On the Shioda Conjecture for Diagonal Projective Varieties over Finite Fields

Matthew Lerner-Brecher, Benjamin Church, Chunying Huangdai, Ming Jing, Navtej Singh

January 15, 2022

1 Affine Varieties

Theorem 1.1. *Suppose X is the affine variety over F_q defined by the zero set of:*

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r}$$

For each $0 \leq i \leq r$, let $L_i = \operatorname{lcm}(\{n_j\}|_{j\neq i})$ and let $n_i' = \gcd(n_i, L_i)$. Then the affine variety X' over $\mathbb{F}_q$ defined by the zero set of:

$$a_0x_0^{n_0'} + a_1x_1^{n_1'} + \cdots + a_rx_r^{n_r'}$$

has $|X'| = |X|$.

Proof. Let $d_i = \gcd(n_i, q-1)$ and let $d_i' = \gcd(n_i', q-1)$. By equation (3) from Weil's paper we have:

$$|X| = q^r + (q-1)\sum_{\alpha\in S}\chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})j(\alpha)$$

where $S = \{\alpha = (\alpha_0,\ldots,\alpha_r) : d_i\alpha_i \in \mathbb{Z}; \sum\alpha_i \in \mathbb{Z}; 0 < \alpha_i < 1\}$. Similarly, we get:

$$|X'| = q^r + (q-1)\sum_{\alpha\in S'}\chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})j(\alpha)$$

where $S' = \{\alpha = (\alpha_0,\ldots,\alpha_r) : d_i'\alpha_i \in \mathbb{Z}; \sum\alpha_i \in \mathbb{Z}; 0 < \alpha_i < 1\}$. We will show that $S = S'$ and hence the two expressions must be equal. Note that as $n_i'|n_i$, $d_i'|d_i$. Thus $d_i'\alpha \in \mathbb{Z}$ implies $d_i\alpha \in \mathbb{Z}$. As such, $S' \subset S$. Now suppose $\alpha \in S$. If $d_i = d_i'$ for all i, the two sets are equal and we're done. As such assume j is such that $d_j' \neq d_j$. As gcd is commutative, $d_j' = \gcd(d_j, L_j)$. Then we can write, $d_j = d_j'm$. Now for each i, as $d_i\alpha_i \in \mathbb{Z}$ and $0 < \alpha_i < 1$, there exists a_i such that $\alpha_i = \frac{b_i}{d_i}$. Now, as $\alpha \in S$,

$$\frac{b_j}{d_j'm} + \sum_{i\neq j}\frac{b_i}{d_i} \in \mathbb{Z}$$

Let $\frac{B}{D} = \sum_{i\neq j}\frac{b_i}{d_i} \in \mathbb{Z}$ be a fraction in simplest form. Thus we have

$$\frac{b_j}{d_j'm} + \sum_{i\neq j}\frac{b_i}{d_i} = \frac{b_j}{d_j'm} + \frac{B}{D} = \frac{b_jD + d_j'mA}{d_j'mD} \in \mathbb{Z}$$

As $d_i|n_i|L_j$ for all $i \neq j$, we have $D|L_j$. For the above expression to be an integer we must have $d_j'm|b_jD$. As $d_j' = \gcd(d_j'm, D)$, this implies $m|b_j$. However, this means $d_j'\alpha_j = \frac{b_j}{m} \in \mathbb{Z}$. By our reasoning, this holds for all j. Thus $S' \subset S$.

As explained before, this implies $S = S'$ and thus $|X| = |X'|$. ∎

Theorem 1.2. *Let X be the affine variety over $\mathbb{F}_q$ defined by the zero set of:*

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r}$$

where the a_i are nonzero and the n_i are positive integers. If for all $1 \leq i \leq r$ we have $\gcd(n_0, n_i) = 1$, then X is supersingular.

Proof. By theorem 1.1, X has the same number of solutions as the variety X' defined by the zero set of

$$a_0x_0^{n_0'} + \cdots + a_rx_r^{n_r'}$$

As n_0 is relatively prime to the other n_i, $n_0' = 1$. However, then a_0x_0 achieves every element of $\mathbb{F}_q$ exactly once. Hence, regardless of the choice of $x_1, \ldots, x_r$ there is precisely one value of x_0 for which the defining equation of X' is 0. Thus $|X| = q^r$. By the same reasoning if we define N_k to be the number of points of X defined over $\mathbb{F}_{q^k}$, we have

$$N_k = (q^k)^r = q^{rk}$$

As such the zeta function ζ_X is:

$$\begin{aligned}\zeta_X(T) &= \exp\left(\sum_{m\geq 1} \frac{q^{rm}}{m} T^m\right) \\ &= \exp\left(-\log(1-q^rT)\right) \\ &= \frac{1}{1-q^rT}\end{aligned}$$

which implies that X is supersingular, as desired. □

2 Projective Varieties

2.1 Conversion to Weighted Projective Space

Note on notation. From now on, unless otherwise specified, let X be an affine variety over $\mathbb{F}_q$ defined to be the zero set of

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r}$$

such that the a_i are nonzero. Let $L = \operatorname{lcm}(n_i)$ and $N_i = L/n_i$. For a given point $P = (P_0, \ldots, P_r)$ let

$$S_P = \{N_i \ : \ P_i \neq 0\}$$

Let $d_P = \gcd(S_P)$. We also define V to be the image of X in weighted projective space.

Theorem 2.1. *Suppose λ acts on X as follows: For any point $(x_0, \ldots, x_r)$ we have*

$$\lambda \cdot (x_0, \ldots, x_r) = (\lambda^{N_0}x_0, \ldots, \lambda^{N_r}x_r)$$

Then for all $P = (P_0, \ldots, P_r) \in X$,

$$|\mathrm{Stab}(P)| = \gcd(S_P)$$

In particular, $P_i \neq 0$ for all i, $|\mathrm{Stab}(P)| = 1$.

Proof. Suppose $\lambda \cdot P = P$. Then we have:

$$((\lambda^{N_0} - 1)P_0, \ldots, (\lambda^{N_r} - 1)P_r) = (0, \ldots, 0)$$

This holds if and only if $\lambda^{N_i} = 1$ for all $P_i \neq 0$. This is equivalent to $\lambda^{\gcd(d_P, q-1)} = 1$, which has exactly $\gcd(d_P, q-1)$ solutions. □

Corollary 2.1.1.
$$|V| = \sum_{P\in X/\{0\}} \frac{\gcd(d_P, q-1)}{q-1}$$

Proof. By the orbit-stabilizer theorem, under the scaling action of weighted projective space, $orb(P) = \frac{q-1}{\gcd(d_P,q-1)}$. This then follows from the fact that:

$$|V| = \sum_{P\in X/\{0\}} \frac{1}{orb(P)}$$

□

We'll now introduce one more piece of notation. Suppose $t = (t_0, \ldots, t_r) \in \{0,1\}^{r+1}$. Say

$$C_t := \{P \in X \ : \ P_i = 0 \iff t_i = 0\}$$

and

$$S_t := \{N_i \ : \ t_i = 1\}$$

and as before $d_t = \gcd(S_t)$. Note that the C_ts form a partition of X. We also define an ordering on $\{0,1\}^{r+1}$. Suppose $u = (u_0, \ldots, u_r), t = (t_0, \ldots, t_r) \in \{0,1\}^{r+1}$. We say that $t \prec u$ if for all i, $u_i = 0 \implies t_i = 0$. Let

$$X_u = \bigcup_{t\prec u} C_t$$

(Note that there is a bijection between X_u and the zero set of the equation: $\sum_j a_{i_j} x^{n_{i_j}}$ where i_j ranges only over the values of i such that $u_i = 1$. We make this note because using Weil's paper we can count X_u more directly than C_u). Lastly, for convenience, let $T = \{0,1\}^{r+1}/\{(0,0,\ldots,0)\}$

Theorem 2.2.
$$|C_u| = \sum_{t\prec u} (-1)^{sum(u)-sum(t)} |X_u|$$

Proof. As the C_t are disjoin we have:
$$|X_u| = \sum_{t\prec u} |C_t|$$

Let $p_0, p_1, \ldots, p_r$ be distinct primes and for $t \in \{0,1\}^{r+1}$ let:

$$P(t) = \prod_{i=0}^{r} p_i^{t_i}$$

Let Q be the inverse of P. Note then that $P(t)|P(u)$ if and only if $t \prec u$. Thus our above equation becomes:

$$|X_u| = \sum_{d|P(u)} |C_{Q(d)}|$$

By the Mobius Inversion formula:
$$|C_u| = \sum_{d|P(u)} |X_{Q(u)}| \mu\left(\frac{P(u)}{d}\right)$$

Let $t = Q(u)$. As $P(u), d$ are squarefree, $\mu\left(\frac{P(u)}{d}\right) = \mu(P(u))/\mu(d)$. Note that $\mu(P(u)) = (-1)^{sum(u)}$. Thus, by the equivalence between $P(t)|P(u)$ and $t \prec u$, this summation is equivalent to

$$|C_u| = \sum_{t\prec u} (-1)^{sum(u)-sum(t)} |X_u|$$

as desired. □

Theorem 2.3.

$$|V| = \sum_{t \in T} |C_t| \frac{\gcd(d_t, q-1)}{q-1}$$

Proof. Note that for all $P \in C_t$, $d_P = d_t$. As the C_t form a partition of X, this formula is just a restatement of Corollary 2.1.1 □

2.2 Supersingular Projective Varieties

Lemma 2.4. *For a given prime power q and integer N. Suppose N' is the largest divisor of N relatively prime to q. Define:*

$$g(k) = \gcd(N, q^k - 1)$$

Furthermore define

$$f_r(k) = \begin{cases} 1 & r|k \\ 0 & else \end{cases}$$

Then

$$g(k) = \sum_{i=1}^{M} a_i f_i(k)$$

where $M = \text{ord}_{N'}(q)$ and

$$a_i = \sum_{d|i} g(d)\mu(i/d)$$

for $i|M$ and $a_i = 0$ otherwise with μ the moebius function.

Proof. Set a_i to be as claimed in the lemma statement. Note that

$$g(k) = \gcd(N, q^k - 1) = \gcd(N', q^k - 1)$$

By the Moebius inversion formula for $k|M$ we have:

$$g(k) = \sum_{i|k} a_i$$

As $f_i(k) = 1$ if $i|k$ and 0 otherwise this is equivalent to:

$$g(k) = \sum_{i=1}^{M} a_i f_i(k)$$

We now claim $g(k) = g(\gcd(k, M))$. Clearly if $A|q^{\gcd(k,M)} - 1$, then $A|q^k - 1$. Thus $g(\gcd(k, M))|g(k)$. Now suppose $A|q^k - 1$ for $A|N'$. As $A|N'$, $A|q^M - 1$. Thus for all x, y $A|q^{kx+My} - 1$. By Bezout's identity, $A|q^{\gcd(k,M)} - 1$. Thus $g(k)|g(\gcd(k, M))$ and so $g(k) = g(\gcd(k, M))$. Now let k be any integer. Note that a_i and $f_i(k)$ are both nonzero only if i divides M and k and hence $\gcd(i, k)$. Thus we have:

$$\sum_{i=1}^{M} a_i f_i(k) = \sum_{i|\gcd(k,M)} a_i$$

However, as $\gcd(k, M)$ divides M we have already shown the latter expression to be $g(\gcd(k, M))$. As this equals $g(k)$, we have for all k:

$$g(k) = \sum_{i=1}^{M} a_i f_i(k)$$

as desired □

Lemma 2.5. *For a given prime power q and integer N, define $g(k)$ and a_i and M as in the preceding lemma. Then for all w, we have $w|a_w$.*

Proof. If w is not a divisor of M then $a_w = 0$ and so the statement follows immediately. As such, from now on we will assume w is a divisor of M so that we may use the inversion formula for a_w.
We'll begin by showing this is true for all N, q in the case where $w = p^i$ for some prime p. We have:

$$a_w = \sum_{d|w} g(d)\mu(w/d) = g(p^i) - g(p^{i-1})$$

If $g(p^i) = g(p^{i-1})$ then we have $a_w = 0$ and so $w|a_w$. Suppose $g(p^i) \neq g(p^{i-1})$. As $q^{p^{i-1}} - 1|q^{p^i} - 1$, we have $g(p^{i-1})|g(p^i)$. Now let B be such that $g(p^i) = Bg(p^{i-1})$. Note that

$$\gcd\left(\frac{q^{p^i}-1}{q^{p^{i-1}}-1}, q^{p^{i-1}} - 1\right)$$

can only be a power of p. If $p|B$, then $p|q^{p^i} - 1$ which occurs if and only if $p|q-1$. If $p|q-1$, then by lifting the exponent lemma $p^i|q^{p^{i-1}} - 1$. So either p^i divides both $g(p^{i-1})$ and $g(p^i)$, in which case we're done or $p \nmid B$. As $p \nmid B$ and

$$\gcd\left(\frac{q^{p^i}-1}{q^{p^{i-1}}-1}, q^{p^{i-1}} - 1\right)$$

can only be a power of p, all prime factors of B cannot be factors of $q^{p^{i-1}} - 1$. Thus for all primes $t|B$ we have $q^{p^{i-1}} \not\equiv 1 \pmod t$ but $q^{p^i} \equiv 1 \pmod t$ which implies $p^i|\text{ord}_t(q)|t-1$. As for all primes $t|B$ we have $t \equiv 1 \pmod p)^i$, we have $B \equiv 1 \pmod p)^i$. Now

$$g(p^i) - g(p^{i-1}) = (B-1)g(p^{i-1})$$

and thus $p^i|g(p^i) - g(p^{i-1})$ as desired.

We'll now show that if m, n are relatively prime positive integers such that regardless of the choice of N, q we have $n|a_n$ and $m|a_m$, then $mn|a_{mn}$. For notational purposes let $g_{N,q}(k)$ be $g(k)$ for given N, q. We have

$$\begin{aligned}
a_{mn} &= \sum_{d|mn} g(d)\mu(mn/d) \\
&= \sum_{x|m} \mu(m/x) \sum_{y|n} g(xy)\mu(n/y) \\
&= \sum_{x|m} \mu(m/x) \sum_{y|n} \gcd(N, (q^x)^y - 1)\mu(n/y) \\
&= \sum_{x|m} \mu(m/x) \sum_{y|n} g_{N,q^x}(y)\mu(n/y)
\end{aligned}$$

By our assumption that regardless of the choice of N, q we have $n|a_n$ and $m|a_m$ we have $n|\sum_{y|n} g_{N,q^x}(y)\mu(n/y)$ (as the latter is the formula for a_n for N, q^x given). Thus n divides the total expression and hence a_{mn}. By symmetry, $m|a_{mn}$.

Now suppose $w = \prod_i p_i^{e_i}$. By the first part of our proof $p_i^{e_i}|a_{p_i^{e_i}}$. By the second part of our proof all of these divisibility statements together imply

$$w = \prod_i p_i^{e_i} | a_{\prod_i p_i^{e_i}} = a_w$$

as desired. ∎

Definition 2.6. Let $\frac{p(T)}{s(T)}$ be a rational function. Define $\frac{p(T)}{s(T)}$ to be *supersingular* if every root of both p, s is of the form $r\alpha$ where $r \in \mathbb{R}_{\geq 0}$ and α is a root of unity.

Theorem 2.7. *For given N, q let $g(k) = \gcd(N, q^k - 1)$. Suppose*

$$\exp\left(\sum_{k\geq 1} h(k)\frac{T^k}{k}\right)$$

defines a rational function $\frac{p(T)}{s(T)}$. Then,

$$B(T) := \exp\left(\sum_{k\geq 1} h(k)g(k)\frac{T^k}{k}\right)$$

also defines a rational function equal to

$$\prod_{i=1}^{M}\left(\frac{p_i(T^i)}{s_i(T^i)}\right)^{b_i}$$

for some integers b_i, M and with $p_k(T) = \prod_{j=1}^{k} p(Te^{\frac{2\pi i j}{k}})$ and s_k defined similarly. Furthermore, if $\frac{p(T)}{s(T)}$ is supersingular, then so is $B(T)$.

Proof. By Lemmas 2.4, for some M, we can write

$$g(k) = \sum_{i=1}^{M} a_i f_i(k)$$

Plugging this into our formula for $B(T)$ gives:

$$\begin{aligned} B(T) &= \exp\left(\sum_{k\geq 1} h(k)\sum_{i=1}^{M} a_i f_i(k)\frac{T^k}{k}\right) \\ &= \exp\left(\sum_{i=1}^{M} a_i \sum_{k\geq 1} h(k) f_i(k)\frac{T^k}{k}\right) \\ &= \exp\left(\sum_{i=1}^{M} a_i \sum_{k\geq 1} h(ik)\frac{T^{ik}}{ik}\right) \\ &= \prod_{i=1}^{M} \exp\left(\sum_{k\geq 1} h(ik)\frac{T^{ik}}{k}\right)^{\frac{a_i}{i}} \end{aligned}$$

Let

$$A(T) = \sum_{k\geq 1} h(k)\frac{T^k}{k}$$

so that $\frac{p(T)}{s(T)} = \log(A(T))$. Note note that if ζ_i is an i-th root of unity:

$$\begin{aligned} \sum_{k\geq 1} h(ik)\frac{T^{ik}}{ik} &= \frac{\sum_{j=1}^{i} A(T\zeta_i^j)}{i} \\ \exp\left(\sum_{k\geq 1} h(ik)\frac{T^{ik}}{k}\right) &= \prod_{j=1}^{i} \exp(A(T\zeta_i^j)) \\ &= \frac{p_i(T)}{s_i(T)} \end{aligned}$$

so our above expression becomes:

$$B(T) = \prod_{i=1}^{M} \left(\frac{p_i(T)}{s_i(T)} \right)^{b_i}$$

with $b_i = \frac{a_i}{i} \in \mathbb{Z}$ by Lemma 2.5. Now note that if p, s are supersingular, so are $p_i(T)$ and $s_i(T)$ and thus $B(T)$. ☐

Corollary 2.7.1. *Let V be the weighted projective space over $\mathbb{F}_q$ defined to be the zero set of*

$$x^{r_1} + x^{r_2} = 0$$

Then V is supersingular over $\mathbb{F}_{q^i}$ for some i.

Proof. Let X be the same curve just over affine space instead of projective space. Using our notation from before, note that $|C_{[0,1]}| = |C_{[1,0]}| = 0$ and $|C_{[0,0]}| = 1$ and thus $|C_{[1,1]}| = |X| - 1$. By our definitions $d_{[1,1]} = 1$. Thus:

$$|V| = \frac{|X| - 1}{q - 1}$$

Let $R = \gcd(r_1, r_2)$. By Lemma 1.1, $|X| = |X'|$ where X' is the set of solutions to

$$x_1^R + x_2^R = 0$$

over $\mathbb{F}_q$. There is one solution where one of the components is 0. If $x_1, x_2 \neq 0$, this equation is equivalent to:

$$(x_1 x_2^{-1})^R = -1$$

If $y^R = -1$ has no solutions in $\mathbb{F}_q$, the number of solutions is 0. If it does have a solution, then it has precisely $\gcd(R, q-1)$ solutions. In which case there are $(q-1)\gcd(R, q-1)$ solutions as there are R choices for which root $x_1 x_2^{-1}$, $q-1$ choices for x_1 and then 1 choice for x_2. In net, $|V| = \gcd(R, q-1)$ if $y^R = -1$ has a solution as 0 otherwise. $y^R = -1$ will have a solution if and only if $2\gcd(R, q-1) | q-1$.

Now consider when $y^R = -1$ has a solution over various $\mathbb{F}_{q^k}$. As this will depend on what the highest power of 2 divising $q^k - 1$ is (we need $v_2(q^k - 1) \geq v_2(R) + 1$), there will exist an i such that $y^R = -1$ has a solution if and only if $i|k$. Thus, over $\mathbb{F}_{q^i}$,

$$\zeta_V = \sum_{k \geq 1} \gcd(R, q^{ik} - 1) \frac{T^k}{k}$$

which is supersingular by theorem 2.7. ☐

3 Some Conjectures and Basic Theorems

Theorem 3.1. *Let X be a variety. If X is supersingular over $\mathbb{F}_q$ then it is supersingular over $\mathbb{F}_{q^k}$. Furthermore, if X is nonsingular (weighted) projective and defined by the reduction modulo p of a nonsingular variety over a number field, then if it is supersingular over $\mathbb{F}_{q^k}$ it is also supersingular over $\mathbb{F}_q$.*

Proof. Let ζ_X be the zeta function of X over $\mathbb{F}_q$:

$$\zeta_X = \exp\left(\sum_{i \geq 0} a_i \frac{T^i}{i} \right)$$

Then the zeta function ζ_{X_k} for X over $\mathbb{F}_{q^k}$ is:

$$\zeta_{X_k} = \exp\left(\sum_{i \geq 0}^{\infty} a_{ik} \frac{T^i}{i} \right)$$

Let

$$A(T) = \sum_{i \geq 0} a_i \frac{T^i}{i}$$

Let ζ be a k-th root of unity. Then

$$\frac{\sum_{j=1}^{k} A(T\zeta^j)}{k} = \sum_{i \geq 0} a_{ik} \frac{T^{ik}}{ik}$$

$$\sum_{j=1}^{k} A(T^{1/k}\zeta^j) = \sum_{i \geq 0} a_{ik} \frac{T^i}{i}$$

And thus:

$$\zeta_{X_k} = \prod_{j=1}^{k} \zeta_X(T^{1/k}\zeta^j)$$

Now suppose

$$\zeta_X = \frac{P(T)}{S(T)} = \frac{\prod_{i=1}^{m}(T - r_i)}{\prod_{i=1}^{m}(T - s_i)}$$

Then

$$\zeta_{X_k} = \pm \frac{\prod_{i=1}^{m}(T - r_i^k)}{\prod_{i=1}^{m}(T - s_i^k)}$$

which implies that ζ_{X_k} is supersingular if ζ_X is.

We'll now do the second part. WLOG assume $\frac{P}{S}$ is in simplest form. Note that the only way ζ_{X_k} is supersingular but ζ_X is not is if the roots that do not have complex unit part a root of unity cancel in ζ_{X_k}. However, by the fourth part of the weil conjectures, the numerator and denominator of the rational functions of ζ_X and ζ_{X^k} have the same degree. Thus there is no cancellation, and so ζ_X is supersingular. □

Theorem 3.2. *Given*

$$x_0^{n_0} + \cdots + x_3^{n_3} = 0$$

over field F_p, there exists d such that the variety is unirational if $q \equiv -1 \mod d$, where $d = lcm(n_0, \ldots, n_3)$.

Proof. Given

$$x_0^{n_0} + \cdots + x_3^{n_3} = 0,$$

let $l = \operatorname{lcm}(n_0, n_1, n_2, n_3)$ Let $x_i' = x_i^{l/n_i}$. Then we get a homogeneous equation of degree l, which is unirational over $\mathbb{F}_p$ if there exists a v such that $p^v \equiv -1 \mod l$ by Shioda's paper. □

Theorem 3.3. *Let X be the variety defined by*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r}.$$

If all the exponents are coprime, then X is isomorphic to the hyperplane H_{r-1} in $\mathbb{P}^r$, where r is the dimension of image of Veronese embedding.

Proof. Notice that X is in the weighted projective space $\mathbb{P}(w_0, \ldots, w_r)$. If $d = \operatorname{lcm}(n_0, \ldots, n_r)$, then $w_i = d/n_i$, and we see that our equation has weighted homogeneous degree d. Then the image of our variety by Vernose embedding will be in $\mathbb{P}^R$, and the coordinate ring of the image is generated by $y_i = x_i^{n_i}$, and these elements only.
The reason is that a monomial $\prod x_i^{a_i}$ has weighted degree d is and only if $\sum a_i w_i = d$, which is equivalent to

$$\sum \frac{a_i}{n_i} = 1$$

because we know $w_i = d/n_i$. And again, we can write this sum as

$$\frac{a_0}{n_0} + \frac{A}{N} = \frac{a_0 N + A n_0}{n_0 N} = 1, a_i \in \mathbb{Z}^+.$$

Since n_0 divides $a_0 N + An_0$, we will have $n_0 | a_0 N$. But we assume that all the exponents are coprime, so $\gcd(n_0, N) = 1$, and $n_0 | a_0$, so either $a_0 = 1$ or $a_0 = n_0$. We know that a_0 cannot be any larger because $\sum \frac{a_i}{n_i} = 1$. Therefore, we know that the only monomial that will appear in the image of Vernose embedding are of the form $y_i = x_i^{n_i}$, and there will be no other cross terms. Then we also know that the only relation that these new coordinate satisfies is the diagonal equation that we have, i. e., $y_0 + \cdots + y_r = 0$. Since a variety is isomorphic to the image of the Vernose embedding, and the image of the Vernose embedding give us a hyperplane in $\mathbb{P}^r$, we know that X is isomorphic to a hyperplane in $\mathbb{P}^r$. ☐

Theorem 3.4. *A variety X defined by*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r}.$$

in weighted projective space is singular in $\mathbb{F}_q$ if and only if (i) $q | n_i$ for some i, or (ii) in weighted projective space $\mathbb{P}(w_0, \ldots, w_r)$, there exists a prime number p such that set $x_j = 0$ when p does not divide n_j, we get a new equation that has solution over $\mathbb{F}_q$.

Proof. First, if $q | n_i$ for some i, then the Jacobian ring for X will be

$$(n_0 x_0^{n_0 - 1}, \ldots, 0, \ldots, n_r x_r^{n_r - 1}).$$

And we see that this ideal can be zero for some nonzero point. Thus (i) is true.

Second, we claim that the only singular points of the weighted projective space $\mathbb{P}(w_0, \ldots, w_r)$ are of the form

$$\mathrm{Sing}_p \mathbb{P}(w_0, \ldots, w_r) = \{x \in \mathbb{P}(w_0, \ldots, w_r) : x_i \neq 0 \text{ only if } p | w_i\}$$

for some prime p.

We contend that

$$\mathrm{Sing}\mathbb{P}(w_0, \ldots, w_r) = \bigcup \mathrm{Sing}_p \mathbb{P}(w_0, \ldots, w_r).$$

☐

Corollary 3.4.1. *If X is singular over $\mathbb{F}_q$, then it is singular over $\mathbb{F}_q^k$.*

Theorem 3.5. *Let X be a variety defined by,*

$$a_0 x^{n_0} + \cdots + a_r x^{n_r} = 0$$

over $\mathbb{F}_q$ where $q = p^f$ and let $\tilde{n}_i = \frac{n_i}{p^{v_p(n_i)}}$ i.e. n_i with all powers of p removed. Define the "base" variety $\bar{X}$ by the equation,

$$a_0 x^{\tilde{n}_0} + \cdots + a_r x^{\tilde{n}_r} = 0$$

over $\mathbb{F}_q$. Then $\bar{X}$ is smooth as an affine variety away from zero. Furthermore, There exits a bijective morphism $X \to \bar{X}$ so $\#(X) = \#(\bar{X})$ over each $\mathbb{F}_q$ and thus $\zeta_X = \zeta_{\bar{X}}$.

Proof. Let $t_i = v_p(n_i)$. Let $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$ denote the Frobenius automorphism $x \mapsto x^p$. Now we define the Frobenius morphism $X \to \bar{X}$ via $(x_0, \cdots, x_r) \mapsto (\mathrm{Frob}_p^{t_0}(x_0), \cdots, \mathrm{Frob}_p^{t_r}(x_r)) = (x_0^{p^{t_0}}, \cdots, x_r^{p^{t_r}})$. This map is well defined because if,

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

then we have,

$$a_0 (x_0^{p^{t_0}})^{\tilde{n}_0} + \cdots + a_r (x_r^{p^{t_r}})^{\tilde{n}_r} = 0$$

Clearly this map is a morphism and it is bijective because I can exhibit an inverse map, $(x_0, \cdots, x_r) \mapsto (\mathrm{Frob}_p^{-t_0}(x_0), \cdots, \mathrm{Frob}_p^{-t_r}(x_r))$. Therefore, $\#(X) = \#(\bar{X})$ over any $\mathbb{F}_q$. This implies that $\zeta_X = \zeta_{\bar{X}}$. Furthermore, as an affine variety, $\bar{X}$ has Jacobian,

$$(a_0 \tilde{n}_0 x_0^{\tilde{n}_0 - 1}, \cdots, a_r \tilde{n}_r x_r^{\tilde{n}_r - 1})$$

Since $p \nmid \tilde{n}_i$ for the Jacobian to have rank zero we must have $a_i \tilde{n}_i x_i^{\tilde{n}_i - 1} = 0 \implies x_i = 0$ for each i. Therefore, $\bar{X}$ is smooth away from zero. ☐

4 Additional Facts

Fact 4.1. A variety is rational over affine space if and only if it is rational over weighted projective space.

Fact 4.2. $\mathbb{P}(w,x,y,z) \cong \mathbb{P}(w,xd,yd,zd)$

Corollary 4.2.1. *The two varieties described in Theorem* 1.1 *are isomorphic over weighted projective space*

Fact 4.3. Let X be the variety defined by the curve:

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r} = 0$$

Let $L = \operatorname{lcm}(n_0, \ldots, n_r)$ and let $w_i = L/n_i$. If

$$\sum_i w_i - L > 0$$

then X is rational.

5 Zeta Functions

Definition 5.1. For a r-tuple of exponents n,

$$A_{n,q} = \left\{(\alpha_0, \ldots, \alpha_r) : 0 < \alpha_i < 1 \text{ and } d_i\alpha_i \in \mathbb{Z} \text{ and } \sum \alpha_i \in \mathbb{Z} \text{ where } d_i = \gcd(n_i, q-1)\right\}$$

Theorem 5.2. *The variety X defined by,*

$$x_0^{n_0} + \cdots + x_r^{n_r} = 0$$

and the variety X_a defined by,

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r} = 0$$

have equal zeta functions up to multiplication of the roots by z^{th}-roots of unity where

$$z = [E : \mathbb{F}_q]$$

and E is the splitting field of the polynomial,

$$\prod_{i=0}^{r}(x_i^n - a_i)$$

over $\mathbb{F}_q$.

Proof. Consider the variety X_a defined over E. Each a_i has all n_i^{th} roots so we can write $a_i = b_i^{n_i}$ for each i. Therefore, X_a is defined by the polynomial equation over E,

$$b_0^{n_0}x_0^n + \cdots + b_r^{n_r}x_r^{n_r} = (b_0x_0)^{n_0} + \cdots + (b_rx_r)^{n_r} = 0$$

Therefore, over E the varieties X_a and X are isomorphic via the linear E-map $(x_0, \cdots, x_r) \mapsto (b_0x_0, \cdots, b_rx_r)$ so $\zeta_{X_E} = \zeta_{X_{a,E}}$. However, the zeta function over E and over $\mathbb{F}_q$ are equal up to replacing each root and pole of ζ by a z^{th} root. Thus ζ_X and ζ_{X_a} are equal up to choices of z^{th} root and thus up to multiplications by z^{th} roots of unity. ◻

Theorem 5.3. *For the weighted projective variety (with points counted via the stack quotient) defined by*

$$a_0x_0^{n_0} + \cdots + a_rx_r^{n_r} = 0$$

over $\mathbb{F}_q$ such that $q \equiv 1 \mod (\operatorname{lcm}(n_i))$, the zeta function of X equals,

$$\zeta_X(t) = \prod_{i=0}^{r-1}\frac{1}{1-q^it} \cdot \left[\prod_\alpha\left(1 + (-1)^rB(\alpha)j_q(\alpha)t\right)\right]^{(-1)^r},$$

where $B(\alpha) = \chi_{\alpha_0}(a_0^{-1})\ldots\chi_{\alpha_r}(a_r^{-1})$ is a root of unity determined by α and the coefficients.

Proof. Notice that $A_{n,\alpha}$, the set of all possible (α_i), is the same for $\mathbb{F}_{q^k}$ for any positive integer k. The reason is that

$$q \equiv 1 \mod (\mathrm{lcm}\,(n_i)) \iff q \equiv 1 \mod n_i.$$

Then $d_i = \gcd(n_i, q-1) = n_i$, and we know $d_i \leq n_i$, so d_i will not increase as the size of field increase. Thus the set $A_{n,p}$ is completely determined by the situation in $\mathbb{F}_q$. And we shall determine $A_{n,p}$ explicitly later. By Weil's paper, the formula for the number of solution over F_q is

$$N_1 = q^r + (q-1) \sum_{\alpha \in A_{n,p}} B(\alpha) j_q(\alpha),$$

where,

$$B(\alpha) = \chi_{\alpha_0}(a_0^{-1}) \dots \chi_{\alpha_r}(a_r^{-1}) \quad \text{and} \quad j_q(\alpha) = \frac{1}{q} g(\chi_{\alpha_0}) \dots g(\chi_{\alpha_r})$$

are algebraic numbers depends on r-tuple α. Because the set of α for each extension of $\mathbb{F}_q$ are defined over $\mathbb{F}_q$ we can use the reduction formula,

$$g'(\chi'_\alpha) = -[-g(\chi_\alpha)]^k$$

where g' is the gaussian sum in the extension $\mathbb{F}_{q^k}$. Furthermore, for $x \in \mathbb{F}_q$,

$$\chi'_\alpha(x) = \chi_\alpha(x)^k$$

Therefore, the number of solution in $\mathbb{F}_{q^k}$ is,

$$N_k = q^{rk} + (q^k - 1) \sum_{\alpha \in A_{n,p}} (-1)^{(r+1)(k+1)} B(\alpha)^k j(\alpha)^k.$$

Using the stack quotient, we get the formula for the number of solution in weighted projective space:

$$N'_k = \frac{N_k - 1}{q^k - 1} = \sum_{i=0}^{r-1} (q^{ik}) + \sum_{\alpha \in A_{n,p}} (-1)^{(r+1)(k+1)} B(\alpha)^k j(\alpha)^k.$$

Thus, the zeta function becomes,

$$\begin{aligned}
\zeta_X(t) &= \exp\left(\sum_{i=0}^{r-1} \sum_{k=1}^{\infty} \frac{q^{ik}}{k} t^k + \sum_{\alpha \in A_{n,p}} (-1)^{r+1} \sum_{k=1}^{\infty} (-1)^{k(r+1)} \frac{B(\alpha)^k j(\alpha)^k}{k} t^k \right) \\
&= \exp\left(-\sum_{i=0}^{r-1} \log\left[1 - q^i t\right] - (-1)^{r+1} \sum_{\alpha \in A_{n,p}} \log\left[1 - (-1)^{(r+1)} B(\alpha) j(\alpha) t\right] \right) \\
&= \prod_{i=0}^{r-1} \frac{1}{1 - q^i t} \cdot \left[\prod_{\alpha} \left(1 + (-1)^r B(\alpha) j(\alpha) t \right) \right]^{(-1)^r}
\end{aligned}$$

□

Proposition 5.4. *Up to multiplying the roots by roots of unity, the zeta function of the weighted projective variety (with points counted via the stack quotient) defined by*

$$a_0 x_0^{n_0} + \dots + a_r x_r^{n_r} = 0$$

over any $\mathbb{F}_q$ is equal to,

$$\zeta_X(t) = \prod_{i=0}^{r-1} \frac{1}{1 - q^i t} \cdot \left[\prod_{\alpha} \left(1 + (-1)^r B(\alpha) j_q(\alpha) t \right) \right]^{(-1)^r},$$

where $B(\alpha) = \chi_{\alpha_0}(a_0^{-1}) \dots \chi_{\alpha_r}(a_r^{-1})$ is a root of unity determined by α and the coefficients.

Proof. By Theorem 3.1 we can reduce the zeta function for X over $\mathbb{F}_q$ to zeta function for X over $\mathbb{F}_{q^v}$, where $v = \mathrm{ord}_n(q)$ and $n = \mathrm{lcm}\,(n_i)$ such that $q^v \equiv 1 \mod (\mathrm{lcm}\,(n_i))$. We know that ζ_{X_q} is equal to $\zeta_{X_{q^v}}$ with each root β replaced by $\beta^{1/v}$. Therefore, ζ_{X_q} is determined up to roots of unity by Theorem 5.3. □

Corollary 5.4.1. *The variety X is supersingular if and only if $j_q(\alpha) = \omega q^{\frac{r-1}{2}}$ where ω is a root of unity for each $\alpha \in A_{n,q^v}$.*

Proof. By Theorem 5.3 the roots and poles of the zeta function have the form $(-1)^r B(\alpha) j_q(\alpha)$ or q^i. Since $B(\alpha)$ is a product of characters it is always a root of unity. Therefore, each root of ζ_X has argument a root of unity if and only if $j_q(\alpha)$ does for each α. □

Corollary 5.4.2. *Note that $|g(\chi_\alpha)| = q$ and thus,*

$$|j_q(\alpha)| = \frac{1}{q}|g(\chi_{\alpha_0})| \cdots |g(\chi_{\alpha_r})| = \frac{1}{q} q^{\frac{r+1}{2}} = q^{\frac{r-1}{2}}$$

Since the characters are roots of unity,

$$\left|(-1)^{(r+1)} B(\alpha) j(\alpha)\right| = q^{\frac{r-1}{2}}$$

By the Riemann hypothesis, each of the α-derived roots are roots of P_{r-1} in Weil's factorization of the zeta function. If $r-1$ is even then a factor of $(1 - q^{\frac{r-1}{2}} t)$ from the zeta function of $\mathbb{P}^r$ will also appear in P_{r-1}. Therefore, we can write,

$$\zeta_X = \zeta_{\mathbb{P}^r} \cdot \tilde{P}_{r-1}^{(-1)^r}$$

where $\zeta_{\mathbb{P}^r}$ is the zeta function of projective r-space and,

$$\tilde{P}_{r-1}(t) = \prod_{\alpha} \left(1 + (-1)^r B(\alpha) j(\alpha) t\right)$$

Therefore, we can write the Weil factorization of ζ_X as,

$$P_i(t) = \begin{cases} 1 - q^{\frac{i}{2}} t & 0 \le i \le 2(r-1) \text{ is even and } i \ne r-1 \\ (1 - q^{\frac{r-1}{2}} t) \cdot \tilde{P}_{r-1}(t) & i = r-1 \text{ is even} \\ \tilde{P}_{r-1}(t) & i = r-1 \text{ is odd} \end{cases}$$

Remark. The only interesting cohomology group is H^{r-1} which shows up in the dimension of the surface.

Theorem 5.5. *Let X be the weighted projective variety (with points counted via the stack quotient) defined by*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

over any $\mathbb{F}_q$. Then the Betti numbers are determined,

$$\dim H^i(X) = \begin{cases} 1 & 0 \le i \le 2(r-1) \text{ is even and } i \ne r-1 \\ |A_{n,q}| + 1 & i = r-1 \text{ is even} \\ |A_{n,q}| & i = r-1 \text{ is odd} \end{cases}$$

Proof. By Theorem 3.1, changing the base field only changes the zeta function by multiplying its roots by roots of unity. In particular, the magnitudes of the degrees of each P_i and thus the Betti numbers are not changed. Therefore, given X defined over $\mathbb{F}_q$ take $v = \mathrm{ord}_n(q)$ and $n = \mathrm{lcm}\,(n_i)$ such that $q^v \equiv 1(\mod n)$. Then we know that $\zeta_{X_{p^v}}$ factors with,

$$P_i(t) = \begin{cases} 1 - q^{\frac{i}{2}} t & 0 \le i \le 2(r-1) \text{ is even and } i \ne r-1 \\ (1 - q^{\frac{r-1}{2}} t) \cdot \tilde{P}_{r-1}(t) & i = r-1 \text{ is even} \\ \tilde{P}_{r-1}(t) & i = r-1 \text{ is odd} \end{cases}$$

Therefore, the Betti numbers of X which are equal to the Betti numbers of X_{p^v} are equal to the degrees of these polynomials. □

Remark. Notice that whether a variety is supersingular or not is now determined explicitly by one computation of Gaussian sum.

Proposition 5.6. *If $\alpha_1 + \alpha_2 = 1$, then $g(\chi_{\alpha_1})g(\chi_{\alpha_2}) = \chi_{\alpha_1}(-1)p$.*

Proof. Notice that if $\alpha_1 + \alpha_2 = 1$, then $\chi_{\alpha_1} = \overline{\chi_{\alpha_2}}$. We know that

$$\begin{aligned} g(\chi)g(\overline{\chi}) &= \sum_{x\neq 0}\sum_{y\neq 0} \chi(xy^{-1})\psi(x+y) \\ &= \sum_{x\neq 0} \chi(x) \sum_{y\neq 0} \psi[(x+1)y] \end{aligned}$$

The second sum has the value $p-1$ for $x=-1$, and -1 when $x \neq 0$. As sum over all $x \in k^*$ is 0, we get $g(\chi_{\alpha_1})g(\chi_{\alpha_2}) = \chi_{\alpha_1}(-1)p$. ☐

In our example when $n = 4$ and $\alpha_1 = 1/4$, $\chi_{1/4}(-1) = 1$ if $p \equiv 1 \mod 8$, and $\chi_{1/4}(-1) = -1$ otherwise.

Fact 5.7. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field. Then $\mathcal{O}_K$ is a PID if and only if $n = m$ or, when m is odd, $n = 2m$ where m is one of the following,

$$1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$$

Lemma 5.8 (Coyne)**.** *Let $d = \operatorname{lcm}(n_i)$ and $w_i = d/n_i$ then,*

$$\#\left\{(x_0, \cdots, x_r) : \sum_{i=0}^{r} w_i x_i \equiv 0 \mod (d) \text{ and } 0 \le x_i < n_i\right\} = \frac{1}{\operatorname{lcm}(n_i)} \prod_{i=0}^{r} n_i$$

Proof. Consider the homomorphism,

$$\Phi : \prod_{i=0}^{r} (\mathbb{Z}/n_i\mathbb{Z}) \to \mathbb{Z}/d\mathbb{Z}$$

via $(x_0, \cdots, x_r) \mapsto w_0 x_0 + \cdots + w_r x_r$. Thus,

$$\ker \Phi = \left\{(x_0, \cdots, x_i) : \sum_{i=0}^{r} w_i x_i \equiv 0 \mod (d) \text{ and } 0 \le x_i < n_i\right\}$$

Suppose that $p^r \mid\mid d$ then we know that $p^r \mid\mid n_i$ for some n_i. Thus, $p \nmid w_i$ so each prime dividing d cannot divide all w_i. However, $w_i \mid d$ so the list $w_0, \cdots, w_r$ cannot share any common factors. Thus, the ideal $(w_0, \cdots, w_r) = \mathbb{Z}$ so the map Φ is surjective. Therefore, by the first isomorphism theorem,

$$\#(\ker \Phi) = \#\left(\prod_{i=0}^{r} \mathbb{Z}/n_i\mathbb{Z}\right) \Big/ \#(\mathbb{Z}/d\mathbb{Z}) = \frac{1}{d}\prod_{i=0}^{r} n_i$$

☐

Lemma 5.9. *The number of alphas $A_{n,q}$ is given by the formula,*

$$\#(A_{n,q}) = \sum_{t\in T} \frac{(-1)^{r+1-sum(t)}}{\operatorname{lcm}(d_i \mid t_i = 1)} \prod_{i\in\{i : t_i = 1\}} d_i$$

where $d_i = \gcd(n_i, q-1)$.

Proof. For each $t \in T$, define the number,

$$C_t = \#\left\{(x_0, \cdots, x_r) : \sum_{i=0}^{r} w_i x_i \equiv 0 \mod \operatorname{lcm}(d_i) \text{ and } 0 \le x_i < d_i \text{ and } x_i = 0 \text{ if } t_i = 0\right\}$$

By inclusion-exclusion,

$$\#(A_{n,q}) = \#\left\{(x_0, \cdots, x_r) : \sum_{i=0}^{r} w_i x_i \equiv 0 \mod \operatorname{lcm}(d_i) \text{ and } 0 < x_i < d_i\right\} = \sum_{t\in T} (-1)^{r+1-sum(t)} C_t$$

However, letting,

$$g = \frac{\operatorname{lcm}(d_i)}{\operatorname{lcm}(d_i \mid t_i = 1)}$$

then we know that $g \mid w_i$ for $t_i = 1$ since $w_i = \operatorname{lcm}(d_i)/d_i$ and thus,

$$\tilde{w}_i^t = \frac{w_i}{g} = \frac{\operatorname{lcm}(d_i \mid t_i = 1)}{d_i} \in \mathbb{Z}$$

since d_i is such that $t_i = 1$. Therefore, the conditions,

$$\sum_{i=0}^{r} w_i x_i \equiv 0 \mod \operatorname{lcm}(d_i) \iff \sum_{i=0}^{r} \tilde{w}_i^t x_i \equiv 0 \mod \operatorname{lcm}(d_i \mid t_i = 1)$$

are equivalent when $x_i = 0$ for $t_i = 0$. By Coyne's Lemma,

$$C_t = \frac{1}{\operatorname{lcm}(d_i \mid t_i = 1)} \prod_{i\in\{i:t_i=1\}} d_i$$

and thus the lemma follows. □

6 Gauss Sums

6.1 Previously Known Facts and Some Lemmas

Theorem 6.1. *$g(\chi_\alpha) = \omega q^{\frac{1}{2}}$ where ω is a root of unity if and only if $\alpha = 1, \frac{1}{2}$.*

Proof. See Chowla. □

Lemma 6.2. *Let χ be a character on $\mathbb{F}_q$ of order m. Then $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.*

Proof. Well-known fact. See Evans' generalization of Chowla's paper. □

Lemma 6.3. *Let χ be a character of order m on $\mathbb{F}_q$ for $q = p^r$. Let $K = \mathbb{Q}(\zeta_{pr})$ with $m|r$ and a an integer 1 $\pmod m$ with $(a, 2p(q-1)) = 1$. Let $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ be the element such that*

$$\sigma(\zeta_{2p(q-1)}) = \zeta_{2p(q-1)}^a$$

Then $\sigma(g(\chi)) = \bar{\chi}(a)g(\chi)$.

Proof. Let ψ be the nontrivial additive character such that:

$$g(\chi) = \sum_{a\in\mathbb{F}_q} \chi(a)\psi(a)$$

Note that $\psi(x)^p = \psi(px) = \psi(0) = 1$. Thus $\psi(x) = \zeta_p^{t(x)}$ for $t : \mathbb{F}_q \to \mathbb{Z}$. We can select ζ_p to be the p-th root of unity so that $t(1) = 1$. Note that as $\psi(x + y) = \psi(x)\psi(y)$, $t(x + y) = t(x) + t(y)$. Thus as a is an integer $t(a) = a$ and $t(ax) = at(x)$.

$$\sigma(\psi(x)) = \sigma(\zeta_p)^{t(x)} = \zeta_p^{at(x)} = \zeta_p^{t(ax)} = \psi(ax)$$

If w is a generator of $\mathbb{F}_q^\times$, as $a \equiv 1 \pmod m$ and χ has order m, we have $\sigma(\chi(w)) = \chi(w)^a = \chi(w)$. Thus as χ is nontrivial,

$$\sigma(g(\chi)) = \sum_{x\in\mathbb{F}_q^\times} \sigma(\chi(x))\sigma(\psi(x))$$
$$= \sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi(ax)$$

Making the substitution $ax \mapsto x$ gives,

$$\sigma(g(\chi)) = \sum_{x\in\mathbb{F}_q^\times} \chi(a^{-1}x)\psi(x)$$
$$= \bar{\chi}(a) \sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi(x)$$
$$= \bar{\chi}(a)g(\chi)$$

□

Theorem 6.4. *[See Lang's Algebraic Number Theory] Let $\mathfrak{p}$ be a prime lying over p in $\mathbb{Q}(\zeta_m)$ and let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$ in $\mathbb{Q}(\zeta_m, \zeta_p)$. Let f be the order of p modulo m and $q = p^f$. Let χ be a character of $\mathbb{F} = \mathbb{F}_q$ such that*

$$\chi(a) \equiv a^{-(q-1)/m} \pmod{\mathfrak{p}}$$

Then for any integer $r \geq 1$ we have:

$$\tau\left(\chi^r\right) \sim \mathfrak{P}^{\alpha(r)}$$

where

$$\alpha(r) = \frac{1}{f}\sum_{\mu} s\left(\frac{(q-1)\mu r}{m}\right)\sigma_\mu^{-1}$$

where the summation runs over all $0 < \mu < p-1$ relatively prime to $p-1$ and where $s(v)$ is the sum of the digits of the p-adic expansion of v modulo $q-1$. Furthermore, if μ, μ' are such that $\sigma_\mu^{-1}\mathfrak{P} = \sigma_{\mu'}^{-1}\mathfrak{P}$ then

$$s\left(\frac{(q-1)\mu r}{m}\right) = s\left(\frac{(q-1)\mu' r}{m}\right)$$

Remark. If $f = 1$, then $\sigma_\mu^{-1}\mathfrak{P}$ is distinct for all $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$. In general, by cyclotomic reciprocity, there are $\frac{\phi(m)}{f}$ distinct values of $\sigma_\mu^{-1}\mathfrak{P}$ as μ ranges over all the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$

Lemma 6.5.

$$s\left(v\right) = (p-1)\sum_{i=0}^{f-1}\left\{\frac{p^i v}{q-1}\right\}$$

Theorem 6.6. *(From Evans' Chowla Generalization) Let χ, ψ be two multiplicative characters modulo p of order > 2. Then $g(\chi)^j g(\psi)^k$ has argument a root of unity if and only if $j = k$ and $\chi = \bar{\psi}$ or $j = 2k$, $\chi = \bar{\psi}^2$ and ψ has order 6.*

6.2 Jacobi Sums

Proposition 6.7. *Let $J(\chi_1, \chi_2) = \sum_x \chi_1(x)\chi_2(1-x)$, where χ is a character of $\mathbb{F}_q$. If $\chi_1\chi_2 \neq 1$, then*

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$$

.

Proof.

$$\begin{aligned}
g(\chi_1)g(\chi_2) &= \sum_x \sum_y \chi_1(x)\chi_2(y)\psi(x+y) \\
&= \sum_x \sum_y \chi_1(x)\chi_2(y-x)\psi(y) \\
&= \sum_x \sum_{a\neq 0} \chi_1(x)\chi_2(a-x)\psi(a) + \sum_x \chi_1(x)\chi_2(-x) \\
&= (\sum_a \chi_1\chi_2(a)\psi(a)) \cdot (\sum_x \chi_1(x)\chi_2(1-x))
\end{aligned}$$

□

Proposition 6.8. *If $\chi_1 \dots \chi_4|_{\mathbb{F}_q^\times} = \chi_0$ where χ_0 is the trivial character then,*

$$g(\chi_1)\dots g(\chi_4) = J(\chi_1, \chi_2)J(\chi_3, \chi_1\chi_2)\chi_4(-1)q$$

6.3 Products of Gauss Sums

Theorem 6.9. *Let $\chi_1, \dots, \chi_n$ be nontrivial characters on $\mathbb{F}_q$ for $q = p^r$ with p an odd prime. If n is even and $\chi_1 \cdots \chi_n|_{\mathbb{F}_p^\times}$ is not the trivial character or n is odd and $\chi_1 \cdots \chi_n|_{\mathbb{F}_p^\times}$ is not -1 or 1 everywhere, then*

$$\prod_{i=1}^n g(\chi_i)$$

does not have argument equal to a root of unity.

Proof. (adapted from theorem 1 in Evans' Generalizations of Chowla paper)
Let L be the lcm of the orders of the χ_i. Let

$$G = \prod_{i=1}^n g(\chi_i)$$

By Lemma 6.2, $g(\chi_i)^L \in \mathbb{Q}(\zeta_L)$. Thus $G^L \in \mathbb{Q}(\zeta_L)$. Let ϵ be the number of order 1 such that $G = q^{n/2}\epsilon$. Now suppose G does have argument equal to a root of unity. As $G^L \in \mathbb{Q}(\zeta_L)$, G^L must be a $2L$-th root of unity. Thus $\epsilon = \zeta_{2L^2}^v$ for some integer v.

Now let a be an integer such that $a \equiv 1 \pmod 2L^2$ and $a \equiv g^{-1} \pmod p$ where g is a generator modulo p. Note that such an a exists as $L|q-1$ and hence must be relatively prime to p. Now consider the Galois group $Gal(\mathbb{Q}(\zeta_{2pL^2})/\mathbb{Q}(\zeta_{2L^2}))$ and the element σ contained in it such that:

$$\sigma(\zeta_{2pL^2}) = \zeta_{2pL^2}^a$$

This is a well-defined element as $(a, 2pL^2) = 1$ $a \equiv 1 \pmod 2L^2$ so it fixes $\mathbb{Q}(\zeta_{2L^2})$. Note that as ϵ is a $2L^2$-th root of unity $\sigma(\epsilon) = \epsilon$. Furthermore, $\sigma(\sqrt{(q)}) = \pm\sqrt{q}$. As

$$\sigma(G) = \sigma(q^{n/2})\sigma(\epsilon)$$

So $\sigma(G) = G$ if n is even and $\sigma(G) = \pm G$ if n is odd. However, we also have by lemma 6.3,

$$\sigma(G) = \prod_{i=1}^n \sigma(g(\chi_i)) = \prod_{i=1}^n \chi_i(a^{-1})g(\chi_i) = G\prod_{i=1}^n \chi_i(a^{-1})G\prod_{i=1}^n \chi_i|_{\mathbb{F}_p}(g)$$

Hence if n is even,

$$\prod_{i=1}^n \chi_i|_{\mathbb{F}_p}(g) = 1$$

and if n is odd,

$$\prod_{i=1}^{n} \chi_i|_{\mathbb{F}_p}(g) = \pm 1$$

Thus, as g is a generator, $\prod_{i=1}^{n} \chi_i|_{\mathbb{F}_p}$ must be the trivial character if n is even and take value ± 1 everywhere if n is odd. □

Proposition 6.10. *If χ_1, χ_2 are two different nontrivial character on $\mathbb{F}_q$ of same order, and*

$$\mu = g^j(\chi_1) g^k(\chi_2) q^{(j+k)/2} \in U,$$

where $q = p^r$, and $j \neq k$, $g(\chi)$ is gauss sum on $\mathbb{F}_q$, U denote the group of all root of unity, then in $\mathbb{Q}(\zeta_{p(q-1)})$, we have $(q^{1/2})$ divides $(g(\chi_i))$, i.e.,

$$\mathcal{O}g(\chi_1) = \mathcal{O}(q^{1/2})\mathfrak{a}.$$

Proof. Notice that

$$\mu = \frac{g^j(\chi_1)\chi_2^k(-1)}{q^{(j-k)/2} g^k(\overline{\chi_2})}.$$

And

$$V(g(\chi_1)) = V(g(\chi_2)) = \min_{(a,q-1)=1} s\left(\frac{a(q-1)}{m}\right)$$

But we also have $V(g^j(\chi_1)) = V(q^{(j-k)/2} g^k(\overline{\chi_2}))$, while $V(q^{1/2}) = (p-1)r/2$. This give us the result. □

Remark. When is $e_i = (p-1)r/2$ for each i? Let us just act by Galois group again.

Remark. When is the conjugate of a gauss sum a gauss sum? Why is the equation

$$\sigma_a(G_r(\chi)) = \overline{\chi}(a) G_r(\chi)?$$

Lemma 6.11. *If $K/\mathbb{Q}$ is abelian then $|\sigma(z)|^2 = \sigma(|z|^2)$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. In particular, if $|z|^2 \in \mathbb{Q}$ then $\sigma(|z|^2) = |z^2|$ and thus $|\sigma(z)| = |z|$.*

Proof. Since $K/\mathbb{Q}$ is Galois complex conjugation $\tau : K \to K$ is an automorphism fixing $\mathbb{Q}$ so $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, $|\sigma(z)|^2 = \sigma(z)\tau(\sigma(z)) = \sigma(z)\sigma(\tau(z)) = \sigma(z\tau(z)) = \sigma(|z|^2)$ since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. □

Lemma 6.12. *Let K be a number field and $z \in \mathcal{O}_K$ such that $|\sigma(z)| = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ then z is a root of unity.*

Proposition 6.13. *The element $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is an algebraic integer if and only if it is a root of unity.*

Proof. We know that $|q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)| = 1$ and since σ takes $g(\chi)$ to another Gaussian sum which must also have magnitude $q^{\frac{1}{2}}$ we know that,

$$|\sigma(q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r))| = |\sigma(q^{-(r+1)/2})||\sigma(g(\chi_0))| \cdots |\sigma(g(\chi_r))| = |\pm q^{-(r+1)/2}| q^{(r+1)/2} = 1$$

Thus, if $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is an algebraic integer then by Lemma 6.12 we know that $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is a root of unity. Conversely, if $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is a root of unity then clearly it is an algebraic integer. □

Corollary 6.13.1. *The element $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is a root of unity if and only if the principal fractional ideal generated by it in $K = \mathbb{Q}(\zeta_m, \zeta_p)$ is $\mathcal{O}_K$ if and only if it is an algebraic integer.*

Proof. If it is a root of unity, then the ideal generated will be $\mathcal{O}_K$. If it is not a root of unity, by the Proposition 6.13 it is not an algebraic integer. Thus the ideal cannot be $\mathcal{O}_K$. □

Remark. By Stickelberger's theorem, we can determine exactly when $q^{-(r+1)/2} g(\chi_0) \dots g(\chi_r)$ is a unit.

Theorem 6.14. *Let p be an odd prime (or $r+1$ is even) and $q = p^f$. The normalized product $\omega = q^{-\frac{r+1}{2}} g(\chi^{e_0}) \cdots g(\chi^{e_r})$ is a root of unity if and only if,*

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu e_i}{m}\right) = \frac{r+1}{2}(p-1)f$$

for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. Consider the ideals generated by $g(\chi^{e_0}) \cdots g(\chi^{e_r})$ and by $q^{\frac{r+1}{2}}$ respectivly. By Lang's formula, we know the Gaussian sum factors into prime ideals as,

$$(g(\chi^{e_0}) \cdots g(\chi^{e_r})) = \mathfrak{P}_1^{D_1} \cdots \mathfrak{P}_w^{D_w}$$

where,

$$D_j = \sum_{i=0}^{r} s\left(\frac{(q-1)\mu e_i}{m}\right)$$

Lang's formula contains a factor of f^{-1}. However, $\sigma_\mu^{-1}\mathfrak{P}$ ranges over each prime above p a total of f times because the decomposition group has order f. The sets of σ_μ mapping to a fixed prime are exactly the cosets of the decomposition groups of which there are $w = \phi(m)/f$. In the field $K = \mathbb{Q}(\zeta_m, \zeta_p)$ the ideal (p) factors as,

$$(p) = \mathfrak{P}_1^{(p-1)} \cdots \mathfrak{P}_w^{(p-1)}$$

Therefore, since $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$ for p an odd prime, the ideal $(q^{\frac{r+1}{2}}) = (p^{\frac{r+1}{2}f})$ fractors into primes as,

$$(q^{\frac{r+1}{2}}) = (p^{\frac{r+1}{2}})^f = \mathfrak{P}_1^{\frac{r+1}{2}(p-1)f} \cdots \mathfrak{P}_w^{\frac{r+1}{2}(p-1)f}$$

Therefore, the principal fractional ideal genreated by ω factors as,

$$(\omega) = (q^{\frac{r+1}{2}})^{-1}(g(\chi^{e_0}) \cdots g(\chi^{e_r})) = \mathfrak{P}_1^{D_1 - \frac{r+1}{2}(p-1)f} \cdots \mathfrak{P}_w^{D_w - \frac{r+1}{2}(p-1)f}$$

Which implies that $\omega \in \mathcal{O}_K$ if and only if,

$$D_w = \sum_{i=0}^{r} s\left(\frac{(q-1)\mu e_i}{m}\right) \geq \frac{r+1}{2}(p-1)f$$

such that the fractional ideal it generates is an actual ideal of $\mathcal{O}_K$. However, by Proposition 6.13, $\omega \in \mathcal{O}_K$ if and only if ω is a root of unity. In particular, if $\omega \in \mathcal{O}_K$ then ω is a unit. Therefore, ω is a root of unity if and only if,

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu e_i}{m}\right) \geq \frac{r+1}{2}(p-1)f$$

for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ if and only if

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu e_i}{m}\right) = \frac{r+1}{2}(p-1)f$$

for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$. □

Theorem 6.15. *Let X defined by,*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

be a variety over $\mathbb{F}_{p^t}$. Let $n = \operatorname{lcm}(n_i)$. And consider it's zeta function over $\mathbb{F}_q$, where $q = p^f$ such that $f = ord_n(p)$. This means that $q \equiv 1 \mod n$. Then X is supersingular over $\mathbb{F}_q$ if and only if

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu \ell_i}{n}\right) = \frac{r+1}{2}(p-1)f,$$

for each,

$$\ell \in \left\{ (\ell_0, \ldots, \ell_r) : \ell_i \in \mathbb{Z} \text{ and } n \mid \sum_{i=0}^{r} \ell_r \text{ and } 0 < \ell_i < n \text{ and } n \mid \ell_i n_i \right\}$$

and each $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$. *Notice in Lang (p97) that if* $\sigma_\mu(\mathfrak{P}_j) = \mathfrak{P}_j$, *then* $s\left(\frac{(q-1)\mu r_i}{n}\right) = s\left(\frac{(q-1)r_i}{n}\right)$.

Proof. When $q = p^f$, then X is supersingular over $\mathbb{F}_p$ if and only if X is supersingular over $\mathbb{F}_q$ if and only if X is supersingular over $\mathbb{F}_{p^t}$. Thus, we need only consider the supersingularity of X over $\mathbb{F}_q$. However, by Lang, the above condition gives that the product of each tuple of Gaussian sums generates the same ideal as $q^{\frac{r+1}{2}}$ and thus their ratio is a unit. By Proposition 6.13, this implies that each product has argument root of unity. Therefore, by Corollary 5.4.1, we know that X is supersingular over $\mathbb{F}_q$. □

Theorem 6.16. *Let* χ *be a multiplicative character of order* $p-1$ *modulo* p. *Let* χ^a, χ^b, χ^c *be three multiplicative distinct characters modulo* p *of order* > 2. *Then* $g(\chi^a)g(\chi^b)g(\chi^c)^2$ *does not have argument a root of unity.*

Proof. Assume $g(\chi^a)g(\chi^b)g(\chi^c)^2$ is a root of unity. To begin note that the unit part of $g(\chi^a)g(\chi^b)g(\chi^c)^2$ is:

$$p^{-2}g(\chi^a)g(\chi^b)g(\chi^c)^2 = \frac{g(\chi^a)g(\chi^b)\chi^c(-1)}{g(\chi^{-c})^2}$$

Thus the above must be a root of unity. Now consider the principal ideal generated by it in $\mathbb{Q}(\zeta_{p-1}, \zeta_p)$. By Theorem 6.4, for each μ relatively prime to $p-1$, the prime ideal $\sigma_\mu^{-1}\mathfrak{P}$ has index:

$$s(\mu a) + s(\mu b) - 2s(-\mu c) = 0$$

WLOG assume $0 < a, b < p-1$ and let $0 < d < p-1$ be such that $d \equiv -c \pmod{p} - 1$. As $s(\mu a) = (p-1)\left\{\frac{\mu c}{p-1}\right\}$, the above is equivalent to:

$$\left\{\frac{\mu a}{p-1}\right\} + \left\{\frac{\mu b}{p-1}\right\} = 2\left\{\frac{\mu c}{p-1}\right\}$$

for all μ relatively prime to $p-1$. Taking $\mu = 1$ gives $2d = a+b$. Now let c', t be such that $t = \gcd(d, p-1)$ and $d = c't$. As χ^c has order > 2 we must have $t < \frac{p-1}{2}$. Now there exists $\nu < \frac{p-1}{t}$ such that $\nu d \equiv t \pmod{p-1}$ and ν is relatively prime to $\frac{p-1}{t}$. Furthermore, for each k we will have $\left(\nu + \frac{p-1}{t}k\right) d \equiv \pmod{p-1}$. Taking $\mu = \nu + \frac{p-1}{t}k$ for some k gives:

$$\left\{\frac{\left(\nu + \frac{p-1}{t}k\right)a}{p-1}\right\} + \left\{\frac{\left(\nu + \frac{p-1}{t}k\right)b}{p-1}\right\} = \frac{2t}{p-1} < 1$$

This implies that for all k:

$$\left\{\frac{\nu a + \frac{p-1}{t}ka}{p-1}\right\} \leq \frac{2t}{p-1}$$

and similarly for b. Now let $s = \gcd(a, t)$ and take $a = a's$. Then this becomes:

$$\left\{\frac{\nu a + \frac{(p-1)}{t/s}ka'}{p-1}\right\} \leq \frac{2t}{p-1}$$

Note that k, a' are both relatively prime to t/s. Thus $\nu a + \frac{(p-1)}{t/s}ka' \pmod{p-1}$ ranges over all residues $x \equiv \nu a \pmod{\frac{p-1}{t/s}}$. Pick the k that gives the largest $x = \nu a + \frac{(p-1)}{t/s}ka' \pmod{p-1}$ with $0 < x < p-1$. We know $x \geq p - 1 - \frac{(p-1)}{t/s}$ (with equality if and only if $\frac{(p-1)}{t/s}$ divides a and hence $\frac{(p-1)}{t}$ divides a').

However, as $x \leq 2t$ by the above, this implies:

$$2t + \frac{(p-1)}{t/s} \geq p - 1$$

where equality can only occur if $\frac{(p-1)}{t}$ divides a'. If $s = t$ this follows immediately. Otherwise, note that t is at most $\frac{p-1}{3}$ and $\frac{(p-1)}{t/s}$ is at most $\frac{p-1}{2}$. Thus we have the following possibilities:

1. $s = t$
2. $t = 2s$, $t = \frac{p-1}{3}$
3. $t = 2s$, $t = \frac{p-1}{4}$, and $\frac{(p-1)}{t} = 4$ divides a'
4. $t = 3s$, $t = \frac{p-1}{3}$, and $\frac{(p-1)}{t} = 3$ divides a'

Note that possibilities 3 and 4 can't actually happen as the fact that $4|a'$ contradicts $t = 2s$ and $3|a'$ contradicts $t = 3s$. This same reasoning can be applied to b. Now suppose $t < \frac{p-1}{3}$. Then for both a, b we must have case 1. Thus $t|a$ and $t|b$. Let $d = c't, a = a't, b = b't$. Note that the minimum value of $\left\{\frac{\mu a}{p-1}\right\}$ is $\frac{\gcd(a,p-1)}{p-1}$ and similarly the minimum of $\left\{\frac{\mu b}{p-1}\right\}$ is $\frac{\gcd(b,p-1)}{p-1}$. As $\gcd(a, p-1), \gcd(b, p-1) \geq t$ and taking $\mu = \nu$ gives us:

$$\left\{\frac{\nu a}{p-1}\right\} + \left\{\frac{\nu b}{p-1}\right\} = \frac{2t}{p-1}$$

We must have:

$$\left\{\frac{\nu a}{p-1}\right\} = \left\{\frac{\nu b}{p-1}\right\} = \frac{t}{p-1}$$

and thus $\gcd(a, p-1) = \gcd(b, p-1) = t$. Now note that ν satisfies: $\nu d \equiv t \pmod{p-1}$ and $\nu a \equiv t \pmod{p-1}$. This implies:

$$\nu(a - d) \equiv 0 \pmod{p-1}$$

which further gives:

$$\nu(a' - c') \equiv 0 \pmod{\frac{p-1}{t}}$$

But as ν is relatively prime to $\frac{p-1}{t}$ this implies $a' \equiv c' \pmod{\frac{p-1}{t}}$, which implies $a = d$. By the same reasoning $b = d$, which is a contradiction.

Thus we have shown that χ^c must have order 3. Let $s_1 = \gcd(t, a)$ and $s_2 = \gcd(t, b)$. As s_1, s_2 are either t or $\frac{t}{2}$, a and b must both be multiples of $\frac{p-1}{6}$. However, as $c = \frac{p-1}{3}$ or $\frac{2(p-1)}{3}$ the only way that we can have $a + b = 2c$ is if a or b is $\frac{p-1}{2}$, which is a contradiction on χ^a, χ^b having order > 2.

As we have exhausted all possibilities,

$$g(\chi^a)g(\chi^b)g(\chi^c)^2$$

does not have argument a root of unity. □

7 Fermat Surfaces

Definition 7.1. Let F_r^n denote the projective variety of dimension $r - 1$ in $\mathbb{P}^r$ defined by the polynomial,

$$x_0^n + \cdots + x_r^n = 0$$

We call this the Fermat n, r hypersurface.

Conjecture 7.2. *Let p be an odd prime. Let ζ_{X_p} be the zeta function of the Fermat-4,3 hypersurface over $\mathbb{F}_p$. Then*

$$\zeta_{X_p} = \begin{cases} \frac{-1}{(T-1)(p^2T-1)(pT+1)^{10}(pT-1)^{12}} & p \equiv 3 \pmod 4 \\ \\ \frac{-1}{(T-1)(p^2T-1)(pT-1)^8 g_p(T) h_p(T)} & p \equiv 1 \pmod 4 \end{cases}$$

where

$$g_p(T) = \begin{cases} (pT+1)^{12} & p \equiv 5 \pmod 8 \\ \\ (pT-1)^{12} & p \equiv 1 \pmod 8 \end{cases}$$

and

$$h_p(T) = \left(pT - \frac{s^2}{p}\right)\left(pT - \frac{\bar{s}^2}{p}\right)$$

where $s = a + bi$ is the unique complex number with a an odd positive integer, b an even positive integer, and $|s| = p$.

Proposition 7.3. *For Fermat variety F_r^n defined over $\mathbb{F}_q$, the number of possible α is determined by the formula,*

$$\#A_{n,q} = \sum_{i=1}^{r} (-1)^i (d-1)^i,$$

where $d = \gcd(n, q-1)$.

Proof. Recall that $A_{n,p} = \{(\alpha_0, \ldots, \alpha_r) : 0 < \alpha_i < 1, \sum d\alpha_i \in \mathbb{Z}, i = 0, \ldots, r\}$ in this case. Since α_i have the same denominator, we consider only the numerator of α_i, and our problem become counting x_i such that

$$x_0 + x_1 + \cdots + x_r \in d\mathbb{Z}.$$

Suppose we let $x_1, \ldots, x_r$ take arbitrary value in $\{1, \ldots, d-1\}$, then the value of x_0 is uniquely determined. This gives us $(d-1)^r$ possibilities. But we may be over counting. So apply the inclusion-exclusion formula. □

Corollary 7.3.1. *The Betti numbers of the Fermat n,r hypersurface are,*

$$\dim H^i(F_r^n) = \begin{cases} 1 & 0 \le i \le 2(r-1) \text{ is even and } i \neq r-1 \\ \sum_{j=0}^{r-1} (-1)^j (n-1)^j + 1 & i = r-1 \text{ is even} \\ \sum_{j=0}^{r-1} (-1)^j (n-1)^j & i = r-1 \text{ is odd} \end{cases}$$

Corollary 7.3.2. *The Euler Characteristic of the Fermat n,r hypersurface is,*

$$\chi(F_r^n) = r + (-1)^{r-1} \sum_{j=0}^{r-1} (-1)^j (n-1)^j$$

Theorem 7.4. *The Fermat hypersurface F_{n-1}^n is never supersingular over $\mathbb{F}_p$ when $p \equiv 1 \mod n$ and $n > 2$.*

Proof. The Gaussian sum $g(\chi_\alpha)$ over $\mathbb{F}_p$ is never a root of unity when normalized to the unit circle unless $\alpha = 1, 1/2$ (Chowla). Therefore, consider $\alpha = (1/n, \cdots, 1/n)$ which satisfied the conditions to be in $A_{n,p}$ since $r + 1 = n$. Therefore,

$$(-1)^r B(\alpha) j(\alpha) = (-1)^r B(\alpha) g(\chi_{1/n})^n$$

which is a root of ζ_X cannot be a root of unity when normalized to the unit circle because $(-1)^r B(\alpha)$ is a root of unity but $g(\chi_{1/n})^n$ is not since $g(\chi_{1/n})$ is not either by Chowla because $n > 2$. Therefore, ζ_X contains a root which is not of the form $\omega q^{\frac{i}{2}}$ where ω is a root of unity so X is not supersingular. □

Theorem 7.5. *Let $n \geq 4$ be an integer and let $p \equiv 1 \pmod n$ be a prime number. Then the zeta function for the Fermat curve (with points counted via the "stack quotient") given by the zero set of:*

$$w^n + x^n + y^n + z^n = 0$$

is not supersingular

Proof. By Theorem 5.3, we just need to show that

$$\prod_{i=0}^{3} g(\chi_{\alpha_i})$$

has argument not equal to a root of unity. For $n = 4$ we take $\alpha_i = \frac{1}{4}$ for all i. By Theorem 6.1 this is does not have argument equal to a root of unity. For $n = 6$ we take $\alpha_0 = \frac{1}{2}$ and $\alpha_i = \frac{1}{6}$ for $i \neq 0$. Again, by Theorem 6.1 this is does not have argument equal to a root of unity. For all other $n \geq 4$ we take $\alpha_0 = \frac{n-3}{n}$ and $\alpha_i = \frac{1}{n}$ for $i \neq 0$. By Theorem 6.6 this does not have argument equal to a root of unity. □

8 Non-Supersingularity using Factorization of Gauss Sums

In this section, let X be a variety defined by,

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

over $\mathbb{F}_p$, where p is a prime not dividing $m = \operatorname{lcm}(n_0, \ldots, n_r)$. Furthermore, let $f = \operatorname{ord}_m(p)$.

Proposition 8.1. *If $p \equiv 1 \mod m$ for $m \geq 4$ and $r \geq 3$ then F_r^m is not supersingular.*

Proof. Notice that in this case $f = 1$, and $q = p$. If F_r^m were supersingular then, by Theorem 6.15, for each choice of $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ and character powers $e_0, \cdots e_r$ that,

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu r_i}{m}\right) = \frac{r+1}{2}(p-1)f$$

Consider the case $\mu = 1$ and choose a set of characters such that

$$e_0 + \cdots + e_r = m\left\lfloor \frac{r}{2} \right\rfloor$$

This is always possible with $0 < e_i < m$ since $r + 1 \leq m\left\lfloor \frac{r}{2} \right\rfloor < mr$. In this case, since $f = 1$ and $\mu = 1$,

$$\sum_{i=0}^{r} s\left(\frac{(q-1)\mu r_i}{m}\right) = (p-1)\sum_{i=0}^{r}\left\{\frac{e_i}{m}\right\} = (p-1)\sum_{i=0}^{r}\frac{e_i}{m} = (p-1)\left\lfloor\frac{r}{2}\right\rfloor < (p-1)\frac{r+1}{2}$$

Therefore, by Theorem 6.14, F_r^m cannot be supersingular. □

Proposition 8.2. *Let p be a prime, and $f > 2$, let $n = \frac{p^f-1}{p-1}$. Then F_3^n is not supersingular over $\mathbb{F}_p$.*

Proof. Let $\mu = 1$, and $\overline{r} = (1, 1, 1, m-3)$. We know that $s(\frac{(q-1)\mu r}{m}) = p - 1$ when $r = 1$ using the fraction part formula for s because all the terms are less than 1.

Now consider

$$s\left(\frac{(m-3)(q-1)}{m}\right) = (p-1)\sum_{i=1}^{f-1}\left\{\frac{(m-3)p^i}{m}\right\}$$

If $i < f - 1$, then $3p^i < m$, so

$$\left\{\frac{(m-3)p^i}{m}\right\} = 1 - \frac{3p^i}{m}$$

. If $i = f-1$, then use the relation

$$p^{f-1} = m - (1 + p + \cdots + p^{f-2}),$$

so
$$\left\{\frac{(m-3)(m-(1+p+\cdots+p^{f-2}))}{m}\right\} = \frac{3(1+p+\cdots+p^{f-2})}{m}$$

. As a result, $s\left(\frac{(q-1)(m-3)}{m}\right) = (p-1)(f-1)$. And

$$\sum_{i=0}^{r} s\left(\frac{(q-1)r_i}{n}\right) = (f+2)(p-1) < 2f(p-1)$$

if $f > 2$. Therefore, F_3^n cannot be supersingular if $f > 2$. $\square$

Proposition 8.3. *When f is even, and $n = \frac{p^f-1}{p^2-1}$, then F_3^n is not supersingular.*

Proof. Let $\mu = 1$, $\overline{r} = (1, 1, 1, n-3)$, and write $m = 1 + p^2 + p^4 + \cdots + p^{f-2}$. Notice that $p^{f-1} = pm - (p + p^3 + \cdots + p^{f-3})$. When $r = 1$,

$$\begin{aligned} s(\frac{(q-1)}{m}) &= (p-1)\sum_{i=1}^{f-1}\{\frac{p^i}{m}\} \\ &= (p-1)(\sum_{i=0}^{f-2}(\frac{p^i}{m}) + \{\frac{pm-(p+p^3+\cdots+p^{f-3})}{m}\}) \\ &= (p-1)(1 + \frac{1+p^2+\cdots+p^{f-2}}{m}) \\ &= 2(p-1). \end{aligned}$$

When $r = m-3$, we have

$$\begin{aligned} s(\frac{(q-1)(m-3)}{m}) &= (p-1)\sum_{i=1}^{f-1}\{\frac{p^i(m-3)}{m}\} \\ &= (p-1)(\sum_{i=0}^{f-2}(1-\frac{3p^i}{m}) + \{\frac{(m-3)(pm-(p+p^3+\cdots+p^{f-3}))}{m}\}) \\ &= (p-1)(f-1+\sum_{i=0}^{f-2}(-\frac{3p^i}{m}) + \frac{3(p+p^3+\cdots+p^{f-3})}{m}) \\ &= (p-1)(f-1-\frac{3m}{m}) \\ &= (p-1)(f-4). \end{aligned}$$

In total we still have
$$\sum_{i=0}^{r} s(\frac{(q-1)r_i}{n}) = (f+2)(p-1) < 2f(p-1).$$

$\square$

Proposition 8.4. *When $n = p + a$ for $1 < a < p$, and $\mathrm{ord}_n(p) = 2$, the Fermat variety X_n is not supersingular.*

Proof. Still consider $\mu = 1$, $\overline{r} = (1, 1, 1, n-3)$. We have $\{1/n\} + \{p/n\} = (1+p)/n < 1$ for $r = 1$. And since $\mathrm{ord}_n(p) = 2$, n does not divides $p-1$ but n divides p^2-1, so $n|(p+1)$. Then $\{(n-3)/n\} + \{(n-3)p/n\}$ is an integer. Thus it has to be 1. This tell us that the sum of the s functions is less than $4(p-1)$. Therefore, X_n is not supersingular. $\square$

Conjecture 8.5. *For p a prime, and $f > 2$, let $n = \Phi_f(p) = \frac{p^f-1}{k(p)}$, then $\mathrm{ord}_n(p) = f$, and the Fermat surface F_3^n is not supersingular.*

Lemma 8.6. *Let X be a variety defined by the zero set of the equation:*

$$a_0x_0^{n_0} + a_1x_1^{n_1} + a_2x_2^{n_2} + a_3x_3^{n_3} = 0$$

over $\mathbb{F}_{p^k}$ with $a_i \in \mathbb{Z}, n_i \in \mathbb{Z}_{\geq 1}$. Let $m = \mathrm{lcm}\,(n_0, n_1, n_2, n_3)$ and let $w_i = \frac{m}{n_i}$ for $i = 0, 1, 2, 3$. Then X is supersingular if and only if for all $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $e_0, e_1, e_2, e_3 \in \mathbb{Z}$ with $m|e_0 + e_1 + e_2 + e_3$, $w_i|e_i$, $0 < e_i < m$ we have:

$$\sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0p^i}{m}\right\} + \left\{\frac{\mu e_1p^i}{m}\right\}\right) = \sum_{i=0}^{f-1}\left(\left\{\frac{-\mu e_2p^i}{m}\right\} + \left\{\frac{-\mu e_3p^i}{m}\right\}\right)$$

Proof. By Theorem 3.1, we only need to prove that it is supersingular over $\mathbb{F}_q$ for some power $q = p^f$. Suppose r is the smallest positive integer such that $p^r \equiv -1 \pmod{m}$. We'll take $f = 2r$, so that f is the minimal integer for which $m|p^f - 1$.

Let χ be a character of order m. Now, by Corollary 5.4.1, X is supersingular if the product of Gaussian sums for each α has argument root of unity. That is,

$$\prod_{i=0}^{3} g(\chi^{e_i})$$

must always have argument a root of unity where $m|e_0 + e_1 + e_2 + e_3$, $0 < e_i < m$, and $w_i|e_i$ for each i.

Consider the ideal generated by,

$$q^{-2}\prod_{i=0}^{3} g(\chi^{e_i}) = \frac{g(\chi^{e_0})g(\chi^{e_1})\chi^{e_2+e_3}(-1)}{g(\chi^{-e_2})g(\chi^{-e_3})}$$

By Corollary 6.13.1, this is a root of unity if and only if the ideal generated by it is $\mathcal{O}$, which will occur if and only if the valuation of each prime ideal in $\mathbb{Q}(\zeta_m, \zeta_p)$ is 0. By Theorem 6.4, this will occur if and only if:

$$s\left(\frac{(q-1)\mu e_0}{m}\right) + s\left(\frac{(q-1)\mu e_1}{m}\right) = s\left(\frac{-(q-1)\mu e_2}{m}\right) + s\left(\frac{-(q-1)\mu e_3}{m}\right)$$

for all μ relatively prime to m where $s(n)$ is the sum of the digits of $n \pmod{q-1}$ in base p. Even Further, by [Lang's Algebraic Number Theory Page 96], this is equivalent to:

$$\sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0p^i}{m}\right\} + \left\{\frac{\mu e_1p^i}{m}\right\}\right) = \sum_{i=0}^{f-1}\left(\left\{\frac{-\mu e_2p^i}{m}\right\} + \left\{\frac{-\mu e_3p^i}{m}\right\}\right)$$

as desired. □

Definition 8.7. Define the sum,

$$S_\mu(e_0, \ldots, e_t) = s\left(\frac{(q-1)\mu e_0}{m}\right) + \cdots + s\left(\frac{(q-1)\mu e_t}{m}\right) = \sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0p^i}{m}\right\} + \cdots + \left\{\frac{\mu e_tp^i}{m}\right\}\right)$$

Corollary 8.7.1. *X is supersingular if and only if the value of the sum,*

$$S_\mu(e_0, e_1) = \sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0p^i}{m}\right\} + \left\{\frac{\mu e_1p^i}{m}\right\}\right)$$

for each fixed value of $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ depends only on $E \equiv e_0 + e_1 \mod m$.

Proof. We know that X is supersingular if and only if,

$$\sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0 p^i}{m}\right\}+\left\{\frac{\mu e_1 p^i}{m}\right\}\right)=\sum_{i=0}^{f-1}\left(\left\{\frac{-\mu e_2 p^i}{m}\right\}+\left\{\frac{-\mu e_3 p^i}{m}\right\}\right)$$

for each $\mu \in (Z/m\mathbb{Z})^\times$ and e_0, e_1, e_2, e_3 such that $m \mid e_0+e_1+e_2+e_3$ and $w_i \mid e_i$. Therefore, whenever,

$$E \equiv e_0+e_1 \equiv -e_2-e_3 \mod m$$

we must have that $S_\mu(e_0,e_1)=S_\mu(-e_2,-e_3)$. This is equivalent to S_μ depending on E alone. □

Lemma 8.8. *Let p be a prime number, f be a positive integer, m be an integer not divisible by p, and $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$. For integers $m \nmid e_0, e_1$ define:*

$$N_\mu(e_0,e_1)=\#\left\{i\ :\ \left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}<\left\{\frac{\mu e_0 p^i}{m}\right\}\right\},$$

where $i=0,\dots,f-1$, then

$$S_\mu(e_0,e_1)=\sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0 p^i}{m}\right\}+\left\{\frac{\mu e_1 p^i}{m}\right\}\right)=N_\mu(e_0,e_1)+\sum_{i=0}^{f-1}\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}=N_\mu(e_0,e_1)+S_\mu(e_0+e_1).$$

Proof. Note that

$$\left\{\frac{\mu e_0 p^i}{m}\right\}+\left\{\frac{\mu e_1 p^i}{m}\right\}$$

is either equal to $\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}$ or $\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}+1$. If it is equal to the former, then

$$\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}\geq\left\{\frac{\mu e_0 p^i}{m}\right\}$$

If it is equal to the latter, then

$$\left\{\frac{\mu e_0 p^i}{m}\right\}=\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}-\left\{\frac{\mu e_1 p^i}{m}\right\}+1>\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}$$

Thus we have:

$$\left\{\frac{\mu e_0 p^i}{m}\right\}+\left\{\frac{\mu e_1 p^i}{m}\right\}=\begin{cases}\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\} & \left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}\geq\left\{\frac{\mu e_0 p^i}{m}\right\}\\ \left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}+1 & \left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}<\left\{\frac{\mu e_0 p^i}{m}\right\}\end{cases}$$

□

Corollary 8.8.1. *If $e_0+e_1\equiv 0 \mod m$ then $S_\mu(e_0,e_1)=N_\mu(e_0,e_1)=f$.*

Proof.

$$S_\mu(e_0,e_1)=\sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0 p^i}{m}\right\}+\left\{\frac{\mu e_1 p^i}{m}\right\}\right)=N_\mu(e_0,e_1)+\sum_{i=0}^{f-1}\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}$$

However, $m \mid e_0+e_1$ so the fractional part of all multiplies of their quotient is zero. Thus,

$$\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}=0$$

Therefore, the second sum is zero. Furthermore, since $m \nmid e_0$ and $(m,p)=(m,\mu)=1$ we have that,

$$0\leq\left\{\frac{\mu e_0 p^i}{m}\right\}$$

for each i. Therefore, $N(e_0,e_1)=f$. □

Lemma 8.9. *The product $q^{-2}g(\chi^{e_0})g(\chi^{e_1})g(\chi^{e_2})g(\chi^{e_3})$ is a root of unity if and only if $N_\mu(e_0,e_1)+N_\mu(e_2,e_3) = f$ for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$*

Proof. By Theorem 6.14 we need only check if,

$$\sum_{i=0}^{3} s\left(\frac{(q-1)\mu e_i}{m}\right) = 2(p-1)f$$

for each $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$. However, because $m \mid e_0+e_1+e_3+e_4$ by Corollary 8.8.1,

$$S_\mu(e_0+e_1) + S_\mu(e_2+e_3) = S_\mu(e_0+e_1, e_2+e_3) = f$$

Furthermore, by Lemma, 8.8,

$$S_\mu(e_0,e_1)+S_\mu(e_2,e_3) = N_\mu(e_0,e_1)+N_\mu(e_2,e_3)+S_\mu(e_0+e_1)+S_\mu(e_2+e_3) = N_\mu(e_0,e_1)+N_\mu(e_2,e_3)+f$$

Thus,

$$S_\mu(e_0,e_1)+S_\mu(e_2,e_3) = \frac{1}{p-1}\sum_{i=0}^{3} s\left(\frac{(q-1)\mu e_i}{m}\right) = 2f \iff N_\mu(e_0,e_1)+N_\mu(e_2,e_3) = f$$

□

Theorem 8.10. *Let X be a variety defined by the zero set of the equation:*

$$a_0x_0^{n_0} + a_1x_1^{n_1} + a_2x_2^{n_2} + a_3x_3^{n_3} = 0$$

over $\mathbb{F}_{p^k}$ with $a_i \in \mathbb{Z}, n_i \in \mathbb{Z}_{\geq 1}$. Let $m = \operatorname{lcm}(n_0,n_1,n_2,n_3)$. If $a_i \neq 0$ in $\mathbb{F}_p$ for all i and there exists r such that $p^r \equiv -1 \pmod{m}$, then X is supersingular.

Proof. By Corollary 8.7.1, if we can show that for all $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ and e_0, e_1 with $0 < e_0, e_1 < m$ the sum $S_\mu(e_0,e_1)$ is only a function of $E = e_0+e_1$, then X is supersingular. Let $N(e_0,e_1)$ be as defined in lemma 8.8. If $m|E$, then we will always have:

$$\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\} < \left\{\frac{\mu e_0 p^i}{m}\right\}$$

and thus $N(e_0,e_1) = f$. If $m \nmid E$, then note that as $p^r \equiv -1 \pmod{m}$, we have:

$$\left\{\frac{\mu E p^{i+r}}{m}\right\} = \left\{\frac{-\mu E p^i}{m}\right\} = 1 - \left\{\frac{\mu E p^i}{m}\right\}$$

Therefore, applying this procedure to the above inequality,

$$\left\{\frac{\mu(e_0+e_1)p^{i+r}}{m}\right\} < \left\{\frac{\mu e_0 p^{i+r}}{m}\right\} \iff 1-\left\{\frac{\mu(e_0+e_1)p^i}{m}\right\} < 1-\left\{\frac{\mu e_0 p^i}{m}\right\} \iff \left\{\frac{\mu e_0 p^i}{m}\right\} < \left\{\frac{\mu(e_0+e_1)p^i}{m}\right\}$$

Furthermore, since $m \nmid e_0, e_1$ the inequality must always be strict. Since $f = 2r$, this symmetry implies that $N(e_0,e_1) = \frac{f}{2}$. Note that $N(e_0,e_1)$ is constant. Thus by Lemma 8.8,

$$S_\mu(e_0,e_1) = \sum_{i=0}^{f-1}\left(\left\{\frac{\mu e_0 p^i}{m}\right\} + \left\{\frac{\mu e_1 p^i}{m}\right\}\right)$$

is a function of E alone and thus X is supersingular. □

Theorem 8.11. *If there exists $v \in \mathbb{Z}$ such that $p^v \equiv -1 \mod m$ then F_r^m is supersingular for any r.*

Proof. Consider the sum,

$$S_\mu(e_1,\ldots,e_r) = \frac{1}{p-1}\sum_{i=0}^{r} s\left(\frac{\mu(q-1)e_i}{m}\right) = \sum_{i=0}^{r}\sum_{j=0}^{f-1}\left\{\frac{\mu e_i p^j}{m}\right\}$$

which we can rearrange as,

$$S_\mu(e_1,\ldots,e_r) = \sum_{i=0}^{r}\left(\sum_{j=0}^{\frac{f}{2}-1}\left\{\frac{\mu e_i p^j}{m}\right\} + \sum_{j=0}^{\frac{f}{2}-1}\left\{\frac{\mu e_i p^{j+\frac{f}{2}}}{m}\right\}\right)$$

However, since $f = \text{ord}_m p$ and the hypothesis, we know that $p^{\frac{f}{2}} \equiv -1 \mod m$. Thus,

$$\left\{\frac{\mu e_i p^{j+\frac{f}{2}}}{m}\right\} = \left\{\frac{-\mu e_i p^j}{m}\right\} = 1 - \left\{\frac{\mu e_i p^j}{m}\right\}$$

Therefore, plugging in,

$$S_\mu(e_1,\ldots,e_r) = \sum_{i=0}^{r}\left(\sum_{j=0}^{\frac{f}{2}-1}\left\{\frac{\mu e_i p^j}{m}\right\} + \sum_{j=0}^{\frac{f}{2}-1}\left[1 - \left\{\frac{\mu e_i p^j}{m}\right\}\right]\right) = \sum_{i=0}^{r}\sum_{j=0}^{\frac{f}{2}-1} 1 = (r+1)\frac{f}{2}$$

Thus, by Theorem 6.15, F_r^m is supersingular. □

Lemma 8.12. *Let $\sigma \in S_n$ be a permutation and $C \in S_n$ be the standard n-cycle,*

$$C = (1\,2\,3\,\cdots\,n)$$

Define the function,

$$g(\sigma,k) = \#\{i \in [n] \mid \sigma(i) < \sigma C^k(i)\}$$

Then $g(\sigma,k) + g(\sigma,n-k) = n$ for all $0 < k < n$.

Proof. Since σ is a permutation, we can reindex the set in the definition of g by $j = \sigma(i)$ such that,

$$g(\sigma,k) = \#\{j \in [n] \mid j < \sigma C^k \sigma^{-1}(j)\}$$

However, conjugation is an automorphism so,

$$\sigma C^k \sigma^{-1} = (\sigma C \sigma^{-1})^k = C_\sigma^k$$

where $C_\sigma = \sigma C \sigma^{-1}$ is also an n cycle (with order n) since conjugation preserves cycle type. Thus,

$$g(\sigma,k) = \#\{j \in [n] \mid j < C_\sigma^k(j)\}$$

However, if $j < C_\sigma^k(j)$ then define $\tilde{j} = C_\sigma^k(j)$ or equivalently $C_\sigma^{n-k}(\tilde{j}) = j$ such that,

$$C_\sigma^{n-k}(\tilde{j}) < \tilde{j}$$

However, n cycles act freely on $[n]$ so there are no fixed points of C_σ^k for any $0 < k < n$. Thus, the set of $\tilde{j}$ such that $C_\sigma^{n-k}(\tilde{j}) < \tilde{j}$ is exactly the compliment of the set such that $\tilde{j} < C_\sigma^{n-k}(\tilde{j})$. Therefore, $j \in g(\sigma,k) \iff \tilde{j} \notin g(\sigma,n-k)$ so,

$$g(\sigma,k) = \{\tilde{j} \in [n] \mid C_\sigma^{n-k}(\tilde{j}) < \tilde{j}\} = n - g(\sigma,n-k)$$

□

Corollary 8.12.1. *If there exists $\sigma \in S_n$ such that $g(\sigma,k) = g(\sigma,n-k)$ then $g(\sigma,k) = \frac{n}{2}$. In particular, this is true if $g(\sigma,k)$ is constant for $0 < k < n$.*

Corollary 8.12.2. *If n is odd then $g(\sigma, k) \neq g(\sigma, n-k)$ for all $0 < k < n$. In particular, this means that if n is odd, then there cannot exits $\sigma \in S_n$ such that $g(\sigma, k)$ is constant for all $0 < k < n$.*

Lemma 8.13. *Let $m, p, e_0, e_1, f, N(e_0, e_1)$ be as in lemma 8.8. If $f > 1$, $m | p^f - 1$ and E is such that $m \nmid E(p-1)$ and there exists a K such that for all $e_1 + e_2 \equiv E \pmod{M}$ with $m \nmid e_1, e_2$, we have*

$$N_\mu(e_0, e_1) = K$$

then $K = \frac{f}{2}$ where $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$ is fixed.

Proof. Suppose that such an E exists. Let

$$a_i = \left\{ \frac{\mu E p^i}{m} \right\}$$

Note as $m | p^f - 1$, we have $a_{i+f} = a_i$. Suppose $a_i = a_j$ for some integers i, j. Then we have:

$$Ep^i \equiv Ep^j \pmod{m}$$

which is true if and only if

$$E(p^{i-j} - 1) \equiv 0 \pmod{m}$$

This we hold only when $i - j$ is multiple of some integer t. As a result $a_{i+t} = a_i$ but $a_0, a_1, \ldots, a_{t-1}$ are distinct. Furthermore, since $m \nmid E(p-1)$ we have $t > 1$. For notation purposes. We now let permutations $\pi \in S_t$ act on the sequence a_i. As $a_0, a_1, \ldots, a_{t-1}$ are distinct, there exists a permutation $\sigma \in S_t$ such that for $i = 0, \ldots, t-1$. $a_\sigma(i) < a_\sigma(j)$ if and only if $i < j$ for $0 \leq i, j \leq t-1$. Since the condition $N_\mu(e_0, e_1) = K$ must hold for all $e_0 + e_1 \equiv E \mod m$ we may pick a particualr value of,

$$e_0|_j = Ep^j \text{ and } e_1|_j = E - e_0|_j$$

for any $1 \leq j \leq t-1$. In this case,

$$\left\{ \frac{\mu e_0|_j p^i}{m} \right\} = a_{i+j}$$

Thus if we let $C = (1\ 2\ \cdots\ t) \in S_t$, then this can be rewritten as:

$$\left\{ \frac{\mu e_0|_j p^i}{m} \right\} = a_{C^j(i)}$$

By definition,

$$K = N_\mu(e_0|_j, e_1|_j) = \#\{0 \leq i < t \ : \ a_i < a_{i+j}\}$$

As a_i is periodic, this is implies

$$\begin{aligned} K &= \frac{f}{t} \#\{i \ : \ a_i < a_{C^j(i)}\} \\ &= \frac{f}{t} \#\{i \ : \ \sigma^{-1}(i) < \sigma^{-1}(C^j(i))\} = \frac{f}{t} g(\sigma^{-1}, j) \end{aligned}$$

However, by lemma 8.12,

$$g(\sigma^{-1}, j) = g(k) = t - g(t-k)$$

As $t > 1$, taking $k = 1$ implies $g(\sigma^{-1}, k) = \frac{t}{2}$. Thus:

$$K = \left(\frac{f}{t}\right)\left(\frac{t}{2}\right) = \frac{f}{2}$$

□

Theorem 8.14. *If f is odd and $f > 1$, then F_3^m is not supersingular*

Proof. By Corollary 8.7.1, F_3^m is supersingular only if for all e_0, e_1 with $0 < e_0, e_1 < m$ we have that

$$S_\mu(e_0, e_1) = \sum_{i=0}^{f-1} \left(\left\{ \frac{\mu e_0 p^i}{m} \right\} + \left\{ \frac{\mu e_1 p^i}{m} \right\} \right)$$

is only a function of $E = e_0 + e_1$. Consider the case $E = 1$. Let $N(e_0, e_1)$ be defined as in lemma 8.8. By the same lemma, the above being a function of E is equivalent to $N(e_0, e_1)$ being constant across $e_0 + e_1$. By lemma 8.13, if it is constant for fixed E, then it must always be $\frac{f}{2}$. However, as $N(e_0, e_1)$ is integer-valued this is impossible. Thus we have a contradiction, so F_3^m is not supersingular. □

Theorem 8.15. *Let $f = \mathrm{ord}_n(p)$. If f is odd and $f > 1$, then F_2^n is not supersingular*

Proof. By Theorem 3.1, we only need to prove that it is supersingular over $\mathbb{F}_q$ for some power $q = p^f$. Let χ be a character of order n. By Theorem 5.3, we have that

$$\zeta(T) = \frac{p(T)}{q(T)}$$

where $p(T) = -1$ and the roots of $q(T)$ are of the form:

$$\prod_{i=0}^{2} \chi^{e_i}(a_i^{-1}) \prod_{i=0}^{2} g(\chi^{e_i})$$

where $m | e_0 + e_1 + e_2$ and $0 < e_i < n$, and $w_i | e_i$ for each i. The product $\prod_{i=0}^{2} \chi^{e_i}(a_i^{-1})$ will always be a root of unity. Thus to show $\zeta(T)$ is supersingular, we just need to show that $\prod_{i=0}^{2} g(\chi^{e_i})$ always has argument a root of unity. We will now do so.

Consider the ideal generated by,

$$q^{-3/2} \prod_{i=0}^{2} g(\chi^{e_i}) = \frac{g(\chi^{e_0}) g(\chi^{e_1}) \chi^{e_2}(-1)}{q^{-1/2} g(\chi^{-e_2})}$$

By Corollary 6.13.1, this is a root of unity if and only if the ideal generated by it is R, which will occur if and only if the valuation of each prime ideal in $\mathbb{Q}(\zeta_n, \zeta_p)$ is 0. By Theorem 6.4, this will occur if and only if:

$$s\left(\frac{(q-1)\mu e_0}{n}\right) + s\left(\frac{(q-1)\mu e_1}{n}\right) = s\left(\frac{-(q-1)\mu e_2}{n}\right) + \frac{f}{2}$$

By [Lang Algebra Page 96] this is equal to,

$$\sum_{i=0}^{f} \left(\left\{ \frac{\mu e_0 p^i}{n} \right\} + \left\{ \frac{\mu e_1 p^i}{n} \right\} - \left\{ \frac{\mu - e_2 p^i}{n} \right\} \right) = \frac{f}{2}$$

However, as $e_0 + e_1 \equiv -e_2 \pmod{n}$, each term in the above summation must be either 1 or 0. Thus the left hand side is an integer. However, if f is odd, the right hand side is not. Thus this equality cannot possibly happen. □

Theorem 8.16. *Let f be odd and m be even, then the Fermat variety F_3^m is not supersingular.*

Proof. We know that X is supersingular if and only if $q^{-2} \prod_{i=0}^{3} g(\chi^{e_i})$ is a root of unity, where $m | e_0 + e_1 + e_2 + e_3$ and $0 < e_i < m$ for each i.
Let $e_0 + e_1 = E_0$, and $e_2 + e_3 = E_2$. By lemma 8.9, we know that V_m is supersingular if and only if $N(e_0, e_1) + N(e_2, e_3) = f$. Now let $E_0 + E_2 = 3m$, and $e_0 = e_2$, $e_1 = e_3$. Then $E_0 = 3/2m$ is an integer because m is even. But $N_0 \neq f/2$ because N_0 is an integer but f is odd, so $f/2$ is not an integer. We also know that $N_0 = N_2$, since $e_0 = e_2$, $e_1 = e_3$. Thus it is impossible that $N_0 + N_2 = f$. Therefore, F_3^m is not supersingular. □

Theorem 8.17. *Let f be odd, the Fermat variety F_r^m is not supersingular if r is odd.*

Proof. We prove this using Theorem **??** and Lemma 8.8.

We know that F_r^m is supersingular if and only if

$$\sum_{i=0}^{r} S_\mu(e_i) = (p-1)(r+1)f/2$$

for all $\mu \in (\mathbb{Z}/m\mathbb{Z})^\times$, and $m|e_0 + e_1 + \cdots + e_r$ and $0 < e_i < m$ for each i. Thus, we can choose e_i for $i > 3$ such that $m|e_i + e_{i+1}$. Then for any given μ, $S_\mu(e_i, e_{i+1}) = f$ by Lemma 8.8.

On the other hand, choose $e_0, \ldots, e_3$ as in Theorem **??**, then $S_\mu(e_0, e_1, e_2, e_3) \neq 2f$.

Therefore, we have

$$\sum_{i=0}^{r} S_\mu(e_i) \neq (p-1)(r+1)f/2$$

for this chosen set of e_i, so F_r^m is not supersingular.

□

Conjecture 8.18. *Let $q = p^n$, p a prime and $n \in \mathbb{Z}^+$, be the order of our finite field $\mathbb{F}_q$ and let N_μ be the number of solutions (e_0, e_1, e_2, e_3) with $0 < e_i < q-1$ all distinct and $\mu \in \mathbb{Z}^+$ with $(\mu, q-1) = 1$ satisfying $s(\mu e_0) + s(\mu e_1) = s(\mu e_2) + s(\mu e_3)$. We conjecture that $N_1 = N_p$, and for $\mu_j, \mu_k > p$, $N_{\mu_j} = N_{\mu_k}$ if μ_j and μ_k share the same largest factor.*

9 Sum-Product Varieties

9.1 Introduction

In this section we concern ourselves with the family of varieties,

$$x_1 + \cdots + x_d = \lambda x_1 \cdots x_d$$

over the finite field $\mathbb{F}_q$. In the process, we will study the m-values which are solutions to the set of simultaneous equations,

$$x_1 + \cdots + x_d = z \quad \text{and} \quad x_1 \cdots x_d = y$$

over $\mathbb{F}_q$. (Motivation?)

Definition 9.1. The integer, $m_{y,z}^{d,q}$ is the number of solutions to the set simultaneous of equations,

$$\begin{aligned} x_1 + \cdots + x_d &= z \\ x_1 \cdots x_d &= y \end{aligned}$$

over $\mathbb{F}_q$.

Definition 9.2. The diagonal hyper-plane number is the number of solutions,

$$H_z^d(S) = \#\{x_1 + \cdots + x_d = z \mid x_i \in S\}$$

where $S \subset K$ and $z \in K$ for some field K.

Proposition 9.3. *For any $z \in \mathbb{F}_q$ we have $H_z^d(\mathbb{F}_q) = q^{d-1}$ and for $z \in \mathbb{F}_q$ we have,*

$$H_z^d(\mathbb{F}_q^\times) = \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

Proof. For any choice of $x_1, \cdots, x_{d-1} \in \mathbb{F}_q$ there is a unique $x_d \in \mathbb{F}_q$ such that $x_1 + \cdots + x_d = z$. Thus, $H_z^d(\mathbb{F}_q) = q^{d-1}$. We will no count how many solutions contain no zeros. By inclusion exclusion,

$$\begin{aligned}
H_z^d(\mathbb{F}_q^\times) &= H_z^d(\mathbb{F}_q) - \binom{d}{1} H_z^{d-1}(\mathbb{F}_q) + \binom{d}{2} H_z^{d-2}(\mathbb{F}_q) + \cdots + \binom{d}{d}(-1)^d H_z^0(\mathbb{F}_d) \\
&= \sum_{i=0}^{d-1} \binom{d}{i} (-1)^i q^{d-1-i} + (-1)^d \delta_z = \frac{1}{q}\left[\sum_{i=0}^{d-1} \binom{d}{i}(-1)^i q^{d-i}\right] + (-1)^d \delta_z \\
&= \frac{1}{q}\left[(q-1)^d - (-1)^d\right] + (-1)^d \delta_z
\end{aligned}$$

where the factor of δ_z comes from the fact that for $z \neq 0$ the set $H_z^0(\mathbb{F}_q)$ is empty but for $z = 0$ has one element representing the all zero solution to the original problem. Therefore,

$$H_z^d(\mathbb{F}_q^\times) = \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

□

Proposition 9.4.

$$m_{0,z}^{d,q} = q^{d-1} - \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

Proof. Solutions to the set of simultaneous equations $x_1 + \cdots x_d = z$ and $x_1 \cdots x_d = 0$ are exactly those solutions to $x_1 + \cdots + x_d = z$ which are not all elements of $\mathbb{F}_q^\times$. Therefore,

$$m_{0,z}^{d,q} = H_z^d(\mathbb{F}_q) - H_z^d(\mathbb{F}_q^\times) = q^{d-1} - \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

□

Corollary 9.4.1. *For $z \neq 0$ we have, $m_{0,z}^{d,q} - m_{0,0}^{d,q} = (-1)^d$*

Proposition 9.5.

$$\sum_{y \in \mathbb{F}_q} m_{y,z}^{d,q} = q^{d-1} \quad \text{and} \quad \sum_{z \in \mathbb{F}_q} m_{y,z}^{d,q} = \begin{cases} (q-1)^{d-1} & y \neq 0 \\ q^d - (q-1)^d & y = 0 \end{cases}$$

Proof.

$$\sum_{y \in \mathbb{F}_q} m_{y,z}^{d,q} = \# \{x_1 + \cdots + x_d = z \mid x_i \in \mathbb{F}_q\} = H_z^d(\mathbb{F}_q) = q^{d-1}$$

Likewise,

$$\sum_{z \in \mathbb{F}_q} m_{y,z}^{d,q} = \# \{x_1 \cdots x_d = z \mid x_i \in \mathbb{F}_q\} = \begin{cases} (q-1)^{d-1} & y \neq 0 \\ q^d - (q-1)^d & y = 0 \end{cases}$$

because if $y \neq 0$ then every solution to $x_1 \cdots x_d = y$ must have $x_i \neq 0$ for each i and for any choice of $x_1, \cdots, x_{d-1} \in \mathbb{F}_q^\times$ there is a unique choice of x_d such that $x_1 \cdots x_d = y$. Thus, in the case $y \neq 0$ there are exactly $(q-1)^{d-1}$ solutions. However, if $y = 0$ then the condition $x_1 \cdots x_d = 0$ is equivalent to not all x_i being in $\mathbb{F}_q$ and thus $\#(\mathbb{F}_q)^d - \#(\mathbb{F}_q^\times)^d = q^d - (q-1)^d$. □

Proposition 9.6.

$$\sum_{y \in \mathbb{F}_q^\times} m_{y,z}^{d,q} = \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

Proof. Since having some product $y \neq 0$ is equivalent to all $x_i \neq 0$ we have,

$$\sum_{y \in \mathbb{F}_q^\times} m_{y,z}^{d,q} = \# \{x_1 + \cdots x_d = z \mid x_i \neq 0\} = H_z^d(\mathbb{F}_q^\times) = \frac{1}{q}\left[(q-1)^d + (q\delta_z - 1)(-1)^d\right]$$

□

9.2 Relationships Between m-values

Lemma 9.7.

$$\#\left(\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n\right) = \gcd(n, q-1)$$

Proof. Let $w \in \mathbb{F}_q^\times$ be a generator. The group, $\mathbb{F}_q^\times)^n$ is generated by w^n which has order $\frac{q-1}{\gcd(n,q-1)}$. Therefore, $\#(\mathbb{F}_q^\times)^n = \frac{q-1}{\gcd(n,q-1)}$ and thus,

$$\#\left(\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n\right) = \gcd(n, q-1)$$

□

Proposition 9.8. *Let $\pi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^d$ be the projection map. If $\pi(y) = \pi(y')$ then $m_{y,0}^{d,q} = m_{y',0}^{d,q}$.*

Proof. Suppose that $\pi(y) = \pi(y')$. Then, $y' = y\lambda^d$. Suppose that $x_1 + \cdots + x_d = 0$ and $x_1 \cdots x_d = y$ is a solution for $m^{d,q}y, 0$. Then, consider the point $\lambda x_1, \cdots, \lambda x_d$. We have,

$$\lambda x_1 + \cdots + \lambda x_d = \lambda(x_1 + \cdots + x_d) = 0$$

and

$$\lambda x_1 \cdots \lambda x_d = \lambda^d(x_1 \cdots x_d) = \lambda^d y = y'$$

Therefore, $\lambda x_1, \cdots, \lambda x_d$ is a solution for $m_{y',0}^{d,q}$. Furhtermore, $\lambda \neq 0$ so multiplication by λ is invertible. □

Corollary 9.8.1. *If $\gcd(d, q-1) = 1$ then $m_{y,0}^{d,q} = m_{y',0}^{d,q}$ for all $y, y' \in \mathbb{F}_q$.*

Proposition 9.9. *Let σ be an automorphism of $\mathbb{F}_q$ then $m_{y,z}^{d,q} = m_{\sigma(y),\sigma(z)}^{d,q}$.*

Proof. Since σ is an automorphism, it is an invertible map which preserves the structure of polynomial equations and therefore gives a bijection between $m_{y,z}^{d,q}$ and $m_{\sigma(y),\sigma(z)}^{d,q}$. □

Proposition 9.10. *If $y, z \neq 0$ then for any $\lambda \in \mathbb{F}_q^\times$ we have $m_{y,z}^{d,q} = m_{\lambda^d y,\lambda z}^{d,q}$.*

Proof. Multiplication by $\lambda \in \mathbb{F}_q^\times$ is invertible and takes solutions for $m_{y,z}^{d,q}$ to solutions for $m_{\lambda^d y,\lambda z}^{d,q}$. □

Corollary 9.10.1. *If $q - 1 \mid d$ then for $y, z, z' \neq 0$ we have $m_{y,z}^{d,q} = m_{y,z'}^{d,q}$.*

Proof. We know that for any $\lambda \in \mathbb{F}_q^\times$ we have $m_{y,z}^{d,q} = m_{\lambda^d y,\lambda z}^{d,q}$. However, $q - 1 \mid d$ so d is an exponent of $\mathbb{F}_q^\times$ so $\lambda^d = 1$. □

Lemma 9.11. *Let $Z_y = \frac{1}{q-1} m_{y,0}^{d,q}$. If $q - 1 \mid d$ then Z_y is an integer.*

Proof. Any solution $x_1 + \cdots + x_d = 0$ and $x_1 \cdots x_y = y$ can be taken to another distinct solution $\lambda x_1 + \cdots + \lambda x_d = \lambda(x_1 + \cdots + x_d) = 0$ and $\lambda x_1 \cdots \lambda x_d = \lambda^d(x_1 \cdots x_d) = \lambda^d y = y$ by multiplication by λ. Since $y \neq 0$ we have that $x_1, \cdots, x_d \in \mathbb{F}_q^\times$ for any such solution (since their product is nonzero) and thus multiplication by $\lambda \in \mathbb{F}_q^\times$ acts freely on the set of solutions. Thus, each orbit has size $\#(\mathbb{F}_q^\times) = q - 1$ but the orbits form a partition so $q - 1 \mid m_{y,0}^{d,q}$. □

Lemma 9.12. *If for $y, z, z' \neq 0$ we have $m_{y,z}^{d,q} = m_{y,z'}^{d,q}$ then,*

$$m_{y,z}^{d,q} = (q-1)^{d-2} - Z_y$$

Proof. For $y, z \neq 0$ we have that,

$$(q-1)m_{y,z}^{d,q} + m_{y,0}^{d,q} = \sum_{z \in \mathbb{F}_q} m_{y,z}^{d,q} = (q-1)^{d-1}$$

Thus,

$$m_{y,z}^{d,q} = \frac{1}{q-1}\left[(q-1)^{d-1} - m_{y,0}^{d,q}\right]$$

□

Lemma 9.13. *If $m_{y,0}^{d,q} = m_{y',0}^{d,q}$ for all $y, y' \in \mathbb{F}_q^\times$ then,*

$$m_{y,0}^{d,q} = \frac{1}{q}\left[(q-1)^{d-1} + (-1)^d\right]$$

for each $y \in \mathbb{F}_q^\times$.

Proof. We have that,

$$(q-1)m_{y,0}^{d,q} = \sum_{y \in \mathbb{F}_q} m_{y,0}^{d,q} = \frac{1}{q}\left[(q-1)^d + (q-1)(-1)^d\right]$$

Therefore,

$$m_{y,0}^{d,q} = \frac{1}{q}\left[(q-1)^{d-1} + (-1)^d\right]$$

□

9.3 Powers of Gauss Sums

Theorem 9.14. *Let $\chi : \mathbb{F}_q \to \mathbb{C}^\times$ be a multiplicative character. If $q-1 \mid d$ then,*

$$g(\chi)^d = q \sum_{y \in \mathbb{F}_q^\times} Z_y \chi(y) - \delta_\chi \cdot \left[(q-1)^{d-1} + (-1)^d\right]$$

Proof. Let $\phi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial additive character. Consider,

$$\begin{aligned} g(\chi)^d &= \left[\sum_{x \in \mathbb{F}_q} \chi(x)\psi(x)\right]^d = \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_d \in \mathbb{F}_q} \chi(x_1)\cdots\chi(x_d)\psi(x_1)\cdots\psi(x_d) \\ &= \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_d \in \mathbb{F}_q} \chi(x_1 \cdots x_d)\psi(x_1 + \cdots + x_d) = \sum_{y \in \mathbb{F}_q} \sum_{z \in \mathbb{F}_q} \sum_{\substack{x_1 + \cdots + x_d = z \\ x_1 \cdots x_d = y}} \chi(y)\psi(z) \\ &= \sum_{y \in \mathbb{F}_q} \chi(y) \sum_{z \in \mathbb{F}_q} m_{y,z}^{d,q} \psi(z) \end{aligned}$$

However, since $q-1 \mid d$, by Lemma 9.10.1 we know that $m_{y,z}^{d,q} = m_{y,z'}^{d,q}$ if $y, z, z' \in \mathbb{F}_q^\times$. Therefore,

$$\begin{aligned} g(\chi)^d &= \sum_{y \in \mathbb{F}_q^\times} \chi(y) \sum_{z \in \mathbb{F}_q} m_{y,z}^{d,q}\psi(z) + \chi(0) \sum_{z \in \mathbb{F}_q} m_{0,z}^{d,q}\psi(z) \\ &= \sum_{y \in \mathbb{F}_q^\times} \chi(y) \left[m_{y,0}^{d,q}\psi(0) + m_{y,z}^{d,q} \sum_{z \in \mathbb{F}_q^\times} \psi(z)\right] + \chi(0)\left[m_{0,0}^{d,q}\psi(0) + m_{0,z}^{d,q} \sum_{z \in \mathbb{F}_q} \psi(z)\right] \end{aligned}$$

Because ψ is a nontrivial character,

$$\sum_{z \in \mathbb{F}_q} \psi(z) = 0 \implies \sum_{z \in \mathbb{F}_q^\times} \psi(z) = -1$$

since $\psi(0) = 1$. Therefore,

$$g(\chi)^d = \sum_{y \in \mathbb{F}_q^\times} \chi(y)\left[m_{y,0}^{d,q} - m_{y,z}^{d,q}\right] + \chi(0)\left[m_{0,0}^{d,q} - m_{0,z}^{d,q}\right]$$

where z is an arbitrary nonzero element (since these numbers are independent of choice of $z \neq 0$). Furthermore, by Lemma 9.12 we know that,

$$m_{y,0}^{d,q} - m_{y,z}^{d,q} = m_{y,0}^{d,q} + \frac{1}{q-1} m_{y,0}^{d,q} - (q-1)^{d-2} = qZ_y - (q-1)^{d-2}$$

Furthermore, by Lemma 9.4.1, $m_{0,z}^{d,q} - m_{0,0}^{d,q} = (-1)^d$. Putting these facts together,

$$g(\chi)^d = \sum_{y \in \mathbb{F}_q^\times} \chi(y) \left[qZ_y - (q-1)^{d-2} \right] - \chi(0)(-1)^d$$

Now we consider the case when χ is the trivial character χ_0 and when $\chi \neq \chi_0$. When $\chi \neq \chi_0$ we know that $\chi(0) = 0$ and that,

$$\sum_{y \in \mathbb{F}_q^\times} \chi(y) = 0$$

Therefore we get,

$$g(\chi)^d = q \sum_{y \in \mathbb{F}_q^\times} Z_y \chi(y)$$

When χ is the trivial character, $\chi(y) = 1$ for all $y \in \mathbb{F}_q$. Therefore,

$$g(\chi)^d = q \sum_{y \in \mathbb{F}_q^\times} Z_y \chi(y) - \left[(q-1)^{d-1} + (-1)^d \right]$$

□

Theorem 9.15. *Let $\widehat{\mathbb{F}_q}$ be the character group of $\mathbb{F}_q$ and $q-1 \mid d$. Then,*

$$Z_y = \frac{1}{q(q-1)} \left(\sum_{\chi \in \widehat{\mathbb{F}_q}} g(\chi)^d \, \overline{\chi}(y) + \left[(q-1)^{d-1} + (-1)^d \right] \right)$$

Proof. By Theorem 9.15, we know that,

$$q \sum_{y \in \mathbb{F}_q^\times} Z_y \chi(y) = g(\chi)^d + \delta_\chi \left[(q-1)^{d-1} + (-1)^d \right]$$

We will make use the character orthogonality relation,

$$\sum_{\chi \in \widehat{\mathbb{F}_q}} \chi(x) \overline{\chi}(y) = \begin{cases} (q-1) & x = y \\ 0 & x \neq y \end{cases}$$

for $x, y \in \mathbb{F}_q^\times$. Using this relation,

$$\sum_{\chi \in \widehat{\mathbb{F}_q}} \left(g(\chi)^d + \delta_\chi \left[(q-1)^{d-1} + (-1)^d \right] \right) \overline{\chi}(y) = q \sum_{\chi \in \widehat{\mathbb{F}_q}} \sum_{z \in \mathbb{F}_q^\times} Z_z \chi(z) \overline{\chi}(y) = q \sum_{z \in \mathbb{F}_q^\times} Z_z (q-1) \delta_{y-z} = q(q-1) Z_z$$

Furthermore, for $\chi = \chi_0$ we have $\overline{\chi}(y) = 1$. Thus,

$$q(q-1) Z_z = \sum_{\chi \in \widehat{\mathbb{F}_q}} g(\chi)^d \, \overline{\chi}(y) + \left[(q-1)^{d-1} + (-1)^d \right]$$

□

9.4 Special Cases of Sum-Product Varieties

Definition 9.16. The sum-product variety, $V_\lambda^{d,q}$ is defined by the equation $x_1 + \cdots + x_d = \lambda x_1 \cdots x_d$ over $\mathbb{F}_q$. Clearly, the number of points on a sum-product variety is given by,

$$\#(V_\lambda^{d,q}) = \sum_{y \in \mathbb{F}_q} m_{y,\lambda y}^{d,q}$$

Proposition 9.17. *Suppose that $m_{y,z}^{d,q} = m_{y,z'}^{d,q}$ for all $y, z, z' \in \mathbb{F}_q^\times$ then,*

$$\#(V_\lambda^{d,q}) = q^{d-1} - (-1)^d$$

Proof. We know that,

$$\#(V_\lambda^{d,q}) = \sum_{y \in \mathbb{F}_q} m_{y,\lambda y}^{d,q} = m_{0,0}^{d,q} + \sum_{y \in \mathbb{F}_q^\times} m_{y,\lambda y}^{d,q} = m_{0,0}^{d,q} + \sum_{y \in \mathbb{F}_q^\times} m_{y,1}^{d,q} = \sum_{y \in \mathbb{F}_q} m_{y,1}^{d,q} + [m_{0,0}^{d,q} - m_{0,1}^{d,q}]$$
$$= q^{d-1} - (-1)^d$$

□

Corollary 9.17.1. *If $q - 1 \mid d$ then,*

$$\#(V_\lambda^{d,q}) = q^{d-1} - (-1)^d$$

Proposition 9.18. *The number of points on a sum-product variety is determined entirely by $m_{\lambda^{-1},0}^{d,q}$ via,*

$$\#(V_\lambda^{d,q}) = \#(V_\lambda^{d,q}) = q^{d-1} - (q-1)^{d-2} + q m_{\lambda^{-1},0}^{d,q}$$

Proof. Choose any $x_1, \cdots, x_{d-1} \in \mathbb{F}_q$. Denote $S = x_1 + \cdots + x_{d-1}$ and $P = x_1 \cdots x_{d-1}$. Then finding a point on the variety is equivalent to solving,

$$S + x_d = \lambda P x_d \iff x_d = \frac{S}{\lambda P - 1}$$

when $P \neq \lambda^{-1}$. Therefore, for any choice of $x_1, \cdots, x_{d-1} \in \mathbb{F}_q$ there is a unique point on the variety when $P \neq \lambda^{-1}$. When $P = \lambda^{-1}$ there are no solutions for $S \neq 0$ and any x_d gives a point on the variety if $S = 0$. There are $q^{d-1} - (q-1)^{d-2}$ choices for $x_1, \cdots, x_{d-1} \in \mathbb{F}_q$ which do not have $P = \lambda^{-1}$ since to get $P = \lambda^{-1}$ we can take the first $d-2$ to be arbitrary elements of $\mathbb{F}_q^\times$ and then there is a unique $x_{d-1} \in \mathbb{F}_q^\times$ such that $x_1 \cdots x_{d-1} = \lambda^{-1}$. Thus, the total number of solutions is,

$$\#(V_\lambda^{d,q}) = q^{d-1} - (q-1)^{d-2} + q m_{\lambda^{-1},0}^{d,q}$$

□

Proposition 9.19. *If $m_{y,0}^{d,q} = m_{y',0}^{d,q}$ for all $y, y' \in \mathbb{F}_q^\times$ then,*

$$\#(V_\lambda^{d,q}) = q^{d-1} + (q-2)(q-1)^{d-2} + (-1)^d$$

for each $\lambda \in \mathbb{F}_q^\times$.

Proof. By Lemma 9.13 we know that,

$$m_{\lambda^{-1},0}^{d,q} = \frac{1}{q}\left[(q-1)^{d-1} + (-1)^d\right]$$

Therefore, by Proposition 9.4,

$$\#(V_\lambda^{d,q}) = q^{d-1} - (q-1)^{d-2} + (q-1)^{d-1} + (-1)^d = q^{d-1} + (q-2)(q-1)^{d-2} + (-1)^d$$

□

Corollary 9.19.1. *If $\gcd(d, q-1) = 1$ then for each $\lambda \in \mathbb{F}_q^\times$,*

$$\#(V_\lambda^{d,q}) = q^{d-1} + (q-2)(q-1)^{d-2} + (-1)^d$$

Theorem 9.20. *Let $q = p^r$ and $d = p^s$ then, for each $\lambda \in \mathbb{F}_q^\times$, the zeta function of the variety, $V_\lambda^{d,q}$ equals,*

$$\zeta_{V_\lambda^{d,q}} = \frac{1}{1-q^{d-1}t}\left[\frac{1}{1-t}\right]^{(-1)^d}\prod_{i=0}^{d}\left[\frac{(1-q^it)^2}{1-q^{i+1}t}\right]^{\binom{d}{i}(-1)^{d-i}}$$

and therefore, $V_\lambda^{d,q}$ is supersingular.

Proof.

$$\zeta_{V_\lambda^{d,q}} = \exp\left(\sum_{k\geq 1}\frac{\#(V_\lambda^{d,q^k})}{k}t^k\right)$$

However, $(d, q^k - 1) = (p^s, p^{rk} - 1) = 1$ for all k. Therefore, by Corollary 9.19.1,

$$\#(V_\lambda^{d,q^k}) = q^{(d-1)k} + (q^k-2)(q^k-1)^{d-2} + (-1)^d = q^{k(d-1)} + (-1)^d + (q^k-2)\sum_{i=0}^{d}\binom{d}{i}(-1)^{d-i}q^{ki}$$

Thus,

$$\begin{aligned}
\zeta_{V_\lambda^{d,q}} &= \exp\left(\sum_{k\geq 1}\frac{q^{k(d-1)}}{k}t^k + \frac{(-1)^d}{k}t^k + (q^k-2)\sum_{i=0}^{d}\left[\binom{d}{i}(-1)^{d-i}\sum_{k\geq 1}\frac{q^{ki}}{k}t^k\right]\right)\\
&= \exp\left(\sum_{k\geq 1}\frac{q^{k(d-1)}}{k}t^k + \frac{(-1)^d}{k}t^k + \sum_{i=0}^{d}\left[\binom{d}{i}(-1)^{d-i}\sum_{k\geq 1}\frac{q^{k(i+1)}}{k}t^k\right] - 2\sum_{i=0}^{d}\left[\binom{d}{i}(-1)^{d-i}\sum_{k\geq 1}\frac{q^{ki}}{k}t^k\right]\right)\\
&= \exp\left(-\log\left[1-q^{d-1}t\right] - (-1)^d\log\left[1-t\right] - \sum_{i=0}^{d}\left[\binom{d}{i}(-1)^{d-i}\log\left[1-q^{i+1}\right]\right] + 2\sum_{i=0}^{d}\left[\binom{d}{i}(-1)^{d-i}\log\left[1-q^{i}\right]\right]\right)\\
&= \frac{1}{1-q^{d-1}t}\left[\frac{1}{1-t}\right]^{(-1)^d}\prod_{i=0}^{d}\left[\frac{(1-q^it)^2}{1-q^{i+1}t}\right]^{\binom{d}{i}(-1)^{d-i}}
\end{aligned}$$

□

Lemma 9.21. *Let $w \in \mathbb{F}_q^\times$ be a generator. Then, $a = w^r$ is a n^{th} power if and only if* $\gcd(nq-1) \mid r$.

Proof. Suppose that $a = b^n$ where $b = w^x$. Then, $w^r = w^{nx}$ which is equivalent to $nx \equiv r \mod (q-1)$. This equation has solutions if and only if $\gcd(n, q-1) \mid r$. □

10 Relationships Between Diagonal Varieties

Lemma 10.1. *Let $\varphi : X \to Y$ be a surjective morphism then the induced map on ℓ-adic cohomology $\varphi^* : H^*(Y, \mathbb{Q}_\ell) \to H^*(X, \mathbb{Q}_\ell)$ is injective.*

Proof. See Kleiman, Algebraic Cycles and the Weil Conjectures, Proposition 1.2.4. Further, use the fact that ℓ-adic cohomology is a Weil cohomlogy theory. □

Proposition 10.2. *We say a scheme X over $\mathbb{F}_q$ is supersingular if and only if the frobenius map $F_X : X \to X$ induces a map $F_X^* : H^i(X, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$ on ℓ-adic cohomology with all eigenvalues of the form $\omega q^{\frac{i}{2}}$ where ω is a root of unity.*

Theorem 10.3. *Let $\varphi : X \to Y$ be a surjective morphism then X being supersingular implies that Y is supersingular.*

Proof. The induced map $\varphi^* : H^i(Y, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$ is injective by Proposition 10.2 and commutes with the Frobenuius maps,

$$\begin{array}{ccc} H^i(Y,\mathbb{Q}_\ell) & \xhookrightarrow{\varphi^*} & H^i(X,\mathbb{Q}_\ell) \\ \downarrow F_Y^* & & \downarrow F_X^* \\ H^i(Y,\mathbb{Q}_\ell) & \xhookrightarrow{\varphi^*} & H^i(X,\mathbb{Q}_\ell) \end{array}$$

Suppose that X is supersingular then every eigenvalue of $F*_X : H^i(X,\mathbb{Q}_\ell) \to H^i(X,\mathbb{Q}_\ell)$ has the form $\lambda = \omega q^{\frac{i}{2}}$ where ω is a root of unity. Suppose that $v \neq 0$ is an eigenvector of F_Y^* such that $F_Y^* = \lambda v$. By commutativity of the diagram,

$$\varphi^* \circ F_Y^*(v) = F_X^*(\varphi^*(v))$$

Furthermore, since φ^* is a linear map,

$$\varphi^* \circ F_Y^*(v) = \varphi^*(\lambda v) = \lambda \varphi^*(v)$$

and therefore,

$$F_X^*(\varphi^*(v)) = \lambda \varphi^*(v)$$

Since φ^* is injective and $v \neq 0$ we know that $\varphi^*(v) \neq 0$ so $\varphi^*(v)$ is an eigenvector of F_X^* with eigenvalue λ. Therefore, since X is supersingular, $\lambda = \omega q^{\frac{i}{2}}$ with ω a root of unity. Since λ is an abitrary eigenvalue of F_Y^* we have that Y is supersingular. ☐

Definition 10.4. Let X and Y be diagonal varieties of dimension $r-1$ over the field k, defined respectively by the equations,

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0 \text{ and } b_0 x_0^{m_0} + \cdots + b_r x_r^{n_r} = 0$$

Then we say that $X \mid Y$ iff $n_i \mid m_i$ for each $0 \leq i \leq r$.

Lemma 10.5. *If X and Y are diagonal varieties of dimension $r-1$ over an algebraically closed field k and $X \mid Y$ then there exists a surjective morphism, $\varphi : Y \to X$.*

Proof. Define the map $\varphi : Y \to X$ via,

$$(x_0, \dots, x_r) \mapsto (x_0^{\frac{m_0}{n_0}}, \dots, x_r^{\frac{m_r}{n_r}})$$

This map is well-defined because if the point $(x_0, \dots, x_r)$ satisfies,

$$x_0^{m_0} + \cdots + x_r^{m_r} = 0$$

Then the point $(y_0, \dots, y_r) = (x_0^{\frac{m_0}{n_0}}, \dots, x_r^{\frac{m_r}{n_r}})$ satisfies the equation,

$$y_0^{n_0} + \cdots + y_r^{n_r}$$

Furthermore, φ is surjective because k is algebraically closed and thus each $y_i \in k$ is an $\left(\frac{m_i}{n_i}\right)^{\text{th}}$ power. ☐

Remark. Theorem 3.5 is a special case of this result in which the map φ has additional properties due to the characteristic of k.

Corollary 10.5.1. *Suppose $X \mid Y$. If Y is supersingular then X is supersingular.*

Proof. This follows immediately from Lemma 10.3 and Lemma 10.5. However, we also give an elementary proof. Take q to be a power of p such that $q \equiv 1$ modulo the LCM for X and Y. Since $X \mid Y$ each $\alpha \in A_{X,q}$ for X satisfies the correct divisibility relations for Y. Thus, $A_{X,q} \subset A_{Y,q}$. Therefore, if Y is supersingular then each $\alpha \in A_{Y,q}$ gives a product of gauss sums which is a root of unity. Since $A_{X,q} \subset A_{Y,q}$ the same holds for X so X is supersingular. ☐

Corollary 10.5.2. *Let X be a diagonal variety over an algebraically closed field k defined by the equation,*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

Define the LCM extension X_ℓ and GCD reduction X_g of X by,

$$X_\ell = F_r^{\mathrm{lcm}\,(n_i)} \text{ and } X_g = F_r^{\mathrm{gcd}\,(n_i)}$$

respectively. Then there exist surjective maps,

$$X_\ell \xrightarrow{\varphi_\ell} X \xrightarrow{\varphi_g} X_g$$

Corollary 10.5.3. *If X_ℓ is supersingular then X is supersingular. If X_g is not supersingular then X is not supersingular.*

Theorem 10.6. *Let X be a diagonal variety. Then X is supersigular over $\mathbb{F}_p$ if there exists $v \in \mathbb{Z}$ such that $p^v \equiv -1 \mod \mathrm{lcm}\,(n_i)$ and X is not supersingular if for all $v \in \mathbb{Z}$ we have $p^v \not\equiv -1 \mod \mathrm{gcd}\,(n_i)$.*

Proof. This follows from Shioda's theorem via Corollary 10.5.3. □

11 Newton Polygons

Proposition 11.1. *The set of slopes that appear in the Newton polygon is determined by*

$$\frac{1}{(p-1)f} \sum_{i=0}^{3} s(\frac{(q-1)r_i}{m}) - 1,$$

where $\sum \frac{r_i}{m} \in \mathbb{Z}$, i. e., the set of $\frac{r_i}{m}$ is in the set of all possible α.

Proof. See Koblitz's paper p-adic variation of the zeta function over the families of varieties defined over finite fields. □

Proposition 11.2. *When $f = 1$, the Newton Polygon of the Fermat variety $F_{p,r}^n$ is of the form*

$$(0,0),\ (0,a),(b_2 - a, b_2 - 2a),(b_2,b_2),$$

where $a = \binom{m-1}{3}$, and b_2 is the second betti number.

Proof. Since $f = 1$, we know that

$$\sum_{i=0}^{3} s(\frac{(q-1)r_i}{m}) = \sum_{i=0}^{3} \left\{\frac{r_i}{m}\right\}$$

But $m | r_0 + r_1 + r_2 + r_3$, so the only possible value for $\sum_{i=0}^{3} \left\{\frac{r_i}{m}\right\}$ is $1, 2, 3$, and these corresponds to slope $0, 1, 2$.

To count the length of x-axis where the slope is 0, we need to find the number of solution to the equation

$$r_0 + r_1 + r_2 + r_3 = m,$$

which is $\binom{m-1}{3}$. By duality of the cohomology, this length is equal to the length of the last segment, i. e., the segment with slope 2. □

12 Surfaces of the form $x^p + y^q + z^{ps} + w^{qs}$

Theorem 12.1. *Let p, q, w be primes such that $p, q, w \equiv 1 \mod s$ for some s and let X be the variety defined by,*

$$x_0^p + x_1^{ps} + x_2^q + x_3^{qs} = 0$$

over $\mathbb{F}_w$. If w is a primitive root modulo p and q then X is supersingular.

Proof. By Theorem 6.14, we need only check that for each $\alpha = (e_0/m, \dots, e_3/m) \in A(X)$ that,

$$S_\mu(e_0, e_1, e_2, e_3) = \sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\{ \frac{\mu e_i w^j}{m} \right\} = 2f$$

where $m = pqs$ and $f = \text{ord}_{pqs}(w)$. However, we also know that α can be written as a tuple, $(a_0, \dots, a_3)$ such that,

$$\frac{a_0}{p} + \frac{a_1}{ps} + \frac{a_2}{q} + \frac{a_3}{qs} = \frac{sa_0 + a_1}{ps} + \frac{sa_2 + a_3}{qs} = \frac{q(sa_0 + a_1) + p(sa_2 + a_3)}{pqs} \in \mathbb{Z}$$

Since p and q are coprime, we must have,

$$p \mid sa_0 + a_1 \quad \text{and} \quad q \mid sa_2 + a_3$$

Thus, let, $sa_0 + a_1 = pn_p$ and $sa_2 + a_3 = qn_q$. This reduces the above condition to,

$$\frac{n_p}{s} + \frac{n_q}{s} \in \mathbb{Z} \iff n_p + n_q \equiv 0 \mod s$$

Now, using Lemma 8.8,

$$\begin{aligned} S_\mu(e_0, e_1, e_2, e_3) &= S_\mu(e_0, e_1) + S_\mu(e_2, e_3) \\ &= N_\mu(e_0, e_1) + N_\mu(e_2, e_3) + \sum_{j=0}^{f-1} \left[\left\{ \frac{\mu(e_0 + e_1)w^j}{m} \right\} + \left\{ \frac{\mu(e_2 + e_3)w^j}{m} \right\} \right] \end{aligned}$$

However, $e_0 + e_1 = q(sa_0 + a_1) = pqn_p$ and $e_2 + e_3 = p(sa_2 + a_3) = pqn_q$ and thus,

$$\sum_{j=0}^{f-1} \left[\left\{ \frac{\mu(e_0 + e_1)w^j}{m} \right\} + \left\{ \frac{\mu(e_2 + e_3)w^j}{m} \right\} \right] = \sum_{j=0}^{f-1} \left[\left\{ \frac{\mu n_p w^j}{s} \right\} + \left\{ \frac{\mu n_q w^j}{s} \right\} \right] = \sum_{j=0}^{f-1} 1 = f$$

since $\mu w^j (n_p + n_q) \equiv 0 \mod s$. We need not worry about the case $n_p \equiv n_q \equiv 0 \mod s$ because in that case $m \mid e_0 + e_1$ and $m \mid e_2 + e_3$ so $S_\mu(e_0, e_1) = S_\mu(e_2, e_3) = f$ which is the condition we need.

It remains to show that,

$$N_\mu(e_0, e_1) + N_\mu(e_2, e_3) = f \implies S_\mu(e_0, e_1, e_2, e_3) = 2f$$

Consider the number, $N_\mu(e_0, e_1)$ which counts all $0 \le j < f$ such that,

$$\left\{ \frac{\mu n_p w^j}{s} \right\} < \left\{ \frac{\mu a_0 w^j}{p} \right\}$$

However, $w \equiv 1 \mod s$ and thus,

$$\left\{ \frac{\mu n_p w^j}{s} \right\} = \left\{ \frac{\mu n_p}{s} \right\} = \frac{[\mu n_p]_s}{s}$$

Furthermore, w is a primitve root modulo p so the numbers $\mu a_0 w^j$ give a complete set of residues modulo p. Because $p - 1 = \text{ord}_p(w) \mid \text{ord}_{pqs}(w) = f$ we can write $f = u_p(p-1)$ and similarly $f = u_q(q-1)$. Therefore,

$$N_\mu(e_0, e_1) = u_p \left[\# \left\{ 0 \le i < p - 1 \;\middle|\; \frac{[\mu n_p]_s}{s} < \frac{i}{p} \right\} \right] = u_p \left(p - 1 - \left\lfloor \frac{p[\mu n_p]_s}{s} \right\rfloor \right)$$

However, $p \equiv 1 \mod s$ so $p = sk_p + 1$ and thus because $0 < [\mu n_p]_s < s$ we have,

$$\left\lfloor k_p[\mu n_p]_s + \frac{[\mu n_p]_s}{s} \right\rfloor = k_p[\mu n_p]_s$$

Finally,

$$N_\mu(e_0, e_1) = f - u_p k_p[\mu n_p]_s = f - u_p \frac{p-1}{s}[\mu n_p]_s = f\left(1 - \frac{[\mu n_p]_s}{s}\right)$$

and identical argument gives,

$$N_\mu(e_2, e_3) = f\left(1 - \frac{[\mu n_q]_s}{s}\right)$$

and thus,

$$N_\mu(e_0, e_1) + N_\mu(e_2, e_3) = f\left(2 - \frac{[\mu n_p]_s + [\mu n_q]_s}{s}\right) = f$$

because $[\mu n_p]_s + [\mu n_q]_s = s$. □

Theorem 12.2. *Let X be the variety defined by,*

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

and let $n = \operatorname{lcm} n_i$. Now define the polynomial,

$$B_X(x) = \left[\prod_{i=0}^{r} \frac{x^{2n} - x^{2w_i}}{x^{2w_i} - 1} - \prod_{i=0}^{r} \frac{x^{n(r+1)} - x^{w_i(r+1)}}{x^{w_i(r+1)} - 1}\right]$$

Suppose that $p \equiv 1 \mod n$ then the total degree of X minus the picard number of X is given by,

$$P^C(X) = \sum_{i=1}^{n(r+1)} B_X(\zeta_{n(r+1)}^i)$$

In particular, X is supersingular iff $P^C(X) = 0$.

Proof. When $p \equiv 1 \mod n$ then $f = 1$ so we know that a given product of Gaussian sums applied for $\alpha \in A_{n,p}$ is a root of unity if and only if,

$$\sum_{i=0}^{r} \left\{\frac{\mu e_0}{n}\right\} = \frac{r+1}{2}$$

for each $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$. (WIP) □

13 Rationality

Theorem 13.1. *The variety X defined by equation*

$$x^q + y^q + z^p + w^p = 0$$

is rational when $\gcd(p, q) = 1$.

Proof. This variety is in the weighted projected space $\mathbb{P}(p, p, q, q)$. We want to define a map f from $\mathbb{P}(p, p, q, q)$ to $\mathbb{P} \times \mathbb{P}$ by

$$(x_0 : x_1 : x_2 : x_3) \mapsto ((x_0 : x_1), (x_2 : x_3)),$$

and we consider the locus $D_+(x_0 x_2) \subset \mathbb{P}(p, p, q, q)$ and its image $D_+(x_0) \times D_+(x_2) \cong \mathbb{A} \times \mathbb{A} \subset \mathbb{P} \times \mathbb{P}$ under f.

We know that

$$D_+(x_0x_2) = \mathrm{Spec}R \quad \text{where} \quad R = k\left[x_0, x_1, x_2, x_3\right]\left[\frac{1}{x_0x_2}\right]_0$$

Define the change of variable

$$x_{1,0} = \frac{x_1}{x_0}, \;\; x_{3,2} = \frac{x_3}{x_2}, \;\; x_{2,0} = \frac{x_2^p}{x_0^q},$$

we content that $D_+(x_0x_2) = \mathrm{Spec}(k[x_{1,0}, x_{3,2}, x_{2,0}, x_{2,0}^{-1}])$, as proved in lemma.

On the other hand, we can write $D_+(x_0) \times D_+(x_2) = \mathrm{Spec}(k[s] \otimes_k k[t]) = \mathbb{A} \times \mathbb{A}$ by let

$$s = \frac{x_1}{x_0}, \;\; t = \frac{x_3}{x_2}.$$

Then we can define the ring map

$$f_* : k[s] \otimes_k k[t] \to R$$

by

$$s \mapsto x_{1,0}, \;\; t \mapsto x_{3,2}.$$

Now consider the variety $X = V(x_0^q + x_1^q + x_2^p + x_3^p) = V(I)$ in the affine patch $D_+(x_0x_2)$. The defining equation of X after change of variable can be written as

$$f = 1 + x_{1,0}^q + x_{2,0} + x_{3,2}^p x_{2,0} = x_{2,0}(1 + x_{3,2}^p) + (1 + x_{1,0}^q)$$

Thus it is clear that

$$k[x_{1,0}, x_{3,2}, x_{2,0}, x_{2,0}^{-1}]/(x_{2,0}(1 + x_{3,2}^p) + (1 + x_{1,0}^q)) \cong \mathrm{Frac}(R/I)$$

Notice that $\overline{f^*} : k[s] \otimes_k k[t] \to \mathrm{Frac}(R/I)$ is surjective because we can write $x_{2,0}$ and $x_{2,0}^{-1}$ as a rational function in term of $x_{1,0}$ and $x_{3,2}$. Furthermore, it is easy to see that f^* is injective. Thus, f^* is a bijective rational map. For the inverse map of f^*, we map

$$x_{1,0} \mapsto s, \;\; x_{3,2} \mapsto t.$$

We thus show that X is birationally equivalent to $\mathbb{P} \times \mathbb{P}$. □

Lemma 13.2. *Let $R = k\left[x_0, x_1, x_2, x_3\right]$ be a weighted ring with weight (p, p, q, q) and $\gcd(p, q) = 1$. Then*

$$R_+ = k\left[x_0, x_1, x_2, x_3\right]\left[\frac{1}{x_0x_2}\right]_0 \cong k[x_{1,0}, x_{3,2}, x_{2,0}, x_{2,0}^{-1}],$$

where

$$x_{1,0} = \frac{x_1}{x_0}, x_{3,2} = \frac{x_3}{x_2}, x_{2,0} = \frac{x_2^p}{x_0^q}.$$

Proof. We proceed by showing that if

$$m = \frac{x_0^{a_0}x_1^{a_1}x_2^{a_2}x_3^{a_3}}{x_0^{b_0}x_2^{b_2}}$$

for $a_i, b_j > 0$ with $i = 0, 1, 2, 3$ and $j = 0, 1$, and m has degree 0, then m can be written as a product of $x_{1,0}, x_{3,2}, x_{2,0},$ or $x_{0,2}$.

If $a_0 > b_0$ and $a_2 > b_2$, then it is impossible for m to have degree 0.

If $a_0 > b_0$ and $a_2 < b_2$, then let $b_2 - a_2 = c_2$ and $a_0 - b_0 = c_0$. For m to have degree 0, we need

$$pc_0 + pa_1 + qa_3 = qc_2.$$

Since $\gcd(p, q) = 1$, it must be the case that $q|(c_0 + a_1)$. Write $c_0 + a_1 = qk$ for some $k \in \mathbb{Z}$. Our equation now become

$$pk + a_3 = c_2$$

Thus we can write m as

$$m = \left(\frac{x_0^{a_1} x_0^{c_0} x_1^{a_1} x_3^{a_3}}{x_0^{a_1} x_2^{pk}} \right) \left(\frac{x_3}{x_2} \right)^{a_3} = x_{1,0}^{a_1} x_{3,2}^{a_3} x_{0,2}^{k}$$

If $a_0 < b_0$ and $a_2 < b_2$, let $c_0 = b_0 - a_0$ and $c_2 = b_2 - a_2$. Then we have the equation

$$pa_1 + qa_3 = pc_0 + qc_2$$

with $a_1, a_3, c_0, c_2 > 0$.

Since $\gcd(p, q) = 1$, we can write $d_1 p + d_2 q = 1$, and $|d_1| < q$ and $|d_2| < p$. Notice that $d_1 d_2 < 0$.

Moreover, any other such equation can be written as $(d_1 + qr)p + (d_2 - pr)q = 1$ for $r \in \mathbb{Z}$. Without loss of generality, let $d_1 > 0$ and $d_2 < 0$. Then

$$\begin{aligned}(d_1 + qr)(d_2 - pr) &= d_1 d_2 - prd_1 + r(1 - d_1 p) - pqr^2 \\ &= d_1 d_2 + r - 2d_1 pr - pqr^2\end{aligned}$$

If $r > 0$, the only positive term is r thus we know $(d_1 + qr)(d_2 - pr) < 0$.

If $r < 0$, we have $-2d_1 pr > 0$, but $2d_1 p < pq|r|$ since $|d_1| < q$. Thus, it is impossible for both of the coefficient to be positive at the same time. However, $a_1, a_3, c_0, c_2 > 0$. Therefore, it is also impossible for m in this case to have degree 0. ☐

14 Surfaces of the Form $x^a + y^b + z^c + w^{abc}$

Lemma 14.1. *(From Shioda's On Fermat Varieties) Let p be a prime, n be an integer not divisible by p, and $f = \operatorname{ord}_n(p)$. Suppose that for all μ relatively prime to n:*

$$\sum_{i=0}^{f-1} \left\{ \frac{\mu p^i}{n} \right\} = \frac{f}{2}$$

Then there does not exist a primitive character χ modulo n such that $\chi(-1) = -1$ and $\chi(p) = 1$.

Proof. Suppose there does exist such a character. As χ is primitive with $\chi(-1) = -1$,

$$0 \neq L(1, \chi) = \frac{i\pi g(\chi)}{n^2} \sum_{k=1}^{n} \bar{\chi}(k)k$$

As $g(\chi)$ is non-zero we must have:

$$\sum_{k=1}^{n} \bar{\chi}(k)k \neq 0$$

Now let G be $(\mathbb{Z}/abc\mathbb{Z})^\times$ and let H be the subgroup of G generated by p. As χ is trivial on H:

$$\sum_{k=1}^{n} \bar{\chi}(k)k = \sum_{\mu \in G/H} \chi(\mu) \sum_{k \in \mu H} k$$

Now we have that:

$$\frac{f}{2} = \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i}{n} \right\} = \sum_{k \in \mu H} \frac{k}{n}$$

Thus

$$\sum_{k=1}^{n} \bar{\chi}(k)k = \frac{nf}{2} \sum_{\mu \in G/H} \chi(\mu)$$

Note that χ is a nontrivial character on G/H. Thus

$$\sum_{\mu \in G/H} \chi(\mu) = 0$$

and so we have a contradiction. ☐

Lemma 14.2. *Let $p, a_1, a_2, \ldots, a_r$ be distinct primes. Suppose $f = \text{ord}_{abc}(p)$ and $f_i = \text{ord}_{a_i}(p)$. There exists a primitive character modulo $a_1a_2\cdots a_r$ such that $\chi(-1) = -1$ and $\chi(p) = 1$ if and only if there exist integers $0 < \alpha_i < a_i - 1$ for each i such that*

$$\sum_{i=1}^{r} \frac{\alpha_r}{f_r} \in \mathbb{Z}$$

and $\alpha_1 + \alpha_2 + \cdots + \alpha_r$ is odd.

Proof. Let $A = a_1a_2\cdots a_r$ and $\chi : (\mathbb{Z}/A\mathbb{Z})^\times \to S^1$ be a character. As:

$$(\mathbb{Z}/A\mathbb{Z})^\times = \prod_{i=1}^{r} (\mathbb{Z}/a_i\mathbb{Z})^\times$$

There exists characters $\chi_i : (\mathbb{Z}/a_i\mathbb{Z})^\times \to S^1$ such that

$$\chi(j) = \chi_1(j)\chi_2(j)\cdots\chi_r(j)$$

As the a_i are prime, there exists generators g_i modulo a_i for each i such that:

$$g_i^{\frac{a_i-1}{f_i}} \equiv p \pmod{a_i}$$

Now there exists α_i for each i such that:

$$\chi(g_i) = \exp\left(\frac{2\pi\alpha_i}{a_i - 1}\right)$$

Using these above definitions, the condition $\chi(p) = 1$ is equivalent to

$$\sum_{i=1}^{r} \frac{\alpha_r}{f_r} \in \mathbb{Z}$$

and the condition $\chi(-1) = -1$ translates to $\alpha_1 + \alpha_2 + \cdots + \alpha_r$ is odd. Lastly, the condition that χ is primitive just implies that χ_1, χ_2, χ_3 are not trivial. Thus we lastly need $\alpha_1 \neq a - 1, \alpha_2 \neq b - 1, \alpha_3 \neq c - 1$, as desired. □

Lemma 14.3. *Let a, b, c, p be distinct primes. Suppose $f = \text{ord}_{abc}(p), f_1 = \text{ord}_a(p), f_2 = \text{ord}_b(p)$, and $f_3 = \text{ord}_c(p)$ and let $2^r, 2^s, 2^t$ be the highest power of 2 dividing f_1, f_2, f_3 respectively. Then there exists a character χ primitive modulo abc such that $\chi(-1) = -1$ and $\chi(p) = 1$ only if one of the following holds*

- $p^{f/2} \equiv -1 \pmod{abc}$
- $f_2 = b - 1, f_3 = c - 1, r > s, s = 1, t = 1$
- $f_1 = a - 1, f_2 = b - 1, f_3 = c - 1, r > s, s = 2, t = 1$

Proof. We will do this by casework, using the result of lemma 14.2. To make things easier for ourselves suppose f_1', f_2', f_3' are the largest odd numbers dividing f_1, f_2, f_3 respectively. Let $\alpha_1, \alpha_2, \alpha_3$ be as in the statement of lemma 14.2:

Case ($r = s = t$): This is simply equivalent to $w^{f/2} \equiv -1 \pmod{p}$.

Case ($r > s > t$): If $t \neq 1$ taking $\alpha_1 = f_1'2^{r-s}, \alpha_2 = f_2'(2^{s-t} - 1), \alpha_3 = f_3'2^{t-1}$ gives us a primitive character satisfying the desired conditions. If $t = 1$ and $s \neq 2$, taking $\alpha_1 = f_1'2^{r-t-1}, \alpha_2 = f_2'2^{s-t-1}, \alpha_3 = f_3'(2^t - 1)$ gives us a primitive character satisfying the desired conditions. As there exists no such characters, these cases are impossible. Hence $r > s = 2 > t = 1$.

Now suppose we have $r > s = 2 > t = 1$. Consider the case $\alpha_1 = f_1' 2^{r-s}, \alpha_2 = 3f_2', \alpha_3 = 2f_3'$. This implies that $f_3 = 2f_3' = c - 1$, as otherwise this gives a character and hence a contradiction. Similarly, consider the case $\alpha_1 = f_1' 2^{r-s+1}, \alpha_2 = 4f_2', \alpha_3 = f_3'$. By the same reasoning, this implies that $f_2 = 4f_2' = qb - 1$. Lastly, consider the case $\alpha_1 = f_1' 2^r, \alpha_2 = 2f_2', \alpha_3 = f_3'$. Again, this implies that $f_1 = 2^r f_2' = a - 1$. This completes our analysis of this case.

Case ($r = s > t$): Taking $\alpha_1 = f_1', \alpha_2 = f_2'(2^{s-t} - 1), \alpha_3 = f_3'(2^t - 1)$ gives us a primitive character satisfying the desired conditions. Thus we get a contradiction, so this case is impossible.

Case ($r > s = t$): If $t \neq 1$, taking $\alpha_1 = 2^{r-s} f_1', \alpha_2 = f_2'(2^s - 2), \alpha_3 = f_3'$ gives us a primitive character satisfying the desired conditions. Hence $t = 1$.

Now suppose we have $r > s = t = 1$. Consider the case $\alpha_1 = f_1' 2^{r-1}, \alpha_2 = f_2', \alpha_3 = 2f_3'$. This implies that $f_3 = 2f_3' = c - 1$, as otherwise this gives a character and hence a contradiction. Similarly, consider the case $\alpha_1 = f_1' 2^{r-1}, \alpha_2 = 2f_2', \alpha_3 = f_3'$. By the same reasoning, $f_2 = 2f_2' = b - 1$.

We have now exhausted all possible cases and have shown that the only possible choices are those in the theorem statement. ☐

Lemma 14.4. *(Coyne) Let R be a positive integer and let $a_1, a_2, \ldots, a_k$ be positive integers all dividing R. Then the number of solutions $(b_1, \ldots, b_k) \in \prod_{i=1}^k \mathbb{Z}/a_i\mathbb{Z}$ to*

$$\sum_{i=1}^{k} \frac{Rb_i}{a_i} \equiv 0 \pmod R$$

is equal to

$$\frac{\gcd(a_1, a_2, \ldots, a_k) \prod_{i=1}^k a_i}{R}$$

Proof. Consider the homomorphism:

$$\phi : \prod_{i=1}^{k} \mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/R\mathbb{Z}$$

given by

$$\phi(b_1, \ldots, b_k) = \sum_{i=1}^{k} \frac{Rb_i}{a_i} \pmod R$$

The size of the kernel of this map is precisely the quantity we are looking for. Now consider im ϕ. This will be the elements of $\mathbb{Z}/R\mathbb{Z}$ with nonzero image in $\mathbb{Z}/\gcd(a_1, a_2, \ldots, a_k)\mathbb{Z}$. Thus:

$$|\text{im } \phi| = \frac{R}{\gcd(a_1, a_2, \ldots, a_k)}$$

Lastly, by the first isomorphism theorem,

$$|\ker \phi| = \frac{|\prod_{i=1}^k \mathbb{Z}/a_i\mathbb{Z}|}{|\text{im}\phi|} = \frac{\gcd(a_1, a_2, \ldots, a_k) \prod_{i=1}^k a_i}{R}$$

☐

Lemma 14.5. *Let a, b, c, p be distinct primes. Suppose $f = \text{ord}_{abc}(p), f_1 = \text{ord}_a(p), f_2 = \text{ord}_b(p)$, and $f_3 = \text{ord}_c(p)$ and let $2^r, 2^s, 2^t$ be the highest power of 2 dividing f_1, f_2, f_3 respectively. Lastly, let f_1', f_2', f_3' be the largest odd integers dividing f_1, f_2, f_3 respectively. If $r \geq s \geq t \geq 1$ and $p^{f/2} \not\equiv -1 \pmod{abc}$, there does not exist a character χ primitive modulo a, b, c such that $\chi(-1) = -1$ and $\chi(p) = 1$ if and only if f_1', f_2', f_3' are pairwise coprime and one the following two conditions holds:*

1. $f_2 = b - 1, f_3 = c - 1, r > s, s = 1, t = 1$

2. $f_1 = a-1, f_2 = b-1, f_3 = c-1, r > s, s = 2, t = 1$

Proof. By lemma 14.3, all that is left to show is that if one of the two cases holds then f_1', f_2', f_3' being pairwise coprime is a necessary and sufficient condition on the existence of a character. By lemma 14.2, such a character exists if and only if we can find $\alpha_1, \alpha_2, \alpha_3$ such that:

$$S := \frac{\alpha_1}{2^r f_1'} + \frac{\alpha_2}{2^s f_2'} + \frac{\alpha_3}{2^t f_3'} \in \mathbb{Z}$$

and $\alpha + \alpha_2 + \alpha_3 \in \mathbb{Z}$. In the first of our two conditions, the only possible values of $\alpha_1, \alpha_2, \alpha_3$ modulo $2^r, 2^s, 2^t$ such that the sum of the α_i is odd and the denominator of S is odd are $\alpha_1 \equiv 2^{r-1} \pmod{2^r}$ and exactly one of α_2, α_3 is odd. Thus, as the choice of $\alpha_1, \alpha_2, \alpha_3$ modulo f_1', f_2', f_3' will determine if S is an integer, there does not exist such a primitive character if and only if the only choices of α_2, α_3 have $f_2'|\alpha_2$ and $f_3'|\alpha_3$.

Similarly, in the second of our two conditions, the only possible values have one of $\alpha_1, \alpha_2, \alpha_3$ modulo $2^r, 2^s, 2^t$ that do give rise to a character has one of the αs 0 in the respective modulus. Furthermore, there exists at least one choice of modular remainders for which each of them is 0 and no others are. Thus there does not exist such a primitive character if and only the only choices of $\alpha_1, \alpha_2, \alpha_3$ are divisible by f_1', f_2', f_3' respectively.

In both cases, this comes down to determining whether there are solutions to:

$$T(\gamma_1, \gamma_2, \gamma_3) := \frac{\gamma_1}{f_1'} + \frac{\gamma_2}{f_2'} + \frac{\gamma_3}{f_3'} \in \mathbb{Z}$$

with $f_i \nmid \gamma_i$ as we can pick $\alpha_1, \alpha_2, \alpha_3$ modulo f_1', f_2', f_3' respectively such that $\gamma_1 = 2^i\alpha_1, \gamma_2 = 2^j\alpha_2, \gamma_3 = 2^k\alpha_3$ for any i, j, k.

Let $R = \operatorname{lcm}(f_1'f_2'f_3')$ and w_i. Any choice of γ_i with $T \in Z$ will have $f_2'|\alpha_2, f_3'|\alpha_3$ if and only if $f_1'|\alpha_1$. Thus $T \in Z$ if and only if the number of solutions to:

$$\frac{R\gamma_1}{f_1'} + \frac{R\gamma_1}{f_1'} + \frac{R\gamma_1}{f_1'} \equiv 0 \pmod{R}$$

is 1. By lemma 14.4, this occurs if and only if:

$$f_1 f_2 f_3 \gcd(f_1, f_2, f_3) = \operatorname{lcm}(f_1, f_2, f_3)$$

Which occurs if and only if f_1, f_2, f_3 are pairwise coprime, as desired. □

Theorem 14.6. *Let a, b, c, p be distinct primes. Suppose that the order of p modulo each of a, b, c is even. Then he projective variety V defined by*

$$w^{abc} + x^a + y^b + z^c = 0$$

over $\mathbb{F}_p$ is supersingular if and only if for all μ relatively prime to abc,

$$\left\{\frac{\mu p^i}{abc}\right\} = \frac{f}{2}$$

Proof. By (Insert Citation), V is supersingular if and only if for all $a \nmid \beta_1, b \nmid \beta_2, c \nmid \beta_3, abc \nmid \beta_4$ such that

$$\frac{\beta_1}{a} + \frac{\beta_2}{b} + \frac{\beta_3}{c} + \frac{\beta_4}{abc} \in Z$$

we have:

$$\sum_{i=0}^{f}\left[\left\{\frac{\mu\beta_1 p^i}{a}\right\} + \left\{\frac{\mu\beta_2 p^i}{b}\right\} + \left\{\frac{\mu\beta_3 p^i}{c}\right\} + \left\{\frac{\mu\beta_4 p^i}{abc}\right\}\right] = 2f$$

As p has even order modulo each of a, b, c there exists a power of it which is -1 modulo each of a, b, c. As such we can pair up to get

$$\sum_{i=0}^{f}\left\{\frac{\mu\beta_1 p^i}{a}\right\} = \sum_{i=0}^{f}\left\{\frac{\mu\beta_2 p^i}{b}\right\} = \sum_{i=0}^{f}\left\{\frac{\mu\beta_3 p^i}{c}\right\} = \frac{f}{2}$$

Hence the above condition is equivalent to:

$$\left\{\frac{\mu\beta_4 p^i}{abc}\right\} = \frac{f}{2}$$

As $\mu\beta_4$ ranges over the same set as just μ, this is equivalent to for all μ relatively prime to abc:

$$\left\{\frac{\mu p^i}{abc}\right\} = \frac{f}{2}$$

as desired ☐

Theorem 14.7. *Let a, b, c, p be distinct primes. Suppose $f = \text{ord}_{abc}(p), f_1 = \text{ord}_a(p), f_2 = \text{ord}_b(p)$, and $f_3 = \text{ord}_c(p)$ and let $2^r, 2^s, 2^t$ be the highest power of 2 dividing f_1, f_2, f_3 respectively. Lastly, let f_1', f_2', f_3' be the largest odd integers dividing f_1, f_2, f_3 respectively. If $r \geq s \geq t \geq 1$ and the projective variety V defined by*

$$w^{abc} + x^a + y^b + z^c = 0$$

over $\mathbb{F}_p$ is supersingular and $p^{f/2} \not\equiv -1 \pmod{abc}$ then f_1', f_2', f_3' are pairwise coprime and one the following two holds:

- $f_2 = b - 1, f_3 = c - 1, r > s, s = 1, t = 1$
- $f_1 = a - 1, f_2 = b - 1, f_3 = c - 1, r > s, s = 2, t = 1$

Proof. By theorem 14.6, we have for all μ relatively prime to abc:

$$\left\{\frac{\mu p^i}{abc}\right\} = \frac{f}{2}$$

The result of lemma 14.1 then implies that there does not exist a character χ primitive modulo abc such that $\chi(p) = 1, \chi(-1) = -1$. From this, lemma 14.5 gives us the desired result. ☐

Lemma 14.8. *Suppose a, b, c, p are primes with $f = \text{ord}_{abc}(p)$ and $f_1 = \text{ord}_{bc}(a)$. Let H be the subgroup of $(\mathbb{Z}/a\mathbb{Z})^\times$ generated by p^{f_1}. Then for all μ not divisible by a, b, c we have:*

$$\sum_{h \in (\mathbb{Z}/a\mathbb{Z})^\times / H} \sum_{i=0}^{f-1} \left\{\frac{\mu h p^i}{abc}\right\} = \frac{f_1(a-1)}{2}$$

if and only if for all μ not divisible by b, c we have:

$$\sum_{i=0}^{f_1-1} \left\{\frac{\mu p^i}{bc}\right\} = \sum_{i=0}^{f_1-1} \left\{\frac{\mu u p^i}{bc}\right\}$$

where $u \equiv a^{-1} \pmod{bc}$.

Proof. Note that we have:

$$\sum_{h \in H} \sum_{i=0}^{f-1} \left\{\frac{\mu h p^i}{abc}\right\} = \sum_{k \in (\mathbb{Z}/a\mathbb{Z})^\times} \sum_{i=0}^{f_1-1} \left\{\frac{\mu k p^i}{abc}\right\} = \sum_{k \in (\mathbb{Z}/a\mathbb{Z})} \sum_{i=0}^{f_1-1} \left\{\frac{\mu k p^i}{abc}\right\} - \sum_{i=0}^{f_1-1} \left\{\frac{\mu u p^i}{bc}\right\} \tag{1}$$

where we view $k \in (\mathbb{Z}/a\mathbb{Z})^\times$ as the element x for which:

$$\begin{aligned} x &\equiv k \pmod{a} \\ x &\equiv 1 \pmod{b} \\ x &\equiv 1 \pmod{c} \end{aligned}$$

Now as $f_1 = \mathrm{ord}_p(bc)$ for each pair of remainders $f \pmod b, g \pmod c$ there exists at most one remainder modulo $e \pmod a$ such that there exists an i for which p^i is equivalent to each of those in the respective modulus. As such we have:

$$\sum_{k\in(\mathbb{Z}/a\mathbb{Z})^\times} \sum_{i=0}^{f_1-1} \left\{\frac{\mu k p^i}{abc}\right\} = \sum_{j=0}^{a-1}\sum_{i=0}^{f_1-1} \left\{\frac{\mu p^i + jbc}{abc}\right\}$$

Now for each i let j_i be the j for which

$$\left\{\frac{\mu p^i + jbc}{abc}\right\} < \frac{1}{a}$$

We then get:

$$\begin{aligned}
\sum_{k\in(\mathbb{Z}/a\mathbb{Z})^\times} \sum_{i=0}^{f_1-1} \left\{\frac{\mu k p^i}{abc}\right\} &= \sum_{j=0}^{a-1}\sum_{i=0}^{f_1-1} \left\{\frac{\mu p^i + j_0bc + jbc}{abc}\right\} \\
&= \sum_{j=0}^{a-1}\left[\sum_{i=0}^{f_1-1} \left\{\frac{\mu p^i + j_0bc}{abc}\right\} + \frac{j}{a}\right] \\
&= \frac{(a-1)f_1}{2} + \sum_{i=0}^{f_1-1} a\left\{\frac{\mu p^i + j_0bc}{abc}\right\}
\end{aligned}$$

Now as $\left\{\frac{\mu p^i + j_0bc}{abc}\right\} < \frac{1}{a}$ we have

$$a\left\{\frac{\mu p^i + j_0bc}{abc}\right\} = \left\{\frac{\mu a p^i + j_0abc}{abc}\right\} = \left\{\frac{\mu p^i}{bc}\right\}$$

Thus we get:

$$\sum_{k\in(\mathbb{Z}/a\mathbb{Z})^\times} \sum_{i=0}^{f_1-1} \left\{\frac{\mu k p^i}{abc}\right\} = \frac{(a-1)f_1}{2} + \sum_{i=0}^{f_1-1}\left\{\frac{\mu p^i}{bc}\right\}$$

Plugging this back into equation gives:

$$\sum_{h\in H}\sum_{i=0}^{f-1}\left\{\frac{\mu h p^i}{abc}\right\} = \frac{(a-1)f_1}{2} + \sum_{i=0}^{f_1-1}\left\{\frac{\mu p^i}{bc}\right\} - \sum_{i=0}^{f_1-1}\left\{\frac{\mu u p^i}{bc}\right\}$$

Rearranging we get:

$$\sum_{i=0}^{f_1-1}\left\{\frac{\mu u p^i}{bc}\right\} = \sum_{i=0}^{f_1-1}\left\{\frac{\mu p^i}{bc}\right\} + \frac{(a-1)f_1}{2} - \sum_{h\in H}\sum_{i=0}^{f-1}\left\{\frac{\mu h p^i}{abc}\right\}$$

which implies the desired result. □

Theorem 14.9. *Suppose a, b, c, p are primes with $f = \mathrm{ord}_{abc}(p)$. Let $f_1 = \mathrm{ord}_a(p), f_2 = \mathrm{ord}_b(p), f_3 = \mathrm{ord}_c(p)$. Let $2^r, 2^s, 2^t$ be the highest power of 2 dividing f_1, f_2, f_3 respectively. If $r > s = t = 1$, $f_2 = b-1$, $f_3 = c-1$, the largest odd divisors of f_1, f_2, f_3 are comprime, and there exists i, j such that $p^i \equiv b \pmod{ac}$ and $p^i \equiv \pmod{ab}$ then the projective variety V defined by*

$$w^{abc} + x^a + y^b + z^c = 0$$

over $\mathbb{F}_p$ is supersingular.

Proof. Let u be defined to be the integer satisfying the following equivalences:

$$\begin{aligned} u &\equiv 1 \pmod a \\ u &\equiv -1 \pmod b \\ u &\equiv 1 \pmod c \end{aligned}$$

Similarly let v be an integer such that

$$\begin{aligned} v &\equiv 1 \pmod a \\ v &\equiv 1 \pmod b \\ v &\equiv -1 \pmod c \end{aligned}$$

Let H be the subgroup of $(\mathbb{Z}/abc\mathbb{Z})^\times$ generated by p. Let S be a set of coset representatives for H in $(\mathbb{Z}/abc\mathbb{Z})^\times$. We claim for all $x \in S$ the cosets $xH, -xH, uxH, vxH$ are distinct. Note that as $r > s = t > 0$ $-1, u, v$ cannot be powers of p. Thus $uH, vH, -H$ are distinct from H. Now note that $u^2 = v^2 = 1$. Furthermore, $uv \in -H$ as:

$$\begin{aligned} -p^{f/2} &\equiv 1 \pmod a \\ -p^{f/2} &\equiv -1 \pmod b \\ -p^{f/2} &\equiv -1 \pmod c \end{aligned}$$

Thus $(uH)^2 = H, (vH)^2 = H, (uH)(vH) = -H$. Thus implies $H, -H, uH, vH$ are the distinct cosets of H and hence $xH, -xH, uxH, vxH$ are distinct. Now define

$$g(\mu) := \sum_{i=1}^{f} \left\{ \frac{\mu p^i}{abc} \right\}$$

By theorem 14.6, V is supersingular if and only if:

$$g(\mu) = \frac{f}{2}$$

for all μ relatively prime to abc. As $g(\mu) = g(p\mu)$, we then only need to show equation 14 holds for all $\mu \in S$. We will now show that those equivalences holds. Due to pairing up:

$$g(\mu) + g(-\mu) = f$$

Now as b lies in the subgroup generated by p modulo ac, we have for all μ:

$$\sum_{i=0}^{f_2-1} \left\{ \frac{\mu p^i}{ac} \right\} = \sum_{i=0}^{f_2-1} \left\{ \frac{\mu b p^i}{ac} \right\}$$

Thus by lemma 14.8, for all μ relatively prime to abc,

$$\sum_{g \in (\mathbb{Z}/b\mathbb{Z})^\times / G} \sum_{i=1}^{f-1} \left\{ \frac{\mu g p^i}{abc} \right\} = \frac{f_2(b-1)}{2}$$

where G is the subgroup of $(\mathbb{Z}/b\mathbb{Z})^\times$ generated by p^{f_4} for $f_4 = \mathrm{ord}_{ac}(p) = \mathrm{lcm}\,(f_1, f_3)$. As the odd parts of f_1, f_2, f_3 are coprime, p is a primitive root modulo b, and $r > s = 1$, we will have $\gcd(f_4, b-1) = \gcd(f_4, f_2) = 2$. Thus G will be the set of squares modulo b. As $s = 1$, $b \equiv 3 \pmod 4$ and so -1 is not a square modulo b. As such, $1, u$ are the coset representatives of $(\mathbb{Z}/b\mathbb{Z})^\times / G$. Thus we have:

$$g(\mu) + g(u\mu) = f$$

As $(uv\mu H) = -\mu H$, plugging in $-\mu$ gives:

$$g(-\mu) + g(v\mu) = f$$

As $g(-\mu) + g(\mu) = f$, this means $g(\mu) = g(v\mu)$. Applying the same reasoning to the subgroup generated by p modulo ab:

$$g(\mu) + g(v\mu) = f$$

which implies for all μ relatively prime to abc we have: $g(\mu) = f/2$. As stated before, this implies V is supersingular. □

Theorem 14.10. *Suppose d, e, g, p are primes with p a primitive root modulo e, g and $v_2(e-1) > v_2(g-1) = 1$ and $\gcd(e-1, g-1) = 2$. If the projective variety V defined by*

$$w^{deg} + x^d + y^e + z^g = 0$$

over $\mathbb{F}_p$ is supersingular then there exists i such that $p^i \equiv d \pmod{eg}$.

Proof. As p is a primitive root modulo e, g and $\gcd(e-1, g-1) = 2$, p generates a subgroup of order $\frac{\phi(eg)}{2}$ modulo eg. Thus if there does not exist an i for which $p^i \equiv d \pmod{eg}$, d, p must generate $(\mathbb{Z}/eg\mathbb{Z})^\times$. By theorem 14.6 and lemma 14.8, we must have for each μ relatively prime to ac

$$\sum_{i=0}^{\frac{\phi(eg)}{2}-1} \left\{\frac{\mu p^i}{eg}\right\} = \sum_{i=0}^{\frac{\phi(eg)}{2}-1} \left\{\frac{\mu d p^i}{eg}\right\}$$

However, as d, p generate $(\mathbb{Z}/eg\mathbb{Z})^\times$, this implies for each μ

$$\sum_{i=0}^{\frac{\phi(eg)}{2}-1} \left\{\frac{\mu p^i}{eg}\right\}$$

is constant and thus equal to $\frac{\phi(eg)}{2}$ as summing the sums for $\mu = 1, \mu = -1$ gives $\phi(eg)$ by cancellation. However, by lemma 14.1, this implies there cannot exist a character primitive modulo eg with $\chi(-1) = -1, \chi(p) = 1$. However, if we take $\alpha_1 = \frac{e-1}{2}, \alpha_3 = \frac{g-1}{2}$ then:

$$\frac{\alpha_1}{f_1} + \frac{\alpha_3}{f_3} \in \mathbb{Z}$$

and $\alpha_1 + \alpha_3$ is odd. Thus by lemma 14.2, there should exist such a character satisfying those conditions, which gives us a contradiction. Thus d is in the group generated by p modulo eg. □

Corollary 14.10.1. *Suppose a, b, c, p are primes with p a primitive root modulo a, b, c, $v_2(a-1) > v_2(b-1) = 2 > v_2(a-1) = 1$, and the odd parts of $a-1, b-1, c-1$ relatively prime. If the projective variety V defined by*

$$w^{abc} + x^a + y^b + z^c = 0$$

over $\mathbb{F}_p$ is supersingular then there exists i, j, k such that $p^i \equiv a \pmod{bc}$, $p^j \equiv b \pmod{ac}$, $p^k \equiv c \pmod{ab}$.

Proof. The existence of i, j follow from theorem **??**. Note that p generates a group of order $\frac{\phi(ab)}{4}$ modulo ab. By theorem 14.6 and lemma 14.8, we must have for each μ relatively prime to ab

$$\sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{\mu p^i}{ab}\right\} = \sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{\mu c p^i}{ab}\right\}$$

Now if c, p generate $(\mathbb{Z}/ab\mathbb{Z})^\times$, then

$$\sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{\mu p^i}{ab}\right\}$$

is constant across all μ relatively prime to ab. If c, p don't generate $(\mathbb{Z}/ab\mathbb{Z})^\times$ then they generate a group $N = \langle c, p\rangle$ of index 2 over $\langle p\rangle$. As a result, $c^2 \in \langle p\rangle$. Thus there exists an i such that

$$p^i \equiv c^2 \pmod{ab}$$

Assume the i above is minimal. If i is odd then $v_2(\text{ord}_{ab}(c)) = r+1$, which cannot happen as $\max(v_2(a-1), v_2(b-1)) = r$. If r is even, then there exists a u such that $u^2 = 1 \pmod{ab}$ and

$$p^{i/2} \equiv uc \pmod{ab}$$

u must be ± 1 modulo each of a, b. If it is 1 mod b, then it is either equal to $p^{\phi(ab)/4}$ or $p^{\phi(ab)/8}$. Otherwise, either $p^{\phi(ab)/8}u = -1$ or $u = -1$. Either way we have $-1 \in \langle c, p\rangle$. However, this implies

$$\sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{\mu p^i}{ab}\right\} = \sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{-\mu p^i}{ab}\right\}$$

However, by cancellation the two sides of the above equality sum to $\phi(ab)/4$. Thus in both of our cases we have:

$$\sum_{i=0}^{\frac{\phi(ab)}{2}-1} \left\{\frac{\mu p^i}{ab}\right\} = \frac{\phi(ab)}{8}$$

However, by lemma 14.1, this implies there cannot exist a character primitive modulo ab with $\chi(-1) = -1, \chi(p) = 1$. However, if we take $\alpha_1 = \frac{a-1}{4}, \alpha_3 = \frac{3(b-1)}{4}$ then:

$$\frac{\alpha_1}{f_1} + \frac{\alpha_3}{f_3} \in \mathbb{Z}$$

and $\alpha_1 + \alpha_3$ is odd. Thus by lemma 14.2, there should exist such a character satisfying those conditions, which gives us a contradiction. Thus c is in the group generated by p modulo ab, as desired.

□

Theorem 14.11. *Suppose a, b, c, p are primes with $f = \text{ord}_{abc}(p)$. Let $f_1 = \text{ord}_a(p), f_2 = \text{ord}_b(p), f_3 = \text{ord}_c(p)$. Let $2^r, 2^s, 2^t$ be the highest power of 2 dividing f_1, f_2, f_3 respectively. If $r > s = 2 > t = 1$, $f_1 = a-1$, $f_2 = b-1$, $f_3 = c-1$, the largest odd divisors of f_1, f_2, f_3 are coprime, and there exists i, j, k such that $p^i \equiv a \pmod{bc}$, $p^j \equiv b \pmod{ac}$, and $p^k \equiv c \pmod{ab}$ then the projective variety V defined by*

$$w^{abc} + x^a + y^b + z^c = 0$$

over $\mathbb{F}_p$ is supersingular.

Proof. Suppose i is an integer such that $i^2 \equiv -1 \pmod{b}$. Let α_1 be defined to be the integer satisfying the following equivalences:

$$\alpha_1 \equiv 1 \pmod{a}$$
$$\alpha_1 \equiv i \pmod{b}$$
$$\alpha_1 \equiv 1 \pmod{c}$$

Let $H = \langle p\rangle$ in $G = (\mathbb{Z}/abc\mathbb{Z})^\times$. Note that $-1, \alpha_1$ generate the 8 cosets of H. Let G_a be the subgroup of G with elements $\equiv 1 \pmod{bc}$ and let G_b, G_c be defined similarly. Let $H_a = G_a \cap H$ and let H_b, H_c be defined similarly. Observe the following:

- The cosets of H_c in G_c are generated by $-\alpha_1^2$
- The cosets of H_b in G_b are generated by α_1
- The cosets of H_c in G_c are generated by $-\alpha_1$

Let

$$g(\mu) = \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i}{abc} \right\}$$

As a is in the group generated by p in $(\mathbb{Z}/bc\mathbb{Z})^\times$ we have for all μ relatively prime to bc

$$\sum_{i=0}^{f_1-1} \left\{ \frac{\mu p^i}{bc} \right\} = \sum_{i=0}^{f_1-1} \left\{ \frac{\mu a p^i}{bc} \right\}$$

Thus by lemma 14.8, for all μ relatively prime to abc,

$$\sum_{g \in G_b/H_b} \sum_{i=1}^{f-1} \left\{ \frac{\mu g p^i}{abc} \right\} = \frac{f_1(a-1)}{2}$$

Which by observation 1, is equivalent to:

$$g(\mu) + g(-\alpha_1^2 \mu) = f$$

By the same reasoning observation (2) becomes:

$$g(\mu) + g(\alpha_1 \mu) + g(\alpha_1^2 \mu) + g(\alpha_1^3 \mu) = 2f$$

and observation (3) becomes:

$$g(\mu) + g(-\alpha_1 \mu) + g(\alpha_1^2 \mu) + g(-\alpha_1^3 \mu) = 2f$$

These equations combined with:

$$g(\mu) + g(-\mu) = f$$

gives:

$$g(\mu) = \frac{f}{2}$$

By theorem 14.6, V is supersingular. □

Conjecture 14.12. *Let a, b, c, p be distinct primes. Let $f = \mathrm{ord}_{abc}(p), f_1 = \mathrm{ord}_a(p), f_2 = \mathrm{ord}_b(p), f_3 = \mathrm{ord}_c(p)$ and let $2^r, 2^s, 2^t$ be the largest powers of 2 dividing f_1, f_2, f_3 respectively. If $r \geq s \geq t$, the variety V defined by the equation:*

$$x^a + y^b + z^c + w^{abc}$$

is supersingular if and only if $p^{f/2} \equiv -1 \pmod{abc}$ or if conditions 1,2 hold and either of 3,4 hold:

1. *$r > s$ and $\frac{f_1}{2^r}, \frac{f_2}{2^s}, \frac{f_3}{2^t}$ are pairwise coprime.*
2. *$f_2 = b-1, f_3 = c-1$ and there exists an integer j such that $p^j \equiv c \pmod{ab}$*
3. *$s = t = 1$ and there exists an integer i such that $p^i \equiv b \pmod{ac}$*
4. *$s = 2, t = 1,\ f_1 = a-1$, and there exists an integer i such that $p^i \equiv a \pmod{bc}$ and there exists an integer j such that $p^j \equiv b \pmod{ac}$*

15 Surfaces of the Form $w^a + x^a + y^{ab} + z^{ab}$

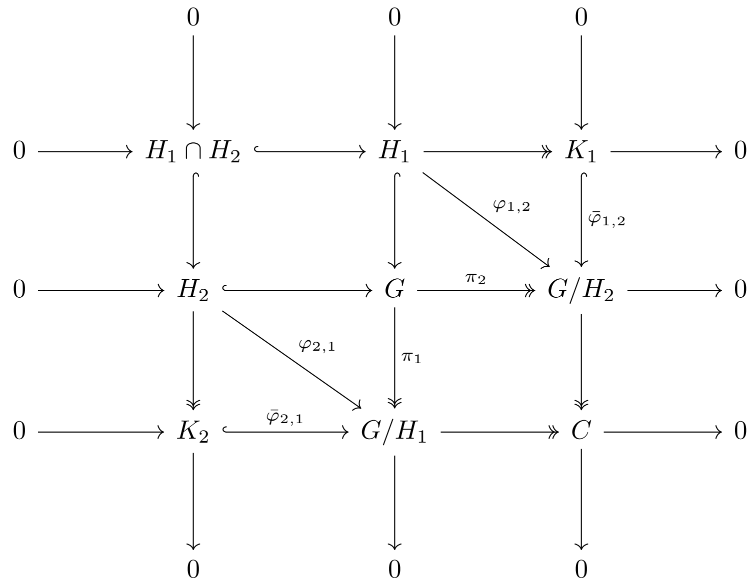
Let X be the diagonal surface defined by $w^a + x^a + y^{ab} + z^{ab}$ over $\mathbb{F}_p$.

Lemma 15.1. *Let $H_1, H_2 \lhd G$ be normal subgroups with quotient maps $\pi_i : G \to G/H_i$ and consider the maps,*

$$\varphi_{i,j} : H_i \hookrightarrow G \overset{\pi_j}{\twoheadrightarrow} G/H_j$$

Then $\varphi_{1,2}$ is surjective iff $\varphi_{2,1}$ is surjective.

Proof. Consider the commutative diagram with exact rows and columns,



where $K_i = H_i/(H_1 \cap H_2)$ and the maps $\bar{\varphi}_{i,j} : K_i \to G/H_j$ are induced by the maps $\varphi_{i,j}$ and are injective by the first isomorphism theorem. Exactness and commutativity are obvious except at C which I have yet to define! By commutativity and surjectivity, $\text{im}\bar{\varphi}_{i,j} = \pi_j(H) \lhd \text{im}\pi_j = G/H_j$ so $\Im\bar{\varphi}_{i,j}$ is a normal subgroup and thus $\text{coker}\bar{\varphi}_{i,j} = (G/H_j)/\text{im}\bar{\varphi}_{i,j}$ exists. Take $C = \text{coker}\bar{\varphi}_{1,2}$. Furthermore, the exactness of columns gives a surjective map $G/H_1 \to C$ which makes the bottom right square commute. By the nine lemma, the bottom row is exact proving that $C = \text{coker}\bar{\varphi}_{2,1}$. Finally, by exactness,

$$\bar{\varphi}_{1,2} \text{ is an isomorphism} \iff C = 0 \iff \bar{\varphi}_{2,1} \text{ is an isomorphism}$$

But $\varphi_{i,j}$ is a surjection iff $\bar{\varphi}_{i,j}$ is an isomorphism so $\varphi_{1,2}$ is surjective iff $\varphi_{2,1}$ is surjective. □

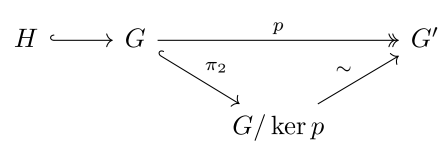
Lemma 15.2. *Let $p : G \to G'$ be surjective and $H \lhd G$ a normal subgroup. Then there exist coset representatives for G/H with fixed image in G' if and only if $p(H) = G'$. Furthermore, we if this holds, we may take the coset representatives to be trivial in G'.*

Proof. A set $S \subset G$ contains a full set of coset represenatives for G/H if $\pi(S) = G/H$. Therefore, we require that $\pi(p^{-1}(x)) = G/H$ for some $x \in G'$. Since we must hit the identity, $H \cap p^{-1}(x) \neq \varnothing$ so there exits $h \in H$ such that $p(h) = x$. Thus, $p^{-1}(x) = h \ker p$ so $\pi(p^{-1}(h)) = \pi(h)\pi(\ker p) = \pi(\ker p)$ so we may take $h = e$. The conclusion holds if and only if $\pi(\ker p) = G/H$.

Take $H_1 = H$ and $H_2 = \ker p$ in Lemma 15.1 and thus,

$$\text{im}\varphi_{2,1} = \pi(\ker p) = G/H \iff \text{im}\varphi_{1,2} = \pi_2(H) = G/\ker p$$

but the map p naturally factors through $G/\ker p$ as,



so $p(H) = G' \iff \pi_2(H) = G/\ker p$. □

Theorem 15.3. *Suppose there exists a subgroup $H \subset (\mathbb{Z}/ab\mathbb{Z})^\times$ such that $p \in H$ and $-1 \notin H$*

$$H \hookrightarrow (\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/a\mathbb{Z})^\times$$

is surjective. Then X is not supersingular.

Proof. By Theorem 6.15, if X is supersingular then,

$$\sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\{ \frac{\mu e_i p^j}{ab} \right\} = 2f$$

However, there is a projection map $X \to F_a^3$ so F_a^3 is supersingular and thus, by Shioda, $p^v \equiv -1 \mod a$. However, we know that,

$$\frac{e_0'}{a} + \frac{e_1'}{a} + \frac{e_2'}{ab} + \frac{e_2'}{ab} = \frac{b(e_0' + e_1') + e_2' + e_3'}{ab} \in \mathbb{Z}$$

and thus $b \mid e_2' + e_3'$. Thus we have,

$$\sum_{j=0}^{f-1} \left\{ \frac{\mu e_0' p^j}{a} \right\} + \sum_{j=0}^{f-1} \left\{ \frac{\mu e_1' p^j}{a} \right\} + \sum_{j=0}^{f-1} \left\{ \frac{\mu e_2' p^j}{ab} \right\} + \sum_{j=0}^{f-1} \left\{ \frac{\mu e_3' p^j}{ab} \right\} = 2f$$

however because $p^v \equiv -1 \mod a$,

$$\sum_{j=0}^{f-1} \left\{ \frac{\mu e_0' p^j}{a} \right\} + \sum_{j=0}^{f-1} \left\{ \frac{\mu e_1' p^j}{a} \right\} = f$$

so we know that,

$$\sum_{j=0}^{f-1} \left\{ \frac{\mu e_2' p^j}{ab} \right\} + \sum_{j=0}^{f-1} \left\{ \frac{\mu e_3' p^j}{ab} \right\} = f$$

Define the sum,

$$S(x) = \sum_{j=0}^{f-1} \left\{ \frac{x p^j}{ab} \right\}$$

The above gives the functional equation,

$$S(x) + S(y) = f$$

whenever $x + y \equiv 0 \mod b$. In particular, if $x \equiv y \mod b$ then $S(x) = S(y)$.

Let $\chi : (\mathbb{Z}/ab\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character such that $\chi(H) = 1$ and $\chi(-1) = -1$. This is possible assuming that $-1 \notin H$. Let m_0 be the conductor of χ with a map $\varphi : (\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/m_0\mathbb{Z})^\times$ and $H_0 = \varphi(H)$ and character $\chi_0 : (\mathbb{Z}/m_0\mathbb{Z})^\times \to \mathbb{C}^\times$ inducing χ. Now define the sum,

$$S_0(x) = \sum_{t \in \varphi(\langle p \rangle)} \left\{ \frac{xt}{m_0} \right\} = \frac{1}{|\langle p \rangle \cap \ker \varphi|} \sum_{t \in \langle p \rangle} \left\{ \frac{(ab/m_0)xt}{ab} \right\} = \frac{1}{|\langle p \rangle \cap \ker \varphi|} S\left(\frac{ab}{m_0} x \right)$$

Thus, $S_0(x) = S_0(y)$ whever $m_0 \mid a(x - y) \iff x \equiv y \mod \bar{m}_0 = m_0/(m_0, a)$. Next, let $G = (\mathbb{Z}/m_0\mathbb{Z})^\times$ and $K = \varphi(\langle p \rangle)$ and consider,

$$\begin{aligned}
\sum_{x \in G} \chi_0(x) \frac{x}{m_0} &= \sum_{gH_0 \in G/H_0} \sum_{h \in H_0/K} \sum_{x \in hgK} \chi_0(x) \frac{x}{m_0} = \sum_{gH_0 \in G/H_0} \chi_0(g) \sum_{h \in H_0/K} \sum_{x \in ghK} \frac{x}{m_0} \\
&= \sum_{gH_0 \in G/H_0} \chi_0(g) \sum_{h \in H_0/K} S_0(gh)
\end{aligned}$$

since χ_0 is trivial on H_0 and thus descends to a nontrivial character on G/H_0. By Lemma 15.2, the surjective map,

$$H \hookrightarrow (\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/a\mathbb{Z})^\times$$

alows us to choose coset representatives of G/H_0 which are all trivial under the map $(\mathbb{Z}/m_0\mathbb{Z})^\times \to (\mathbb{Z}/\bar{m}_0\mathbb{Z})^\times$. Therefore, $gh \equiv h \mod \bar{m}_0$ and thus,

$$\sum_{x \in G} \chi_0(x) \frac{x}{m_0} = \sum_{gH_0 \in G/H_0} \chi_0(g) \sum_{h \in H_0/K} S_0(h) = \left(\sum_{h \in H_0/K} S_0(h) \right) \cdot \left(\sum_{gH_0 \in G/H_0} \chi_0(g) \right) = 0$$

since χ_0 is a nontrivial character on G/H_0. This is a contradiction because,

$$\sum_{gH_0 \in G/H_0} \chi_0(g) \sim L(1; \chi_0) \neq 0$$

□

16 Other Families

Theorem 16.1. *Let X be the variety defined by,*

$$x_0^a + x_1^a + x_2^b + x_3^{ab}$$

where a and b are coprime. Suppose that $\operatorname{ord}_b(p)$ is even. Then X is supersingular over $\mathbb{F}_p$ if and only if $p^v \equiv -1 \mod ab$ for some v.

Theorem 16.2. *Let X be the variety defined by,*

$$x_0^a + \cdots + x_{k_a-1}^a + x_{k_a}^b + \cdots + x_{k_a+k_b}^b + x_{k_a+k_b+1}^{ab} + \cdots + x_r^{ab}$$

where a and b are coprime and $k_a, k_b \geq 2$. Then X is supersingular over $\mathbb{F}_p$ if and only if $p^v \equiv -1 \mod ab$ for some v.

17 Conjectures

Lemma 17.1. *If,*

$$S(a) = \sum_{i=0}^{f-1} \left\{ \frac{ap^j}{m} \right\} = \frac{f}{2}$$

for all a coprime to m then there does not exist a primitive character χ modulo m such that $\chi(-1) = -1$ and $\chi(p) = 1$.

Lemma 17.2. *If,*

$$S(a) = \sum_{i=0}^{f-1} \left\{ \frac{ap^j}{m} \right\} = \frac{f}{2}$$

for all $a \in \mathbb{Z}/m\mathbb{Z}$ then $p^v \equiv -1 \mod m$ for some $v \in \mathbb{Z}$.

References

[1] S. Chowla, On Gaussian Sums, *Proceedings of the National Academy of Sciences*, 48 (7), 1127-8, 1962.

[2] R. Evans, Generalizations of a Theorem of Chowla on Gaussian Sums, *Houston Journal of Mathematics*, 3, 1977.

[3] N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Mathematica*, 31, 119-218, 1975.

[4] S. Lang, *Algebraic Number Theory*, Springer, 1994.

[5] T. Shioda, An example of Unirational Surfaces in Characteristic p, *Mathematische Annalen*, 221, 233-236, 1974.

[6] T. Shioda, T. Katsura, On Fermat Varieties, *Tohoku Math Journal*, 31, 97-115, 1979.r

[7] A. Weil, Numbers of Solutions of Equations in Finite Fields, *Bulletin of the American Mathematical Society*, 55 (5), 497-508, 1949