MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 142
APRIL 1978, PAGES 559–569

Computation of the 2-Rank of Pure Cubic Fields

By H. Eisenbeis, G. Frey and B. Ommerborn

Abstract. For $k \in \mathbf{Z}\setminus\{0\}$ there is a close connection between a certain subgroup of the Selmer group of the elliptic curve given by: $y^2 = x^3 + k$, and the group of elements of order 2 of the class group $\mathrm{Cl}(k)$ of $\mathbf{Q}(\sqrt[3]{k})$ denoted by $\mathrm{Cl}_2(k)$ (cf. [4]). In the following paper we give some consequences of this fact, that make the computation of $\mathrm{Cl}_2(k)$ considerably easier. For $k < 10\,000$ we compute $\mathrm{Cl}_2(k)$ by methods developed in [2], and by using [1] we get the structure of the 2-primary part of $\mathrm{Cl}(k)$ with the exception of 39 cases.

1. Introduction and Notation. Let $k \neq 0$ be a rational integer. Then A_k denotes the elliptic curve, given over $\mathbf{Q}$ by the equation: $y^2 = x^3 + k$. From now on we assume that no nontrivial cube divides k. Let $\mathrm{Cl}(k)$ be the class group of $\mathbf{Q}(\sqrt[3]{k})$, $\mathrm{Cl}_2(k) := \mathrm{Cl}(k)/2\mathrm{Cl}(k)$. We want to compute $\mathrm{Cl}_2(k)$ with the method described in [2].

If K is an overfield of $\mathbf{Q}$ (e.g. the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$), then $A_k(K)$ is the group of K-rational points of A_k; If M is any abelian group, then M_2 are the elements of order 2 of M.

For a prime $\mathfrak{p}$ (resp. p) of K (resp. $\mathbf{Q}$) $K_\mathfrak{p}$ ($\mathbf{Q}_p$) is the completion of K ($\mathbf{Q}$) with respect to the normalized valuation $v_\mathfrak{p}$ (v_p) given by $\mathfrak{p}$ (p); if $\mathfrak{P}$ is a prime of $\bar{K}$ (i.e. the algebraic closure of K) dividing $\mathfrak{p}$, then $G_\mathfrak{p}$ is the decomposition group of $\mathfrak{P}$ ($G_\mathfrak{p} = \{\sigma \in G(\bar{K}/K),\ \sigma\mathfrak{P} = \mathfrak{P}\}$).

In our theory we are only interested in nonarchimedean primes. If L/K is a Galois extension with Galois group G and M is a G-module, then $H^i(G, M)$ denotes the ith (Tate-) cohomology group. If $L = \bar{K}$, then $H^i(K, M) := H^i(G(\bar{K}/K), M)$.

For any prime $\mathfrak{p}$ of K we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_k(K)/2A_k(K) & \xrightarrow{\delta} & H^1(K, A_k(\bar{K})_2) & \xrightarrow{\varphi} & H^1(K, A_k(\bar{K}))_2 & \longrightarrow & 0 \\ & & \downarrow\alpha_\mathfrak{p} & & \downarrow\beta_\mathfrak{p} & & \downarrow\gamma_\mathfrak{p} & & \\ 0 & \longrightarrow & A_k(K_\mathfrak{p})/2A_k(K_\mathfrak{p}) & \xrightarrow{\delta_\mathfrak{p}} & H^1(K_\mathfrak{p}, A_k(\bar{K}_\mathfrak{p})_2) & \xrightarrow{\varphi_\mathfrak{p}} & H^1(K_\mathfrak{p}, A_k(\bar{K}_\mathfrak{p}))_2 & \longrightarrow & 0 \end{array}$$

Definition.

$$Ш(K, A_k)_2 := \bigcap \ker \gamma_\mathfrak{p},\ \mathfrak{p} \text{ prime of } K,$$

(elements of order 2 in the Tate-Šafarevič group),

Received September 1, 1977.
AMS (MOS) subject classifications (1970). Primary 12A30, 12–04, 12A50.
Key words and phrases. Pure cubic fields, elements of order 2 of the class group, Selmer group of elliptic curves, computation of 2-coverings of elliptic curves.

$$S(K, A_k)_2 := \varphi^{-1}(Ш(K, A_k)_2)$$
$$= \{\alpha \in H^1(K, A_k(\bar{K})_2); \beta_\mathfrak{p}(\alpha) \in \mathrm{im}(\delta_\mathfrak{p}) \ \forall \mathfrak{p}\}.$$

(Selmer group for 2).

In [4] we found a close connection between $S(A_{k2}, \mathbf{Q})_2$ and $\mathrm{Cl}_2(k)$. In the following paper we want to give a correction of Satz 4 of [4] (Theorem 1) and some easy consequences of Theorem 1 (Section 2) that make the computation of $\mathrm{Cl}_2(k)$ considerably easier. Using these results, we computed $\mathrm{Cl}_2(k)$ for $k < 10\,000$ (Section 3) by methods developed in [2].

We want to thank the staff of the Rechenzentrum der Universität des Saarlandes for its kind help during the computations.

2. We first give a correction of Satz 4 of [4].

Let ζ be a cube root of unity, $K := \mathbf{Q}(\zeta, \sqrt[3]{k})$, $G(K/\mathbf{Q}) \cong S_3 = \langle \sigma, \tau \rangle$ with $\sigma^2 = 1$, $\sigma(\sqrt[3]{k}) = \sqrt[3]{k}$, and $\tau^3 = 1$, $\tau(\zeta) = \zeta$.

Definition. K'/K is an admissible extension iff either $K' = K$ or

(i) $K'/\mathbf{Q}$ is a Galois extension.

(ii) $G(K'/K) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$.

(iii) There are generators ϵ_1, ϵ_2 of $G(K'/K)$ such that

$$\tau(\epsilon_1) = \epsilon_2; \qquad \sigma(\epsilon_1) = \epsilon_1;$$
$$\tau(\epsilon_2) = \epsilon_1\epsilon_2; \qquad \sigma(\epsilon_2) = \epsilon_1\epsilon_2.$$

To any admissible K'/K we can associate exactly one element of $H^1(\mathbf{Q}, A_{k2}(\bar{\mathbf{Q}})_2)$ in the following way:

If $K' = K$, then $K'/K \longmapsto 0 \in H^1(\mathbf{Q}, A_{k2}(\bar{\mathbf{Q}})_2)$.

If $[K' : K] = 4$, then $K'/K \longmapsto \alpha$, where $\mathrm{res}_K(\alpha)$ is given by:

$$\alpha(\epsilon_1) = (-\sqrt[3]{k^2}, 0), \qquad \alpha(\epsilon_2) = (-\zeta\sqrt[3]{k^2}, 0) \quad (K' \text{ is a splitting field of } \alpha)$$

(cf. [4]).

Definition. $S_0' = \{\alpha \in H^1(\mathbf{Q}, A_{k2}(\bar{\mathbf{Q}})_2)$, α corresponds to an admissible K'/K, and K'/K is unramified$\}$.

LEMMA 1. *If* $k^2 \not\equiv 1 \bmod 9$, *then* $S_0' \subset S(\mathbf{Q}, A_{k2})_2$.

Proof. Let $\alpha \in S_0'$ correspond to K'/K. Let p be a prime. At first assume $p \nmid 6k$. Then A_{k2} has good reduction mod p, and as $K'/\mathbf{Q}$ is unramified in p we have:

$$H^1(G(K_\mathfrak{p}'/\mathbf{Q}_p), A_{k2}(K_\mathfrak{p}'))_2 = 0 \quad \text{for } \mathfrak{p} \mid p$$

(cf. [4]), hence $\gamma_p(\varphi(\alpha)) = 0$. Now assume $p \mid k$, $p \neq 2$. As $\sqrt[3]{k} \notin \mathbf{Q}_p$ we conclude $A_{k2}(\mathbf{Q}_p)_2 = \{(\infty, \infty)\}$; and the theorem of Lutz [5] gives: $A_{k2}(\mathbf{Q}_p)/2A_{k2}(\mathbf{Q}_p) = \{0\}$. Using the Tate pairing [7] we get $H^1(\mathbf{Q}_p, A_{k2}(\bar{\mathbf{Q}}_p))_2 = \{0\}$, and hence we have again $\gamma_p(\varphi(\alpha)) = 0$.

The argument above works in the same way if $p = 3 \nmid k$, as $k^2 \not\equiv 1 \bmod 9$.

Let p be equal to 2, $p \nmid k$. Then A_{k2} has bad reduction of type c_3 [6], as

$A_k(\mathbf{Q}_p)$ contains $(0, k)$. $K'/\mathbf{Q}$ is unramified at all divisors $\mathfrak{P}$ of 2, hence:

$$H^1(G(K'_{\mathfrak{P}}/\mathbf{Q}_p), A_{k2}(K'_{\mathfrak{P}}))_2 = 0,$$

and hence:

$$\beta_2(\alpha) \in \operatorname{im} \delta_2(A_{k2}(\mathbf{Q}_p)/2A_{k2}(\mathbf{Q}_p)).$$

Now assume: $2|k$. Then 2 is completely ramified in $\mathbf{Q}(\sqrt[3]{k})$, and not decomposed in K. Let $\mathfrak{P}$ be an extension of 2 to K', and $Z_{\mathfrak{P}}$ the decomposition field of $\mathfrak{P}$. Then $4 \geqslant [Z_{\mathfrak{P}} : \mathbf{Q}] \geqslant 2$, as K'/K is not cyclic. Assume $[Z_{\mathfrak{P}} : \mathbf{Q}] = 2$. Then $Z_{\mathfrak{P}} = \mathbf{Q}(\zeta)$ (this is the only subfield of K' of degree 2 over $\mathbf{Q}$, belonging to $A_4 \subset S_4 = G(K'/\mathbf{Q})$), and this is impossible. So $[Z_{\mathfrak{P}} : \mathbf{Q}] = 4$, and hence all extensions of 2 are fully decomposed in K'/K. Hence, $\beta_2(\alpha) = 0$.

The situation is more delicate if $k^2 \equiv 1 \bmod 9$, for then $A_{k2}(\mathbf{Q}_3)$ contains a point $(-\sqrt[3]{k^2}, 0)$ of order 2. Nevertheless, we have in this case too:

LEMMA 2. $S'_0 \subset S(\mathbf{Q}, A_{k2})_2$.

Proof. Again let $\alpha \in H^1(\mathbf{Q}, A_{k2}(\bar{\mathbf{Q}})_2)$ correspond to K'/K. Then we have as above for $p \neq 3$:

$$\gamma_p(\varphi(\alpha)) = 0.$$

The same is true for the infinite place, as

$$H^1(G(\mathbf{C}/\mathbf{R}), \ A_{k2}(\mathbf{C})_2) = 0.$$

α corresponds to a so-called 2-covering D of A_{k2}, and we have a $\mathbf{Q}$-rational map: $D \longrightarrow C$ of degree 2, where C is a rational curve defined over $\mathbf{Q}$ (cf. [2]). We want to show: C has a $\mathbf{Q}$-rational point. We know: C has a divisor of degree 2, and hence C admits an equation:

$$a_1 Y^2 + a_2 X^2 + a_3 XY + a_4 X + a_5 Y + a_6$$

and C has a $\mathbf{R}$-rational point and a $\mathbf{Q}_p$-rational point for all $p \neq 3$. Then a refinement of the theorem of Hasse-Minkowski gives: C has a $\mathbf{Q}$-rational point. Hence D has a divisor of degree 2, and so D admits an equation:

$$Y^2 = aX^4 + bX^3 + cX^2 + dX + e = g(X); \quad \text{with } 3|c \text{ and } ae \equiv bd \bmod 3.$$

(This follows from the conditions for the invariants of D: $0 = j(A_{k2}) = 12ae - 3bd + c^2$.)

Now we look at a place $\mathfrak{P}|3$ of K'. Then $K'_{\mathfrak{P}}$ is either equal to $\mathbf{Q}_3(\sqrt{-3})$, or equal to $\mathbf{Q}_3(\sqrt{-3}, \sqrt{-1})$.

In the first case we have: $\mathfrak{P}$ is fully decomposed in K'/K, and $\beta_2(\alpha) = 0$ (as $H^1(G(\mathbf{Q}_3(\sqrt{-3})/\mathbf{Q}_3), A_{k2}(\mathbf{Q}_3(\sqrt{-3}))_2) = 0$).

Assume the second case. We know by use of the inflation-restriction sequence: $\beta_3(\alpha) \in H^1(G(\mathbf{Q}_3(\sqrt{-1})/\mathbf{Q}_3), A_{k2}(\mathbf{Q}_3(\sqrt{-1}))_2)$.

Let $x_0 \in \mathbf{Q}_3$. Then

$$g(x_0) = \begin{cases} 0 & \text{(i)} \\ a^2 & \text{(ii)} \\ -a^2 & \text{(iii)} \\ 3a^2 & \text{(iv)} \\ -3a^2 & \text{(v)} \end{cases}$$

for some $a \in \mathbf{Q}_3^*$.

In case (i) $\beta_3(\alpha)$ is split by $\mathbf{Q}_3$, and we have a contradiction. In the second and in the fifth cases $\varphi_3(\beta_3(\alpha))$ is split by $\mathbf{Q}_3(\sqrt{-3})$, and as $H^1(G(\mathbf{Q}_3(\sqrt{-3})/\mathbf{Q}_3), A_{k2}(\mathbf{Q}_3(\sqrt{-3}))) = 0$ we have: $\varphi_3(\beta_3(\alpha))$ is split by $\mathbf{Q}_3$, and so

$$\beta_3(\alpha) = \delta_3(a), \qquad a \in A_{k2}(\mathbf{Q}_3).$$

As $A_{k2}(\mathbf{Q}_3)/2A_{k2}(\mathbf{Q}_3) \cong \langle a_2 \rangle$ where $a_2 = (-\sqrt[3]{k^2}, 0)$ is the $\mathbf{Q}_3$-rational point of order 2, we have:

$$\beta_3(\alpha) = \delta_3(a_2) \quad \text{or} \quad \beta_3(\alpha) = 0.$$

Now a_2 is divisible by 2 only after adjunction of a point of order 4, and this adjunction gives a ramified extension L of degree 4 over $\mathbf{Q}_3(\sqrt{-1})$, $(L = \mathbf{Q}_3(\sqrt[4]{3}, \sqrt{-1}))$, and so $\delta_3(a_2)$ is not split by $\mathbf{Q}_3(\sqrt{-1})$, hence $\beta_3(\alpha) = 0$, and we have a contradiction again.

Assume now: $g(x_0) = -a^2$ or $g(x_0) = 3a^2$.

Define: α': $y^2 = -g(x) \in H^1(\mathbf{Q}, A_{-k2}(\bar{\mathbf{Q}})_2)$. Then $\varphi_3(\beta_2(\alpha'))$ is split by $\mathbf{Q}_3(\sqrt{-3})$, and as above we conclude (arguing with A_{-k2} instead of A_{k2}) that α' is split in $\mathbf{Q}_3$, and hence α is split in $\mathbf{Q}_3$, and the lemma is proved.

We even proved more than Lemma 1 and Lemma 2: For any $\alpha \in S_0'$ we have $\beta_3(\alpha) = 0$, and so: All divisors of 3 are completely decomposed in K'/K.

The information for $p = 2$ we obtained is as follows: If $\alpha \in S_0'$ and $2 \nmid k$, then $\beta_2(\alpha) = \delta_2(a)$, $a \in A_{k2}(\mathbf{Q}_2)$; and $\mathbf{Q}_2(\sqrt{a})$ is unramified over $\mathbf{Q}_2$. If $2 \mid k$, then $\beta_2(\alpha) = 0$.

An easy consequence of Lemma 1 and Lemma 2 is:

THEOREM 1 (correction of Satz 4 in [4]). *There is a one-to-one correspondence between* $\mathrm{Cl}_2(k)$ *and the set of all unramified admissible extensions* K'/K. *If* $2 \mid k$, *then all divisors of* 2 *are fully decomposed in* K'/K. *If* $\mathfrak{p} \mid 3$, *then* $\mathfrak{p}$ *is fully decomposed in* K'/K.

Now define: $S_0 = \{\alpha \in S(\mathbf{Q}, A_{k2})_2, \beta_2(\alpha) = \beta_3(\alpha) = 0\}$. Then $S_0 \subset S_0'$, for if K' corresponds to $\alpha \in S_0$, then K'/K is unramified outside $\{2, 3\}$. But as $\beta_p(\alpha) = 0$ for $p = 2, 3$ we must have: All primes $\mathfrak{P}$ of K dividing 6 are completely split in K'/K, and hence K'/K is unramified.

If $2 \mid k$, we have $S_0' = S_0$. Assume $2 \nmid k$. $A_{k2}(\mathbf{Q}_2)/2A_{k2}(\mathbf{Q}_2) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$, an explicit base is given by $\langle a_1, a_2 \rangle$ with $a_1 = (-\sqrt[3]{k^2}, 0)$ and $a_2 = (4, y_0)$ with $y_0^2 = 4^3 + k$. Then $\alpha \in S_0'$ iff $\beta_3(\alpha) = 0$ and $\beta_2(\alpha) \in \langle \delta_2(a_2) \rangle$, and hence

$$S_0' = \{\alpha \in S(\mathbf{Q}, A_{k2})_2, \beta_3(\alpha) = 0 \text{ and } \alpha \in \beta_2^{-1}(\delta_2(a_2))\}.$$

We have already proved this assertion in one direction. The converse: Let $\alpha \in S(\mathbf{Q}, A_{k2})_2$ with $\beta_3(\alpha) = 0$ and $\beta_2(\alpha) = \delta(a_2)$. Then the associated K'/K is ramified at most in the primes $\mathfrak{P}|2$. As $\mathrm{res}_{K'_{\mathfrak{P}}}(\beta_2(\alpha)) = 0$, there is a $b \in A_{k2}(K'_{\mathfrak{P}})$ with $2b = a_2$, and $\beta_2(\alpha)$ is split in $K_{\mathfrak{p}}(b)$ ($\mathfrak{p} = \mathfrak{P}|K$), an unramified extension of $K_{\mathfrak{p}}$ of degree 2. Hence, $\mathrm{res}_{K_{\mathfrak{p}}(b)}(\beta_2(\alpha)) = 0$, and so $K'_{\mathfrak{P}} = K_{\mathfrak{p}}(b)$. If $\beta_2(\alpha) = 0$, then $K'_{\mathfrak{P}} = K_{\mathfrak{p}}$ (see above). So we proved the

THEOREM 2 (correction of Satz 5 of [4]). *$S_0 \subset \mathrm{Cl}_2(k)$, and $[\mathrm{Cl}_2(k): S_0] \leqslant 2$. We have:*

$[\mathrm{Cl}_2(k): S_0] = 2$ *if and only if there is* $\alpha \in \ker(\beta_3) \cap S(\mathbf{Q}, A_{k2})_2$ *with* $\beta_2(\alpha) = \delta(a_2)$.

Example. $k = 11$. Then $(12, 43) \in A_{k2}(\mathbf{Q})$, $S(\mathbf{Q}, A_{k2})_2 = \mathbf{Z}/2$, $S_0 = \{0\}$, $\ker(\beta_3) = S(\mathbf{Q}, A_{k2})_2$, and $\beta_2(S(\mathbf{Q}, A_{k2})_2) = \langle \delta a_2 \rangle = \langle \delta(12, 43) \rangle$. So $S'_0 = \mathbf{Z}/2$, and $\mathrm{Cl}_2(11) = 2$ (as known).

3. Computation of S'_0. Following [2] we have to look for (inequivalent) forms

$$y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e$$

with $a, b, c, d, e \in \mathbf{Z}$, and

$$0 = 12ae - 3bd + c^2, \tag{1}$$

$$\epsilon \cdot 3^3 k^2 = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3, \tag{2}$$

where $\epsilon = 1$ or $\epsilon = 2^6$.

The case $\epsilon = 2^6$ would require 85% of the computation time and so we are glad to have the following fact: If α corresponds to $y^2 = g(x)$ with $\epsilon = 2^6$, then $\alpha \notin S'_0$.

The reason for this fact is the following

LEMMA 3. *Let $k \in \mathbf{Z}\backslash\{0\}$ be arbitrary, $\alpha \in S(\mathbf{Q}, A_k)_2$, α corresponding to the form $y^2 = g(x)$. If $\beta_2(\alpha)$ is split by an unramified extension of $\mathbf{Q}_2$, then $\epsilon = 1$.*

Proof. $g(x)$ has a zero in an unramified extension of $\mathbf{Q}_2$, and an easy checking of polynomials of degree 4 mod 2 shows that then $\epsilon = 1$. (For details see [3].)

We now use the condition that for $\alpha \in S'_0$ we have $\beta_3(\alpha) = 0$. Let $k \in \mathbf{Z}\backslash\{0\}$ be arbitrary again. A_k and A_{-k} are isomorphic over $\mathbf{Q}(\sqrt{-1})$, an isomorphism $\epsilon\colon A_k \longrightarrow A_{-k}$ is given by $(x, y) \longrightarrow (-x, \sqrt{-1}y)$.

If $G(\mathbf{Q}(\sqrt{-1})/\mathbf{Q}) = \langle \sigma \rangle$, then $\sigma \circ \epsilon = \ominus \epsilon \circ \sigma$ ($\ominus$ means the inverse in A_{-k}). Hence, $A_k(\bar{\mathbf{Q}})_2 \xrightarrow{\epsilon}{\sim} A_{-k}(\bar{\mathbf{Q}})_2$ is a $G(\bar{\mathbf{Q}}/\mathbf{Q})$-isomorphism, and so we have

$$H^1(\mathbf{Q}, A_k(\bar{\mathbf{Q}})_2) \xrightarrow{\epsilon}{\sim} H^1(\mathbf{Q}, A_{-k}(\bar{\mathbf{Q}})_2)$$

given by: $y^2 = g(x) \longrightarrow y^2 = -g(x)$.

LEMMA 4. *For $\alpha \in H^1(\mathbf{Q}, A_k(\bar{\mathbf{Q}})_2)$ we have:*

$$\beta_3(\alpha) = 0 \quad \text{if and only if } \gamma_3(\varphi(\alpha)) = \gamma_3(\varphi(\epsilon\alpha)) = 0.$$

Proof. If $\beta_3(\alpha) = 0$, then $\beta_3(\epsilon(\alpha)) = 0$ and so

$$\gamma_3(\varphi(\alpha)) = \gamma_3(\varphi(\epsilon\alpha)) = 0.$$

Assume conversely that $\gamma_3(\varphi(\alpha)) = \gamma_3(\varphi(\epsilon\alpha)) = 0$. Then $\epsilon(\alpha) \in H^1(\mathbf{Q}, A_{-k})_2$, and

$$\xi := \gamma_3(\varphi(\epsilon(\alpha))) \in H^1(G(\mathbf{Q}_3(\sqrt{-1})/\mathbf{Q}_3), A_{-k}(\mathbf{Q}_3(\sqrt{-1}))) = H^1(\langle\sigma\rangle, A_{-k}(\mathbf{Q}_3(\sqrt{-1}))).$$

So there is an element $b \in A_{-k}(\mathbf{Q}_3(\sqrt{-1}))$ with $\sigma b + b = 0$ and $\xi(\sigma) = \sigma b - b$. But now we use the assumption that $\xi = 0$ in $H^1(\langle\sigma\rangle, A_{-k}(\mathbf{Q}_3(\sqrt{-1})))$ and conclude that b has the form: $b = \sigma b' - b'$, $b' \in A_{-k}(\mathbf{Q}_3(\sqrt{-1}))$. Then $a := \epsilon^{-1}(b) \in A_k(\mathbf{Q}_3)$ (as $0 = \epsilon^{-1}(\sigma b + b) = -\sigma(\epsilon^{-1}(b)) + \epsilon^{-1}(b)$) and $\beta_3(\alpha) = \delta(a)$, and there is $a' = \epsilon^{-1}(b')$ such that $a = a' + \sigma a'$. As $A_k(\mathbf{Q}_3(\sqrt{-1}))_2 = A_k(\mathbf{Q}_3)_2$, we have $N_\sigma(A_k(\mathbf{Q}_3(\sqrt{-1}))) = 2A_k(\mathbf{Q}_3)$; hence $a = 2a''$, $a'' \in A_k(\mathbf{Q}_3)$, and so $\beta_3(\alpha) = 0$.

Remark. Lemma 4 means: If $y^2 = g(x) \in S(\mathbf{Q}, A_k)_2$ and $y^2 = -g(x) \in S(\mathbf{Q}, A_{-k})_2$, then g has a zero in $\mathbf{Q}_3$. This can be checked by an elementary discussion of $g(x)$ without using cohomology, cf. [3]. (Unfortunately, this elementary proof is too extensive to print here.)

LEMMA 5. *If $2|k$ and $2^3 \nmid k$, and $\alpha \in H^1(\mathbf{Q}, A_k)_2$, then $\beta_2(\alpha) = 0$ if and only if $y_2(\varphi(\alpha)) = \gamma_2(\varphi(\epsilon(\alpha))) = 0$.*

Proof. As in the proof of Lemma 4 we have:

$$\beta_2(\alpha) = \delta(a), \qquad a \in N_\sigma(A_k(\mathbf{Q}_2(\sqrt{-1}))).$$

As $A_k(\mathbf{Q}_2)/2A_k(\mathbf{Q}_2) \cong \mathbf{Z}/2$ and $2A_k(\mathbf{Q}_2) \subset N_\sigma(A_k(\mathbf{Q}_2(\sqrt{-1})))$ we have only to show:

$$H^0(G(\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2), A_k(\mathbf{Q}(\sqrt{-1}))) \neq 0.$$

But an easy computation shows that any $(x, y) \in A_k(\mathbf{Q}_2)$ with $v_2(x) = -4$ is not in $N_\sigma(A_k(\mathbf{Q}_2(\sqrt{-1})))$.

Remark. If $2 \nmid k$ and $\alpha \in S_0'$, then $\alpha \hat{=} (y^2 = g(x))$, with

$$g(x) \equiv \begin{cases} x^4 + x + 1 \\ x^4 + x^3 + 1 \\ x^4 + x^3 + x^2 + x + 1 \end{cases} \mod 2$$

or $g(x)$ has a zero in $\mathbf{Q}_2$. Then $y^2 = -g(x)$ has a $\mathbf{Q}_2$-rational point. Using this and Lemmas 3, 4 we see that $S_0' \subset \{\alpha \in S(\mathbf{Q}, A_{k2})_2;\ \alpha \hat{=} (y^2 = g(x))$ with $\epsilon = 1$ and $(y^2 = -g(x)) \in S(\mathbf{Q}, A_{-k2})_2\} =: S_0''$. (In the program $S(\mathbf{Q}, A_{k2})_2$ and $S(\mathbf{Q}, A_{-k2})_2$ are computed simultaneously.) We have $S_0' = S_0''$ if $2|k$. An easy checking of polynomials of degree 4 mod 2 shows that $S_0' = S_0''$ if $2 \nmid k$.

If we summarize our results obtained till now we see: Given $S(\mathbf{Q}, A_{k2})_2$ we can pick out at once the elements belonging to S_0'. The remaining unpleasant feature is that in order to compute $\mathrm{Cl}_2(k)$ we have to deal with k^2!

$$S_0'(k) := \{\alpha \in S(\mathbf{Q}, A_k);\ \beta_3(\alpha) = 0 \text{ and } \beta_2(\alpha) \text{ is split by an unramified extension of } \mathbf{Q}_2\}.$$

LEMMA 6. $|S_0'(k)| = |S_0'|$, *and $S_0'(k)$ is characterized in $S(\mathbf{Q}, A_k)$ in the same way as S_0' in $S(\mathbf{Q}, A_{k2})$.*

Proof. The second assertion is clear as in Lemmas 3, 4, 5, k was arbitrary (and not necessarily a square). If we had done our theory with k^4 instead of k^2, we would have got the same results, so $|S_0'| = |S_0'(k^4)|$.

We have to show: $|S_0'(k^4)| = |S_0'(k)|$. A_{k4} is isomorphic to A_k over $\mathbf{Q}(\sqrt{k})$. Again we denote this isomorphism by ϵ, and so we have an isomorphism

$$\epsilon\colon H^1(\mathbf{Q}, A_{k4}(\bar{\mathbf{Q}})_2) \xrightarrow{\sim} H^1(\mathbf{Q}, A_k(\bar{\mathbf{Q}})_2).$$

Now let $\alpha \in S_0'(k^4)$. Then α is split by an admissible unramified extension K'/K. Let $\mathfrak{P}$ be a prime of K'. If $\mathfrak{P} \nmid 6 \cdot k$, $\mathfrak{P} | p$, then A_k has good reduction in p, and $K'/\mathbf{Q}$ is unramified in p. Hence, $\varphi_p(\beta_p(\epsilon(\alpha))) = 0$. If $\mathfrak{P} | k$, $\mathfrak{P} \nmid 6$, then

$$H^1(\mathbf{Q}_p, A_{k4}(\bar{\mathbf{Q}}_p))_2 \cong A_{k4}(\mathbf{Q}_p)/2A_{k4}(\mathbf{Q}_p) = 0$$

as $A_{k4}(\mathbf{Q}_p)$ is divisible by two, and by the Tate duality $H^1(\mathbf{Q}_p, A_{k4}(\bar{\mathbf{Q}}_p))$ is dual to $A_{k4}(\mathbf{Q}_p)/2A_{k4}(\mathbf{Q}_p)$. The same thing is true for A_k. Hence, $\beta_p(\alpha) = 0$, and so $\beta_p(\epsilon\alpha) = 0$ too.

If $\mathfrak{P} | 3$, then $\beta_3(\alpha) = 0$ as $\alpha \in S_0'(k^4)$, and so $\beta_3(\epsilon\alpha) = 0$. If $\mathfrak{P} | 2$ and $2 | k$, then again $\beta_2(\alpha) = \beta_2(\epsilon\alpha) = 0$. If $\mathfrak{P} | 2$ and $2 \nmid k$, then $\beta_2(\alpha)$ is given by $y^2 = g_2(x)$, where g_2 is a polynomial described on page 564. But then $\beta_2(\epsilon(\alpha))$ is given by the *same* form mod 2. Hence, $\epsilon(\alpha) \in S_0'(k)$.

The converse direction is proved in the same way. The only point one has to think about is that the admissible extension K' belonging to $\alpha \in S_0'(k)$ is unramified over K: If $\mathfrak{P} \nmid 6k$, then A_k has good reduction in $\mathfrak{P}$, and

$$\begin{aligned} H^1(G(K_{\mathfrak{P}}'/\mathbf{Q}_p), A_k(K_{\mathfrak{P}}')) &= H^1(G(K_{\mathfrak{P}}'/L), A_k(K_{\mathfrak{P}}'))^{G(K_{\mathfrak{P}}'/\mathbf{Q}_p)} \\ &= \operatorname{Hom}(G(K_{\mathfrak{P}}'/L), A_k(K_{\mathfrak{P}}')_2)^{G(L/\mathbf{Q}_p)}. \end{aligned}$$

If $L \neq K_{\mathfrak{P}}'$, then $\operatorname{res}_L(\beta_p(\alpha)) \neq 0$, and we have $\varphi_p(\beta_p(\alpha)) \neq 0$, and hence $\alpha \notin S(\mathbf{Q}, A_k)_2$.

If $\mathfrak{P} | 3k$, $\mathfrak{P} \nmid 2$, then $\beta_p(\alpha) = 0$, and so L has to be equal to $K_{\mathfrak{P}}'$. Let $\mathfrak{P} | 2$. If $2 | k$, then $\beta_2(\alpha)$ is split by an unramified extension of $\mathbf{Q}_2$ if and only if $\beta_2(\alpha) = 0$, and hence again L has to be equal to $K_{\mathfrak{P}}'$. If $2 \nmid k$ there are two possibilities:

(i) $\mathbf{Q}_2(\sqrt{k})$ is unramified over $\mathbf{Q}_2$, and $\beta_2(\alpha) = \delta((4, y_0))$ with $y^2 \equiv k \bmod 2$. As in the proof of Lemma 1 we see: $L = K_{\mathfrak{P}}'$.

(ii) $\mathbf{Q}_2(\sqrt{k})$ is ramified over $\mathbf{Q}_2$. Then $\mathbf{Q}_2(\sqrt{-k})/\mathbf{Q}_2$ is unramified. $\beta_2(\alpha)$ is split by $K_{\mathfrak{P}}'$, hence $\beta_2(\tilde{\epsilon}(\alpha))$ is split by $K_{\mathfrak{P}}'$, ($\tilde{\epsilon}\colon A_k \longrightarrow A_{-k}$ over $\mathbf{Q}(\sqrt{-1})$), and we are in the case (i) using the curve A_{-k} instead of A_k, so $L = K_{\mathfrak{P}}'$ in this case, too.

4. Results. The program was written in ALGOL 60 and implemented on a TELEFUNKEN-COMPUTER TR 440. For the detailed algorithm see [2]. We remark that we have spent much time in making the algorithm more efficient, that is, in making it quicker. Birch and Swinnerton-Dyer calculated Selmer groups up to 400 and we would be unable to get up to 10 000 with their unaltered algorithm. This work was very technical (congruences, calculations with invariants, etc.). For details, which cannot be given here, see [3]. We have computed $\mathrm{Cl}_2(k)$ for $1 \leqslant k \leqslant 10\,000$. The calculation of one $\mathrm{Cl}_2(k)$ required about $0.0063 * k$ seconds. Of course, this formula is only approximate, because the computing time also depends on the number of elements in S_0'.

To illustrate our method we give the example $k = 1259$. The first stage is to

find all forms $y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e$ ($a, b, c, d, e \in \mathbf{Z}$) with the invariants

(i) $I = 0 = 12ae - 3bd + c^2$,

(ii) $J = 27 \cdot k = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$.

Birch and Swinnerton-Dyer give bounds for a, b, c. For a fixed triple a, b, c one can compute d and e. If d and e are integers, then we have found a new form. Here, a is an element of the interval $B = [-1, 23]$. For each $a \in B$ we have the following values for b: $-2|a| \leqslant b \leqslant 2|a|$.

Take $a = +4, b = -7$. Then c ranges in the interval $[-10, 20]$, but only for $c = -6$ do we succeed in finding integers d and e ($d = +28, e = -13$). So we get the form (*). At the end of stage 1 we obtain a list of 6 forms.

$$y^2 = x^3 + 1259 \text{ (the curve itself satisfies (i) and (ii))},$$

$$y^2 = g_1(x) = 11x^4 + 12x^3 + 12x^2 + 15x + 3,$$

$$y^2 = g_2(x) = 4x^4 - 7x^3 - 6x^2 + 28x - 13 \text{ (*)},$$

$$y^2 = g_3(x) = 3x^4 - 6x^2 + 21x - 1,$$

$$y^2 = g_4(x) = 3x^4 + 4x^3 + 18x^2 + 15x - 4,$$

$$y^2 = g_5(x) = 3x^4 + 3x^3 - 15x^2 + 21x - 1.$$

This step of the program requires by far most of the computing time.

In stage 2 we reject those forms which are equivalent to a form previously obtained. Two quartics $g(x)$ and $g^*(x)$ are equivalent if and only if there are integers $\alpha, \beta, \gamma, \delta$ such that

$$g(x) = \frac{(\gamma x + \delta)^4}{(\alpha\delta - \beta\gamma)^2} g^*\left(\frac{\alpha x + \beta}{\gamma x + \delta}\right).$$

In our specific example we have the following equivalences:

$$g_1(x) = x^4 g_5\left(\frac{x+1}{x}\right) \quad \text{(i.e. } \alpha = \beta = \gamma = 1, \delta = 0\text{)},$$

$$g_2(x) = \frac{(-x+2)^4}{9} g_4\left(\frac{-x-1}{-x+2}\right) \quad \text{(i.e. } \alpha = \beta = \gamma = -1, \delta = 2\text{)}.$$

So we delete the forms $y^2 = g_4(x)$ and $y^2 = g_5(x)$.

We remark that no $g_i(x)$ has a rational zero and so no $g_i(x)$ can be equivalent to the curve $y^2 = x^3 + 1259$.

Up to this stage all calculations were carried through for $y^2 = x^3 + 1259$ and $y^2 = x^3 - 1259$ simultaneously, because the forms only differ by their sign.

From now on we have to deal with the curves separately. In stage 3 we reject those forms for which $y^2 = g(x)$ is insoluble in some p-adic field. Using the ideas of Newton's Approximation Lemma, Birch and Swinnerton-Dyer give two lemmata which decide the local solubility [2]. We obtain the following results:

For $k = 1259$ we have the forms:

$$y^2 = x^3 + 1259, \qquad y^2 = g_2(x).$$

For $k = -1259$ we have the forms:

$$y^2 = x^3 - 1259, \quad y^2 = -g_1(x), \quad y^2 = -g_2(x), \quad y^2 = -g_3(x).$$

Following the remark on page 9 we conclude that $|\mathrm{Cl}_2(1259)| = 2$. We know from [1] that $|\mathrm{Cl}(1259)| = 4$ and so $\mathrm{Cl}(1259) \cong \mathbf{Z}/4$.

Our final output was a table consisting of 46 pages, which will be placed in the UMT file. We have listed the class number $|\mathrm{Cl}(k)|$, the 2-class number $|\mathrm{Cl}_2(k)|$ and, if possible, the 2-type of the class group. The determination of the 2-type was not possible in 39 cases. The class numbers of the pure cubic fields $\mathbf{Q}(\sqrt[3]{k})$ we took from the table of P. Barrucand, H. C. Williams and L. Baniuk [1]. None of our calculations contradicted their table. The authors would like to thank Dr. D. Shanks and Dr. H. C. Williams for sending us this table.

Altogether we have examined 8122 numbers. See Table 1 for the frequency of the 2-class numbers appearing. Table 2 indicates the frequency of the 2-class numbers for the 1229 primes. In Tables 3 and 4 we divided the primes into classes modulo 4 and modulo 9. We remark that all primes p with $|\mathrm{Cl}_2(p)| = 8$ are congruent to 3 modulo 4, which could happen by chance, of course.

The primes $p \equiv \pm 1 \bmod 9$ have relatively small 2-class numbers. It seems that the reason for this is the fact that $A_k\colon y^2 = x^3 + k$ has a point of order 2 in $\mathbf{Q}_3$ iff $k^2 \equiv 1 \bmod 9$ and so

$$H^1(\mathbf{Q}_3, A_k(\bar{\mathbf{Q}}_3))_2 \cong A_k(\mathbf{Q}_3)/2A_k(\mathbf{Q}_3) \cong \mathbf{Z}/2,$$

whereas in the case $k^2 \not\equiv 1 \bmod 9$ we have

$$H^1(\mathbf{Q}_3, A_k(\bar{\mathbf{Q}}_3))_2 \cong A_k(\mathbf{Q}_3)/2A_k(\mathbf{Q}_3) \cong \{0\}.$$

Hence elements lying in the Selmer group of A_k have "more chances" not to be in the kernel of the reduction mod 3 if $k \equiv \pm 1 \bmod 9$. We do not think that the above-mentioned fact depends on the discriminant d of $\mathbf{Q}(\sqrt[3]{p})$:

$$d = \begin{cases} -3p^2 & \text{if } p \equiv \pm 1 \bmod 9, \\ -27p^2 & \text{if } p \not\equiv \pm 1 \bmod 9. \end{cases}$$

For we calculated the quotient $N_1^d(c)/N_2^d(c)$, where

$$N_i^d(c) = \begin{cases} \#\text{ primes} \equiv c \bmod 9, \text{ class number odd}, \\ \#\text{ primes} \equiv c \bmod 9, \text{ class number even}, \end{cases} \text{ for } \begin{cases} \text{discriminant} \leqslant d \ (i = 1), \\ \text{discriminant} \leqslant d \ (i = 2), \end{cases}$$

as a function of the congruence class c mod 9. As one can see in Table 5 the quotient is nearly constant and not far from 1 if the congruence class is not equal to ± 1 modulo 9 and greater than 2 in the other cases.

The division of the primes into other residue classes did not indicate any irregularity.

TABLE 1

$\lvert CL_2(k)\rvert = 1$	4612	56.79%
$\lvert CL_2(k)\rvert = 2$	2983	36.72%
$\lvert CL_2(k)\rvert = 4$	513	6.32%
$\lvert CL_2(k)\rvert = 8$	14	0.17%

TABLE 2

$\lvert CL_2(p)\rvert = 1$	676	55.01%
$\lvert CL_2(p)\rvert = 2$	468	38.08%
$\lvert CL_2(p)\rvert = 4$	80	6.51%
$\lvert CL_2(p)\rvert = 8$	5	0.40%

TABLE 3

	$\lvert CL_2(p)\rvert = 1$	$\lvert CL_2(p)\rvert = 2$	$\lvert CL_2(p)\rvert = 4$	$\lvert CL_2(p)\rvert = 8$
$p \equiv 1 \bmod 4$	348	217	44	0
$p \equiv 3 \bmod 4$	327	251	36	5

TABLE 4

	$\lvert CL_2(p)\rvert = 1$	$\lvert CL_2(p)\rvert = 2$	$\lvert CL_2(p)\rvert = 4$	$\lvert CL_2(p)\rvert = 8$
$p \equiv 1 \bmod 9$	149	50	4	0
$p \equiv 2 \bmod 9$	94	85	26	2
$p \equiv 4 \bmod 9$	97	92	15	2
$p \equiv 5 \bmod 9$	99	94	16	0
$p \equiv 7 \bmod 9$	96	88	17	1
$p \equiv 8 \bmod 9$	140	59	2	0

TABLE 5

$-d \cdot 10^{-6} \leqslant$	3	12	27	48	75	108	147	192	243	300	2700
$\frac{N_1^d(1)}{N_2^d(1)}$	8.0	5.7	4.1	3.2	3.4	3.5	3.2	3.0	2.9	2.8	–
$\frac{N_1^d(-1)}{N_2^d(-1)}$	2.2	2.1	2.2	2.3	2.5	2.7	2.7	2.7	2.5	2.3	–
$\frac{N_1^d(2)}{N_2^d(2)}$	1.2	1.0	1.0	1.0	0.8	0.8	0.9	0.9	0.9	0.9	0.8
$\frac{N_1^d(4)}{N_2^d(4)}$	1.5	0.7	0.9	1.2	1.4	1.3	1.3	1.2	1.2	1.3	0.9
$\frac{N_1^d(5)}{N_2^d(5)}$	2.0	1.2	0.9	0.9	0.9	0.9	0.9	0.8	0.8	0.8	0.9
$\frac{N_1^d(7)}{N_2^d(7)}$	0.6	1.1	1.0	1.0	1.0	0.9	1.0	1.1	1.0	1.0	0.9

Fachbereich Mathematik
Universität des Saarlandes
D–6600 Saarbrücken, West Germany

1. P. BARRUCAND, H. C. WILLIAMS & L. BANIUK, "A computational technique for determining the class number of a pure cubic field," *Math. Comp.*, v. 30, 1976, pp. 312–323.

2. B. J. BIRCH & H. P. F. SWINNERTON-DYER, "Notes on elliptic curves. I," *J. Reine Angew. Math.*, v. 212, 1963, pp. 7–25.

3. H. EISENBEIS & B. OMMERBORN, *Die Berechnung der 2-Klassenzahl rein kubischer Körper mit Hilfe der Selmergruppen gewisser elliptischer Kurven*, Diplomarbeit, Saarbrücken, 1977.

4. G. FREY, "Die Klassengruppen quadratischer und kubischer Zahlkörper und die Selmergruppen gewisser elliptischer Kurven," *Manuscripta Math.*, v. 16, 1975, pp. 333–362.

5. E. LUTZ, "Sur l'équation $y^2 = x^3 - AX - B$ dans les corps $\mathfrak{p}$-adiques," *J. Reine Angew. Math.*, v. 177, 1937, pp. 237–247.

6. A. NÉRON, "Modèles minimaux des variétés abéliennes sur les corps locaux et globaux," *Publ. Math. Inst. Hautes Études Sci.*, v. 21, 1964, 128 pp.

7. J. TATE, *WC Groups Over $\mathfrak{P}$-Adic Fields*, Séminaire Bourbaki, Vol. 10, No. 156, 1957, 13 pp.