Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Göttingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online-systems to access or download a digitized document you accept these Terms and Conditions.

Reproductions of materials on the web site may not be made for or donated to other repositories, nor may they be further reproduced without written permission from the Göttingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:
Niedersächsische Staats- und Universitätsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de
HEEGNER POINTS ON $X_0(11)$

by

Benedict H. GROSS

-:-:-:-

In this paper, I would like to illustrate a new method for studying Heegner points on $X_0(N)$ 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 $J_0(N)$. 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 $X_0(11)$ be the modular curve over $\mathbb{Q}$ which classifies elliptic curves together with an 11-isogeny. The curve $X_0(11)$ has genus 1; its Jacobian is an elliptic curve $E = J_0(11)$ 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 $O$ be an order in $K$ whose discriminant $d(O) = d_K c^2$ is prime to $11$, and let $p$ denote a prime ideal of $O$ with residue field $\mathbb{Z}/11$.

Fix an embedding of $K$ in $\mathbb{C}$; the modular data $x = (\mathbb{C}/O, \ker p)$ then determines a complex point of $X_0(11)$. In fact, the point $x$ is rational over the ring-class extension $H = K(j(O))$ of $K$ with conductor $c$, and the theory of complex multiplication gives an isomorphism $G = \text{Gal}(H/K) \cong \text{Pic}(O)$.

Let $\infty$ and $0$ denote the cusps of $X_0(11)$; both of these points are defined over $\mathbb{Q}$ and the class of the divisor $(0) - (\infty)$ generates the cyclic group $E(\mathbb{Q}) \cong \mathbb{Z}/5$. Let $y$ denote the class of the divisor $(x) - (\infty)$ in $E(H)$. For any complex character $\chi$ of $G$ of conductor equal to $c$, we define $y = \sum_{\chi} \chi^{-1}(\sigma)y^\sigma$ in $(E(H) \otimes \mathbb{C})^\chi$. A central question in the theory is to determine precisely when $y \neq 0$. 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 $\chi$ is quadratic, and satisfies $\chi(p) = -1$. Then $\chi$ corresponds to a pair of quadratic extensions of $\mathbb{Q}$, say $k$ and $k'$, whose discriminants satisfy $dd' = d(O) = d_K c^2$. Assume that $d > 0$, so the field $k$ is real and $k'$ is imaginary. Let $\varepsilon$ and $\varepsilon'$ be the Dirichlet characters associated to these fields and let $h$ and $h'$ denote their class numbers. Since $\chi(p) = \varepsilon(11) = \varepsilon'(11) = -1$, 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 $\chi$ in $G$. Here is a diagram of the fields in question:

```
  H
   |
   L = Kk
   /  \
  |   \
 k  k' K
  /  \
 |   \
 \Q
```
Note that the point $y^\chi$ 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 $h \neq 0 \pmod{5}$ then $y^\chi \neq 0$ and $E(L)^\chi \cong \mathbb{Z}$.

In fact, we will show that, under the hypotheses of proposition 1, the point $y^\chi$ is not in the subgroup $5E(L)^\chi$, and the $\chi$-component of the group $\text{Hom}(E/L)_5$ 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 $E(k) \cong \mathbb{Z}/5 \oplus \mathbb{Z}$ and $\text{Hom}(E/k)_5 = 0$.

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 $E(K) \cong \mathbb{Z}/5 \oplus \mathbb{Z}$ and $\text{Hom}(E/K)_5 = 0$.

We note that when 11 splits in $K$, 11 = $p \cdot \overline{p}$, then $h_A$ is simply the quotient of $h_K$ by the order of $p$ 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 $E = J_0(11)$ over $F$. One has an exact sequence:

$$0 \to E(F)/5E(F) \xrightarrow{\alpha} S_5(E/F) \to \text{Hom}(E/F)_5 \to 0.$$ Since the 5-torsion $E_5 = \mu_5 \oplus \mathbb{Z}/5$ 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 $\mathfrak{O}_F[1/11]$ and let $\text{Pic} A$ denote the class group of $A$. There is an exact sequence:

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

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

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

The cokernel of $\beta$ can be tricky to determine; of more interest to us here is a concrete description of the composite homomorphism $\delta = \beta \circ \alpha : E(F)/5E(F) \longrightarrow F^*/F^{*5}$. Let $f(z) = \{ \Delta(z)/\Delta(11z) \}^{\frac{1}{2}}$; this modular unit lies in the rational function field of $X_0(11)$ and has divisor $(f) = 5 \{(0) -(\infty)\}$. If $a$ is any divisor of degree 0 on $X_0(11)$ which is prime to the cusps and rational over $F$, and $\bar{a}$ is the image of $a$ in $E(F)$, we have the formula $f(a) = \delta(\bar{a}) \pmod{F^{*5}}$.

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 $\chi$-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 $\text{Hom}(\text{Pic} A, \mathbb{Z}/5)^\chi = \text{Pic} A_5^\chi = 0$. Hence the map $\beta$ is an injection and the group $H^1(A, \mu_5)^\chi \cong (A^*/A^{*5})^\chi$ is isomorphic to $U/U^5$, where $U$ denotes the unit group of the real quadratic field $k$. We have a diagram:

$$E(L)^\chi/5E(L)^\chi \xrightarrow{\alpha} S_5(E/L)^\chi \xrightarrow{\beta} U/U^5 \cong \mathbb{Z}/5.$$ 

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

Using the explicit description of $\delta$ we find $\delta(\chi) = E = \chi \pmod{U^5}$, where $E = \prod_{\text{Pic} \mathfrak{O}} (\Delta(a)/\Delta(p \cdot a))^{\chi(a)}$ is an elliptic unit in $U$. If $L(\chi, s)$ is the abelian $L$-function of the character $\chi$, then Kronecker's limit formula gives the relation

$$\log |E| = -12 L'(\chi, 0).$$

We now use the factorization of $L$-series

$$L(\chi, s) = L(\epsilon, s) L(\epsilon', s)$$

and the explicit formula for the Dirichlet $L$-series at $s = 0$. Namely $L'(\epsilon, 0) = -h \log |u|$, where $0 < u < 1$ is a fundamental unit in $k$, and $L(\epsilon', 0) = 2h'/w'$, where $w'$ is the number of roots of unity in $k'$. 

Since the units $u$ and $E_{\chi}$ are both real, the relation between the $L$-series gives the identity $E_{\chi} = \pm u^{2h'w'/24$h'w'$. Since $hh' \not\equiv 0 \pmod{5}$, this shows that $E_{\chi}$ 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 $\mathfrak{d}$ be the order of $K$ of discriminant $dd'$, and construct the point $y_{\chi}$ in $E(L)^{\chi}$ as in proposition 1. Since $E(L)^{\chi} = E(k)^{\xi} \otimes E(k')^{\xi'} \cong \mathbb{Z}$ and $\text{ord}_{5}(E/L)^{\chi} = 0$, we will be finished once we show $E(k') = E(\mathbb{Q}) \cong \mathbb{Z}/5$. This follows the descent, as $S_{5}(E/k') \cong \mathbb{Z}/5$.

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

---

**BIBLIOGRAPHY**


(texe reçu le 27 mai 1982)

---

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