MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 371-384

Class Numbers of the Simplest Cubic Fields

By Lawrence C. Washington*

To my friend and colleague Daniel Shanks on his seventieth birthday

Abstract. Using the "simplest cubic fields" of D. Shanks, we give a modified proof and an extension of a result of Uchida, showing how to obtain cyclic cubic fields with class number divisible by n, for any n. Using 2-descents on elliptic curves, we obtain precise information on the 2-Sylow subgroups of the class groups of these fields. A theorem of H. Heilbronn associates a set of quartic fields to the class group. We show how to obtain these fields via these elliptic curves.

In [10], D. Shanks discussed a family of cyclic cubic fields and showed that they could be regarded as the cubic analogues of the real quadratic fields $\mathbf{Q}(\sqrt{a^2+4})$. These fields had previously appeared in the work of H. Cohn [4], who used them to produce cubic fields of even class number. Later, they appeared in the work of K. Uchida [12], who showed that for each n there are infinitely many cubic fields with class number divisible by n.

In the following we first give another proof of Uchida's result and extend the techniques to handle some new cases. In the second part of the paper we study the relationship between elliptic curves and the 2-part of the class group, interpreting and extending the work of Cohn.

1. The Simplest Cubic Fields. Let $m \geqslant 0$ be an integer such that $m \not\equiv 3 \bmod 9$. Let K be the cubic field defined by the irreducible (over $\mathbf{Q}$) polynomial

$$f(X) = X^3 + mX^2 - (m+3)X + 1.$$

The discriminant of $f(X)$ is $D^2 = (m^2+3m+9)^2$ (note that $m \not\equiv 3 \bmod 9$ implies $D \not\equiv 0 \bmod 27$). Let ρ be the negative root of $f(X)$. Then

$$\rho' = 1/(1-\rho) \quad \text{and} \quad \rho'' = 1 - 1/\rho$$

are the other two roots, so $K = \mathbf{Q}(\rho)$ is a cyclic cubic field. Note that ρ, ρ', ρ'' are units; in fact, ρ, ρ' are independent, hence generate a subgroup of finite index in the full group of units of K. Since

$$-m-2 < \rho < -m-1 < 0 < \rho' < 1 < \rho'' < 2,$$

it follows easily that all 8 combinations of signs may be obtained from units and their conjugates; hence, every totally positive unit is a square and the narrow and wide class numbers are equal.

Received January 3, 1986.
1980 *Mathematics Subject Classification*. Primary 12A30, 12A50, 14K07.
*Research partially supported by NSF and the Max Planck Institut, Bonn.

0025-5718/87 $1.00 + $.25 per page

Let $\alpha = -1 + \rho - \rho^2$. Then α ($\notin \mathbf{Q}$) is a root of

$$g(X) = X^3 + D(X+1)^2,$$

which has discriminant $D^2(4D-27)^2$ (this is the polynomial used by Uchida). Write $D = bc^3$ with b cube-free (note that $D \not\equiv 0 \bmod 27$ implies that the 3-part of D is contained in b). The polynomial

$$h(X) = c^{-3}g(cX) = X^3 + b(cX+1)^2$$

has integral coefficients and discriminant $b^2(4D-27)^2$. Since $\gcd(D, b(4D-27)) = \gcd(D, 27b) = b$, we see that only primes dividing b can ramify in $K/\mathbf{Q}$. But if p divides b and β is a root of $h(X)$, then $3v_p(\beta) = v_p(b) + 2v_p(c\beta+1)$. Hence $v_p(\beta) > 0$, so $v_p(c\beta+1) = v_p(1) = 0$ and $v_p(\beta) = v_p(b)/3 = 1/3$ or $2/3$. Therefore p ramifies in $K/\mathbf{Q}$.

If $p \neq 3$ then p is tamely ramified, so $p^{e-1} = p^2$ is the exact power of p dividing the discriminant of K [3, p. 21]. If 3 is ramified then it is wildly ramified, so 3^3 divides the discriminant, which is a square. So 81 divides the discriminant. Since $D \not\equiv 0 \bmod 27$, we see that 81 is the exact power of 3 in the discriminant. We have proved the following

PROPOSITION 1. *Let $m \not\equiv 3 \bmod 9$ and write $m^2 + 3m + 9 = bc^3$ with b cube-free. Then the discriminant of K is $(\delta \prod_{p|b} p)^2$, where $\delta = 1$ if $3 \nmid b$ and $\delta = 3$ if $3 \mid b$.*

COROLLARY. *If $m^2 + 3m + 9$ is square-free, then $\{1, \rho, \rho^2\}$ forms an integral basis for K and $\{-1, \rho, \rho'\}$ generates the full group of units of K.*

Proof. The first part is immediate. The second follows, for example, from estimates on the regulator of a cyclic cubic field [5].

2. Divisibility of Class Numbers. In this section we prove a result of Uchida which yields, for any n, cubic fields with class number divisible by n.

PROPOSITION 2. *Let $n \geqslant 2$ be an integer. Let $x, y \in \mathbf{Q}$, and suppose*

$$y^n = x^3 + mx^2 - (m+3)x + 1.$$

If D is not cube-free, we also assume that the g.c.d. of the numerator of $x^2 - x + 1$, the numerator of y, and c (defined above) is 1. If $n \not\equiv 0 \bmod 3$ or if $x \in \mathbf{Z}$, then the principal ideal $(x - \rho)$ is the nth power of an ideal of K. If $x \notin \mathbf{Z}$ and $n \equiv 0 \bmod 3$, it is the $(n/3)$rd power of an ideal.

Proof. Let $\mathfrak{p}$ be a prime ideal of K. If $\mathfrak{p}^a$ is the exact power of $\mathfrak{p}$ in the denominator of $x - \rho$, then $\mathfrak{p}^{3a}$ is the exact power of $\mathfrak{p}$ in the denominator of y^n. Therefore n divides $3a$. This takes care of the denominator. Now assume $\mathfrak{p}^a$, with $a > 0$, is the exact power of $\mathfrak{p}$ dividing $x - \rho$. Let p be the rational prime below $\mathfrak{p}$. If p is ramified, then $\mathfrak{p}$ equals its Galois conjugates, so $\mathfrak{p}^a$ is the exact power of $\mathfrak{p}$ dividing each of $x - \rho'$ and $x - \rho''$. Therefore $\mathfrak{p}^{3a} = p^a$ exactly divides $y^n = (x-\rho)(x-\rho')(x-\rho'')$, so n divides a. Now suppose p is unramified. If $\mathfrak{p}$ does not divide $(x-\rho')(x-\rho'')$, then $\mathfrak{p}^a$ exactly divides y^n, so n divides a. So suppose $\mathfrak{p}$ divides $x - \rho'$ or $x - \rho''$. Then $\mathfrak{p}$ divides $\rho - \rho'$ or $\rho - \rho''$, hence $\mathfrak{p}$ divides D. If D is cube-free, this implies that p ramifies, so we are done. In any case, from the fact that $\rho' = 1/(1-\rho)$ and $\rho'' = 1 - 1/\rho$ we find that $x \equiv 1/(1-x)$ or $1 - 1/x \bmod \mathfrak{p}$. Therefore $x^2 - x + 1 \equiv 0 \bmod \mathfrak{p}$. Since $\mathfrak{p} \mid x - \rho$ implies $\mathfrak{p} \mid y$, the

numerators of $x^2 - x + 1$ and y have a common factor. This contradicts our assumption and completes the proof.

In order to obtain results on class numbers, we need conditions which will ensure that $(x - \rho)$ is not, for example, the nth power of a principal ideal. The most effective way seems to be to consider the various values of x separately. The case $x = -1$ corresponds to the result of Uchida.

PROPOSITION 3. *Suppose* $(-1, y)$ *satisfies the conditions of Proposition* 2 (*so* $y^n = 2m + 3$) *and* $m \not\equiv 0 \bmod 3$. *Assume that for each prime factor* l *of* n *there exist corresponding prime factors* p *and* q *of* y *such that* 2 *is an* l*th power nonresidue modulo both* p *and* q *and such that* 3 *is an* l*th power residue* mod p *and an* l*th power nonresidue* mod q. *Then the ideal* $(-1 - \rho)$ *is the* n*th power of an ideal* I *whose ideal class has order* n.

Proof. Any $p \mid y$ divides $y^n = (-1 - \rho)(-1 - \rho')(-1 - \rho'')$; since the three factors are conjugate, we may choose a prime $\mathfrak{p}$ above p such that $\rho \equiv -1 \bmod \mathfrak{p}$. Then $\rho' \equiv 1/2$ and $\rho'' \equiv 2 \bmod \mathfrak{p}$. Since $-1 \not\equiv 2 \bmod \mathfrak{p}$, it follows that p splits in K.

If $m^2 + 3m + 9$ is square-free, then we know from above that the group E' generated by $\{-1, \rho, \rho'\}$ is the full group E of units, but in general this is not the case. Let l be a prime dividing n and suppose l divides $[E : E']$. Then there is a unit ε such that $\varepsilon^l = \pm\rho^a(\rho')^b$ with $a, b \in \mathbf{Z}$ not divisible by l. First suppose l is odd, so we may ignore the possible negative sign. We then have $\varepsilon^l \equiv (-1)^a 2^{-b} \bmod \mathfrak{p}$. Since 2 is an lth power nonresidue mod p, we must have $b \equiv 0 \bmod l$. In addition, $(\varepsilon')^l = (\rho')^a(\rho'')^b$, so $(\varepsilon')^l \equiv 2^{b-a} \bmod \mathfrak{p}$. Hence $b - a \equiv 0 \bmod l$, so $a \equiv 0 \bmod l$. It follows that $[E : E']$ is prime to l. Now let $l = 2$, so $\varepsilon^2 = \pm\rho^a(\rho')^b$. The left side is totally positive, hence a and b must both be even and the positive sign must be used. Therefore 2 does not divide $[E : E']$. We have shown that $[E : E']$ is prime to n.

Now suppose $(-1 - \rho) = (\alpha)^l$ for some α and for some prime l dividing n. Then

$$-1 - \rho = \varepsilon\alpha^l$$

for some unit ε. The above implies that we may write

$$-1 - \rho = \pm\rho^a(\rho')^b\alpha_1^l$$

for some a, b, and α_1. Therefore

$$-1 - \rho' = \pm(\rho')^a(\rho'')^b(\alpha_1')^l,$$

so

$$-\tfrac{3}{2} \equiv \pm 2^{b-a}(\alpha_1')^l \bmod \mathfrak{p}.$$

This congruence also holds mod $\mathfrak{q}$, where $\mathfrak{q}$ is the prime above q with $\rho \equiv -1 \bmod \mathfrak{q}$. We first treat the case where l is odd. The negative signs may be ignored, so we find that $b - a + 1 \equiv 0 \bmod l$ since 3 is an lth power residue mod p, but $b - a + 1 \not\equiv 0 \bmod l$ since 3 is not an lth power residue mod q. Contradiction. Now suppose $l = 2$. Since $-1 - \rho' < 0$, we have

$$-1 - \rho' = -(\rho')^a(\rho'')^b(\alpha_1')^2.$$

But

$$0 > -1 - \rho'' = -(\rho'')^a \rho^b (\alpha_1'')^2,$$

so b is even. Also

$$0 < -1 - \rho = -\rho^a (\rho')^b \alpha_1^2,$$

so a is odd. The above equations yield

$$-\tfrac{3}{2} \equiv -2^{b-a}(\alpha_1')^2 \bmod \mathfrak{q},$$

so 3 is a quadratic residue mod q. Contradiction. (We also could have used the expression for $-1 - \rho''$ to obtain $-3 \equiv -2^a(-1)^b(\alpha_1'')^2 \bmod \mathfrak{p}$. Therefore, for $l = 2$ we only need a prime divisor of y for which at least one of 2 and 3 is a quadratic nonresidue.) Since $(-1 - \rho) \neq (\alpha)^l$ for any l dividing n, it follows that the ideal class of I has order n, as desired.

COROLLARY (UCHIDA). *Let y and n be positive integers with $y > 1$ and $(y, 6) = 1$. Assume that for each prime l dividing n there are corresponding primes p and q, as in the statement of Proposition 3. Let $m = (y^n - 3)/2$. Then the field K determined by the polynomial $X^3 + mX^2 - (m + 3)X + 1$ has class number divisible by n.* (Uchida used the polynomial $X^3 + D(X + 1)^2$ with $D = (y^{2n} + 27)/4$.)

This is just a restatement of Proposition 3. Uchida deduces from this that there are infinitely many cyclic cubic fields with class number divisible by n.

It is possible to use the above techniques with values of x other than -1 and obtain similar results. The following is a sample:

$x = 2$. This yields the same value for y and the same result as above. This should not be surprising since $\rho \equiv -1$ implies $\rho'' \equiv 2$, so the above congruences can be used with ρ'' in place of ρ.

$x = 1$. If n is odd we obtain the point $(1, -1)$, which does not yield any information, since $x - \rho = 1 - \rho$ is a unit.

$x = 3$. Choose an integer $y > 1$ with $(y, 7) = 1$. The parameter m is given by $m = (y^n - 19)/6$. We also assume $m \in \mathbf{Z}$ (so, for example, we could take $y \equiv 1 \bmod 6$). In the notation of the proof of Proposition 3, we have $\rho \equiv 3$, $\rho' \equiv -1/2$, $\rho'' \equiv 2/3 \bmod \mathfrak{p}$. We need to show that the subgroup of units E' has index prime to n. This index is 1 if $m^2 + 3m + 9$ is square-free. In other cases we can impose conditions as in Proposition 3. For example, it suffices to assume that for each l dividing n there is a divisor p of y with 3 an lth power residue and 2 an lth power nonresidue. We next need to show that $(3 - \rho) \neq (\alpha)^l$ for each prime l dividing n. If we assume, in addition to the above assumptions on 2 and 3, that for each such l the prime p has 7 as an lth power nonresidue and that there is also a prime q dividing y with 3 and 7 as lth power residues and 2 a nonresidue, then it follows that $(3 - \rho) \neq (\alpha)^l$. We thus find, under these assumptions, that n divides the class number.

$x = 4$. We give a numerical example which shows how the above techniques can be modified. Let $m = 256$, so $X^3 + mX^2 - (m + 3)X + 1 = 5^5$. Since $m^2 + 3m + 9 = 66313 = 13 \cdot 5101$ is square-free, the units are generated by $\{-1, \rho, \rho'\}$. We only need to show that $(4 - \rho) \neq (\alpha)^5$. But there is only one rational prime dividing $5 = y$, so we cannot find primes p and q as before. Observe that

$$(3 - \rho)(3 - \rho')(3 - \rho'') = 3^3 + m \cdot 3^2 - (m + 3) \cdot 3 + 1 = 1555 = 5 \cdot 311$$

(the main point is that $311 \equiv 1 \bmod 5$, so there are 5th power nonresidues). We may therefore choose a prime $\mathfrak{p}$ dividing 311 with $\rho \equiv 3$, $\rho' \equiv -1/2$, $\rho'' \equiv 2/3 \bmod \mathfrak{p}$. Suppose

$$4 - \rho = \rho^a(\rho')^b\alpha^5.$$

Then, taking the three conjugates of this equation and then reducing mod $\mathfrak{p}$, we obtain

$$1 \equiv 3^a 2^{-b}\alpha_1^5, \quad 9/2 \equiv 2^{-a}(2/3)^b\beta^5, \quad 10/3 \equiv (2/3)^a 3^b\gamma^5.$$

Straightforward calculations show that 2 and 3 are not 5th power residues mod 311 and that $3^{123} \equiv 2 \bmod 311$. Therefore $0 \equiv a - 123b \bmod 5$ and $2 - 123 \equiv -123a + 122b \bmod 5$. These yield $a \equiv b \equiv 0 \bmod 5$. But $10/3$ is not a 5th power residue mod 311; so we have a contradiction. It follows that 5 divides the class number of the cyclic cubic field corresponding to $m = 256$. Note that the advantage of the present method is that we obtain three equations mod $\mathfrak{p}$ instead of two, since we did not take $\mathfrak{p}$ to be a divisor of $x - \rho$.

3. Elliptic Curves and the 2-Part of the Class Group. We now relate the 2-part of the class group of the simplest cubic fields to elliptic curves. This reinterprets and extends a method of Harvey Cohn for producing cyclic cubic fields of even class number.

Consider the elliptic curve E defined over $\mathbf{Q}$ by

$$Y^2 = X^3 + mX^2 - (m + 3)X + 1.$$

For simplicity, we assume

$$D = m^2 + 3m + 9 \text{ is square-free.}$$

The j-invariant of E is $256D$ and the conductor is $16D^2$ if m is even, $8D^2$ if $m \equiv 1 \bmod 4$, and $4D^2$ if $m \equiv 3 \bmod 4$. The real points of E are as in Figure 1.

Note that the right-hand part E° of the real curve is the connected component of the identity and the sum of two points of $E - E^\circ$ lies in E°. Let $E(\mathbf{Q})$ denote the group of rational points of E. Mordell's Theorem states that it is a finitely generated abelian group. Let $\operatorname{rank}(E(\mathbf{Q}))$ denote its rank over $\mathbf{Z}$, and let $Ш_2$ denote the 2-torsion of the Tate-Shafarevich group (defined below).

Let C be the ideal class group of the cubic field K and $C_2 = \{x \in C \mid x^2 = 1\}$. The 2-rank ($\operatorname{rk}_2$) will denote its dimension as a $\mathbf{Z}/2\mathbf{Z}$-vector space.

THEOREM 1. $\operatorname{rank}(E(\mathbf{Q})) \leqslant 1 + \operatorname{rk}_2(C_2)$. *In fact, there is an exact sequence*

$$1 \to E^\circ(\mathbf{Q})/2E(\mathbf{Q}) \to C_2 \to Ш_2 \to 1.$$

Proof. The 2-torsion on E consists of the points $(\rho, 0)$, $(\rho', 0)$, $(\rho'', 0)$, none of which is rational. Therefore $\operatorname{rank}(E(\mathbf{Q})) = \operatorname{rk}_2(E(\mathbf{Q})/2E(\mathbf{Q}))$. Since $(0, 1) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, it follows that $\operatorname{rk}_2(E(\mathbf{Q})/2E(\mathbf{Q})) = 1 + \operatorname{rk}_2(E^\circ(\mathbf{Q})/2E(\mathbf{Q}))$. Therefore the inequality follows from the exact sequence.

The exact sequence follows from a standard argument involving a 2-descent. The middle term above is known to be related to C_2 (see [2], [6]). The main point is that for the present family of curves it is exactly C_2. We sketch the details.

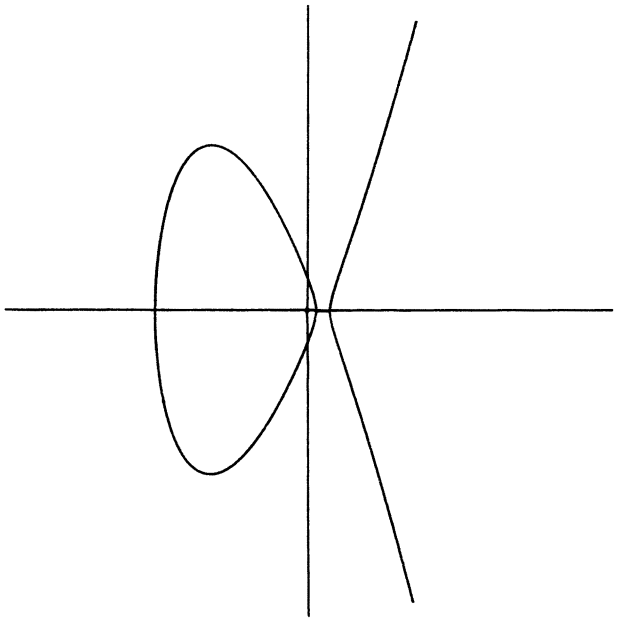

FIGURE 1

For each rational prime $p \leqslant \infty$, let $\mathbf{Q}_p$ denote the completion of $\mathbf{Q}$ at p. If p does not split in the cubic field K, let K_p denote the completion of K at the prime above p and define the homomorphism

$$\lambda_p\colon E(\mathbf{Q}_p) \to K_p^\times/\left(K_p^\times\right)^2, \qquad (x, y) \mapsto x - \rho.$$

If p splits, let

$$\begin{aligned}
&\lambda_p\colon E(\mathbf{Q}) \to \left(\mathbf{Q}_p^\times/\left(\mathbf{Q}_p^\times\right)^2\right)^3,\\
&(x, y) \mapsto (x - \rho, x - \rho', x - \rho''), \qquad x \neq \rho, \rho', \rho'',\\
&(\rho, 0) \mapsto (z, \rho - \rho', \rho - \rho''),
\end{aligned}$$

where z is chosen so that $z(\rho - \rho')(\rho - \rho'') \in (K^\times)^2$. One defines $\lambda_p(\rho', 0)$ and $\lambda_p(\rho'', 0)$ similarly. Let S_2, the Selmer group, be the subgroup of elements of $K^\times/(K^\times)^2$ which are in the image of λ_p for all p (K embeds into K_p (p nonsplit) as usual, and into $\mathbf{Q}_p^3$ (p split) via the three Galois conjugates). The Tate-Shafarevich group $Ш_2$ is defined by the exactness of the sequence

$$0 \to E(\mathbf{Q})/2E(\mathbf{Q}) \to S_2 \to Ш_2 \to 0.$$

We first compute S_2. Let $\alpha \in K^\times$ represent an element of S_2, so $\alpha \in \operatorname{Im} \lambda_p$ for all p. If p is not split in K, then $\alpha = (x - \rho)\beta^2$ for some $\beta \in K_p^\times$ and $(x, y) \in E(\mathbf{Q}_p)$. Since $x - \rho$, $x - \rho'$, $x - \rho''$ are Galois conjugates, they all have the same p-adic valuation and their product is y^2, so $x - \rho$ has even valuation in K_p. Therefore α has even valuation in K_p. Now suppose p splits in K. Letting α', α'' denote the conjugates of α over $\mathbf{Q}$, we have

$$(\alpha, \alpha', \alpha'') = \left((x - \rho)\beta_1^2, (x - \rho')\beta_2^2, (x - \rho'')\beta_3^2\right)$$

for some $\beta_t \in \mathbf{Q}_p$ and $(x, y) \in E(\mathbf{Q}_p)$. If $x - \rho$ and $x - \rho'$ or $x - \rho''$ have positive valuation, then so does $\rho - \rho'$ or $\rho - \rho''$, hence p divides $D = m^2 + 3m + 9$. Since D is assumed to be square-free, p ramifies by Proposition 1. Contradiction. If only $x - \rho$ has positive valuation, it must be even. If $x - \rho$ has negative valuation, so do $x - \rho'$ and $x - \rho''$, and all valuations are the same, hence even. Therefore, α must have even valuation at all primes, so the ideal (α) is the square of an ideal: $(\alpha) = I^2$. If I is principal, then $\alpha = \varepsilon\beta^2$ for some $\beta \in K^\times$ and some unit ε. But $\alpha \in \operatorname{Im} \lambda_\infty$. Since $x - \rho > x - \rho' > x - \rho''$ and the product is $y^2 \geqslant 0$, we must have the signs of α, α', α'' be $+, +, +$ or $+, -, -$. Therefore ε, ε', ε'' also have these two possibilities for signs. Since ρ, ρ', ρ'' have signs $-, +, +$, we find that either ε or $-\rho\varepsilon$ is totally positive, hence a square. Therefore, if I is principal, either α or $-\rho\alpha$ is a square, so we have an exact sequence

$$1 \to \{1, -\rho\}(K^\times)^2/(K^\times)^2 \to S_2 \to C_2.$$

We now show that the last map is surjective. Suppose I is an ideal with $I^2 = (\alpha)$ for some $\alpha \in K^\times$. We may change α by a unit, if necessary, and assume it is totally positive. Then $\alpha \bmod (K^\times)^2$ is clearly equal to $\lambda_\infty(x, y)$ for any $x > \rho''$ and suitable y. The following two lemmas will be useful for treating the finite primes.

LEMMA. *Let L be a number field in which 2 is inert and let $\alpha \in L$ be relatively prime to 2. Then, $L(\sqrt{\alpha})/L$ is unramified at the prime above 2 if and only if α is congruent to a square* mod 4. *This extension is unramified at the other finite primes of L if and only if the (fractional) ideal (α) is the square of an ideal of K. If K is totally real, then the extension is unramified at the infinite primes if and only if α is totally positive.*

Proof. This is a well-known result. For a "proof" see [13, Exercises 9.1–9.3].

LEMMA. *Let $x \in K^\times$ be relatively prime to 2. Then there exists a unit ε of K such that εx is congruent to a square* mod 4.

Proof. Since 2 is inert in $K/\mathbf{Q}$ (see [10]), there are 56 residue classes mod 4 relatively prime to 2. The units generate, modulo squares, the classes ± 1, $\pm\rho$, $\pm(1 - \rho)$, $\pm(\rho - \rho^2)$. The group of square residue classes mod 4 may be calculated explicitly. For example, if $m \equiv 3 \bmod 4$, then the nonzero squares mod 4 are 1, $3 + \rho + 3\rho^2$, ρ^2, $1 + \rho + 2\rho^2$, $\rho + \rho^2$, $1 + 2\rho + \rho^2$, $2 + 3\rho$. It is found that there is only the trivial intersection with the above set of units. Therefore, the units times the squares yield all 56 residue classes. This proves the lemma.

By the first lemma, $K(\sqrt{\alpha})/K$ is unramified at all primes, finite and infinite, except possibly at 2. By the second lemma, we can choose ε so that $K(\sqrt{\varepsilon\alpha})/K$ is unramified at 2. This extension is also unramified at the other finite primes. Since the narrow and wide class numbers are equal, class field theory implies that the extension must be unramified at the infinite primes, so $\varepsilon\alpha$ is totally positive. Since α is totally positive, so is ε, hence ε is a square. Therefore $K(\sqrt{\alpha})/K$ is unramified everywhere.

If p is inert in $K/\mathbf{Q}$, then (p) is a principal prime ideal of K, so it splits completely in the unramified extension $K(\sqrt{\alpha})/K$, by class field theory. Therefore $\alpha \in (K_p^\times)^2$. In particular, $\alpha \in \operatorname{Im} \lambda_p$.

If p ramifies in $K/\mathbf{Q}$, then $\mathfrak{p}^3 = (p)$, where $\mathfrak{p}$ is the prime above p. Therefore, the ideal class of $\mathfrak{p}$ is of order 1 or 3, so $\mathfrak{p}$ splits completely in an unramified extension of degree 2. Therefore $\alpha \in (K_p^\times)^2$ and $\alpha \in \operatorname{Im} \lambda_p$.

Finally, suppose p splits in $K/\mathbf{Q}$. Then the 2-torsion points of E are rational over $\mathbf{Q}_p$, so $E(\mathbf{Q}_p)/2E(\mathbf{Q}_p)$ contains $(\mathbf{Z}/2\mathbf{Z})^2$ (use the reduction mod p), and it injects into $(\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2)^3$. Since p does not divide D, only one of the $x - \rho$, $x - \rho'$, $x - \rho''$ can be divisible by p when embedded in $\mathbf{Q}_p$, and it must therefore have even valuation. (If p is in the denominator of x, then again it is easy to see we get even valuation.) Hence we can map into the group represented by units, $(\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2)^3$. If (a, b, c) is in the image, we also have $abc \in (\mathbf{Z}_p^\times)^2$, so this characterizes the image, since we have now restricted enough to get $(\mathbf{Z}/2\mathbf{Z})^2$. Since $(\alpha) = I^2$, $(\alpha, \alpha', \alpha'') \in (\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2)^3$ can be represented by an element of $(\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2)^3$. Also, $(\alpha\alpha'\alpha'') = (\operatorname{Norm} I)^2$, so $\alpha\alpha'\alpha'' = \varepsilon n^2$ for some unit ε and some n. Since α is assumed to be totally positive, so is ε. Hence ε is a square. It follows that $\alpha\alpha'\alpha''$ is a square, so $(\alpha, \alpha', \alpha'') \in \operatorname{Im} \lambda_p$.

We have now shown that $\alpha \in \operatorname{Im} \lambda_p$ for all p, and hence the above map $S_2 \to C_2$ is surjective.

Now consider the exact sequence

$$1 \to E(\mathbf{Q})/2E(\mathbf{Q}) \to S_2 \to Ш_2 \to 1.$$

Note that the point $(0, 1) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$ maps to $-\rho \in S_2$. Therefore, if we replace $E(\mathbf{Q})$ by $E^\circ(\mathbf{Q})$ and S_2 by C_2, we obtain

$$1 \to E^\circ(\mathbf{Q})/2E(\mathbf{Q}) \to C_2 \to Ш_2 \to 1,$$

as desired. This completes the proof.

The Galois structure of C_2 shows that it must have even rank [13, p. 187]. If the 2-primary part of Ш is finite, then the existence of a nondegenerate skew-symmetric pairing shows that $Ш_2$ has even 2-rank. Therefore $E^\circ(\mathbf{Q})/2E(\mathbf{Q})$ should have even 2-rank. It follows then that $E(\mathbf{Q})/2E(\mathbf{Q})$ has odd 2-rank, hence $E(\mathbf{Q})$ has odd rank, at least under the assumption that Ш is finite.

A result similar to that of the theorem, but phrased without elliptic curves, was proved by H. Cohn [4]. However, he worked only with integral points on $E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, hence he was unable to explain why the field generated by

$$f(X) = X^3 + 136X^2 - 139X + 1$$

has even class number ($h = 100$), since there are no integral points other than $(0, \pm 1)$ on $E(\mathbf{Q}) - E^\circ(\mathbf{Q})$. In the present setting we observe that $(33/4, 745/8)$ is a rational point. Proposition 4 will show that this point is not in $2E(\mathbf{Q})$. It follows easily that $E(\mathbf{Q})$ has rank at least 2, so the class number must be even.

However, it should be mentioned that Cohn actually worked with the number $-\rho(x - \rho)$. This corresponds to the image of $(0, 1) + (x, y)$ under λ. If $(x, y) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, then this point is in $E^\circ(\mathbf{Q})$, so in fact he was working on $E^\circ(\mathbf{Q})$.

4. Quartic Fields. We now derive a criterion for determining whether or not a point in $E(\mathbf{Q})$ is in $2E(\mathbf{Q})$.

PROPOSITION 4. *Let $f(X) \in \mathbf{Q}[X]$ be a cubic polynomial with distinct roots and let E be the elliptic curve $Y^2 = f(X)$. Let $(d, e) \in E(\mathbf{Q})$ and let*

$$f(X + d) = aX^3 + bX^2 + cX + e^2$$

with $a, b, c \in \mathbf{Q}$. *Then* $(d, e) \in 2E(\mathbf{Q})$ *if and only if*

$$q(X) = X^4 - 2bX^2 - 8aeX + b^2 - 4ac$$

has a rational root.

Proof. Let $2(x_0, y_0) = (d, e)$, so there is a line $Y = m(X - d) - e$ through $(d, -e)$ tangent to $Y^2 = f(X)$ at (x_0, y_0). From $(m(X - d) - e)^2 = f(X)$ we obtain

$$(mX - e)^2 = f(X + d) = aX^3 + bX^2 + cX + e^2$$

for $X = x_0 - d$, $x_0 - d$, 0. So we have $(m^2 - b)/a = 2(x_0 - d)$, hence

$$x_0 = \frac{1}{2a}(m^2 - b) + d \quad \text{and} \quad y_0 = \frac{m}{2a}(m^2 - b) - e.$$

Since the line is tangent at (x_0, y_0), we have

$$2y_0 m = 3a(x_0 - d)^2 + 2b(x_0 - d) + c,$$

which becomes

$$0 = m^4 - 2bm^2 - 8aem + b^2 - 4ac = q(m).$$

The four roots m of this equation correspond to the four solutions of $2(x_0, y_0) = (d, e)$. Note that $\mathbf{Q}(x_0, y_0) = \mathbf{Q}(m)$, so there exists a solution $(x_0, y_0) \in E(\mathbf{Q})$ if and only if $q(X)$ has a rational root.

Remarks. The polynomial $q(X)$ arises naturally in other ways, at least in the case $a = 1$. First, the quartic curve $Y^2 = q(X)$ is birationally equivalent to $Y^2 = f(X)$ [1, p. 483]. Second, the resolvent of $q(X)$ (in the sense of Weber [14, p. 136]) is $-64f((-X/4) + d)$, so $q(X)$ is essentially the "anti-resolvent" of $f(X + d)$.

A theorem of Heilbronn [7] states that if the class group C of the cyclic cubic field K has t elements of order exactly 2, then there are precisely $t/3$ sets of conjugate quartic fields with discriminant equal to that of K and whose Galois closures contain K. Shanks has pointed out that the "anti-resolvent" $q(X)$ allows us to find such fields. Using the above proposition, we can make this more precise via the theory of elliptic curves.

Assume $Ш_2 = 0$, so $E^\circ(\mathbf{Q})/2E(\mathbf{Q}) \simeq C_2$. Then every ideal class of order 2 comes from a point of $E^\circ(\mathbf{Q})$. Let I represent such a class, with $I^2 = (d - \rho)$ for some $(d, e) \in E(\mathbf{Q})$. The point (d, e) gives rise to the quartic polynomial $q(X)$ above. As noted in the proof of Proposition 4, a root m of $q(X)$ generates the same field as the coordinates (x_0, y_0) of some square root of (d, e). So if $(d, e) \equiv (d_1, e_1) \bmod 2E(\mathbf{Q})$, then the roots of the polynomials $q(X)$ and $q_1(X)$ yield the same fields.

Let F be the splitting field of $q(X)$. Since F contains the coordinates of all solutions of $2(x, y) = (d, e)$, it must contain the points of order 2, namely $(0, \rho)$, $(0, \rho')$, $(0, \rho'')$. So $F \supseteq K$. If $F = K$, then $q(X)$ is reducible. It cannot have an irreducible quadratic factor, since such a factor would not split in the cubic field K. Hence $q(X)$ must have a linear factor, so $(d, e) \in 2E(\mathbf{Q})$ by Proposition 4. Now suppose $F \neq K$. Since $f(X)$ is essentially the resolvent of $q(X)$, the discriminants of f and q differ by a square. Therefore the discriminants of K and a quartic field, call it K_4, associated with $q(X)$, differ by a square. But K is a cyclic cubic field, hence has square discriminant. So K_4 and $q(X)$ have square discriminants. Therefore $\mathrm{Gal}(F/\mathbf{Q})$ is a subgroup of A_4. Since A_4 has no subgroups of order 6, we must have $\mathrm{Gal}(F/\mathbf{Q}) \simeq A_4$.

We have shown that a point $(d, e) \in E(\mathbf{Q}) - 2E(\mathbf{Q})$ yields a quartic field whose Galois closure F contains K and has Galois group A_4. But we also need to know whether or not the discriminant of the quartic field equals that of K. If L is any field containing K, there is an injection

$$E(L)/2E(L) \to \left(L^\times/(L^\times)^3\right)^3: \qquad (x, y) \mapsto (x - \rho, x - \rho', x - \rho'')$$

(if $x = \rho, \rho', \rho''$, make modifications, as in the definition of λ_p for p split in the proof of Theorem 1). The smallest field containing K and the coordinates of $\frac{1}{2}(d, e)$ is the smallest extension field in which $d - \rho$, $d - \rho'$, and $d - \rho''$ are all squares, namely $K(\sqrt{d - \rho}, \sqrt{d - \rho'})$. (We can omit $d - \rho''$ since it differs from the product of the other two by a square.) So $F = K(\sqrt{d - \rho}, \sqrt{d - \rho'})$. As shown in the proof of Theorem 1, if $(d, e) \in E^\circ(\mathbf{Q})$, then $K(\sqrt{d - \rho})/K$ is unramified, hence so is $K(\sqrt{d - \rho'})/K$. Therefore F/K is unramified. It follows as in Heilbronn's paper, that the discriminant of each of the four quartic subfields of F has discriminant equal to that of K.

If $(d - \rho) = I^2$ for some ideal I of K, then $(d - \rho') = (I')^2$. Under the assumption $Ш_2 = 0$, there is an ideal $J = (\beta)I'$ in the same class as I' and a point $(d', e') \in E^\circ(\mathbf{Q})$ with $(d' - \rho) = J^2$ (how to find this point remains a mystery), so $d' - \rho = \varepsilon\beta^2(d - \rho')$ for some unit ε. Since (d, e), $(d', e') \in E^\circ(\mathbf{Q})$, $d - \rho'$ and $d' - \rho$ are totally positive. Therefore ε is totally positive, hence a square. So $K(\sqrt{d' - \rho}) = K(\sqrt{d - \rho'})$. Similarly, there is a point $(d'', e'') = (d, e) + (d', e')$ with $K(\sqrt{d'' - \rho}) = K(\sqrt{d - \rho''})$. Corresponding to F there are thus three points (actually, cosets in $E^\circ(\mathbf{Q})/2E(\mathbf{Q})$) such that F is the field obtained by adjoining the coordinates of all the square roots of any of these points, and these three points correspond to an orbit of $\mathrm{Gal}(K/\mathbf{Q})$ in C_2.

Suppose $(x, y) \in E(\mathbf{Q})$ is also such that the coordinates of $\frac{1}{2}(x, y)$ lie in F. It is easy to see that $\mathrm{Gal}(F/K)$ acts on $\frac{1}{2}(x, y)$ in the same way as on $\frac{1}{2}(d, e)$, $\frac{1}{2}(d', e')$, or $\frac{1}{2}(d'', e'')$; for definiteness, assume it is $\frac{1}{2}(d, e)$. So (x, y) differs from (d, e) by an element of $2E(K)$. But, as shown above, the square root of an element of $E(\mathbf{Q})$ is controlled by the fourth-degree polynomial $q(X)$. It follows that if a rational point has a square root in $E(K)$, then it has one in $E(\mathbf{Q})$. Therefore $(x, y) \equiv (d, e) \bmod 2E(\mathbf{Q})$, so F corresponds to exactly three cosets of $E^\circ(\mathbf{Q})/2E(\mathbf{Q})$, hence to three elements of C_2. This agrees with the $t/3$ of Heilbronn's result.

Now suppose $(d, e) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$. Since $d - \rho$ is not totally positive, $K(\sqrt{d - \rho})/K$ is ramified at an infinite prime (in fact, at two of them). As before, this extension is unramified at all finite primes not above 2. If it were also unramified at 2, then it would be unramified at all finite primes but ramified at an infinite prime, which is impossible, since the narrow and wide class numbers are equal. Therefore $K(\sqrt{d - \rho})/K$ is ramified at 2. We can replace $d - \rho$ by $\beta = g^2(d - \rho)$, where g^2 is the exact denominator of d. If 2 divided β then, since $\{1, \rho, \rho^2\}$ is an integral basis for K, both $g^2 d$ and g^2 would be even. But then g^2 would not be the exact denominator of d. So β is prime to 2. Since $K(\sqrt{\beta})/K$ is wildly ramified at 2, the relative discriminant is divisible by 4 [3, p. 21]. But $\mathrm{Norm}(2\sqrt{\beta}) = -4\beta$, so the discriminant divides 4β. Therefore it is exactly 4, which implies that the absolute discriminant of $K(\sqrt{\beta}) = K(\sqrt{d - \rho})$ is 64 times the

square of the discriminant of K. It follows by a calculation with Artin L-functions, as in [7], that $\zeta(s)\zeta_6(s) = \zeta_3(s)\zeta_4(s)$, hence $D_6 = D_3D_4$, where $\zeta_i(s)$ and D_i are the Dedekind zeta function and the discriminant of the field of degree i (for $i = 4$, the field is K_4, generated by a root of $q(X)$). Therefore, the discriminant of the quartic field K_4 is 64 times the discriminant of K.

Finally, suppose $(d', e') \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$ yields the same set of conjugate quartic fields as (d, e). If $(d', e') \not\equiv (d, e) \bmod 2E(\mathbf{Q})$, then $(d'', e'') = (d, e) + (d', e') \in E^\circ(\mathbf{Q}) - 2E(\mathbf{Q})$. Therefore $K(\sqrt{d'' - \rho})/K$ is unramified, hence so is its Galois closure $K(\sqrt{d'' - \rho}, \sqrt{d'' - \rho'})/K$. But $(d - \rho)(d' - \rho)(d'' - \rho) \in (K^\times)^2$ (consider the map λ above), so $K(\sqrt{d'' - \rho}) \subseteq K(\sqrt{d - \rho}, \sqrt{d' - \rho})$. Since the latter field is Galois over $\mathbf{Q}$, we have $K(\sqrt{d'' - \rho}, \sqrt{d'' - \rho'}) \subseteq K(\sqrt{d - \rho}, \sqrt{d' - \rho})$, hence they are equal, since both have degree 12 (from the above, $K(\sqrt{d'' - \rho})/\mathbf{Q}$ cannot be Galois). But the first is unramified over K and the second is ramified at 2. Contradiction. So $(d', e') \equiv (d, e) \bmod 2E(\mathbf{Q})$.

We summarize what we have proved in the following

THEOREM 2. (a) *Let (d, e) denote a point in $E(\mathbf{Q})$, not in $2E(\mathbf{Q})$, and let $q(X)$ be the corresponding quartic polynomial (as in Proposition 4). The set of conjugate quartic fields K_4 determined by $q(X)$ depends only on the class of $(d, e) \bmod 2E(\mathbf{Q})$.*

(b) *If $(d, e) \in E^\circ(\mathbf{Q})$, then K_4 has the same discriminant as K. The extension $K(\sqrt{d - \rho})/K$ is unramified.*

(c) *If $(d, e) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, then the discriminant of K_4 is 64 times the discriminant of K. The extension $K(\sqrt{d - \rho})/K$ is ramified at 2 and at two infinite places.*

(d) *The splitting field of $q(X)$ is $K(\sqrt{d - \rho}, \sqrt{d - \rho'})$.*

(e) *If $Ш_2 = 0$, then each orbit (necessarily of length 3) of $\mathrm{Gal}(K/\mathbf{Q})$ in C_2 corresponds to three cosets in $E^\circ(\mathbf{Q})/2E(\mathbf{Q})$ with representatives (d_i, e_i), $i = 1, 2, 3$. We have $\sum(d_i, e_i) \in 2E(\mathbf{Q})$. The splitting fields of the corresponding polynomials are all equal to $K(\sqrt{d_1 - \rho}, \sqrt{d_2 - \rho})$. This field is also obtained by adjoining to $\mathbf{Q}$ the coordinates of all solutions of $2(x, y) = (d_i, e_i)$ for any fixed i.*

(f) *If $(d_i, e_i) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, $i = 1, 2$, yield the same set of conjugate quartic fields, then $(d_1, e_1) \equiv (d_2, e_2) \bmod 2E(\mathbf{Q})$.*

COROLLARY. *Suppose $(d, e) \in E^\circ(\mathbf{Q})$. Let $d = a/4^s b^2$ with $a \in \mathbf{Z}$, b odd, and $s \geqslant 0$ (a is odd if $s > 0$). Then*

(i) *if m is even, then $s > 0$ and $a \equiv 1 \bmod 4$;*

(ii) *if $m \equiv 1 \bmod 4$ and $s = 0$, then $a \equiv 3 \bmod 4$;*

(iii) *if $m \equiv 3 \bmod 4$ and $s = 0$, then $a \equiv 2 \bmod 4$;*

(iv) *if $m \equiv 1$ or $3 \bmod 4$ and $s > 0$, then $a \equiv 1 \bmod 4$.*

Proof. If $(d, e) \in E^\circ(\mathbf{Q})$, then $K(\sqrt{d - \rho})/K$ is unramified at 2, so $g^2(d - \rho)$ is a square mod 4, where g^2 is the denominator of d. This is true even if $(d, e) \in 2E(\mathbf{Q})$, since then $g^2(d - \rho)$ is actually a square. If $m \equiv 0$, or 2 (mod 4), then the only square residue classes mod 4 of the form $x + y\rho$ are $2 + \rho$ ($m \equiv 0$), $1 + \rho$ ($m \equiv 2$), and 1. Clearly, $g^2 d - g^2\rho$ cannot be congruent mod 4 to either of the first two choices. Therefore it must be the last, so $g^2 = 4^s b^2$ is even and $a = g^2 d \equiv 1 \bmod 4$. If $m \equiv 1 \pmod 4$, then the only suitable square congruence classes are 1 and $3 + 3\rho$, and if $m \equiv 3 \bmod 4$, they are 1 and $2 + 3\rho$. A similar analysis yields the result.

Note that these congruences do not hold for $E(\mathbf{Q}) - E^\circ(\mathbf{Q})$: $(-9, 17)$ is a point on $Y^2 = X^3 + 11X^2 - 14X + 1$.

We can now return to the polynomial $q(X)$, which we defined in the discussion preceding the theorem. More precisely, we start with the polynomial $f(X) = X^3 + mX^2 - (m+3)X + 1$ and a rational point (d, e) on $Y^2 = f(X)$. Translate to obtain

$$g(X) = f(X+d) = X^3 + (3d+m)X^2 + (3d^2 + 2md - m - 3)X + e^2.$$

Then $-g(-X)$ is the resolvent cubic of

$$Q(X) = X^4 - \tfrac{1}{2}(3d+m)X^2 + eX + \tfrac{1}{16}(-3d^2 - 2md + m^2 + 4m + 12).$$

This has nonintegral coefficients. But Shanks pointed out that this situation can sometimes be remedied by replacing $Q(X)$ by

$$Q(X + \tfrac{1}{2}) = X^4 + 2X^3 + \tfrac{1}{2}(-3d - m + 3)X^2 + \tfrac{1}{2}(-3d - m + 1 + 2e)X + \tfrac{1}{16}(-3d^2 - 2md + m^2 + 2m + 13 + 8e - 6d).$$

Suppose $m \equiv 3 \pmod 4$ and $d \in \mathbf{Z}$, so $d \equiv 2 \pmod 4$. Then e must be odd. A straightforward calculation shows that all the coefficients of $Q(X + \frac{1}{2})$ are integral, so in fact there is a quartic integral polynomial (not just a quartic field) of discriminant equal to that of K. Of course, if $(d, e) \in 2E(\mathbf{Q})$, then this polynomial is reducible, by the theorem. We note that the condition $(d, e) \in E^\circ(\mathbf{Q})$ is also necessary for the above procedure to work: We need $(d, e) \in E(\mathbf{Q})$ in order to make the constant term of $g(X)$ a square. If $(d, e) \in E(\mathbf{Q}) - E^\circ(\mathbf{Q})$, then the corresponding quartic field has discriminant 64 times the discriminant of $f(X)$, hence cannot equal the discriminant of $Q(X)$. So it is impossible to translate $Q(X)$ to obtain an integral polynomial.

5. Examples. We now give some examples. Let $m = 11$, $m^2 + 3m + 9 = 163$, so we are considering the curve

$$Y^2 = X^3 + 11X^2 - 14X + 1.$$

This has (at least) the following integral points: $(0,1) = A$, $(2,5) = B$, $(6,23) = C$, $(-4,13) = -A + B$, $(-9,17) = A + B$, $(-12,5) = A - B - C$, $(-1,5) = -A + C$, $(26,157) = -2A + C$, $(30,191) = B - C$, $(38,265) = 2A$, $(3170,178789) = -2A + B - C$, $(7502,650255) = -2A - B + 2C$. Of course, we can double the size of the list by including $(0,-1) = -A$, $(2,-5) = -B$, etc. Note that the points containing A but not $2A$ are those in $E(\mathbf{Q}) - E^\circ(\mathbf{Q})$. The points of $E(\mathbf{Q})/2E(\mathbf{Q})$ which we have listed are represented by the point at infinity (which we ignore) and $(2,5)$, $(6,23)$, $(0,1)$, $(-4,13)$, $(-12,5)$, $(-1,5)$, $(30,191)$. The corresponding polynomials $q(X)$ are easily seen to be irreducible, so none of these points is in $2E(\mathbf{Q})$. So $A = (0,1)$, $B = (2,5)$, and $C = (6,23)$ are independent mod $2E(\mathbf{Q})$; hence they are independent points of $E(\mathbf{Q})$. Therefore $E(\mathbf{Q})$ has rank at least 3. But the class number of K is 4 (see [10]), so Theorem 1 implies that $E(\mathbf{Q})$ has rank exactly 3. The theorem now implies that $K(\sqrt{2-\rho}, \sqrt{6-\rho})/K$ is the Hilbert class field of K.

Another interesting example is obtained by taking $m = 143$. Then $m^2 + 3m + 9$ is the prime 20887. The cubic field K has class number 64, so there is the possibility of a large rank for $E(\mathbf{Q})$. We have the following rather long list of integral points

(we do not guarantee the list is complete):

$$
\begin{aligned}
(0,1) &= A & (2,17) &= B\\
(-1,17) &= A + C - D & (6,67) &= C\\
(-4,53) &= -A + D & (30,389) &= D\\
(-28,307) &= A + C & (90,1369) &= E\\
(-33,353) &= -A + D + E & (114,1823) &= 2A + C - D\\
(-64,577) &= -A + B & (182,3277) &= C - D\\
(-81,647) &= A + B & (290,6031) &= B - C\\
(-105,659) &= A - B - D & (846,26603) &= -B + C + E\\
(-124,557) &= A + C + E & (854,26963) &= B - D - E\\
(-144,17) &= -A - B - C + D & (4182,275027) &= B + C + D + E\\
& & (5186,378577) &= 2A\\
& & (17342,2293147) &= -2A - C + D + E\\
& & (414290,266705281) &= -2A + B + C + D + E
\end{aligned}
$$

Of course, there are also the above points with the second coordinates negative. Note that the second coordinate of E is 37^2. By Proposition 2, $(90 - \rho) = I^4$. From Proposition 4, $(90 - \rho)$ is not the square of a principal ideal, so K has an ideal class of order 4. It is shown in [13, p. 187] that not only is the 2-rank of the class group even, but also the 4-rank, 8-rank, etc. Therefore the class group is either $(\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/4\mathbf{Z})^2$ or $(\mathbf{Z}/8\mathbf{Z})^2$. It is possible to show that A, B, C, D, E are independent mod $2E(\mathbf{Q})$, hence are independent. This can be done via Proposition 4. Therefore $E(\mathbf{Q})$ has rank at least 5, so the class group has rank at least 4. Consequently, the class group is $(\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/4\mathbf{Z})^2$, and $E(\mathbf{Q})$ has rank exactly 5.

It can be shown (we thank Daniel Shanks for the calculations) that each of the following groups of three points corresponds to a set of four conjugate quartic fields:

$$
\begin{aligned}
&B, C - D, B + C + D,\\
&C, -B + C + E, B + E,\\
&D, C + E, C + D + E,\\
&E, B - C + E, B + D,\\
&B - C, D + E, B + C + D + E.
\end{aligned}
$$

(A few of the above points were not listed previously, since they are rational but not integral.) This agrees with Heilbronn's theorem since the class group has 15 elements of order exactly 2, so there are $15/3 = 5$ sets of quartic fields. To get the fields of discriminant $64 \times (20887)^2$, consider the point A, and A added to each of the above points. This gives us 16 points of $E(\mathbf{Q}) - E^\circ(\mathbf{Q})$ which are noncongruent mod $2E(\mathbf{Q})$. By part (f) of the theorem, the corresponding quartic fields are nonconjugate.

We note that it follows from Theorem 1 that $Ш_2 = 0$ in both the above examples.

Instead of considering the curve E defined by $Y^2 = f(X)$, we could also have considered $Y^2 = -f(-X)$. We end up working with the same field, and the above analysis also works. But for some unexplained reason this curve does not work as well for obtaining information about the class group C_2, since $Ш_2$ empirically tends to be nontrivial in this case. For example, for $m = 11$, a calculation with the L-series for the curve indicates that Ш should have order 4, hence $Ш_2$ should have 2-rank 2. Since C_2 has rank 2, none of the class group should come from the curve, in contrast to the above.

For many years, several people have tried to find quadratic fields with large 3-rank in the class group. A corresponding problem is to find cubic fields with large 2-rank. This problem may be attacked in the spirit of a paper of Mestre [8]. Let E be the curve $Y^2 = X^3 + mX^2 - (m+3)X + 1$. Choose m so that $E \bmod p$ has a large number of points for all small p. This tends to yield curves with high rank; hence the corresponding cubic fields should have large 2-rank, as desired. For example, $m = 11$ is optimal for $p = 2, 3, 7, 11$ and $m = 143$ is optimal for $m = 2, 3, 5, 11$. The choice $m = 27038$ is optimal for $p \leqslant 23$, $p \neq 13$. Mestre's bounds [8] indicate that the rank of this curve should be at most 7, hence the cubic field could have a class group whose 2-rank is 6. However, it does not seem easy to find rational points on this curve.

Finally, we remark that it is possible to look at Proposition 3 geometrically when $n \geqslant 3$. This type of argument has been given by Mestre [9] in a slightly different situation.

Acknowledgment. The author wishes to thank R. Schoof, D. Shanks and D. Zagier for helpful conversations during the preparation of this paper.

Department of Mathematics
University of Maryland
College Park, Maryland 20742

1. W. ADAMS & M. RAZAR, "Multiples of points on elliptic curves and continued fractions," *Proc. London Math. Soc.*, v. 41, 1980, pp. 481–498.

2. A. BRUMER & K. KRAMER, "The rank of elliptic curves," *Duke Math. J.*, v. 44, 1977, pp. 715–743.

3. J. W. S. CASSELS & A. FRÖHLICH, *Algebraic Number Theory*, Thompson Book Co., Washington, D. C., 1967.

4. H. COHN, "A device for generating fields of even class number," *Proc. Amer. Math. Soc.*, v. 7, 1956, pp. 595–598.

5. T. CUSICK, "Lower bounds for regulators," *Number Theory (Noordwijkerhout*, 1983), Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 63–73.

6. H. EISENBEIS, G. FREY & B. OMMERBORN, "Computation of the 2-rank of pure cubic fields," *Math. Comp.*, v. 32, 1978, pp. 559–569.

7. H. HEILBRONN, "On the 2-classgroup of cubic fields," in *Studies in Pure Mathematics* (L. Mirsky, ed.), Academic Press, New York, 1971, pp. 117–119.

8. J. F. MESTRE, "Courbes elliptiques et formules explicites," *Séminaire Théorie des Nombres, Grenoble*, 1982.

9. J. F. MESTRE, "Groupes de classes d'idéaux non cycliques de corps de nombres," *Séminaire Théorie des Nombres, Paris*, 1981–1982, Birkhäuser, Boston-Basel-Stuttgart, 1983, pp. 189–200.

10. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.

11. J. TATE, "Algorithm for determining the type of a singular fiber in an elliptic pencil," *Modular Functions of One Variable IV*, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975, pp. 33–52.

12. K. UCHIDA, "Class numbers of cubic cyclic fields," *J. Math. Soc. Japan*, v. 26, 1974, pp. 447–453.

13. L. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

14. H. WEBER, *Lehrbuch der Algebra*, vol. I, 3rd ed., 1898; reprinted, Chelsea, New York, 1961.