HEEGNER POINTS ON $X_o(11)$

by

Benedict H. GROSS

-:-:-:-

In this paper, I would like to illustrate a new method for studying Heegner points on $X_o(N)$ by a consideration of the first non-trivial case. A central question is the determination of the image of the group of divisors on these points in the Jacobian $J_o(N)$. Birch [1, 2] and Mazur [3, 4] have already established many beautiful results on these divisor classes, using geometric arguments. Our approach is more arithmetic, and perhaps a bit more flexible.

It is a pleasure to thank the number-theorists at Bordeaux for their kind invitation, Henri Cohen for his generous on-the-spot computations, and the entire family Cassou-Noguès for their wonderful hospitality.

§ 1. - Heegner points

Let $X_o(11)$ be the modular curve over $\mathbb{Q}$ which classifies elliptic curves together with an 11-isogeny. The curve $X_o(11)$ has genus 1 ; its Jacobian is an elliptic curve $E = J_o(11)$ with Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$.

Let K be an imaginary quadratic field where the rational prime 11 is split, let $\mathcal{O}$ be an order in K whose discriminant $d(\mathcal{O}) = d_K c^2$ is prime to 11, and let $\mathfrak{p}$ denote a prime ideal of $\mathcal{O}$ with residue field $\mathbb{Z}/11$.

Fix an embedding of K in $\mathbb{C}$; the modular data $x = (\mathbb{C}/\mathcal{O}, \ker \mathfrak{p})$ then determines a complex point of $X_o(11)$. In fact, the point x is rational over the ring-class extension $H = K(j(\mathcal{O}))$ of K with conductor c, and the theory of complex multiplication gives an isomorphism $G = \mathrm{Gal}(H/K) \simeq \mathrm{Pic}(\mathcal{O})$.

Let ∞ and 0 denote the cusps of $X_o(11)$; both of these points are defined over $\mathbb{Q}$ and the class of the divisor $(0) - (\infty)$ generates the cyclic group $E(\mathbb{Q}) \simeq \mathbb{Z}/5$. Let y denote the class of the divisor $(x) - (\infty)$ in $E(H)$. For any complex character χ of G of conductor equal to c, we define $y_\chi = \sum_G \chi^{-1}(\sigma) y^\sigma$ in $(E(H) \otimes_{\mathbb{Z}} \mathbb{C})^\chi$. A central question in the theory is to determine precisely when $y_\chi \neq 0$. Secret computations of Birch and Stephens lead one to expect that this will be the case precisely when the vector space $(E(H) \otimes \mathbb{C})^\chi$ has dimension 1. This expectation is supported by the results below.

Assume now that the character χ is quadratic, and satisfies $\chi(\mathfrak{p}) = -1$. Then χ corresponds to a pair of quadratic extensions of $\mathbb{Q}$, say k and k', whose discriminants satisfy $d d' = d(\mathcal{O}) = d_K c^2$. Assume that $d > 0$, so the field k is real and k' is imaginary. Let ε and ε' be the Dirichlet characters associated to these fields and let h and h' denote their class numbers. Since $\chi(\mathfrak{p}) = \varepsilon(11) = \varepsilon'(11) = -1$, the rational prime 11 is inert in k and in k'.

The biquadratic extension $L = Kk = Kk'$ is the subfield of H fixed by the kernel of χ in G. Here is a diagram of the fields in question :

$$\begin{tikzcd}[column sep=small]
 & H \arrow[d, dash] & \\
 & L = Kk \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k \arrow[dr, dash] & k' \arrow[d, dash] & K \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Note that the point y_χ defined above actually lies in the group $E(L)^\chi$; this is just the minus eigenspace for the action of the group $Gal(L/K)$ on $E(L)$.

PROPOSITION 1. - If $hh' \not\equiv 0 \pmod 5$ then $y_\chi \neq 0$ and $E(L)^\chi \simeq \mathbb{Z}$.

In fact, we will show that, under the hypotheses of proposition 1, the point y_χ is not in the subgroup $5E(L)^\chi$, and the χ-component of the group $Ш(E/L)_5$ is trivial.

As an immediate corollary of proposition 1, we shall obtain :

PROPOSITION 2. - Let k be a real quadratic field where the prime 11 is inert. Assume that the class number h of k is prime to 5. Then $E(k) \simeq \mathbb{Z}/5 \oplus \mathbb{Z}$ and $Ш(E/k)_5 = 0$.

Mazur has obtained a similar result over imaginary quadratic fields where 11 is split [4, pg 237]. Using similar methods as in the proof of proposition 1 (but working with the character $\chi = 1$), I can give a slight refinement of his result.

PROPOSITION 3. - Let K be an imaginary quadratic field where the prime 11 is split. Assume that the class number h_A of the Dedekind domain $A = \mathcal{O}_K[1/11]$ is prime to 5. Then $E(K) \simeq \mathbb{Z}/5 \oplus \mathbb{Z}$ and $Ш(E/K)_5 = 0$.

We note that when 11 splits in K : $11 = \mathfrak{p}.\bar{\mathfrak{p}}$, then h_A is simply the quotient of h_K by the order of $\mathfrak{p}$ in the class group.

§ 2. - The descent

Let F be a number field and let $S_5(E/F)$ denote the 5-Selmer group of $E = J_o(11)$ over F. One has an exact sequence :

$$0 \longrightarrow E(F)/5E(F) \xrightarrow[\alpha]{} S_5(E/F) \longrightarrow Ш(E/F)_5 \longrightarrow 0 .$$

Since the 5-torsion $E_5 \simeq \mu_5 \oplus \mathbb{Z}/5$ has a simple structure as a Galois module over $\mathbb{Q}$, the Selmer group $S_5(E/F)$ can be calculated in a fairly explicit manner. We will simply state the result.

Let A be the Dedekind domain $\mathcal{O}_F[1/11]$ and let Pic A denote the class group of A. There is an exact sequence :

$$0 \longrightarrow \mathrm{Hom}(\mathrm{Pic}\,A\,,\ \mathbb{Z}/5) \longrightarrow S_5(E/F) \xrightarrow[\beta]{} H^1(A,\mu_5)$$

and the group $H^1(A,\mu_5) \subset H^1(F,\mu_5) \simeq F^*/F^{*5}$ itself lies in an exact sequence :

$$0 \longrightarrow A^{\times}/A^{\times 5} \longrightarrow H^1(A,\mu_5) \longrightarrow \mathrm{Pic}\,A_5 \longrightarrow 0\ .$$

The cokernel of β can be tricky to determine ; of more interest to us here is a concrete description of the composite homomorphism $\delta = \beta \circ \alpha \ :\ E(F)/5\,E(F) \longrightarrow F^*/F^{*5}$. Let $f(z) = \{\Delta(z)/\Delta(11\,z)\}^{\frac{1}{2}}$; this modular unit lies in the rational function field of $X_o(11)$ and has divisor $(f) = 5\{(0)-(\infty)\}$. If $\mathfrak{a}$ is any divisor of degree 0 on $X_o(11)$ which is prime to the cusps and rational over F, and $\tilde{\mathfrak{a}}$ is the image of $\mathfrak{a}$ in $E(F)$, we have the formula $f(\mathfrak{a}) \equiv \delta(\tilde{\mathfrak{a}})\ (\mathrm{mod}\ F^{*5}$

Now assume that $F = L$, the field of concern to us in proposition 1. All of the above sequences remain exact when we pass to the χ-components, and the torsion subgroup of $E(L)^{\chi}$ is easily seen to be trivial. Since the relevant class numbers h and h' are prime to 5, we have $\mathrm{Hom}(\mathrm{Pic}\,A\,,\ \mathbb{Z}/5)^{\chi} = \mathrm{Pic}\,A_5^{\chi} = 0$. Hence the map β is an injection and the group $H^1(A\,,\mu_5)^{\chi} \simeq (A^*/A^{*5})^{\chi}$ is isomorphic to U/U^5, where U denotes the unit group of the real quadratic field k. We have a diagram :

$$E(L)^{\chi}/5\,E(L)^{\chi} \underset{\alpha}{\hookrightarrow} S_5(E/L)^{\chi} \underset{\beta}{\hookrightarrow} U/U^5 \simeq \mathbb{Z}/5\ .$$

Hence $E(L)^{\chi}$ has rank at most 1. To show α and β are both isomorphisms we will show that $\delta(y_{\chi}) = \beta \circ \alpha(y_{\chi}) \neq 0$ in U/U^5.

Using the explicit description of δ we find $\delta(y_{\chi}) = E_{\chi}$ mod. U^5, where $E_{\chi} = \{\prod_{\mathrm{Pic}\,\mathcal{O}} (\Delta(\mathfrak{a})/\Delta(\mathfrak{p}\,\mathfrak{a}))^{\chi(\mathfrak{a})}\}^{\frac{1}{2}}$ is an elliptic unit in U. If $L(\chi\,,s)$ is the abelian L-function of the character χ, then Kronecker's limit formula gives the relation $\log|E_{\chi}| = -12\,L'(\chi\,,0)$. We now use the factorization of L-series $L(\chi\,,s) = L(\varepsilon\,,s)\,L(\varepsilon',s)$ and the explicit formula for the Dirichlet L-series at $s=0$. Namely $L'(\varepsilon\,,0) = -h\log|u|$, where $0<u<1$ is a fundamental unit in k, and $L(\varepsilon',0) = 2h'/w'$, where w' is the number of roots of unity in k'.

Since the units u and E_χ are both real, the relation between the L-series gives the identity $E_\chi = \pm\, u^{24hh'/w'}$. Since $hh' \not\equiv 0 \pmod 5$, this shows that E_χ is not a 5^{th} power in U.

We now turn to the proof of proposition 2. Along with k, choose an auxiliary imaginary quadratic field k' where 11 is inert and h' is prime to 5. Let K be the third field contained in the biquadratic extension $L = kk'$; then K is imaginary and 11 splits in K. Let $\mathcal{O}$ be the order of K of discriminant dd', and construct the point y_χ in $E(L)^\chi$ as in proposition 1. Since $E(L)^\chi = E(k)^\varepsilon \oplus E(k')^{\varepsilon'} \simeq \mathbb{Z}$ and $Ш\,(E/L)_5^\chi = 0$, we will be finished once we show $E(k') = E(\mathbb{Q}) \simeq \mathbb{Z}/5$. This follows the descent, as $S_5(E/k') \simeq \mathbb{Z}/5$.

The reader is invited to find a proof of proposition 3 for himself, using the fact that $\{\Delta(\mathcal{O})/\Delta(\mathfrak{p})\}^{\frac{1}{2}}$ is an integer in H which generates the ideal $\mathfrak{p}^6$ of K.

-:-:-:-

BIBLIOGRAPHY

[1] B. J. BIRCH, Diophantine Analysis and modular functions, Proc. Colloquium on algebraic geometry at Bombay (1968), 35-42.

[2] B. J. BIRCH, Elliptic curves and modular functions, Symposia Mathematica IV, Inst. Naz. di Alti Mathematica (1970), 27-32.

[3] B. MAZUR, Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. 47 (1978), 33-186.

[4] B. MAZUR, On the arithmetic of special values of L-functions, Invent. Math. 55 (1979), 207-240.

(texte reçu le 27 mai 1982)

-:-:-:-

Benedict H. GROSS
Department of Mathematics
Brown University, Box 1917
PROVIDENCE, R.I. 02912
U.S.A.