TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 264, Number 1, March 1981

ARITHMETIC OF ELLIPTIC CURVES UPON QUADRATIC EXTENSION

BY
KENNETH KRAMER[1]

ABSTRACT. This paper is a study of variations in the rank of the Mordell-Weil group of an elliptic curve E defined over a number field F as one passes to quadratic extensions K of F. Let $S(K)$ be the Selmer group for multiplication by 2 on $E(K)$. In analogy with genus theory, we describe $S(K)$ in terms of various objects defined over F and the local norm indices $i_v = \dim_{\mathbf{F}_2} E(F_v)/\mathrm{Norm}\{E(K_w)\}$ for each completion F_v of F. In particular we show that $\dim S(K) + \dim E(K)_2$ has the same parity as Σi_v. We compute i_v when E has good or multiplicative reduction modulo v. Assuming that the 2-primary component of the Tate-Shafarevitch group Ш(K) is finite, as conjectured, we obtain the parity of rank $E(K)$. For semistable elliptic curves defined over $\mathbf{Q}$ and parametrized by modular functions our parity results agree with those predicted analytically by the conjectures of Birch and Swinnerton-Dyer.

1. Introduction. Let E be an elliptic curve defined over a number field F. Our motivating question is this: What can be said about variations in the rank of the Mordell-Weil group $E(K)$ over quadratic extensions $K = F(d^{1/2})$? Let $E^{(d)}$ denote the twist of E which becomes isomorphic to E over K but not over F. Concretely, if we choose for E a model over F of the form $y^2 = f(x)$ then a model for $E^{(d)}$ is given by $dy^2 = f(x)$. If σ denotes the generator of $\mathrm{Gal}(K/F)$, then $E(F)$ can be identified with the $(+1)$-eigenspace and $E^{(d)}(F)$ with the (-1)-eigenspace of σ acting on $E(K)$. It follows that rank $E(K)$ = rank $E(F)$ + rank $E^{(d)}(F)$. An equivalent question therefore is to describe changes in the rank of $E^{(d)}(F)$ as d varies. For certain specific curves defined over $\mathbf{Q}$ this question has been discussed for example in [**1**], [**11**].

Let N: $E(K) \to E(F)$ be the norm mapping defined naively by $N(P) = P + P^\sigma$. Our starting point is to determine the dimension (as a vector space over $\mathbf{F}_2$) of the cokernel of its local counterpart N_w: $E(K_w) \to E(F_v)$ for each completion K_w of K. The results depend of course on the ramification in K_w over F_v and the type of reduction of E. We restrict our attention to semistable (i.e., good or multiplicative) reduction and, in case of residue characteristic 2, an unramified ground field F_v. These local calculations are of interest in themselves, and may be read independently. The situation for cases of additive reduction seems to be more complicated;

Received by the editors November 28, 1979; preliminary report presented to the Society April 20, 1979 under the title Elliptic Curves Over Quadratic Fields.

AMS (MOS) subject classifications (1970). Primary 14G25, 14K15, 14G20, 10B10.

Key words and phrases. Elliptic curve, quadratic extension, twist, Mordell-Weil group, Selmer group, Tate-Shafarevitch group, Birch and Swinnerton-Dyer conjecture, local norm index.

[1] Research partially supported by a grant from the National Science Foundation.

we hope to resolve it in the future. (See [**8**, §4] for a general discussion of local norm problems.)

The standard way to obtain at least a bound for the rank of $E(F)$ is by a descent [**6**, §23]. §3 below contains a review of this procedure, wherein one determines a finite group of exponent 2, the Selmer group $S(F)$, into which $E(F)/2E(F)$ injects. In §4 we use methods borrowed from genus theory of the ideal class groups of quadratic fields to relate $S(K)$, the Selmer group for $E(K)/2E(K)$, to $S(F)$. For example, we prove that if $S(F) = 0$ then $\dim S(K) = \Sigma_v i_v$ where $i_v = \dim E(F_v)/N\{E(K_w)\}$ is the local norm index as computed in §2.

In linking local information to global information we are led to consider a subgroup Φ of $S(F)$ consisting of those elements which are norms from $E(K_w)$ for all primes w of K (including Archimedean ones). The local/global norm group $\Phi/N\{S(K)\}$ does not seem to have been studied explicitly before. We prove in §5 that its dimension as a vector space over $\mathbf{F}_2$ is even by constructing a nondegenerate, strictly alternating bilinear form on it, related to the pairings [**6**, §26] on the Tate-Shafarevitch groups $Ш(F)_2$ and $Ш^{(d)}(F)_2$ of the curve E and its twist $E^{(d)}$. If $Ш(F)_2 = Ш^{(d)}(F)_2 = 0$ we prove that $\Phi/N\{S(K)\}$ is trivial; we also give an example in which it has dimension 2.

One of our general results is that rank $E(K)$ + dim $Ш(K)_2$ has the same parity as the sum of the local norm indices Σi_v. Using the conjectured finiteness of $Ш(K)$ to conclude that dim $Ш(K)_2$ is even [**6**, §26], and using the local calculations of §2, we obtain the parity of rank $E(K)$. For example, if E is a semistable curve of conductor N defined over $\mathbf{Q}$ and if $K = \mathbf{Q}(d^{1/2})$ then

$$(-1)^{\operatorname{rank} E(K)} = (-1)^b \chi_d(-N_1) \tag{1}$$

where χ_d is the quadratic character for K, N_1 is the product of primes dividing N which are unramified in K, and b is the number of primes p dividing N and ramified in K such that the tangent directions at the node of E modulo p are in $\mathbf{F}_p$. This agrees with the parity of rank predicted from the L-function of E by the conjectures of Birch and Swinnerton-Dyer if E is a modular curve. (See [**A-L**].)

Formula (1) can also be interpreted to yield the following analog of a conjecture formulated by Birch and Stephens [**12**, p. 30]. Let E be a semistable curve defined over $\mathbf{Q}$ and let $K = \mathbf{Q}(d^{1/2})$. Let t be the number of primes w of K such that E has a node modulo w at which the tangent directions are in the residue field $k(w)$. If $Ш(K)$ is finite then

$$(-1)^{\operatorname{rank} E(K)} = (-1)^t \cdot (\operatorname{sign} d).$$

Finally, we remark on the case in which F is a function field of transcendence degree one over a finite constant field. If $\operatorname{char}(F) \neq 2$ the results of this paper are valid as proved once one checks that Lemma 6.2 of [**4**] holds. In particular, the finiteness of $Ш(K)$ implies that rank $E(K)$ has the same parity as the sum of the local norm indices, and these are as computed in §2 for places of good or multiplicative reduction. Of course one must omit factors $\chi_d(-1)$ or $\operatorname{sign}\{N_{F/\mathbf{Q}}d\}$ corresponding to Archimedean primes in Corollaries 1 and 2.

It is a pleasure to thank Armand Brumer for many important suggestions used in this work. I also wish to thank Winnie Li for valuable discussions about the sign in the functional equation of an L-function arising from a twist of a modular form.

2. The cokernel of the local norm. Throughout this section, F is a finite extension of $\mathbf{Q}_p$ and its valuation v is written additively. E is an elliptic curve defined over F, with an integral model whose discriminant Δ has minimal valuation. We consider those $d \in F$ for which $K = F(d^{1/2})$ is a quadratic extension of F. The cokernel of the local norm mapping N: $E(K) \to E(F)$ is a finite vector space over $\mathbf{F}_2$ whose dimension we denote by $i(K/F)$. We shall often express $i(K/F)$ in terms of the Hilbert norm-residue symbol, a bimultiplicative form $(\ ,\ )_F$: $F^* \times F^* \to \mu_2$ whose properties are described in [9, pp. 212–220].

If K over F is unramified and E has good reduction then $i(K/F) = 0$ according to [8, Corollary 4.2]. To treat the case of multiplicative reduction we recall the following information. If E is a Tate curve [7, p. 197] over F, then there is an element q in F with

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

such that E is isomorphic to $\mathbf{G}_m/q^{\mathbf{Z}}$ via a parametrization by p-adic theta functions. If E is *twisted* by the quadratic extension L, then E becomes isomorphic to $\mathbf{G}_m/q^{\mathbf{Z}}$ over any field containing L. However, if the field M contains F but not L, then $E(M)$ is isomorphic to $I(M)/q^{\mathbf{Z}}$ where $I(M) = \{z \in ML | N_{ML/M} z \in q^{\mathbf{Z}}\}$. In that case, the connected component of the identity in the Neron model of E corresponds to

$$I_0(M) = \{z \in ML | N_{ML/M} z = 1\}.$$

PROPOSITION 1. *Suppose that E is a Tate curve. Then $i(K/F)$ is* 0 *or* 1, *according to whether* $(\Delta, d)_F$ *is* -1 *or* $+1$.

PROOF. From the explicit formulas for parametrization by p-adic theta functions [7, p. 197] one sees that the norm mapping on E corresponds to field-theoretic norm modulo $q^{\mathbf{Z}}$. Thus $E(F)/N\{E(K)\} = F^*/(NK^*)q^{\mathbf{Z}}$. By local class field theory, $i(K/F)$ therefore is at most 1, and $i(K/F) = 1$ precisely when $q \in NK^*$, or equivalently when $(\Delta, d)_F = +1$. Here and again later on we use the fact that Δq^{-1} is a square in F.

PROPOSITION 2. *Suppose that E is a twisted Tate curve, twisted by the unramified quadratic extension L.*

(a) *If K is unramified over F, then $i(K/F)$ is* 0 *or* 1 *according to whether $v(\Delta)$ is odd or even.*

(b) *If K is ramified over F, then*

$$i(K/F) = \begin{cases} 0 & \textit{if } (\Delta, d)_F = +1 \textit{ and } v(\Delta) \textit{ odd}, \\ 1 & \textit{if } (\Delta, d)_F = -1, \\ 2 & \textit{if } (\Delta, d)_F = +1 \textit{ and } v(\Delta) \textit{ even}. \end{cases}$$

Proof. In case (a) we have the commutative square:

$$\begin{tikzcd}
E(K) \arrow[r, "\sim"] \arrow[d, "N"'] & K^*/q^{\mathbf{Z}} \arrow[d] \\
E(F) \arrow[r, "\sim"] & I(F)/q^{\mathbf{Z}}
\end{tikzcd}$$

If we denote the generator of $\mathrm{Gal}(K/F)$ by σ, then the vertical arrow on the right is induced by $z \to z^{1-\sigma}$ because of the twist. Using Hilbert's Theorem 90 one sees that $E(F)/N\{E(K)\}$ is isomorphic to $I(F)/I_0(F)q^{\mathbf{Z}}$, which clearly has the dimension specified in (a).

In case (b), letting U denote units and letting τ be the generator of $\mathrm{Gal}(L/F)$, we have the exact commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & U_K \arrow[r] \arrow[d, "N"'] & U_{KL} \arrow[r, "f"] \arrow[d, "N"'] & E_0(K) \arrow[r] \arrow[d, "N"'] & 0 \\
0 \arrow[r] & U_F \arrow[r] & U_L \arrow[r, "f"'] & E_0(F) \arrow[r] & 0
\end{tikzcd}$$

Here the norm on U is the field-theoretic norm, and we have identified E_0 with I_0, so that the map f is induced by $z \to z^{1-\tau}$. We obtain the exact sequence of cokernels

$$U_F/NU_K \xrightarrow{g} U_L/NU_{KL} \xrightarrow{\bar{f}} E_0(F)/N\{E_0(K)\} \to 0. \tag{2}$$

Now by naturality properties of the Hilbert symbol, if $x \in F$, then $(x, d)_L = (N_{L/F}x, d)_F = (x^2, d)_F = 1$. Hence any element of F, when lifted to L, becomes a norm from KL to L. Therefore in (2), the map g is 0 and $\bar{f}$ is an isomorphism. Since KL over L is ramified, the dimension of $E_0(F)/N\{E_0(K)\}$ therefore is 1.

Let us denote by $P(z)$ the point in $E(K)$ parametrized by the element z in KL such that $N_{KL/K}z = q^e$. Then $N\{P(z)\} = P(y)$, where $y = N_{KL/L}z$. Now $P(y) = P(yq^{-e})$ and yq^{-e} lies in $I_0(F)$. Hence $N\{E(K)\}$ is contained in $E_0(F)$.

Since K over F is ramified while KL over K is unramified, q becomes a norm from KL to K. Say $q = N_{KL/K}z$. Clearly the group $E(K)/E_0(K)$ has order 2 and is generated by $P(z)$. We have therefore shown that

$$i(K/F) = \dim E(F)/E_0(F) + \begin{cases} 0 & \text{if } N\{P(z)\} \notin N\{E_0(K)\}, \\ 1 & \text{if } N\{P(z)\} \in N\{E_0(K)\}. \end{cases}$$

Now $\dim E(F)/E_0(F)$ is 0 or 1 according to whether $v(\Delta)$ is odd or even. To complete the proof of part (b) we therefore need to show that $N\{P(z)\}$ is in $N\{E_0(K)\}$ if and only if $(\Delta, d)_F = (-1)^{v(\Delta)}$. We do this in the following tedious but straightforward calculation, in which the underlying idea is to make an explicit choice for z and use the isomorphism $\bar{f}$ of (2). There is a somewhat simpler calculation when the residue characteristic of F is not 2, but we give a uniform argument.

Let π_K be a prime for K and $N_{K/F}\pi_K = \pi_F$ a prime for F. Then there is a unit $a \in F$ such that $q = a\pi_F^n$. Since L over F is unramified, there is a unit b of L such that $N_{L/F}b = a$ and a unit c of KL such that $N_{KL/K}c = \pi_K^{\sigma-1}$. Let $x = N_{KL/L}c$. By Hilbert's Theorem 90 we have $x = y^{1-\tau}$ for some unit y in L.

If we let $z = b(c\pi_K)^n$ then $N_{KL/K}z = q$. Also,

$$N_{KL/L}z = b^2(x\pi_F)^n = b^2x^nqa^{-1} = b^{1-\tau}(y^n)^{1-\tau}q.$$

Using the isomorphism $\bar{f}$ in (2) it follows that $N\{P(z)\} = P(N_{KL/L}z)$ is in $N\{E_0(K)\}$ if and only if by^n is a norm from KL to L, or equivalently $(by^n, d)_L = 1$. We now proceed to evaluate this Hilbert symbol.

First we show that $(y, d)_L = -1$. Otherwise we could write y as a norm, say $y = N_{KL/L}w$. But then $N_{KL/L}(cw^{\tau-1}) = 1$ so that $c = w^{1-\tau}u^{\sigma-1}$ for some u in KL. Taking norms from KL to K we find that $\pi_K^{\sigma-1} = N_{KL/K}c = (N_{KL/K}u)^{\sigma-1}$. Therefore $\pi_K = (N_{KL/K}u) \cdot$ (element of F). But the right side of this equation has even valuation in K, a contradiction.

Hence $(y, d)_L = -1$. Since π_F was arranged to be a norm from K, we have $(\pi_F, d)_F = 1$. Hence

$$\begin{aligned}(by^n, d)_L &= (b, d)_L(-1)^n = (N_{L/F}b, d)_F(-1)^{v(q)} = (a, d)_F(-1)^{v(q)}\\ &= (q, d)_F(-1)^{v(q)} = (\Delta, d)_F(-1)^{v(\Delta)}.\end{aligned}$$

Now by our previous discussion, $N\{P(z)\}$ is in $N\{E_0(K)\}$ if and only if $(\Delta, d)_F = (-1)^{v(\Delta)}$, as desired.

PROPOSITION 3. *Suppose that K over F is a ramified extension with residue field k having odd characteristic. If E has good reduction modulo π_F then $i(K/F) = \dim \bar{E}(k)_2$. Moreover $i(K/F)$ is even or odd according to whether $(\Delta, d)_F = \pm 1$.*

PROOF. Let E_1 denote the kernel of reduction. Then by [**8**, Corollary 4.6] there is an exact sequence

$$E_1(F)/N\{E_1(K)\} \xrightarrow{f} E(F)/N\{E(K)\} \to \bar{E}(k)/2\bar{E}(k) \to 0. \tag{3}$$

Since $E_1(F)$ is uniquely divisible by 2 via [**15**, p. 189] and $N \circ$ (inclusion) is multiplication by 2, the left-hand group in (3) is trivial and $i(K/F) = \dim \bar{E}(k)/2\bar{E}(k) = \dim \bar{E}(k)_2$. It is clear for example by [**9**, p. 305] that $\dim \bar{E}(k)_2$ is even if and only if, upon reduction, Δ becomes a square in k, or equivalently $(\Delta, d)_F = 1$.

We now restrict our attenton to ground fields F with residue characteristic 2, and elliptic curves E with *good reduction*. We make the simplifying assumption that F is *unramified* over $\mathbf{Q}_2$. Suppose that E has minimal model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4}$$

and discriminant Δ. Let $E_n(F)$ consist of the point at infinity and those (x, y) in $E(F)$ for which $v(x) \leqslant -2n$. There is a formal group law for addition on the maximal ideal $\mathfrak{p}_F$ giving rise to an isomorphism $\mathfrak{p}_F \xrightarrow{\sim} E_1(F)$ which we denote by $z \to P(z)$. Then $P(z_1) + P(z_2) = P(z_3)$ with

$$\begin{aligned}z_3 = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - 2a_3(z_1^3z_2 + z_1z_2^3)\\ + (a_1a_2 - 3a_3)z_1^2z_2^2 + (\text{degree} \geqslant 5).\end{aligned} \tag{5}$$

(See [**15**, §3].)

We may assume that $K = F(d^{1/2})$ is a *ramified* extension of F; otherwise, $i(K/F) = 0$. The injection $E(F)/E_1(F) \to E(K)/E_1(K)$ then is onto, since both sides are isomorphic to $\bar{E}(k)$ via the reduction map. Hence $E(K) = E(F) + E_1(K)$ and $N\{E(K)\} = 2E(F) + N\{E_1(K)\}$. It follows that for the map f in exact sequence (3) we have

$$\operatorname{kernel} f = (E_1(F) \cap 2E(F))/(N\{E_1(K)\} \cap 2E(F)). \tag{6}$$

PROPOSITION 4. *Assume that F is an unramified extension of $\mathbf{Q}_2$ and that K over F is ramified. If E has supersingular reduction modulo 2 then*

$$i(K/F) = \begin{cases} 0 & \text{if } v(d) \text{ is even,} \\ [F: \mathbf{Q}_2] & \text{if } v(d) \text{ is odd.} \end{cases}$$

Moreover, $i(K/F)$ is even or odd according to whether $(\Delta, d)_F = \pm 1$.

PROOF. Supersingular reduction forces $E(F)/E_1(F) \simeq \bar{E}(k)$ to have odd order. Therefore the map f in (3) is surjective and furthermore, $E_1(F) \cap 2E(F) = 2E_1(F)$, so that f is injective by (6). Hence $i(K/F) = \dim E_1(F)/N\{E_1(K)\}$, which we now evaluate.

Since the formal group law (5) has height 2, the coefficient a_1 is divisible by the prime element 2 of F. By a suitable translation we can therefore arrange for $a_1 = a_2 = 0$ in the minimal model (4). Using (5), the formal group multiplication then looks like $\psi_2(z) = 2z + (\text{degree} \geqslant 4)$, from which it is clear that $E_2(F) = 2E_1(F)$.

It is easy to check that the following diagram is commutative.

$$\begin{tikzcd} E_1(K)/E_2(K) \arrow[r, "\sim"] \arrow[d, "N"'] & \mathfrak{p}_K/\mathfrak{p}_K^2 \arrow[d, "\mathrm{tr}"] \\ E_1(F)/E_2(F) \arrow[r, "\sim"] & \mathfrak{p}_F/\mathfrak{p}_F^2 \end{tikzcd}$$

where the formal group law on $\mathfrak{p}/\mathfrak{p}^2$ reduces to ordinary addition and the vertical arrow on the right is induced by trace.

Since $E_2(F)$ is contained in $N\{E_1(K)\}$ we find that $E_1(F)/N\{E_1(K)\}$ is isomorphic to the cokernel of tr. If $v(d)$ is even tr is surjective; hence $i(K/F) = 0$. If $v(d)$ is odd tr is the 0-map; hence $i(K/F) = \dim \mathfrak{p}_F/\mathfrak{p}_F^2 = [F: \mathbf{Q}_2]$.

As for the parity of $i(K/F)$, the explicit formula given in [**15**, p. 180] for Δ in terms of the coefficients of the model (4) shows that Δ is in $-3 \cdot F^2$. If $v(d)$ is even, then $(\Delta, d)_F = 1$. If $v(d)$ is odd, then $(\Delta, d)_F = 1$ precisely when -3 is a square in F, or equivalently $[F: \mathbf{Q}_2]$ is even.

To treat the case of ordinary reduction modulo 2 we shall use the following lemma. Since the formal group law for multiplication by 2 is to have height 1, the coefficient a_1 in (5) is a unit. By suitable translation we arrange for a minimal model (4) with $a_1 = -1$ and $a_3 = 0$.

Lemma 1. *The following diagram is commutative, where the horizontal arrows are induced by* $P(z) \to 1 + z - a_2z^2$:

$$\begin{tikzcd}
 & E_1(K) \arrow[r, "g_K"] \arrow[d, "N"'] & U_K/U_K^2 \arrow[r] \arrow[d, "N"] & 0 \\
0 \arrow[r] & E_1(F)/2E_1(F) \arrow[r, "g_F"] & U_F/U_F^2 \arrow[r] & 0
\end{tikzcd}$$

Proof. One uses (tedious) direct computation involving the formal group law (5) with $a_1 = -1$, $a_3 = 0$, and the information that $1 + \mathfrak{p}_K^5 \subset U_K^2$ and $1 + \mathfrak{p}_F^3 \subset U_F^2$, to show that the horizontal arrows are homomorphisms and to check commutativity. The surjectivity of the g's is clear and injectivity of g_F results from direct computation.

Proposition 5. *Assume that F is an unramified extension of $\mathbf{Q}_2$ and that K over F is ramified. If E has ordinary good reduction modulo* 2 *then $i(K/F)$ is* 2 *or* 1 *according to whether* $(\Delta, d)_F = \pm 1$.

Proof. By Lemma 1, $E_1(F)/N\{E_1(K)\}$ is isomorphic to U_F/NU_K so has dimension 1. Since E is ordinary modulo 2, the reduction $\bar{E}$ already has a point of order 2 over $\mathbf{F}_2$. Hence $\bar{E}(k)/2\bar{E}(k)$ is 1 dimensional. We show below that the group in (6) is trivial if and only if $(\Delta, d)_F = 1$, so that $i(K/F)$ is as desired, using exact sequence (3).

Suppose first that Δ is a square in F. Since $E_1(F)$ contains a unique point of order 2 by [**2**, Lemma 3.5], there must also be another point of order 2, say P_0, in $E(F) - E_1(F)$. Since the 2-Sylow subgroup of $E(F)/E_1(F) \simeq \bar{E}(k)$ is cyclic, P_0 generates $\{E(F)/E_1(F)\}_2$. Then clearly $E_1(F) \cap 2E(F) = 2E_1(F)$ and the group in (6) is trivial while $(\Delta, d)_F = 1$.

Suppose next that Δ is not a square in F. By [**2**, §2] there is an injection $\lambda\colon E(F)/2E(F) \to H^1(\mathrm{Gal}(\bar{F}/F), E(\bar{F})_2)$ in which this cohomology group H^1 is isomorphic to $F(\Delta^{1/2})^*/F(\Delta^{1/2})^{*2}$. Moreover, by [**2**, Lemma 3.5] the map λ when restricted to $E_1(F)$ has the form $\lambda\{P(z)\} = \text{coset}\{1 + z - a_2z^2\}$. Find a unit u in F such that in the residue field k we have $\bar{\Delta} = \bar{u}^2$, and solve for z_0 such that $1 + z_0 - a_2z_0^2 \equiv \Delta u^{-2}$ modulo $\mathfrak{p}_F^3$. Then $P(z_0)$ is in $2E(F)$ but not in $2E_1(F)$, since $\Delta \notin F^2$. Now by the isomorphism $E_1(F)/N\{E_1(K)\} \xrightarrow{\sim} U_F/NU_K$ coming from Lemma 1 we see that $P(z_0)$ is in $N\{E_1(K)\}$, or equivalently, the group in (6) is trivial, if and only if $(\Delta, d)_F = 1$.

Proposition 6. *For Archimedean primes $i(\mathbf{C}/\mathbf{R})$ is* 0 *or* 1 *according to whether Δ is negative or positive.*

Proof. Since $E(\mathbf{C}) = 2E(\mathbf{C})$ we find that $N\{E(\mathbf{C})\} = 2E(\mathbf{R})$. Hence $i(\mathbf{C}/\mathbf{R}) = \dim E(\mathbf{R})/2E(\mathbf{R})$, which is as given above, say by [**2**, Proposition 3.7].

We cull from the above propositions the following results on the parity of $i(K/F)$. Consistent with later usage, we say $i(K/F) = 0$ if d is in F^2. We let Δ denote the discriminant of E and π_F a prime in F. In case of multiplicative reduction we must distinguish between a Tate curve, for which the tangent directions at the node on the reduction of E are in the residue field of F, and a twisted Tate curve, for which those directions lie in an unramified quadratic extension of the residue field.

$$(-1)^{i(K/F)} = \begin{cases} (\Delta\pi_F, d)_F & \text{if } E \text{ has multiplicative reduction} \\ & \text{and } K/F \text{ is unramified,} \\ -(\Delta, d)_F & \text{if } E \text{ is a Tate curve over } F \text{ and} \\ & K/F \text{ is ramified,} \\ (-\Delta, d)_F & \text{if } F = \mathbf{R}, \\ (\Delta, d)_F & \text{otherwise.} \end{cases}$$

We close this section by giving a global version of the above parity results. Suppose that F is a number field and $K = F(d^{1/2})$ for some $d \in F$. We define a quadratic character χ_d on the free abelian group generated by -1 and the non-Archimedean primes π of F which are unramified in K by

$$\chi_d(-1) = \prod_{v|\infty} (-1, d)_v = \operatorname{sign} N_{F/\mathbf{Q}} d,$$

$$\chi_d(\pi) = (\pi, d)_\pi = \begin{cases} +1 & \text{if } \pi \text{ splits in } K, \\ -1 & \text{if } \pi \text{ inert in } K. \end{cases}$$

COROLLARY 1. *Suppose that F is a number field in which 2 does not ramify, and that $K = F(d^{1/2})$. Let E be a semistable curve defined over F. Let $i_v = \dim E(F_v)/N\{E(K_w)\}$ be the local norm index at the completion F_v of F, with the convention that $i_v = 0$ if v splits in K. Let N_1 be the symbolic product of the primes of F which are unramified in K and at which E has bad reduction. Let b be the number of primes of F which are ramified in K and at which E is a Tate curve. Then*

$$(-1)^{\Sigma i_v} = (-1)^b \chi_d(-N_1).$$

Let t be the number of primes w of K at which E is a Tate curve over K_w. Then

$$(-1)^{\Sigma i_v} = \operatorname{sign}\{N_{F/\mathbf{Q}} d\} \cdot (-1)^t.$$

PROOF. To obtain the first formula, we multiply the parity of local norm indices given in terms of Hilbert symbols above, and note that $\Pi_v(\Delta, d)_v = 1$ by reciprocity. To obtain the second formula, we use the fact that if E has multiplicative reduction at the prime v of F and E is not already a Tate curve over F_v, then E becomes a Tate curve over K_w, where $w|v$, if and only if v is inert in K.

3. A review of descent and related dualities. For the moment, let E be an elliptic curve defined over a field F of characteristic not 2. We use Galois cohomology with the notation $H^*(F, E_2)$ for $H^*(\mathrm{Gal}(\bar{F}/F), E(\bar{F})_2)$. From the cohomology of the short exact sequence $0 \to E(\bar{F})_2 \to E(\bar{F}) \xrightarrow{2} E(\bar{F}) \to 0$ one sees that there is an injection

$$\lambda_F \colon E(F)/2E(F) \to H^1(F, E_2). \tag{7}$$

Suppose now that F is a number field. If F_v denotes the completion of F at the prime v, then the *local Selmer group* $S(F_v)$ is defined to be the image of λ_{F_v} and is of course isomorphic to $E(F_v)/2E(F_v)$. The *global Selmer group* is defined to be

$$S(F) = \{s \in H^1(F, E_2) | s \in S(F_v) \text{ for all } v\}$$

and is a finite vector space over $\mathbf{F}_2$. Letting $\text{Ш}(F)$, the Tate-Shafarevitch group, be the kernel of $H^1(F, E) \to \Pi_v H^1(F_v, E)$ we have the exact sequence $0 \to E(F)/2E(F) \to S(F) \to \text{Ш}(F)_2 \to 0$.

We recall from local duality theory [13] that $S_v = S(F_v)$ is its own orthogonal complement in the perfect pairing

$$h_v\colon H^1(F_v, E_2) \times H^1(F_v, E_2) \to \mu_2$$

given by cup-product followed by invariant. Let F_v^{unr} be the maximal unramified extension of F_v and let $\mathbf{H} = \Pi H^1(F_v, E_2)$ be the restricted direct product with respect to $H^1(\text{Gal}(F_v^{\text{unr}}/F_v), E(F_v^{\text{unr}})_2)$. There is a global perfect pairing (using [4, Lemma 6.2], but note correction in [5, Appendix 2])

$$h_F\colon \mathbf{H}/\left\{H^1(F, E_2)\cdot \Pi S_v\right\} \times S \to \mu_2$$

with h_F being the product of the local h_v's and $H^1(F, E_2)$ being embedded in the diagonal of $\mathbf{H}$.

There is an alternating bimultiplicative form ([4, Theorem 1.1] or [14, Theorem 3.2]) on the Tate-Shafarevitch group $\text{Ш}(F)$, which becomes nondegenerate modulo the (conjecturally trivial) divisible subgroup of Ш. For our purposes, we need only to know that the following construction provides us with an alternating form on $\text{Ш}(F)_2$ with values in μ_2. Let

$$\gamma_F\colon E(F)/4E(F) \to H^1(F, E_4) \tag{8}$$

be the connecting homomorphism obtained from the cohomology of the short exact sequence $0 \to E(\bar{F})_4 \to E(\bar{F}) \xrightarrow{4} E(\bar{F}) \to 0$. From the cohomology of $0 \to E(\bar{F})_2 \to E(\bar{F})_4 \xrightarrow{2} E(\bar{F})_2 \to 0$ we get the exact sequence

$$E(F)_2 \xrightarrow{\lambda_F} H^1(F, E_2) \to H^1(F, E_4) \xrightarrow{2^*} H^1(F, E_2). \tag{9}$$

Then $2^*\gamma_F = \lambda_F$, with λ_F as in (7).

Given $a \in S(F)$ there exists for each prime v of F a point $P_v \in E(F_v)$ such that $a = \lambda_v(P_v) = 2^*\gamma_v(P_v)$. It follows from Tate's Lemma [4, Lemma 6.1] that globally $a = 2^*c$ for some $c \in H^1(F, E_4)$. Since $c - \gamma_v(P_v)$ is killed by 2^*, we may view $c - \gamma_v(P_v)$ as an element of $H^1(F_v, E_2)$ by (9). Given $b \in S(F)$, let $T(a, b) = h_F(c - \gamma_v(P_v), b)$.

THEOREM ([4, THEOREM 1.1], [14, THEOREM 3.2]). *The bilinear form* $T\colon S(F) \times S(F) \to \mu_2$ *is well defined and strictly alternating in the sense that* $T(a, a) = 1$. *It induces a nondegenerate pairing on* $\text{Ш}(F)_2/2\text{Ш}(F)_4$.

Next we examine the effects on these pairings of passing to a Galois extension K over F. It is convenient to collect together the local Selmer groups at all the primes of K lying over a fixed prime v of F, and to denote with a dash those objects with ground field K. Thus $S_v = S(F_v)$. $S'_v = \Pi_{w|v} S(K_w)$, $S = S(F)$ and $S' = S(K)$.

It follows from the diagram below (commutative if one uses only the restriction maps or only the corestrictions) that $N_v(S'_v) \subseteq S_v$ and $i_v(S_v) \subseteq S'_v$. Hence also globally $N(S') \subseteq S$ and $i(S) \subseteq S'$.

$$\begin{tikzcd}
0 \arrow[r] & \prod_{w|v} E(K_w)/2E(K_w) \arrow[r, "\lambda'_v"] \arrow[d, shift right] & \prod_{w|v} H^1(K_w, E_2) \arrow[r] \arrow[d, shift right, "N_v"'] & \prod_{w|v} H^1(K_w, E) \arrow[d, shift right] \\
0 \arrow[r] & E(F_v)/2E(F_v) \arrow[r, "\lambda_v"] \arrow[u, shift right, dashed] & H^1(F_v, E_2) \arrow[r] \arrow[u, shift right, dashed, "i_v"'] & H^1(F_v, E) \arrow[u, shift right, dashed]
\end{tikzcd} \tag{10}$$

Let $i_v^{-1}(S_v') = \{s \in H^1(F_v, E_2) | i_v(s) \in S_v'\}$ and globally let $i^{-1}(S') = \{s \in H^1(F, E_2) | i(s) \in S'\}$. By naturality properties of cup-product with respect to restriction and corestriction [3, Chapter XII, §8] we obtain from the pairing h_v the perfect pairing $\bar{h}_v$: $i_v^{-1}(S_v')/S_v \times S_v/NS_v' \to u_2$. The implications of this on the global pairing h_F are given in the following lemma.

Lemma 2. *Let $\Phi = \{s \in S | s \in N_v S_v'$ for all $v\}$. The orthogonal complement of Φ in the pairing h_F is $H^1(F, E_2) \cdot \Pi i_v^{-1}(S_v')$ modulo $H^1(F, E_2) \cdot \Pi S_v$ and is isomorphic to*

$$A = \prod i_v^{-1}(S_v') / \left\{ i^{-1}(S') \cdot \prod S_v \right\}.$$

Proof. An element $s \in S$ is orthogonal to $\Pi i_v^{-1}(S_v')$ in the pairing h_F if and only if for each prime v we have $\bar{h}_v(t, s) = 1$ for all $t \in i_v^{-1}(S_v')$; that is, if and only if for each v, $s \in N_v S_v'$ by the nondegeneracy of $\bar{h}_v$. Thus $\Phi^\perp = H^1(F, E_2) \cdot \Pi i_v^{-1}(S_v')$ modulo $H^1(F, E_2) \cdot \Pi S_v$ and is isomorphic to A by elementary isomorphism theorems.

4. The Selmer group $S(K)$. We continue to assume that E is an elliptic curve defined over a number field F and that $K = F(d^{1/2})$ is a quadratic extension with $G = \mathrm{Gal}(K/F)$ generated by σ. At each completion F_v of F we denote the local Selmer group $S(F_v)$ by S_v. For completions of K we write $S_v' = \Pi_{w|v} S(K_w)$. Also, $S = S(F)$ and $S' = S(K)$. Let $i_v = i(K_w/F_v)$ be the local norm index as computed in §2. By the perfect pairing $\bar{h}_v$ and the fact that $N\{E(K_w)\} \supseteq 2E(F_v)$ we have

$$i_v = \dim E(F_v)/N\{E(K_w)\} = \dim S_v/N_v S_v' = \dim i_v^{-1}(S_v')/S_v. \tag{11}$$

In the exact sequences used to prove the following theorem, we relate S' to various objects defined over F, namely the "ambiguous Selmer elements" of S' given by

$$i^{-1}(S') = \left\{ s \in H^1(F, E_2) | i(s) \in S' \right\},$$

the everywhere-local norms from S_v' given by

$$\Phi = \{ s \in S | s \in N_v S_v' \text{ for all } v \},$$

and the global norms, NS'.

Theorem 1. *The rank of $E(K)$ is $\Sigma i_v + \dim \Phi + \dim NS' - 2 \dim E(F)_2 - \dim$ Ш$(K)_2$. rank $E(K)$ has the same parity as $\Sigma i_v + \dim$ Ш$(K)_2$.*

Proof. From Lemma 3 below we deduce that the sequence

$$0 \to E(F)_2/N\{E(K)_2\} \xrightarrow{\alpha} i^{-1}(S') \xrightarrow{i} S' \xrightarrow{N} NS' \to 0 \tag{12}$$

is exact. Let ^ denote Pontrjagen dual. It follows from Lemma 2 of §3 that the cokernel of f is $(S/\Phi)^\wedge$, and the rest is clear in the exact sequence

$$0 \to S \to i^{-1}(S') \xrightarrow{f} \prod i_v^{-1}(S_v')/S_v \to (S/\Phi)^\wedge \to 0. \tag{13}$$

We also have the exact sequence $0 \to E(F)_2 \to E(K)_2 \xrightarrow{N} N\{E(K)_2\} \to 0$. Taking Euler characteristics and using (11) we obtain the claimed formula for rank $E(K)$ upon noting that $\dim S' = \text{rank}\, E(K) + \dim E(K)_2 + \dim Ш(K)_2$. The parity statement follows from the fact that $\dim \Phi/NS'$ is even, as we show in Theorem 2 of §5.

COROLLARY 2. *Assume finiteness of the 2-primary component of* Ш(K), *as conjectured. Under the hypotheses and in the notation of Corollary* 1

$$(-1)^{\text{rank}\, E(K)} = (-1)^b \chi_d(-N_1) = \text{sign}\{N_{F/\mathbf{Q}}d\} \cdot (-1)^t.$$

REMARK. If $S = 0$ then its subgroups Φ and NS' also are trivial. Moreover, since $E(F)/2E(F)$ injects into S, it follows that $E(F)_2 = 0$. By exact sequence (12), S' then is isomorphic to the ambiguous Selmer elements $i^{-1}(S')$. Furthermore, $\dim S' = \sum i_v$, the sum of the local norm indices, each of which is zero except possibly if E has bad reduction or K over F is ramified at v. We therefore have an analog of genus theory for elements of order 2 in the ideal class group of a quadratic extension of a field with odd class number.

In a Weierstrass model $y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$ for E the points of order 2 have the form $P = (t, 0)$ where $f(t) = 0$. A model for the twisted curve $E^{(d)}$ is given by $y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6$. We identify E_2 with $E_2^{(d)}$ and thus also $H^*(F, E_2)$ with $H^*(F, E_2^{(d)})$ via the Galois isomorphism $P \to P^{(d)} = (dt, 0)$.

LEMMA 3. *Let F be any field whose characteristic is not* 2. *The following sequence is exact, with i being restriction, N corestriction, and* $\alpha = \lambda_F \cdot \lambda_F^{(d)}$ *where* λ_F *and* $\lambda_F^{(d)}$ *are the homomorphisms of* (7) *for the curves E and* $E^{(d)}$ *respectively*:

$$0 \to E(F)_2/N\{E(K)_2\} \xrightarrow{\alpha} H^1(F, E_2) \xrightarrow{i} H^1(K, E_2) \xrightarrow{N} H^1(F, E_2).$$

PROOF. By inflation-restriction we obtain the exact sequence

$$0 \to H^1(G, E(K)_2) \xrightarrow{\alpha} H^1(F, E_2) \xrightarrow{i} H^1(K, E_2).$$

Since $1 - \sigma = 1 + \sigma$ on $E(K)_2$ it follows from the cohomology of cyclic groups that $H^1(G, E(K)_2)$ is isomorphic to $E(F)_2/N\{E(K)_2\}$. Making this identification and tracing through the maps in terms of cochains one sees that $\alpha(P) = \lambda(P) \cdot \lambda^{(d)}(P^{(d)})$ for P in $E(F)_2$.

$H^1(F, E_2)$ is killed by 2, so that $N \circ i$ is trivial. Suppose that E is given by a Weierstrass model $y^2 = f(x)$, and let A_F be the F-algebra $F[T]/(f(T))$. View A_F as a direct sum of fields according to the number of roots of $f(T) = 0$ in F. Recall [2, §2] that $H^1(F, E_2)$ is isomorphic to the multiplicative group of elements of $\bar{A}_F = A_F^*/A_F^{*2}$ whose norms to F^*/F^{*2} are trivial. Suppose that $x \in A_K^*$ represents an element $\bar{x}$ of $\bar{A}_K$ whose norm to K^*/K^{*2} is trivial and such that $N_{\bar{A}_K/\bar{A}_F}\bar{x} = 1$. Then there is $a \in A_F^*$ such that $N_{A_K/A_F}xa^{-1} = 1$. Using Hilbert's Theorem 90 we can write $x = az^{\sigma-1}$ for some $z \in A_K^*$. Let $b = N_{A_K/A_F}z$ and let c be the image of $N_{A_F/F}(ab)$ under the natural inclusion from F to A_F. Since norm composed with this inclusion is cubing, $N_{A_F/F}(abc)$ is in F^2. Moreover, $N_{A_K/K}(ab) = N_{A_K/K}(xz^2)$ is a square in K. Hence c becomes a square in A_K and $x \equiv abc$ (modulo A_K^{*2}). Therefore $\bar{x} = i(\overline{abc})$ and we have exactness around $H^1(K, E_2)$.

5. The everywhere-local/global norm group Φ/NS'. In this section, we attempt to treat symmetrically both the curve E and its twist $E^{(d)}$. We continue to identify the Galois-isomorphic modules E_2 and $E_2^{(d)}$. Let $S_v^{(d)} \simeq E^{(d)}(F_v)/2E^{(d)}(F_v)$ be the local Selmer group for $E^{(d)}$ at the prime v, and let $S^{(d)}$ be the global Selmer group for $E^{(d)}$.

PROPOSITION 7. *Locally, $i_v^{-1}(S_v') = S_v \cdot S_v^{(d)}$ and $N_vS_v' = S_v \cap S_v^{(d)}$ all viewed as subgroups of $H^1(F_v, E_2)$. Globally the everywhere-local norm group $\Phi = S \cap S^{(d)}$.*

PROOF. Applying diagram (10) of §3 for both the curve E and the curve $E^{(d)}$ we find that $i_v^{-1}(S_v')$ contains $S_v \cdot S_v^{(d)}$. For the reverse inclusion suppose that $x \in i_v^{-1}(S_v')$. By the usual conventions there is nothing to prove if v splits in K, so suppose there is one prime w over v. Then $i_v(x) \in S_v' = \text{Image}\, \lambda_v'$ and we may write $i_v(x) = \lambda_v'(P)$ for some $P \in E(K_w)$. Using the commutativity of the left side of (10) and the fact that $N_v \circ i_v$ is the 0-map on $H^1(F_v, E_2)$ we have $\lambda_v(NP) = N_v\lambda_v'(P) = N_vi_v(x) = 0$. Hence $NP = 2Q$ for some $Q \in E(F_v)$. If we let $R = P - Q$, then $R^\sigma = P^\sigma - Q^\sigma = (2Q - P) - Q = -R$. Hence we may view R as an element of $E^{(d)}(F_v)$. Now $i_v(x) = \lambda_v'(P) = \lambda_v'(Q) \cdot \lambda_v'(R) = i_v(\lambda_v(Q) \cdot \lambda_v^{(d)}(R))$. It follows from Lemma 3 that the kernel of i_v is contained in $S_v \cdot S_v^{(d)}$. Hence $x \in S_v \cdot S_v^{(d)}$ as desired.

Using the perfect pairing $\bar{h}_v$ of §3 and its analog for the curve $E^{(d)}$ it is now clear that $NS_v' = S_v \cap S_v^{(d)}$. Hence also globally $\Phi = S \cap S^{(d)}$.

In §3 we reviewed the definition of the Cassels-Tate pairing T on Ш$(F)_2$. Let $T^{(d)}$ denote the corresponding pairing on the Tate-Shafarevitch group Ш$^{(d)}(F)_2$ arising from the descent involving $E^{(d)}(F)/2E^{(d)}(F)$. Since $\Phi = S \cap S^{(d)}$ there are natural maps from Φ to both Ш$(F)_2$ and Ш$^{(d)}(F)_2$. Let

$$\langle\, ,\, \rangle = T \cdot T^{(d)} \colon \Phi \times \Phi \to u_2$$

be the bilinear form induced by the product $T \cdot T^{(d)}$. We can now state our main result about Φ/NS'.

THEOREM 2. *The bilinear form $\langle\ ,\ \rangle$ is strictly alternating and puts Φ/NS' in perfect self-duality. The dimension of Φ/NS' is even.*

PROOF. The modules E_2 and $E_2^{(d)}$ are Gal$(\bar{F}/F)$-isomorphic, and we have identified them. However E_4 and $E_4^{(d)}$ only become Gal$(\bar{F}/K)$-isomorphic. Our strategy therefore is to compare the choices involved in defining T and $T^{(d)}$ by lifting to K and using the corestrictions

$$N\colon C^*(K, E_4) \to C^*(F, E_4) \quad \text{and} \quad \hat{N}\colon C^*(K, E_4) \to C^*(F, E_4^{(d)}).$$

We denote each of the restriction maps reversing these arrows by i.

It is easy to check that on $C^*(K, E_4)$

$$i \circ N + i \circ \hat{N} = \text{mult. by } 2 = 2^* \tag{14}$$

noting for example in dimension 0 that $\hat{N}(P) = P - P^\sigma$ because of the twist.

We shall do some calculations on the cochain level, adopting the convention that upper case letters denote cocycles and lower case letters the corresponding cohomology classes.

Given $a \in \Phi = S \cap S^{(d)}$ we can find $c \in H^1(F, E_4)$ and $\hat{c} \in H^1(F, E_4^{(d)})$ such that $a = 2^*c = 2^*\hat{c}$. Then there are in fact cocycles such that $A = 2^*C = 2^*\hat{C}$. Let $X = i(C) + i(\hat{C})$. Then $2^*X = i(2^*C) + i(2^*\hat{C}) = i(2A) = 0$. Hence X actually is a cocycle in $Z^1(K, E_2)$. Moreover, since σ fixes $i(C)$ and inverts $i(\hat{C})$ we have $NX = A$. Passing to cohomology we obtain $x \in H^1(K, E_2)$ such that $Nx = a$ and

$$x = i(c) + i(\hat{c}) \quad \text{in } H^1(K, E_4). \tag{15}$$

By definition of Φ, for each prime v of F there is $Q_v \in \Pi_{w|v}E(K_w)$ such that $a = N_v\lambda_v'(Q_v)$. By the commutativity of diagram (10) for the curve E and also for $E^{(d)}$ we find that $a = \lambda_v(NQ_v) = \lambda_v^{(d)}(\hat{N}Q_v)$. Hence, for the definition of T and $T^{(d)}$ we may choose $P_v = NQ_v$ and $\hat{P}_v = \hat{N}Q_v$. Then

$$\langle a, b\rangle = T(a, b)T^{(d)}(a, b) = h_F((z_v), b)$$

where $z_v = c - \gamma_v(P_v) + \hat{c} - \hat{\gamma}_v(\hat{P}_v)$ is in $H^1(F_v, E_2)$. Here $\hat{\gamma}_v$ is the map of (8) for the curve $E^{(d)}$ over F_v. We also have a map

$$\gamma_v'\colon \prod_{w|v} E(K_w)/4E(K_w) \to \prod_{w|v} H^1(K_w, E_4).$$

Replacing E_2 by E_4 or $E_4^{(d)}$ in diagram (10) we see that $\gamma_v \circ N = N_v\gamma_v'$ and $\hat{\gamma}_v \circ \hat{N} = \hat{N}\gamma_v'$. Using (14) and working in $H^1(K, E_4)$ we get

$$\begin{aligned} i[\gamma_v(P_v) + \hat{\gamma}_v(\hat{P}_v)] &= [i \circ N_v + i \circ \hat{N}_v][\gamma_v'(Q_v)] \\ &= 2^*\gamma_v'(Q_v) = \lambda_v'(Q_v). \end{aligned}$$

Now using (15), $i(z_v) = x - \lambda_v'(Q_v)$ in $H^1(K, E_4)$. But since the left and right sides of this equation are killed by 2^* it follows from exact sequence (9) that Q_v may be changed by an element of $\Pi_{w|v}E(K_w)_2$ so that in fact

$$i(z_v) = x - \lambda_v'(Q_v) \quad \text{in } H^1(K, E_2).$$

By Lemma 2 of §3, the pairing $\langle a, b\rangle = h_F((z_v), b)$ is trivial for all $b \in \Phi$ if and only if there exists $f \in H^1(F, E_2)$ and $t_v \in i^{-1}(S_v')$ such that $z_v = f + t_v$ for each prime v. If so, $i(f) + x = i(t_v) + \lambda_v'(Q_v)$ is an element of S_v' for each v. Hence $i(f) + x \in S'$ and $a = N(i(f) + x) \in NS'$.

Conversely, if $a = Ny$ for some $y \in S'$ then by Lemma 3 of §4, $y - x = i(f)$ for some $f \in H^1(F, E_2)$. Define t_v by the equation $z_v = f + t_v$. Then $i(t_v) = i(z_v) + i(f) = y + \lambda_v'(Q_v)$ is in S_v' for each v. Hence by Lemma 2 of §3, $h_F((z_v), b) = 1$ for all $b \in \Phi$. It follows that $\langle\ ,\ \rangle$ provides us with a perfect duality on Φ/NS', as desired.

PROPOSITION 8. *Let $\text{Ш}_0^{(d)}(F)$ be $\{x \in \text{Ш}^{(d)}(F)_2 | i(x) = 0 \text{ in } \text{Ш}(K)\}$. Then Φ/NS' fits into an exact sequence*

$$\text{Ш}_0^{(d)}(F) \to \Phi/NS' \to \text{Ш}(F)_2/N\{\text{Ш}(K)_2\}.$$

PROOF. We have the commutative triangle

$$\begin{tikzcd} E(F)/N\{E(K)\} \arrow[rr, "\lambda"] \arrow[dr, "f"'] & & S/NS' \arrow[dl, "g"] \\ & \prod S_v/NS_v' & \end{tikzcd}$$

in which, by abuse of notation, λ is the map induced by (7), and g maps to the diagonal. We shall examine the resulting exact sequence $\to \operatorname{Ker} f \to \operatorname{Ker} g \to \operatorname{Coker} \lambda \to$. Clearly $\operatorname{Coker} \lambda$ is isomorphic to $\text{Ш}(F)_2/N\{\text{Ш}(K)_2\}$ and $\operatorname{Ker} g$ is Φ/NS'. From the definition of Ш we obtain the exact sequence below, with the vertical arrows being restrictions.

$$\begin{tikzcd} 0 \arrow[r] & \text{Ш}^{(d)}(F)_2 \arrow[r] \arrow[d, "i"] & H^1(F, E^{(d)})_2 \arrow[r] \arrow[d, "\text{res}"] & \prod H^1(F_v, E^{(d)})_2 \arrow[d, "\Pi\text{res}_v"] \\ 0 \arrow[r] & \text{Ш}(K)_2 \arrow[r] & H^1(K, E)_2 \arrow[r] & \prod H^1(K_w, E)_2 \end{tikzcd}$$

The kernel of res is the image under inflation of $H^1(G, E^{(d)}(K))$, which is isomorphic to $E(F)/N\{E(K)\}$ taking into account the twist. Similarly, the kernel of res_v is $E(F_v)/N\{E(K_w)\} \simeq S_v/NS_v'$. Hence we obtain the exact sequence $0 \to \text{Ш}_0^{(d)}(F) \to E(F)/N\{E(K)\} \xrightarrow{f} \Pi S_v/NS_v'$ giving $\operatorname{Ker} f$ as desired.

COROLLARY 3. *If $\text{Ш}(F)_2 = \text{Ш}^{(d)}(F)_2 = 0$ then $\Phi/NS' = 0$.*

REMARK. Replacing E by $E^{(d)}$ above does not change Φ/NS' and yields the exact sequence $\text{Ш}_0(F) \to \Phi/NS' \to \text{Ш}^{(d)}(F)_2/\hat{N}\{\text{Ш}(K)_2\}$. One might try to prove the perfect self-duality of Φ/NS' by then studying the pairing $\text{Ш}_0(F) \times \text{Ш}(F)_2/N\{\text{Ш}(K)_2\}$ and extending the above exact sequences to five terms. This did not seem any easier to us.

EXAMPLE. Let E be the curve $y^2 + xy = x^3 + 244x^2 + 61x$, of conductor $N = 3 \cdot 5 \cdot 13 \cdot 61$ and discriminant $\Delta = 25N^2$. Let $d = 109$ and $K = \mathbf{Q}(d^{1/2})$. The local norm indices are

$$i_v = \begin{cases} 2, & v = 109, \\ 1, & v = 13, \\ 0, & \text{otherwise.} \end{cases}$$

$\dim \Phi = 3$ and $\dim NS' = 1$ so that Φ/NS' is not trivial. The other numerical invariants are as follows.

	$E(\mathbf{Q})$	$E^{(d)}(\mathbf{Q})$	$E(K)$
dim E_2	2	2	2
dim Selmer	4	5	5
dim Ш_2	0	2	0
rank	2	1	3

Outline of proof. Translate to obtain the model $y^2 = x^3 + (244\frac{1}{4})x^2 + 61x$ for E. Setting $y = 0$ we see that the points of order 2 are rational. We identify $H^1(\mathbf{Q}, E_2)$ with a subgroup of $\mathbf{Q}^* \oplus \mathbf{Q}^* \oplus \mathbf{Q}^*$ modulo squares as in [2, §2], with the map λ of (7) induced by $P \rightarrow (x(P), 4x(P) + 1, x(P) + 244)$. In [2, §§3 and 4] we have local descent information at primes of semistable reduction over $\mathbf{Q}$ or K. However, we need to determine $E_d^{(d)}(\mathbf{Q}_d)/2E^{(d)}(\mathbf{Q}_d) \simeq S_d^{(d)}$.

By [2, Lemma 3.1], dim $S_d^{(d)} = 2$. One then sees that it must be generated by the cosets of $(1, d, d)$ and $(d, 2, 2d)$ coming from the points of order 2 in $E^{(d)}(\mathbf{Q}_d)$. By a straightforward calculation which we leave to the reader, the elements of the Selmer groups $S(\mathbf{Q})$, $S^{(d)}(\mathbf{Q})$ and $S(K)$ and the dimensions of these groups can then be determined. By inspection dim $N\{S(K)\}$ is then found to be 1, and dim $\Phi = \dim(S \cap S^{(d)}) = 3$.

The points of order 2 in $E(\mathbf{Q})$ and the points P_1^+, P_2^+ with abscissas $x = 1$, $x = 81$ then provide a basis for $S(\mathbf{Q})$. Hence rank $E(\mathbf{Q}) = 2$ and $\text{Ш}(\mathbf{Q})_2 = 0$. The points of order 2 in $E^{(d)}(\mathbf{Q})$ and the point P_1^- on $E^{(d)}(\mathbf{Q})$, with $x(P_1^-) = -244$ give 3 independent elements of $S^{(d)}(\mathbf{Q})$. Hence rank $E^{(d)}(\mathbf{Q}) > 1$ and rank $E(K) > 3$. Since dim $S(K) = 5$ we must have equality. Furthermore dim $\text{Ш}(K)_2 = 0$ and dim $\text{Ш}^{(d)}(\mathbf{Q})_2 = 2$.

It is interesting to note that there are actual points on $E(\mathbf{Q})$, for example the points of order 2, which are norms from $E(K_w)$ for each completion K_w, but not globally from $E(K)$. Moreover, $\text{Ш}^{(d)}(\mathbf{Q})_2$ is "twisted away" by passing to K.

References

[A-L] A. O. L. Atkin and W. Li, *Twists of new forms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), 221-243.

1. B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295-299.

2. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715-743.

3. H. Cartan and S. Eilenberg, *Homological algebra*. Princeton Univ. Press, Princeton, N.J., 1956.

4. J. W. S. Cassels, *Arithmetic on curves of genus* 1. IV, J. Reine Angew. Math. **211** (1962), 95-112.

5. ______, *Arithmetic on curves of genus* 1. VII, J. Reine Angew. Math. **216** (1964), 150-158.

6. ______, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193-291.

7. S. Lang, *Elliptic functions*, Addison-Wesley, Reading, Mass., 1973.

8. B. Mazur, *Rational points of Abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183-266.

9. J.-P. Serre, *Corps locaux*, Publ. Inst. Math. Univ. Nancago VIII, Hermann, Paris, 1968.

10. ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

11. J. B. Slater, *Determination of L-functions of elliptic curves parametrized by modular functions*, Proc. London Math. Soc. (3) **28** (1974), 439-456.

12. H. P. F. Swinnerton-Dyer and B. J. Birch, *Elliptic curves and modular functions*, Lecture Notes in Math., Vol. 476, Springer-Verlag, Berlin-Heidelberg-New York, 1975, pp. 2-32.

13. J. T. Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki, 1957/58, Exposé 156, Secrétariat Math., Paris, 1958.

14. ______, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Math., Almqvist & Wiksells, Uppsala, 1963, pp. 288-295.

15. ______, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179-206.

Department of Mathematics, Queens College (CUNY), Flushing, New York 11367