DIVISION BY $1 - \zeta$ ON SUPERELLIPTIC CURVES AND JACOBIANS

VISHAL ARUL

Abstract. Yuri Zarhin gave formulas for “dividing a point on a hyperelliptic curve by 2.” Given a point $P$ on a hyperelliptic curve $C$, Zarhin gives the Mumford’s representation of every degree $g$ divisor $D$ such that $2(D - g\infty) \sim P - \infty$.

The aim of this paper is to generalize Zarhin’s result to the superelliptic situation; instead of dividing by 2, we divide by $1 - \zeta$. Even though there is no Mumford’s representation for superelliptic curves, we give a formula for functions which cut out $D$.

Additionally, we study the intersection of the pullback $(1 - \zeta)^*C$ and the theta divisor $\Theta$ inside the jacobian. The intersection is exactly $J[1 - \zeta]$ and the intersection multiplicities are the inflectionary weights with respect to the point at infinity.

Contents

1. Introduction 2
   1.1. A minor translation. 3
   1.2. Notation for matrices 3
   1.3. Dividing by $1 - \zeta$ 4
2. Computational Lemmas 4
3. Main Proof 7
   3.1. Vanishing loci of $N_{i,j}$ 7
   3.2. Orders at infinity 9
   3.3. Proof of 1.1 10
4. Varying the choice of $r_i$ 11
5. Intersection of $(1 - \zeta)^{-1}C$ and $\Theta$ 12
6. Acknowledgements 22
References 23

This research was supported in part by a grant from the Simons Foundation (#402472 to Bjorn Poonen).
1. Introduction

Fix an integer \( n \geq 2 \) and an algebraically closed field \( K \) of characteristic not dividing \( n \). Let \( \mathcal{C} \) be the smooth projective model of the curve given by the equation

\[
y^n = \prod_{i=1}^{d} (x + \alpha_i)
\]

in \( A^2_K \). Suppose that \( n, d \) are coprime and that the \( \alpha_i \) are distinct. Then \( \mathcal{C} \) has a unique point at infinity, denoted by \( \infty \). The genus of \( \mathcal{C} \) is

\[
g = \frac{1}{2} (n - 1)(d - 1).
\]

Let \( J \) be the jacobian of \( \mathcal{C} \). Then \( \mathcal{C} \) naturally embeds into \( J \) via the map \( P \mapsto P - \infty \); that is, the point \( P \) of \( \mathcal{C} \) goes to the divisor class \([P - \infty]\). Given divisors \( X \) and \( Y \) on \( \mathcal{C} \), we write “\( X \sim Y \)” to indicate that \( X \) is linearly equivalent to \( Y \). Moreover, the notation “\( X \geq Y \)” means that \( X - Y \) is effective. Define the “gcd” of a collection of divisors \( \{X_i\} \) to be the maximal \( X \) such that \( X \leq X_i \) for all \( i \). For more details about curves, their jacobians, and divisor classes, see [Poo06] or [Ful69].

Given a rational function \( f \) on \( \mathcal{C} \), we write \( \text{div}(f) \) to be the principal divisor associated to \( f \) and \( \text{div}_0(f) \) to be the effective portion of \( \text{div}(f) \).

We use \( \zeta \) to denote both the primitive \( n \)-th root of unity in \( K \) and the endomorphism \( \zeta : \mathcal{C} \to \mathcal{C} \) which acts on points of \( \mathcal{C} \) via

\[
\zeta : (x, y) \mapsto (x, \zeta y).
\]

Then \( 1 - \zeta \) is an endomorphism of \( J \).

Our goal is to provide formulas for “division by \( 1 - \zeta \)” for points of \( \mathcal{C} \). For a fixed point \( P \) on \( \mathcal{C} \), we seek to find rational functions on \( \mathcal{C} \) which cut out a divisor \( D \) satisfying the property

\[
(1 - \zeta)D \sim P - \infty.
\]

In the case where \( n = 2 \), the curve \( \mathcal{C} \) is hyperelliptic and we seek to divide by \( 1 - \zeta = 2 \). In [Zar19], Zarhin provides formulas for division by 2 in the hyperelliptic setting. His formulas are written in terms of the Mumford’s representation (see [Mum84], page 3.17), which describes an effective degree \( g \) divisor \( D \) on a hyperelliptic curve by giving two rational functions \( f_1, f_2 \) on \( \mathcal{C} \) such that \( D = \gcd(\text{div}_0(f_1), \text{div}_0(f_2)) \). If \( \iota \) is the hyperelliptic involution on \( \mathcal{C} \), then there is an effective degree \( g \) divisor \( E \) such that

\[
\text{div}(f_1) = D + \iota(E) - 2g\infty,
\]

\[
\text{div}(f_2) = D + E + \iota(P) - (2g + 1)\infty,
\]

From this, we get \( (1 - \iota)D \sim P - \infty \), or equivalently, that \( 2(D - g\infty) \sim P - \infty \).

In the superelliptic setting, we instead find \( n \) rational functions \( f_1, \cdots, f_n \) such that for some degree \( g \) effective divisor \( E \),

\[
\text{div}(f_1) = D + \zeta^{-1}(E) - 2g\infty
\]

\[
\text{div}(f_2) = D + \zeta^{-2}(E) + \zeta^{-1}(P) - (2g + 1)\infty
\]

\[
\vdots
\]

\[
\text{div}(f_n) = D + E + \zeta^{-1}(P) + \zeta^{-2}(P) + \cdots + \zeta^{-(n-1)}(P) - (2g + n - 1)\infty
\]
From the first two equations, we get that \( \text{div}(f_1/\zeta^*f_2) = (1 - \zeta)D - (P - \infty) \), so it follows that \((1 - \zeta)D \sim P - \infty \). Moreover, we will show that

\[
D = \gcd_{1 \leq j \leq n} \text{div}_0 f_j.
\]

When \( n = 2 \), our formulas reduce exactly to those of Zarhin’s in the hyperelliptic case. In this sense, this representation of \( D \) is the analogue of the Mumford’s representation in the hyperelliptic case. Zarhin’s techniques do not readily extend from \( n = 2 \) to general \( n \); the main obstruction is the lack of a Mumford’s representation when \( n > 2 \).

- When \( n = 2 \), it is the case that \((f_1, f_2) = (U(x), y - V(x)) \) for \( U(x), V(x) \in K[x] \) satisfying \( U|V^2 - \prod(x + \alpha_i) \). (The pair \((U, V)\) is called the Mumford’s representation of \( D \).) Assuming that \( f_1, f_2 \) are in this special format greatly simplifies the rest of the computation. However, even when \( n = 3 \), one cannot assume that \( f_1, f_2 \) will have this special form; one must work with the more general \( f_i = U_{0,i}(x) + U_{1,i}(x)y + U_{2,i}(x)y^2 \).

- Suppose we tried to work with a “pseudo-Mumford representation” by attempting to represent \( D \) as \( \gcd(\text{div}_0 U(x), \text{div}_0(y - V(x))) \) for some \( U, V \in K[x] \) when \( n > 2 \). First of all, this form might not exist for some \( D \) when \( n > 2 \). Even if it did exist for \( D \) satisfying \((1 - \zeta)D \sim P - \infty \), it is crucial for Zarhin’s argument that

\[
\text{div}\left(\frac{U(x)}{y - V(x)}\right) = (1 - \zeta)D - (P - \infty),
\]

and there is no reason for this to hold when \( n > 2 \).

- There are other ways to represent divisor classes on superelliptic curves; see [GPS02] for another possible representation and algorithms for computations in that representation. However, we were not able to use their representation for our formulas.

As an application, we can divide any point \((-\alpha_i,0)\) by \(1 - \zeta \). Since \((-\alpha_i,0) - \infty \in J[1 - \zeta] \), we obtain generators for \(J[(1 - \zeta)^2] \). In particular, for the case \( n = 3 \) we know that \( J[(1 - \zeta_3)^2] = J[3] \), so our formulas give a representation of every 3-torsion element of the Jacobian of a trigonal superelliptic curve. We also hope that our formula can be used to perform explicit descent and compute the rational points on some superelliptic curves.

One curious aspect of this formula is that every \( D \) satisfying \((1 - \zeta)D \sim P - \infty \) never lands on the Theta divisor \( \Theta \) of the Jacobian whenever \( P \neq \infty \). That is, \( \mathcal{C} \cap (1 - \zeta)\Theta = \{0\} \), which implies that \((1 - \zeta)^*\mathcal{C} \cap \Theta = J[1 - \zeta] \). In section 5, we compute the intersection multiplicity of \((1 - \zeta)^*\mathcal{C} \) and \( \Theta \) at any \( D \in J[1 - \zeta] \). This multiplicity turns out to be the inflectionary weight of \( D \) with respect to \( \infty \).

1.1. A minor translation. For notational convenience we will divide the point \( P = (0, b) \) by \(1 - \zeta \) on \( \mathcal{C} \). To handle the general case \( P = (a, b) \), apply a translation to consider the division of the point \( P' = (0, b) \) on the curve \( \mathcal{C}' \) given as the projective normalization of the affine plane \( K \)-curve \( y^n = \prod_{i=1}^d (x + a + \alpha_i) \).

1.2. Notation for matrices. The notation “\( \text{adj} T \)” stands for the adjugate matrix of \( T \) and \( T_{i,j} \) denotes the \((i, j)\)-th entry of \( T \). If \( T \) is an \( n \times n \) matrix, then the indices \( i, j \) will be taken modulo \( n \) to make sense of expressions of the form \( T_{-1,2n} \) (this means \( T_{n-1,n} \)).
1.3. Dividing by $1 - \zeta$. Let $P = (0, b)$ lie on $C$. Choose $r_i$ such that

$$r_i^n = \alpha_i$$

$$\prod r_i = b$$

Let $s_j$ be the $j$-th elementary symmetric polynomial evaluated on the $r_i$, where the convention is that $s_m = 0$ for $m < 0$ and for $m > d$. (So $b = s_d$.) Define the following polynomials in $x$ for all $\ell \geq 0$.

$$A_\ell(x) = \sum_{k \geq 0} (-1)^{(n-1)k} s_{\ell-nk} x^k$$

Let $A, Z, M, N$ be the following $n \times n$ matrices.

\[
A := \begin{bmatrix}
A_d & A_{d-1} & \cdots & A_{d-n+2} & A_{d-n+1} \\
A_{d+1} & A_d & \cdots & A_{d-n+3} & A_{d-n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
A_{d+n-2} & A_{d+n-3} & \cdots & A_d & A_{d-1} \\
A_{d+n-1} & A_{d+n-2} & \cdots & A_{d+1} & A_d
\end{bmatrix}
\]

\[
Z := \begin{bmatrix}
\zeta^0 & 0 & \cdots & 0 & 0 \\
0 & \zeta^{-1} & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \zeta^{-(n-2)} & 0 \\
0 & 0 & \cdots & 0 & \zeta^{-(n-1)}
\end{bmatrix}
\]

\[
M := A - yZ \\
N := \text{adj } M
\]

The goal is to prove the following proposition.

**Proposition 1.1.** There is an effective degree $g$ divisor $D$ on $C$ such that

$$(1 - \zeta)D \sim P - \infty$$

The divisor $D$ can be expressed as

$$D = \gcd_{1 \leq j \leq n} \text{div}_0 N_{1,j}.$$  

2. Computational Lemmas

**Definition 2.1.** Let $L = K[x, y]/(y^n - f(x))$, the affine coordinate ring of $C$. We define $\sigma$ to be the automorphism of $L$ sending $y \mapsto \zeta^{-1} y$.

From now on we work in the ring $L$, upon which $\sigma$ acts. We also consider the entries of $A, Z, M, N$ as elements of $L$.

**Lemma 2.2.** Choose $T$ such that $T^n + (-1)^n x = 0$. For $1 \leq k \leq n$, define

$$\lambda_k := \prod_{i=1}^d (r_i + \zeta^k T) = A_d + \zeta^k T A_{d-1} + \cdots + \zeta^{k(n-1)} T^{n-1} A_{d-n+1}.$$  

Then the $\lambda_k$ are all the eigenvalues of $A$.

**Proof.** An eigenvector of $A$ with eigenvalue $\lambda_k$ is $v_k = [1 \quad \zeta^k T \quad \cdots \quad \zeta^{(n-1)k} T^{n-1}]^T$.  

$\square$
Lemma 2.3. We have

\[ \det A = \prod_{i=1}^{d} (x + \alpha_i) \]

\[ \det M = \prod_{i=1}^{d} (x + \alpha_i) - y^n. \]

Proof. The first equality comes directly from multiplying the eigenvalues computed in Lemma 2.2 and by observing that

\[ n \prod_{k=0}^{n-1} (r_i - \zeta^k T) = r_i^n - (-1)^n T^n = \alpha_i + x. \]

From degree considerations, \( \det M \) is a polynomial in \( y \) of degree exactly \( n \), with leading term given by \( \prod_{i=1}^{d} (x + \alpha_i) \). Moreover \( \det M \) is invariant under \( \sigma \), as \( \sigma M \) can be obtained from \( M \) by permuting the rows and columns by the permutation \( (1 \ n \ n \ - \ 2) \). Therefore \( \det M \) can have no other terms in \( y \), so it is of the form \( \det M = q(x) - y^n \). By plugging in \( y = 0 \) we see that \( q(x) = \det(A - 0 \cdot Z) = \det A \), so the rest comes from the computation of \( \det A \).

Now we seek to understand how the automorphism \( \sigma \) of \( L \) operates on the entries of \( N \).

We do so in Lemma 2.5 and the following notation makes it easier to express those relations.

Definition 2.4. Define \( \delta_{i,t} \) to be the indicator function of \( \{i \equiv t \mod n\} \), so that

\[ \delta_{i,t} = \begin{cases} 1 & \text{if } i \equiv t \mod n \\ 0 & \text{otherwise.} \end{cases} \]

Lemma 2.5. We have the relation

\[ N_{i+1,j+1} = ((-1)^{n-1} x)^{\delta_{j,n-\delta_{i,n}}} \cdot \sigma N_{i,j} \]

Proof. First, we claim that the same relation holds for \( M \); namely, that

\[ M_{i+1,j+1} = ((-1)^{n-1} x)^{\delta_{j,n-\delta_{i,n}}} \cdot \sigma M_{i,j} \]

This follows from the fact that \( A_{\ell+n} = (-1)^{n-1} x A_{\ell} \) and the fact that for \( 1 \leq i,j \leq n \) we have \( M_{i,j} = A_{d+i-j} - \delta_{i,j} \zeta^{1-i} y \).

Now consider the relation for \( N \). We will verify it for \( (x, y) \in A^2 \setminus C \). This equation describes a closed condition, so it will follow that it holds on all of \( A^2 \). When \( (x, y) \notin C \) we know from Lemma 2.3 that \( M \) is invertible, so the equation \( MN = (\det M)I \) uniquely determines \( N \).

Define \( N' \) to be the matrix whose \((i+1,j+1)\)-th entry is \(((-1)^{n-1} x)^{\delta_{j,n-\delta_{i,n}}} \cdot \sigma N_{i,j} \). Hence it suffices to verify that \( MN' = (\det M)I \). We will check this using the relation for \( M \) and the
fact that $MN = (\det M)I$. We have

$$
(MN')_{i+1,j+1} = \sum M_{i+1,k+1}N'_{k+1,j+1} = ((-1)^{n-1}x)^{\delta_{i+1,n}-\delta_{i+1,n}} \sum \sigma M_{i,k} \sigma N_{k,j} = ((-1)^{n-1}x)^{\delta_{i+1,n}-\delta_{i+1,n}} \sigma ((MN)_{i,j}) = ((-1)^{n-1}x)^{\delta_{i+1,n}-\delta_{i+1,n}} \delta_{i,j} \cdot (\sigma (\det M)) = \delta_{i,j} \cdot (\det M),
$$

where the last line follows as both sides are zero whenever $i \neq j$.

Lemma 2.6. For $1 \leq i, j \leq n$ we have

$$
\text{div } N_{i,j} \geq \sum_{k=j-n+1}^{i-2} \zeta^k P.
$$

Proof. Using (1) from Lemma 2.5 reduces us to the case of checking this for $i = 1$. Since $N_{i,j}$ is $(-1)^{i+j}$ times the determinant of the submatrix of $M$ obtained by deleting the $j$-th row and $i$-th column, it suffices to check that this submatrix has vanishing determinant at the points $(0, \zeta^{-n}s_d), (0, \zeta^{-n+1}s_d), \ldots, (0, \zeta^{-1}s_d)$. We may as well then set $x = 0$ in this submatrix. Using that $A_\ell(0) = 0$ for $\ell \geq d + 1$ and $A_\ell(0) = s_\ell$ for $\ell \leq d$, the submatrix in consideration (obtained by deleting the first row and $j$-th column of $M$) is of the form

$$
\begin{bmatrix}
U & V \\
0 & W
\end{bmatrix}
$$

where

$$
U = \begin{bmatrix}
s_{d-1} & s_{d-2} & s_{d-3} & \cdots & s_{d-j+1} \\
s_d - \zeta^{-1}y & s_{d-1} & s_{d-2} & \cdots & s_{d-j+2} \\
s_d - \zeta^{-2}y & s_{d-1} & s_{d-2} & \cdots & s_{d-j+3} \\
& \ddots & \ddots & \ddots & \ddots \\
s_d - \zeta^{2-j}y & s_{d-1}
\end{bmatrix}
$$

$$
V = \begin{bmatrix}
s_{d-j} & s_{d-j-1} & \cdots & s_{d-n+1} \\
s_{d-j+1} & s_{d-j} & \cdots & s_{d-n+2} \\
s_{d-j+2} & s_{d-j+1} & \cdots & s_{d-n+3} \\
& \ddots & \ddots & \ddots & \ddots \\
s_{d-2} & s_{d-3} & \cdots & s_{d-n+j-1}
\end{bmatrix}
$$

$$
W = \begin{bmatrix}
s_d - \zeta^{-j}y & s_{d-1} & \cdots & s_{d-n+j+1} \\
s_d - \zeta^{-(j+1)}y & s_{d-1} & \cdots & s_{d-n+j+2} \\
& \ddots & \ddots & \ddots & \ddots \\
s_d - \zeta^{-(n-1)}y
\end{bmatrix}
$$

Hence the determinant of this submatrix is $\det U \cdot \det W$, and $\det W$ vanishes when $y \in \{\zeta^1s_d, \ldots, \zeta^{n-1}s_d\}$, as desired.

Lemma 2.7. The rank of $A$ is always at least $n - 1$ (for any $x$).
Proof. The eigenvalues of $A$ were computed in Lemma 2.2. If $\lambda_k$ and $\lambda_\ell$ were both simultaneously zero, then there exist $i,j$ such that $T = -\zeta^k r_i$ and $T = -\zeta^\ell r_j$. Hence $(-T)^n$ simultaneously equals both $r_i^n = \alpha_i$ and $r_j^n = \alpha_j$, so $i = j$ (as the $\alpha_i$ were assumed to be distinct). Then $\zeta^k = -r_i T^{-1} = -r_j T^{-1} = \zeta^\ell$, so $\lambda_k = \lambda_\ell$. Hence at most one eigenvalue is zero, so the rank of $A$ is at least $n - 1$. □

Lemma 2.8. The rank of $M$ is always at least $n - 1$, as $(x,y)$ varies in $A^2$.

Proof. From linear algebra, the rank of a matrix $F$ is at most $n - 2$ if and only if $\text{adj} F = 0$.

Consider the matrix $N + \sigma N + \cdots + \sigma^{n-1} N$; it is $\sigma$-invariant and it involves powers of $y$ only between 0 and $n - 1$, so it is independent of $y$. Hence

$$(N + \sigma N + \cdots + \sigma^{n-1} N)(x,y) = (N + \sigma N + \cdots + \sigma^{n-1} N)(x,0) = nN(x,0) = n \text{adj} A(x).$$

For contradiction suppose there exists some point $Q$ where the rank of $M$ is at most $n - 2$. Let $Q = (Q_x, Q_y)$ be its coordinates. Then $N(Q_x, Q_y) = 0$. By Lemma 2.5 we know that $N + \sigma N + \cdots + \sigma^{n-1} N$ also vanishes at $Q$. The above computation gives that $n \cdot \text{adj} A(Q_x) = 0$. As the characteristic of $k$ is coprime to $n$ we conclude that $\text{adj} A(Q_x) = 0$, so that $A(Q_x)$ has rank at most $n - 2$, contradicting Lemma 2.7. □

Lemma 2.9. Any $2 \times 2$ submatrix of $N$ has determinant 0 when evaluated on points on $C$.

Proof. Since $MN = (\text{det} M) I$ and $\text{det} M$ is the equation of $C$ (by Lemma 2.3), it follows that $MN = 0$ for points on $C$. Therefore the image of $N$ is contained in the kernel of $M$, which has dimension at most 1 since the rank of $M$ is at least $n - 1$. Hence the image of $N$ is at most one-dimensional, which means any $2 \times 2$ submatrix has zero determinant. □

3. Main Proof

3.1. Vanishing loci of $N_{i,j}$.

Definition 3.1. Let $Q_{i,j} = \text{div} \sum_{k=j-n}^{i-2} \zeta^k P$. By Lemma 2.6 we know that $Q_{i,j} \geq 0$; all the $Q_{i,j}$ are effective divisors on $C$.

Our first task is to translate the lemmas in the previous section to results about $Q_{i,j}$.

Lemma 3.2. For $1 \leq i, j \leq n$, there exist effective divisors $D_i$, $E_j$ with the property that

$$D_i + E_j = Q_{i,j}.$$

Proof. From Lemma 2.9 we obtain

$$(2) \quad Q_{i,j} + Q_{k,\ell} = Q_{i,\ell} + Q_{k,j}$$

Now define

$$D_i = \gcd_{1 \leq k \leq n} Q_{i,k}$$

$$E_j = Q_{1,j} - \gcd_{1 \leq k \leq n} Q_{1,k}$$
Note that $D_i \geq 0$ always holds since $Q_{i,k} \geq 0$ for all $i, k$. By definition of gcd, $E_j \geq 0$ also holds. Hence the $D_i, E_j$ are effective divisors with the property that

$$D_i + E_j = \gcd_{1 \leq k \leq n} Q_{i,k} + Q_{1,j} - \gcd_{1 \leq k \leq n} Q_{1,k}$$

$$= \left( \gcd_{1 \leq k \leq n} Q_{i,1} - Q_{1,1} + Q_{1,k} \right) + Q_{1,j} - \gcd_{1 \leq k \leq n} Q_{1,k} \quad \text{(by applying equation [2])}$$

$$= (Q_{i,1} - Q_{1,1}) + \left( \gcd_{1 \leq k \leq n} Q_{1,k} \right) + Q_{1,j} - \gcd_{1 \leq k \leq n} Q_{1,k}$$

$$= Q_{i,1} - Q_{1,1} + Q_{1,j}$$

$$= Q_{i,j}. \quad \text{(by applying equation [2])}$$

**Lemma 3.3.** Choose $D_i, E_j$ as in Lemma 3.2. Then

$$\gcd_{1 \leq i \leq n} D_i = \gcd_{1 \leq j \leq n} E_j = 0.$$

**Proof.** If there existed a point $X$ on $C$ such that $Q_{i,j} \geq X$ for all $i, j$, then all the $N_{i,j}$ would vanish on $X$. Then $X$ would be a point of $C$ for which rank $M \leq n - 2$, contradicting Lemma 2.8. Therefore $0 \geq \gcd_{i,j} Q_{i,j}$. As each $Q_{i,j}$ is effective itself, we get the reverse inequality $\gcd_{i,j} Q_{i,j} \geq 0$. Hence

$$\gcd_{1 \leq i,j \leq n} Q_{i,j} = 0.$$

From Lemma 3.2 we know that

$$\gcd_{1 \leq i \leq n} D_i + \gcd_{1 \leq j \leq n} E_j = \gcd_{1 \leq i,j \leq n} Q_{i,j}$$

and that $\gcd_{i} D_i, \gcd_{j} E_j$ are both effective. Therefore $\gcd_{i} D_i, \gcd_{j} E_j$ are effective divisors whose sum is 0; hence they must both be 0. □

**Proposition 3.4.** There exist effective divisors $D, E$ on $C$ such that for $1 \leq i, j \leq n$, we have

$$\operatorname{div}_0 N_{i,j} = \zeta^{i-1}D + \zeta^{j-1}E + \sum_{k=j-n}^{i-2} \zeta^k P.$$

**Proof.** Choose $D_i, E_j$ as in Lemma 3.2. Then Lemma 2.5 implies $Q_{i+1,j+1} = \zeta Q_{i,j}$, which translates to

$$D_{i+1} + E_{j+1} = \zeta D_i + \zeta E_j$$

Taking $\gcd_j$ of both sides of the above equations and applying Lemma 3.3 produces

$$D_{i+1} = \zeta D_i.$$

Similarly,

$$E_{j+1} = \zeta E_j.$$

Define $D = D_1$ and $E = E_1$, so that we have

$$Q_{i,j} = \zeta^{i-1}D + \zeta^{j-1}E.$$

Putting this information together into the definition of $Q_{i,j}$ gives the proposition. □
It remains to compute the order of the poles at the point at infinity.

3.2. Orders at infinity.

**Lemma 3.5.** There are no principal divisors on \( C \) having a pole only at \( \infty \) such that the pole order at \( \infty \) is \( nd - n - d \).

**Proof.** Let \( R \) be the ring \( R = K[x, y]/(y^n - \prod_{i=1}^{d}(x + \alpha_i)) \); this is the affine coordinate ring of \( C \). Note that a \( K \)-basis for \( R \) is given by \( \{x^ay^b : 0 \leq a \text{ and } 0 \leq b \leq n - 1\} \). Then \( v_\infty(x^ay^b) = na + db \), so coprimality of \( d, n \) implies that each element of this basis has a different order pole at \( \infty \). Therefore, the order of the pole at \( \infty \) of any element of \( R \) is of the form \( na + db \) for nonnegative \( a, b \).

If \( \text{div}(f) \) is a principal divisor on \( C \) having only a pole at \( \infty \), then \( f \in R \). From the previous paragraph, we have \( v_\infty(f) = na + db \) for nonnegative \( a, b \).

If it were the case that \( na + db = nd - n - d \), then \( a \equiv -1 \pmod{d} \) and \( b \equiv -1 \pmod{n} \), so by nonnegativity of \( a, b \) we conclude that \( a \geq d - 1 \) and \( b \geq n - 1 \). But then

\[
nd - n - d = na + db \geq (nd - n) + (nd - d) = 2nd - n - d,
\]

which is a contradiction. \( \square \)

**Proposition 3.6.** Let \( C \) be a superelliptic curve cut out by the following equation in \( \mathbb{P}^2 \).

\[
y^n = f_d(x)
\]

where \( n, d \) are coprime and \( f_d \) is a separable polynomial of degree \( d \). Let \( \infty \) be the point at infinity of \( C \) (it is unique) and use that to produce a map \( C \to J \). Identify \( C \) with its image in the jacobian \( J \) and let \( \Theta \subseteq J \) be the theta divisor. Then

1. the intersection of \( C \) and \( (1 - \zeta)\Theta \) in \( J \) is exactly \( \{0\} \).
2. the intersection of \( C \) and \( (\zeta - 1)\Theta \) in \( J \) is also exactly \( \{0\} \).

**Proof.** Both parts are similar to prove, so we prove the former.

Suppose there were a point \( P \neq \infty \) on \( C \) and a divisor \( D \in \Theta \) such that \( (1 - \zeta)D \sim P - \infty \) and \( v_\infty(D) = 0 \). Then \( D \) is effective of degree \( r \) where \( r \leq g - 1 \). Let \( E \) be an effective divisor of degree \( s \leq g \) such that \( D + E \sim (r + s)\infty \) and \( v_\infty(E) = 0 \). Define

\[
t = (2g - 1) - (r + s).
\]

By assumption, \( t \geq 0 \). Consider the following divisor \( F \) defined as

\[
F = \zeta^tD + E + \sum_{i=0}^{t-1}\zeta^iP.
\]

Notice that

\[
F = \zeta^tD + E + \sum_{i=0}^{t-1}\zeta^iP
\]

\[
\sim \zeta^tD - D + \sum_{i=0}^{t-1}(\zeta^iD - \zeta^{i+1}D) + (r + s + t)\infty
\]

\[
= 0 + (r + s + t)\infty
\]

\[
= (nd - n - d)\infty.
\]
Since \( v_\infty(F) = 0 \) and \( F \sim (nd-n-d)\infty \), this contradicts Lemma 3.5. This contradiction implies that \( D \) could not have been on \( \Theta \).

We have shown the following so far.

**Proposition 3.7.** There exist an effective divisors \( D, E \) on \( C \) such that for \( 1 \leq i, j \leq n \), we have

\[
\text{div } N_{i,j} = \zeta^{i-1} D + \zeta^{j-1} E + \sum_{k=j-n}^{i-2} \zeta^k P - (2g + (i-1) + (n-j))\infty.
\]

**Proof.** The only new statement (compared to Proposition 3.4) is about \( v_\infty(N_{ij}) \), so it suffices to check that \( \deg D = \deg E = g \).

Proposition 3.4 implies that \( D \) satisfies \( (1 - \zeta) D = P \) and \( E \) satisfies \( (\zeta - 1) E = \zeta P \). Therefore if either \( \deg D < g \) or \( \deg E < g \) then this would contradict Proposition 3.6, so this completes the proof.

3.3. **Proof of 1.1.** Now we can finally finish the proof of Proposition 1.1. It suffices to check that \( \gcd_{1 \leq j \leq n} \text{div}_0 N_{1,j} = D \). From Proposition 3.7 we have

\[
\begin{align*}
\text{div}_0 N_{1,n} &= D + \zeta^{n-1} E \\
\text{div}_0 N_{1,n-1} &= D + \zeta^{n-2} E + \zeta^{-1} P \\
\text{div}_0 N_{1,n-2} &= D + \zeta^{n-3} E + \zeta^{-1} P + \zeta^{-2} P \\
&\vdots \\
\text{div}_0 N_{1,1} &= D + E + \zeta^{-1} P + \cdots + \zeta^{-(n-1)} P,
\end{align*}
\]

from which it is follows that

\[
\gcd_{1 \leq j \leq n} \text{div}_0 N_{1,j} \geq D.
\]

Suppose now for contradiction that there exists some point \( Q \) such that

\[
Q \leq \gcd_{1 \leq j \leq n} (\text{div}_0 N_{1,j} - D).
\]

Then for each \( 1 \leq j \leq n \) we have

\[
(3) \quad Q \leq \zeta^{n-j} E + \sum_{k=1}^{j-1} \zeta^{-k} P.
\]

By Lemma 3.3, there must be some \( U \) such that \( Q \nleq \zeta^{n-U} E \). Then we have

\[
Q \leq \sum_{k=1}^{U-1} \zeta^{-k} P
\]

From the last inequality, it follows that \( Q = \zeta^{-V} P \) for some \( V \) satisfying \( 1 \leq V \leq U - 1 \) (in particular, \( U \geq 2 \)).

Now either \( P \) is fixed by \( \zeta \) or it is not. We will show that in either case, we have \( P \leq E \).

Suppose first that \( P \) is fixed by \( \zeta \). Substituting \( j = 1 \) into equation (3) produces \( Q \leq \zeta^{n-1} E \), so we conclude that \( \zeta Q \leq E \), and consequently that \( P \leq E \) (since \( \zeta Q = \zeta^{V+1} P \) and we assume that \( \zeta \) fixes \( P \)).
Now suppose that $P$ is not fixed by $E$, in which case the $\zeta^{-k}P$ are distinct. Applying equation (3) with $j = V$ then gives

$$ Q \leq \zeta^{n-V}E + \sum_{k=1}^{V-1} \zeta^{-k}P $$

Since $Q = \zeta^{-V}P$ and the $\zeta^{-k}P$ are distinct, we conclude that $\zeta^{-V}P \leq \zeta^{n-V}E$, which implies that $P \leq E$.

Hence in both cases we conclude that $P \leq E$. Now let $E' = \zeta^{-1}E - \zeta^{-1}P$; since $P \leq E$, we see that $E'$ is an effective degree $g-1$ divisor on $C$ satisfying

$$ (\zeta - 1)E' = (\zeta - 1)\zeta^{-1}E - (\zeta - 1)\zeta^{-1}P $$

$$ \sim (\zeta - 1)(2g\infty - D) - (P - \zeta^{-1}P) $$

$$ \sim (\zeta - 1)(-D) - (P - \zeta^{-1}P) $$

$$ = (1 - \zeta)(D) - (P - \zeta^{-1}P) $$

$$ \sim P - \infty - (P - \zeta^{-1}P) $$

$$ = \zeta^{-1}P - \infty, $$

which contradicts part (2) of Proposition 3.7.

4. VARYING THE CHOICE OF $x_i$

Since the definition of $D$ depends on the choice of $x_i$, we will write $D_{r_1,\ldots,r_d}$ to denote the divisor in Proposition 1.1. Recall that if $P = (0,b)$, then the $x_i$ are chosen to be any collection of $n$ elements of $K$ satisfying

$$ r_i^n = \alpha_i $$

$$ \prod r_i = b. $$

In particular, it is a consequence of our main proposition that

$$ (1 - \zeta)D_{\zeta^{-a_1r_1},\ldots,\zeta^{-a_dr_d}} \sim \zeta^{-(a_1+\cdots+a_d)}P - \infty $$

Consequently, the divisor

$$ D_{r_1,\ldots,r_d} - \zeta^{a_1+\cdots+a_d}D_{\zeta^{-a_1r_1},\ldots,\zeta^{-a_dr_d}} $$

is a degree zero $(1 - \zeta)$-torsion divisor. The following proposition tells us which one it is.

**Proposition 4.1.** For any collection of integers $a_1,\ldots,a_d$ we have

$$ D_{r_1,\ldots,r_d} - \zeta^{a_1+\cdots+a_d}D_{\zeta^{-a_1r_1},\ldots,\zeta^{-a_dr_d}} \sim a_1(-\alpha_1,0) + \cdots + a_d(-\alpha_d,0) - \left(\sum a_j\right)\infty. $$

**Proof.** By induction, it suffices to treat the case $(a_1,\ldots,a_d) = (1,0,\ldots,0)$. To do so, we will first reformulate Proposition 1.1 in terms of a family over $\text{Spec} \, K[r_1,\ldots,r_d]$.

Consider the superelliptic curve $C$ over $A_K^d = \text{Spec} \, K[r_1,\ldots,r_d]$ given by the equation

$$ y^n = \prod_{i=1}^d (x + r_i^n). $$
This curve has a unique point at $\infty$, and it maps into its jacobian $\mathcal{J}$ via the Abel-Jacobi map. We have written formulas for dividing the point $(0, \prod r_i)$ on $\mathcal{C}$ by $1 - \zeta$.

The calculation before the statement of the proposition shows that the map

$$(r_1, \ldots, r_d) \mapsto D_{r_1, \ldots, r_d} - \zeta D_{1, r_1, r_2, \ldots, r_d}$$

defines an algebraic map $\mathbb{A}_K^d \to \mathcal{J}[1 - \zeta]$. Since the space $\mathcal{J}[1 - \zeta]$ is discrete and $\mathbb{A}_K^d$ is connected, it follows that this map must be constant. Suppose then that the image is

$$b_1(-r_1^n, 0) + \ldots + b_d(-r_d^n, 0) - \left(\sum b_i\right) \infty$$

where $0 \leq b_i < n$. Restricting to the hyperplane cut out by $r_1 = 0$, it follows that

$$D_{0, r_2, \ldots, r_d} - \zeta D_{0, r_2, \ldots, r_d} \sim b_1(0, 0) + b_2(-r_2^n, 0) + b_d(-r_d^n, 0) - \left(\sum b_i\right) \infty.$$  

Note that the left hand side is precisely $(1 - \zeta)D_{0, r_2, \ldots, r_d}$, so that Proposition 1.1 implies this is equal to $(0, 0) - \infty$. From this we conclude we may choose $(b_1, \ldots, b_d) = (1, 0, \ldots, 0)$, as desired.

**Remark 4.2.** From Proposition 4.1, it follows that our formula in Proposition 1.1 produces every effective degree $g$ divisor $D$ satisfying $(1 - \zeta)D \sim P - \infty$.

5. Intersection of $(1 - \zeta)^{-1}\mathcal{C}$ and $\Theta$

In this section, we will work over the complex numbers; that is, $K = \mathbb{C}$.

From Proposition 3.6 it follows that $(1 - \zeta)^{-1}\mathcal{C}$ and $\Theta$ must intersect exactly at the $(1 - \zeta)$-torsion points. In this section, we will compute the intersection multiplicities of this intersection at each such point.

From now on, we write $\mathcal{C}'$ to denote $(1 - \zeta)^{-1}\mathcal{C}$ and $\iota': \mathcal{C}' \to J$ to denote the inclusion map.

**Definition 5.1.** Let $P_i \in \mathcal{C}$ be the superelliptic branch points $P_i = (-\alpha_i, 0)$.

**Lemma 5.2.** Let $D \in J[1 - \zeta]$. Then $D$ has a unique representation of the form

$$D \sim a_1P_1 + \cdots + a_{d-1}P_{d-1} - (a_1 + \cdots + a_{d-1}) \infty.$$

where $0 \leq a_j < n$.

**Proof.** Note that there are $n^{d-1}$ choices for the $a_i$, which is exactly the number of $(1 - \zeta)$-torsion divisors (since multiplication by $1 - \zeta$ has degree $n^{d-1}$ on $J$). It suffices to check that these are all distinct. Using the relations $n(P_i - \infty) \sim 0$, it suffices to check that if the divisor $a_1P_1 + \cdots + a_{d-1}P_{d-1}$ is principal, then all the $a_i$ are zero. Suppose we have a function $f(x, y)$ such that

$$\text{div } f(x, y) = (a_1P_1 + \cdots + a_{d-1}P_{d-1}) - (a_1 + \cdots + a_{d-1}) \infty.$$  

Then $f(x, y)$ is necessarily a polynomial since its poles are only at $\infty$. Moreover, since the above is a $1 - \zeta$ torsion divisor, it follows that $\text{div } f(x, \zeta y) = \text{div } f(x, y)$, so

$$f(x, \zeta y) = cf(x, y) \quad (4)$$

for some constant $c$.

From the proof of Lemma 3.5 we may assume that $f(x, y)$ is a $\mathbb{C}$-linear combination of $x^ay^b$ where $na + db \leq \sum a_i \leq (n - 1)(d - 1)$. By comparing coefficients on both sides of
equation \([4]\) it follows that \(f(x, y) = y^k g(x)\) for some polynomial \(g(x)\). If \(k \geq 1\) then \(f(x, y)\) would have to vanish at \(P_d\), but it does not. Hence \(k = 0\) and \(f(x, y) = g(x)\). But this means that at the points where \(f\) vanishes, it must vanish to an order that is divisible by \(n\). Hence all the \(a_i\) must be zero. \(\square\)

**Definition 5.3.** Fix a point \(P \in C\) and a divisor \(D \in J\). An integer \(\ell\) is a gap of \(D\) with respect to \(P\) if there is no meromorphic section of \(D\) that is (i) holomorphic everywhere except at \(P\) and (ii) has a pole of exact order \(\ell\) at \(P\). In other words, \(\ell\) is a gap if
\[
h^0(L(D + \ell P)) = h^0(L(D + (\ell - 1)P)).
\]

From Riemann-Roch, it follows that if \(D\) is a degree zero divisor, then the set of gaps is a subset of \(\{0, 1, \ldots, 2g - 1\}\) of size \(g\).

We recall the definition of inflectionary weight as in [Bir03].

**Definition 5.4.** Fix a point \(P \in C\) and a divisor \(D \in J\). Let \(0 \leq \ell_1 < \ell_2 < \cdots < \ell_g \leq 2g - 1\) be the gaps of \(D\) with respect to \(P\). Then the inflectionary weight of \(P\) with respect to \(D\), denoted \(w_P(D)\), is
\[
w_P(D) = \sum_{i=1}^{g} (\ell_i - (i - 1)).
\]

**Definition 5.5.** For any \(D \in C' \cap \Theta\), let \(i(D)\) be the intersection multiplicity of \(C'\) and \(\Theta\).

Now we can state the main proposition of this section.

**Proposition 5.6.** For any \(D \in C' \cap \Theta\), we have the equality
\[
i(D) = w_\infty(D).
\]

Equivalently,
\[
(i')^*\Theta = \sum_{D \in C' \cap \Theta} w_\infty(D)D.
\]

This proposition will be proved at the end of the section. We first need a few lemmas.

We would like to characterize the non-gaps of a particular divisor \(D\). To do so, we define the following.

**Definition 5.7.** Let \(R\) be the ring
\[
R = \mathbb{Z}[X_1, \ldots, X_d]/(X_1^n - 1, \ldots, X_d^n - 1, X_1 \cdots X_d - 1)
\]
It has a natural basis of the form \(\{X_1^{a_1} \cdots X_d^{a_{d-1}} : 0 \leq a_j < n\}\). Consider the projection maps
\[
pr_{a_1,\ldots,a_{d-1}} : R \to \mathbb{Z}
\]
that extract the \(X_1^{a_1} \cdots X_d^{a_{d-1}}\)-coefficient. By abuse of notation, we also use \(pr_{a_1,\ldots,a_{d-1}}\) to denote the same map, but tensored up to \(\mathbb{Z}[T]\):
\[
pr_{a_1,\ldots,a_{d-1}} : R[T] \to \mathbb{Z}[T]
\]
Finally, define \(\rho \in R[T]\) as
\[
\rho = (1 + T^n + T^{2n} + \cdots) \cdot \prod_{i=1}^{d}(1 + X_i T + \cdots + X_i^{n-1}T^{n-1})
\]
and define \( \rho_{a_1,..,a_{d-1}} \in \mathbb{Z}[T] \) as

\[
\rho_{a_1,..,a_{d-1}} = \text{pr}_{a_1,..,a_{d-1}}(\rho).
\]

The next proposition (and its corollary) explains the connection between \( \rho_{a_1,..,a_{d-1}} \) and the non-gaps of a \((1 - \zeta)\)-torsion divisor in Lemma 5.2.

**Proposition 5.8.** Let \( D \in J[1 - \zeta] \) be of the form

\[
D \sim a_1 P_1 + \cdots + a_{d-1} P_{d-1} - (a_1 + \cdots + a_{d-1}) \infty.
\]

where \( 0 \leq a_j < n \). If \( \ell(D) \) is the set of gaps of \( D \), then \( \rho_{a_1,..,a_{d-1}} \) equals

\[
\rho_{a_1,..,a_{d-1}} = \sum_{i \in \mathbb{Z}_{\geq 0} \setminus \ell(D)} T^i.
\]

In other words, \( \rho_{a_1,..,a_{d-1}} \) is sum of \( T^i \) where \( i \) ranges over all of the non-gaps.

**Proof.** Writing out an explicit sum for \( \rho \) gives

\[
\rho = \left( \sum_{f \geq 0} (T^n)^f \right) \left( \sum_{e_1,..,e_d=0}^{n-1} X_1^{e_1} \cdots X_d^{e_d} T^{e_1+\cdots+e_n} \right)
\]

\[
= \sum_{e_1,..,e_d \in [0,n-1], f \geq 0} X_1^{e_1} \cdots X_d^{e_d} T^{e_1+\cdots+e_d+nf}
\]

Using the relation \( X_1 X_2 \cdots X_d = 1 \), the above equals

\[
\rho = \sum_{e_1,..,e_d \in [0,n-1], f \geq 0} X_1^{e_1-e_d} \cdots X_d^{e_d-1-e_d} T^{(e_1-e_d)\cdots+(e_d-1-e_d)+nf+de_d},
\]

Making the change of variables \( a_j \equiv e_j - e_d \mod n \) and using the relations \( X_1^n = \cdots = X_{d-1}^n = 1 \), the above equals

\[
\rho = \sum_{a_1,..,a_{d-1},e_d \in [0,n-1], f \geq 0} X_1^{a_1} \cdots X_{d-1}^{a_{d-1}} T^{(\sum a_j)+n\left(f-\sum \left\lfloor \frac{a_j+e_d}{n} \right\rfloor \right)+de_d}
\]

and hence

\[
(5) \quad \rho_{a_1,..,a_{d-1}} = \sum_{e_d=0}^{n-1} \sum_{f \geq 0} T^{(\sum a_j)+n\left(f-\sum \left\lfloor \frac{a_j+e_d}{n} \right\rfloor \right)+de_d}
\]

First we claim that in the above series, each choice of \((e_d,f)\) gives a different exponent; that is, no terms combine. (We are assuming that the \( a_j \) are fixed now.) To see this, note: (i) considering the exponent modulo \( n \) shows that the exponent uniquely determines \( e_d \), (ii) once \( e_d \) is determined, \( f \) is also uniquely determined.

Next we claim that each exponent that arises in the expression is indeed a non-gap. An integer \( i \) is a non-gap if there exists a function \( g \) such that \( D + \text{div}(g) \) is effective everywhere but at \( \infty \), where it has a pole of exact order \( i \). To each pair \((e_d,f)\), the function

\[
g_{e_d,f} = y^{e_d}(x + \alpha_d)^f \prod_{j=1}^{d-1} (x + \alpha_j)^{-\left\lfloor \frac{a_j+e_d}{n} \right\rfloor}
\]

is effective at \( \infty \) and satisfies \( \alpha_d \equiv e_d \mod n \). Using the relation \( \alpha_j \equiv e_j - e_d \mod n \), we see that \( g_{e_d,f} \) is effective everywhere but at \( \infty \), where it has a pole of exact order \( e_d \). Thus \((e_d,f)\) is a non-gap.
satisfies
\[
\text{div}(g_{ed,f}) = \sum_{j=1}^{d-1} \left( e_d - n \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) P_j + (nf + e_d)P_d - \left( n \left( f - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) + de_d \right) \infty
\]
and hence
\[
D + \text{div}(g_{ed,f}) = \sum_{j=1}^{d-1} \left( a_j + e_d - n \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) P_j + (nf + e_d)P_d - \left( \left( \sum a_j \right) + n \left( f - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) + de_d \right) \infty
\]
is seen to be effective everywhere except at \( \infty \), where it has a pole whose order matches the exponent in the expression \([5]\).

Finally, it suffices to check that expression \([5]\) does indeed go through all the nongaps of \( D \). To do so, we may as well check that the complement of the set of exponents arising in \([5]\) is of size exactly \( g \) (since we know that all of the exponents are already non-gaps, and that there are exactly \( g \) gaps). This would then complete the proof. We show this in the following self-contained lemma.

The following lemma completes the proof of Proposition 5.8.

**Lemma 5.9.** Suppose we have integers \( a_1, \ldots, a_{d-1} \in [0, n-1] \). Define the set
\[
S = \left\{ \left( \sum a_j \right) + n \left( f - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) + de_d : e_d \in [0, n-1], f \geq 0 \right\}
\]
Then the complement set \( \mathbb{Z}_{\geq 0} \setminus S \) is finite and has size exactly \( g \).

**Proof.** Defining \( a_d = 0 \), we rewrite
\[
S = \left\{ n \left( f + \sum_{j=1}^{d} \left\{ \frac{a_j + e_d}{n} \right\} \right) : e_d \in [0, n-1], f \geq 0 \right\},
\]
where this notation \( \{x\} = x - \lfloor x \rfloor \) denotes the fractional part. Moreover, we define for \( 0 \leq e \leq n - 1 \) the following.
\[
S_e = \left\{ n \left( f + \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right) : f \geq 0 \right\}
\]
Note that \( S \) is the union of the \( S_e \), and that each element of \( S_{e} \) is \( de + (\sum a_j) \) modulo \( n \); in particular, these are distinct as \( e \) ranges in \([0, n-1] \). Hence the \( S_e \) partition \( S \) into distinct congruence classes modulo \( n \). Moreover, if \( m_e \) is the minimal element of \( S_e \), then it is clear that
\[
S_e = m_e + n\mathbb{Z}_{\geq 0}.
\]
Hence each \( (\mathbb{Z}_{\geq 0} \cap (m_e + n\mathbb{Z})) \setminus S_e \) is finite, and then taking the union over all \( e \) shows that \( \mathbb{Z}_{\geq 0} \setminus S \) is also finite.

Now we would like to determine the size of \( \mathbb{Z}_{\geq 0} \setminus S \). To do so, we do this for each \( S_e \) first:
\[
| (\mathbb{Z}_{\geq 0} \cap (m_e + n\mathbb{Z})) \setminus S_e | = \left\lfloor \frac{m_e}{n} \right\rfloor.
\]
Moreover we also know that

\[ m_e = n \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\}, \]

so we have

\[ |Z_{\geq 0} \setminus S| = \sum_{e=0}^{n-1} \left| \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right| \]

To finish, we must show this sum equals \( g \). To suppress notation, let \( a = \sum_{j=1}^{d} a_j \). Then this sum equals

\[ = n \sum_{e=0}^{n-1} \left( \frac{a + de}{n} - \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right) \]

\[ = \sum_{e=0}^{n-1} \left( n - \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right) \]

\[ = - \sum_{e=0}^{n-1} \frac{a + de}{n} + \sum_{j=1}^{d} \sum_{e=0}^{n-1} \frac{a_j + e}{n} \]

Note that the numbers \( \{a + de : e \in [0, n-1]\} \) hit each residue class modulo \( n \) exactly once. The same goes for \( \{a_j + e : e \in [0, n-1]\} \). Hence the we have that

\[ \sum_{e=0}^{n-1} \frac{a + de}{n} = \sum_{e=0}^{n-1} \frac{a_j + e}{n} = \frac{0}{n} + \frac{1}{n} + \cdots + \frac{n-1}{n} = \frac{n-1}{2}. \]

Substituting this in the previous equation gives us the desired

\[ |Z_{\geq 0} \setminus S| = - \left( \frac{n-1}{2} \right) + \sum_{j=1}^{d} \left( \frac{n-1}{2} \right) = \frac{(n-1)(d-1)}{2} = g. \]

So we have shown that \( Z_{\geq 0} \setminus S \) has size exactly \( g \). \( \square \)

This finishes the proof of Proposition 5.8. To extract the weight from \( \rho_{a_1, \ldots, a_{d-1}} \), we have the following corollary.

**Corollary 5.10.** Keeping the notation of Proposition 5.8, we have

\[ w_\infty(D) + \frac{g(g-1)}{2} = [T^2g \{ T^2(1 + T + \cdots)^2 \rho_{a_1, \ldots, a_{d-1}} \} ]. \]
where this notation on the right hand side means “the $T^{2g}$-coefficient of $T^2(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}$.”

**Proof.** Using Proposition 5.8, we see that

$$[T^{2g}]\{T^2(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}\} = [T^{2g-1}]\{T(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}\} = \sum_{i\in[0,2g-1]\setminus\ell(D)} (2g-1-i) = g(2g-1) - \sum_{i\in[0,2g-1]\setminus\ell(D)} i.$$ 

Since there are exactly $g$ gaps and they are in the range $[0, 2g-1]$, we see that

$$\sum_{i\in[0,2g-1]\setminus\ell(D)} i + \sum_{j\in\ell(D)} j = \sum_{i=0}^{2g-1} i = g(2g-1).$$

Therefore, we conclude that

$$[T^{2g}]\{T^2(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}\} = g(2g-1) - \sum_{i\in[0,2g-1]\setminus\ell(D)} i = \sum_{j\in\ell(D)} j = \frac{g(g-1)}{2} + w_{\infty}(D),$$

as desired. \[\square\]

**Lemma 5.11.** We have

$$\sum_{D\in J[1-\zeta]} w_{\infty}(D) = \frac{g(n+1)n^{d-1}}{12}.$$ 

**Proof.** We sum both sides of Corollary 5.10 over all $D \in J[1-\zeta]$. On the right hand side, the net effect is to set $X_1 = \cdots = X_d = 1$ in the power series for $\rho$. Therefore,

$$\left(\sum_{D\in J[1-\zeta]} w_{\infty}(D)\right) + \frac{g(g-1)n^{d-1}}{2} = [T^{2g}]\{T^2(1+T+\cdots)^2\rho|_{X_1=\cdots=X_n=1}\}.$$ 

Now note that

$$\rho|_{X_1=\cdots=X_n=1} = (1+Tn+T^{2n}+\cdots)(1+T+\cdots+T^{n-1})^d = (1+T+T^2+\cdots)(1+T+\cdots+T^{n-1})^{d-1},$$

so

$$\sum_{D\in J[1-\zeta]} w_{\infty}(D) + \frac{g(g-1)n^{d-1}}{2} = [T^{2g}]\{T^2(1+T+\cdots)^3(1+T+\cdots+T^{n-1})^{d-1}\}$$

Define $c_i$ so that

$$\sum_{i=0}^{(n-1)(d-1)} c_i T^i = (1 + T + \cdots + T^{n-1})^{d-1}.$$
Since \(2g = (n-1)(d-1)\), it follows that

\[
T^{2g}\{T^2(1 + T + \ldots)^3(1 + T + \ldots + T^{n-1})^{d-1}\} = \sum_{i=0}^{2g} \binom{2g - i}{2} c_i
\]

We differentiate (twice) both sides of \(7\) to get

\[
\sum_{i=0}^{2g} c_i T^i = (1 + T + \ldots + T^{n-1})^{d-1}
\]

\[
\sum_{i=0}^{2g} ic_i T^{i-1} = (d-1)(1 + 2T + 3T^2 + \ldots + (n-1)T^{n-2})(1 + T + \ldots + T^{n-1})^{d-2}
\]

\[
\sum_{i=0}^{2g} i(i-1)c_i T^{i-2} = (d-1)(2 + 6T + \ldots + (n-1)(n-2)T^{n-3})(1 + T + \ldots + T^{n-1})^{d-2} + (d-1)(d-2)(1 + 2T + 3T^2 + \ldots + (n-1)T^{n-2})^2(1 + T + \ldots + T^{n-1})^{d-3}
\]

Substituting \(T = 1\) everywhere above gives

\[
\sum_{i=0}^{2g} c_i T^i = n^{d-1}
\]

\[
\sum_{i=0}^{2g} ic_i T^{i-1} = (d-1) \left( \frac{n-1}{2} \right) n^{d-1}
\]

\[
= gn^{d-1}
\]

\[
\sum_{i=0}^{2g} i(i-1)c_i T^{i-2} = (d-1) \left( \frac{(n-1)(n-2)}{3} \right) n^{d-1} + (d-1)(d-2) \left( \frac{n-1}{2} \right)^2 n^{d-1}
\]

\[
= g \left( g + \frac{n-5}{6} \right) n^{d-1}.
\]

This allows us to conclude

\[
\sum_{i=0}^{2g} \binom{2g - i}{2} c_i = \frac{1}{2} \left( \sum_{i=0}^{2g} (i^2 - i)c_i \right) - (2g - 1) \left( \sum_{i=0}^{2g} ic_i \right) + g(2g - 1) \left( \sum_{i=0}^{2g} c_i \right)
\]

\[
= \left( \frac{1}{2} g \left( g + \frac{n-5}{6} \right) - (2g - 1)g + g(2g - 1) \right) n^{d-1},
\]

which gives

\[
\sum_{i=0}^{2g} \binom{2g - i}{2} c_i = \left( \frac{1}{2} g^2 + \frac{g(n-5)}{12} \right) n^{d-1}.
\]

Combining equations \((6)\), \((8)\), and \((9)\) finishes the proof.

\[
\Box
\]

**Lemma 5.12.** If \(D\) is a degree zero \((1 - \zeta)\)-torsion divisor that lies outside of \(\Theta\), then \(w_\infty(D) = 0\).
Proof. Since $D$ lies outside of $\Theta$, it follows that the set of gaps must contain \{0, 1, \ldots, g - 1\}; for if an integer $k \in [0, g - 1]$ is a non-gap, then there would be an effective degree $k$ divisor $E$ such that $D \sim E - k\infty$, which would then lie in $\Theta$.

Since the gap sequence contains exactly $g$ integers, it follows that the gaps are exactly \{0, 1, \ldots, g - 1\} and hence

$$w_\infty(D) = (0 - 0) + (1 - 1) + \cdots + ((g - 1) - (g - 1)) = 0,$$

as desired. \hfill \square

**Lemma 5.13.** We have

$$\sum_{D \in C' \cap \Theta} w_\infty(D) \geq \frac{g(n + 1)n^{d-1}}{12}.$$

**Proof.** Note that $C'$ contains $J[1 - \zeta]$, so

$$\sum_{D \in C' \cap \Theta} w_\infty(D) \geq \sum_{D \in J[1 - \zeta] \cap \Theta} w_\infty(D).$$

By Lemma 5.12 we know that elements of $J[1 - \zeta] \setminus (J[1 - \zeta] \cap \Theta)$ contribute no weight, so

$$\sum_{D \in J[1 - \zeta] \cap \Theta} w_\infty(D) = \sum_{D \in J[1 - \zeta]} w_\infty(D).$$

Now combining equations (10), (11), and Lemma 5.12 finishes the proof. \hfill \square

**Lemma 5.14.** We have

$$\sum_{D \in C' \cap \Theta} i(D) = \frac{g(n + 1)n^{d-1}}{12}.$$  

**Proof.** To compute the left hand side, we will work in singular cohomology with integral coefficients. Recall that $H^1(J, \mathbb{Z}) = H^1(C, \mathbb{Z}) \cong \mathbb{Z}^g$ and $H^*(J, \mathbb{Z}) = \Lambda(H^1(J, \mathbb{Z}))$.

Denote the (singular) cohomology classes dual to the cycles $C'$ and $\Theta$ by $[C']$ and $[\Theta]$, respectively. So $[C'] \in H^{g-1}(J, \mathbb{Z})$ and $[\Theta] \in H^1(J, \mathbb{Z})$. Then the total intersection of $C'$ and $\Theta$ will be

$$[C'],[\Theta] \in H^{g}(J, \mathbb{Z}) \cong \mathbb{Z}.$$

Therefore,

$$\sum_{D \in C' \cap \Theta} i(D) = [C'],[\Theta]$$

It remains to compute this intersection pairing.

A basis for $H^1(C, \mathbb{Z})$ consists of (i) the holomorphic differentials $x^i y^j \mathop{dx}$ for nonnegative integers $i, j$ satisfying $ni + dj \leq nd - n - d$ and (ii) the antiholomorphic differentials which are the conjugates of the ones in (i). Labeling the holomorphic ones as \{v_1, \ldots, v_g\}, one can easily check that these are an eigenbasis for the action by $\zeta^k$ (indeed, $x^i y^j \mathop{dx}$ has eigenvalue $\zeta^{-j}$) and that each eigenvalue of the form $\zeta^k$ for $k$ not dividing $n$ appears $g/(n - 1)$ times.
Now we write

\[
[T] = \sum_{i=1}^{g} v_i \wedge \overline{v_i}
\]

\[
[C] = \sum_{i=1}^{g} v_1 \wedge \overline{v_1} \wedge \cdots \wedge \hat{v_i} \wedge \cdots \wedge v_g \wedge \overline{v_g}.
\]

(The hat indicates that the term is not there.) A computation yields that

\[
[(1 - \zeta)^* C].[T] = \frac{g}{n - 1} \left( \prod_{j=1}^{n-1} (1 - \zeta^j) \right)^{d-1} \sum_{i=1}^{n-1} \frac{1}{(1 - \zeta^i)(1 - \zeta^{-i})}
\]

\[
= \frac{g n^{d-1}}{n - 1} \cdot \sum_{i=1}^{n-1} \frac{1}{(2i \sin \left( \frac{\pi}{n} \right))^2}
\]

\[
= \frac{g n^{d-1}}{4(n - 1)} \sum_{i=1}^{n-1} \csc^2 \left( \frac{\pi}{n} \right).
\]

This last sum is well known, and its value is \((n^2 - 1)/3\); see the next lemma. Therefore the total sum is

\[
\frac{g n^{d-1}}{4(n - 1)} \cdot \frac{n^2 - 1}{3} = \frac{g(n + 1)n^{d-1}}{12}.
\]

Lemma 5.15. We have

\[
\sum_{k=1}^{n-1} \csc^2 \left( \frac{k\pi}{n} \right) = \frac{n^2 - 1}{3}.
\]

Proof. Consider the following identity.

\[
\frac{\cos(nx) + i \sin(nx)}{\sin^n(x)} = (\cot x + i)^n.
\]

Taking the imaginary part of both sides and applying the binomial theorem gives

\[
\frac{\sin(nx)}{\sin^n(x)} = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} (-1)^j \binom{n}{2j + 1} \cot^{n-2j-1}(x).
\]

Note that the left hand side vanishes whenever \(x = k\pi/n\), so it follows by considering the right hand side that the polynomial

\[
\binom{n}{1} T^{n-1} - \binom{n}{3} T^{n-3} + \cdots + (-1)^{\lfloor (n-1)/2 \rfloor} \binom{n}{2\lfloor (n-1)/2 \rfloor + 1} T^{n-2\lfloor (n-1)/2 \rfloor + 1}
\]

has roots

\[
\cot \left( \frac{\pi}{n} \right), \cot \left( \frac{2\pi}{n} \right), \ldots, \cot \left( \frac{(n-1)\pi}{n} \right).
\]
By considering coefficients of this polynomial we see that
\[
\sum_{k=1}^{n-1} \cot^2 \left( \frac{k\pi}{n} \right) = \left( \sum_{k=1}^{n-1} \cot \left( \frac{k\pi}{n} \right) \right)^2 - \left( \sum_{k_1 \neq k_2} \cot \left( \frac{k_1\pi}{n} \right) \cot \left( \frac{k_2\pi}{n} \right) \right) \\
= 0^2 - 2 \left( \frac{-\binom{n}{3}}{\binom{n}{1}} \right) \\
= \frac{(n-1)(n-2)}{3}.
\]

Adding \( n - 1 \) to both sides then gives
\[
\sum_{k=1}^{n-1} \csc^2 \left( \frac{k\pi}{n} \right) = \sum_{k=1}^{n-1} \left( \cot^2 \left( \frac{k\pi}{n} \right) + 1 \right) = \frac{(n-1)(n-2)}{3} + (n-1) = \frac{n^2 - 1}{3},
\]
as desired. \(\square\)

**Proof of Proposition 5.6.** A basis for the space of invariant differential forms on \( C \) is given by \( z^{a-1} dx \) where \( 1 \leq a \leq d - 1 \) and \( 1 \leq b \leq n - 1 \) satisfy \( na < db \). We may choose a local coordinate \( z \) around \( \infty \) such that
\[
\frac{x^a dx}{y^b} = (z^{bd-an-1} + O(z^{bd-an})) \ dz
\]
The quantity \( bd - an \) uniquely determines the pair \((a, b)\) (assuming \( 1 \leq a \leq d - 1 \) and \( 1 \leq b \leq n - 1 \) satisfy \( na < db \)). It takes values \( 1 \leq w_1 < \cdots < w_i < \cdots < w_g \leq 2g - 1 \) and we will denote by \( \omega_i \) the invariant form corresponding to \( w_i := x^{w_i-1} dx/y^{w_i} \).

The Abel-Jacobi map then becomes
\[
P \in C(C) \mapsto \left( \int_{\infty}^{P} \omega_i \right)_{1 \leq i \leq g} \in C^g/\Lambda,
\]
where \( \Lambda \) is the period lattice of \( J \). We extend this map linearly to all of \( J(C) \) and denote this isomorphism by \( \varphi_{AJ} : J(C) \to C^g/\Lambda \).

The theta divisor \( \Theta \) is given by the vanishing of an analytic function \( \theta \) (see \cite{Mum83}, sections II.2 and II.3). We are thus interested in the order of vanishing of the composite
\[
\theta \circ \varphi_{AJ} : (1 - \zeta)^* C(C) \to \mathbb{C}
\]
at some \( D \in J(C)[1 - \zeta] \).

Let \( t := (1 - \zeta)^* z \) be a local coordinate around \( D \). Note that \((1 - \zeta)^* \omega_i = (1 - \zeta^{-b_i}) \omega_i \).

Therefore, we obtain
\[
\int_{D}^{E} \omega_i = \frac{1}{1 - \zeta^{-b_i}} \int_{D}^{E} (1 - \zeta)^* \omega_i = \frac{1}{1 - \zeta^{-b_i}} \int_{\infty}^{(1-\zeta)E} \omega_i
\]
and write the following expansion around \( D \).
\[
\varphi_{AJ} : (1 - \zeta)^* C = \left( \frac{1}{w_i(1 - \zeta^{-b_i})} t^{w_i} + O(t^{w_i+1}) \right)_{1 \leq i \leq g}
\]
Let \( u_{w_1}, \cdots, u_{w_g} \) be local coordinates on \( C^g \) around \( D \) such that \( u_{w_i} \circ \varphi_{AJ}(E) = \int_{D}^{E} \omega_i \). Then \( \theta \) has some power-series expansion around \( D \) in terms of the \( u_{w_i} \). When we pull this expansion
back to the Abel-Jacobi image of $(1 - \zeta)^* C$, we are substituting $u_{w_i} = \frac{1}{w_i(1 - \zeta^{-w_i})} t^{w_i} + O(t^{w_i+1})$ into this expansion; finding the order of vanishing is thus equivalent to finding the lowest degree term. Letting $u_{w_i}$ have weight $w_i$, we have reduced to finding the lowest weight terms in the power series expansion of $\theta$. Nakayashiki [Nak] performs this computation; we summarize his result in the following lemma.

**Lemma 5.16.** The lowest weight terms in the power series expansion of $\theta$ around $D$ have weight equal to $w_\infty(D)$.

**Proof.** To use Nakayashiki’s result, we first briefly summarize his notation. Choose a canonical homology basis $\{\alpha_i, \beta_j\}$ of $C$ and a basis of holomorphic one forms $dv_i$ normalized such that $\int_{\alpha_j} dv_i = \delta_{ij}$. Nakayashiki’s Abel-Jacobi map, denoted by $\varphi_{AJ,N}$, is defined by integrating with respect to the $dv_i$; the image of $P$ is $(\int_P dv_i)_i$. Moreover, Nakayashiki’s $\theta$-function will be denoted by $\theta_N$ and $\Theta$-divisor will be denoted by $\Theta_N$. Letting $\delta$ be Riemann’s constant, the relationship between $\Theta_N$ and $\Theta$ is $\Theta_N = \Theta - \delta$. Furthermore, the vanishing of $\theta_N \circ \varphi_{AJ,N}$ gives $\Theta_N$ and the vanishing of $\Theta \circ \varphi_{AJ}$ gives $\Theta$; hence, if we let $T_{-\delta}$ denote translation by $-\delta$, then the relation $\Theta_N = \Theta - \delta$ implies

$$\theta_N \circ \varphi_{AJ,N} \circ T_{-\delta} = \theta \circ \varphi_{AJ}$$

Let $M$ be the $g \times g$ matrix such that $\omega = M dv$ (that is, if one works with components then $\omega_i = \sum_{j=1}^g c_{ij} dv_j$) and denote $u$ to be the vector $u := (u_{w_1}, \ldots, u_{w_g})$. To be consistent with Nakayashiki’s notation, note that $du_{w_i} = \omega_i$. The relation $\omega = M dv$ implies

$$\varphi_{AJ} = M \circ \varphi_{AJ,N}.$$ 

Let $0 \leq \ell_1 < \ell_2 < \cdots < \ell_g \leq 2g - 1$ be the gaps of $D$ with respect to $\infty$ and $\lambda$ be the partition $\lambda := (\lambda_\ell, \lambda_{\ell-1}, \cdots, \lambda_1) - (g - 1, g - 2, \cdots, 0)$. Theorem 10 of [Nak] with $e = D - \delta$ then shows that for some constant $C$,

$$C \theta_N(M^{-1} u + \varphi_{AJ,N}(D - \delta)) = s_\lambda(t)|_{t_{w_i} = u_{w_i}} + \text{higher weight terms}.$$ 

Converting this to our $\theta$ and our $\varphi_{AJ}$ gives

$$C \theta(u + \varphi_{AJ}(D)) = s_\lambda(t)|_{t_{w_i} = u_{w_i}} + \text{higher weight terms}.$$ 

The Schur function $s_\lambda(t)$ is a weight-homogeneous polynomial that is defined in terms of infinitely many variables $t = (t_1, t_2, t_3, \cdots)$, but Nakayashiki shows that it only depends on the $t_{w_i}$. The weight of $s_\lambda(t)$ is $|\lambda|$, and $|\lambda| = (\lambda_g - (g - 1)) + (\lambda_{g-1} - (g - 2)) + \cdots + (\lambda_1 - 0)$ coincides with our definition of $w_\infty(D)$, so this completes the proof. \qed

Pulling back to $(1 - \zeta)^* C$, we conclude that

$$i(D) \geq w_\infty(D).$$

But now from Lemmas 5.13 and 5.14 it follows that $i(D) = w_\infty(D)$, as desired. \qed

6. **Acknowledgements**

I would like to thank my advisor, Bjorn Poonen, for suggesting the problem and for his guidance. I would also like to thank Aaron Pixton for helpful conversations regarding the computations of the intersection multiplicities.
References


