PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 2, February 2017, Pages 577–584
http://dx.doi.org/10.1090/proc/13265
Article electronically published on October 24, 2016

BIRCH'S LEMMA OVER GLOBAL FUNCTION FIELDS

YI OUYANG AND SHENXING ZHANG

(Communicated by Romyar T. Sharifi)

Abstract. We obtain a function field version of Birch's Lemma, which reveals non-torsion points in quadratic twists of an elliptic curve over a global function field, where the quadratic twists have many prime factors. The proof uses Brown's Euler system of Heegner points over function fields and a result of Vigni on the ring class eigenspaces of Mordell-Weil groups in positive characteristic.

1. Introduction and main results

In this note, we shall give a function field version of Coates-Li-Tian-Zhai's generalization of Birch's Lemma.

1.1. **Birch's Lemma.** Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $f : X_0(N) \to E$ be a modular parametrization of E such that the cusp $[\infty] \in f^{-1}(O)$. Assume $f([0]) \notin 2E(\mathbb{Q})$. Assume $l > 3$ is a prime number such that $l \equiv 3 \bmod 4$ and every prime factor of N splits in $\mathbb{Q}(\sqrt{-l})$, i.e., the Heegner Hypothesis is satisfied for $(\mathbb{Q}(\sqrt{-l}), N)$. Birch showed that if $E^{(-l)}(\mathbb{Q})$ is the quadratic twist of E by $-l$, then the Mordell-Weil group $E^{(-l)}(\mathbb{Q})$ has rank 1.

Recently Birch's Lemma was generalized by Coates, Li, Tian and Zhai in [CLTZ, §2]. If there is a good supersingular prime q_1 for E such that $q_1 \equiv 1 \bmod 4$ and N is a square module q_1, they showed that for any fixed integer $k \geq 1$, there are infinitely many square free integers M with exactly k prime factors, such that the Mordell-Weil rank of the quadratic twist $E^{(M)}$ is 1. In particular, $E = X_0(14)$ with $q_1 = 5$ and $E = X_0(49)$ with $q_1 = 5$ are two examples satisfying the assumptions.

1.2. **Heegner points over function fields and Vigni's result.** Let $\mathcal{C}$ be a geometrically connected, smooth, projective algebraic curve over a finite field $\mathbb{F}$ of characteristic $p > 2$. Denote by $F := \mathbb{F}(\mathcal{C})$ the function field of $\mathcal{C}$. Let ∞ be a fixed closed point of $\mathcal{C}$ and denote by $\mathcal{O}_F$ the Dedekind domain of elements of F that are regular outside ∞. Let F_∞ be the completion of F at ∞ and let C be the completion of a fixed algebraic closure of F_∞.

Suppose E/F is a non-isotrivial (i.e., $j(E) \notin \overline{\mathbb{F}}$) elliptic curve defined over F. We assume that E has split multiplicative reduction at ∞. This assumption is not essential since we can replace F by a suitable finite separable extension and ∞ by another closed point. Then the conductor of E can be written as $\mathfrak{n}\infty$ with $\mathfrak{n}$ an ideal of $\mathcal{O}_F$. As explained in [GR], there is a non-constant morphism

$$f : X_0(\mathfrak{n}) \to E \tag{1}$$

Received by the editors December 16, 2015 and, in revised form, April 21, 2016 and April 30, 2016.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11D25, 11G40.

defined over F, where $X_0(\mathfrak{n})$ is the compactified Drinfel′d modular curve of level $\mathfrak{n}$. Fix a cusp P_0 defined over F; then we can translate the modular parametrization f to ensure that $f^{-1}(O)$ contains P_0.

Let $K = F(\sqrt{l})$ ($l \in \mathcal{O}_F$) be a quadratic extension of F, and $\mathcal{O}_K$ be the integral closure of $\mathcal{O}_F$ in K. Write $\mathrm{Gal}(K/F) = \{1, \tau\}$.

Assumption I. *The place ∞ is ramified in K and the class number h of $\mathcal{O}_K$ is odd.*

Note. Assumption I means that the class number of K and the degree of ∞ are both odd, and the constant field of K is still $\mathbb{F}$. By abuse of notation, we denote by ∞ the only place of K above ∞ and identify $\mathrm{Gal}(K_\infty/F_\infty) = \mathrm{Gal}(K/F)$.

Assumption II. *The pair $(K, \mathfrak{n})$ satisfies the* Heegner Hypothesis*, i.e., every prime dividing $\mathfrak{n}$ splits in K.*

Note. By Assumption II, $\mathfrak{n}\mathcal{O}_K = \mathfrak{N}\mathfrak{N}^\tau$ with $\mathfrak{N}$ an ideal of $\mathcal{O}_K$.

Fix a non-zero ideal $\mathfrak{M}$ of $\mathcal{O}_F$ which is prime to $\mathfrak{n}$. Then we can construct a Drinfel′d-Heegner point as follows. Let $\mathcal{O}_\mathfrak{M} = \mathcal{O}_F + \mathfrak{M}\mathcal{O}_K$ be the order of conductor $\mathfrak{M}$ in $\mathcal{O}_K$. The proper ideal $\mathfrak{N}_\mathfrak{M} = \mathfrak{N} \cap \mathcal{O}_\mathfrak{M}$ of $\mathcal{O}_\mathfrak{M}$ satisfies

$$\mathcal{O}_\mathfrak{M}/\mathfrak{N}_\mathfrak{M} \cong \mathcal{O}_K/\mathfrak{N} \cong \mathcal{O}_F/\mathfrak{n}.$$

Thus the two lattices $\mathcal{O}_\mathfrak{M}$ and $\mathfrak{N}_\mathfrak{M}^{-1}$ of C give a pair $(\Phi_\mathfrak{M}, \Phi'_\mathfrak{M})$ of Drinfel′d modules of rank 2 with a cyclic $\mathfrak{n}$-isogeny, hence define a point $P_\mathfrak{M}$ on $X_0(\mathfrak{n})$. Furthermore, $P_\mathfrak{M}$ is defined over the ring class field $H_\mathfrak{M}$ of conductor $\mathfrak{M}$ of K. As described in [B2, Chapter 2], this field is an abelian extension of K which is unramified outside $\mathfrak{M}$. Moreover, ∞ splits completely in $H_\mathfrak{M}$, thus we can embed $H_\mathfrak{M}$ into K_∞ and we regard $H_\mathfrak{M}$ as a subfield of K_∞ from now on.

Denote

$$x_\mathfrak{M} = f(P_\mathfrak{M}). \tag{2}$$

For a complex character χ of $G = \mathrm{Gal}(H_\mathfrak{M}/K)$, let

$$E(H_\mathfrak{M})^\chi_\mathbb{C} := \{x \in E(H_\mathfrak{M}) \otimes \mathbb{C} : x^\sigma = \chi(\sigma)x \text{ for all } \sigma \in G\} \tag{3}$$

be the χ-eigenspace of $E(H_\mathfrak{M}) \otimes \mathbb{C}$. Denote

$$\chi^{-1}\text{-}\mathrm{Tr}_{H_\mathfrak{M}/K} = \sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma. \tag{4}$$

Vigni in [V, Theorem 1.1] shows that

$$\chi^{-1}\text{-}\mathrm{Tr}_{H_\mathfrak{M}/K}(x_\mathfrak{M}) \neq 0 \text{ in } E(H_\mathfrak{M})^\chi_\mathbb{C} \Longrightarrow \dim_\mathbb{C} E(H_\mathfrak{M})^\chi_\mathbb{C} = 1. \tag{5}$$

For a quadratic extension $K(\sqrt{M})$ of K in $H_\mathfrak{M}$ with $M \in \mathcal{O}_F$, let χ_M be the associated quadratic character. Under certain assumptions, we will show that $\chi_M\text{-}\mathrm{Tr}(x_\mathfrak{M})$ is non-torsion for some M.

1.3. **Main results.** For a finite prime $\mathfrak{q}$ of $\mathcal{O}_F$, i.e., $\mathfrak{q} \neq \infty$, denote

$$a_\mathfrak{q} = \#\kappa(\mathfrak{q}) + 1 - \tilde{E}(\kappa(\mathfrak{q})),$$

where $\tilde{E}$ is the reduced curve of E and $\kappa(\mathfrak{q})$ is the residue field of $\mathcal{O}_F$ at $\mathfrak{q}$. Let $d_\mathfrak{q}$ be the order of the class of $\mathfrak{q}$ in the class group of $\mathcal{O}_F$. Let $q^* \in \mathcal{O}_F$ be a generator of $\mathfrak{q}^{d_\mathfrak{q}}$ such that q^* is a square in K_∞. This is reachable since ∞ is ramified in K/F and any generator of $\mathfrak{q}^{d_\mathfrak{q}}$ is of even valuation at ∞ in K_∞. Adjusting it by a

suitable root of unity we can make it a square in K_∞. Let $q = q^*$ or lq^* such that $\tau(\sqrt{q}) = \sqrt{q}$. Denote this by q_i for $\mathfrak{q} = \mathfrak{q}_i$.

Definition. A finite prime $\mathfrak{q}$ is called *sensitive* for E if it satisfies (i) $a_\mathfrak{q} = 0$, (ii) $\#\kappa(\mathfrak{q}) \equiv 1 \bmod 4$, and (iii) the Artin symbol $[\mathfrak{n}, F(\sqrt{q^*})/F] = 1$.

Assumption III. *The curve E possesses a sensitive prime $\mathfrak{q}_1$ of $\mathcal{O}_F$ inert in K.*

Definition. For each integer $k \geq 2$, Σ_k is the set of finite primes $\mathfrak{q} \neq \mathfrak{q}_1$ of $\mathcal{O}_F$ satisfying (i) $a_\mathfrak{q} \equiv 0 \bmod 2^k$, (ii) $\#\kappa(\mathfrak{q}) \equiv 1 \bmod 4$, (iii) $[\mathfrak{n}, F(\sqrt{\mathfrak{q}^*})/F] = 1$, (iv) $\mathfrak{q}$ is inert in K.

Let

$$d_\mathfrak{n} := \text{ the order of } \mathfrak{n} \text{ in } \mathrm{Pic}(\mathcal{O}_F) \tag{6}$$

and $n^\dagger$ be a generator of $\mathfrak{n}^{d_\mathfrak{n}}$ such that $(-1)^{\deg(\mathfrak{n})} n^\dagger$ is a square in K_∞. Then by Hasse's reciprocity law and the fact that the Hilbert symbol $(q^*, n^\dagger)_\infty = 1$,

$$[\mathfrak{q}, F(\sqrt{n^\dagger})/F] = [\mathfrak{n}, F(\sqrt{q^*})/F].$$

Note. We will see in Lemma 2.5 that Σ_k is infinite if Assumption III is satisfied.

The Atkin-Lehner operator $w_\mathfrak{n}$ acts on a pair $(D, Z) \in X_0(\mathfrak{n})$ of Drinfel'd modules as follows:

$$w_\mathfrak{n} = \prod_{\mathfrak{p}|\mathfrak{n}} w_\mathfrak{p}, \quad w_\mathfrak{p}(D, Z) = (D/Z_{\mathfrak{p}^k}, (D_{\mathfrak{p}^k} + Z)/Z_{\mathfrak{p}^k}), \tag{7}$$

where $\mathfrak{p}^k \| \mathfrak{n}$ and $D_{\mathfrak{p}^k}$ (resp. $Z_{\mathfrak{p}^k}$) is the subgroup scheme of D (resp. Z) annihilated by $\mathfrak{p}^k$. Let

$$w := w_\mathfrak{n}^{d_\mathfrak{n}}. \tag{8}$$

If we compose f with multiplication by a suitable odd integer, we may assume $f(P_0^w)$ is of order a power of 2.

Assumption IV. $f(P_0^w) \notin 2E(F)$.

Theorem A. *Assume Assumptions* I-IV. *For each integer $k \geq 0$, let $\mathfrak{q}_2, \ldots, \mathfrak{q}_k$ be distinct primes in the set Σ_k and $M = q_1 \cdots q_k$. Then $E(F(\sqrt{lM}))^-$, the $\tau = -1$ part of $E(F(\sqrt{lM}))$, is infinite. Moreover, $E^{(lM)}(F)$ has Mordell-Weil rank* 1 *and the BSD conjecture holds for $E^{(lM)}/F$.*

Theorem B. *Under Assumptions* I-IV, *if the degree of $\mathfrak{q}_1$ is even, then for each integer $k \geq 1$ there are infinitely many square-free M having exactly k prime factors, such that $E^{(lM)}(F)$ has Mordell-Weil rank* 1 *and the BSD conjecture holds for $E^{(lM)}/F$.*

2. Proofs of Theorems A and B

2.1. **Quadratic subfields.**

Lemma 2.1. *Let $\mathfrak{q}$ be a finite prime of $\mathcal{O}_F$ unramified in K.*

i) The order of $\mathfrak{q}$ in the ideal class group of $\mathcal{O}_F$ divides $h = h(\mathcal{O}_K)$.

ii) If the size of its residue field $\kappa(\mathfrak{q})$ is $\equiv 1 \bmod 4$, then $H_\mathfrak{q}$ contains a unique quadratic extension of K, which is $K(\sqrt{q})$.

Proof. i) Let a be a generator of $\mathfrak{q}^d$ where d is the order of $\mathfrak{q}$ in $\mathrm{Pic}(\mathcal{O}_F)$. We claim that d is odd. If not, $\mathfrak{q}^{d/2}\mathcal{O}_K$ is principal since h is odd by Assumption I. Let b be a generator of $\mathfrak{q}^{d/2}\mathcal{O}_K$; then $b^2 = a\varepsilon$ for some $\varepsilon \in \mathbb{F}^\times$, and $K = F(\sqrt{a\varepsilon})$. Since the degree of ∞ is odd, this implies that the valuation of $a\varepsilon$ at ∞ in $\mathcal{O}_F$ is even, which contradicts the fact that ∞ is ramified in K.

The order of $\mathfrak{q}\mathcal{O}_K$ in $\mathrm{Pic}(\mathcal{O}_K)$ divides the greatest common divisor (d, h), the ideal $(\mathfrak{q}\mathcal{O}_K)^{(d,h)}$ is principal and generated by some $c \in \mathcal{O}_K$. If $d \nmid h$, let $\alpha = d/(d, h)$; then $c \in a^{1/\alpha}\mathbb{F}^\times$. But $\alpha > 2$ is impossible! Hence $d \mid h$.

ii) By class field theory, there is a canonical isomorphism

$$\mathrm{Gal}(H_\mathfrak{q}/H_K) \cong \frac{(\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)^\times}{(\mathcal{O}_F/\mathfrak{q})^\times},$$

so $\mathrm{Gal}(H_\mathfrak{q}/H_K)$ has cardinality $\#\kappa(\mathfrak{q})+1$ (see [B2, (2.3.8)]). By Assumption I, the degree of the extension H_K/K is odd, thus $[H_\mathfrak{q} : K] \equiv 2 \bmod 4$ and there exists a unique quadratic sub-extension, denoted by $K(\sqrt{a'})$, of $H_\mathfrak{q}/K$.

We see that $\mathfrak{q}$ is the only prime ramified in $K(\sqrt{a})/K$ and $K(\sqrt{a'})/K$. Then a'/a has even valuations at every finite place, and $(a'/a)\mathcal{O}_K = I^2$ for a fractional ideal I of $\mathcal{O}_K$. Since h is odd, I must be principal, and $K(\sqrt{a'}) = K(\sqrt{\varepsilon a})$ with $\varepsilon \in \mathbb{F}^\times$. Hence we may assume $a' = \varepsilon a$.

Notice that ∞ is ramified and K_∞ and F_∞ have the same residue fields. Since a' is a square in K_∞, it follows that $K(\sqrt{a'}) = K(\sqrt{q})$. □

2.2. **Heegner points and the Atkin-Lehner operator.** Let Λ, Λ' be two $\mathcal{O}_F$-lattices of rank 2 in C with $\Lambda'/\Lambda \cong \mathcal{O}_F/\mathfrak{n}$. They define a pair of Drinfel′d modules with an $\mathfrak{n}$-isogeny, thus a point on $X_0(\mathfrak{n})$, which we denote by $P(\Lambda, \Lambda')$.

For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_\mathfrak{M}$, the Galois group acts on the set of the Heegner points by

$$P(\mathfrak{a}, \mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1})^{[\alpha, H_\mathfrak{M}/K]} = P(\mathfrak{a}\alpha^{-1}, \mathfrak{a}\alpha^{-1}\mathfrak{N}_\mathfrak{M}^{-1}), \tag{9}$$

where α is a non-zero fractional ideal prime to $l\mathfrak{M}$ and $[-, H_\mathfrak{M}/K]$ is the Artin symbol; see [B2, §4.5]. The Atkin-Lehner operator $w_\mathfrak{n}$ acts on the Heegner points by

$$w_\mathfrak{n} P(\mathfrak{a}, \mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1}) = P(\mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1}, \mathfrak{a}\mathfrak{n}^{-1}). \tag{10}$$

Let w be as in (8). By Lemma 2.1, the order $d_\mathfrak{n}$ of $\mathfrak{n}$ in the ideal class group of F is odd, thus

$$wP(\mathfrak{a}, \mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1}) = P(\mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1}\mathfrak{n}^{-\frac{d_\mathfrak{n}-1}{2}}, \mathfrak{a}\mathfrak{n}^{-\frac{d_\mathfrak{n}+1}{2}}). \tag{11}$$

Let

$$P_\mathfrak{M} := P(\mathcal{O}_\mathfrak{M}, \mathfrak{N}_\mathfrak{M}^{-1}),$$

then (see [B2, 4.6.17])

$$\tau P_\mathfrak{M}^{[\mathfrak{N}^\tau \mathfrak{n}^{\frac{d_\mathfrak{n}-1}{2}}, H_\mathfrak{M}/K]} = w_\mathfrak{n}(P_\mathfrak{M}). \tag{12}$$

Let $H_0 = K(\sqrt{q_1}, \ldots, \sqrt{q_k})$. This is a subfield of $H_\mathfrak{M}$ and $[H_\mathfrak{M} : H_0]$ is odd.

Lemma 2.2. *Let S be the orbit of $P_\mathfrak{M}$ under the action of $\mathrm{Gal}(H_\mathfrak{M}/H_0)$. Then $wS = \tau S$ set-theoretically.*

Proof. This is because the restriction of $[\mathfrak{N}^\tau \mathfrak{n}^{\frac{d_\mathfrak{n}-1}{2}}, H_\mathfrak{M}/K]$ to $F(\sqrt{q_i})$ is

$$[\mathfrak{n}, F(\sqrt{q_i})/F]^{d_\mathfrak{n}} = [\mathfrak{n}, F(\sqrt{q_i^*})/F]^{d_\mathfrak{n}} = 1.$$ □

Lemma 2.3. *The operator w has a fixed point on $X_0(\mathfrak{n})$.*

Proof. Since the degree of ∞ in F is odd, we may choose $c \in C - F_\infty$ such that c^2 generates $\mathfrak{n}^{d_\mathfrak{n}}$. Note that $d_\mathfrak{n}$ is odd by Lemma 2.1, and write $d_\mathfrak{n} = 2t+1$. Let $\Lambda = \mathfrak{n} + \mathfrak{n}^{-t}c^{-1}$ and $\Lambda' = \mathcal{O}_F + \mathfrak{n}^{-t}c^{-1}$ be two lattices in C; then $\Lambda'/\Lambda \cong \mathcal{O}_F/\mathfrak{n}$ and

$$\begin{aligned} wP(\Lambda,\Lambda') &= P(\mathfrak{n}^{-t}\Lambda', \mathfrak{n}^{-t-1}\Lambda) \\ &= P(\mathfrak{n}^{-t} + \mathfrak{n}^{-2t}c^{-1}, \mathfrak{n}^{-t} + \mathcal{O}_F c) \\ &= P(\mathfrak{n}^{-t}c^{-1} + \mathfrak{n}^{-2t}c^{-2}, \mathfrak{n}^{-t}c^{-1} + \mathcal{O}_F) \\ &= P(\Lambda,\Lambda') \in X_0(\mathfrak{n}). \end{aligned}$$

That is to say, $P(\Lambda,\Lambda')$ is a fixed point of w. □

Lemma 2.4. *The morphism $f + f \circ w : X_0(\mathfrak{n}) \to E$ is constant.*

Proof. We can write f as the composite of

$$X_0(\mathfrak{n}) \to J_0(\mathfrak{n}) = \mathrm{Jac}(X_0(\mathfrak{n})) \xrightarrow{g} A = J_0(\mathfrak{n})/(T_\mathfrak{p} - a_\mathfrak{p}; \mathfrak{p} \nmid \mathfrak{n}) \xrightarrow{h} E.$$

Here $T_\mathfrak{p}$ is the $\mathfrak{p}$-th Hecke operator and h is an isogeny. Let $f_A : P \mapsto g([P] - [P_0])$ be the composite of the first two maps.

By definition, w is a linear involution on $J_0(\mathfrak{n})$ as

$$w([P] - [P_0]) = [P^w] - [P_0^w].$$

It induces a linear involution $w = \pm 1$ on A since $w \circ T_n = T_n \circ w$.

If $w = +1$, then

$$\begin{aligned} &(f_A - f_A \circ w)(P) = w(f_A - f_A \circ w)(P) \\ =&w \circ g(([P] - [P_0]) - ([P^w] - [P_0])) = w \circ g([P] - [P^w]) \\ =&g([P^w] - [P]) = (f_A \circ w - f_A)(P). \end{aligned}$$

The image of $f_A - f_A \circ w$ lies in $A[2]$, which is finite. Thus $f_A - f_A \circ w$ is a constant. Let Q be a fixed point of w; then

$$f_A(P_0^w) = f_A(P_0^w) - f_A(P_0) = f_A(Q^w) - f_A(Q) = O$$

and $f(P_0^w) = O$, which contradicts Assumption IV. Hence $w = -1$.

On one hand,

$$2g([P] + [P^w] - [P_0] - [P_0^w]) = f_A(P) + f_A(P^w) + wf_A(P) + wf_A(P^w) = 0.$$

On the other hand,

$$\begin{aligned} &g([P] + [P^w] - [P_0] - [P_0^w]) \\ =&(f_A + f_A \circ w)(P) - g([P_0^w] - [P_0]) \\ =&(f_A + f_A \circ w)(P) - f_A(P_0^w). \end{aligned}$$

The image of $f_A + f_A \circ w$ lies in $f_A(P_0^w) + A[2]$, which is finite. Thus $f_A + f_A \circ w$ is constant, and so is $f + f \circ w = f(P_0^w)$. □

Lemma 2.5. *Assume E possesses a sensitive prime $\mathfrak{q}_1$ of $\mathcal{O}_F$ inert in K. Then for each integer $k \geq 2$, Σ_k is infinite of positive density in the set of primes.*

Proof. Set $J = F(\sqrt{n^\dagger}, E[2^k])$; then $K \cap J = F$ and $\mathfrak{q}_1$ is unramified in J. There is a unique element σ in $\Delta = \mathrm{Gal}(JK/F)$ whose restriction to K is τ and whose restriction to J is the Frobenius automorphism of some prime of J above $\mathfrak{q}_1$.

Assume $\mathfrak{q}$ is a finite prime not dividing $l\mathfrak{q}_1\mathfrak{n}$, whose Frobenius automorphisms in Δ lie in the conjugate class of σ. The characteristic polynomials of the Frobenius automorphisms of $\mathfrak{q}_1$ and $\mathfrak{q}$ acting on the 2-adic Tate module $T_2(E)$ are $X^2+\#\kappa(\mathfrak{q}_1)$ and $X^2 + a_q X + \#\kappa(\mathfrak{q})$, respectively. Since $E[2^k] = T_2(E)/2^kT_2(E)$, we have $a_\mathfrak{q} \equiv 0 \bmod 2^k$ and $\#\kappa(\mathfrak{q}) \equiv \#\kappa(\mathfrak{q}_1) \bmod 2^k$. Also $\mathfrak{q}$ is inert in K since $\mathfrak{q}_1$ is inert in K, and $\mathfrak{q}$ splits in $F(\sqrt{n^\dagger})$ since $\mathfrak{q}_1$ splits in this field. Hence Σ_k contains all such primes and it follows that Σ_k is infinite of positive density in the set of all primes by the Chebotarev density theorem. □

Lemma 2.6. *We have* $E(H_0)[2^\infty] = E(F)[2]$.

Proof. Since in every subfield of H_0 which is strictly larger than F, at least one prime dividing $l\mathfrak{q}_1 \cdots \mathfrak{q}_k$ ramifies, but only the primes dividing $2\mathfrak{n}\infty$ may ramify in the field $F(E[2^\infty])$, we have

$$E(H_0)[2^\infty] = E(F)[2^\infty] = E(F)[2]. \tag{13}$$

Note that $\mathfrak{q}_1$ is a sensitive prime for E, reduction modulo $\mathfrak{q}_1$ is injective on $E(F)[2^\infty]$, and there are $\#\kappa(\mathfrak{q}_1)+1$ points with coordinates in $\kappa(\mathfrak{q}_1)$ on the reduced curve $\tilde{E}$. It follows that $E(F)[2^\infty]$ has order at most 2. □

2.3. **Euler system.** For a factor $\mathfrak{d}$ of $\mathfrak{M}$, let $d = \prod_{\mathfrak{q}_i \mid \mathfrak{d}} q_i$. The following result ensures that Heegner points form an Euler system, as in the classical case (see [B2, (4.6.8), (4.8.3)]):

Proposition 2.7. *For* $\mathfrak{q} \mid \frac{\mathfrak{M}}{\mathfrak{d}}$, *we have* $\mathrm{Tr}_{H_{\mathfrak{q}\mathfrak{d}}/H_\mathfrak{d}} x_{\mathfrak{q}\mathfrak{d}} = a_\mathfrak{q} x_\mathfrak{d}$.

Let $\psi_M = \mathrm{Tr}_{H_\mathfrak{M}/H_0}(x_\mathfrak{M})$. Define $K(\sqrt{d})$-points y_d, z_d of E by

$$z_d := \chi_d\text{-}\mathrm{Tr}_{H_\mathfrak{M}/K}(x_\mathfrak{M}) = \chi_d\text{-}\mathrm{Tr}_{H_0/K}(\psi_M), \tag{14}$$

$$y_d := \chi_d\text{-}\mathrm{Tr}_{H_\mathfrak{d}/K}(x_\mathfrak{d}). \tag{15}$$

Then $z_M = y_M$ and $z_d = b_d y_d$ where $b_d = \prod_{\mathfrak{q} \mid \frac{\mathfrak{M}}{\mathfrak{d}}} a_\mathfrak{q} = 2^k e_d$ for $\mathfrak{d} \neq \mathfrak{M}$.

2.4. **End of proof.**

Proof of Theorem A. If $k = 0$, $y_1 = \mathrm{Tr}_{H_K/K}(x_1)$, $y_1 + \tau(y_1) = h(\mathcal{O}_K)f(P_0^w) = f(P_0^w)$. If y_1 is torsion, then there is an odd number m such that $my_1 \in E(K)[2^\infty] = E(F)[2]$. It follows that $f(P_0^w) = m(y_1 + \tau(y_1)) = 2my_1$, which contradicts Assumption IV. Hence y_1 is non-torsion, and so is $2y_1 \in E(K)^-$.

Now assume $k \geq 1$. Let $\sigma \in \mathrm{Gal}(H_0/K)$ which maps $\sqrt{q_1}$ to $-\sqrt{q_1}$ and fixes all other $\sqrt{q_i}$ for $i > 1$. Then

$$\sigma(\psi_M) + \psi_M = \mathrm{Tr}_{H_\mathfrak{M}/K(\sqrt{q_i}, i>1)}(x_\mathfrak{M}) = a_{\mathfrak{q}_1}\, \mathrm{Tr}_{H_{\frac{\mathfrak{M}}{\mathfrak{q}_1}}/K(\sqrt{q_i}, i>1)}(x_{\frac{\mathfrak{M}}{\mathfrak{q}_1}}) = 0.$$

Since $a_{\mathfrak{q}_1} = 0$,

$$\sigma(v_M) + v_M = \mathrm{Tr}_{H_\mathfrak{M}/K}(x_\mathfrak{M}) = a_{\mathfrak{q}_1}\, \mathrm{Tr}_{H_{\frac{\mathfrak{M}}{\mathfrak{q}_1}}/K}(x_{\frac{\mathfrak{M}}{\mathfrak{q}_1}}) = 0,$$

where

$$v_M = \mathrm{Tr}_{H_\mathfrak{M}/K(\sqrt{M})}(x_\mathfrak{M}) = \mathrm{Tr}_{H_0/K(\sqrt{M})}(\psi_\mathfrak{M}).$$

Then $y_M = v_M - \sigma(v_M) = 2v_M$, $\sigma(y_M) + y_M = 0$.

By Lemma 2.2 and Lemma 2.4, we have

$$\psi_M + \tau(\psi_M) = [H_{\mathfrak{M}} : H_0] f(P_0^w) = f(P_0^w).$$

Thus $y_M + \tau(y_M) = 2(v_M + \tau(v_M)) = 0$. Hence $y_M \in E(F(\sqrt{lM}))^-$. Similarly, we have $y_d + \tau(y_d) = 0$ if $\mathfrak{q}_1 \mid \mathfrak{d}$.

By the definition of y_d, we have

$$y_M + \sum_{\mathfrak{d}|\mathfrak{M}, \mathfrak{d}\neq\mathfrak{M}} z_d = 2^k \psi_M.$$

Let

$$u_M = \psi_M - \sum_{\mathfrak{d}|\mathfrak{M}, \mathfrak{d}\neq\mathfrak{M}} e_d y_d;$$

then $y_M = 2^k u_M$. Since $e_d = 0$ if $\mathfrak{q}_1 \nmid \mathfrak{d}$, it follows that $u_M + \tau(u_M) = f(P_0^w)$. If u_M is torsion, then there is an odd number m such that $mu_M \in E(H_0)[2^\infty] = E(F)[2]$. It follows that $f(P_0^w) = m(u_M + \tau(u_M)) = 2mu_M$, which contradicts Assumption IV. Hence u_M is non-torsion, and so is y_M.

The rest of the proof is similar to [V, Theorem 7.1]. By [V, Theorem 6.1], we can take a suitable rational prime t such that the $\mathbb{F}_t$-vector space $\mathrm{Sel}_t(E/H_{\mathfrak{M}})^{\chi_M}$ is one-dimensional and $E[t](H_{\mathfrak{M}}) = 0$. Since the Selmer groups can be controlled via the injections

$$\mathrm{Sel}_t(E/F(\sqrt{lM}))^{\chi_M} \hookrightarrow \mathrm{Sel}_t(E/K(\sqrt{M}))^{\chi_M} \hookrightarrow \mathrm{Sel}_t(E/H_{\mathfrak{M}})^{\chi_M},$$

they must be all one-dimensional $\mathbb{F}_t$-vector spaces.

We know that $E^{(lM)}(F) \cong E(F(\sqrt{lM}))^-$. By injectivity of the restriction map, $\dim_{\mathbb{F}_t} \mathrm{Sel}_t(E^{(lM)}/F) = 1$ and $Ш(E^{(lM)}/F)[t] = 0$. By the result of Tate, Milne, Kato and Trihan ([V, Theorem 7.2]), the conjecture of BSD holds for $E^{(lM)}/F$. □

Proof of Theorem B. If the degree of $\mathfrak{q}_1$ is even, the 2-adic valuation of $\#\kappa(\mathfrak{q}_1)$ is $r \geq 2$; then the 2-adic valuation of $\#\mathbb{F} - 1$ is less than r. Take $\mathfrak{q}_2, \ldots, \mathfrak{q}_k$ in Σ_{k+r}. We have $\#\kappa(\mathfrak{q}) \equiv \#\kappa(\mathfrak{q}_1) \bmod 2^r$ as in Lemma 2.5. Thus the degree of $\mathfrak{q}_i$ is even and then $q_i = q_i^*$. Therefore, M has exactly k prime factors and the result follows from Lemma 2.5. □

Acknowledgements

The authors would like to thank Professor Ye Tian for his vision and help. The authors would also like to thank Yu Liu, Jie Shu and Jinbang Yang for many helpful discussions. The second author would like to thank Professor Xinyi Yuan for helpful discussions and generous hospitality. This research was partially supported by National Key Basic Research Program of China (Grant No. 2013CB834202) and National Natural Science Foundation of China (Grant No. 11171317 and 11571328).

References

[B1] M. L. Brown, *On a conjecture of Tate for elliptic surfaces over finite fields*, Proc. London Math. Soc. (3) **69** (1994), no. 3, 489–514, DOI 10.1112/plms/s3-69.3.489. MR1289861

[B2] M. L. Brown, *Heegner modules and elliptic curves*, Lecture Notes in Mathematics, vol. 1849, Springer-Verlag, Berlin, 2004. MR2082815

[CLTZ] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 2, 357–394, DOI 10.1112/plms/pdu059. MR3335282

[G] Ernst-Ulrich Gekeler, *Drinfel′d modular curves*, Lecture Notes in Mathematics, vol. 1231, Springer-Verlag, Berlin, 1986. MR874338

[GR] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93, DOI 10.1515/crll.1996.476.27. MR1401696

[H] David R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York-London, 1979, pp. 173–217. MR535766

[P] Mihran Papikian, *On the degree of modular parametrizations over function fields*, J. Number Theory **97** (2002), no. 2, 317–349, DOI 10.1016/S0022-314X(02)00016-1. MR1942964

[S] Andreas Schweizer, *Hyperelliptic Drinfeld modular curves*, Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), World Sci. Publ., River Edge, NJ, 1997, pp. 330–343. MR1630612

[T] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. MR1610977

[U] Douglas Ulmer, *Elliptic curves and analogies between number fields and function fields*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 285–315, DOI 10.1017/CBO9780511756375.011. MR2083216

[V] Stefano Vigni, *On ring class eigenspaces of Mordell-Weil groups of elliptic curves over global function fields*, J. Number Theory **128** (2008), no. 7, 2159–2184, DOI 10.1016/j.jnt.2007.11.007. MR2423756

[WY] Fu-Tsun Wei and Jing Yu, *On the independence of Heegner points in the function field case*, J. Number Theory **130** (2010), no. 11, 2542–2560, DOI 10.1016/j.jnt.2010.05.006. MR2678861

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China

E-mail address: yiouyang@ustc.edu.cn

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China – and – Morningside Center of Mathematics, Chinese Academy of Sciences, Beijing 100190, People's Republic of China

E-mail address: zsxqq@mail.ustc.edu.cn