On the Irreducibility of $X^q - 1$ in Monoid Rings with Positive Characteristic

R. C. Daileda

December 21, 2021

1 Introduction

Let $\Gamma$ be a commutative monoid, written additively. We say that $\Gamma$ is torsion-free if for every $n \in \mathbb{N}$ and every $\alpha, \beta \in \Gamma$, the equation $n\alpha = n\beta$ implies $\alpha = \beta$. If $\Gamma$ is torsion-free, $\alpha \in \Gamma$ and $n \in \mathbb{N}$, the equation $nx = \alpha$ has at most one solution in $\Gamma$. If $px = \alpha$ has no solution in $\Gamma$ for every prime $p$, the authors of [1] say that $\alpha$ has height $(0, 0, \ldots)$. If this is the case and $n \geq 2$ is an integer, choose any prime $p$ dividing $n$. Then $nx = p(kx)$ for some $k \in \mathbb{N}$. Since $px = \alpha$ has no solution in $\Gamma$, this implies that $nx = \alpha$ doesn’t either. We conclude that $\alpha$ has height $(0, 0, \ldots)$ if and only if for every $n \geq 2$ the equation $nx = \alpha$ has no solution in $\Gamma$. We prefer to term such an $\alpha$ to be indivisible. One advantage of this formulation is that it has a simple positive expression: $\alpha \in \Gamma$ is indivisible if and only if $nx = \alpha$ with $n \in \mathbb{N}$ and $x \in \Gamma$ implies $n = 1$ and $x = \alpha$.

Given an additive monoid $\Gamma$ and a commutative ring $R$, let $R[X; \Gamma]$ denote the monoid ring of all polynomials in $X$ with exponents in $\Gamma$ and coefficients in $R$.

Given $\pi \in \Gamma$, consider the binomial $X^\pi - 1 \in R[X; \Gamma]$. If $\pi = n\alpha$ for some $n \geq 2$ and $\alpha \in \Gamma$, note that we have the factorization

$$X^\pi - 1 = (X^\alpha - 1)^{n-1} X^{n\alpha}.$$  

If $\Gamma$ is torsion-free and cancellative ($\alpha + \beta = \alpha + \gamma$ implies $\beta = \gamma$), neither factor on the right is a unit in $R[X; \Gamma]$, which shows that $X^\pi - 1$ is not irreducible in $R[X; \Gamma]$.

$$\left\{ \begin{array}{l} R[X; \Gamma] \\
\end{array} \right.$$  

We will explain and recompute these factorizations in section 7. For an arbitrary positive (prime) characteristic $p$, we call a prime $q$ exceptional for $p$ if $X^q - 1$ fails to be irreducible in $F_p[X; M]$, and we let $E(p)$ denote the set of primes that are exceptional for $p$. Then $M$ fails to be a Matsuda monoid of type $p$ precisely when $E(p) \neq \emptyset$. Our main result shows that, assuming a suitable generalized Riemann hypothesis (GRH), not only is $E(p)$ always nonempty, it is infinite!

**Theorem 1.** If we assume that for every number field $K$ the Dedekind zeta function $\zeta_K(s)$ satisfies the Riemann hypothesis, then for any prime number $p$ the set $E(p)$ has a subset with positive natural density. In particular, $E(p)$ is infinite (under GRH).  

---

1For a more careful definition and other essential properties of monoid rings, see [3].

2This needs to be checked. I can show that $X^\alpha - 1$ is not a unit if $\alpha \neq 0$, but I’m not sure about the other factor. This is certainly true if $\Gamma$ is a submonoid of $\mathbb{Q}_0^+$, which is the situation in which we will ultimately be interested.
Corollary 1. Assume GRH for Dedekind zeta functions. Then $M = \langle 2, 3 \rangle$ is not a Matsuda monoid of any positive type.

The interested reader may consult [8] or [5] for more on Dedekind zeta functions and the Riemann hypothesis. We recall that if $P$ denotes the set of prime numbers and $S \subseteq P$, then the natural density of $S$ (in $P$) is defined to be

$$d(S) = \lim_{x \to \infty} \frac{\#(S \cap [1, x])}{\#(\mathbb{P} \cap [1, x])},$$

when it exists. Because natural density is the only density we will be working with, we will frequently omit the word “natural” in our discussion and simply refer to “the density” of a particular set of primes. Roughly speaking, $d(S)$ is the proportion of the prime numbers that belong to $S$. Note that if $S$ is finite, then $d(S) = 0$. Therefore if $d(S)$ exists and is nonzero, then $S$ must be infinite:

$$d(S) \neq 0 \implies \#S = \infty.$$

The converse of this implication is false, however, since there are infinite sets of primes with zero density. This means that a set of primes with $d(S) = 0$ may or may not be infinite. Ultimately our goal is to find a nonempty $S \subseteq E(p)$. Although $d(S) = 0$ doesn’t force $S = \emptyset$, this also doesn’t prevent it. So the easiest way to prove that $S \neq \emptyset$ is to prove that $d(S) \neq 0$, since this implies that $S$ is infinite. In other words, the best way to show $S$ has at least one element is to show that $S$ has infinitely many!

The proof of Theorem 1 occupies sections 2 through 6. Treating $\mathbb{F}_p[X; M]$ as a subring of $\mathbb{F}_p[X]$, in section 2 we reverse the order of the coefficients of the factors in a potential factorization of $X^g - 1$, in order to move the “missing” linear terms to a more field-theoretically convenient location. Because the new missing terms can be interpreted using the Galois theory of finite fields, we are led to a very simple condition that guarantees membership in a certain subset $E'(p) \subseteq E(p)$. In section 3 we reinterpret this condition in the context of number fields. In section 4 we partition $E'(p)$ according to the index of $\langle p \rangle$ in $(\mathbb{Z}/q\mathbb{Z})^\times$, and show that $E'(p)$ contains the set

$$E'_2(p) = \{ q \text{ prime} \mid q \equiv \pm 1 \pmod{4p}, \frac{[\langle \mathbb{Z}/q\mathbb{Z} \rangle^\times : \langle p \rangle]}{2} = 2 \}.$$

In section 5 we apply results of Lenstra [7] which show that the density of $E'_2(p)$ exists (under GRH) and is nonzero, proving Theorem 1. In section 6 we explicitly compute the density of $E'_2(p)$. Section 7 includes remarks, examples, and computations.

2 Reversal

Fix a prime $p$. It will be convenient to view $\mathbb{F}_p[X; M]$ as a subring of $\mathbb{F}_p[X]$. Given $f \in \mathbb{F}_p[X]$ we write

$$f(X) = \sum_{j=0}^m a_j X^j$$

with $m = \deg f$, so that $a_m \neq 0$. Define the reversal operator $R : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ by

$$R(f)(X) = \sum_{j=0}^m a_{m-j} X^j.$$

Note that $\deg(R(f)) = \deg f$ if and only if $X \nmid f$, and in this case $R^2(f) = f$. We also have

$$R(f)(X) = X^{\deg f} f \left( \frac{1}{X} \right),$$

which implies that $R$ is multiplicative.

If $m = \deg f \geq 1$, we call $a_{m-1}$ the trace coefficient of $f$, and say that $f$ is traceless if $a_{m-1} = 0$. By definition a traceless polynomial must have positive degree. Let

$$\mathcal{F}_1 = \{ f \in \mathbb{F}_p[X; M] : f \text{ is nonconstant and } X \nmid f \},$$

$$\mathcal{F}_2 = \{ f \in \mathbb{F}_p[X] : f \text{ is traceless and } X \nmid f \}.$$
It is easy to see that \( R : \mathcal{F}_1 \to \mathcal{F}_2 \) is an involution. For any prime \( q \) we have
\[
R(X^q - 1) = 1 - X^q = -(X^q - 1).
\]
Because \( X \nmid X^q - 1 \) and \( R \) is multiplicative, it follows that \( X^q - 1 \) factors in \( \mathcal{F}_1 \) if and only if it factors in \( \mathcal{F}_2 \). This proves:

**Lemma 1.** For any primes \( p \) and \( q \), \( X^q - 1 \) factors nontrivially in \( \mathbb{F}_p[X; M] \) if and only if it factors as the product of traceless polynomials in \( \mathbb{F}_p[X] \).

We now assume that \( q \neq p \). Let
\[
\Phi_q(X) = \sum_{j=0}^{q-1} X^j
\]
denote the \( q \)th cyclotomic polynomial. Suppose \( \Phi_q = fg \) in \( \mathbb{F}_p[X] \) with \( f \) traceless. Multiplying by \( X - 1 \) we obtain \( X^q - 1 = f \bar{g} \). Because \( X^q - 1 \) and \( f \) are both traceless, so is \( \bar{g} \). Applying Lemma 1 we conclude that if \( \Phi_q \) has a traceless factor in \( \mathbb{F}_p[X] \), then \( X^q - 1 \) factors nontrivially in \( \mathbb{F}_p[X; M] \).

Let \( f \) be the order of the subgroup generated by \( p \) in \( (\mathbb{Z}/q\mathbb{Z})^\times \). It is well known that in \( \mathbb{F}_p[X] \) the polynomial \( \Phi_q \) has \( r \) distinct irreducible factors, each of degree \( f \). Therefore if \( \zeta \neq 1 \) is any \( q \)th root unity over \( \mathbb{F}_p \), then \( [\mathbb{F}_p(\zeta) : \mathbb{F}_p] = f \). Moreover, \( \mathbb{F}_p(\zeta)/\mathbb{F}_p \) is a Galois extension, with group generated by the Frobenius automorphism \( \alpha \mapsto \alpha^p \). It follows that if \( m(X) \in \mathbb{F}_p[X] \) is the minimal polynomial for \( \zeta \) over \( \mathbb{F}_p \), then
\[
m(X) = \prod_{j=0}^{f-1} (X - \zeta^{p^j}) = X^f - \left( \sum_{j=0}^{f-1} \zeta^{p^j} \right) X^{f-1} - \cdots.
\]
We therefore see that \( m(X) \) is traceless if and only if \( \zeta \) is a root of the trace polynomial
\[
T_q(X) = \sum_{j=0}^{f-1} X^{p^j}.
\]
Since \( m|\Phi_q \), we arrive at:

**Lemma 2.** For any primes \( p \neq q \), if \( \gcd(\Phi_q, T_q) \) is nontrivial in \( \mathbb{F}_p[X] \), then \( X^q - 1 \) factors nontrivially in \( \mathbb{F}_p[X; M] \).

**Proof.** If \( \Phi_q \) and \( T_q \) have a nontrivial common factor in \( \mathbb{F}_p[X] \), then they have a common root \( \zeta \) over \( \mathbb{F}_p \). The result follows from the discussion above. \( \square \)

## 3 Number Fields

The condition that \( \Phi_q \) and \( T_q \) have a nontrivial common factor over \( \mathbb{F}_p \) is equivalent to the statement that \( T_q \) fails to be a unit in \( \mathbb{F}_p[X]/(\Phi_q) \). To understand this condition we introduce a little algebraic number theory. Let \( \zeta_q \in \mathbb{C} \) denote a primitive \( q \)th root of unity and set \( K_q = \mathbb{Q}(\zeta_q) \). Let \( \mathcal{O}_q = \mathbb{Z}[\zeta_q] \) denote the ring of integers in \( K_q \). Because \( \Phi_q \) is the minimal polynomial of \( \zeta_q \) over \( \mathbb{Q} \), we have natural isomorphisms
\[
\mathbb{F}_p[X]/(\Phi_q) \cong (\mathbb{Z}/p\mathbb{Z}[X])/((\Phi_q)) \cong \mathbb{Z}[X]/(p, \Phi_q) \cong (\mathbb{Z}[X]/(\Phi_q))/\langle p \rangle \cong \mathcal{O}_q/\langle p \rangle,
\]
under which (the coset of) \( X \) corresponds to \( \zeta_q \). We immediately find that \( T_q \) is not a unit in \( \mathbb{F}_p[X]/(\Phi_q) \) if and only if \( \alpha_q = T_q(\zeta_q) \) is divisible by one of the primes of \( \mathcal{O}_q \) lying over \( p \). This occurs if and only if \( p \) divides the (ideal) norm \( N_q(\alpha_q) = |\mathcal{O}_q/\alpha_q\mathcal{O}_q| \).

We can go a bit further if we introduce some Galois theory. The extension \( K_q/\mathbb{Q} \) is Galois with group isomorphic to \( (\mathbb{Z}/q\mathbb{Z})^\times \). Explicitly, an element \( a \in (\mathbb{Z}/q\mathbb{Z})^\times \) corresponds to the automorphism induced

\[\text{Is the converse true? If not, can I produce a counterexample?}\]
by $\zeta_q \mapsto \zeta_q^a$. If $a_1, \ldots, a_r$ are coset representatives for $\langle p \rangle$ in $(\mathbb{Z}/q\mathbb{Z})^\times$, then the $T_q(\zeta_q^a)$ are the distinct conjugates of $\alpha_q$ over $\mathbb{Q}$. It follows that

$$m_q(X) = \prod_{i=1}^{r} (X - T_q(\zeta_q^a)) \in \mathbb{Z}[X]$$

is the minimal polynomial for $\alpha_q$ over $\mathbb{Q}$ (the coefficients are integral because $\alpha_q$ is an algebraic integer). Up to a sign, the constant coefficient of $m_q(X)$ is equal to the (algebraic) norm

$$N_q(\alpha_q) = \prod_{i=1}^{r} T_q(\zeta_q^a).$$

Because $[K_q : \mathbb{Q}(\alpha_q)] = \frac{q-1}{r} = f$, the two notions of norm are related by the equation

$$N_q(\alpha_q \mathcal{O}_q) = N_q(\alpha_q)^f.$$

This means that $p$ divides $N_q(\alpha_q \mathcal{O}_q)$ if and only if $p$ divides $N_q(\alpha_q)$. The preceding paragraph and Lemma 2 now yield:

**Lemma 3.** For any primes $p \neq q$, if $p|N_q(\alpha_q)$, then $X^q - 1$ factors nontrivially in $\mathbb{F}_p[X; M]$.

### 4 The Index

Recall that $E(p)$ is the set of all primes $q$ so that $X^q - 1$ factors nontrivially in $\mathbb{F}_p[X; M]$. If we let

$$E'(p) = \{ q \mid q \text{ is prime, } q \neq p, p|N_q(\alpha_q) \},$$

then Lemma 3 shows that $E'(p) \subseteq E(p)$\(^4\) To further study $E'(p)$, for each $k \in \mathbb{N}$ let

$$E'_k(p) = \left\{ q \in E'(p) \mid q \equiv 1 \pmod{k}, f = \frac{q-1}{k} \right\},$$

which is just the set of primes in $E'(p)$ for which the index

$$r = \frac{q-1}{f} = |(\mathbb{Z}/q\mathbb{Z})^\times : \langle p \rangle| = |\mathbb{Q}(\alpha_q) : \mathbb{Q}|$$

is equal to $k$. For these primes $\alpha_q$ has degree $k$ over $\mathbb{Q}$. This makes $N_q(\alpha_q)$ difficult to describe explicitly in general, but when $k = 2$ things simplify somewhat. If $q \in E'_2(p)$, then $\alpha_q$ has a single distinct Galois conjugate $\beta_q$ and

$$\alpha_q + \beta_q = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^a = -1, \quad (1)$$

since $\Phi_q(\zeta_q) = 0$.

Equation (1) has two important consequences. Because $\mathcal{O}_q = \mathbb{Z}[\zeta_q]$ and $\mathbb{Q}(\alpha_q) = K_q^{(p)}$, it is not hard to show that the ring of integers in $\mathbb{Q}(\alpha_q) = \mathbb{Q}(\alpha_q, \beta_q)$ is $\mathbb{Z}[\alpha_q, \beta_q] = \mathbb{Z}[\alpha_q]$, by (1). This means that $\text{disc}(\mathbb{Q}(\alpha_q)) = \text{disc}(\alpha_q)$\(^5\). Furthermore, the minimal polynomial for $\alpha_q$ over $\mathbb{Q}$ is

$$m_q(X) = (X - \alpha_q)(X - \beta_q) = X^2 + X + N_q(\alpha_q),$$

which means that

$$\text{disc}(\alpha_q) = \text{disc}(X^2 + X + N_q(\alpha_q)) = 1 - 4N_q(\alpha_q).$$

---

\(^4\)I suspect the two sets are actually the same, but I have no real evidence one way or the other. This merits further investigation.

\(^5\)In general the discriminants differ by a factor of $[\mathbb{Z}[T_q(\zeta_q^a)]] : [\mathbb{Z}[\alpha_q]]^2$, which is a source of difficulty.
For odd $q$, the unique quadratic subfield of $K_q$ is known to be $\mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{\frac{q-1}{2}} q$. Since $\mathbb{Q}(\alpha_q)$ also has degree 2 over $\mathbb{Q}$, we must have $\mathbb{Q}(\sqrt{q^*}) = \mathbb{Q}(\alpha_q)$. In particular

$$q^* = \text{disc } \mathbb{Q}(\sqrt{q^*}) = \text{disc } \mathbb{Q}(\alpha_q) = \text{disc}(\alpha_q) = 1 - 4N_q(\alpha_q).$$

Therefore $p|N_q(\alpha_q)$ if and only if $q^* \equiv 1 \pmod{4p}$. For odd $p$ this congruence is equivalent to system $q^* \equiv 1 \pmod{4}$ and $q^* \equiv 1 \pmod{p}$, by the Chinese remainder theorem. The condition $q^* \equiv 1 \pmod{4}$ is automatic, while $q^* \equiv 1 \pmod{p}$ is equivalent to

$$q \equiv \pm 1 \pmod{4p}.$$ (2)

Since (2) holds when $p = 2$ as well, we have proven:

**Lemma 4.** For any prime $p$, $E(p)$ contains the set

$$E'_2(p) = \left\{ q \text{ prime} \mid q \equiv \pm 1 \pmod{4p}, f = \frac{q-1}{2} \right\}.$$

We remark that for odd $p$, $E'_2(p)$ consists of the primes $q \equiv \pm 1 \pmod{4p}$ for which $\langle p \rangle$ has index 2 in $(\mathbb{Z}/q\mathbb{Z})^\times$. Notice that the condition $f = \frac{q-1}{2}$ implies

$$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \equiv 1 \pmod{q},$$

where $\left(\frac{p}{q}\right)$ is the Legendre symbol. When $p = 2$, quadratic reciprocity tells us that this is equivalent to $q \equiv \pm 1 \pmod{8}$. It follows that

$$E'_2(2) = \left\{ q \text{ prime} \mid f = \frac{q-1}{2} \right\},$$ (3)

so that $E'_2(2)$ actually contains all primes $q$ for which (2) has index 2 in $(\mathbb{Z}/q\mathbb{Z})^\times$.

### 5 $E'_2(p)$ and a generalized Artin conjecture

To prove that $E'_2(p)$ has positive density we will make use of a generalization of Artin’s primitive root conjecture due to Lenstra [7], which we formulate as follows. Given a prime number $q$ and an integer $n$, let $\nu_q^\times : \mathbb{Q} \to \mathbb{Z}$ denote the $q$-adic valuation (with $\nu_q(0) = \infty$), and let

$$R_q = \{ a \in \mathbb{Q} \mid \nu_q(a) \geq 0 \} \quad \text{and} \quad R_q^\times = \{ a \in \mathbb{Q} \mid \nu_q(a) = 0 \}$$

be the valuation ring and unit group at $q$, respectively. There is a natural surjection $\psi : R_q^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$ obtained by composing reduction modulo $qR_q$ with the isomorphism $R_q/qR_q \cong \mathbb{Z}/q\mathbb{Z}$. For a subgroup $W \subseteq R_q^\times$, we let $r_q(W)$ denote the index of $\psi(W)$ in $(\mathbb{Z}/q\mathbb{Z})^\times$.

If $F$ is a finite Galois extension of $\mathbb{Q}$, $C \subseteq G(F/\mathbb{Q})$ is a union of conjugacy classes, $W$ is finitely generated with positive rank, and $k$ is a positive integer, let $\mathcal{S}(F, C, W, k)$ denote the set of primes $q$ so that

$$\left(\frac{F/\mathbb{Q}}{q}\right) \subseteq C, \quad W \subseteq R_q^\times, \quad \text{and} \quad r_q(W)|k,$$

where $\left(\frac{F/\mathbb{Q}}{q}\right)$ is the Frobenius symbol. [7] Conjecture (2.3)] asserts that the natural density of $\mathcal{S}(F, C, W, k)$ exist and is equal to (see [7] (2.15))

$$\delta(F, C, W, k) = \sum_n \frac{\mu(n)c(n)}{|F\cdot L_n : \mathbb{Q}|},$$ (4)

where for squarefree $n$, $L_n = \mathbb{Q}(\zeta_{q(n)}, W^{1/q(n)})$ with $q(n) = \prod_{d|n} p^{\nu_r(k)+1}$, and $c(n) = \#(C \cap G(F/F \cap L_n))$.

[7] Theorem (3.1)] tells us that Lenstra’s conjecture is true, provided we assume the Dedekind zeta function of any number field obeys the Riemann hypothesis (an assumption we hereafter abbreviate as GRH). The question of whether or not $\delta(F, C, W, k) = 0$ must be addressed separately, however. Let $h$ be

---

6Lenstra actually allows $\mathbb{Q}$ to be replaced by any so-called global field $K$. $K = \mathbb{Q}$ is sufficient for our purposes.

7As Lenstra notes [7 p. 203], we are free to use natural density in place of Dirichlet density.

8A somewhat weaker GRH is sufficient, but it would be irritating to state it carefully. See [7].
the product of the primes \( \ell \) so that \( W \subseteq \mathbb{Q}^{ \times q(t)} \). By [7, Theorem (4.1)]\(^9\) \( \delta(F,C,W,k) \neq 0 \) if and only if there is a \( \sigma \in G(F(\zeta_h)/\mathbb{Q}) \) so that

\[
\sigma|F \in C, \quad \sigma|L_\ell \neq \text{id whenever } L_\ell \subset F(\zeta_h). \quad (5)
\]

Set \( F = \mathbb{Q}(\zeta_{4p}) \). For each \( a \in (\mathbb{Z}/4p\mathbb{Z})^\times \) the rule \( \zeta_{4p} \mapsto \zeta_{4p}^a \) defines a unique automorphism \( \sigma_a \in G(F/\mathbb{Q}) \), and the association \( a \mapsto \sigma_a \) is an isomorphism. We claim that

\[
E_2'(p) = S(F, \{ \pm 1 \}, \langle p \rangle, 2). \quad (7)
\]

Since \( \left( \frac{F/q}{q} \right) = \{ q \} \) and \( r_q(\langle p \rangle) = \frac{q-1}{2} \), the only question is why membership in \( S(F, \{ \pm 1 \}, \langle p \rangle, 2) \) guarantees that \( \frac{q-1}{2} \) is divisible by 2. To that end, let \( q \in S(F, \{ \pm 1 \}, \langle p \rangle, 2) \). If \( p = 2 \), then \( q \equiv \pm 1 \pmod{2} \), so that \( \left( \frac{2}{q} \right) = 1 \). If \( p \) is odd, then \( q^* \equiv 1 \pmod{p} \), and quadratic reciprocity gives

\[
\left( \frac{p}{q} \right) = \left( \frac{q^*}{p} \right) = 1.
\]

In either case we conclude that \( \langle p \rangle \) is a subgroup of the group of squares in \( (\mathbb{Z}/q\mathbb{Z})^\times \). Because the squares have index 2 in \( (\mathbb{Z}/q\mathbb{Z})^\times \), this implies \( \frac{q-1}{2} \) is divisible by 2. But we also have that \( r_q(\langle p \rangle) \) divides 2. Since \( r_q(\langle p \rangle) = \frac{q-1}{2} \), we are finished.

It immediately follows from [7] and [7, Theorem (3.1)] that GRH implies \( E_2'(p) \) has natural density

\[
a(p) = \delta(\mathbb{Q}(\zeta_{4p}), \{ \pm 1 \}, \langle p \rangle, 2),
\]

given by [4]. It remains to show that \( a(p) \neq 0 \). When \( p = 2 \) this is immediate from [7, p. 216]. When \( p \) is odd, \( h = 1 \) since \( p \) is not an \( m \)th power in \( \mathbb{Q} \) for any \( m \geq 2 \). So \( F(\zeta_h) = F \) and from [5] and [6] we find that \( a(p) \neq 0 \) if and only if there is a \( \sigma \in \{ \pm 1 \} \) so that

\[
\sigma|L_\ell \neq \text{id whenever } L_\ell \subseteq F. \quad (8)
\]

However, \( L_\ell \) contains the subextension \( \mathbb{Q}(p^{1/\ell}) \) \( (\mathbb{Q}(p^{1/\ell}) \) when \( \ell = 2 \), which fails to be Galois over \( \mathbb{Q} \). Since \( F/\mathbb{Q} \) is abelian, this implies \( L_\ell \) is never contained in \( F \). So [8] is vacuously satisfied for any \( \sigma \in G(F/\mathbb{Q}) \), and hence \( a(p) \neq 0 \). This proves Theorem 1.

6 The Density of \( E_2'(p) \)

We can also show that \( a(p) \) is nonzero directly, by expressing it as the product of a certain nonzero rational number and Artin’s constant,

\[
A = \prod_{\ell \text{ prime}} \left( 1 - \frac{1}{\ell(\ell-1)} \right) = 0.37395 \ldots \quad (9)
\]

In [8] Wagstaff obtained similar results for the densities of the sets

\[
S(a, t) = \{ q \text{ prime} \mid \langle a \rangle \text{ has index } t \text{ in } (\mathbb{Z}/q\mathbb{Z})^\times \},
\]

which are also amenable to Lenstra’s technique. Notice that \( E_2'(p) \neq S(p, 2) \) (when \( p \neq 2 \)), since in \( S(p, 2) \) one has no control over the residue classes of its members. However, equation [8] shows that \( E_2'(2) = S(2, 2) \), and [8, Theorem 2.2] then implies that \( a(2) = \frac{3}{4}A \). In general we have:

**Lemma 5.** For any odd prime \( p \),

\[
a(p) = \frac{3(2p-1)}{4(p^2-p-1)} A, \quad (10)
\]

and \( a(2) = \frac{3}{4}A \).

\(^9\)Be aware that Lenstra’s \( p \) is the characteristic of \( K \), which in our case is zero.
Proof. Suppose \( p \) is odd. With \( F = \mathbb{Q}(\zeta_{4p}) \), \( C = \{ \pm 1 \} \), \( W = \langle p \rangle \) and \( k = 2 \) in section 5, we have
\[
L_n = \begin{cases} \mathbb{Q}(\zeta_n, p^{1/n}) & \text{if } 2 \nmid n, \\ \mathbb{Q}(\zeta_{2n}, p^{1/2n}) & \text{otherwise,} \end{cases}
\]
so that
\[
c(n) = \begin{cases} 2 & \text{if } F \cap L_n \subseteq \mathbb{R}, \\ 1 & \text{otherwise} \end{cases} = \begin{cases} 2 & \text{if } (2p, n) = 1, \\ 1 & \text{otherwise.} \end{cases}
\]
Taking advantage of [6, Theorem VI.9.4] we also find that
\[
[F : L_n : \mathbb{Q}] = \begin{cases} 2n\varphi(n)(p - 1) & (p, n) = 1, \\ 2n\varphi(n) & p | n \text{ and } 2 \nmid n, \\ 4n\varphi(n) & 2p | n. \end{cases}
\]
It then follows from (4) that
\[
a(p) = \frac{1}{2} \sum_{n} \frac{\mu(n)}{n\varphi(n)} + \frac{1}{4} \sum_{p|n} \frac{\mu(n)}{n\varphi(n)} + \frac{1}{2(p - 1)} \sum_{p|n} \frac{\mu(n)}{n\varphi(n)} + \frac{1}{p - 1} \sum_{(2p, n) = 1} \frac{\mu(n)}{n\varphi(n)}.
\]
Because \( \mu \) is multiplicative,
\[
\sum_{(2p, n) = 1} \frac{\mu(n)}{n\varphi(n)} = \prod_{\ell \text{ prime}, \ell \neq 2, p} \left( 1 - \frac{1}{\ell(\ell - 1)} \right) = 2 \frac{p(p - 1)}{p^2 - p - 1} A.
\]
Therefore
\[
\frac{1}{2} \sum_{n} \frac{\mu(n)}{n\varphi(n)} = \frac{1}{2} \sum_{(2p, n) = 1} \frac{\mu(mp)}{mp\varphi(mp)} = - \frac{1}{p(p - 1)} \frac{p(p - 1)}{p^2 - p - 1} A = - \frac{1}{p^2 - p - 1} A.
\]
Likewise
\[
\frac{1}{4} \sum_{p|n} \frac{\mu(n)}{n\varphi(n)} = \frac{1}{4} \sum_{(2p, m) = 1} \frac{\mu(2pm)}{2pm\varphi(2pm)} = \frac{1}{4p(p - 1)} \frac{p(p - 1)}{p^2 - p - 1} A = \frac{1}{4(p^2 - p - 1)} A.
\]
Finally,
\[
\frac{1}{2(p - 1)} \sum_{p|n} \frac{\mu(n)}{n\varphi(n)} = \frac{1}{2(p - 1)} \sum_{(2p, m) = 1} \frac{\mu(2m)}{2m\varphi(2m)} = - \frac{1}{2(p - 1)} \frac{p(p - 1)}{p^2 - p - 1} A = - \frac{p}{2(p^2 - p - 1)} A.
\]
Formula (10) follows immediately. The computation of \( a(2) \) is similar but is simplified somewhat by the fact that in this case \( [F : L_n : \mathbb{Q}] = 4n\varphi(n) \) for all \( n \). As noted above, the value for \( a(2) \) also follows from [9, Theorem 2.2]. \( \square \)

7 Remarks

Given a prime \( q \), if we use the Euclidean algorithm to compute \( (\Phi_q, T_q) \), we can use Lemma 2 to effectively determine whether or not \( q \) belongs to \( E'(p) \), and to factor \( X^q - 1 \) in \( \mathbb{F}_p[X; M] \) when it does. The only potential difficulty is that \( \deg T_q = p^{j-1} \) can be prohibitively large. However, notice that \( X^q \equiv 1 \pmod{\Phi_q} \). This implies
\[
T_q \equiv \sum_{j=0}^{f-1} X^{p^j \pmod{q}} \pmod{\Phi_q}.
\]
Therefore \( \gcd(\Phi_q, T_q) = \gcd(\Phi_q, \overline{T_q}) \). Since the degrees of \( \Phi_q \) and \( \overline{T_q} \) don’t exceed \( q \), the number of steps required by the Euclidean algorithm to compute \( \gcd(\Phi_q, \overline{T_q}) \) is polynomial in \( q \). So we have an efficient way to computationally determine membership in \( E'(p) \).

For example, when \( p = 2 \) we find that

\[
E'(2) = \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97, 103, 109, 113, 127, 137, 151, 157, 167, 191, 193, 199, \ldots \},
\]

\[
E'_2(2) = \{7, 17, 23, 41, 47, 71, 79, 97, 103, 137, 167, 191, 193, 199, \ldots \}.
\]

Notice that \( q = 7 \) is the least member of \( E'(2) \). Over \( \mathbb{F}_2 \) we have

\[
(\Phi_7, T_7) = X^3 + X + 1.
\]

Long division in \( \mathbb{F}_2[X] \) yields

\[
X^7 - 1 = (X^3 + X + 1)(X^4 + X^2 + X + 1).
\]

Applying the reversal operator \( R \) we find that

\[
X^7 - 1 = -R(X^7 - 1) = R(X^3 + X + 1)R(X^4 + X^2 + X + 1)
\]

\[
= (X^3 + X^2 + 1)(X^4 + X^3 + X^2 + 1)
\]

is a factorization of \( X^7 - 1 \) in \( \mathbb{F}_2[X; M] \). This is the factorization given in [1].

When \( p = 3 \) we have

\[
E'(3) = \{11, 13, 23, 37, 41, 47, 59, 61, 71, 73, 83, 97, 107, 109, 131, 157, 167, 179, 181, 191, 193, \ldots \},
\]

\[
E'_2(3) = \{11, 23, 37, 47, 59, 71, 83, 97, 107, 131, 157, 167, 179, 191, \ldots \}.
\]

Applying the same procedure to \( q = 11 \), in \( \mathbb{F}_3[X] \) we find that

\[
(\Phi_{11}, T_{11}) = X^5 + 2X^3 + X^2 + 2X + 2
\]

and

\[
X^{11} - 1 = (X^5 + 2X^3 + X^2 + 2X + 2)(X^6 + X^4 + 2X^3 + 2X^2 + 2X + 1).
\]

Reversing coefficients and negating, we have

\[
X^{11} - 1 = (X^5 + X^4 + 2X^3 + X^2 + 2)(X^6 + 2X^5 + 2X^4 + 2X^3 + X^2 + 1)
\]

in \( \mathbb{F}_3[X; M] \), as in [1].

Membership in \( E(p) \) in general appears to be a more difficult question. It would be interesting to know by how much (if at all) \( E'(p) \) and \( E(p) \) differ. It would also be interesting to determine the densities of the sets \( E_k'(p) \) for \( k \geq 3 \). Computational evidence suggests that the density exists for each \( k \geq 2 \), but we have only been able to treat the case \( k = 2 \) thus far. The overall density of \( E'(p) \) would also be nice to know.

Finally, we remark that empirical evidence supports the GRH-conditional result

\[
d(E'_2(p)) = a(p).
\]

Table [1] compares the approximate density \( #(E'_2(p) \cap [1, 10^6])/#(\mathcal{P} \cap [1, 10^6]) \) to \( a(p) \), for the first ten values of \( p \). It is interesting to note that for \( p < 100 \), the percentage error in the approximate density is substantially larger for \( p = 3 \) than it is for other primes. This appears to persist as we increase the size of the primes included in the approximation. It might be interesting to know the source of this phenomenon.

So where is the Riemann hypothesis, exactly? It’s buried a bit. Lenstra’s [7, Theorem (3.1)] is a consequence of Cooke and Weinberger’s [2, Theorem 1.1], which gives an asymptotic expression for the counting function of the set of prime ideals in an abelian extension of number fields, that belong to a fixed coset of the kernel of the Artin map, and fail to split completely in the splitting fields of certain polynomials of the form \( X^m - w \). Akin to the proof of the prime number theorem, it is the analytic techniques used to prove Cooke and Weinberger’s theorem that require the assumption of GRH.
Table 1: Approximate and conjectural densities of $E'_2(p)$

| $p$ | $\pi_p(10^6)/\pi(10^6)$ | $a(p)$ |
|-----|--------------------------|--------|
| 2   | 0.28143                  | 0.28046|
| 3   | 0.30052                  | 0.28046|
| 5   | 0.13815                  | 0.13285|
| 7   | 0.09112                  | 0.08892|
| 11  | 0.05461                  | 0.05403|
| 13  | 0.04635                  | 0.04523|
| 17  | 0.03448                  | 0.03415|
| 19  | 0.03076                  | 0.03043|
| 23  | 0.02563                  | 0.02499|
| 29  | 0.01949                  | 0.01971|

References

[1] K. Christensen, R. Gipson, and H. Kulosman, *Irreducibility of certain binomials in semigroup rings for nonnegative rational monoids*, Int. Electron. J. Algebra 24 (2018), 50–61.

[2] G. Cooke and P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to SL_{2},* Comm. Algebra 3(6) (1975), 481–524.

[3] R. Gilmer, *Commutative Semigroup Rings*, Chicago Lectures in Math., The University of Chicago Press (1984).

[4] C. Hooley, *On Artin’s conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.

[5] G. Janusz, *Algebraic Number Fields* (2nd ed.), Grad. Stud. Math. 7, American Mathematical Society (1996).

[6] S. Lang, *Algebra* (3rd ed.), GTM 211, Springer (2002).

[7] H. W. Lenstra, Jr., *On Artin’s Conjecture and Euclid’s Algorithm in Global Fields*, Invent. Math. 42 (1977), 201–224.

[8] D. Marcus, *Number Fields*, Springer (1977).

[9] S. S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin’s conjecture*, Acta Arith. 41 (1982), 141–150.