations seemed to have nothing to do with Mersenne primes or 2-rooted primes. To explain further, we need a definition. A ring \( R \) is said to have the diagonal property if its multiplication table has 1’s only on the diagonal. More precisely, this means that whenever \( ab = 1 \) in \( R \), then \( a = b \). The diagonal property for rings was introduced by the first author in [4], where it was shown that \( \mathbb{Z}_n \) has the diagonal property if and only if \( n \) is a divisor of 24. (In [4], the reader will find 5 different proofs of this fundamental result. These proofs are based on the Chinese Remainder Theorem, Dirichlet’s theorem on primes in an arithmetic progression, the structure of units in \( \mathbb{Z}_n \), the Bertrand–Chebyshev Theorem, and generalizations of the Bertrand–Chebyshev Theorem by Erdös and Ramanujan.) In [5], the first author and Mayers proved that the diagonal property holds for the ring of polynomials in \( m \) commuting variables over \( \mathbb{Z}_n \) if and only if \( n \) is a divisor of 12. (Note that the answer is independent of \( m \).) In [8], the second author and Genzlinger consider the proportion of units of order at most 2 in \( 
\mathbb{Z}_n \), proving for example that this proportion is the reciprocal of a prime \( p \) if and only if \( p \) is a Sophie Germain prime. Continuing this line of research, in Section 2 we investigate the diagonal property for group algebras and prove the following result. Write \( C_p^r \) to denote the direct sum of \( r \) copies of \( C_p \).

**Theorem 1.4.** Let \( G \) be a group and let \( k \) be a field. The group algebra \( kG \) has the diagonal property if and only if \( kG \) is either \( \mathbb{F}_2C_2^r \) or \( \mathbb{F}_3C_2^r \) for some \( 0 \leq r \leq \infty \).

After proving this result, we consider the following natural generalization of the diagonal property. Call a ring \( R \) a \( \Delta_n \)-ring if \( u^n = 1 \) for every unit of \( R \). If \( n \) is the smallest positive integer such that \( R \) satisfies this property, then call \( R \) a strict \( \Delta_n \)-ring. A ring \( R \) satisfies the diagonal property if and only if \( R \) is a \( \Delta_2 \)-ring. This generalization is what led us to Mersenne primes. In Section 2, we prove the following theorem.

**Theorem 1.5.** Let \( G \) be a non-trivial abelian group, let \( k \) be a field, and let \( p \) be an odd prime. The group algebra \( kG \) is a \( \Delta_p \)-ring if and only if \( p \) is a Mersenne prime and \( kG \) is either \( \mathbb{F}_2(C_p^r) \) or \( \mathbb{F}_{p+1}(C_p^r) \) for some \( 0 < r \leq \infty \).
It was the proof of this theorem and related investigations that gave us severals of the characterizations of Mersenne primes and 2-rooted primes mentioned in Theorems 1.1 and 1.2.

Organization. In Section 2, we find all group algebras which are \( \Delta_2 \)-rings and all abelian group algebras which are \( \Delta_p \)-rings for \( p \) an odd prime. In Section 3, we examine the structure of the units in \( \mathbb{F}_2C_p \) with a view toward the study of 2-rooted primes. Several characterizations of 2-rooted primes leading to Theorem 1.2 are obtained in Section 4. The element \( 1 + x + x^2 \) in \( \mathbb{F}_2C_p \) plays an important role in this paper and is studied in Section 5, where we obtain a characterization of Mersenne primes in terms of binomial coefficients (see statement 7 in Theorem 1.1). We translate our results into the world of circulant algebras in Section 6. Making use of the connection between determinants, permanents, and perfect matchings, we provide graph theoretic characterizations of Mersenne and 2-rooted primes in Section 7. In the last section we demonstrate how to tie up the various results in this paper to obtain complete proofs of Theorems 1.1 and 1.2.

2. Group algebras

In this section we will prove Theorems 1.4 and 1.5. Let \( R \) be a ring and let \( R^\times \) denote its group of units. If \( R \) is a \( \Delta_n \)-ring (see Section 1 for the definition), then it is automatically a \( \Delta_m \)-ring whenever \( n \) divides \( m \). Call \( R \) a strict \( \Delta_n \)-ring if \( n \) is the smallest positive integer such that \( R \) is a \( \Delta_n \)-ring. Subrings of \( \Delta_n \)-rings are \( \Delta_n \)-rings, and \( R = S \times T \) is a \( \Delta_n \)-ring if and only if \( S \) and \( T \) are each \( \Delta_n \)-rings.

If \( R \) is both a field and a \( \Delta_n \)-ring, we refer to \( R \) as a \( \Delta_n \)-field. Our first lemma characterizes all \( \Delta_p \)-fields for \( p \) a prime.

**Lemma 2.1.** Let \( p \) be prime. A field \( k \) is a \( \Delta_p \)-field if and only if \( k = \mathbb{F}_2 \), \( k = \mathbb{F}_3 \) with \( p = 2 \), or \( k = \mathbb{F}_{p+1} \) with \( p \) a Mersenne prime.

The field \( \mathbb{F}_2 \) is in fact a \( \Delta_1 \)-field and thus automatically a \( \Delta_p \)-field for all primes \( p \). The other fields are strict \( \Delta_p \)-fields.

**Proof.** It is straightforward to verify the ‘if’ direction. For the converse, suppose \( k \) is a \( \Delta_p \)-field. Then all elements of \( k^\times \) satisfy \( x^p = 1 \). This forces \( k \) to be a finite field whose multiplicative group is necessarily cyclic, so either \( |k^\times| = 1 \) or \( |k^\times| = p \). Hence, either \( |k| = 2 \) or \( |k| = p + 1 \). If \( |k| = 2 \), then \( k = \mathbb{F}_2 \). If \( |k| = p + 1 \), then we obtain \( \mathbb{F}_3 \) if \( p = 2 \). If \( p > 2 \), then \( p + 1 \) must be a power of the characteristic of the field, which must be 2 since \( p + 1 \) is even. Thus \( p \) is a Mersenne prime, and the proof is complete. \( \square \)

We next provide a list of group algebras which are \( \Delta_p \)-rings.
Lemma 2.2. Let \( p \) be prime, let \( k \) be a field, and let \( G \) be an elementary abelian \( p \)-group. The group algebra \( kG \) is a \( \Delta_p \)-ring if any of the following conditions are satisfied:

1. \( k = \mathbb{F}_3 \) and \( p = 2 \),
2. \( k = \mathbb{F}_{p+1} \) and \( p \) is a Mersenne prime,
3. \( k = \mathbb{F}_2 \) and \( p \) is a Mersenne prime, or
4. \( k = \mathbb{F}_2 \) and \( p = 2 \).

Proof. First, suppose \( kG \) is a group algebra satisfying any of the first three conditions. Any element \( t \in kG \) is a finite sum \( t = \sum k_i g_i \), where \( k_i \in k \) and \( g_i \in G \). Now,

\[
\begin{align*}
t^{p+1} &= \left( \sum k_i g_i \right)^{p+1} \\
&= \sum k_i^{p+1} g_i^{p+1} \quad (\text{since } p \text{ is a power of char } k) \\
&= \sum k_i^{p+1} g_i \quad (\text{since the exponent of } G \text{ is } 1 \text{ or } p) \\
&= \sum k_i g_i \quad (\text{since } |k| - 1 \text{ divides } p) \\
&= t.
\end{align*}
\]

If \( t \) is a unit, we must have \( t^p = 1 \), so \( kG \) is indeed a \( \Delta_p \)-ring.

Now suppose \( kG = \mathbb{F}_2 G \) and \( p = 2 \). The first step of the above argument now fails; for example, in \( \mathbb{F}_2 C_2 \cong \mathbb{F}_2[x]/(x^2 - 1) \), we have \((1 + x)^3 = 0\). Instead, we argue as follows. Consider the augmentation map \( \epsilon : \mathbb{F}_2 G \to \mathbb{F}_2 \) that sends any element to the sum of its coefficients. Let \( t = \sum k_i g_i \in kG \) be a unit. Since \( \epsilon \) is a \( k \)-algebra homomorphism, \( \epsilon(t) = 1 \). We have

\[
t^2 = \sum k_i^2 g_i^2 = \sum k_i^2 = \sum k_i = \epsilon(t) = 1,
\]

so every unit of \( \mathbb{F}_2 G \) has order 2. This completes the proof. \( \square \)

We are now able to prove Theorems 1.4 and 1.5, which we restate for the convenience of the reader. We state these theorems separately because although a group of exponent 2 must be abelian, a group of exponent \( p > 2 \) need not be abelian, so our result for \( \Delta_2 \)-rings is stronger.

Theorem 2.3. Let \( G \) be a group and let \( k \) be a field. The group algebra \( kG \) satisfies the diagonal property if and only if \( kG \) is either \( \mathbb{F}_2 C_2^r \) or \( \mathbb{F}_3 C_2^r \) for some \( 0 \leq r \leq \infty \).

Proof. By Lemma 2.2, it suffices to prove the ‘only if’ direction of the theorem. Let \( k \) be a field and let \( G \) be a group such that \( kG \) is a \( \Delta_2 \)-ring. Since \( k \) is a subring of \( kG \), it is a \( \Delta_2 \)-field. By Lemma 2.1, \( k = \mathbb{F}_2 \) or \( k = \mathbb{F}_3 \). Since every element of \( G \) is a unit, the order of every element of \( G \) is a divisor of 2. This implies \( G \) is abelian, so \( G \) is an elementary
abelian 2-group. Since any such group is isomorphic to $C_2^r$ for some $r$ with $0 \leq r \leq \infty$, the proof is complete. □

**Theorem 2.4.** Let $G$ be a non-trivial abelian group, let $k$ be a field, and let $p$ be an odd prime. The group algebra $kG$ is a $\Delta_p$-ring if and only if $p$ is a Mersenne prime and $kG$ is either $\mathbb{F}_2C_p^r$ or $\mathbb{F}_{p+1}C_p^r$ for some $0 < r \leq \infty$.

Note that the statement of the theorem requires $G$ to be non-trivial. This is simply to avoid $kG = \mathbb{F}_2$, the unique $\Delta_1$-ring that is also a group algebra, because $\mathbb{F}_2$ is a $\Delta_p$-ring for any prime $p$. All $\Delta_p$-rings appearing in the statement of the theorem are strict.

**Proof.** As in the previous proof, it suffices to prove the ‘only if’ direction. Let $G$ be an abelian group and let $k$ be a field. Again using **Lemma 2.1** and the fact that every element of $G$ is a unit in $kG$, we have that $G$ is a non-trivial elementary abelian $p$-group (hence $G \cong C_p^r$, where $0 < r \leq \infty$), and $k = \mathbb{F}_{p+1}$ with $p$ Mersenne or $k = \mathbb{F}_2$. To complete the proof, we must prove that if $\mathbb{F}_2C_p^r$ is a $\Delta_p$-ring, then $p$ is Mersenne. Since $\mathbb{F}_2C_p$ is a subring of $\mathbb{F}_2C_p^r$, we may without loss of generality assume $r = 1$. The group ring $\mathbb{F}_2C_p$ is isomorphic to $\mathbb{F}_2[x]/(x^p - 1)$ (the isomorphism sends a generator of $C_p$ to $x$). The irreducible factors of $x^p - 1$ are distinct since this polynomial has no factors in common with its derivative $px^{p-1}$ over $\mathbb{F}_2$ (recall that $p > 2$). By the structure theorem for modules over a principal ideal domain, this ring is therefore isomorphic to a product of fields of characteristic 2 (each factor has the form $\mathbb{F}_2[x]/(r(x))$ with $r(x)$ irreducible). At least one such factor must have order greater than 2 since $x^p - 1$ must have at least one non-linear irreducible factor $f(x)$. The corresponding summand $\mathbb{F}_2[x]/(f(x))$ must be a $\Delta_p$-field of order at least 4, so by **Lemma 2.1**, $p$ is a Mersenne prime. □

Although we assume $G$ is abelian in the odd primary case, one may draw a more general conclusion in one direction. For any group $G \neq \{e\}$, if $kG$ is a $\Delta_p$-ring for an odd prime $p$, then $p$ is a Mersenne prime, $k$ is a $\Delta_p$-field, $G$ has exponent $p$, and $kG$ contains $kC_p$ as a $\Delta_p$-subring. This observation, together with **Theorem 2.4**, demonstrates the equivalence of the first four statements of **Theorem 1.1**.

**3. Units in $\mathbb{F}_2C_p$**

With a view toward the study of 2-rooted primes in the next section, we now take a closer look at the structure of units in $\mathbb{F}_2C_p$. We begin with a useful lemma on the factorization of cyclotomic polynomials.

**Lemma 3.1.** Let $p$ be an odd prime. The cyclotomic polynomial

$$
\Phi_p(x) := 1 + x + x^2 + \cdots + x^{p-1}
$$
factors as a product of \((p - 1)/\text{ord}_p(2)\) distinct irreducible polynomials in \(F_2[x]\) of degree \(\text{ord}_p(2)\), where \(\text{ord}_p(2)\) is the smallest positive integer \(t\) such that \(2^t \equiv 1 \mod p\).

This result can be found in [7, p. 556, Exercise 8]. We give a proof here for completeness.

**Proof.** Let \(p(x)\) be an arbitrary irreducible factor of \(\Phi_p(x)\) over \(F_2[x]\) and let \(\alpha\) be a root of \(p(x)\) in \(F_2\). Then we have \(\deg p(x) = \dim_{F_2}[F_2(\alpha) : F_2]\). Since \(\alpha\) is a root of \(p(x)\), it is also a root of \(x^p - 1\), and it is not 1. Therefore \(\alpha\) is a primitive \(p\)th root of 1 in \(F_2\). Let \(n\) be the smallest integer such that \(\alpha\) is contained in \(F_2^n\). Since the multiplicative group of a finite field is cyclic, it follows that \(n\) is the smallest integer such that \(\alpha^{2^n-1} = 1\) in \(F_2\).

On the other hand since \(\alpha\) is also a primitive \(p\)th root of unity, we have \(\alpha^p = 1\) in \(F_2\). Combining the last two facts, we conclude that \(n\) is the smallest positive integer such that \(2^n - 1\) is a multiple of \(p\). That is, \(n\) is precisely the order of \(2\) in \(F_p\). Thus we have

\[
\deg p(x) = \dim_{F_2}[F_2(\alpha) : F_2] = \dim_{F_2}[F_2^n : F_2] = n = \text{ord}_p(2).
\]

Since \(p(x)\) was chosen to be an arbitrary irreducible factor, it follows that every irreducible factor of \(\Phi_p(x)\) has degree \(\text{ord}_p(2)\). Finally, note that all the irreducible factors of \(x^p - 1\), and hence also of \(\Phi_p(x)\), are distinct because \(x^p - 1\) and its derivative \((px^{p-1})\) share no common factors in \(F_2[x]\). □

Recall that there is a ring isomorphism

\[
F_2C_p \cong \frac{F_2[x]}{(x^p - 1)},
\]

where the isomorphism takes a generator of \(C_p\) to \(x\). The polynomial \(x^p - 1\) factors as \((x - 1)\Phi_p(x)\), where \(\Phi_p(x)\) is the cyclotomic polynomial

\[
\Phi_p(x) = 1 + x + x^2 + \cdots x^{p-1}.
\]

Using Lemma 3.1, we can write \(x^p - 1\) in \(F_2[x]\) as

\[
x^p - 1 = (x - 1) \times \prod_{i=1}^{(p-1)/\text{ord}_p(2)} p_i(x),
\]

where the polynomials \(p_i(x)\) are distinct irreducible polynomials of degree \(\text{ord}_p(2)\). By the structure theorem for modules over a PID, we have

\[
\frac{F_2[x]}{(x^p - 1)} \cong \frac{F_2[x]}{(x - 1)} \times \prod_{i=1}^{(p-1)/\text{ord}_p(2)} \frac{F_2[x]}{(p_i(x))}.
\]
Since each $p_i(x)$ is irreducible and has degree $\text{ord}_p(2)$, we have
\[
\frac{\mathbb{F}_2[x]}{(x^{p_i} - 1)} \cong \mathbb{F}_2 \times \prod_{i=1}^{(p-1)/\text{ord}_p(2)} \mathbb{F}_{2^{\text{ord}_p(2)}},
\]
a product of finite fields.

Taking units on both sides of the last isomorphism, we obtain
\[
\left( \frac{\mathbb{F}_2[x]}{(x^{p_i} - 1)} \right)^\times \cong \left( \mathbb{F}_2 \right)^\times \times \prod_{i=1}^{(p-1)/\text{ord}_p(2)} \left( \mathbb{F}_{2^{\text{ord}_p(2)}} \right)^\times.
\]

Since the multiplicative group of a finite field is always a cyclic group, we have the following result.

**Lemma 3.2.** For any odd prime $p$,
\[
(\mathbb{F}_2 C_p)^\times \cong \prod_{i=1}^{(p-1)/\text{ord}_p(2)} C_{2^{\text{ord}_p(2)}-1}.
\]

In particular,
\[
|(\mathbb{F}_2 C_p)^\times| = (2^{\text{ord}_p(2)} - 1)^{(p-1)/\text{ord}_p(2)}.
\]

**Remark 3.3.** The foregoing discussion unfolds nearly identically if one replaces the prime 2 with a prime $q \neq p$. Our decision to only consider the case $q = 2$ is motivated by our particular interest in 2-rooted primes and our desire to connect the present work to graph theory, where the entries of adjacency matrices are elements of $\mathbb{F}_2$.

We now turn our attention to 2-rooted primes.

4. 2-Rooted primes

An odd prime $p$ is said to be 2-rooted if 2 is a primitive root mod $p$. This is equivalent to saying that 2 generates the multiplicative group of $\mathbb{F}_p$. Therefore $p$ is 2-rooted precisely when $\text{ord}_p(2) = p-1$. In this section we will characterize 2-rooted primes by studying the units in $\mathbb{F}_2 C_p$. In particular, we will show that the first four statements of Theorem 1.2 are equivalent.

**Corollary 4.1.** Let $p$ be an odd prime. Then
\[
|(\mathbb{F}_2 C_p)^\times| \leq (2^{p-1} - 1).
\]

Moreover, equality holds if and only if $p$ is 2-rooted.
Note that this shows that statements (1) and (2) in Theorem 1.2 are equivalent.

**Proof.** This follows immediately from Lemma 3.2 and the following more general and elementary fact. If $a$ and $b$ are positive integers such that $a$ divides $b$, then

$$(2^a - 1)^{b/a} \leq 2^b - 1,$$

and equality holds if and only if $a = b$. The corollary follows when we apply this elementary fact to $a = \text{ord}_p(2)$ and $b = p - 1$. □

**Remark 4.2.** One can see this upper bound directly as follows. Consider the augmentation map $\epsilon: \mathbb{F}_2 C_p \rightarrow \mathbb{F}_2$ which sends an element of $\mathbb{F}_2 C_p$ to the sum of its coefficients. The kernel of this map is an $\mathbb{F}_2$ subspace of index 2 in $\mathbb{F}_2 C_p$. Since no element in this kernel can be a unit, we have $|\langle (\mathbb{F}_2 C_p)^\times \rangle| \leq 2^{p-1}$. Moreover, the norm element $\eta = 1 + x + x^2 + \cdots + x^{p-1}$, where $x$ is a generator of $C_p$, is a zero divisor because $\eta(1 - x) = 0$. In particular, $\eta$ is not a unit. Since $p$ is an odd prime, $\eta$ does not belong to the kernel of $\epsilon$. Hence $|\langle (\mathbb{F}_2 C_p)^\times \rangle| \leq 2^{p-1} - 1$.

This remark implies the following corollary which shows the equivalence of statements (1) and (4) in Theorem 1.2.

**Corollary 4.3.** Let $p$ be an odd prime and let $\theta$ be an element of the ring $\mathbb{F}_2 C_p$. If $\theta$ is a unit, then $\epsilon(\theta) \neq 0$ and $\theta \neq \eta$. Moreover, the converse holds precisely when $p$ is 2-rooted.

**Remark 4.4.** Note that these results will allow us to reformulate a special case of Artin’s Conjecture on primitive roots stated in the introduction. For instance, it is natural to ask whether the equality in Corollary 4.1 or the converse of the first statement in Corollary 4.3 will hold for infinitely many primes $p$. These hold if and only if 2 is a primitive root for infinitely many primes $p$, which is a special case of Artin’s Conjecture.

In the next proposition, we analyze the units of order $p$ in $\mathbb{F}_2 C_p$ to obtain another characterization of 2-rooted primes. This characterization is the equivalence of statements (1) and (3) in Theorem 1.2.

**Proposition 4.5.** An odd prime $p$ is 2-rooted precisely when the only units of order $p$ in $\mathbb{F}_2 C_p$ are the non-identity elements of $C_p$.

**Proof.** Recall the structure of units in $\mathbb{F}_2 C_p$:

$$\left(\mathbb{F}_2 C_p\right)^\times \cong \prod_{i=1}^{(p-1)/\text{ord}_p(2)} C_{2^{\text{ord}_p(2)}-1}.$$

Since $p$ divides $2^{\text{ord}_p(2)} - 1$, there is a unique copy of $C_p$ inside $C_{2^{\text{ord}_p(2)}-1}$, and thus a unique elementary abelian $p$-group of rank $(p-1)/\text{ord}_p(2)$ inside $(\mathbb{F}_2 C_p)^\times$. Therefore
the number of units of order $p$ in $\mathbb{F}_2 C_p$ is equal to $p^{(p-1)/\text{ord}_p(2)} - 1$. The only units of order $p$ in $\mathbb{F}_2 C_p$ are the non-identity elements of $C_p$ if and only if

$$p^{(p-1)/\text{ord}_p(2)} - 1 = p - 1.$$  

This equality holds if and only if $p - 1 = \text{ord}_p(2)$, or equivalently when 2 is a primitive root mod $p$. □

What we have seen here is a striking contrast between Mersenne primes and 2-rooted primes. For the former primes, every non-trivial unit of $\mathbb{F}_2 C_p$ is of order $p$; for the latter primes, only the non-identity elements of $C_p$ will have order $p$. This suggests that these two sets of primes are disjoint. More precisely, the following is true.

**Proposition 4.6.** The prime 3 is the only prime which is both Mersenne and 2-rooted.

**Proof.** Let $p$ be a 2-rooted prime. Then $\text{ord}_p(2) = p - 1$ and by Lemma 3.2,

$$(\mathbb{F}_2 C_p)^\times \cong C_{2^{p-1} - 1}.$$  

If $p$ is also Mersenne, then $\mathbb{F}_2 C_p$ is a $\Delta_p$-ring and every unit has order $p$. Since the group of units is cyclic, this forces $2^{p-1} - 1 = p$, and the only prime satisfying this equation is $p = 3$. □

**Remark 4.7.** The above result is often obtained as an easy consequence of the quadratic reciprocity law. Our proof is different and it is relatively more elementary. A noteworthy feature of our approach is that we connect both sets of primes in question (Mersenne and 2-rooted primes) to a common concept, namely the structure of units in $\mathbb{F}_2 C_p$.

5. The element $1 + x + x^2$

Recall that when $p$ is a Mersenne prime, every unit in

$$\mathbb{F}_2 C_p \cong \mathbb{F}_2[x]/(x^p - 1) \cong \mathbb{F}_2 \times \mathbb{F}_2[x]/(\Phi_p(x))$$  

has order $p$. So it is natural to ask for some explicit non-trivial examples. (The non-identity elements of the group $C_p$ are of course trivial examples of units which have order $p$.) To begin, consider the element $x^n + 1 \in \mathbb{F}_2[x]/(\Phi_p(x))$ when $(n, p) = 1$.

**Lemma 5.1.** Let $p$ be an odd prime and let $n$ be a positive integer relatively prime to $p$. The element $x^n + 1$ is a unit in $\mathbb{F}_2[x]/(\Phi_p(x))$. This unit has order $p$ if and only if $p$ is a Mersenne prime.

**Proof.** Let $p$ be an odd prime and let $(n, p) = 1$. If $\alpha$ is a common root of the polynomials $x^n - 1$ and $x^p - 1$ in the algebraic closure of $\mathbb{F}_2$, then $\alpha^p = 1 = \alpha^n$. This forces the
multiplicative order of $\alpha$ to be 1 since $(n, p) = 1$, so $\alpha = 1$ is the only common root. Since $x^n - 1 = (x - 1)\Phi_p(x)$, we obtain that $x^n - 1 = x^n + 1$ is relatively prime to $\Phi_p(x)$ in $\mathbb{F}_2[x]$. Thus, $x^n + 1$ is a unit in $\mathbb{F}_2[x]/(\Phi_p(x))$.

The element $x^n + 1$ has order $p$ in $\mathbb{F}_2[x]/(\Phi_p(x))$ if and only if $(x + 1)\Phi_p(x) = x^p - 1$ divides

$$(x + 1)[(x^n + 1)^p - 1] = \sum_{i=1}^{p} \left( \begin{array}{c} p \\ i \end{array} \right) x^{ni} + \sum_{i=1}^{p} \left( \begin{array}{c} p \\ i \end{array} \right) x^{ni+1}.$$ 

Working modulo $x^p - 1$, we may reduce powers of $x$ modulo $p$ and the resulting coefficients of $1, x, \ldots, x^{p-1}$ must all be zero modulo 2. We therefore obtain, for each degree $0 \leq k \leq p - 1$,

$$\left( \begin{array}{c} n^{-1}k \mod p \\ p \end{array} \right) \equiv \left( \begin{array}{c} n^{-1}k - n^{-1} \mod p \\ p \end{array} \right) \mod 2.$$ 

Taken together, these congruences imply that the binomial coefficients $\left( \begin{array}{c} p \\ 0 \end{array} \right), \ldots, \left( \begin{array}{c} p \\ p-1 \end{array} \right)$ are mutually congruent modulo 2 and therefore all congruent to $\left( \begin{array}{c} p \\ 0 \end{array} \right) = 1$. This last condition is equivalent to $p$ being a Mersenne prime (see [10, Theorem 8.14]). □

The element $x^n + 1$ in the lemma above lifts to the unit $1 + x^n + \Phi_p(x)$ in $\mathbb{F}_2C_p$ (use the isomorphism in equation (5.1) at the beginning of this section to see this), providing an example of a single unit whose order is $p$ if and only if $p$ is a Mersenne prime. In the remainder of this section, we examine another such example, $1 + x + x^2$. It is noteworthy that it is an irreducible polynomial whose degree does not depend on $p$.

**Theorem 5.2.** Let $p > 3$ be a prime and let $x$ be a generator of the cyclic group $C_p$. Then, $(1 + x + x^2)^p = 1$ in $\mathbb{F}_2C_p$ if and only if $p$ is a Mersenne prime.

Though there are other units in $\mathbb{F}_2C_p$ which will have order $p$ precisely when $p$ is Mersenne, the unit $1 + x + x^2$ is the ‘smallest’ example with this property, because $1 + x$ is not a unit and $x$ has order $p$ for any prime. This result is exactly the equivalence of statements (1) and (5) of Theorem 1.1. In this section, we will prove this equivalence by showing that

$$(1) \implies (5) \implies (6) \implies (7) \implies (1)$$

in Theorem 1.1.

Since every unit in $\mathbb{F}_2C_p$ will have order $p$ when $p$ is Mersenne, to establish the ‘if’ part of Theorem 5.2, it is enough to show that $1 + x + x^2$ is a unit in $\mathbb{F}_2[x]/(x^p - 1)$ when $p > 3$. This is indeed the case: when $p > 3$, $\text{ord}_p(2) > 2$, so the degree of every irreducible factor of $\Phi_p(x)$ is greater than 2 by Lemma 3.1. Hence, $1 + x + x^2$ and $\Phi_p(x)$ are relatively prime, and $1 + x + x^2$ is a unit in $\mathbb{F}_2C_p$. 


In remainder of this section, we will prove the converse. That is, we will show that if \( p > 3 \) is a prime and \((1 + x + x^2)^p = 1\) in \(\mathbb{F}_2C_p\), then \( p \) is Mersenne. We will do this by showing \((5) \implies (6) \implies (7) \implies (1)\) in Theorem 1.1.

To this end, we need a formula of Lucas which gives an efficient algorithm for computing the binomial coefficients mod 2, and a characterization of Mersenne primes in terms of binomial coefficients.

**Theorem 5.3 (Lucas).** Let \( m \) and \( n \) be positive integers. Then the binomial coefficients mod 2 can be computed using the formula:

\[
\binom{m}{n} = \prod_{i=0}^{k} \binom{m_i}{n_i} \mod 2
\]

where

\[
m = \sum_{i=0}^{k} m_i 2^i \quad \text{and} \quad n = \sum_{i=0}^{k} n_i 2^i
\]

are the expansions of the integers \( m \) and \( n \) respectively in base 2.

The next proposition can be easily deduced from Lucas’ theorem.

**Proposition 5.4.** [10] Let \( p \) be an odd prime. Then \( p \) is Mersenne if and only if \( \left( \frac{p}{2^m} \right) = 1 \mod 2 \) for all \( m \) such that \( 0 \leq 2^m \leq p \).

The next proposition shows \((5) \implies (6) \implies (7)\) in Theorem 1.1.

**Proposition 5.5.** Let \( p > 3 \) be an odd prime and let \( x \) be a generator for the cyclic group \( C_p \). If \((1 + x + x^2)^p = 1\) in \(\mathbb{F}_2C_p\), then

\[
\binom{p}{j} \equiv \left( \frac{p}{3j \mod p} \right) \mod 2 \quad \text{for} \ 0 \leq j \leq p.
\]

**Proof.** Since \((1 + x + x^2)(1 + x) = 1 + x^3\) in \(\mathbb{F}_2C_p\), raising to the \( p \)th powers on both sides, we get

\[(1 + x + x^2)^p(1 + x)^p = (1 + x^3)^p.\]

Since \((1 + x + x^2)^p = 1\), we have

\[(1 + x)^p = (1 + x^3)^p.\]
Expanding both these expressions using the binomial series, we get
\[
\sum_{i=0}^{p} \binom{p}{i} x^i = \sum_{j=0}^{p} \binom{p}{j} x^{3j}.
\]

This last equation holds in the group algebra \(\mathbb{F}_2 C_p\) where we can equate the coefficients of like powers of \(x\). This gives the desired result: \(\binom{p}{j} \equiv \binom{p}{3j \mod p} \mod 2\) for all \(0 \leq j \leq p\). \(\square\)

We will now show that the condition
\[
\binom{p}{j} \equiv \binom{p}{3j \mod p} \mod 2 \quad \text{for } 0 \leq j \leq p,
\]
implies that \(p\) is Mersenne. To this end, we need the following lemma.

**Lemma 5.6.** Let \(p\) be an odd prime and let \(k\) be a nonnegative integer. Then we have the following.

1. \(\binom{p}{2k} \equiv \binom{p}{2k+1} \mod 2\) for all \(k\).
2. If \(\binom{p}{4k+2} \equiv 1 \mod 2\) then \(\binom{p}{4k} \equiv 1 \mod 2\).

**Proof.** One can easily verify that \((2k+1)\binom{p}{2k+1} = \binom{p}{2k}(p-2k)\). Now, since \(p-2k\) and \(2k+1\) are both odd, it follows that \(\binom{p}{2k+1} \equiv \binom{p}{2k} \mod 2\).

For the second statement, we first verify that
\[
(4k+1)(2k+1)\binom{p}{4k+2} = \binom{p}{4k} \frac{(p-4k)(p-4k-1)}{2}.
\]

Now we note that \((4k+1)(2k+1)\) is odd and \((p-4k)(p-4k-1)\) is even. So we have \(\binom{p}{4k+2} \equiv \binom{p}{4k} \frac{(p-4k)(p-4k-1)}{2} \mod 2\). It is now clear that if \(\binom{p}{4k}\) is even, then so is \(\binom{p}{4k+2}\). \(\square\)

**Proposition 5.7.** Let \(p > 3\) be a prime such that \(\binom{p}{j} \equiv \binom{p}{3j \mod p} \mod 2\) for all \(1 \leq j \leq p-1\). Then \(p\) is Mersenne.

**Proof.** By Proposition 5.4, it is enough to show that \(\binom{p}{2i} \equiv 1 \mod 2\) for all \(i\) such that \(0 \leq 2i \leq p\). We will prove this using induction on \(i\). When \(i = 0\), \(\binom{p}{2i} = \binom{p}{0} = 1 \mod 2\) because \(p\) is odd. When \(i = 1\), \(\binom{p}{2i} \equiv \binom{p}{2} \equiv \binom{p}{3} \equiv \binom{p}{1} \equiv p \equiv 1 \mod 2\). (Here the second congruence follows from part 1 of Lemma 5.6 and the third follows from the given hypothesis.) For the induction step, we assume that \(\binom{p}{2i} \equiv 1 \mod 2\) for all \(i < s\), and we will show that \(\binom{p}{2s} \equiv 1 \mod 2\). Let \(p = \sum_{i=0}^{n} a_i 2^i\) be the base 2 expansions of \(p\). We first claim that all the \(a_i\)'s for \(i < s\) have to be 1. This is so because for \(i\) in this
range, using the induction hypothesis, we have, $1 \equiv \binom{p}{2^s+1} \equiv \binom{a_i}{a_i} \equiv a_i \mod 2$. Since $2^s$ is not a multiple of 3, note that either $2^s + 1$ or $2^s + 2$ has to be a multiple of 3.

**Case 1:** Suppose that $2^s + 1$ is a multiple of 3. Then we can write $2^s + 1 = 3k$ for some $k$ where $k < 2^s$. We let $k = \sum_{i=0}^{s-1} a_i 2^i$ be the base 2 expansions of $k$.

Note that by part 1 of Lemma 5.6, it is enough to show that $\binom{p}{2^s+1} \equiv 1 \mod 2$. Using the given hypothesis, applying Lucas theorem, and the fact that $a_i = 1$ for $i < s$, we get

$$\binom{p}{2^s+1} = \binom{p}{3k} \equiv \binom{p}{k} = \left( \sum_{i=0}^{n} \alpha_i 2^i \right) \cdot \left( \sum_{i=0}^{s-1} a_i 2^i \right) \equiv \prod_{i=1}^{s-1} \alpha_i \equiv \prod_{i=1}^{s} \left( \frac{1}{\alpha_i} \right) \equiv \prod_{1}^{(1)} = 1.$$ 

Hence, $\binom{p}{2^s+1} \equiv 1 \mod 2$.

**Case 2:** Suppose $2^s + 2$ is a multiple of 3. This case is similar to Case 1 except that we now use part 2 of Lemma 5.6. Let $2^s + 2 = 3r$ for some $r$ where $r < 2^s$, and let $r = \sum_{i=0}^{s-1} \beta_i 2^i$ be the base 2 expansion of $r$. As before, working mod 2, we have

$$\binom{p}{2^s+2} = \binom{p}{3r} \equiv \binom{p}{r} = \left( \sum_{i=0}^{n} \alpha_i 2^i \right) \cdot \left( \sum_{i=0}^{s-1} \beta_i 2^i \right) \equiv \prod_{i=1}^{s-1} \alpha_i \equiv \prod_{i=1}^{s} \left( \frac{1}{\beta_i} \right) \equiv \prod_{1}^{(1)} = 1.$$ 

Consequently, $\binom{p}{2^s+2} \equiv 1 \mod 2$. $\square$

This completes the proof of the main theorem of this section.

6. Circulant matrices

An $n \times n$ square matrix $C$ over a field $k$ is circulant if each column of $C$ is obtained by rotating one element down relative to its preceding column. Thus, a circulant matrix is completely determined by specifying the first column $\mathbf{v}$ because all the remaining column vectors are each cyclic permutations of $\mathbf{v}$ with offset equal to the column index. We denote this by $\text{circ}(\mathbf{v})$. The collection of all $n \times n$ circulant matrices over a field $k$ forms a ring, and we denoted by $Cr_n(k)$.

It turns out that the results in this paper can be formulated in terms of circulant matrices. To see this connection, let $x$ be a generator of $C_n$, and consider the natural map

$$\rho: kC_n \longrightarrow Cr_n(k)$$

defined by $\rho(\sum_{i=0}^{n-1} \alpha_i x^i) = \text{circ}(\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1})$.

**Proposition 6.1.** The map $\rho$ establishes an isomorphism between the rings $kC_n$ and $Cr_n(k)$. 
The proof is a straightforward verification, and we leave it to the reader. Under this isomorphism, we have the following dictionary.

(1) Units in $kC_n$ correspond to the invertible matrices.
(2) Group elements correspond to circulant permutation matrices.
(3) The identity element of $kC_n$ corresponds to the identity matrix.
(4) The elements $1 + x, 1 + x^3, 1 + x + x^2$ in $F_2C_n$ correspond respectively to the circulant matrices $\text{circ}(1,1,0,0,\cdots,0)$, $\text{circ}(1,0,0,1,0,\cdots,0)$, and $\text{circ}(1,1,1,0,0,\cdots,0)$.
(5) The norm element $1 + x + x^2 + \cdots + x^{n-1}$ in $kC_n$ corresponds to the $n \times n$ matrix $J$ which consists of all 1’s.

With this dictionary at hand, we can immediately translate our results to the world of circulant matrices.

**Theorem 6.2.** Let $p > 3$ be a prime. Then the following are equivalent.

(1) $p$ is a Mersenne prime.
(8) The group of invertible $p \times p$ circulant matrices over $F_2$ is an elementary abelian $p$-group.
(9) $[\text{circ}(1,1,1,0,0,\cdots,0)]^p = I_p \pmod{2}$.
(10) $[\text{circ}(1,1,0,0,\cdots,0)]^p = [\text{circ}(1,0,0,1,0,\cdots,0)]^p \pmod{2}$.

**Proof.** We consider the isomorphism

$$\rho: F_2C_p \longrightarrow Cr_p(F_2)$$

defined above. Under this isomorphism (which gives the above dictionary), statements (8), (9), and (10) are equivalent respectively to statements (4), (5) and (6) of Theorem 1.1. The latter statements were already shown to be equivalent to statement (1) in Section 3 and Section 5. So we are done. □

We now translate the characterizations of 2-rooted primes in the language of circulant matrices.

**Theorem 6.3.** Let $p$ be an odd prime. Then the following are equivalent.

(1) $p$ is 2-rooted.
(5) There are $2^{p-1} - 1$ invertible circulant matrices of size $p \times p$ over $F_2$.
(6) The only invertible circulant matrices over $F_2$ that have order dividing $p$ are the circulant permutation matrices.
(7) If $A$ is a $p \times p$ circulant matrix over $F_2$ which is not $J$ (matrix with all 1’s) and the vector of all 1’s is not in the null space of $A$, then $A$ is invertible over $F_2$. 
Proof. Once again we use the aforementioned dictionary given by the isomorphism

\[ \rho: \mathbb{F}_2^C \longrightarrow \mathbb{C}_p(\mathbb{F}_2). \]

Under this isomorphism, statements (5), (6) and (7) are equivalent respectively to statements (2), (3) and (4) of Theorem 1.2. To see the equivalence of (4) and (7), observe that an element \( \sum_{i=0}^{p-1} a_i x^i \) in \( \mathbb{F}_2^C \) will not be in the kernel of the augmentation map exactly when \( \sum a_i \) is equal to 1. This is equivalent to saying that the \( p \times 1 \) vector of all 1’s is not in the null space of the circulant matrix \( \text{circ}(a_0, a_1, \cdots, a_{p-1}) \). Statements (2), (3) and (4) of Theorem 1.2 were already shown to be equivalent to (1) in Section 4. So we are done. \( \square \)

7. Bipartite graphs

In this section we will make graph theoretic translations of our results using simple definitions and ideas from graph theory. We use the standard terminology of graphs which can be found in any textbook on graph theory; see [2] for instance.

Given any \( n \times n \) binary matrix (one in which every entry is either a 0 or a 1) \( M = (m_{ij}) \), we can associate to it an \((n, n)\) bipartite graph as follows. Take two sets \( A := \{a_1, a_2, \cdots, a_n\} \) and \( B := \{b_1, b_2, \cdots, b_n\} \). Vertex \( a_i \) is adjacent to \( b_j \) if and only if \( m_{ij} = 1 \). This association clearly establishes a 1-1 correspondence between \( n \times n \) binary matrices and the collection of bipartite graphs on sets \( A \) and \( B \). The matrix corresponding to a graph in this bijection is often called the biadjacency matrix of the graph. A bipartite graph \( G \) is called circulant if its biadjacency matrix is a circulant matrix.

Some algebraic invariants and operations in the world of matrices can be interpreted graph theoretically. Here we will discuss the graph theoretic interpretation of the determinant and matrix multiplication. To do this we need a few definitions.

The permanent of an \( n \times n \) square matrix \( T = (t_{ij}) \) is defined as

\[ \text{perm}(T) = \sum_{\pi \in S_n} t_{1\pi(1)} t_{2\pi(2)} \cdots t_{n\pi(n)}, \]

where \( S_n \) is the set of all permutations of the set \( \{1, 2, 3, \cdots, n\} \). This looks almost like the definition of the determinant. The only difference is that we do not have the extra \( \text{sgn}(\pi) \) in front of each term in the above sum. Therefore, note that when working modulo 2, the two notions are the same. That is,

\[ \text{det}(T) \equiv \text{perm}(T) \mod 2. \]

A matching in a graph \( G \) is a set of edges \( F \subseteq E(G) \) such that no vertex of \( G \) is incident to more than one edge of \( F \). A perfect matching is a matching that will cover all the vertices of \( G \). Matching theory is a rich branch of graph theory and we refer the reader to the excellent book [12] for a wealth of useful information on matchings.
When $M$ is the biadjacency matrix of an $(n, n)$-bipartite graph as explained above, then $\text{perm}(M)$ is equal to the number of perfect matchings in $G$. (This is easy to see. Note that every perfect matching corresponds to a permutation $\pi$ in $S_n$ such that $m_{i\pi(i)} = 1$ for all $i$. Therefore in the formula for the permanent,

$$\text{perm}(M) = \sum_{\pi \in S_n} m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)},$$

a term will be equal to 1 precisely when $\pi$ corresponds to a perfect matching, and will be 0 otherwise.) This gives:

**Lemma 7.1.** Let $G$ be an $(n, n)$ bipartite graph. $G$ has an odd number of perfect matchings if and only if the biadjacency matrix $M$ of $G$ is invertible mod 2.

To explain matrix multiplication for biadjacency matrices graph theoretically, we need one more definition. A pseudopath of length $r$ in an $(n, n)$ bipartite graph $G$ is an ordered sequence $\{e_1, e_2, \cdots, e_r\}$ of $r$ edges in $G$ such that for all $i$ from 1 to $r-1$, the tail of $e_i$ in $B$ and the head of $e_{i+1}$ in $A$ have the same subscript. One can now easily verify that the $(i, j)$th entry in $M^r$ counts the number $s_{ij}(r)$ of pseudopaths of length $r$ in $G$ between $a_i$ and $b_j$.

Let $\mathcal{G}_p$ be the collection of all $(p, p)$ labeled bipartite circulant graphs. It is easy to see that these graphs are regular (i.e., all vertices have the same degree). We now have a natural bijection from $\mathcal{G}_p$ to the ring of $p \times p$ circulant matrices over $\mathbf{F}_2$.

$$\eta: \mathcal{G}_p \rightarrow Cr_p(\mathbf{F}_2),$$

which assigns to each graph in $\mathcal{G}_p$ its biadjacency matrix. Note that this is a well-defined map, which endows $\mathcal{G}_p$ the structure of a unital associative ring. This isomorphism of rings gives the following dictionary in view of the above discussion.

1. Graphs which have an odd number of perfect matchings correspond to invertible matrices.
2. The identity matrix corresponds to the graph of the trivial perfect matching in which $a_i$ is adjacent to $b_i$ for all $i$.
3. Non-identity matrices of order $p$ correspond to graphs which have the property that $s_{ij}(p)$ (the number of pseudopaths between vertex $a_i$ and vertex $b_j$) is equal to $\delta_{ij}$, the Kronecker delta symbol.
4. The matrix $J$ corresponds to the complete bipartite graph.
5. The degree of the graph will be the sum of the entries in any row or column of the biadjacency matrix.
6. Graphs of degree 1 correspond to circulant permutation matrices.
We are now ready to translate our algebraic results into the world of circulant bipartite graphs.

**Proposition 7.2.** There are exactly \( (2^{\text{ord}_p(2)} - 1)^{(p-1)/\text{ord}_p(2)} \) labeled \((p, p)\) bipartite circulant graphs which have an odd number of perfect matchings. Moreover, this collection is naturally equipped with a structure of an abelian group.

**Proof.** Under the isomorphisms \( \eta: G_p \rightarrow Cr_p(\mathbb{F}_2) \) and \( \rho: \mathbb{F}_2 C_p \rightarrow Cr_p(\mathbb{F}_2) \), the collection in question is exactly equal to \((\mathbb{F}_2 C_p)^\times\). This is the abelian group of units in \( \mathbb{F}_2 C_p \) and its structure and order was computed in Section 3. \( \square \)

**Proposition 7.3.** Let \( p > 3 \) be a prime. The \((p, p)\) bipartite graph corresponding to the \( p \times p \) Circulant matrix \( \text{circ}(1, 1, 1, 0 \cdots, 0) \) will have an odd number of perfect matchings.

**Proof.** It is enough to show that the \( p \times p \) matrix \( \text{circ}(1, 1, 1, 0 \cdots, 0) \) is invertible over \( \mathbb{F}_2 \) whenever \( p > 3 \). This is equivalent to showing that the element \( 1 + x + x^2 \) is a unit in \( \mathbb{F}_2 C_p \), where \( x \) is a generator of \( C_p \). We proved this in Section 5. \( \square \)

**Theorem 7.4.** Let \( p > 3 \) be a prime. Then the following are equivalent.

1. \( p \) is a Mersenne
2. Every circulant \((p, p)\) bipartite graph with an odd number of perfect matchings has \( s_{ij}(p) \mod 2 = \delta_{ij} \), where \( s_{ij}(p) \) is the number of pseudopaths between vertex \( a_i \) and vertex \( b_j \), and \( \delta_{ij} \) is the Kronecker delta symbol.
3. The \((p, p)\) bipartite graph corresponding to the \( p \times p \) circulant matrix \( \text{circ}(1, 1, 1, 0, 0, \cdots, 0) \) has \( s_{ij}(p) \mod 2 = \delta_{ij} \).

**Proof.** Using the dictionary given by the map \( \eta \), we see that statements (11) and (12) are equivalent respectively to statements (8) and (9) of Theorem 1.1. The latter were shown to be equivalent to (1) in Section 6. \( \square \)

**Theorem 7.5.** Let \( p \) be an odd prime. Then the following are equivalent.

1. \( p \) is 2-rooted.
2. There are \( 2^{p-1} - 1 \) circulant \((p, p)\) bipartite graphs on labeled vertices with an odd number of perfect matchings.
3. If \( G \) is a circulant \((p, p)\) bipartite graph on labeled vertices with an odd degree and is not a complete bipartite graph, then \( G \) has an odd number of perfect matchings.
4. If \( G \) is a circulant \((p, p)\) bipartite graph on labeled vertices with an odd number of perfect matchings and \( s_{ij}(p) \mod 2 = \delta_{ij} \) for all \( 1 \leq i, j \leq p \), then the degree of \( G \) is 1.
Proof. Using the dictionary given by the map $\eta$ we see that statements (8), (9) and (10) are equivalent respectively to statements (5), (7) and (6) of Theorem 1.2. The latter were shown to be equivalent to (1) in Section 6. \qed

8. Proofs of Theorems 1.1 and 1.2

In this section we will explain how to tie up the various results in this paper to complete the proofs of Theorem 1.1 and Theorem 1.2.

Proof of Theorem 1.1. It was observed at the end of Section 2 that statement (3) is equivalent to statement (2). The following diagram shows how to justify the remaining equivalences in Theorem 1.1.

$$
\begin{align*}
(1) & \iff (2) \\
(1) & \iff (4) \iff (8) \iff (11) \\
(5) & \iff (9) \iff (12) \\
(6) & \iff (10) \\
(1) & \iff (5) \iff (6) \iff (7) \iff (1) \quad \Box
\end{align*}
$$

Proof of Theorem 1.2. The following diagram shows how the 10 statements of Theorem 1.2 are equivalent.

$$
\begin{align*}
(1) & \iff (2) \iff (5) \iff (8) \\
(1) & \iff (3) \iff (6) \iff (10) \\
(1) & \iff (4) \iff (7) \iff (9) \\
\end{align*}
$$

It remains to show that each of these statements imply that $p \equiv 3$ or $5 \mod 8$. Since these statements are all equivalent, it is enough to show that statement (1) implies this condition on $p$. To this end, let $p$ be a 2-rooted prime. It is easy to see that 2 is a quadratic non-residue mod $p$; that is, 2 is not a square mod $p$. (For, if $2 \equiv u^2 \mod p$, then $2^{p-1} = 1$ by Fermat’s little theorem, contradicting the fact that $p$ is 2-rooted.) Using the Legendre symbol, this can be expressed as

$$
\left(\frac{2}{p}\right) = -1.
$$

From the quadratic reciprocity law, we know that this equation holds precisely when $p \equiv 3$ or $5 \mod 8$; see [3]. \qed
Acknowledgments

The first author presented this research in the number theory seminar at UIUC and in the Discrete Mathematics seminar at Illinois State University. We would like to thank the valuable feedback we received from these groups. In particular, we are thankful to Papa Sissokho for pointing out to us the connection between the permanent of a matrix and perfect matchings of a graph. We would also like to thank Pieter Moore, Jan Minac, B. Sury, and Shailesh Tipnis for their interest, sharing their thoughts, and giving us valuable references related to this work. This research was inspired by a graduate course in number theory taught by the first author in the fall of 2013. We would like to thank our graduate student Christina Henry for her help in improving the exposition.

References