Most elliptic curves over global function fields are torsion free

by

TRISTAN PHILLIPS (Tucson, AZ)

1. Introduction. Let $E$ be an elliptic curve defined over a global field $K$. For each positive integer $n$ relatively prime to the characteristic of $K$ there is an action of the absolute Galois group $G_K := \text{Gal}(K^{\text{sep}}/K)$ on the $n$-torsion points $E[n](K^{\text{sep}})$ of $E$ which induces a representation

$$\rho_{E,n} : G_K \to \text{Aut}(E[n](K^{\text{sep}})) \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

It is natural to ask how large the image of $\rho_{E,n}$ is. A fundamental result of Serre says that if $E$ is a non-CM elliptic curve over $\mathbb{Q}$, then $\rho_{E,p}$ is surjective for all but finitely many primes $p$ [Ser72]. Duke has shown that the set of elliptic curves over $\mathbb{Q}$ for which $\rho_{E,n}$ is surjective for all $n$ has density 1, when counted by naive height [Duk97]. Call an elliptic curve torsion free if its Mordell–Weil group $E(\mathbb{Q})$ is torsion free. Since $\rho_{E,n}$ being surjective implies $E[n](\mathbb{Q}) = \emptyset$, a pleasing consequence of Duke’s result is that the set of torsion free elliptic curves over $\mathbb{Q}$ has density 1.

In order to get analogous results for more general $K$, one must restrict the codomain of $\rho_{E,n}$. Let $\chi_n$ be the cyclotomic character; it is well known that $\chi_n = \det \circ \rho_{E,n}$. Denote by $\Gamma_n \subseteq \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the subgroup determined by the exact sequence

$$0 \to \text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \Gamma_n \xrightarrow{\det} \chi_n(G_K) \to 0.$$ 

Zywina has shown that when $K$ is a number field, the set of elliptic curves for which the image of $\rho_{E,n}$ equals $\Gamma_n$ for all $n$ has density 1 [Zyw10]. This has the consequence that, over any number field, the set of torsion free elliptic curves has density 1.

2020 Mathematics Subject Classification: Primary 11G05; Secondary 11F80, 11N36. 
Key words and phrases: elliptic curves, torsion points, Galois representations, sieve methods, global function fields.
Received 8 January 2021; revised 16 August 2021.
Published online 22 November 2021.

DOI: 10.4064/aa210108-23-8 © Instytut Matematyczny PAN, 2021
When \( K \) is a global function field, a classical result of Igusa says that for any non-isotrivial elliptic curve \( E \) and any \( n \) relatively prime to \( \text{Char}(K) \), the image of \( \rho_{E,n} \) equals \( \Gamma_n \) for all but finitely many \( n \) [Igu59] (see also [BLV09]). It is then natural to ask for analogs of the results of Duke and Zywina. In this article we shall prove such an analog.

2. Statement of main result. Let \( \mathbb{F}_q \) be a finite field of characteristic \( p > 3 \). Let \( K \) be the function field of a projective smooth genus \( g \) curve \( C \) over \( \mathbb{F}_q \). Assume that there exists a degree 1 rational point \( \infty \) on \( C \) (this assumption is needed in order to apply a version of the large sieve inequality). Let \( \mathcal{O}_K \) be the set of functions on \( C \) regular away from \( \infty \), let \( \text{ord}_\infty : K \times \rightarrow \mathbb{Z} \) be the valuation at \( \infty \), and let \( K_\infty \) denote the completion of \( K \) with respect to the absolute value \( |f|_\infty := q^{-\text{ord}_\infty f} \).

Let \( E \) be an elliptic curve defined over \( K \). As \( \text{Char}(K) > 3 \), \( E \) has a model \( E(a,b) : y^2 = x^3 + ax + b \) with \( a, b \in \mathcal{O}_K \). Conversely, if \( \Delta(a,b) := -16(4a^3 + 27b^2) \) is non-zero then \( E(a,b) \) defines an elliptic curve over \( K \).

An elliptic curve \( E \) over a field of characteristic \( p \) is ordinary if \( E[p](K_{\text{sep}}) \cong \mathbb{Z}/p\mathbb{Z} \), otherwise \( E[p](K_{\text{sep}}) \) is trivial and we call \( E \) supersingular.

For a prime \( \ell \neq p \) we define \( \rho_{E,\ell} \) as in the introduction. If \( E \) is ordinary then the action of \( G_K \) on \( E[p] \) induces a representation

\[
\rho_{E,p} : G_K \rightarrow \text{Aut}(E[p]) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}.
\]

If \( E \) is supersingular, set \( \rho_{E,p}(G_K) = \{1\} \).

Define the sets

\[
\mathcal{C}(x) := \{(a, b) \in \mathcal{O}_K^2 : \Delta(a,b) \neq 0, \max\{|a|_\infty, |b|_\infty\} \leq q^x\},
\]

\[
\mathcal{E}_\ell(x) := \{(a, b) \in \mathcal{C}(x) : \rho_{E(a,b),\ell}(G_K) \neq \Gamma_\ell\},
\]

\[
\mathcal{E}_p(x) := \{(a, b) \in \mathcal{C}(x) : \rho_{E(a,b),p}(G_K) \neq (\mathbb{Z}/p\mathbb{Z})^{\times}\},
\]

\[
\mathcal{E}(x) := \bigcup_\ell \mathcal{E}_\ell(x),
\]

where the union is over all primes, including \( \ell = p \).

Let \( f, g \) be positive real-valued functions. Then \( f \sim g \) means that \( \lim_{x \to \infty} f(x)/g(x) = 1 \), and \( f \ll g \) means that there exists a constant \( c \) such that for all sufficiently large \( x \), \( f(x) \leq c \cdot g(x) \). We sometimes use the alternate notation \( f = O(g) \) for \( f \ll g \). Subscripts on \( \ll \) and \( O \) will be used to denote the variables the implied constant depends on.
Applying the Riemann–Roch theorem to the divisor $x\infty$ on the curve $\mathcal{C}$ we see that
\begin{equation}
\#\mathcal{C}(x) \sim cq^{2x}
\end{equation}
where $c$ is a positive constant depending on $K$.

The following result of Cojocaru and Hall gives an explicit version of the previously mentioned result of Igusa:

**Theorem 2.1** ([CH05, Theorem 1.1]). Define a constant, depending only on $g = \text{genus}(K)$, by
\[
c(g) := 2 + \max \left\{ \ell : \frac{\ell - (6 + 3e_4 + 4e_3)}{12} \leq g \right\},
\]
where
\[
e_j := \begin{cases} 
1 & \text{if } \ell \equiv 1 \pmod{j}, \\
-1 & \text{else}.
\end{cases}
\]
Then $\rho_{E,\ell}(G_K)$ equals $\Gamma_\ell$ for all $\ell \geq c(g)$.

We now state our main result:

**Theorem 2.2.** Let $K$ be a genus $g$ global function field of characteristic $p$. If there are no primes $\ell \neq p$ less than $c(g)$ such that $p | (\ell \pm 1)$, then
\[
\frac{\#\mathcal{E}(x)}{\#\mathcal{C}(x)} \ll_K \frac{x}{q^{x/2}}.
\]
In particular,
\[
\lim_{x \to \infty} \frac{\#\mathcal{E}(x)}{\#\mathcal{C}(x)} = 0.
\]

**Remark 2.3.** The condition $p \nmid (\ell \pm 1)$ in the theorem is needed in order to apply a version of the Chebotarev density theorem for varieties over finite fields (Lemma 4.1).

The theorem implies that the set of torsion free elliptic curves over $K$ has density 1. Our proof uses a multidimensional large sieve for global function fields and is similar to the argument in the number field case.

### 3. Large sieve

Define the *degree* of an ideal $I \subset \mathcal{O}_K$ as $\deg(I) := \dim_{\mathbb{F}_q}(O_K/I\mathcal{O}_K)$.

Extend $|\cdot|_\infty$ to $K_\infty^2$ by
\[
|(f_1, f_2)|_\infty = \max \{|f_1|_\infty, |f_2|_\infty\}.
\]

The following is a 2-dimensional large sieve inequality for global function fields:
Theorem 3.1 (Large sieve). Let \( Q, R \in \mathbb{Z}_{\geq 0} \). For each prime ideal \( P \) of \( \mathcal{O}_K \) let \( \omega_P \) be a real number in \([0, 1)\). Let \( W \) be a subset of \( \mathcal{O}_K^2 \) such that
\[
\#W_P \leq (1 - \omega_P) \cdot q^{2 \deg(P)}
\]
where \( W_P \) denotes the canonical image of \( W \) in \( (\mathcal{O}_K/PO_K)^2 \). Then
\[
\#\{w \in W : |w|_\infty \leq q^R\} \leq \frac{q^{2 \max\{R + 1, 2Q + 2g\}}}{L(Q)}
\]
with
\[
L(Q) = 1 + \sum_{I \in S_Q} \prod_{P|M} \frac{\omega_P}{1 - \omega_P}
\]
where \( S_Q \) denotes the set of square free ideals \( I \subseteq \mathcal{O}_K \) with \( \deg(I) \leq Q \).

Proof. The proof of the \( K = \mathbb{F}_q(T) \) case given in [Hsu96, Theorem 3.2] carries over verbatim to our more general \( K \) (see [Hsu99, Theorem 3.2] for the 1-dimensional case).

4. Elliptic curves over finite fields. Let \( E \) be an elliptic curve over \( \mathbb{F}_q^n \). For a rational prime \( \ell \neq p \) we get a representation
\[
\overline{\rho}_{E, \ell} : \text{Gal}(\overline{\mathbb{F}}_q^n/\mathbb{F}_q^n) \to \Gamma_\ell \subset \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),
\]
and for \( \ell = p \),
\[
\overline{\rho}_{E,p} : \text{Gal}(\overline{\mathbb{F}}_q^n/\mathbb{F}_q^n) \to (\mathbb{Z}/p\mathbb{Z})^\times
\]
where \( \overline{\rho}_{E,p}(\overline{\mathbb{F}}_q^n/\mathbb{F}_q^n) = \{1\} \) if \( E \) is supersingular.

For \((a, b) \in \mathbb{F}_q^2 \) with \( \Delta_{(a, b)} := -16(4a^3 + 27b^2) \) non-zero, let \( E_{(a, b)} \) be the elliptic curve
\[
E_{(a, b)} : y^2 = x^3 + ax + b.
\]

For \( \ell \neq p \) and \( C \) a conjugacy class of \( \Gamma_\ell \) set
\[
\Omega_{\ell, C}(n) := \{(a, b) \in \mathbb{F}_q^n : \Delta_{(a, b)} \neq 0, \overline{\rho}_{E_{(a, b)}, \ell}(\text{Frob}_{q^n}) \in C\}.
\]

For \( \ell = p \) and \( t \in (\mathbb{Z}/p\mathbb{Z})^\times \) set
\[
\Omega_{p, t}(n) := \{(a, b) \in \mathbb{F}_q^n : \Delta_{(a, b)} \neq 0, \overline{\rho}_{E_{(a, b)}, p}(\text{Frob}_{q^n}) = t\}
\]
Applying the Chebotarev density theorem for finite fields, as given in [Kow06, Theorem 1], with \( U = \text{Spec}(\mathbb{F}_q[a, b, 1/(4a^3 + 27b^2)]) \) gives:

Lemma 4.1. For any \( \ell \) such that \( p \nmid \#\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell(\ell + 1)(\ell - 1) \), let \( C \subset \Gamma_\ell \) be a subset closed under conjugation. Then, for any \( n \) such that \( q^n \equiv \text{det}(C) \pmod{\ell} \),
\[
\#\Omega_{\ell, C}(n) = \frac{\#C}{\#\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})} q^{2n} + O(q^{3n/2} \cdot \sqrt{\#C} \cdot \#\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^3)}
\]
where the implied constant is absolute. For $\ell = p$ and $t \in (\mathbb{Z}/p\mathbb{Z})^\times$,
\[
\#\Omega_{p,t}(n) = \frac{1}{p-1}q^n + O\left(q^{3n/2}(p-1)^{3/2}\right)
\]
where the implied constant is absolute.

**Remark 4.2.** The arguments in [Jon10, proof of Theorem 8] can be generalized to give a proof of Lemma 4.1 different from Kowalski’s proof.

**5. Estimating $\#E_\ell(x)$.** For $\ell \neq p$ and $d$ relatively prime to $\ell$, let $\Sigma_K(Q; \ell, d)$ denote the set of prime ideals $P \subset \mathcal{O}_K$ with $\deg(P) \leq Q$ and
\[
q^{\deg(P)} \equiv d \pmod{\ell}.
\]
We may suppose $q^Q \equiv d \pmod{\ell}$; if not, we can decrease $Q$ so that it satisfies this condition. Under this assumption, the prime polynomial theorem implies

\[(5.1) \quad \frac{q^Q}{Q} \ll \#\Sigma_K(Q; \ell, d), \]
where the implied constant is absolute.

**Lemma 5.1.** For any prime $\ell \neq p$ satisfying $p \nmid (\ell \pm 1)$,
\[
\frac{\#E_\ell(x)}{\#C(x)} \ll_{K,\ell} \frac{x}{q^{x/2}}.
\]

**Proof.** Let $C$ be a conjugacy class of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $d = \det(C)$. Set $W_C(x) := \{(a, b) \in C(x) : \rho_{E_{(a,b),\ell}}(G_K \cap C) = 0\}$. Let $C_1, \ldots, C_m$ be the determinant 1 conjugacy classes of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By [Zyw10, Lemma A.10], $E_\ell(x) = \bigcup_{i=1}^m W_{C_i}(x)$. Hence
\[
\frac{\#E_\ell(x)}{\#C(x)} \leq \sum_{i=1}^m \frac{\#W_{C_i}(x)}{\#C(x)}.
\]

We now use the large sieve to estimate $\#W_C(x)$. Take $R = x$ and $Q = x/2$. For $P \in \Sigma_K(Q; \ell, d)$ set $\mathbb{F}_P = \mathcal{O}_K/P\mathcal{O}_K$, $\Omega_P := \Omega_C(\deg(P))$, and
\[
\omega_P := \frac{\#\Omega_P}{q^{2\deg(P)}}.
\]
Denote by $W_P$ the image of $W_C(X)$ in $\mathbb{F}_P^2$.

Let $\text{Frob}_P$ denote the $q^{\deg(P)}$ Frobenius endomorphism. If $(a, b) \in E_\ell(x)$ is such that $(a, b) \mod P$ is in $\Omega_P$ then $\overline{\rho_{E_{(a,b),\ell}}}(\text{Frob}_P) \in C$ implies $(a, b) \notin W_C(x)$. Hence $W_P \subset \mathbb{F}_P^2 \setminus \Omega_P$, which shows $\#W_P \leq (1 - \omega_P) \cdot q^{2\deg(P)}$. Therefore, by the large sieve inequality,
\[
\#W_C(x) \leq \frac{q^2\max\{x+1, x+2g\}}{L(Q)} \ll_{q,g} \frac{q^{2x}}{L(Q)}
\]
where
\[ L(Q) = 1 + \sum_{I \in S_Q} \prod_{P | M} \frac{\omega_P}{1 - \omega_P} \geq \sum_{P \in \Sigma_K(Q; \ell, d)} \omega_P. \]

But by Lemma [4.1]
\[ \omega_P = \frac{\#\Omega_C(\deg(P))}{q^{2\deg(P)}} = \frac{\#C}{\# SL_2(\mathbb{Z}/\ell\mathbb{Z})} + O\left(\sqrt{\#C \cdot \# GL_2(\mathbb{Z}/\ell\mathbb{Z})^3} \right). \]

Therefore
\[ L(Q) \geq \sum_{P \in \Sigma_K(Q; \ell, d)} \left( \frac{\#C}{\# SL_2(\mathbb{Z}/\ell\mathbb{Z})} + O\left(\sqrt{\#C \cdot \# GL_2(\mathbb{Z}/\ell\mathbb{Z})^3} \right) \right) \sim \# \Sigma_K(Q; \ell, d) \frac{\#C}{\# SL_2(\mathbb{Z}/\ell\mathbb{Z})}. \]

Hence
\[ \#W_C(x) \ll q, g, \ell \frac{q^{2x}}{\# \Sigma_K(Q; \ell, d)}. \]

From this, together with (5.1) and (2.1), we find that
\[ \frac{\#E_p(x)}{\# C(x)} \leq \sum_{i=1}^{m} \frac{\#W_{C_i}(x)}{\# C(x)} \ll_{K, \ell} \sum_{i=1}^{m} \frac{1}{\# \Sigma_K(Q; \ell, d)} \ll \frac{x}{q^{x/2}}. \]

6. Estimating \( \#E_p(x) \). Let \( \Sigma_K(Q) \) denote the set of prime ideals \( P \subset \mathcal{O}_K \) with \( \deg(P) \leq Q \). By the prime polynomial theorem,
\[ \frac{q^Q}{Q} \ll \# \Sigma_K(Q) \]
where the implied constant is absolute.

**Lemma 6.1.**
\[ \frac{\#E_p(x)}{\# C(x)} \ll_{K} \frac{x}{q^{x/2}}. \]

**Remark 6.2.** This result says “\( \rho_{E,p} \) is usually surjective.” It is interesting to compare this with Igusa’s theorem, which implies that the mod \( p \) Galois representation of the universal elliptic curve over \( K \) is surjective [Igu68].

**Proof of Lemma 6.1.** We again use the large sieve. Let \( t \in (\mathbb{Z}/p\mathbb{Z})^\times \) be a generator. The setup is similar to the \( \ell \neq p \) case:
\[ W_t(x) := \{(a, b) \in C(x) : t \notin \rho_{E(a,b),p}(G_K)\}, \quad R = x, \quad Q = x/2. \]
For each prime $P \subset \mathcal{O}_K$, let
\[
\Omega_P := \Omega_{p,t}(\deg(P)),
\]
\[
\omega_P := \frac{\#\Omega_P}{q^{2\deg(P)}},
\]
\[
W_P := \text{image of } W_t(X) \text{ in } (\mathcal{O}_K/P\mathcal{O}_K)^2.
\]

Note that $W_t(x) = \mathcal{E}_p(x)$.

If $(a, b) \in \mathcal{C}(x)$ is such that $(a, b) \mod P$ is in $\Omega_P$ then $\overline{\rho}_E(a, b) \mod P = t$ implies $(a, b) \notin W_t(x)$. Hence $W_P \subset \mathbb{F}_p^2 \setminus \Omega_P$, which shows that $\#W_P \leq (1 - \omega_P) \cdot q^{2\deg(P)}$. Therefore, by the large sieve inequality,
\[
\#W_t(x) \leq \frac{q^{2\max\{x+1, x+2g\}}}{L(Q)} \ll_{q, g} q^{2x} L(Q)
\]
where
\[
L(Q) = 1 + \sum_{l \in S_Q} \prod_{P | M} \frac{\omega_P}{1 - \omega_P} \geq \sum_{P \in \Sigma_K(Q)} \omega_P.
\]

By Lemma 4.1,
\[
\omega_P = \frac{1}{p-1} + O\left(\frac{(p-1)^{3/2}}{q^{\deg(P)/2}}\right).
\]

Therefore
\[
L(Q) \geq \sum_{P \in \Sigma_K(Q)} \left( \frac{1}{p-1} + O\left(\frac{(p-1)^{3/2}}{q^{\deg(P)/2}}\right)\right) \sim \frac{\#\Sigma_K(Q)}{p-1}.
\]

Hence
\[
\#W_t(x) \ll_q \frac{q^{2x}}{\#\Sigma_K(Q)}.
\]

From this, together with (6.1) and (2.1), it follows that
\[
\frac{\#\mathcal{E}_\ell(x)}{\#\mathcal{C}(x)} = \frac{\#W_t(x)}{\#\mathcal{C}(x)} \ll_K \frac{1}{\#\Sigma_K(Q)} \ll_K x \frac{1}{q^{x/2}}.
\]

**7. Estimating $\#\mathcal{E}(x)$**. We now prove the main theorem:

*Proof of Theorem 2.2* By Theorem 2.1
\[
\mathcal{E}(x) = \bigcup_{2 \leq \ell < c(K)} \mathcal{E}_\ell(x).
\]

By Lemmas 5.1 and 6.1
\[
\sum_{2 \leq \ell < c(g)} \frac{\#\mathcal{E}_\ell(x)}{\#\mathcal{C}(x)} \ll_K x \frac{1}{q^{x/2}}.
\]
Acknowledgments. The author thanks Doug Ulmer and Bryden Cais for their guidance and encouragement during this project, and also Nathan Jones for clarifying a remark in [Jon10].

References

[BLV09] A. Bandini, I. Longhi, and S. Vigni, *Torsion points on elliptic curves over function fields and a theorem of Igusa*, Expo. Math. 27 (2009), 175–209.
[CH05] A. C. Cojocaru and C. Hall, *Uniform results for Serre’s theorem for elliptic curves*, Int. Math. Res. Notices 2005, 3065–3080.
[Duk97] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. 325 (1997), 813–818.
[Hsu96] Ch.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996), 267–287.
[Hsu99] Ch.-N. Hsu, *The Brun–Titchmarsh theorem in function fields*, J. Number Theory 79 (1999), 67–82.
[Igu59] J. Igusa, *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. 81 (1959), 453–476.
[Igu68] J. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan 20 (1968), 96–106.
[Jon10] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. 362 (2010), 1547–1570.
[Kow06] E. Kowalski, *On the rank of quadratic twists of elliptic curves over function fields*, Int. J. Number Theory 2 (2006), 267–288.
[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.
[Zyw10] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. London Math. Soc. 42 (2010), 811–826.