On Consecutive Primitive nth Roots of Unity Modulo q

Thomas Brazelton*, Joshua Harrington†, Siddarth Kannan‡, Matthew Litman$^{\upsilon}$

*Department of Mathematics, The Johns Hopkins University, Baltimore MD
†Department of Mathematics, Cedar Crest College, Allentown PA
‡Department of Mathematics, Pomona College, Claremont CA
$^{\upsilon}$Department of Mathematics, The Pennsylvania State University, State College PA

Abstract

Given $n \in \mathbb{N}$, we study the conditions under which a finite field of prime order q will have adjacent elements of multiplicative order n. In particular, we analyze the resultant of the cyclotomic polynomial $\Phi_n(x)$ with $\Phi_n(x+1)$, and exhibit Lucas and Mersenne divisors of this quantity. For each $n \neq 1, 2, 3, 6$, we prove the existence of a prime q_n for which there is an element $\alpha \in \mathbb{Z}_{q_n}$ where α and $\alpha + 1$ both have multiplicative order n. Additionally, we use algebraic norms to set analytic upper bounds on the size and quantity of these primes.

Keywords: finite fields, cyclotomic polynomials, resultants

1. Introduction

For a natural number n, the nth cyclotomic polynomial, denoted $\Phi_n(x)$, is the monic, irreducible polynomial in $\mathbb{Z}[x]$ having precisely the primitive nth roots of unity in the complex plane as its roots. We may consider these polynomials over finite fields; in particular, $\alpha \in \mathbb{Z}_q$ is a root of $\Phi_n(x)$ if and only if α is a primitive nth root of unity in $\mathbb{Z}_q$. We can thus find elements of order n in $\mathbb{Z}_q$ by studying the roots of $\Phi_n(x)$.

It is well known that for prime q, a finite field $\mathbb{Z}_q$ will have a cyclic group of units $\mathbb{Z}_q^\times$. For each divisor m of $|\mathbb{Z}_q^\times| = q - 1$, there is a unique multiplicative subgroup of $\mathbb{Z}_q^\times$ of order m. While the algebraic structure of $\mathbb{Z}_q$ has been fully investigated, the additive gaps between elements of these subgroups have not been well studied. To this end, we are concerned with categorizing the finite fields of prime order in which we can guarantee two generators of the same subgroup are of the form α and $\alpha + 1$. By the properties of the cyclotomic polynomial, such an α exists if and only if $\Phi_n(x)$ and $\Phi_n(x+1)$ share a root in $\mathbb{Z}_q$.

Our main tool for finding shared roots of $\Phi_n(x)$ and $\Phi_n(x+1)$ is through the resultant of these polynomials. The resultant of two polynomials over a field K is defined as the

product of the differences of their roots in the algebraic closure of K:

$$\mathrm{Res}(f,g) \;=\; \prod_{x,y\in\overline{K}:f(x)=g(y)=0}(x-y).$$

Clearly, the resultant of two polynomials over a field K vanishes if and only if they share a root in the algebraic closure of K. We can calculate the resultant of our two polynomials $\Phi_n(x)$ and $\Phi_n(x+1)$ over $\mathbb{Q}$, and observe that if this quantity vanishes modulo q, where q is prime, then $\Phi_n(x)$ and $\Phi_n(x+1)$ share a root in the algebraic closure of $\mathbb{Z}_q$. It is well established that the cyclotomic polynomial $\Phi_n(x)$ splits in $\mathbb{Z}_q[x]$ if and only if $q \equiv 1 \pmod{n}$, so our problem is reduced to finding prime divisors of our resultant which are 1 modulo n. Guaranteeing the existence of these divisors is nontrivial. In this paper, we confirm the existence of such divisors for all $n \neq 1, 2, 3, 6$. Further, we give an upper bound on the size and quantity of these divisors.

The resultant of two cyclotomic polynomials has been studied in detail [7]. Additionally, the resultant of the polynomials $x^n - 1$ and $(-x-1)^n - 1$ has been researched; this resultant is known as the Wendt Binomial Circulant Determinant [4]. However, the resultant of $\Phi_n(x)$ and $\Phi_n(x+1)$ has not been thoroughly investigated. Our study of this resultant will allow us to establish the existence of fields containing two consecutive elements of multiplicative order n.

2. Prime Divisors of the Resultant

Throughout this paper, we let $n \in \mathbb{N}$ unless otherwise stated. Here we denote by Γ_n the resultant of $\Phi_n(x)$ and $\Phi_n(x+1)$, and find prime divisors of Γ_n. By the definition of the resultant, it can be written as

$$\Gamma_n = \prod_{\substack{(\ell,n)=1\\(j,n)=1}} (\zeta_n^\ell - \zeta_n^j + 1),$$

where ζ_n denotes a primitive nth root of unity. We use the fact that $\prod_{(\ell,n)=1} \zeta_n^\ell = 1$ in numerous proofs throughout this paper. The following lemma gives a convenient integer factorization of Γ_n.

Lemma 1. *For $n > 1$, we have*

$$\Gamma_n = \prod_{(j,n)=1} N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^j + 1),$$

where $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ denotes the algebraic norm over the field extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$.

Proof. As stated above,

$$\Gamma_n = \prod_{(\ell,n)=1} \prod_{(j,n)=1} (\zeta_n^\ell - \zeta_n^j + 1),$$

and

$$N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^j + 1) = \prod_{(\ell,n)=1} \zeta_n^\ell - \zeta_n^{\ell j} + 1.$$

The result follows from the fact that the sets $\{\zeta_n^\ell - \zeta_n^{\ell j} + 1 : (\ell, n) = (j, n) = 1\}$ and $\{\zeta_n^\ell - \zeta_n^j + 1 : (\ell, n) = (j, n) = 1\}$ are equal. ■

As the norm of an algebraic integer is a rational integer, the above factorization is in fact an explicit integer factorization of Γ_n.

We now discuss a result which provides us with a connection to the Lucas numbers [5].

Lemma 2 (Konvalina)**.** *Let L_n denote the Lucas number of index n. We have that:*

$$\prod_{\ell=1}^n \zeta_n^{2\ell} + \zeta_n^\ell - 1 = \begin{cases} L_n & n \text{ is odd} \\ L_n - 2 & n \text{ is even} \end{cases}$$

The following proposition gives the existence of Lucas divisors of Γ_p when p is prime.

Proposition 1. *For $p > 3$ prime, the pth Lucas number L_p divides Γ_p twice.*

Proof. We have that

$$\begin{aligned} L_p &= \prod_{\ell=1}^{p} (\zeta_p^{2\ell} + \zeta_p^\ell - 1) = \prod_{\ell=1}^{p-1} \zeta_p^{-\ell}(\zeta_p^{2\ell} + \zeta_p^\ell - 1) \\ &= \prod_{\ell=1}^{p-1} (\zeta_p^\ell - \zeta_p^{-\ell} + 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^{p-1} + 1), \end{aligned}$$

where $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^{p-1} + 1)$ divides the resultant. Observe also that

$$\begin{aligned} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^2 + 1) &= \prod_{\ell=1}^{p-1} (\zeta_p^\ell - \zeta_p^{2\ell} + 1) \\ = \prod_{\ell=1}^{p-1} \zeta_p^{-\ell}(\zeta_p^\ell - \zeta_p^{2\ell} + 1) &= \prod_{\ell=1}^{p-1} (\zeta_p^{-\ell} - \zeta_p^\ell + 1) = L_p. \end{aligned}$$

As both norms appear in the factorization of Γ_p, we have $L_p^2 \mid \Gamma_n$, as desired. ■

The following three lemmas guarantee primitive divisors of Lucas numbers of the form 1 modulo n, which is critical in proving our first theorem. We provide a proof for the first of these lemmas; the remaining two may be found in the literature [2, 6].

Lemma 3. *For all $n > 6$, L_n has a primitive prime divisor.*

Proof. Note the property that $F_{2n} = F_n L_n$, where F_n is the Fibonacci number of index n. By Carmichael's Theorem for Fibonacci numbers, F_n has a primitive prime divisor for all $n > 12$, so our result follows. ■

Lemma 4. *Whenever n is odd, $L_n = 4^t M$, where M is odd, $t = 0, 1$, and the prime factors of M are of the form $10m \pm 1$.*

Lemma 5 (Brillhart, Montgomery, Silverman)**.** *If p is a primitive, odd, prime divisor of L_n then:*

$$\begin{array}{lll} p \equiv \pm 1 \pmod{10} & \Rightarrow & p \equiv 1 \pmod{2n} \\ p \equiv \pm 3 \pmod{10} & \Rightarrow & p \equiv -1 \pmod{2n} \end{array}$$

By the previous three lemmas, whenever $n \geq 7$ is odd, every primitive odd prime divisor p of L_n satisfies $p \equiv 1 \pmod{n}$. We now have the necessary machinery to prove one of the main results of this paper.

Theorem 1. *For every odd $n \geq 5$, there exists a prime $q \equiv 1 \pmod{n}$ such that $q | \Gamma_n$.*

Proof. When $n = 5$, $\Gamma_5 = 121$. Thus we have $11 | \Gamma_5$ and the theorem holds.

We now look at $n \geq 7$. As n is odd, we have by Lemma 4 that $L_n = 4^t M$. We first treat the case where $3 \nmid n$.

If $3 \nmid n$, then L_n is odd, therefore $L_n = M$ where M has divisors as defined in Lemma 5. We now have the following statement:

$$\prod_{(\ell,n)=1} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) \Big| \prod_{\ell=1}^{n} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1).$$

As $\prod_{\ell=1}^{n} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) = L_n = M$, it follows that $\prod_{(\ell,n)=1} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) | M$. Similarly, since

$$N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{n-1} + 1) \Big| \Gamma_n$$

and $\prod_{(\ell,n)=1} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{n-1} + 1)$, it follows that $\prod_{(\ell,n)=1} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) \big| \Gamma_n$.

By Lemma 3, L_n has a primitive prime divisor q, so $q | M$ and therefore $q \equiv 1 \pmod{n}$ by Lemmas 4 and 5. It remains to show that $q | N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{n-1} + 1)$, which would imply that $q | \Gamma_n$, yielding the desired result.

Note that

$$L_n = \prod_{\ell=1}^{n} (\zeta_n^{2\ell} + \zeta_n^{\ell} - 1) = \prod_{d|n} \prod_{(\ell,d)=1} (\zeta_d^{2\ell} + \zeta_d^{\ell} - 1) = \prod_{d|n} N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\zeta_d - \zeta_d^{d-1} + 1).$$

Suppose by way of contradiction that $q \nmid N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{n-1} + 1)$. We would then have that $q | N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\zeta_d - \zeta_d^{d-1} + 1)$ for some $d < n$. This implies that $q | L_d$, which contradicts q being a primitive prime divisor of L_n.

Therefore $q|N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n-\zeta_n^{n-1}+1)$, and thus divides our resultant. Since $q \equiv 1 \pmod{n}$, we have shown our result.

In the case where $3|n$, we have that L_n is even and of the form $4M$. Since each Lucas number for $n > 6$ has a primitive prime divisor, and $2|L_3$, there is some odd primitive prime divisor q of L_n. Clearly $q|M$, so $q \equiv 1 \pmod{n}$ by previous lemmas. By the same argument as above, $q|N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{n-1} + 1)$, and therefore divides the resultant. ■

By Theorem 1, we have that when $n \geq 5$ is odd, there exists at least one prime divisor q of Γ_n which satisfies $q \equiv 1 \pmod{n}$. This guarantees that for each such n, there exists a field $\mathbb{Z}_{q_n}$ with $\alpha \in \mathbb{Z}_{q_n}$ such that both α and $\alpha + 1$ are primitive nth roots of unity. In the case where $n = p$ is prime, we provide a constructive method of determining such primes q. This follows immediately from the next lemma.

Lemma 6 (Daykin, Dresel)**.** *When $p > 3$ is prime, each divisor d of L_p satisfies $d \equiv 1 \pmod{p}$.*

The following corollary follows immediately from Proposition 1 and Lemma 6.

Corollary 1. *For any prime $q|L_p$ where $p > 3$ is prime, there exist two adjacent elements of order p in $\mathbb{Z}_q$.*

The following lemma allows us to prove the existence of the desired prime divisors of Γ_{2n} when n is odd.

Lemma 7. *Whenever n is odd, $\Gamma_{2n} = \Gamma_n$.*

Proof. Apply the observation that

$$\begin{aligned}\operatorname{Res}(\Phi_{2n}(x), \Phi_{2n}(x+1)) &= \operatorname{Res}(\Phi_n(-x), \Phi_n(-x-1)) = \prod_{(\ell,n)=1} \prod_{(j,n)=1} (-\zeta_n^\ell - (-\zeta_n^j - 1)) \\ &= \prod_{(\ell,n)=1} \prod_{(j,n)=1} (-\zeta_n^\ell + \zeta_n^j + 1) = \prod_{(\ell,n)=1} \prod_{(j,n)=1} (\zeta_n^j - (\zeta_n^\ell - 1)) \\ &= \operatorname{Res}(\Phi_n(x), \Phi_n(x+1)).\end{aligned}$$

■

Corollary 2. *For q prime, $\mathbb{Z}_q$ has adjacent elements of odd order n if and only if $\mathbb{Z}_q$ contains adjacent elements of order $2n$.*

Proof. If n and q are odd positive integers larger than 1, then $q \equiv 1 \pmod{n}$ if and only if $q \equiv 1 \pmod{2n}$. The result then follows from the previous lemma. ■

When $n > 3$ is odd, or $n = 2k$ for any odd $k > 3$, we have shown that there exists a prime $q \equiv 1 \pmod{n}$ such that $q|\Gamma_n$. Equivalently for any such n, there exists a field $\mathbb{Z}_q$ containing an element α such that α and $\alpha + 1$ are both of multiplicative order n. Using a different algebraic norm, we now obtain equivalent results for $n \equiv 0 \pmod{4}$. We first establish the following two preliminaries. The first lemma, originally due to Bang [1], has been proven independently many times. The interested reader should see [8] for more in depth discussion.

Lemma 8 (Bang)**.** *For each $n > 6$, the Mersenne number $M_n = 2^n - 1$ has a primitive prime divisor.*

Lemma 9. *If $4|n$, then $\Phi_n(-x) = \Phi_n(x)$.*

Proof. Note that $(\ell, n) \neq 1$ if and only if $(\frac{n}{2} + \ell, n) \neq 1$. Therefore

$$\begin{aligned}\Phi_n(-x) &= \prod_{(\ell,n)=1} (-x - \zeta_n^\ell) = \prod_{(\ell,n)=1} (x + \zeta_n^\ell) \\ &= \prod_{(\ell,n)=1} (x + \zeta_n^{(n/2)+\ell}) = \prod_{(\ell,n)=1} (x - \zeta_n^\ell) = \Phi_n(x).\end{aligned}$$

■

Theorem 2. *For each positive $n \equiv 0 \pmod 4$, there exists a prime $q \equiv 1 \pmod n$ such that $q|\Gamma_n$.*

Proof. One may compute $\Gamma_4 = 5$ to verify that theorem holds in this case. Now suppose $n > 6$, and see that $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{(n/2)+1} + 1)|\Gamma_n$, where

$$\begin{aligned}N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^{(n/2)+1} + 1) &= N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - (-1)\zeta_n + 1) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(2\zeta_n + 1) \\ &= \prod_{(\ell,n)=1} (2\zeta_n^\ell + 1) = \prod_{(\ell,n)=1} -\zeta_n^\ell(-2 - \zeta_n^{-\ell}) \\ &= \prod_{(\ell,n)=1} (-2 - \zeta_n^{-\ell}) = \Phi_n(-2).\end{aligned}$$

As $4|n$, we have by the previous lemma that $\Phi_n(-2) = \Phi_n(2)$, which is the primitive part of the nth Mersenne number (which is guaranteed to exist as $n > 6$). We claim that there exists a prime q dividing $\Phi_n(2)$ which must be 1 modulo n. As $\Phi_n(2)$ is the primitive part of $2^n - 1$, it will have a primitive prime divisor q. It follows that $2^n \equiv 1 \pmod q$, and as q is a primitive prime divisor of $2^n - 1$, we have $2^d \not\equiv 1 \pmod q$ for any $d < n$. This implies that n is the order of 2 modulo q, and thus n divides $|\mathbb{Z}_q^\times| = q - 1$. So $q \equiv 1 \pmod n$ and $q|\Phi_n(2)$, where $\Phi_n(2)|\Gamma_n$. ■

The following corollary summarizes the major results we have obtained in this section.

Corollary 3. *There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.*

Proof. All other cases have been treated in Theorems 1 and 2. One computes $\Gamma_1 = \Gamma_2 = 1$, and $\Gamma_3 = \Gamma_6 = 4$, and it is clear that neither $\Phi_3(x)$ nor $\Phi_6(x)$ has any roots modulo 2. ■

3. Analytic Bounds on Relevant Prime Factors

While we have shown the existence of a necessary prime divisor of Γ_n, one might consider the number of such divisors. That is, given $n \neq 1, 2, 3, 6$, how many fields $\mathbb{Z}_q$ have at least one pair of consecutive elements of multiplicative order n? Clearly the number of such fields must be finite, as Γ_n has only a finite number of prime divisors.

In this section, we set an explicit bound on the number of prime divisors, counted with multiplicity, of Γ_n. In a study of the Wendt Binomial Circulant Determinant, Granville and Powell were able to bound the number of prime divisors of the resultant of $x^m - 1$ and $(-x-1)^m - 1$ for even m [4]. Here we adapt their argument to arrive at a similar bound for Γ_n. First we define some necessary terminology. As is convention, let $\varphi(n)$ denote the Euler totient function. Further, let $\mathfrak{d}_n$ be the number of prime divisors $q \equiv 1 \pmod{n}$ of Γ_n, counted with multiplicity. It is immediately clear that $\mathfrak{d}_n$ is finite, and we have already shown in the previous section that $\mathfrak{d}_n \geq 1$ for $n \neq 1, 2, 3, 6$. To establish a bound on $\mathfrak{d}_n$, we first bound Γ_n.

Lemma 10. *The resultant Γ_n satisfies $|\Gamma_n| \leq 3^{\varphi(n)^2}$.*

Proof. We have

$$|\Gamma_n| = \Big| \prod_{(\ell,n)=1} \prod_{(j,n)=1} (\zeta_n^\ell - \zeta_n^j + 1) \Big| \leq \prod_{(\ell,n)=1} \prod_{(j,n)=1} |\zeta_n^\ell - \zeta_n^j + 1| \leq 3^{\varphi(n)^2}.$$

■

The next corollary follows trivially, and gives a bound on the largest prime whose corresponding field may contain consecutive elements of order n.

Corollary 4. *If $q|\Gamma_n$, then $q \leq 3^{\varphi(n)^2}$.*

We now set a bound on $\mathfrak{d}_n$. Again, this gives a bound on the number of relevant prime divisors when counted with multiplicity.

Proposition 2. *The following bound holds for $\mathfrak{d}_n$:*

$$\mathfrak{d}_n \leq \varphi(n)^2 \frac{\log(3)}{\log(n+1)}.$$

If $n = p$ is prime, we have the refined bound

$$\mathfrak{d}_p \leq (p-1)^2 \frac{\log(3)}{\log(2p+1)}.$$

Proof. If q is a prime divisor of Γ_n such that $q \equiv 1 \pmod{n}$, then $q \geq (n+1)$. Therefore

$$(n+1)^{\mathfrak{d}_n} \leq |\Gamma_n| \leq 3^{\varphi(n)^2}.$$

We then have $\mathfrak{d}_n \log(n+1) \leq \varphi(n)^2 \log(3)$, and $\mathfrak{d}_n \leq \varphi(n)^2 \frac{\log(3)}{\log(n+1)}$. If $n = p$ is prime, then $q \geq 2p+1$, so in this case we have the bound $\mathfrak{d}_p \leq (p-1)^2 \frac{\log(3)}{\log(2p+1)}$. ■

We now let $\mathfrak{d}'_n$ denote the number of unique prime divisors of Γ_n. The following results are useful in order to bound $\mathfrak{d}'_p$ where p is prime.

Lemma 11. *For $p \geq 5$, the element $\zeta_p^2 - \zeta_p + 1$ is a unit in the ring of cyclotomic integers; that is, $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^2 - \zeta_p + 1) = 1$.*

Proof. Note that $(\zeta_p^2 - \zeta_p + 1)(\zeta_p + 1) = \zeta_p^3 + 1$. By rearranging terms, we obtain $(\zeta_p^2 - \zeta_p + 1) = (\zeta_p^3 + 1)/(\zeta_p + 1)$. Direct calculation reveals that $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^3 + 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p + 1)$. The result then follows by the multiplicativity of the norm. ■

Proposition 3. *For prime p, Γ_p is a square.*

Proof. We claim that for $k > 1$, $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^k + 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^{-k+1} + 1)$. Observe that

$$\begin{aligned} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^k + 1) &= \prod_{j=1}^{p-1}(\zeta_p^j - \zeta_p^{jk} + 1) = \prod_{j=1}^{p-1}\zeta_p^j(1 - \zeta_p^{jk-j} + \zeta_p^{-j}) \\ &= \prod_{j=1}^{p-1}(\zeta_p^{-j} - \zeta_p^{-j(1-k)} + 1) = \prod_{j=1}^{p-1}(\zeta_p^j - \zeta_p^{j(1-k)} + 1) \\ &= N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^{-k+1} + 1). \end{aligned}$$

For each $k \neq \frac{p+1}{2}$, the corresponding norm in the integer factorization of Γ_p given in Lemma 1 is paired with an identical value. When $k = \frac{p+1}{2}$, we apply the substitution $\xi = \zeta_p^k$ along with the previous lemma to get

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^k + 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\xi^2 - \xi + 1) = 1.$$

We may conclude that

$$\Gamma_p = \prod_{j=1}^{(p-1)/2} (N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^j + 1))^2.$$

■

The following corollary is an immediate consequence of Propositions 2 and 3.

Corollary 5. *For p prime, we have the following bounds for Γ_p, $\mathfrak{d}'_p$, and for any prime q dividing Γ_p:*

$$|\Gamma_p| \leq 3^{(p-1)(p-3)},\ \mathfrak{d}'_p \leq (p-1)(p-3)\frac{\log(3)}{2\log(2p+1)},\ q \leq 3^{\frac{(p-1)(p-3)}{2}}.$$

Proof. For the first bound, observe

$$|\Gamma_p| = |\prod_{j=1}^{p-1}\prod_{\ell=1}^{p-1}(\zeta_p^\ell - \zeta_p^j + 1)| = \prod_{\substack{2\le j\le p-1\\ j\neq(p+1)/2}}\prod_{\ell=1}^{p-1}|\zeta_p^\ell - \zeta_p^j + 1|$$

$$\le \prod_{\substack{2\le j\le p-1\\ j\neq(p+1)/2}}\prod_{\ell=1}^{p-1} 3 \le 3^{(p-1)(p-3)}.$$

Combining this argument with Propositions 2 and 3 gives the second and third bounds. ∎

These bounds give us some notion as to how many primes may satisfy the necessary properties, that is, the number of fields $\mathbb{Z}_q$ that will have adjacent elements of multiplicative order n. The authors of this paper have further conjectures as to precisely which primes will work; we explore these in the next section.

4. Conclusion and Further Conjectures

We have succeeded in showing that for any $n \neq 1, 2, 3, 6$, we can produce a prime $q > n$ so that there is an element $\alpha \in \mathbb{Z}_q$ where both α and $\alpha + 1$ are primitve nth roots of unity. In fact, in the case where $n = p$ is prime, any prime divisor of L_p, the Lucas number of index p, corresponds with such a field. With a similar analysis, we have also shown that when n is any odd number, there exists a prime q dividing $\Gamma_{2n} = \Gamma_n$ satisfying $q \equiv 1 \pmod{2n}$. This provides a finite field of prime order that has both a pair of consecutive primitive nth roots of unity, and a pair of consecutive primitive $2n$th roots of unity. Finally, in the case where $4|n$, we have shown that modulo a primitive prime divisor q of the nth Mersenne number, we will have consecutive primitive nth roots of unity.

There are many logical follow-up questions to ask regarding the relevant primes. We have shown the existence of at least one prime $q \equiv 1 \pmod{n}$ dividing our resultant, but empirically, the following conjecture seems to be true.

Conjecture 1. *For a prime $p \neq 1, 2, 3, 6$, all primes $q > p$ dividing Γ_p satisfy $q \equiv 1 \pmod{p}$.*

One realizes that this conjecture has an equivalent formulation in elegant, field theoretic language:

Conjecture 2. *Let $p \neq 1, 2, 3, 6$ be a prime, and let q be a prime. Whenever α and $\alpha + 1$ are primitive pth roots of unity in a finite field $\mathbb{F}_{q^r}$ where $q > p$, we have $\alpha \in \mathbb{F}_q$.*

The simplicity of the above statement is intriguing; there is certainly an underlying algebraic structure involved. We will now provide the beginning of an argument towards proving Conjecture 1.

Proposition 4. *When p is prime, $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^j + 1) \equiv 1 \pmod{p}$ for each $1 \leq j \leq p-1$.*

Proof. For each j, $\zeta_p - \zeta_p^j \in \langle 1 - \zeta_p \rangle$, where $\langle 1 - \zeta_p \rangle$ is the ideal generated by $1 - \zeta_p$ in $\mathbb{Z}[\zeta_p]$. For all $1 \leq \ell \leq p-1$, we have that $\zeta_p^\ell - \zeta_p^{\ell j} + 1 = 1$ in $\mathbb{Z}[\zeta_p]/\langle 1 - \zeta_p \rangle$. As $\mathbb{Z}[\zeta_p]/\langle 1 - \zeta_p \rangle \cong \mathbb{Z}_p$, we conclude that $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - \zeta_p^j + 1) \equiv 1 \pmod{p}$. ■

The next result follows immediately.

Corollary 6. *When p is prime, $\Gamma_p \equiv 1 \pmod{p}$.*

The preceding arguments confirm that each of the norms dividing Γ_p is 1 modulo p. However, it is more difficult to reach the same conclusion regarding the prime divisors of the norms.

Another area of interest is the relationship between the multiplicity of a prime divisor q of Γ_n and the behavior of $\Phi_n(x)$ over $\mathbb{Z}_q$. In Proposition 3, we have shown that for all prime p, Γ_p is a perfect square. The authors of this paper observe that the multiplicity of a prime divisor q of Γ_p corresponds with the number of roots that $\Phi_p(x)$ and $\Phi_p(x+1)$ share when taken modulo q. This leads us to our final conjecture.

Conjecture 3. *For p prime, let k be the largest integer such that $q^k | \Gamma_p$ for some prime $q \equiv 1 \pmod{p}$. If $k < \frac{p-1}{2}$, then there exist exactly k distinct elements $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_q$ such that the order of α_i and $\alpha_i + 1$ is p for each $1 \leq i \leq k$. If $k \geq \frac{p-1}{2}$, there are exactly $\frac{p-1}{2}$ distinct elements $\alpha_1, \ldots, \alpha_{\frac{p-1}{2}} \in \mathbb{Z}_q$ such that the order of α_i and $\alpha_i + 1$ is p for each $1 \leq i \leq \frac{p-1}{2}$.*

Acknowledgments
The authors acknowledge the National Science Foundation (grant DMS-1560019) and Muhlenberg College for supporting the REU on which this paper is based. The authors would also like to thank Byungchul Cha, Eugene Fiorini, and James Hammer for their support and guidance. A special mention also needs to be made to Loan's Vietnamese Bistro for all the great pho which made this paper possible.

References

[1] A.S. Bang, *Taltheoretiske Undersgelser*, Tidsskrift for Matematik, vol. 4 (1886) 70-80.

[2] J. Brillhart, P. L. Montgomery, R. D. Silverman, *Tables of Fibonacci and Lucas Factorizations*, Mathematics of Computation, vol. 50 (1988) 251-260.

[3] D. E. Daykin, L. A. G. Dresel, *Factorization of Fibonacci Numbers*, Fibonacci Quarterly, (1970) 23-30.

[4] A. Granville, B. Powell, *On Sophie Germain type criteria for Fermat's Last Theorem*, Acta Arithmetica, (1988) 265-277.

[5] J. Konvalina, *Roots of Unity and Circular Subsets Without Consecutive Elements*, Fibonacci Quarterly, (1994) 412-414.

[6] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, John Wiley and Sons, Inc., New York, 2001, pp. 207.

[7] D. H. Lehmer, *Some Properties of the Cyclotomic Polynomials*, Journal of Mathematical Analysis and Applications, 15 (1966) 105-117.

[8] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996.