RATIONAL POINTS OF INFINITE ORDER ON ELLIPTIC CURVES

François Ramaroson

Let N be a prime number of the form $N=u^2+64$, where $u\in\mathbf{Z}$, and let l be a prime greater than 3, congruent to 3 mod 4 which is a quadratic residue mod N. Denote by K the imaginary quadratic field $Q(\sqrt{-l})$.

According to Setzer [13], there are (up to isomorphism) two elliptic curves defined over Q having a rational point of order two and with conductor N:

$$E: y^2=x^3+ux^2-16x \quad \text{and} \quad E': y^2=x^3-2ux^2+Nx$$

where u is chosen, so that $u\equiv 1 \pmod 4$. E and E' are isogenous over Q. In fact, $E'\approx E/C$, where C is the subgroup of E generated by the rational point of order two.

A global minimal model for E is:

$$y^2+xy=x^3+\left(\frac{u-1}{4}\right)x^2-x.$$

Direct calculations from this model give:

(1) The minimal discriminant is N;

(2) The j-invariant is $(N-16)^3/N$.

PROPOSITION 0.1.

(1) $\operatorname{rank}(E(Q))=\operatorname{rank}(E'(Q))=0$;

(2) $Ш(E,Q)_2=Ш(E',Q)_2=0$.

Proof. This proposition follows directly from Mazur [9] (Corollary 9.10, p. 257), as E and E' have prime conductors. □

PROPOSITION 0.2. $E(Q)\approx\mathbf{Z}/2\mathbf{Z}\approx E'(Q)$.

Proof. We work it out for E.

By Proposition 0.1, $E(Q)$ is a torsion group. Suppose $E(Q)$ has a point M of order $p\neq 2$, with p prime. Since E has good reduction at 2, we have an injection $E(Q_2)_p \hookrightarrow \tilde{E}(\mathbf{F}_2)_p$, where $\tilde{E}$ is the reduced curve mod 2 and $\mathbf{F}_2$ the residue field with 2 elements.

After we reduce the global minimal model

$$y^2+xy=x^3+\left(\frac{u-1}{4}\right)x^2-x$$

modulo 2, we get:

$$y^2+xy=x^3+x^2-x \quad \text{if } u\not\equiv 1 \pmod 8,$$
$$y^2+xy=x^3-x \quad \text{if } u\equiv 1 \pmod 8.$$

Received September 21, 1983. Revision received March 28, 1985.
Michigan Math. J. 33 (1986).

Direct calculations now show that

$$\begin{aligned} \#(\tilde{E}(\mathbf{F}_2)) &= 4 \quad \text{if } u \equiv 1 \pmod 8, \\ &= 2 \quad \text{if } u \not\equiv 1 \pmod 8. \end{aligned}$$

In any case $\tilde{E}(\mathbf{F}_2)$ does not contain a subgroup of order $p \neq 2$, contradiction. Therefore, $E(Q)$ contains only 2-torsion points. However, it is easy to see that, of all the 2-torsion points on E, two of them are rational over $Q(\sqrt{N})$; therefore, $E(Q) \approx \mathbf{Z}/2\mathbf{Z}$.

E' is 2-isogenous to E; hence, we also have $E'(Q) \approx \mathbf{Z}/2\mathbf{Z}$. □

We will study the arithmetic of E over $K = Q(\sqrt{-l})$. The Tate–Shafarevich conjecture predicts that rank $E(K)$ is positive. Using the Birch–Heegner method, we will observe that if E is a Weil curve, then a point of infinite order exists on $E(K)$.

1. The arithmetic of E over K.

(1.1) PRELIMINARIES ([5], [7]). (In this section E denotes any elliptic curve over Q).

All fields we deal with are extensions of Q. For any number field k and any place v of k, k_v will denote the completion of k at v. For any field k and any $\mathrm{Gal}(\bar{k}/k)$-module A, the Galois cohomology groups $H^*(\mathrm{Gal}(\bar{k}/k), A)$ are denoted $H^*(k, A)$.

Now let k be a number field and v a place of k.

The short exact sequence

$$0 \to E(\bar{k})_2 \to E(\bar{k}) \xrightarrow{2} E(k) \to 0$$

induces the following exact sequence in cohomology:

$$0 \to E(k)/2E(k) \to H^1(k, E_2) \to H^1(k, E)_2 \to 0.$$

Similarly, we have the exact sequence

$$0 \to E(k_v)/2E(k_v) \to H^1(k_v, E_2) \to H^1(k_v, E)_2 \to 0.$$

The inclusion $k \subset k_v$ gives rise to restriction maps and we have a commutative diagram:

$$\begin{array}{ccccccccc} 0 \to & E(k)/2E(k) & \xrightarrow{\lambda} & H^1(k, E_2) & \xrightarrow{\pi} & H^1(k, E_2) & \to 0 \\ & \downarrow \alpha_v & & \downarrow \beta_v & & \downarrow \gamma_v & \\ 0 \to & E(k_v)/2E(k_v) & \xrightarrow{\lambda_v} & H^1(k_v, E_2) & \xrightarrow{\pi_v} & H^1(k_v, E)_2 & \to 0. \end{array}$$

The local Selmer group, $S(k_v)$ is the image of λ_v and is isomorphic to $E(k_v)/2E(k_v)$.

The global Selmer group is:

$$S(k) = \{\mathfrak{s} \in H^1(k, E_2) \mid \beta_v(\mathfrak{s}) \in S(k_v) \text{ for all } v\}.$$

Let Ш(k), the Tate–Shafarevich group, be the kernel of

$$H^1(k,E) \to \prod_v H^1(k_v,E).$$

Then we have the following fundamental exact sequence:

$$0 \to E(k)/2E(k) \xrightarrow{\lambda} S(k) \xrightarrow{\pi} Ш(k)_2 \to 0.$$

(1.2) NORMS ([7]). Let K be a quadratic extension of Q, and let σ denote the generator of $\mathrm{Gal}(k/Q)$. We define the norm on global points as:

$$\mathbf{N}: E(K) \to E(Q),$$
$$P \to P+P^{\sigma}.$$

On local points, for a quadratic extension K_v/Q_p where v lies over p we define the norm $\mathbf{N}_p: E(K_v) \to E(Q_p)$. We also have the norm on the global Selmer group $\mathbf{N}: S(K) \to S(Q)$ and on the local Selmer groups

$$\mathbf{N}_p: S(K_v) \to S(Q_p).$$

These norms come from co-restrictions in cohomology. The local cokernels $E(Q_p)/\mathbf{N}_p(E(K_v))$ and $S(Q_p)/\mathbf{N}_p(S(K_v))$ are finite dimensional vector spaces over $\mathbf{F}_2$; they have the same dimension, i_p. This dimension is the local norm index at p. We make the convention that $i_p=0$ if p splits in K.

Let Φ denote the subgroup of $S(Q)$ defined by

$$\Phi = \{\mathfrak{s} \in S(Q) \mid \beta_p(\mathfrak{s}) \in \mathbf{N}_p(S(K_v)) \text{ for all } p,\ v \text{ lying over } p\}.$$

Φ is the group of all elements in the global Selmer group $S(Q)$ which are everywhere local norms. Φ clearly contains the group of global norms $\mathbf{N}(S(K))$. In [7], Kramer proved that $\Phi/\mathbf{N}(S(K))$ is always of even dimension over $\mathbf{F}_2$.

(1.3) COMPUTATIONS OF LOCAL INDICES. From now on E is the Neumann–Setzer curve and $K=Q(\sqrt{-l}\,)$ as in the introduction.

PROPOSITION (1.3.1). *Defining the local norm index as before, we have:*

(1) $i_p=0$ if $p \neq N, l$,
(2) $i_N=0$,
(3) $i_l=2$,
(4) $i_\infty=1$.

Proof. We apply [7].

(1) It is known ([9, Corollary 4.4, p. 204]) that if p is a good prime and is unramified in K then $i_p=0$; this is the case when $p \neq N, l$.

(2) Since $(l/N)=+1$, N splits in K; hence $i_N=0$.

(3) At l, E has good reduction but l ramifies in K; since $(-l/N)=+1$, we have that $(N, -l)=+1$ (Norm residue symbol). Hence i_l is even and $i_l=0$ or 2. Moreover, the reduced curve has a non-trivial rational point; hence $i_l=2$.

(4) At infinity, $i_\infty=1$ since the discriminant of the minimal model is positive. □

(1.4) THE GROUP $\Phi/\mathbf{N}(S(K))$. We first observe that, from the known facts about E stated in the introduction and the exact sequence

$$0 \to E(Q)/2E(Q) \to S(Q) \to Ш(Q)_2 \to 0,$$

we have $S(Q) \approx E(Q) \approx \mathbf{Z}/2\mathbf{Z}$.

LEMMA (1.4.1). *Let E be given as $y^2 = x^3 + ux^2 - 16x$ and $P_0 = (0, 0)$, the non-trivial rational point. Then if P is a point such that $2P = P_0$, then P is one of the following four points:* $(4i, \pm 4\sqrt{-u-8i})$, $(-4i, \pm 4\sqrt{-u+8i})$.

Proof. This is a standard calculation and is left to the reader. □

LEMMA (1.4.2). *Let $\mathfrak{s}$ be the non-zero element in $S(Q)$; then $\beta_l(\mathfrak{s}) \neq 0$ in $S(Q_l)$, where β_l is as in* (1.1).

Proof. Since $l \equiv 3 \pmod 4$, Lemma (1.4.1) implies that $P_0 \notin 2E(Q_l)$. Now consider the following commutative diagram:

$$\begin{array}{ccccc} Q \to & E(Q)/2E(Q) & \xrightarrow{\lambda} & S(Q) \\ & \downarrow \alpha_l & & \downarrow \beta_l \\ 0 \to & E(Q_l)/2E(Q_l) & \xrightarrow{\lambda_l} & S(Q_l). \end{array}$$

$\mathfrak{s}$ is the image of P_0 under λ; moreover, since α_l is induced by inclusion, the image of P_0 under α_l is not zero. λ_l is in fact an isomorphism, hence $\beta_l(\mathfrak{s}) \neq 0$. □

LEMMA (1.4.3). *Let v be the place of K lying over l. Then*

$$\mathbf{N}_l(S(K_v)) = 0.$$

Proof. By [4, p. 717], we have $\#(S(Q_l)) = \#(E(Q_l)_2)$, where $\#(X)$ denotes the cardinality of the finite set X. It is easy to see that all the points of order two are rational over $Q(\sqrt{N})$, and since $(N/l) = (l/N) = +1$ we see that all these points are rational over Q_l. Therefore $E(Q_l)_2 \approx \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$; moreover, it is clear that the non-zero elements in $S(Q_l)$ are of order 2, hence $S(Q_l) \approx \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $\dim(S(Q_l)) = 2$ as an $\mathbf{F}_2$-vector space. On the other hand, by Proposition (1.3.1), $i_l = 2$, but $i_l = \dim(S(Q_l)/\mathbf{N}_l(S(K_v))$ where v lies over l. Therefore $\mathbf{N}_l(S(K_v)) = 0$. □

PROPOSITION (1.4.1). *The group Φ defined in* (1.1) *is trivial, hence $\Phi/\mathbf{N}(S(K))$ is also trivial.*

Proof. Just recall that Φ is a subgroup of $S(Q)$ and the rest is clear from there, using the lemmas. □

(1.5). THE RANK OF $E(K)$.

THEOREM (1.5.1). $\operatorname{rank}(E(K)) = 1 - \dim Ш(K)_2$.

Proof. In [7, p. 130], we have the formula

$$\operatorname{rank}(E(K)) = \Sigma i_p + \dim \Phi + \dim \mathbf{N}(S(K)) - 2\dim E(Q)_2 - \dim Ш(K)_2.$$

From the computations done so far we obtain the claimed formula for the rank. □

REMARK. Now we observe from the formula for the rank that the Tate–Shafarevich conjecture says that $Ш(K)_2$ must be trivial and the rank must be one.

2. Existence of points of infinite order. In the rest of this note—under the assumption that E is a Weil curve—we show that a point of infinite order must exist on $E(K)$ and, indeed, the rank is one and $Ш(K)_2 = 0$.

(2.1) SOME BASIC FACTS. Assume that E is a Weil curve. Hence we have a surjective morphism of finite degree defined over Q: $X_0(N) \to E$, where $X_0(N)$ is the modular curve which is a smooth projective model for $Q(j(z), j(Nz))$ over Q. Recall that $l > 3$, $l \equiv 3 \pmod 4$, $(l/N) = 1$ and $K = Q(\sqrt{-l})$; the conditions on l imply that $(-l/4N) = 1$.

The following is a result of Kurchanov.

THEOREM (2.1.1) (Kurchanov). *With l and N as above, let L be the Hilbert class field of K. Then there exists a $\mathbf{Z}_l$-extension $L^{(\infty)}$ of L:*

$$L = L_0 \subset L_1 \subset \cdots \subset \bigcup_{n=0}^{\infty} L_n = L^{(\infty)}$$

such that for each $n \geq 0$, there exists a point $M \in E(L^{(\infty)})$ and $M \notin E(L_n)$.

Proof. See [8, p. 322].

(2.2) A SPECIAL QUARTIC CURVE AND HEEGNER'S LEMMA. Consider the quartic curve $y^2 = X^4 + uX^2 - 16$. We have a rational map defined over Q:

$$\psi : C \to E$$
$$(x, y) \to (x^2, xy).$$

We make the following observations:

(i) $C(Q)_{\text{affine}}$ is empty.

(ii) Take the model $y^2 = x^3 + ux^2 - 16x$ for E, P_0 the non-trivial rational point. Let F be a number field and $M \in E(F)$, with $2M \neq P_0$. The point $2M = M'$ has coordinates of the form (a^2, b) and is rational over F. It is clear then that the point $R = (a, b/a)$ is in $C(F)$ and $\psi(R) = M'$.

Let $C^{(-l)}$ denote the twist of C by K; its equation can be written as $-ly^2 = x^4 + ux^2 - 16$. C and $C^{(-l)}$ are isomorphic over K or any field containing K.

In order to obtain points on E which are rational over certain extensions of K, we shall first obtain points on $C^{(-l)}$ and then on C, carrying these points over to E by mean of ψ. For this purpose, we have the following special case of a lemma due to Heegner.

LEMMA (2.2.1) (Heegner). *Let f be a quartic polynomial with rational coefficients whose leading coefficient is not a square, and let M and L be number fields such that M is an extension of L of odd degree not equal to 3. Suppose that $y^2 = f(x)$ is solvable in M; then it is solvable in L.*

Proof. See [2] or [6, p. 29].

(2.3). THE MORDELL–WEIL GROUP OF E OVER THE HILBERT CLASS FIELD OF K.

PROPOSITION (2.3.1). *Let p be an odd prime and E_p the group of points of order p on $E(\bar{Q})$. Then* $\mathrm{Gal}(Q(E_p)/Q) \approx \mathrm{GL}_2(\mathbf{F}_p)$.

Proof. Suppose that $\mathrm{Gal}(Q(E_p)/Q) \not\approx \mathrm{GL}_2(\mathbf{F}_p)$. Recall that $j=(N-1)^3/N$ and observe that p does not divide $\mathrm{ord}_N(j)=-1$. By Serre [11: Proposition 21, p. 306, especially "Remarque" on p. 307], either:

(i) E has a Q-rational point of order p, or

(ii) E is p-isogenous over Q to a curve $\bar{E}$ which has a Q-rational point of order p.

Proposition 0.2 together with the following lemma give a contradiction.

LEMMA 2.3.2. *E is not p-isogenous over Q to a curve $\bar{E}$ which has a Q-rational point of order p.*

Proof of Lemma 2.3.2. If $\bar{E}$ has a rational point of order 2 then $\bar{E}$ must be E' (see first page for the definition of E'), but $E'(Q) \approx \mathbf{Z}/2\mathbf{Z}$.

If $\bar{E}$ has no rational point of order 2, let P denote the non-trivial rational point of order 2 on $E(Q)$ and f the p-isogeny $f: E \to \bar{E}$. One has $f(P)=0$, so $P \in \ker f$ and 2 must divide $\#(\mathrm{Ker}\, f)=p$, but p is odd. □

Next we want to describe the torsion part of the Mordell–Weil group of E over the Hilbert class field of K; more generally we prove the following.

THEOREM (2.3.3). *Let F/Q be a finite, Galois extension in which N is unramified. Then $E(F)_{\mathrm{tors}}=E(Q)_2 \approx \mathbf{Z}/2\mathbf{Z}$.*

Proof. Assume the contrary and let e be a point in $E(F)_{\mathrm{tors}}$, not in $E(Q)_2$, of (exact) order $m \geq 3$. We separate two cases: m is a power 2 and m is not a power of 2.

First case: $m=2^n$. We may assume $n \geq 2$; then the point $e_1=2^{n-1}e$ is a point of order 2 in $E(F)_{\mathrm{tors}}$. Since N is unramified in F and 2^n is the exact order of e, e_1 must be the non-trivial rational point of order 2. Let us denote by e_2 the point $2^{n-2}e$; then $e_1=2e_2$. Now we consider the model $y^2=x^2+ux^2-16x$ with $e_1=(0,0)$; we see that e_2 has to be one of the four points: $(4i, \pm 4i\sqrt{u-8i})$; $(-4i, \pm 4i\sqrt{u+8i})$ where $i=\sqrt{-1}$. Since e_2 is in $E(F)_{\mathrm{tors}}$, we have that one of the two fields: $Q(i, \sqrt{u-8i})$ and $Q(i, \sqrt{u+8i})$, is contained in F. But N ramifies in both of these fields and hence, *a fortiori,* in F; contradiction.

Second case: $m=2^n m_1$; $m_1 \neq 1$, m_1 odd. Without loss of generality we may assume that $n=0$ and $m_1=p$, an odd prime. We then have $pe=0$; put $L=Q(e)$ and $M=Q(E_p)$.

LEMMA (2.3.4). $p \neq N$.

Proof of Lemma (2.3.4). If $p=N$, consider the following diagram of fields extension:

$$\begin{array}{ccc} F & & Q(E_N) \\ & \diagdown \quad \diagup & \\ & L & \\ & | & \\ & Q. & \end{array}$$

N does not ramify in L/Q, because otherwise it would ramify in F. However some prime must ramify in L/Q because it is a non-trivial extension: say a prime q ramifies in L/Q, hence, *a fortiori*, q ramifies in $Q(E_N)/Q$. But $q \neq N$, therefore E has good reduction at q; by Serre–Tate [12], $Q(E_N)/Q$ is unramified at q; contradiction. □

It is well-known that E_p is a 2-dimensional vector space over $\mathbf{F}_p$. Inside $E(F)_{\text{tors}}$ we have the following.

LEMMA (2.3.5). *If e' is another point of order p rational over F then $e' = ke$ where $k \in \mathbf{F}_p$; clearly k is unique.*

Proof of Lemma (2.3.5). Suppose that there exists a point e_1 in $E(F)_{\text{tors}}$, of order p and linearly independent of e over $\mathbf{F}_p$. Then the whole of E_p is contained in $E(F)_{\text{tors}}$, hence $Q(E_p)$ is contained in F. But by Lemma (2.3.4) and Proposition (2.3.2), N ramifies in $Q(E_p)$ and hence in F, which is against our hypothesis. □

LEMMA (2.3.6). *L/Q is Galois, cyclic of degree dividing $p-1$.*

Proof. By hypothesis, F/Q is Galois. Moreover, E is defined over Q, hence all the conjugates of e are still in $E(F)_{\text{tors}}$ and are of order p; Lemma (2.3.5) now implies that $L = Q(e)$ is Galois over Q. Now consider the map:

$$k\colon \mathrm{Gal}(L/Q) \to \mathbf{F}_p^x$$
$$\sigma \to k(\sigma),$$

where $k(\sigma)$ is defined, through Lemma (2.3.5), by the equation $e^\sigma = k(\sigma)e$. The map k is clearly a homomorphism (multiplicative) and is injective since L/Q is Galois. Hence $\mathrm{Gal}(L/Q)$ is isomorphic to a subgroup of the multiplicative group of the finite field $\mathbf{F}_p$; therefore it is cyclic and its order divides $p-1$. □

Next, choose $e_1 \in E_p$ such that $E_p = \mathbf{F}_p e \oplus \mathbf{F}_p e_1$. Let $G = \mathrm{Gal}(M/L)$; the action of G on E_p gives rise to a faithful representation:

$$\rho\colon G \to \mathrm{GL}_2(\mathbf{F}_p) \approx \mathrm{Gal}(M/Q).$$

With the choice of a basis made above we have:

$$\text{if } \sigma \in G,\ \rho(\sigma) = \begin{pmatrix} 1 & a(\sigma) \\ 0 & b(\sigma) \end{pmatrix};\quad a(\sigma),\ b(\sigma) \text{ are in } \mathbf{F}_p.$$

On the other hand we have the exact sequence:

$$0 \to \mathbf{F}_p e \to E_p \xrightarrow{\pi} \mu_p \to 0$$

where μ_p is the group of pth root of unity and π is defined by:

$$\pi(x)=(e,x),$$

where $(\bullet,\bullet)$ is the Weil pairing. In fact π is a G-homomorphism and $\pi(e_1)$ is a primitive pth root of unity, say $\pi(e_1)=\zeta$. It is well-known that $L(\zeta)\subset M$.

LEMMA (2.3.7). *In the notation above, we have: either*

$$M=L(\zeta) \quad \text{or} \quad [M:L(\zeta)]=p.$$

Proof. Let $H=\mathrm{Gal}(M/L(\zeta))$ which is a subgroup of G. If $\tau\in H$ we have

$$\pi(e_1^\tau)=\pi(e_1)^{b(\tau)}=\tau(e_1)^\tau=\pi(e_1);$$

hence $b(\tau)=1$. Therefore $\rho(H)\subset A\subset \mathrm{GL}_2(\mathbf{F}_p)$, where

$$A=\left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}; *\in \mathbf{F}_p\right\}.$$

Since the cardinality of A is p and ρ is injective we must have either $\rho(H)=\{1\}$ or $\rho(H)=A$; hence either $M=L(\zeta)$ or $[M:L(\zeta)]=p$. □

To finish the proof of the second case of (2.3.3) we look at the following fields extension:

$$\begin{array}{c} M=Q(E_p) \\ | \\ L(\zeta)=Q(e,\zeta) \\ | \\ L=Q(e) \\ | \\ Q. \end{array}$$

By Proposition (2.3.1), $[M:Q]=p(p^2-1)(p-1)$ and by Lemma (2.3.6), $[L:Q]$ divides $(p-1)$. Now Lemma (2.3.7) clearly gives a contradiction. □

COROLLARY (2.3.8). *Let L be the Hilbert class field of K; then:*

$$E(L)_{\mathrm{tors}}=E(Q)_2\approx \mathbf{Z}/2\mathbf{Z}.$$

Proof. L/Q is finite Galois, this is well-known; moreover, L/Q is unramified at N because L/K is unramified anyway and N splits completely in K/Q (recall that $(l/N)=+1$). □

Next we sharpen another result of Kurchanov, in the case of the Neumann–Setzer curve.

THEOREM (2.3.9). *L being the Hilbert class field of K,* $\mathrm{rank}(E(L))>0$.

Proof. Suppose the contrary—that is, $E(L)$ is finite. By Corollary (2.3.8), $E(L)=E(Q)\approx \mathbf{Z}/2\mathbf{Z}$. Now theorem (2.1.1) implies that there exists an integer n_0 such that $E(L_{n_0})\neq E(Q)$. Let $M\in E(L_{n_0})$ and $M\notin E(Q)$, as observed in (2.2), M gives rise to a point R in $C(L_{n_0})$. Because of the isomorphism $C\approx C^{(-l)}$ over L_{n_0}, there exists a point P in $C^{(-l)}(L_{n_0})$—say $P=(a,b)$, a,b in L_{n_0}—and we have $-lb^2=a^4+ua^2-16$. But $[L_{n_0}:L]=l^{n_0}$ is odd and not equal to 3; by Heegner's lemma, there exists a point $P'=(c,d)$ in $C^{(-l)}(L)$, that is, $-ld^2=c^4+uc^2-16$. Again by the isomorphism $C\approx C^{(-l)}$—this time over L—there exists a point T in $C(L)$ (which is not at infinity). Now $T'=\psi(T)$ is a point on $E(L)$. If we use the model $y^2=x^3+ux^2-16x$ for E, then $T'=0$ or $T'=(0,0)$.

On the one hand, T' cannot be 0 since T is affine; on the other hand, if $T'=(0,0)$ then T would be one of $(0,\pm 4i)$. But i is not in L because the class number of K is odd; contradiction. Hence $\operatorname{rank}(E(L))>0$. □

(2.4). POINTS OF INFINITE ORDER ON $E(K)$. (Recall that the class number of K is odd.)

THEOREM (2.4.1). *Suppose that the class number of K is not equal to* 3; *then $E(K)$ has a point of infinite order.*

Proof. By Theorem (2.3.9), $E(L)$ has a point of infinite order, which gives rise to a point on $C^{(-l)}(L)$. Now we apply Heegner's lemma, because $[L:K]$ is odd ($l\equiv 3 \pmod 4$) and not equal to 3, to obtain a point on $C^{(-l)}(K)$. The image of the latter point under the maps $C^{(-l)}(K)\approx C(K)\xrightarrow{\psi} E(K)$ gives a point on $E(K)$ which is not in $E(Q)$ and hence of infinite order. □

3. Conclusions. We now give the main theorem of this note.

THEOREM (3.1.1). *Assume that the Neumann–Setzer curve E of conductor $N=u^2+64$ is a Weil curve. Let l be a prime such that $l\equiv 3$* (mod 4); *denote $K=Q(\sqrt{-l})$.*

(1) *If $(l/N)=+1$, $l>3$ and the class number of K is not equal to* 3, *then* $\operatorname{rank}(E(K))=1$ *and* $Ш(K)_2=0$.

(2) If $(l/N)=-1$ *then* $\operatorname{rank}(E(K))=0$ *and* $Ш(K)_2=0$. *In this case $E(K)=E(Q)$.*

Proof. Part (1) is a combination of Theorem (1.5.1) and Theorem (2.4.1). For part (2), we compute local indices; this gives: $i_N=0$, $i_l=1$, $i_\infty=1$, $i_p=0$ if $p\neq N,l,\infty$. The groups $\Phi=\mathrm{N}(S(K))=0$ as $l\equiv 3 \pmod 4$, hence the formula for the rank gives:

$$\operatorname{rank} E(K)+\dim Ш(K)_2=0,$$

hence part (2). □

We observe that if we decompose $E(K)$ into "plus" and "minus" eigenspaces, then the points of infinite order are in the "minus" part, and we have the following.

THEOREM (3.1.2). *With conditions as in Theorem* (3.1.1),

(1) *if $(l/N)=+1$, $l>3$ and the class number of K is not equal to* 3, *then the curve $E^{(-l)}: y^2=x^3-lux^2-16l^2x$ has a Mordell–Weil group of rank one over Q*;

(2) *if $(l/N)=-1$, $E^{(-l)}(Q)\approx \mathbf{Z}/2\mathbf{Z}$.* □

REMARK. Parts (1) of Theorem (3.1.1) and Theorem (3.1.2) should hold without the assumptions that $l>3$ or that the class number of K not be equal to 3.

4. Examples. For $N=73, 89, 113$ ($u=-3, 5, -7$), respectively) the corresponding Neumann–Setzer curves are known to be Weil curves (see [16]). More specifically let us take $N=113$, $u=-7$, $l=7$; then $(7/113)=1$, and the class number of $Q(\sqrt{-7})$ is one. If we write E as $y^2=x^3-7x^2-16x$, then $E(Q(\sqrt{-7}))$ has rank one and so does $E^{(-7)}(Q)$. The point $P=(4, 4\sqrt{-7})$ is a point of infinite order on $E(Q(\sqrt{-7}))$.

We finally remark that there are very special cases in which it is easy to obtain points of infinite order. Let N be a prime of the form p^2+64, where p itself is a prime congruent to 3 modulo 4 (e.g., $N=73, 113$); if we write the curve as $y^2=x^3+px^2-16x$, then in $E(Q(\sqrt{-p}))$ the points $(\pm 4, \pm 4\sqrt{-p})$ are of infinite order and so are the points $(\pm 4p, \pm 4p^2)$ on $E^{(-p)}(Q)$.

REFERENCES

1. B. J. Birch, *Diophantine analysis and modular functions.* Algebraic geometry (Bombay, 1968), 35–42, Oxford Univ. Press, London, 1969.
2. ———, *Elliptic curves and modular functions.* Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), 27–32, Academic Press, London, 1970.
3. A. Brumer, *Courbes modulaires,* notes rédigeés par D. Duval et R. Gillard, Grenoble, 1975.
4. A. Brumer and K. Kramer, *The rank of elliptic curves,* Duke Math. J. 44 (1977), 715–743.
5. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves,* J. London Math. Soc. 41 (1966), 193–291.
6. K. Heegner, *Diophantische Analysis und Modulfunktionen,* Math. Z. 56 (1952), 227–253.
7. K. Kramer, *Arithmetic of elliptic curves upon quadratic extension,* Trans. Amer. Math. Soc. 264 (1981), 121–135.
8. P. F. Kurchanov, *Elliptic curves of infinite rank over* Γ*-extensions,* Math. USSR-Sb. 19 (1973), 320–324.
9. B. Mazur, *Rational points of abelian varieties with values in towers of number fields,* Invent. Math. 18 (1972), 183–266.
10. B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil curves,* Invent. Math. 25 (1974), 1–61.
11. J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. 15 (1972), 259–331.
12. J. P. Serre and J. Tate, *Good reduction of abelian varieties,* Ann. of Math. 88 (1968), 492–517.
13. B. Setzer, *Elliptic curves of prime conductor,* J. London Math. Soc. (2) 10 (1975), 367–378.
14. J. Tate, *The arithmetic of elliptic curves,* Invent. Math. 23 (1974), 179–206.
15. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funkionalgleichungen,* Math. Ann. 168 (1967), 149–156.
16. *Modular functions of one variable,* Vol. IV, Lecture Notes in Math., 476, Springer, Berlin, 1975.

Department of Mathematics
Howard University
Washington, D.C. 20059