On the Arithmetic of $\ell$-th Power Twists of Jacobian Varieties of Superelliptic Curves

$$y^\ell = f(x).$$

University of Georgia

Sungkon Chang
The Superelliptic Curves: \( y^\ell = f(x) \)

where \( \ell \) is a regular prime number, 
\( f(x) \) is a monic polynomial over \( \mathbb{Z} \) 
of degree \( d \), with distinct roots (in \( \overline{\mathbb{Q}} \)), 
and \( \ell \nmid d \).

Let \( K := \mathbb{Q}(\zeta_\ell) \), and \( C/\mathbb{Q} \) be the normalization 
of \( y^\ell = f(x) \). For \( D \in \mathbb{Q}^* \), we denote by \( C_D/\mathbb{Q} \) 
the normalization of 
\[ D \, y^\ell = f(x). \]

\( J/\mathbb{Q} := \) the Jacobian variety of \( C/\mathbb{Q} \), 
\( J_D/\mathbb{Q} := \) the Jacobian variety of \( C_D/\mathbb{Q} \).

Let \( \lambda := 1 - [\zeta_\ell] \in \text{End}_K(J_D) \).
We denote the \( \lambda \)-Selmer group of \( (J_D)_K \) by 
\[ \text{Sel}^{(\lambda)}(J_D, K). \]

Note rank \( J_D(\mathbb{Q}) \leq \dim_{\mathbb{F}_\ell} \text{Sel}^{(\lambda)}(J_D, K). \)

**Key Fact**

\[ J_D[\lambda] \cong_K J[\lambda] \]
Main Results

Notation: $\mathcal{P}_\ell(X)$ denotes the set of positive, $\ell$-th power-free integers $< X$.

Theorem 1 (C.)
Suppose that $f(x)$ is irreducible over $K$, and $p := \deg f$ is prime ($\neq \ell$).

Then, there is a positive constant $\epsilon < 1$ depending on $C$ such that

$$
\# \left\{ D \in \mathcal{P}_\ell(X) : \dim \mathbb{F}_\ell \text{Sel}^{(\lambda)}(J_D, K) \\
= \dim \mathbb{F}_\ell \text{Sel}^{(\lambda)}(J, K) \right\} \gg C \frac{X}{(\log X)^\epsilon}.
$$
Main Results

Recall

\[
\text{rank } J_D(\mathbb{Q}) \leq \dim_{\mathbb{F}_\ell} \text{Sel}^{(\lambda)}(J_D, K)
\]

**Cor.** Suppose that there is a positive integer \(D_0\) such that

\[
\text{Sel}^{(\lambda)}(J_{D_0}, K) = 0.
\]

Then, there is a positive constant \(\epsilon < 1\) depending on \(C\) such that

\[
\# \{D \in \mathcal{P}_\ell(X) : \text{rank } J_D(\mathbb{Q}) = 0\} \gg_{C, D_0} \frac{X}{(\log X)^\epsilon}.
\] (1)

**K. Ono** showed (1) for all elliptic curves without 2-torsion points using the theory of modular forms.
Main Results

**Theorem 2 (C.)**
Suppose that \( f(x) \) has a root defined over \( K \).

Then, given a positive integer \( n \), there is a positive constant \( \epsilon < 1 \) depending on \( C \) and \( n \) such that

\[
\# \{ D \in \mathcal{P}_\ell(X) : \dim \mathbb{F}_\ell \operatorname{Sel}^{(\lambda)}(J_D, K) > n \} \gg \frac{X}{(\log X)^\epsilon}.
\]

In particular,

\[
\limsup_D \ dim \mathbb{F}_\ell \operatorname{Sel}^{(\lambda)}(J_D, K) = \infty. \quad (2)
\]
Application of Thm 1

On the number of rational points

Suppose $f(x) \in \mathbb{Z}[x]$ is irreducible over $K$, and has prime degree $p$. Suppose the genus of $C$ is $> 1$.

**Cor.** Let $n := \dim_{\mathbb{F}_\ell} \text{Sel}^{(\lambda)}(J_{D_0}, K)$ for a positive integer $D_0$.

Then, there are positive constants $\gamma$, and $\epsilon < 1$ such that

$$\# \{ D \in \mathcal{P}_\ell(X) : \# C_D(\mathbb{Q}) \leq \gamma 7^n \} \gg \frac{X}{(\log X)^\epsilon}. \tag{3}$$

**Example:** Let $A \in \mathbb{Z}$ be square-free, $\not\equiv 0 \pmod{\ell}$, and $\ell > 3$. Let

$$X_D : y(x^{\ell-1} - Ay^{\ell-1}) = D.$$  

Then, (3) holds for $X_D(\mathbb{Q})$. 
Application of Thm 1

Hyperelliptic Curves: $y^2 = f(x)$.

Cor. Suppose $\deg f := p \geq 5$ is prime, and $f(x)$ is irreducible over $\mathbb{Q}$. Suppose that there is $D_0 \in \mathbb{Z}$ such that

$$n := \dim \mathbb{F}_2 \text{Sel}^{(2)}(J_{D_0}, \mathbb{Q}) < (p - 1)/2.$$ Then, there is a positive constant $\epsilon < 1$ depending on $C$ and $n$ such that

$$\# \{ D \in \mathcal{P}_2(X) : \# C_D(\mathbb{Q}) \leq 2n+1 \} \gg \frac{X}{(\log X)^\epsilon}.$$ 

Example: Let $C_D : D \ y^2 = x^5 + x + 12$. Then, $\text{Sel}^{(2)}(J, \mathbb{Q}) = 0$. Hence,

$$\# \{ D \in \mathcal{P}_2(X) : \# C_D(\mathbb{Q}) = \{\infty\} \} \gg \frac{X}{(\log X)^\epsilon}.$$
Application of Thm 1

Quadratic Twists of an Elliptic Curve:
\[ D y^2 = x^3 + ax + b. \]

**Cor.** Let us assume that \( \text{III}(E'/\mathbb{Q}) \) is finite for all elliptic curves \( E'/\mathbb{Q} \). Let \( E/\mathbb{Q} \) be an elliptic curve without \( \mathbb{Q} \)-rational 2-torsion points such that \( \dim \mathbb{F}_2 \text{Sel}^{(2)}(E_{D_0}, \mathbb{Q}) = 1 \) for some positive \( D_0 \in \mathbb{Z} \). Then, there is a positive constant \( \epsilon < 1 \) such that

\[
\# \{ D \in \mathcal{P}_2(X) : \text{rank } E_D(\mathbb{Q}) = 1, \quad \text{III}(E_D/\mathbb{Q})[2] = 0 \} \gg E,D_0 \frac{X}{(\log X)^\epsilon}.
\]

**Thm** (Iwaniec-Sarnak, 2000) Assume RH. Then, for all elliptic curves \( E/\mathbb{Q} \),

\[
\# \{|D| < X : \text{rank } E_D(\mathbb{Q}) = 1 \} \gg X.
\]
Application of Thm 1

Cubic Twists of Elliptic Curves

Let $E/\mathbb{Q}$ be $y^2 = x^3 + A$ such that $A \neq -3, +1$ is a square-free integer, and for $D \in \mathbb{Q}^*$, let $E_D$ be the cubic twist

$$y^2 = x^3 + AD^2.$$ 

**Cor.** Suppose there is a positive integer $D_0$ s.t. $\dim_{\mathbb{F}_3} \text{Sel}^\lambda(E^{D_0}, K) = 0$. Then, there is a positive constant $\epsilon < 1$ such that

$$\# \{D \in \mathcal{P}_3(X) : \text{rank } E_D^D(\mathbb{Q}) = 0\} \gg E \frac{X}{(\log X)^\epsilon}.$$

**Example:** There are infinitely many square-free $A$ s.t. $E/\mathbb{Q} : y^2 = x^3 + A$ has infinitely many cubic twists of rank 0.

**Remark:** What is known is D. Liemann’s result for $x^3 + y^3 = D$ (isomorphic to $y^2 = x^3 - 432D^2$).
Superelliptic Curves \( y^\ell = f(x) \)
Over a Function Field \( \mathbb{F}_q(t) \)

where \( \ell \neq q \) are prime numbers, 
\( f(x) \in \mathbb{F}_q[x] \) is monic irreducible 
over the constant field \( \mathbb{F}_q \) 
of degree \( d \), with distinct roots, 
and \( \ell \nmid d \).

Let \( R := \mathbb{F}_q[t] \), and \( K := \mathbb{F}_q(t) \). For \( D \in K^* \), 
let \( J_D/K \) be the Jacobian of the normalization of \( D y^\ell = f(x) \).

**Thm.** Suppose that \( q \equiv 1 \mod \ell \).
Then, there is a set \( \mathcal{D} \) of prime elements in \( R \) with positive Dirichlet density such that whenever \( D \) is a product of elements \( \in \mathcal{D} \), 
\[
\text{rank } J_D(K) = 0. \tag{4}
\]
In particular, there are infinitely many \( D \) such that (4) holds.