On the Zeta Functions of Supersingular Curves

Gary McGuire\textsuperscript{1} and Emrah Sercan Yılmaz\textsuperscript{2}

School of Mathematics and Statistics
University College Dublin
Ireland

Abstract

In general, the L-polynomial of a curve of genus $g$ is determined by $g$ coefficients. We show that the L-polynomial of a supersingular curve of genus $g$ is determined by fewer than $g$ coefficients.

Keywords: Zeta Functions; L-polynomials; Supersingular Curves.

1 Introduction

Let $p$ be a prime and $r \geq 1$ be an integer. Throughout this paper we let $q = p^r$. Let $X$ be a projective smooth absolutely irreducible curve of genus $g$ defined over $\mathbb{F}_q$. Consider the $L$-polynomial of the curve $X$ over $\mathbb{F}_q$, defined by

$$L_{X/\mathbb{F}_q}(T) = L_X(T) = \exp \left( \sum_{n=1}^{\infty} \left( \#X(\mathbb{F}_{q^n}) - q^n - 1 \right) \frac{T^n}{n} \right)$$

where $\#X(\mathbb{F}_{q^n})$ denotes the number of $\mathbb{F}_{q^n}$-rational points of $X$. The $L$-polynomial is the numerator of the zeta function of $X$. It is well known that $L_X(T)$ is a polynomial of degree $2g$ with integer coefficients, so we write it as

$$L_X(T) = \sum_{i=0}^{2g} c_i T^i, \quad c_i \in \mathbb{Z}. \quad (1)$$

It is also well known that $c_0 = 1$ and $c_{2g-i} = q^{g-i} c_i$ for $i = 0, \cdots, g$. Let $\eta_1, \cdots, \eta_{2g}$ be the roots of the reciprocal of the $L$-polynomial of $X$ over $\mathbb{F}_q$ (sometimes called the Weil numbers

\textsuperscript{1}email gary.mcguire@ucd.ie, Research supported by Science Foundation Ireland Grant 13/IA/1914
\textsuperscript{2}Research supported by Science Foundation Ireland Grant 13/IA/1914
of $X$, or the Frobenius eigenvalues). For any $n \geq 1$ we have

$$\#X(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \eta_i^n.$$  \hfill (2)

We refer the reader to [6] for all background on curves.

A curve $X$ of genus $g$ defined over $\mathbb{F}_q$ is supersingular if any of the following equivalent properties hold.

1. All Weil numbers of $X$ have the form $\eta_i = \sqrt{q} \cdot \zeta_i$ where $\zeta_i$ is a root of unity.
2. The Newton polygon of $X$ is a straight line of slope $1/2$.
3. The Jacobian of $X$ is geometrically isogenous to $E^g$ where $E$ is a supersingular elliptic curve.
4. If $X$ has $L$-polynomial $L_X(T) = 1 + \sum_{i=1}^{2g} c_i T^i$ then

$$\text{ord}_p(c_i) \geq \frac{i r}{2}, \text{ for all } i = 1, \ldots, 2g.$$  

Let $\sqrt{q} \cdot \zeta_1, \ldots, \sqrt{q} \cdot \zeta_{2g}$ be the Weil numbers of a supersingular curve $X$, where the $\zeta_i$ are roots of unity. By equation (2) for any $n \geq 1$ we have

$$-q^{-n/2}[\#X(\mathbb{F}_{q^n}) - (q^n + 1)] = \sum_{i=1}^{2g} \zeta_i^n.$$  \hfill (3)

The smallest positive integer $s = s_X$ such that $\zeta_i^s = 1$ for all $i = 1, \ldots, 2g$ will be called the period of $X$. The period depends on $q$, in the sense that $X(\mathbb{F}_{q^n})$ may have a different period to $X(\mathbb{F}_q)$. Note that this is slightly different from the period as defined in [1].

In this paper we will prove the following theorems. The first theorem is our main theorem.
Theorem 1. Let $X$ be a supersingular curve of genus $g$ defined over $\mathbb{F}_q$ with period $s$. Let $n$ be a positive integer, let $\gcd(n, s) = m$ and write $n = m \cdot t$. If $q$ is odd, then we have

$$
\#X(\mathbb{F}_{q^n}) - (q^n + 1) = \begin{cases} 
q^{(n-m)/2} \left[ \#X(\mathbb{F}_{q^m}) - (q^m + 1) \right] & \text{if } m \cdot r \text{ is even,} \\
q^{(n-m)/2} \left[ \#X(\mathbb{F}_{q^m}) - (q^m + 1) \right] \left( \frac{(-1)^{(t-1)/2}}{p} \right) & \text{if } m \cdot r \text{ is odd and } p \nmid t, \\
q^{(n-m)/2} \left[ \#X(\mathbb{F}_{q^m}) - (q^m + 1) \right] & \text{if } m \cdot r \text{ is odd and } p \mid t.
\end{cases}
$$

If $q$ is even, then we have

$$
\#X(\mathbb{F}_{q^n}) - (q^n + 1) = \begin{cases} 
q^{(n-m)/2} \left[ \#X(\mathbb{F}_{q^m}) - (q^m + 1) \right] & \text{if } m \cdot r \text{ is even,} \\
q^{(n-m)/2} \left[ \#X(\mathbb{F}_{q^m}) - (q^m + 1) \right] \left( -1 \right)^{(t^2-1)/8} & \text{if } m \cdot r \text{ is odd.}
\end{cases}
$$

Theorem 2. Let $X$ be a supersingular curve of genus $g$ defined over $\mathbb{F}_q$ with period $s$. Let $L_X(T) = \sum_{i=0}^{2g} c_i T^i$ be the $L$-polynomial of $X$. Assume we know $c_j$ for $1 \leq j < l \leq g$ where $l \nmid s$. Then $c_l$ is determined. In particular, if we know $c_j$ for $1 \leq j \leq g$ where $j \mid s$, then all coefficients of the $L$-polynomial of $X$ are determined.

In Section 2 we present the background we will need, which includes some basic results on quadratic subfields of cyclotomic fields and Gauss sums. In Section 3 we present the proof of Theorem 1, and in Section 4 the proof of Theorem 2. Section 5 contains some applications of our results.

## 2 Quadratic Fields as Subfields of a Cyclotomic Field

Let $n$ be a positive integer. Let $w_n$ be a primitive $n$-th root of unity which we may take to be $e^{2\pi i/n}$. We call $\Phi_n$ be the $n$-th cyclotomic polynomial and the set of the roots of $\Phi_n$ is

$$
\{ w_n^i \mid 1 \leq i \leq n \text{ and } (i, n) = 1 \}.
$$

It is well-known that $\Phi_n$ is irreducible over $\mathbb{Q}$. For odd primes $p$, define

$$
\sqrt{p^*} = \begin{cases} 
\sqrt{p} & \text{if } p \equiv 1 \mod 4, \\
\sqrt{-1} \cdot \sqrt{p} & \text{if } p \equiv 3 \mod 4.
\end{cases}
$$

The following propositions are useful for our proofs.

**Proposition 1.** Let $n$ and $m$ be positive integers with $(n, m) = d$. Then we have

$$
\mathbb{Q}(w_n) \cap \mathbb{Q}(w_m) = \mathbb{Q}(w_d).
$$
Proof. Let \( f \) be the least common multiple of \( n \) and \( m \). Then we have \( w_n, w_m \in \mathbb{Q}(w_f) \).
Since \( d = \frac{nm}{\text{gcd}(n, m)} \), there exists \( a, b \in \mathbb{Z} \) such that \( an + bm = \frac{nm}{d} \) or \( \frac{a}{m} + \frac{b}{n} = \frac{1}{f} \). Therefore \( w_f = w_n^a w_m^b \in \mathbb{Q}(w_n, w_m) \). Hence we have \( \mathbb{Q}(w_n, w_m) = \mathbb{Q}(w_f) \).

Since \( d \mid n, m \), we have \( w_d \in \mathbb{Q}(w_n) \cap \mathbb{Q}(w_m) \). Since \( \mathbb{Q}(w_n) \) is a normal extension over \( \mathbb{Q} \), we have \( \mathbb{Q}(w_d) \subseteq \mathbb{Q}(w_n) \cap \mathbb{Q}(w_m) \).

Proposition 2. If \( p \) is an odd prime, then
\[
\sqrt{p^e} = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_p^j \in \mathbb{Q}(w_p).
\]
Moreover, if \( p \equiv 3 \mod 4 \), then \( \sqrt{p} \notin \mathbb{Q}(w_p) \).

Proof. The first statement is the quadratic Gauss sum result, see [7] for example.

Let \( p \equiv 3 \mod 4 \) and assume \( \sqrt{p} \in \mathbb{Q}(w_p) \). Since \( i \sqrt{p} \) is in \( \mathbb{Q}(w_p) \), then \( i \in \mathbb{Q}(w_p) \). On the other hand, \( \mathbb{Q}(w_d) \cap \mathbb{Q}(w_p) = \mathbb{Q}(w_2) = \mathbb{Q} \) by Proposition[1], which contradicts \( i \in \mathbb{Q}(w_p) \).

Lemma 3. Let \( p \equiv 1 \mod 4 \) be a prime and \( n \) be a positive integer. Then the element \( \sqrt{p} \) is in \( \mathbb{Q}(w_n) \) if and only if \( p \mid n \).

Proof. If \( p \) does not divide \( n \), we have \( (n, p) = 1 \) and
\[
\mathbb{Q}(w_n) \cap \mathbb{Q}(w_p) = \mathbb{Q}
\]
by Proposition[1]. Moreover, we have
\[
\sqrt{p} = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_p^j \in \mathbb{Q}(w_p)
\]
by Proposition[2]. Therefore
\[
\sqrt{p} \notin \mathbb{Q}(w_n).
\]
On the other hand, assume \( p \mid n \). Then we have
\[
\sqrt{p} = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_p^j = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} \in \mathbb{Q}(w_n)
\]
by Proposition[2].
Lemma 4. Let $p \equiv 3 \mod 4$ be a prime and $n$ be a positive integer. Then the element $\sqrt{p}$ is in $\mathbb{Q}(w_n)$ if and only if $4p \mid n$.

Proof. Assume $4p \mid n$. Since $-i$ and $i \sqrt{p}$ are in $\mathbb{Q}(w_n)$, we have $\sqrt{p} = -i \cdot i \sqrt{p} \in \mathbb{Q}(w_n)$.

If $4p$ does not divide $n$, then $(n, 4p)$ is 1, 2, 4, $p$ or $2p$. If $(n, 4p)$ is 1, 2, $p$ or $2p$, then

$$\mathbb{Q}(w_n) \cap \mathbb{Q}(w_{4p}) = \mathbb{Q}(w_{(n,4p)}) \subseteq \mathbb{Q}(w_{2p}) = \mathbb{Q}(w_p)$$

by Proposition 1. Since $\sqrt{p} \in \mathbb{Q}(w_{4p})$ and $\sqrt{p} \not\in \mathbb{Q}(w_p)$ by Proposition 2 we have $\sqrt{p} \not\in \mathbb{Q}(w_n)$.

So by Proposition 1. Since $\sqrt{p} \in \mathbb{Q}(w_{4p})$ and $\sqrt{p} \not\in \mathbb{Q}[i]$, we have $\sqrt{p} \not\in \mathbb{Q}(w_n)$. $\square$

Lemma 5. Let $n$ be a positive integer. The element $\sqrt{2}$ is in $\mathbb{Q}(w_n)$ if and only if $8 \mid n$.

Proof. Assume 8 divides $n$ and write $n = 8t$ where $t$ is a positive integer. Then we have

$$\sqrt{2} = w_8 - w_8^3 = w_n^t - w_n^{3t} \in \mathbb{Q}(w_n).$$

On the other hand, assume 8 does not divide $n$. Then

$$\mathbb{Q}(w_n) \cap \mathbb{Q}(w_8) \subseteq \mathbb{Q}(w_4).$$

Since $\sqrt{2} \in \mathbb{Q}(w_8)$ and $\sqrt{2} \not\in \mathbb{Q}(w_4) = \mathbb{Q}[i]$, we have $\sqrt{2} \not\in \mathbb{Q}(w_n)$. $\square$

Lemma 6. Let $p$ be a prime and $n$ be a positive integer such that $\sqrt{p} \in \mathbb{Q}(w_n)$. Then the extension degree $[\mathbb{Q}(w_n) : \mathbb{Q}(\sqrt{p})]$ is $\frac{\phi(n)}{2}$.

Proof. Since $\sqrt{p} \in \mathbb{Q}(w_n)$, we have

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(w_n).$$

Hence the result follows by the equality

$$\phi(n) = [\mathbb{Q}(w_n) : \mathbb{Q}] = [\mathbb{Q}(w_n) : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2 [\mathbb{Q}(w_n) : \mathbb{Q}(\sqrt{p})].$$

$\square$
Let $p$ be an odd prime and $n$ be an integer such that $\sqrt{p} \in \mathbb{Q}(w_n)$. Define the index sets $I_n^+$ and $I_n^-$ as follows

$$I_n^+ = \left\{ k \mid (k, n) = 1, \left( \frac{(-1)^{(k-1)/2} k}{p} \right) = 1 \text{ and } 1 \leq k \leq n \right\}$$

and

$$I_n^- = \left\{ k \mid (k, n) = 1, \left( \frac{(-1)^{(k-1)/2} k}{p} \right) = -1 \text{ and } 1 \leq k \leq n \right\}.$$

In same manner, let $p = 2$ and $n$ be an integer divisible by 8. Define the index sets $I_n^+$ and $I_n^-$ as follows

$$I_n^+ = \left\{ k \mid (k, n) = 1, k \equiv \pm 1 \mod 8 \text{ and } 1 \leq k \leq n \right\}$$

and

$$I_n^- = \left\{ k \mid (k, n) = 1, k \equiv \pm 3 \mod 8 \text{ and } 1 \leq k \leq n \right\}.$$

Moreover, define $I_n = I_n^+ \cup I_n^-$. Define the polynomials $\Phi_n^+$ and $\Phi_n^-$ as follows

$$\Phi_n^+(x) = \prod_{j \in I_n^+} (x - w_n^j) \quad \text{and} \quad \Phi_n^-(x) = \prod_{j \in I_n^-} (x - w_n^j).$$

Define $G_n$ to be the Galois group $\text{Gal}(\mathbb{Q}(w_n)/\mathbb{Q})$. Define the group $G_n^+$ and the set $G_n^-$ as follows

$$G_n^+: = \{ \sigma \in G_n | \sigma(w_n) = w_n^k \text{ where } k \in I_n^+ \}$$

and

$$G_n^-: = \{ \sigma \in G_n | \sigma(w_n) = w_n^k \text{ where } k \in I_n^- \}.$$

The following lemmas show that $G_n^+$ is a subgroup of the Galois group $G_n$ of index 2 and shows that the subset $G_n^-$ is the relative coset of $G_n^+$ inside $G_n$.

**Lemma 7.** Let $p \equiv 1 \mod 4$ be a prime and $n$ be a positive integer divisible by $p$. Then the group $G_n^+$ fixes $\sqrt{p}$ and $G_n^-$ takes $\sqrt{p}$ to $-\sqrt{p}$.

**Proof.** For a positive integer $k$ we have $\left( \frac{(-1)^{(k-1)/2} k}{p} \right) = \left( \frac{k}{p} \right) \text{ since } \left( \frac{-1}{p} \right) = 1$.

Let $\sigma \in G_n^+$. Then there exists an integer $k$ with $(k, n) = 1$, $\left( \frac{k}{p} \right) = 1$ and $1 \leq k \leq n$ and $\sigma(w_n) = w_n^k$. Then

$$\sigma(\sqrt{p}) = \sigma \left( \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} \right) = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{kjn/p} = \sum_{j=0}^{p-1} \left( \frac{kj}{p} \right) w_n^{kjn/p}$$
= \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} = \sqrt{p}.

Let \( \sigma \in G_n^- \). Then there exists an integer \( k \) with \( (k, n) = 1 \) and \( 1 \leq k \leq n \) and \( \sigma(w_n) = w_n^k \). Then

\[
\sigma(\sqrt{p}) = \sigma \left( \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} \right) = \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{kjn/p} = \sum_{j=0}^{p-1} \left( \frac{k}{p} \right) w_n^{kjn/p}
\]

\[
= -\sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} = -\sqrt{p}.
\]

\[\square\]

**Lemma 8.** Let \( p \equiv 3 \mod 4 \) be a prime and \( n \) be a positive integer divisible by \( 4p \). Then the group \( G_n^+ \) fixes \( \sqrt{p} \) and \( G_n^- \) takes \( \sqrt{p} \) to \( -\sqrt{p} \).

**Proof.** Let \( \sigma \in G_n \). Then there exists an integer \( k \) with \( (k, n) = 1 \) and \( 1 \leq k \leq n \) and \( \sigma(w_n) = w_n^k \).

Since \( n \) is even, \( k \) is odd. Since \( n \) is divisible by \( p \), \( k \) is not divisible by \( p \).

Moreover, we have

\[
\sigma(-i) = -\sigma(i) = -\sigma(w_n^{n/4}) = -\sigma(w_n)^{n/4} = -(w_n^{n/4})^k = -i^k.
\]

If \( \left( \frac{k}{p} \right) = 1 \), we have

\[
\sigma(\sqrt{p}) = \sigma(-i \cdot i \sqrt{p}) = \sigma(-i) \cdot \sigma \left( \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} \right) = -i^k \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{kjn/p}
\]

\[
= -i^k \sum_{j=0}^{p-1} \left( \frac{k}{p} \right) w_n^{kjn/p} = -i^k \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} = -i^k \cdot i \sqrt{p} = -i^{k+1} \sqrt{p} = (-1)^{(k-1)/2} \sqrt{p}
\]

and if \( \left( \frac{k}{p} \right) = -1 \), we have

\[
\sigma(\sqrt{p}) = \sigma(-i \cdot i \sqrt{p}) = \sigma(-i) \cdot \sigma \left( \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} \right) = -i^k \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{kjn/p}
\]

\[
= -i^k \sum_{j=0}^{p-1} \left( \frac{k}{p} \right) w_n^{kjn/p} = -i^k \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} = -i^k \cdot i \sqrt{p} = -i^{k+1} \sqrt{p} = (-1)^{k/2} \sqrt{p}
\]
\[-i^k \sum_{j=0}^{p-1} \left( \frac{k}{j} \right) w_n^{kj/p} = i^k \sum_{j=0}^{p-1} \left( \frac{j}{p} \right) w_n^{jn/p} = -i^k \cdot i\sqrt{p} = i^{k+1} \sqrt{p} = -(-1)^{(k-1)/2} \sqrt{p}.\]

Now the result follows by the fact \(\left( \frac{-1}{p} \right) = -1.\)

Lemma 9. Let \(p = 2\) and \(n\) be a positive integer divisible by 8. Then the group \(G^+_n\) fixes \(\sqrt{2}\) and \(G^-_n\) takes \(\sqrt{2}\) to \(-\sqrt{2}\).

Proof. Let \(\sigma \in G^+_n\). Then there exists an integer \(k\) with \((k, n) = 1\), \(k \equiv \pm 1\) mod 8 and \(1 \leq k \leq n\) and \(\sigma(w_n) = w_n^k\). Then
\[
\sigma(\sqrt{2}) = \sigma(w_8^3 - w_8^8) = w_8^k - w_8^{3k} = \begin{cases} w_8^3 - w_8^8 & \text{if } k \equiv 1 \text{ mod } 8 \\ w_8^7 - w_8^5 & \text{if } k \equiv 7 \text{ mod } 8 \end{cases} = \sqrt{2}.
\]

Let \(\sigma \in G^-_n\). Then there exists an integer \(k\) with \((k, n) = 1\), \(k \equiv \pm 3\) mod 8 and \(1 \leq k \leq n\) and \(\sigma(w_n) = w_n^k\). Then
\[
\sigma(\sqrt{2}) = \sigma(w_8^3 - w_8^8) = w_8^k - w_8^{3k} = \begin{cases} w_8^3 - w_8^8 & \text{if } k \equiv 3 \text{ mod } 8 \\ w_8^7 - w_8^5 & \text{if } k \equiv 5 \text{ mod } 8 \end{cases} = -\sqrt{2}.
\]

Corollary 1. Let \(p\) be a prime and \(n\) be a positive integer such that \(\sqrt{p} \in \mathbb{Q}(w_n)\). The polynomials \(\Phi_n^+\) and \(\Phi_n^-\) are irreducible over \(\mathbb{Q}(\sqrt{p})\).

Proof. By Lemma 7, 8 and 9 the Galois group \(Gal(\mathbb{Q}(w_n)/\mathbb{Q}(\sqrt{p}))\) is \(G^+_n\). The result follows by this fact.

Corollary 2. Let \(p\) be an odd prime and \(n\) be a positive integer such that \(\sqrt{p} \in \mathbb{Q}(w_n)\). Let \(\ell\) be an integer. There exist rational numbers \(a\) and \(b\) such that
\[
\sum_{j \in I^+_n} w_n^{j\ell} = a + b\sqrt{p} \quad \text{and} \quad \sum_{j \in I^-_n} w_n^{j\ell} = a - b\sqrt{p}.
\]

Proof. Since \(G^+_n\) fixes both sums, they are in \(\mathbb{Q}(\sqrt{p})\). In other words, there exist rational numbers \(a, b, c\) and \(d\) such that
\[
\sum_{j \in I^+_n} w_n^{j\ell} = a + b\sqrt{p} \quad \text{and} \quad \sum_{j \in I^-_n} w_n^{j\ell} = c + d\sqrt{p}.
\]

Since \(G^-_n\) sends one to the other, they are conjugate in \(\mathbb{Q}(\sqrt{p})\). Hence \(c = a\) and \(d = -b\).
3 Proof of Theorem 1

Let $X$ be a supersingular curve of genus $g$ defined over $\mathbb{F}_q$ having period $s$. Let $n$ be a positive integer and let $m = \gcd(s, n)$.

Since $X$ is also a curve of genus $g$ over $\mathbb{F}_{q^m}$, we will consider $X$ on $\mathbb{F}_{q^m}$. Write $s = m \cdot u$. Then $\sqrt{q^m}$ times the roots of $L_X/\mathbb{F}_{q^m}$ are $u$-th roots of unity, i.e., the period of $X$ is $u$ over $\mathbb{F}_{q^m}$ because of equation (3).

Define $M_X(T)$ to be $L_X/\mathbb{F}_{q^m}(q^{-m/2}T)$. Then $M_X$ is monic and the roots of $M_X$ are $\zeta_1^{-m}, \cdots, \zeta_2^{-m}$ where $\zeta_i$’s are in equation (3). Hence the smallest positive integer $k$ such that $w^k = 1$ for all roots $w$ of $M$ is $u$.

Write $n = m \cdot t$. Then we have $(u, t) = 1$ and the extension degree $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] = t$. In the proofs below, we will reduce the case $t > 1$ to the case $t = 1$. We will be using the fact that the roots of the polynomial $L_X/\mathbb{F}_{q^n}(q^{-n/2}T)$ of $X/\mathbb{F}_{q^n}$ are the $t$-th powers of the roots of $M_X(T)$.

3.1 Proof of Theorem 1 for $r$ or $m$ even

Assume that either $r$ or $m$ is even. Then $M_X(T) \in \mathbb{Q}[T]$. Since the roots of $M_X$ are $u$-th roots of unity and $M_X$ is monic, the factorization of $M_X$ in $\mathbb{Q}[T]$ is as follows:

$$M_X(T) = \prod_{d \mid u} \Phi_d(T)^{e_d}$$

(4)

where $e_d$ is a non-negative integer for each $d \mid u$.

Since $(u, t) = 1$, the map $x \to x^t$ permutes the roots of $\Phi_d$ where $d \mid u$. Therefore, we have (by equations (3) and (4))

$$-q^{-n/2}[\#X(\mathbb{F}_{q^n}) - (q^n + 1)] = \sum_{d \mid u} \left( e_d \sum_{j \in I_d} w_d^{-jt} \right)$$

$$= \sum_{d \mid u} \left( e_d \sum_{j \in I_d} w_d^{-j} \right)$$

$$= -q^{-m/2}[\#X(\mathbb{F}_{q^m}) - (q^m + 1)].$$
3.2 Proof of Theorem 1 for \(r\) and \(m\) odd

Assume \(r\) and \(m\) are odd. Note that \(u\) must be even, because equality holds in the Hasse-Weil bound.

We have \(M_X(T) \in \mathbb{Q}(\sqrt{p})[T]\). Since the roots of \(M_X\) are \(u\)-th roots of unity, we can write \(M_X(T)\) as

\[
M_X(T) = \prod_{d|u, \sqrt{p} \in \mathbb{Q}(w_d)} \Phi_d^+(T)^{e_{d,1}} \Phi_d^-(T)^{e_{d,2}} \prod_{d|u, \sqrt{p} \notin \mathbb{Q}(w_d)} \Phi_d(T)^{e_d}
\]

(5)

where \(e_{d,1}, e_{d,2}\) and \(e_d\) are non-negative integers for each \(d|u\).

Since \((u, t) = 1\), the map \(x \to x^t\) permutes the roots of \(\Phi_d\) where \(d|u\).

**Case A.** When \(p\) does not divide \(t\).

We have (by Equation 3 and 5)

\[
-q^{-n/2} \left[ \#X(F_{q^n}) - (q^n + 1) \right] = \sum_{d|u, \sqrt{p} \in \mathbb{Q}(w_d)} \left( e_{d,1} \sum_{j \in I_d^+} w_d^{-jt} + e_{d,2} \sum_{j \in I_d^-} w_d^{-jt} \right)
\]

\[
+ \sum_{d|u, \sqrt{p} \notin \mathbb{Q}(w_d)} \left( e_d \sum_{j \in I_d} w_d^{-jt} \right).
\]

**Case 1.** Assume that \(t\) is a positive integer such that

\[
\left( \frac{(-1)^{(t-1)/2}}{p} \right) = 1 \quad \text{if } p \text{ is odd,}
\]

\[
t \equiv \pm 1 \mod 8 \quad \text{if } p = 2.
\]

By Lemmas 7, 8, and 9 the map \(x \to x^t\) permutes the roots of \(\Phi_d^+\) and permutes the roots of \(\Phi_d^-\).
where $d \mid u$. Hence we have

$$-q^{-n/2} \left[ \# X(F_{q^n}) - (q^n + 1) \right] = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I_d^+} w_d^{-jt} + e_{d,2} \sum_{j \in I_d^-} w_d^{-jt} \right)$$

$$+ \sum_{d \mid u, \sqrt{p} \not\in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d^+} w_d^{-jt} \right)$$

$$= \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I_d^+} w_d^{-j} + e_{d,2} \sum_{j \in I_d^-} w_d^{-j} \right)$$

$$+ \sum_{d \mid u, \sqrt{p} \not\in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d^+} w_d^{-j} \right)$$

$$= -q^{-m/2} \left[ \# X(F_{q^m}) - (q^m + 1) \right].$$

**Case 2.** Assume that $t$ is a positive integer such that

$$\left\{ \frac{(-1)^{(t-1)/2}}{t} \right\} = -1 \quad \text{if } p \text{ is odd},$$

$$t \equiv \pm 3 \mod 8 \quad \text{if } p = 2.$$  

By Lemmas 7, 8 and 9 the map $x \to x^t$ sends the roots of $\Phi_d^+$ to the roots of $\Phi_d^-$ and vice versa where $d \mid u$. Hence we have

$$-q^{-n/2} \left[ \# X(F_{q^n}) - (q^n + 1) \right] = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I_d^+} w_d^{-jt} + e_{d,2} \sum_{j \in I_d^-} w_d^{-jt} \right)$$

$$+ \sum_{d \mid u, \sqrt{p} \not\in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d^+} w_d^{-jt} \right)$$

$$= \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I_d^+} w_d^{-j} + e_{d,2} \sum_{j \in I_d^-} w_d^{-j} \right)$$

$$+ \sum_{d \mid u, \sqrt{p} \not\in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d^+} w_d^{-j} \right).$$

For any $d$ with $d \mid u$, we write $\sum_{j \in I_d^+} w_d^{-j} = a_d + b_d \sqrt{p}$ where $a_d$ and $b_d$ are rational numbers (such rational numbers exist by Corollary 2). Then we have $\sum_{j \in I_d^-} w_d^{-j} = a_d - b_d \sqrt{p}$ by
Corollary 2. Therefore, we also have $\sum_{j \in I_d} w_d^{-j} = 2a_d$. Hence the last line

\[
\sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I^+_d} w_d^{-j} + e_{d,2} \sum_{j \in I^-_d} w_d^{-j} \right) + \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d} w_d^{-j} \right) = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1}(a_d - b_d\sqrt{p}) + e_{d,2}(a_d + b_d\sqrt{p}) \right) + \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} (e_d \cdot 2a_d).
\]

We have therefore shown that

\[
-q^{-n/2}[\#X(F_{q^n}) - (q^n + 1)] = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1}(a_d - b_d\sqrt{p}) + e_{d,2}(a_d + b_d\sqrt{p}) \right) + \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} (e_d \cdot 2a_d).
\]

Note that $n$ is odd because $s$ is even and $m$ is odd. Also $r$ is odd (where $q = p^r$) and $\#X(F_{q^n}) - (q^n + 1)$ is an integer, so $-q^{-n/2}[\#X(F_{q^n}) - (q^n + 1)]$ must have the form $d\sqrt{p}$ where $d$ is a rational number. Therefore we must have

\[
-q^{-n/2}[\#X(F_{q^n}) - (q^n + 1)] = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} ((e_{d,2} - e_{d,1})b_d\sqrt{p}). \tag{6}
\]

By the same argument as in the previous paragraph when $n = m$, we get that $-q^{-m/2}[\#X(F_{q^m}) - (q^m + 1)]$ has the form $c\sqrt{p}$ where $c$ is a rational number.

Now we apply the same reasoning as above when $n = m$. We get

\[
-q^{-m/2}[\#X(F_{q^m}) - (q^m + 1)] = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1} \sum_{j \in I^+_d} w_d^{-j} + e_{d,2} \sum_{j \in I^-_d} w_d^{-j} \right) + \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_d \sum_{j \in I_d} w_d^{-j} \right) = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} \left( e_{d,1}(a_d + b_d\sqrt{p}) + e_{d,2}(a_d - b_d\sqrt{p}) \right) + \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} (e_d \cdot 2a_d) = \sum_{d \mid u, \sqrt{p} \in \mathbb{Q}(u_d)} ((e_{d,1} - e_{d,2})b_d\sqrt{p}).
\]
Comparing this last expression with (6) we see that
\[-q^{-n/2}[\#X(\mathbb{F}_q^n) - (q^n + 1)] = -q^{-m/2}[\#X(\mathbb{F}_q^m) - (q^m + 1)] \cdot (-1).\]

**Case B.** When \( p \) divides \( t \).

Since \((t, u) = 1\) and \( p \mid t \), we have \( p \nmid u \). Therefore, \( \sqrt{p} \notin \mathbb{Q}(w_d) \) for each \( d \mid u \) and so
\[M_X(z) = \prod_{d \mid u} \Phi_d(z)^{e_d} \tag{7}\]
where \( e_d \)'s are non-negative integers. Hence, we have (by Equation 3 and 7)
\[-q^{n/2}[\#X(F_{q^n}) - (q^n + 1)] = \sum_{d \mid u} \left( e_d \sum_{j \in I_d} w_d^{-j} \right) = \sum_{d \mid u} \left( e_d \sum_{j \in I_d} w_d^{-j} \right) = -q^{m/2}[\#X(F_{q^m}) - (q^m + 1)].\]

**4 Proof of Theorem 2**

In this section we will give the proof of Theorem 2. The following well-known proposition will be useful to prove the theorem (see [6] for example).

**Proposition 3.** Let \( X \) be a supersingular curve of genus \( g \) defined over \( \mathbb{F}_q \). Let \( L_X(T) = \sum_{i=0}^{2g} c_i T^i \) be the \( L \)-polynomial of \( X \) and let \( S_n = \#X(\mathbb{F}_{q^n}) - (q^n + 1) \) for all integers \( n \geq 1 \). Then \( c_0 = 1 \) and
\[ic_i = \sum_{j=0}^{i-1} S_{i-j} c_j \]
for \( i = 1, \ldots, g \).

**Proof of Theorem 2** By Proposition 3 we have \( S_1 = c_1 \) and
\[S_i = ic_i - \sum_{j=1}^{i-1} S_{i-j} c_j\]
for \(2 \leq i \leq g\). Since \(c_1, \ldots, c_{l-1}\) are known, we can inductively find \(S_1, \ldots, S_{l-1}\) by above expression. Since \(d = (l, s) < l\) and since we know what \(S_d\) is, we can find \(S_l\) by Theorem 1. Therefore, since

\[
c_l = \frac{1}{l} \sum_{j=0}^{l-1} S_{l-j} c_j
\]

by Proposition 5 and since \(c_0, c_1, \ldots, c_{l-1}\) and \(S_1, \ldots, S_l\) are known, we can find \(c_l\). \qed

5 Applications

In this section we present a few applications of our results.

5.1 An Example

The usefulness of Theorems 1 and 2 is shown by an example. Let is consider the curve \(C : y^5 - y = x^6\) over \(\mathbb{F}_5\) and calculate its L-polynomial. This curve is actually the curve denoted \(B_1^{(5)}\) in [3], and is a curve of genus 10. By Corollary 1 in [3] the roots of the L-polynomial are \(\sqrt{5}\) times a 4-th root of unity (i.e., the period \(s\) is 4). Write \(L_C\) as

\[
L_C(T) = \sum_{i=0}^{20} c_i T^i.
\]

Normally the values \(c_i\) for \(1 \leq i \leq 10\) have to be computed, and then the L-polynomial is determined. We will show using Theorem 2 that only three of the \(c_i\) need to be computed in order to determine the entire L-polynomial.

The three values needed are \(c_1\), \(c_2\) and \(c_4\), because 1, 2, and 4 are the divisors of the period. We calculate \(c_1 = 0\), \(c_2 = -10\) and \(c_4 = -75\). In order to find \(L_C\) we have to find \(c_3, c_5, c_6, c_7, c_8, c_9\) and \(c_{10}\).

Let us apply the recursion in Theorem 2. Firstly, we have \(S_1 = c_1 = 0\) and \(S_2 = 2s_2 - S_1 c_1 = -20\).

Next, we may apply Theorem 1 to get \(S_3\) since \((3, 4) = 1\). Thus by Theorem 1 applied with the values \(s = 4, n = 3, m = 1, r = 1, t = 3\), we get

\[
S_3 = 5^{(n-m)/2} \left( \frac{(-1)^{(t-1)/2} t}{5} \right) S_1 = 0.
\]
Since we have
\[ 3c_3 = S_3c_0 + S_2c_1 + S_1c_2 \]
by Proposition 3, we get \( c_3 = 0 \).

Since we know \( c_4 = -75 \) we get
\[ S_4 = 4c_4 - S_3c_1 - S_2c_2 - S_1c_1 = -500. \]

In a similar way to \( S_3 \) we find all \( S_i \) for \( i = 5, \cdots, 10 \) by Theorem 1. These numbers are
\[ S_5 = S_7 = S_9 = 0, \quad S_6 = -500, \quad S_8 = S_{10} = -12500. \]

Then we can find all \( c_i \) for \( i = 5, \cdots, 10 \) by Theorem 2 inductively using the Equation (8). We get \( c_5 = c_7 = c_9 = 0 \) and
\[ c_6 = \frac{1}{6} \sum_{j=0}^{5} S_{6-j}c_j = 1000, \quad c_8 = \frac{1}{8} \sum_{j=0}^{7} S_{8-j}c_j = 1250, \quad c_{10} = \frac{1}{10} \sum_{j=0}^{9} S_{10-j}c_j = -37500. \]

Therefore the L-polynomial of \( C \) over \( \mathbb{F}_5 \) is
\[
1 - 10T^2 - 75T^4 + 1000T^6 + 1250T^8 - 37500T^{10} \\
+ 31250T^{12} + 625000T^{14} - 1171875T^{16} - 3906250T^{18} + 9765625T^{20}.
\]

### 5.2 Families of Curves

The authors have used the two main theorems of this paper in [3] to calculate the exact number of rational points on curves \( y^p - y = x^{p^k+1} \) and \( y^p - y = x^{p^k+1} + x \) over all extensions of \( \mathbb{F}_p \). The same techniques can be used for other supersingular curves.

Another example of applying these results can be found in our preprint [4]. There we calculated the exact number of points on \( y^q - y = x^{q+1} - x^2 \) in order to count the number of irreducible polynomials with the first two coefficients fixed (providing another proof of a result of Kuzmin).

### 5.3 Point Counting

The results of this paper imply a speedup for point counting algorithms for supersingular curves, at least in theory. In general, to calculate the L-polynomial of a curve defined over \( \mathbb{F}_q \), one needs
to compute the number of $\mathbb{F}_{q^i}$-rational points for all $i = 1, 2, \ldots, g$. However, Theorem 2 means that not all of these values are needed for supersingular curves. The values that are needed are the number of $\mathbb{F}_{q^i}$-rational points where $i$ divides $s$. As seen in the example above, we only needed four values ($i = 1, 2, 4$) instead of ten values.

6 Value of the Period

To apply the results of this paper one needs to know the period $s$ (or a multiple of $s$) of a supersingular curve $X$ of genus $g$. It is sometimes possible to find the period without finding the L-polynomial. This is often the case for Artin-Schreier curves of the form $y^p - y = xL(x)$ where $L(x)$ is a linearized polynomial. Indeed, this is what the authors did in [3] for the curves $y^p - y = x^{p^k+1}$ and $y^p - y = x^{p^k+1} + x$. Another example of this is provided in [2] with the hyperelliptic curves $y^2 = x^{2g+1} + 1$ where $(p, 2g + 1) = 1$. The period is shown to be the smallest $k$ such that $p^k \equiv -1 \pmod{4g+2}$.

For a simple supersingular abelian variety, we have $\phi(s) = 2g$ or $4g$ (see [5]) where $\phi$ is the Euler phi-function. Therefore if the Jacobian of $X$ is simple, we know that $\phi(s) = 2g$ or $4g$. This can be used to make a list of possible values of $s$. If the Jacobian of $X$ is not simple it is isogenous to a product of simple abelian varieties of smaller dimension.

We call $X(\mathbb{F}_{q^n})$ minimal if all the Weil numbers are $\sqrt{q^n}$. Equivalently, $X(\mathbb{F}_{q^n})$ is minimal if and only if $L_X(T) = (1 - \sqrt{q^n}T)^{2g}$. Thus, for a supersingular curve $X$ defined over $\mathbb{F}_q$, the period is the smallest extension degree over which $X$ is minimal.

References

[1] V. Karemaker R. Pries, Fully maximal and fully minimal abelian varieties, preprint, https://arxiv.org/abs/1703.10076

[2] Kodama, T. and Washio, T., A Family of Hyperelliptic Function Fields with Hasse-Witt Invariant Zero. J. Number Theory 36 187-200

[3] G. McGuire, E. S. Yılmaz, Divisibility of L-Polynomials for a Family of Artin-Schreier Curves, preprint, https://arxiv.org/abs/1803.03511

16
[4] G. McGuire, E. S. Yılmaz, The Number of Irreducible Polynomials with the First Two Coefficients Fixed over Finite Fields of Odd Characteristic, preprint, https://arxiv.org/abs/1609.02314

[5] V. Singh, G. McGuire, A. Zaytsev, Classification of Characteristic Polynomial of Simple Supersingular Abelian Varieties over Finite Fields, Functiones et Approximatio Commentarii Mathematici, 51 (2014) no.2, 415-436.

[6] Henning Stichtenoth. Algebraic Function Fields and Codes. Springer-Verlag Berlin Heidelberg, 2009.

[7] Lawrence C. Washington. Introduction to Cyclotomic Fields. EBL-Schweitzer. Springer-Verlag New York, 1997.