Number Theory and its Applications, Proc. Conf. Moscow Univ., Feb. 2–4, 1983 (Izd. Mosk. Univ. 1983).

[PW] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, 1988, pp. 280–312.

[Wa] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), 257–283.

DEPARTMENT OF MATHEMATICS AND STATISTICS
BOWLING GREEN STATE UNIVERSITY
Bowling Green, Ohio 43403-0221 U.S.A.

Received on 30.7.1987
and in revised form on 30.5.1988 (1740)

ACTA ARITHMETICA
LV (1990)

On the arithmetic of an elliptic curve over a Z_p-extension

by

FRANÇOIS RAMAROSON (Washington, D.C.)

1. Introduction. Let E/Q be an elliptic curve with conductor N. Assume that E admits a parametrization by modular functions and let φ be a Weil parametrization:

$$\varphi\colon X_0(N) \to E$$

where $X_0(N)$ is the Shimura canonical model for the Riemann surface $\mathscr{H}/\Gamma_0(N)$, quotient of the upper-half plane by the action by the group

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})\colon\ c \equiv 0 \pmod{N}\right\}.$$

For simplicity let us assume that N is prime and let K be an imaginary quadratic field in which N splits completely and with discriminant less than -4.

In [1], Gross developed the theory of Heegner points on $X_0(N)$. These points are rational over abelian extensions of K, and via the Weil parametrization mentioned above, they should contribute to the Mordell–Weil groups of the elliptic curve E over these abelian extensions.

Let now p be a prime which is ordinary for E, this means that E has good reduction at p and the trace of the Frobenius endomorphism of the reduced curve modulo p, is not divisible by p. For such a p, one can consider K_∞, the anticyclotomic $\boldsymbol{Z}_p$-extension of K, which is contained in the union of all ring class fields corresponding to the orders of K of conductor p^n, $n = 0, 1, 2, \ldots$

The Heegner points are rational over these ring class fields and the Weil parametrization carries them over to E; taking norms gives points in the Mordell–Weil group of E rational over K_∞. The points so obtained in $E(K_\infty)$ fit together into an object called the Heegner module, which is a module over the relevant Iwasawa ring Λ.

In [6], Mazur made a precise conjecture concerning the structure of the Heegner module, namely, under a technical assumption, that it is a cyclic module of rank one, over the Iwasawa ring Λ.

In this note, we study one of the first non-trivial cases and look at $N = 19$. In this case the modular curve $X_0(19)$ is of genus one, and hence it (or rather its jacobian) is an elliptic curve. The Weil parametrization is of degree one (identity) and the vanishing of the Heegner module could happen only upon taking norms. However, under some conditions to be made precise, the Heegner module is non-zero and is of rank one over the Iwasawa ring. Of course, this implies that the Heegner points contribute significantly to the rank of the curve over the various layers of the anticyclotomic extension.

In Section 2, we construct the Heegner points and define the Heegner module, we also study the effect of the Hecke operator on these points. We prove, under some conditions, a non-vanishing result for the norms of Heegner points and thereby deduce Mazur's conjecture in this case. In Section 3, we obtain lower bounds for the rank of the Mordell–Weil groups over the anticyclotomic layers.

Finally, we gratefully thank Howard University for support under grant FY85FRP-AA50.

2. The Heegner module $\mathscr{E}(K_\infty)$ (see [1], [6]). Let $\mathcal{O} = \mathbf{Z}+\mathbf{Z}\omega$ be the ring of integers of K, for some ω in K. For each $n \geqslant 0$, let $\mathcal{O}_n = \mathbf{Z}+\mathbf{Z}p^n\omega$, $\mathcal{O}_n$ is an order of conductor p^n. Assume that 19 splits in K as $(19) = \mathcal{N}\cdot\mathcal{N}^\tau$; then, in $\mathcal{O}_n$, it splits as $(19) = \mathcal{N}_n\cdot\mathcal{N}_n^\tau$ where $\mathcal{N}_n = \mathcal{N}\cap\mathcal{O}_n$ and $\mathcal{N}_n^\tau = \mathcal{N}^\tau\cap\mathcal{O}_n$. Let $H_n = K(j(\mathcal{O}_n))$ be the ring class field of $\mathcal{O}_n$ and $H_\infty = \bigcup_n H_n$. H_∞ contains the anticyclotomic $\mathbf{Z}_p$-extension of K, denoted K_∞. Let $K_n = K_\infty \cap H_n$, $n \geqslant 0$ and $\Gamma = \mathrm{Gal}(K_\infty/K_0) \approx \mathbf{Z}_p$.

Using the notation of [1], let $(\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n])$ be a Heegner point of level p^n. If ∞ denotes the cusp at infinity, then the divisor $((\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n]))-(\infty)$ defines a point $x_n \in E(H_n)$. Let $e_n = N_{H_n/K_n}(x_n) = \sum_\sigma x_n^\sigma$, where the sum is over $\sigma \in \mathrm{Gal}(H_n/K_n)$, then $e_n \in E(K_n)$.

Let $\mathscr{E}(K_n)$ be the submodule of $(E(K_n)\otimes\mathbf{Z}_p)|_{\text{torsion}}$, generated by $\{e_n^\sigma: \sigma\in\mathrm{Gal}(K_n/K)\}$.

Let T_p be the pth Hecke operator. As a correspondence on $X_0(19)$, it stabilize the divisors supported on Heegner points. We have the following formulas:

$$T_p(\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n])$$

$$= (\mathcal{O}_{n+1}, \mathcal{N}_{n+1}, [\mathcal{O}_{n+1}])+(\mathcal{O}_{n-1}, \mathcal{N}_{n-1}, [\mathcal{O}_{n-1}])+\sum_{j=1}^{p-1}(\mathcal{O}_{n+1}, \mathcal{N}_{n+1}, [L_j])$$

valid for $n \geqslant 1$, where L_j is a lattice of index p in $\mathcal{O}_n$ and is a proper $\mathcal{O}_{n+1}$-lattice (see [3]). For $n = 0$, we have

$$T_p(\mathcal{O}, \mathcal{N}, [\mathcal{O}]) = (\mathcal{O}_1, \mathcal{N}_1, [\mathcal{O}_1])+\sum_{j=0}^{p-1}(\mathcal{O}_1, \mathcal{N}_1, [L_j])$$

if p stays prime in K;

$$= (\mathcal{O}_1, \mathcal{N}_1, [\mathcal{O}_1])+(\mathcal{O}, \mathcal{N}, [\mathscr{P}])+\sum_{j=1}^{p-1}(\mathcal{O}_1, \mathcal{N}_1, [L_j])$$

if p ramifies in K as $(p) = \mathscr{P}^2$;

$$= (\mathcal{O}_1, \mathcal{N}_1, [\mathcal{O}_1])+(\mathcal{O}, \mathcal{N}, [\mathscr{P}]+(\mathcal{O}, \mathcal{N}, [\mathscr{P}^\tau])+\sum_{j=2}^{p-1}(\mathcal{O}_1, \mathcal{N}_1, [L_j])$$

if p splits in K as $(p) = \mathscr{P}\cdot\mathscr{P}^\tau$.

As an endomorphism of E, T_p satisfies:

$$T_p(x) = a_p x, \qquad x \in E$$

where $a_p = 1+p-\#(E(F_p))$. If we combine the above, we obtain the following:

for $n \geqslant 1$

$$a_p x_n = N_{H_{n+1}/H_n}(x_{n+1})+x_{n-1} \quad \text{in } E(H_n)$$

along with the appropriate formulas for $n = 0$. Taking norms to K_n we obtain:

for $n \geqslant 1$

$$a_p e_n = N_{K_{n+1}/K_n}(e_{n+1})+e_{n-1}$$

along with the appropriate formulas for $n = 0$.

Let $\varepsilon(p) = 0$, 1 or -1 according to whether p ramifies, splits or stays prime in K. After some manipulation of the formulas above, one obtains the following result of Mazur [6].

THEOREM 2.1. *Suppose that a_p is congruent to neither* 0 *or* $1+\varepsilon(p)$ (mod p). *Then*:

$$N_{K_m/K_n}\mathscr{E}(K_m) = \mathscr{E}(K_n), \qquad m \geqslant n \geqslant 0.$$

Assume now that $a_p \neq 0$ or $1+\varepsilon(p)$ (mod p). The Heegner module is defined to be:

$$\mathscr{E}(K_\infty) = \varprojlim_n \mathscr{E}(K_n)$$

where the projection maps are the norm maps.

Let Λ be the Iwasawa ring $\mathbf{Z}_p[[\Gamma]]$, then $\mathscr{E}(K_\infty)$ is a free Λ-module of rank 0 or 1. Mazur's conjecture is that the rank is 1 [6]. Equivalently, there exists n for which $e_n \neq 0$ in $\mathscr{E}(K_n)$. In some special cases one can show that $e_n \neq 0$ for all n (see also [5]).

THEOREM 2.2. *Assume that* 19 *splits in K and that $p > 3$, $p \neq 19$. Suppose that* 3 *does not divide $h(p-\varepsilon(p))$, where h is the class number of K. Then $e_n \neq 0$ in $\mathscr{E}(K_n)$, for all $n \geqslant 0$.*

The Gross–Zagier theory and the Birch–Swinnerton-Dyer conjecture imply:

Corollary 2.3. *For $n = 0$, the L-function of E over K_0 has a simple pole at $s = 1$ and e_0 generates a subgroup of finite index in $E(K_0)$.*

Proof of Theorem 2.2. Let $n \geqslant 0$. We show that e_n is not a torsion point in $E(K_n)$. Suppose it is torsion, and let r be its order. We need a lemma:

Lemma 2.4. *If $k > 0$ is an integer such that $ke_n = 0$, then 3 divides k. In particular $e_n \neq 0$ in $E(K_n)$.*

Proof. If $ke_n = 0$, then $ke_n^\tau = 0$. In particular, the Heegner divisor:

$$D = k \sum_{\sigma \in \mathrm{Gal}(H_n/K_n)} (\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n])^\sigma - [H_n:K_n](\infty)$$

and its complex conjugate:

$$D^\tau = k \sum_{\sigma \in \mathrm{Gal}(H_n/K_n)} (\mathcal{O}_n, \mathcal{N}_n^\tau, [\mathcal{O}_n])^\sigma - [H_n:K_n](\infty)$$

are linearly equivalent. Hence there exists a function f on $X_0(19)$ such that:

$$D = D^\tau + (f).$$

Let $g(z) = \left(\dfrac{\Delta(z)}{\Delta(19z)}\right)^{1/6}$, then $g(z)$ is a modular unit in $Q(X_0(19))$ whose divisor is: $(g) = 3((0)-(\infty))$; (0, ∞ are the cusps). By Weil reciprocity (see [7]) we get:

$$N_{H_n/K_n}\left[\left(\frac{\Delta(\mathcal{O}_n)}{\Delta(\mathcal{N}_n)}\right)^{1/6}\right]^k = N_{H_n/K_n}\left[\left(\frac{\Delta(\mathcal{O}_n)}{\Delta(\mathcal{N}_n^\tau)}\right)^{1/6}\right]^k u^3$$

for some $u \in K_n$. Looking at the ideals generated by both sides (see [4]) and recalling that $3 \mid h(p-\varepsilon(p))$, we see that $3 \mid k$.

We now continue the proof of the theorem. By Lemma 2.4, 3 divides r, say, $r = 3^a r_1$ with $3 \nmid r_1$. Let $r_1 e_n = e_n'$ so that $3^a e_n' = 0$. We claim that $e_n' \notin E(Q)$. If $e_n' \in E(Q)$ then $r_1(e_n - e_n^\tau) = 0$, but by the proof of Lemma 2.4, this implies that 3 divides r_1. Therefore $e_n' \notin E(Q)$. Let F be the field generated by e_n' and all of its Q-conjugates. Then F/Q is Galois $F \subset K_n$ and we have the diagram:

$$\begin{tikzcd}
Q(E[3^a]) \arrow[dr, dash] & & K_n \arrow[dl, dash] \\
& F \arrow[d, dash] & \\
& Q &
\end{tikzcd}$$

where $Q(E[3^a])$ is the field of 3^a-division points on E. K_n/Q is Galois dihedral and F/Q is Galois, therefore $\mathrm{Gal}(K_n/F)$ is a normal subgroup of the dihedral group $\mathrm{Gal}(K_n/Q)$. Hence, $\mathrm{Gal}(K_n/F) \approx \mathbf{Z}/p^b\mathbf{Z}$, $1 \leqslant b \leqslant n$, and in particular F contains K.

$$\begin{tikzcd}
Q(E[3^a]) \arrow[dr, dash] & & K_n \arrow[dl, dash] \\
& F \arrow[d, dash] & \\
& K \arrow[d, dash] & \\
& Q &
\end{tikzcd}$$

The criterion of Neron–Ogg–Shafarevich and the fact that 19 splits in K now imply that $d_K = -3$ which is against our assumption that $d_K < -4$. ($d_K =$ discriminant of K). This ends the proof of Theorem 2.2.

Corollary 2.5. *The Heegner module $\mathscr{E}(K_\infty)$ is a free Λ-module of rank 1.*

3. The rank of E over K_∞.

In this section we work under the conditions of Theorem 2.1 and 2.2. In particular, e_n is of infinite order for all $n \geqslant 0$, $N_{K_m/K_n}\mathscr{E}(K_m) = \mathscr{E}(K_n)$, $m \geqslant n \geqslant 0$ and $\mathscr{E}(K_\infty)$ is a free Λ-module of rank one.

Lemma 3.1. *For every integer $n \geqslant 1$, the following are equivalent:*

(i) *e_n is rational over K_{n-1},*

(ii) *$pe_n \in \mathscr{E}(K_{n-1})$,*

(iii) *for every integer $k \geqslant 1$, $p^k e_n \in \mathscr{E}(K_{n-1})$,*

(iv) *$\mathscr{E}(K_{n-1}) = p\mathscr{E}(K_n)$,*

(v) *there exists $a \in \mathbf{Z}_p$, $a \neq 0$ such that $ae_n \in \mathscr{E}(K_{n-1})$.*

The proof is straightforward.

Theorem 3.2. *There exists an integer m_0 such that, for all $n \geqslant m_0$, e_n is not rational over K_{n-1}.*

Proof. Assume the contrary, then we can find a strictly increasing sequence of integers: $n_0 < n_1 < n_2 < \ldots$ such that e_{n_k} is rational over K_{n_k-1}. Let us denote the norm from K_m to K_n by $N_{m/n}$, where $m > n$. Then by induction on k, we obtain:

$$\begin{aligned}\mathscr{E}(K_{n_0-1}) &= p\mathscr{E}(K_{n_0}) = pN_{n_1/n_0}\mathscr{E}(K_{n_1}) = p^2 N_{n_1-1/n_0}\mathscr{E}(K_{n_1}) = \ldots \\ &= p^{k+1} N_{n_1-1/n_0} \circ \ldots \circ N_{n_k-1/n_{k-1}} \mathscr{E}(K_{n_k}) \quad \text{for all } k.\end{aligned}$$

Here $N_{n_1-1/n_0} \circ \ldots \circ N_{n_k-1/n_{k-1}} \mathscr{E}(K_{n_k})$ is a submodule of

$$\mathscr{E}(K_{n_k}) \cap [(E(K_{n_0}) \otimes \mathbf{Z}_p)|_{\mathrm{torsion}}].$$

Therefore, looking at $e_{n_0-1} \in \mathscr{E}(K_{n_0-1})$, which is not zero, we get: for every k, there exists $y_k \in (E(K_{n_0}) \otimes \mathbf{Z}_p)|_{\mathrm{torsion}}$ such that

$$e_{n_0-1} = p^{k+1} y_k.$$

But this is clearly impossible since $(E(K_{n_0}) \otimes \mathbf{Z}_p)|_{\mathrm{torsion}}$ is a finitely generated free $\mathbf{Z}_p$-module. This ends the proof of Theorem 3.2.

THEOREM 3.3. *There exists an integer m_0 and a constant c, depending only on m_0 such that for all $n \geqslant m_0$:*

$$\operatorname{rank} E(K_n) \geqslant p^n - c.$$

Proof. Clearly it is enough to prove the same statement as in the theorem with $E(K_n)$ replaced by $\mathscr{E}(K_n)$. We do this by induction on n. Let m_0 be as in Theorem 3.2 and let $c = p^{m_0} - 1$. The statement is clearly true for $n = m_0$ since e_{m_0} is of infinite order. Assume that $\operatorname{rank} \mathscr{E}(K_{n-1}) \geqslant p^{n-1} - c$. The $\operatorname{Gal}(K_n/K_0)$-module $\mathscr{E}(K_n) \otimes Q_p$ decomposes into:

$$\mathscr{E}(K_n) \otimes Q_p \approx (\mathscr{E}(K_{n-1}) \otimes Q_p) \otimes M$$

where M is a stable $\operatorname{Gal}(K_n/K_0)$-module. We make two remarks:

(1) by Theorem 3.2, $\dim M \geqslant 1$.

(2) if $v \in M$ and $v^\sigma = v$ for all $\sigma \in \operatorname{Gal}(K_n/K_{n-1})$, then $v = 0$. Let N be any non-zero, irreducible factor of M. Then we have the eigenspace decomposition: $N \otimes C = \bigoplus N^\chi$, where χ runs through the characters of $\operatorname{Gal}(K_n/K_0)$. By the second remark, $N^\chi = 0$ if χ is equal to one on $\operatorname{Gal}(K_n/K_{n-1})$. Moreover, for Galois-conjugate characters χ and χ^τ, $\dim N^{\chi^\tau} = \dim N^\chi$, therefore, we see that $\dim N = p^n - p^{n-1}$. Now it follows that

$$\begin{aligned}\operatorname{rank} \mathscr{E}(K_n) &= \operatorname{rank} \mathscr{E}(K_{n-1}) + \dim M \\ &\geqslant p^{n-1} - c + p^n - p^{n-1} \geqslant p^n - c.\end{aligned}$$

This ends the proof of Theorem 3.3.

Remark 3.4. For a different point of view on the growth of the ranks of Mordell–Weil groups, see M. Harris [2].

References

[1] B. Gross, *Heegner points on $X_0(N)$*; In R. A. Rankin (ed.): *Modular forms*, Ellis Horwood, Chichester, 1984, pp. 87–106.

[2] M. Harris, *Systematic growth of Mordell–Weil groups of Abelian varieties in towers of number fields*, Inventiones Math. 51 (1979), 123–141.

[3] P. Kurchanov, *On the rank of elliptic curves over Γ-extensions*, Mat. Sbornik 93 (1974), 460–466.

[4] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[5] B. Mazur, *On the arithmetic of special values of L-functions*, Inventiones Math. 55 (1979), 207–240.

[6] – *Modular curves and arithmetic*, Proceedings of Intern. Congress of Mathematicians, Warsaw 1983, Vol. 1, pp. 185–211.

[7] J. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer Verlag, 1986.

DEPARTMENT OF MATHEMATICS
HOWARD UNIVERSITY
Washington, D.C. 20059
U.S.A.

Received on 10.12.1987
and in revised form on 28.7.1988 (1772)

ACTA ARITHMETICA
LV (1990)

Congruences for the Stirling numbers and associated Stirling numbers

by

F. T. HOWARD (Winston-Salem, N.C.)

1. Introduction. In [3] it is proved that if $k+n$ is odd then the Stirling number of the first kind, $s(n, k)$, is divisible by the odd part of $n-1$, and the Stirling number of the second kind, $S(n, k)$, is divisible by the odd part of k. These results can be improved; we show in this paper, for example, that if $k+n$ is odd,

$$s(n, k) \equiv 0 \left(\operatorname{mod} \binom{n}{2}\right), \tag{1.1}$$

$$S(n, k) \equiv 0 \left(\operatorname{mod} \binom{k+1}{2}\right). \tag{1.2}$$

Congruences such as (1.1) and (1.2) are apparently not well known. A few congruences for prime moduli can be found in [2], pp. 218–219, 229 and [4], p. 81. Carlitz [1] worked out a method for finding congruences for $S(n, k) \pmod{p}$, where p is prime, and he found the residues of $S(n, k)$ for $p = 2$, 3 and 5. Carlitz also proved some formulas for special cases such as $S(n, pk)$.

In the present paper we prove (1.1), (1.2) and other congruences for the Stirling numbers and associated Stirling numbers. In particular, we show how to find congruences (mod p) for the Stirling numbers and associated Stirling numbers, and we illustrate our method by finding the residues for $p = 2$, 3 and 5. To the writer's knowledge, these congruences, with the exception of Carlitz's results for $S(n, k)$, have not been published before.

2. Stirling numbers of the first kind. The numbers $s(n, k)$ can be defined by means of

$$x(x+1)\ldots(x+n-1) = \sum_{k=0}^{n} s(n, k) x^k \tag{2.1}$$

or by the generating function

$$(-\log(1-x))^k = k! \sum_{n=k}^{\infty} s(n, k) x^n/n!. \tag{2.2}$$