Jan Nekovář & Norbert Schappacher

On the asymptotic behaviour of Heegner points

Abstract. We prove that all but finitely many Heegner points on a given (modular) elliptic curve (or, more generally, on a given quotient of the modular Jacobian variety $J_0(N)$) are of infinite order in the Mordell-Weil group where they naturally live, i.e., over the corresponding ring class field.

---

1. Notations

1.1 Let $N > 1$. The quasi-projective curve $Y_0(N)$ defined over $\mathbf{Q}$ classifies isogenies $[E \xrightarrow{\lambda} E']$ of elliptic curves with cyclic kernel $\ker\lambda \cong \mathbf{Z}/N\mathbf{Z}$. Over $\mathbf{C}$, the isogeny $[\mathbf{C}/\mathbf{Z}+\mathbf{Z}\tau \xrightarrow{[\times N]} \mathbf{C}/\mathbf{Z}+\mathbf{Z}N\tau]$ corresponds to the point $\Gamma_0(N)\cdot\tau$ of the quotient $\Gamma_0(N)\backslash\mathcal{H} = Y_0(N)(\mathbf{C})$ of the complex upper half-plane $\mathcal{H}$. The dual isogeny $[\mathbf{C}/\mathbf{Z}+\mathbf{Z}N\tau \longrightarrow \mathbf{C}/\mathbf{Z}+\mathbf{Z}\tau]$ induced by the identity on $\mathbf{C}$ corresponds to the point $\Gamma_0(N)\cdot w_N(\tau)$, where $w_N(\tau) = \frac{-1}{N\tau}$ denotes the Fricke involution.

We write as usual $X_0(N)$ for the smooth projective curve defined over $\mathbf{Q}$ which is the compactification of $Y_0(N)$ and classifies cyclic N-isogenies between generalized elliptic curves. And we denote by $J_0(N)$ the Jacobian of $X_0(N)$. We embed $X_0(N)$ in $J_0(N)$ by sending ∞ to 0, where ∞ is the cusp corresponding to the Néron polygon with a single side.

Finally, we fix a nonzero quotient defined over $\mathbf{Q}$, $J_0(N) \longrightarrow A$ of the abelian variety $J_0(N)$, and we let $X_0(N) \xrightarrow{\pi_A} A$ be the nonconstant morphism defined over $\mathbf{Q}$ which arises from composing the fixed embedding of $X_0(N)$ into $J_0(N)$ with the projection of $J_0(N)$ onto A. The following results will therefore apply in particular to the case of a (modular) elliptic curve A over $\mathbf{Q}$.

1.2 Let K be an imaginary quadratic field such that all prime numbers dividing N split in K. Note right away that, for any given N, there are infinitely many K satisfying this so-called "Heegner-condition" (which was introduced by Birch). It implies that there exists an ideal $\mathfrak{n}$ of the ring of integers $\mathfrak{o}_K$ such that one has $\mathfrak{o}_K/\mathfrak{n} \cong \mathbf{Z}/N\mathbf{Z}$.

More explicitly, let D be the discriminant of K and let $\sqrt{D}$ be the square root of D which belongs to $\mathcal{H}$. Then $\mathfrak{o}_K = \mathbf{Z} + \mathbf{Z}\alpha$ and $\mathfrak{n} = N\mathbf{Z} + \mathbf{Z}\alpha$, with $\alpha = \frac{-B+\sqrt{D}}{2}$ such that $\alpha^2 + B\alpha + AN = 0$ and $B^2 - 4AN = D$. Or again, $\mathfrak{o}_K = \mathbf{Z} + \mathbf{Z}\frac{NA}{\alpha}$, $\mathfrak{n}^{-1} = \mathbf{Z} + \mathbf{Z}\frac{A}{\alpha}$.

For every $f \geq 1$ relatively prime to N, we write $\mathfrak{o}_f = \mathbf{Z}+f\mathfrak{o}_K$ for the order of conductor f in K. Its discriminant is $D_f = Df^2$. And we put $\mathfrak{n}_f = \mathfrak{o}_f \cap \mathfrak{n}$. Since $(f, N) = 1$, $\mathfrak{n}_f$ is a proper $\mathfrak{o}_f$-ideal, that is to say, $\mathfrak{o}_f = \{x \in K \mid x\mathfrak{n}_f \subseteq \mathfrak{n}_f\}$.

More explicitly, we have that $\mathfrak{o}_f = \mathbf{Z} + \mathbf{Z}\alpha_f$ and $\mathfrak{n}_f = N\mathbf{Z} + \mathbf{Z}\alpha_f$ for $\alpha_f = f\alpha$. Thus $\alpha_f = \frac{-B_f+\sqrt{D_f}}{2}$, $\alpha_f^2 + B_f\alpha_f + A_fN = 0$ with $B_f = fB$, $A_f = f^2A$, $B_f^2 - 4A_fN = D_f = f^2D$. Or again, $\mathfrak{o}_f = \mathbf{Z} + \mathbf{Z}\frac{NA_f}{\alpha_f} = \mathbf{Z} + \mathbf{Z}\frac{NfA}{\alpha}$, $\mathfrak{n}_f^{-1} = \mathbf{Z} + \mathbf{Z}\frac{A_f}{\alpha_f} = \mathbf{Z} + \mathbf{Z}\frac{fA}{\alpha}$.

Given our choice of $\mathfrak{n}$, the *Heegner point y_f of conductor f on $Y_0(N)$* is defined to be the point represented by the isogeny $[\mathbf{C}/\mathfrak{o}_f \longrightarrow \mathbf{C}/\mathfrak{n}^{-1}]$ which is induced by the identity on $\mathbf{C}$. Its image $\pi_A(y_f) \in A(K_f)$ is called the *Heegner point of conductor f on A*.
The point $w_N(y_f)$ is represented by the dual isogeny

$$[\mathbf{C}/\mathfrak{n}^{-1} \longrightarrow \mathbf{C}/\mathfrak{o}_f] = \left[\mathbf{C}/\mathbf{Z} + \mathbf{Z}\frac{fA}{\alpha} \longrightarrow \mathbf{C}/\mathbf{Z} + \mathbf{Z}\frac{NfA}{\alpha}\right],$$

which is induced by multiplication by N. The point $w_N(y_f)$ therefore corresponds to the point $\Gamma_0(N) \cdot \tau_f$ of $\Gamma_0(N)\backslash\mathcal{H}$, where $\tau_f = -\frac{fA}{\alpha} = \frac{f(B+\sqrt{D})}{2N}$.

1.3 The field of definition K_f of y_f — and therefore also that of $\pi_A(y_f)$ — is the field generated over K by the j-invariants of elliptic curves with complex multiplication by the order $\mathfrak{o}_f$. It is the *ring class field* of conductor f of K, i.e., the abelian extension of K which is unramified outside of f and in which a prime ideal of K not dividing f is totally split if and only if it is not only principal, but can be generated by an element which, modulo f, is congruent to a rational number.

If f and f' are relatively prime, then K_f and $K_{f'}$ are linearly disjoint over the Hilbert class field K_1 of K. Also, $K_{ff'}$ is the compositum of K_f and $K_{f'}$. The same holds true for the rings of integers.

1.4 We can now state our main finiteness result, in which $N > 1$ is a fixed positive integer, D varies over the discriminants of imaginary quadratic fields K satisfying the Heegner condition of 1.2, and f varies over positive integers prime to N.

1.5 Theorem. *There are only a finite number of pairs (D, f) as above such that the point $\pi_A(y_f) \in A(K_f)$ is a torsion point.*

2. The first finiteness result

Theorem 1.5 will result from a quantitative version of the following proposition—see 3.3 below. Proposition 2.1 has already been used in the literature—see [3].

2.1 Proposition. *There exists $f_0 > 0$, depending on the level N and the discriminant D, such that for every $f > f_0$ relatively prime to N, the point $\pi_A(y_f) \in A(K_f)$ is a point of infinite order on the abelian variety A.*

The proof proceeds in three steps, 2.2 – 2.4.

2.2 Let $K_\infty = \bigcup_{f\geq 1} K_f$. We show that *the subgroup of torsion points $A(K_\infty)_{\rm tors}$ is finite.*
Let ℓ be a prime number which is inert in K. Every prime ideal λ of K_f above ℓ has norm $\mathbf{N}\lambda = \ell^2$. — In fact, writing $f = \ell^a f'$ with f' not divisible by ℓ one sees that the prime divisors of $\ell\mathfrak{o}_{K_1}$ are totally ramified in K_{ℓ^a}/K_1 and $\ell\mathfrak{o}_K$ splits completely in $K_{f'}$.

Since ℓ does not divide N (the primes dividing N split in K), the abelian variety A, as any quotient of $J_0(N)$, has good reduction at λ, and for every $f \geq 1$ prime to N the torsion subgroup of order prime to ℓ of $A(K_f)$ reduces injectively modulo λ. This gives

$$\mathrm{card}\big(A(K_f)^{\mathrm{non}-\ell}_{\mathrm{tors}}\big) \mid \mathrm{card}\big(\widetilde{A}_\lambda(\mathbf{F}_{\ell^2})\big).$$

Taking a second prime ℓ', distinct from ℓ, which remains inert in K we see that

$$\mathrm{card}\big(A(K_f)_{\mathrm{tors}}\big) \mid \mathrm{card}\big(\widetilde{A}_\lambda(\mathbf{F}_{\ell^2})\big) \cdot \mathrm{card}\big(\widetilde{A}_{\lambda'}(\mathbf{F}_{\ell'^2})[\ell^\infty]\big),$$

where the suffix $[\ell^\infty]$ signifies taking the ℓ-primary part. This proves 2.2.

2.3 Over $\mathbf{C}$, π_A lifts to a holomorphic mapping F on the completed upper half-plane.

$$\begin{array}{ccccc} \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}) & \xrightarrow{F} & & & \mathbf{C}^{\dim A} \\ \downarrow & & & & \downarrow \\ \Gamma_0(N)\backslash\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}) & \xrightarrow{\pi_A} & A(\mathbf{C}) & \cong & \mathbf{C}^{\dim A}/\Lambda \end{array}$$

We fix F by requiring that $F(\infty) = 0$. Then, *for every $m \geq 1$, there exists $M_m \in \mathbf{R}$ such that for all $\tau \in \mathcal{H}$ with $\mathrm{Im}(\tau) > M_m$ we have:*

$$0 < ||F(\tau)|| < \frac{1}{m} \inf_{0 \neq \gamma \in \Lambda} ||\gamma||.$$

2.4 We now conclude the proof of proposition 2.1 first under the additional hypothesis that the Fricke involution w_N induces an automorphism of A: According to 2.2, put $m = \mathrm{card}\big(A(K_\infty)_{\mathrm{tors}}\big)$, and pick M_m for this choice of m as in 2.3. Let $f_0 = \frac{2N}{|D|^{1/2}} M_m$. Then we find, in the notation introduced at the end of 1.2 above, that for every integer f greater than f_0 and prime to N one has $\mathrm{Im}(\tau_f) = \frac{f|D|^{1/2}}{2N} > M_m$. 2.3 now ensures that the point $\pi_A(w_N(y_f)) \in A(K_f)$, which corresponds to $F(\tau_f)$, is not an m-torsion point on the Jacobian. In view of our choice of m it has to be of infinite order. Since the involution w_N induces an automorphism of A, the same holds for the Heegner point $\pi_A(y_f)$ itself.

Finally, in order to prove the proposition for an arbitrary quotient A of $J_0(N)$, not necessarily invariant under w_N, one only has to modify the preceding argument by applying 2.3 to $w_N(A)$ rather than A.

2.5 *Remarks.* (1) For f as above, put $G_f = \mathrm{Gal}(K_f/K)$. Assume that A is of dimension 1, i.e., a (modular) elliptic curve. For a ring class character $\chi \in \widehat{G_f}$ of conductor dividing f, we define the L-function of A twisted by χ by the following Euler product, which converges for $\mathrm{Re}(s) > 3/2$.

$$L(A/K, \chi, s) = \prod_{\mathfrak{p} \subset \mathfrak{o}_K} \det\big(1 - \mathrm{Frob}_\mathfrak{p} \cdot \chi(\mathrm{Frob}_\mathfrak{p}) \mathbf{N}\mathfrak{p}^{-s} \mid V_l(A)_{I_\mathfrak{p}}\big)^{-1}$$

Here, $\mathrm{Frob}_\mathfrak{p}$ denotes the arithmetic Frobenius, and we put $\chi(\mathrm{Frob}_\mathfrak{p}) = 0$ for $\mathfrak{p} \mid f$. It follows from the Heegner condition of 1.2 that the order of $L(A/K, \chi, s)$ at $s = 1$ is odd and therefore that $L(E/K, \chi, 1) = 0$. Write $\langle\ ,\ \rangle_f$ for the sesquilinear extension to $A(K_f) \otimes_{\mathbf{Z}} \mathbf{C}$ of the canonical Néron-Tate height pairing on $A(K_f)$. Finally, put $e_\chi = \frac{1}{\#G_f} \sum_{\sigma \in G_f} \chi(\sigma)^{-1}\sigma$. Then the following formula is conjectured to hold, with the real period ω_A and some nonzero rational number $r = r(D, f)$.

$$L'(A/K, \chi, 1) = r \frac{\omega_A}{\sqrt{|D|}} \langle e_\chi y_f, e_\chi y_f \rangle_f \qquad (\mathbf{2.6})$$

In the particular case where $f = 1$, this is the well-known theorem of B.H. Gross and D. Zagier [4]. The generalization 2.6 is not completely proved yet. Assuming it, our theorem shows that, for every sufficiently big f, there is at least one ring class character $\chi \in \widehat{G_f}$ such that $L'(A/K, \chi, 1) \neq 0$. On the other hand, guided by results of Rohrlich's [11], one may wonder whether, given K, *there are only a finite number of pairs* (f, χ), *with* $f \geq 1$ *prime to* N *and* $\chi \in \widehat{G_f}$ *a character of conductor* f, *such that* $L'(E/K, \chi, 1) = 0$.

(2) The second step in the above proof transfers to our situation (and simplifies) an argument given in a more general context by S. Bloch and C. Schoen — see [12].

(3) The above proposition generalizes an analogous result proved in a particular case by P.F. Kurčanov [6]. The proof given by Kurčanov is certainly different from ours, but does rely on the similar principles.

3. Effectivity questions

3.1 It follows from the Pólya-Vinogradov theorem that we may always find distinct prime numbers ℓ, ℓ' as in 2.2 such that $\ell, \ell' < |D|^c$ for an absolute constant c. This gives the following bound for m.

$$\mathrm{card}\big(A(K_\infty)_{\mathrm{tors}}\big) \leq \mathrm{card}\big(\widetilde{A}_\lambda(\mathbf{F}_{\ell^2})\big) \cdot \mathrm{card}\big(\widetilde{A}_{\lambda'}(\mathbf{F}_{\ell'^2})\big) \leq \big((\ell+1)(\ell'+1)\big)^{2\dim A} \leq |D|^{4c\dim A}$$

3.2 In 2.3, we may always take

$$M_m = c_1 + \frac{\log(m)}{2\pi},$$

for some constant c_1 depending on the map π_A. Indeed, a local parameter at ∞ is given by $e^{2i\pi\tau}$, and $|e^{2i\pi\tau}| = e^{-2\pi \mathrm{Im}(\tau)}$.

3.3 *Proof of theorem 1.5.* Let us put together 2.4, 3.1 and 3.2. We see that *there exists an absolute constant* c_0 *and a constant* c_1 *depending on* A *such that for all positive integers* f *prime to* N *and satisfying*

$$f > \frac{2N}{|D|^{1/2}} \left\{c_1 + c_0 \dim A \log|D|\right\},$$

the Heegner point $\pi_A(y_f)$ *has infinite order in* A. For $|D|$ sufficiently big, this inequality holds for any $f \geq 1$. This concludes the proof of theorem 1.5.

4. The anticyclotomic $\mathbf{Z}_p$-extension and Mazur's module of Heegner points

We will now restrict to the case where $A/\mathbf{Q}$ is of dimension 1, i.e., A is a (modular) elliptic curve, assumed to be of conductor N. Let p be a prime number which stays prime in K, and such that $a_p = p + 1 - \#\Big(\tilde{A}_p(\mathbf{F}_p)\Big)$, the eigenvalue of the Hecke-operator T_p on A, is not divisible by p. In other words, assume that p is ordinary for A.

Let $H_\infty = \bigcup H_n$ be the anticyclotomic $\mathbf{Z}_p$-extension of our fixed imaginary quadratic field K, i.e., H_∞ is the unique $\mathbf{Z}_p$-extension of K contained in $K_{p^\infty} = \bigcup K_{p^{n+1}}$. We consider the Heegner points $z_n = \mathrm{tr}_{K_{p^{n+1}}/H_n}(\pi_A(y_{p^{n+1}})) \in A(H_n)$ and following Mazur [9], no. 19, we write $\mathcal{E}_\infty$ for the projective limit (with respect to the trace maps) of the submodules $\mathcal{E}_n$ of $(E(H_n) \otimes \mathbf{Z}_p)/(\text{torsion})$ which are generated by all the conjugates of z_n. For $n \geq 2$, the points on different levels are linked by the following distribution relations, which are immediate consequences of [10], p. 430.

$$\mathrm{tr}_{H_{n+1}/H_n}(z_{n+1}) = a_p z_n - z_{n-1}$$

$\mathcal{E}_\infty$ is an Iwasawa module, i.e., a finitely generated module over $\Lambda = \mathbf{Z}_p[[\Gamma]] = \mathbf{Z}_p[[T]]$, where $\Gamma = \mathrm{Gal}(H_\infty/K)$. Moreover, as Mazur observed [9], no. 19, $\mathcal{E}_\infty$ is a Λ-module (in fact, free) of rank 1 if and only if z_n is a point of infinite order for (any, and thus for all) $n >> 0$. Mazur conjectured that this is always the case. Note that this conjecture is a special instance of the question formulated at the end of remark 2.5(1).

Recall the definitions of the relevant Selmer groups. For any number field F and any $m \geq 2$, the m-Selmer group of A over F is defined to be the torsion group

$$\mathrm{Sel}_m(A/F) = \ker\Big(H^1(F, A_m) \longrightarrow \prod_v H^1(F_v, A)_m\Big).$$

Via direct limits, we obtain $\mathbf{Q}_p/\mathbf{Z}_p$-modules

$$\mathrm{Sel}_{p^\infty}(A/F) = \varinjlim \mathrm{Sel}_{p^n}(A/F), \qquad \mathrm{Sel}_{p^\infty}(A/H_\infty) = \varinjlim \mathrm{Sel}_{p^\infty}(A/H_n).$$

4.1 Theorem. *If z_n is a point of infinite order for $n >> 0$, then the Selmer group $\mathrm{Sel}_{p^\infty}(A/K)$ contains a subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$.*

The following immediate consequence of this is particularly interesting when the order of vanishing of $L(A/\mathbf{Q}, s)$ at $s = 1$ is at least 2.

4.2 Corollary. *Assume that the p-part $Ш(A/K)(p^\infty)$ of the Tate-Šafarevič group of A over K is finite and that z_n is a point of infinite order for $n >> 0$. Then $\dim A(K) \otimes \mathbf{Q} \geq 1$.*

4.3 *Proof of theorem 4.1 (argument suggested by K. Rubin).* Put $\mathcal{H}_\infty = \varinjlim \mathcal{E}_n \otimes \mathbf{Q}_p/\mathbf{Z}_p$. By the assumption of the theorem, $\mathcal{E}_\infty$ is a rank one Λ-module, so its coinvariants $(\mathcal{E}_\infty)_\Gamma$ admit a quotient isomorphic to $\mathbf{Z}_p$. Therefore the invariants $\mathcal{H}_\infty^\Gamma \subset \mathrm{Sel}_{p^\infty}(A/H_\infty)^\Gamma \subset H^1(H_\infty, A_{p^\infty})^\Gamma$ contain a copy of $\mathbf{Q}_p/\mathbf{Z}_p$. However, in our case the p^∞-Selmer group along the anticyclotomic extension is "controlled" in the sense that the canonical map $\mathrm{Sel}_{p^\infty}(A/K) \longrightarrow \mathrm{Sel}_{p^\infty}(A/H_\infty)^\Gamma$ has finite kernel and cokernel. This control can be wielded locally, the only interesting place being at p. More precisely, write the local descent sequences

$$\begin{array}{ccccccccc}
0 \longrightarrow & A((H_n)_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & H^1((H_n)_p, A_{p^\infty}) & \longrightarrow & \widehat{\Big(A((H_n)_p) \otimes \mathbf{Z}_p\Big)} & \longrightarrow & 0 \\
& \uparrow & & \uparrow & & \uparrow & & \\
0 \longrightarrow & A((K)_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & H^1((K)_p, A_{p^\infty}) & \longrightarrow & \widehat{\Big(A((K)_p) \otimes \mathbf{Z}_p\Big)} & \longrightarrow & 0
\end{array}$$

where the last vertical arrow is given by the dual of the trace map on local points. It's kernel is bounded independently of n since p is ordinary for A and thus the universal local traces have finite index in the local points $A((K)_p)$. This control theorem is due to Mazur [8]; for our situation see Manin [7], Thm. 4.5 together with Cor. 4.11(a).

4.4 *Remarks.* (1) Bertolini [1] (see also [2]) has established an Iwasawa theoretic analogue of Kolyvagin's method to prove in particular (under additional hypotheses on the prime p) that, if $\mathcal{E}_\infty$ is indeed of rank 1, then it agrees with the dual of the Selmer group up to a torsion module for which he can exhibit an annihilating power series.

(2) 4.1 provides an example of how the behaviour of higher Heegner points (granting the non-triviality assumption) govern the arithmetic of E over K, and therefore over $\mathbf{Q}$. Another striking instance of such a relationship was given by Kolyvagin in [5]. It also depends on an initial non-triviality conjecture, and is more like an ℓ-adic descent, for some fixed prime ℓ different from the primes entering into the conductors of the Heegner points. It would be interesting to be able to combine these two theories.

References

[1] M. Bertolini, Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions, Compositio Math. **99** (1995), 153–182

[2] M. Bertolini, Growth of Mordell-Weil groups in anticyclotomic towers; *in:* Arithmetic geometry (Cortona, 1994; F. Catanese, ed.), Sympos. Math., XXXVII, Cambridge Univ. Press, Cambridge, 1997, pp. 23–44

[3] M. Bertolini and H. Darmon, Non-triviality of families of Heegner points and ranks of Selmer groups over anticyclotomic towers. J. Ramanujan Math. Soc. **13** (1998), 15–24

[4] B.H. Gross and D. Zagier, Heegner points and the derivatives of L-series, Inventiones Math. **84** (1986), 225–320

[5] V.A. Kolyvagin, On the structure of Selmer groups, Mathematische Annalen **291** (1991), 253–259

[6] P.F. Kurčanov, Elliptic Curves of infinite rank over Γ-extensions, Math. USSR Sbornik **19** (1973), 320–324

[7] Yu. Manin, Krugovye polja i moduljarnye krivye, Uspechi Mat. Nauk, **26** (1971), 7–71. English translation: Cyclotomic fields and modular curves, Russian Math. Surveys **26**, no. 6 (1971), 7–78

[8] B. Mazur, Rational points on abelian varieties with values in towers of number fields, Inventiones Math. **18** (1972), 183–266

[9] B. Mazur, Modular Curves and Arithmetic, Proc. ICM Warszawa 1983, vol. I, pp. 185–211

[10] B. Perrin-Riou, Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, Bull. Soc. Math. France **115** (1987), 399–456

[11] D. Rohrlich, Nonvanishing of L-functions for GL(2), Inventiones Math. **97** (1989), 381–403

[12] C. Schoen, Complex multiplication cycles on elliptic modular threefolds, Duke Math. J. **53** (1986), 771–794

Jan Nekovář
D.P.M.M.S.
University of Cambridge
16 Mill Lane
Cambridge CB2 1SB, UK
`nekovar@dpmms.cam.ac.uk`

Norbert Schappacher
U.F.R. de mathématique et d'informatique
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg Cedex, France
`schappa@math.u-strasbg.fr`