

Heegner Points and Elliptic Curves of Large Rank over Function Fields

HENRI DARMON

ABSTRACT. This note presents a connection between Ulmer’s construction [Ulm02] of non-isotrivial elliptic curves over $\mathbb{F}_p(t)$ with arbitrarily large rank, and the theory of Heegner points (attached to parametrisations by Drinfeld modular curves, as sketched in Section 3 of Ulmer’s article (see page ??). This ties in the topics in Section 4 of that article more closely to the main theme of this volume.

A review of the number field setting. Let K be a quadratic imaginary extension of $F = \mathbb{Q}$, and let E/\mathbb{Q} be an elliptic curve of conductor N . When all the prime divisors of N are split in K/F , the Heegner point construction (in the most classical form that is considered in [GZ], relying on the modular parametrisation $X_0(N) \rightarrow E$) produces not only a canonical point on $E(K)$, but also a norm-coherent system of such points over all abelian extensions of K which are of “dihedral type”. (An abelian extension H of K is said to be of *dihedral type* if it is Galois over \mathbb{Q} and the generator of $\text{Gal}(K/\mathbb{Q})$ acts by -1 on the abelian normal subgroup $\text{Gal}(H/K)$.) The existence of this construction is consistent with the Birch and Swinnerton-Dyer conjecture, in the following sense: an analysis of the sign in the functional equation for $L(E/K, \chi, s) = L(E/K, \bar{\chi}, s)$ shows that this sign is always equal to -1 , for all complex characters χ of $G := \text{Gal}(H/K)$. Hence

$$L(E/K, \chi, 1) = 0 \quad \text{for all } \chi : G \rightarrow \mathbb{C}^\times.$$

The product factorisation

$$L(E/H, s) = \prod_{\chi} L(E/K, \chi, s)$$

implies that

$$\text{ord}_{s=1} L(E/H, s) \geq [H : K], \tag{1}$$

so that the Birch and Swinnerton-Dyer conjecture predicts that

$$\text{rank}(E(H)) \stackrel{?}{\geq} [H : K]. \quad (2)$$

In fact, the G -equivariant refinement of the Birch and Swinnerton-Dyer conjecture leads one to expect that the rational vector space $E(H) \otimes \mathbb{Q}$ contains a copy of the regular representation of G .

It is expected in this situation that Heegner points account for the bulk of the growth of $E(H)$, as H varies over the abelian extensions of K of dihedral type. For example we have:

LEMMA 1. *If $\text{ord}_{s=1} L(E/H, s) \leq [H : K]$, then the vector space $E(H) \otimes \mathbb{Q}$ has dimension $[H : K]$ and is generated by Heegner points.*

PROOF. For V any complex representation of G , let

$$V^\chi := \{v \in V \text{ such that } \sigma v = \chi(\sigma)v, \text{ for all } \sigma \in G\}.$$

Since equality is attained in (1), it follows that each $L(E/K, \chi, s)$ vanishes to order exactly one at $s = 1$. Zhang's extension of the Gross-Zagier formula to L -functions $L(E/K, s)$ twisted by (possibly ramified) characters of G [Zh01] shows that

$$\dim_{\mathbb{C}}(HP^\chi) = 1, \quad (3)$$

where HP denotes the subspace of $E(H) \otimes \mathbb{C}$ generated by Heegner points. Theorem 2.2 of [BD90], whose proof is based on Kolyvagin's method, then shows that

$$\dim_{\mathbb{C}}((E(H) \otimes \mathbb{C})^\chi) \leq 1. \quad (4)$$

The result follows directly from (3) and (4). \square

0.1. The case $F = \mathbb{F}_q(u)$. As explained in Section 3 of [Ulm03], the Heegner point construction can be adapted to the case where \mathbb{Q} is replaced by the rational function field $\mathbb{F}_q(u)$.

The basic idea of our construction is to start with an elliptic curve E_0 defined over $\mathbb{F}_p(u)$, and produce a Galois extension H of $\mathbb{F}_q(u)$ (for some power q of p) such that

- (i) the Galois group of H over $\mathbb{F}_q(u)$ is isomorphic to a dihedral group of order $2d$;
- (ii) H satisfies a suitable Heegner hypothesis relative to E_0 over $\mathbb{F}_q(u)$ so that the Birch and Swinnerton-Dyer conjecture implies an inequality like (2);
- (iii) H is the function field of a curve of genus 0, say $H = \mathbb{F}_q(t)$, so that E_0 yields a curve E over $\mathbb{F}_p(t)$ which acquires rank at least d over $\mathbb{F}_q(t)$.

A further argument is then made to show that the rank of E remains large over $\mathbb{F}_p(t)$, provided suitable choices of d and q have been made.

To illustrate the method, let p be an odd prime and let F_0 be the field $\mathbb{F}_p(u)$, with u an indeterminate. Let $K_0 = \mathbb{F}_p(v)$ be the quadratic extension of F_0

defined by $v + v^{-1} = u$. Choose an element $u_\infty \in \mathbb{P}_1(\mathbb{F}_p)$ such that the place $(u - u_\infty)$ is inert in K_0 . (Such a u_∞ always exists when $p > 2$.) The chosen place u_∞ will play the role in our setting of the archimedean place of \mathbb{Q} in the previous discussion. Note that K_0/F_0 becomes a quadratic “imaginary” extension with this choice of place at infinity, and that this continues to hold when \mathbb{F}_p is replaced by \mathbb{F}_q with $q = p^m$, provided that m is odd.

Let $E = E_u$ be an elliptic curve over F_0 having split multiplicative reduction at u_∞ . Let \mathcal{E} denote the Néron model of E over the subring $\mathcal{O} = \mathbb{F}_p[\frac{1}{u-u_\infty}]$ and let N denote its arithmetic conductor, viewed as a divisor of $\mathbb{P}_1 - \{u_\infty\}$. Suppose that

$$\text{all prime divisors of } N \text{ are split in } K_0/F_0, \tag{5}$$

which is the analogue of the classical Heegner hypothesis in our function field setting.

Finally, given any integer d , let o_d be the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$. Assume that

$$\text{the integer } o_d \text{ is odd.} \tag{6}$$

We then set $q = p^{o_d}$ and consider the extensions

$$F = \mathbb{F}_q(u); \quad K = \mathbb{F}_q(v); \quad H = \mathbb{F}_q(t), \text{ with } v = t^d.$$

Note that H/K is an abelian extension with Galois group $G = \text{Gal}(H/K)$ isomorphic to $\mu_d(\mathbb{F}_q) \simeq \mathbb{Z}/d\mathbb{Z}$, and that this extension is of dihedral type, relative to the ground field F . Therefore the analysis of signs in functional equations that was carried out to conclude (1) carries over, mutatis mutandis, to prove the following.

PROPOSITION 2. *Assume the Birch and Swinnerton-Dyer conjecture over function fields. Then the rank of $E(H)$ is at least d . More precisely,*

$$\dim_{\mathbb{C}} ((E(H) \otimes \mathbb{C})^\chi) \geq 1, \quad \text{for all } \chi : G \longrightarrow \mathbb{C}^\times.$$

One also wants to estimate the rank of E over the field $H_0 := \mathbb{F}_p(t)$. Let $\tilde{G} = \text{Gal}(H/K_0)$; then \tilde{G} is the semi-direct product $G \times \langle f \rangle$, where $\langle f \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ is the cyclic group of order o_d generated by the Frobenius element $f \in \text{Gal}(H/H_0) = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, which acts by conjugation on the abelian normal subgroup $G = \mu_d(\mathbb{F}_q)$ in the natural way. Since E is defined over K_0 (and even over F_0), the space $V := E(H) \otimes \mathbb{C}$ is a complex representation of \tilde{G} , and one may exploit basic facts about the irreducible representations of such a semi-direct product to obtain lower bounds for $E(H)^{f=1} = E(\mathbb{F}_p(t))$. More precisely, suppose that the character χ of G is one of the $\phi(d)$ faithful characters of G . Proposition 2 asserts that the space V^χ contains a non-zero vector v_χ . Note that V^χ is not preserved by the action of f , which sends V^χ to V^{χ^p} . Because of this, the vectors $v_\chi, f v_\chi, \dots, f^{o_d-1} v_\chi$ are linearly independent since they belong to different eigenspaces for the action of G . Hence the vector

$$v_{[\chi]} = v_\chi + f v_\chi + \dots + f^{o_d-1} v_\chi$$

is non-zero and belongs to $V^{f=1} = E(H_0) \otimes \mathbb{C}$. Furthermore the $v_{[\chi]}$ are linearly independent, as χ ranges over the f -orbits of faithful characters of G . Hence

$$\text{rank}(E(\mathbb{F}_p(t))) \geq \phi(d)/o_d.$$

By taking into account the contributions coming from all the characters (and not just the faithful ones) one can obtain the following stronger estimate.

PROPOSITION 3. *Assume the Birch and Swinnerton-Dyer conjecture over function fields. Then*

$$\text{rank}(E(\mathbb{F}_p(t))) \geq \sum_{e|d} \frac{\phi(e)}{o_e} \geq \frac{d}{o_d}. \quad (7)$$

PROOF. A complex character χ of G is said to be of level e if its image is contained in the group μ_e of e th roots of unity in \mathbb{C} and in no smaller subgroup. Clearly the level e of χ is a divisor of d , the order o_e of p in $(\mathbb{Z}/e\mathbb{Z})^\times$ divides o_d , and there are exactly $\phi(e)$ distinct characters of G of level e . Note also that if χ is of level e , then f^{o_e} maps V^χ to itself. The same reasoning used to prove Proposition 2, but with d replaced by e , and q by p^{o_e} , shows that (under the Birch and Swinnerton-Dyer assumption)

$$V^\chi \quad \text{contains a non-zero vector fixed by } f^{o_e}.$$

If v_χ is such a vector, then just as before the vectors

$$v_{[\chi]} = v_\chi + f v_\chi + \cdots + f^{o_e-1} v_\chi$$

form a linearly independent collection of $\phi(e)/o_e$ vectors in $E(\mathbb{F}_p(t)) \otimes \mathbb{C}$, as χ ranges over the f -orbits of characters of G of level e . Summing over all e dividing d proves the first inequality in (7). The second is obtained by noting that

$$\sum_{e|d} \frac{\phi(e)}{o_e} \geq \frac{1}{o_d} \sum_{e|d} \phi(e) = \frac{d}{o_d}. \quad \square$$

REMARKS. 1. It is instructive to compare the bound (7) with the formula for the rank of Ulmer's elliptic curves which is given in Theorem 4.2.1 of [Ulm03].
2. Note that the expression which appears on the right of (7) can be made arbitrarily large by setting $d = p^n - 1$ with n odd, so that $o_d = n$.

Some examples. Elliptic curves satisfying the Heegner assumptions of the previous section are not hard to exhibit explicitly. For example, suppose for notational convenience that p is congruent to 3 modulo 4, and let $E[u]$ be a non-isotrivial elliptic curve over $\mathbb{F}_p(u)$ having good reduction everywhere except at $u = 0, 1$ and ∞ , and having split multiplicative reduction at $u_\infty = 0$. There are a number of such curves, for example:

- (i) An (appropriate twist of a) "universal" elliptic curve over the j -line in characteristic $p \neq 2, 3$, with $u = 1728/j$;
- (ii) A "universal" curve over $X_0(2)$, or over $X_0(3)$;

- (iii) The Legendre family $y^2 = x(x - 1)(x - u)$ (corresponding to a universal family over the modular curve $X(2)$).
- (iv) The curve $y^2 + xy = x^3 - u$ that is used in [Ulm03], in which the parameter space has no interpretation as a modular curve.

Choosing any parameter λ in $\mathbb{F}_p - \{0, \pm 1\}$, we see that the curve $E\left[\frac{u}{\lambda + \lambda^{-1}}\right]$ over $\mathbb{F}_p(u)$ satisfies all the desired properties, since two of the places $u = \infty$ and $\lambda + \lambda^{-1}$ dividing the conductor of E are split in K/F , while the third place $u = 0$, which lies below $v = \pm i$, is inert in K/F . (This is where the assumption $p \equiv 3 \pmod{4}$ is used.) Hence Proposition 3 implies

COROLLARY 4. *Assume the Birch and Swinnerton-Dyer conjecture for function fields. Let $E[u]$ be any of the curves over $\mathbb{F}_p(u)$ listed above, and let λ be any element in $\mathbb{F}_p - \{0, \pm 1\}$. Then the curve*

$$E\left[\frac{t^d + t^{-d}}{\lambda + \lambda^{-1}}\right]$$

has rank at least d/o_d over $\mathbb{F}_p(t)$.

Dispensing with the Birch and Swinnerton-Dyer hypothesis. It may be possible, at least for some specific choices of $E[u]$ and of d , to remove the Birch and Swinnerton-Dyer assumption that appears in corollary 4, since the notion of Heegner points which motivated Proposition 2 also suggests a possible construction of a (hopefully, sufficiently large) collection of global points in $E(H)$. To produce explicit examples where the module HP generated by Heegner points in $E(H)$ has large rank, it may not be necessary to invoke the full strength of the theory described in Section 3 of [Ulm03] since quite often the mere knowledge that the Heegner point on $E(K)$ is of infinite order is sufficient to gain strong control over the Heegner points that appear in related towers. It appears worthwhile to produce explicit examples where Propositions 2 and 3 can be made unconditional thanks to the Heegner point construction.

REMARK. Crucial to the construction in this note is the fact that \mathbb{P}_1 has a large automorphism group, containing dihedral groups of arbitrarily large order. Needless to say, this fact breaks down when $\mathbb{F}_p(u)$ is replaced by \mathbb{Q} , which has no automorphisms. In this setting Heegner points are known to be a purely “rank one phenomenon”, and are unlikely to yield any insight into the question of whether the rank of elliptic curves over \mathbb{Q} is unbounded or not.

Remarks on Ulmer’s construction. Let d be a divisor of $q + 1$, where $q = p^n$. The curve

$$E_d : y^2 + xy = x^3 - t^d$$

studied in Theorem 4.2.1 of [Ulm03] is a pullback of the curve

$$E_0 : y^2 + xy = x^3 - u$$

by the covering $\mathbb{P}_1 \rightarrow \mathbb{P}_1$ given by $t \mapsto u := t^d$, a covering that becomes Galois (abelian) over \mathbb{F}_{q^2} . It is not hard on the other hand to see that the curve E_d does not arise as a pullback via any geometrically connected dihedral covering $\mathbb{P}_1 \rightarrow \mathbb{P}_1$. However, one may set

$$F = \mathbb{F}_q(u), \quad K = \mathbb{F}_{q^2}(u), \quad H = \mathbb{F}_{q^2}(t), \quad \text{with } u = t^d.$$

The congruence $q \equiv -1 \pmod{d}$ implies that $\text{Gal}(H/F)$ is a dihedral group of order $2d$. Hence it becomes apparent a posteriori that the curves of [Ulm02] can be approached by a calculation of the signs in functional equations for the L -series of E_0 over K twisted by characters of $\text{Gal}(H/K)$. (See the remarks in sec. 4.3 of [Ulm03] for further details on this calculation and its close connection with the original strategy followed in [Ulm02].)

It should be noted that the elliptic curves produced in our Corollary 4 have smaller rank-to-conductor ratios than the curves E_d in Theorem 4.2.1 of [Ulm03], which are essentially optimal in this respect.

References

- [BD90] Massimo Bertolini and Henri Darmon, “Kolyvagin’s descent and Mordell–Weil groups over ring class fields”, *J. Reine Angew. Math.* **412** (1990), 63–74.
- [GZ] Benedict Gross and Don Zagier, “Heegner points and derivatives of L -series”, *Invent. Math.* **84:2** (1986), 225–320.
- [Ulm02] Douglas Ulmer, “Elliptic curves with large rank over function fields”, *Ann. of Math.* (2) **155:1** (2002), 295–315.
- [Ulm03] Douglas Ulmer, “Elliptic curves and analogies between number fields and function fields”, pp. 285–315 in *Heegner Points and Rankin L -Series*, edited by Henri Darmon and Shou-Wu Zhang, *Math. Sci. Res. Inst. Publications* **49**, Cambridge U. Press, New York, 2004.
- [Zh01] Shou-Wu Zhang, “Gross–Zagier formula for GL_2 ”, *Asian J. Math.* **5:2** (2001), 183–290.

HENRI DARMON
 MATHEMATICS AND STATISTICS DEPARTMENT
 MCGILL UNIVERSITY
 805 SHERBROOKE W.
 MONTREAL, QUEBEC
 CANADA H3A 2K6
 darmon@math.mcgill.ca