ON THE ASYMPTOTIC BEHAVIOUR OF HEEGNER POINTS

Jan Nekovář & Norbert Schappacher

Dedicated to Professor Masatoshi Ikeda on the occasion of his 70th birthday

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

We write as usual \( X_0(N) \) for the smooth projective curve defined over \( \mathbb{Q} \) 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 \( \infty \) to \( 0 \), where \( \infty \) is the cusp corresponding to the Néron polygon with a single side.

Finally, we fix a nonzero quotient defined over \( \mathbb{Q} \), \( J_0(N) \longrightarrow A \) of the abelian variety \( J_0(N) \), and we let \( X_0(N) \xrightarrow{\pi A} A \) be the nonconstant morphism defined over \( \mathbb{Q} \) 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 \( \mathbb{Q} \).
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 \( \mathfrak{o}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z} \).

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

For every \( f \geq 1 \) relatively prime to \( N \), we write \( \mathfrak{o}_f = \mathbb{Z} + f\mathfrak{o}_K \) 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 \( \mathfrak{o}_f = \mathbb{Z} + \mathbb{Z}\alpha_f \) and \( \mathfrak{n}_f = N\mathbb{Z} + \mathbb{Z}\alpha_f \) for \( \alpha_f = f\alpha \). Thus \( \alpha_f = \frac{-Bf + \sqrt{Df}}{2} \), \( \alpha_f^2 + Bf\alpha_f + AfN = 0 \) with \( B_f = fB \), \( A_f = f^2A \), \( B_f^2 - 4A_fN = D_f = f^2D \). Or again, \( \mathfrak{o}_f = \mathbb{Z} + \mathbb{Z}\frac{NA_f}{\alpha_f} = \mathbb{Z} + \mathbb{Z}\frac{NA}{\alpha} \), \( \mathfrak{n}^{-1}_f = \mathbb{Z} + \mathbb{Z}\frac{A}{\alpha_f} = \mathbb{Z} + \mathbb{Z}\frac{A}{\alpha} \).

Given our choice of \( \mathfrak{n} \), the Heegner point \( y_f \) of conductor \( f \) on \( \mathcal{O}_K(N) \) is defined to be the point represented by the isogeny \( \mathbb{C}/\mathfrak{o}_f \rightarrow \mathbb{C}/\mathfrak{n}^{-1}_f \) which is induced by the identity on \( \mathbb{C} \). 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

\[
[\mathbb{C}/\mathfrak{n}^{-1} \rightarrow \mathbb{C}/\mathfrak{o}_f] = \left[ \mathbb{C}/\mathbb{Z} + \mathbb{Z}\frac{fA}{\alpha} \rightarrow \mathbb{C}/\mathbb{Z} + \mathbb{Z}\frac{NA}{\alpha} \right],
\]

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 $A(K_\infty)_{\text{tors}}$ is finite.
Let $\ell$ be a prime number which is inert in $K$. Every prime ideal $\wp$ of $K_f$ above $\ell$ has norm $N\wp = \ell^2$. In fact, writing $f = \ell^s f'$ with $f'$ not divisible by $\ell$ one sees that the prime divisors of $\ell\wp_K$ are totally ramified in $K_{\ell^s}/K_1$ and $\ell\wp_K$ splits completely in $K_{f'}$. Since $\ell$ 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 $\lambda$, and for every $f \geq 1$ prime to $N$ the torsion subgroup of order prime to $\ell$ of $A(K_f)$ reduces injectively modulo $\lambda$. This gives
\[
\text{card}(A(K_f)_{\text{tors}}) | \text{card}(\tilde{A}_\lambda(F_{\ell^s})).
\]
Taking a second prime $\ell'$, distinct from $\ell$, which remains in $K$ we see that
\[
\text{card}(A(K_f)_{\text{tors}}) | \text{card}(\tilde{A}_\lambda(F_{\ell'})) \cdot \text{card}(\tilde{A}_\lambda(F_{\ell'^s})[\ell^\infty]),
\]
where the suffix $[\ell^\infty]$ signifies taking the $\ell$-primary part. This proves 2.2.

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

\[
\begin{array}{ccc}
\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) & \xrightarrow{F} & \mathbb{C}^{\text{dim } A} \\
\downarrow & & \downarrow \\
\Gamma_0(N) \backslash \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) & \xrightarrow{\pi_A} & A(\mathbb{C}) \cong \mathbb{C}^{\text{dim } A}/\Lambda
\end{array}
\]
We fix $F$ by requiring that $F(\infty) = 0$. Then, for every $m \geq 1$, there exists $M_m \in \mathbb{R}$ such that for all $\tau \in \mathcal{H}$ with $\text{Im}(\tau) > M_m$ 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 $m = \text{card}(A(K_\infty)_\text{tors})$, 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 $\text{Im}(\tau_f) = \frac{D^{1/2}}{2N} > M_m$. 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 of $A$. 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 $G_f = \text{Gal}(K_f/K)$. Assume that $A$ is of dimension 1, i.e., a (modular) elliptic curve. For a ring class character $\chi \in \hat{G_f}$ of conductor dividing $f$, we define the $L$-function of $A$ twisted by $\chi$ by the following Euler product, which converges for $\text{Re}(s) > 3/2$.

$$L(A/K, \chi, s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \det(1 - \text{Frob}_{\mathfrak{p}} \cdot \chi(\text{Frob}_{\mathfrak{p}}) N\mathfrak{p}^{-s} | V_{\mathfrak{p}}(A)_{\mathfrak{f}})^{-1}$$

Here, $\text{Frob}_{\mathfrak{p}}$ denotes the arithmetic Frobenius, and we put $\chi(\text{Frob}_{\mathfrak{p}}) = 0$ for $\mathfrak{p} | f$. 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 $(\ , \ )_f$ for the sesquilinear extension to $A(K_f) \otimes_{\mathbb{Z}} \mathbb{C}$ of the canonical Néron-Tate height pairing on $A(K_f)$. Finally, put $e_\chi = \frac{1}{[\mathcal{O}_f : \mathfrak{p}]} \sum_{\sigma \in G_f} \chi(\sigma)^{-1}\sigma$. Then the following formula is conjectured to hold, with the real period $\omega_A$ and some nonzero rational number $r = r(D, f)$.

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

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
NEKOVAR, SCHAPPACHER

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 $(f, \chi)$, 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 similar principles.

3. Effectivity questions

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

$$\text{card}(\mathcal{A}(K_{\infty})_{tors}) \leq \text{card}(\mathcal{A}(\mathbb{F}_{\ell^2})) \cdot \text{card}(\mathcal{A}(\mathbb{F}_{\ell'^2})) \leq ((\ell+1)(\ell'+1))^{2 \dim A} \leq |D|^{4c \cdot \dim A}$$

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 $\pi_A$. Indeed, a local parameter at $\infty$ is given by $e^{2\pi \tau}$, and $|e^{2\pi \tau}| = e^{-2\pi \text{Im} \tau}$.

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 $\mathbb{Z}_p$-extension and Mazur’s module of Heegner points

We will now restrict to the case where $A/\mathbb{Q}$ 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 $a_p = p + 1 - \#(\mathcal{A}_p(F_p))$, 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 $\mathbb{Z}_p$-extension of our fixed imaginary quadratic field $K$, i.e., $H_\infty$ is the unique $\mathbb{Z}_p$-extension of $K$ contained in $K_{p^n+1} = \bigcup K_{p^n+1}$. We consider the Heegner points $z_n = \text{tr}_{K_{n+1}/K_{n}}(\pi_A(y_{n+1})) \in A(H_n)$ and following Mazur [9], no. 19, we write $E_\infty$ for the projective limit (with respect to the trace maps) of the submodules $E_n$ of $(E(H_n) \otimes \mathbb{Z}_p)/(\text{torsion})$ 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.

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

$E_\infty$ is an Iwasawa module, i.e., a finitely generated module over $\Lambda = \mathbb{Z}_p[[\Gamma]] = \mathbb{Z}_p[[T]]$, where $\Gamma = \text{Gal}(H_\infty/K)$. Moreover, as Mazur observed [9], no. 19, $E_\infty$ is a $\Lambda$-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

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

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

$$\text{Sel}_{p^\infty}(A/F) = \varprojlim \text{Sel}_{p^n}(A/F), \quad \text{Sel}_{p^\infty}(A/H_\infty) = \varprojlim \text{Sel}_{p^n}(A/H_n).$$

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

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

4.2 Corollary. Assume that the $p$-part $\mathcal{H}(A/K)(p^\infty)$ 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 $\dim A(K) \otimes \mathbb{Q} \geq 1$. 

554
4.3 Proof of theorem 4.1 (argument suggested by K. Rubin). Put \( \mathcal{H}_\infty = \lim_{\rightarrow} \mathcal{E}_n \otimes Q_p/Z_p \).

By the assumption of the theorem, \( \mathcal{E}_\infty \) is a rank one \( \Lambda \)-module, so its coinvariants \( (\mathcal{E}_\infty)_\Gamma \) admit a quotient isomorphic to \( Z_p \). Therefore the invariants \( \mathcal{H}_\infty^\Gamma \subset Sel_p(A/H_\infty)^\Gamma \subset H^1(H_\infty, A_p) \) contain a copy of \( Q_p/Z_p \). However, in our case the \( p^\infty \)-Selmer group along the anticyclotomic extension is “controlled” in the sense that the canonical map \( Sel_p(A/K) \rightarrow Sel_p(A/H_\infty) \) 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

\[
0 \rightarrow A((H_n)_p) \otimes Q_p/Z_p \rightarrow H^1((H_n)_p, A_p) \rightarrow \left( A((H_n)_p) \otimes Z_p \right) \rightarrow 0
\]

\[
0 \rightarrow A((K)_p) \otimes Q_p/Z_p \rightarrow H^1((K)_p, A_p) \rightarrow \left( A((K)_p) \otimes Z_p \right) \rightarrow 0
\]

where the last vertical arrow is given by the dual of the trace map on local points. Its 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 \( Q \). 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 \( \ell \)-adic descent, for some fixed prime \( \ell \) 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


NEKOVAR, SCHAPPACHER


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


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

Received 24.11.1998

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