ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 34, Number 2, Summer 2004

USING ELLIPTIC CURVES TO PRODUCE QUADRATIC NUMBER FIELDS OF HIGH THREE-RANK

MATT DELONG

ABSTRACT. We use a connection between the arithmetic of elliptic curves of the form $y^2 = x^3 + k$ and the arithmetic of the quadratic number fields $\mathbf{Q}(\sqrt{k})$ and $\mathbf{Q}(\sqrt{-3k})$ to look for quadratic fields with high three-rank. We give a geometric proof of known results on polynomials that give rise to infinite families of quadratic number fields possessing non-trivial lower bounds on their three-rank. We then generalize the method to produce infinitely many such polynomials. Finally, we produce specific examples of quadratic number fields with high three-rank.

1. Introduction. Previous authors have documented polynomials that give rise to infinite families of quadratic number fields possessing non-trivial lower bounds on their three-ranks [**2, 3, 8, 9**]. Their methods of proof were usually straight-forward but lengthy calculations involving ideals, or appeals to class field theory.

In this paper we give a new and shorter proof of the results on some of these families of fields. The method of proof leads us to a way of generating infinitely many such polynomials. The method is geometric in nature, and relies on a well-known connection between the arithmetic of elliptic curves of the form $y^2 = x^3 + d$ and the arithmetic of the quadratic number fields $\mathbf{Q}(\sqrt{d})$ and $\mathbf{Q}(\sqrt{-3d})$. We use a precise form of the connection, given by Satgé [**6**].

We first illustrate the method in detail on a family of Shanks [**8**]. We then discuss other previously discovered polynomials in our context. Following this, we show how to generalize our method to produce infinitely many such polynomials. Finally, we give some numerical data derived using some of our new polynomials.

The specific examples of three-ranks of quadratic fields, the orders of rational points on elliptic curves, and the conjectural upper bounds on

2000 AMS *Mathematics Subject Classification.* 11R29, 11G05.
Received by the editors on August 20, 2001.

ranks of elliptic curves were all calculated using GP/PARI Calculator version 2.0.11. The systems of equations solved with Maple were solved using Maple V, version 3.

2. A geometric proof of a result of Shanks. Shanks used the polynomial

$$D_3(t) = 27t^4 - 74t^3 + 84t^2 - 48t + 12 \tag{1}$$

to give an infinite family of quadratic imaginary fields each with non-cyclic 3-Sylow subgroup of the class group. Note that $D_3(t) > 0$ for all $t \in \mathbf{R}$.

Definition 2.1. *Series* 3 consists of the square-free values of $D_3(t_0)$ evaluated at integers $t_0 \equiv -1 \pmod 6$.

The following theorem was first proved by Shanks [**8**]. (By $r_3(a)$ we mean the 3-rank of the number field $\mathbf{Q}(\sqrt{a})$.)

Theorem 2.2. *All of the fields associated with Series* 3 *satisfy*

$$r_3(-D_3(t_0)) = r_3(3D_3(t_0)) + 1 \geq 2.$$

In order to derive Shanks's result in a different context, we study elliptic surfaces over $\mathbf{C}$ given by

$$y^2 = x^3 + k(t), \tag{2}$$

where $k(t) \in \mathbf{Q}[t]$ is an irreducible square-free polynomial of degree four. We note that (2) can also be considered as an elliptic curve over $\mathbf{C}(t)$, and we will interchange terminology throughout.

Shioda has given an algorithm for determining the Mordell-Weil lattice over $\mathbf{C}(t)$ for a rational elliptic surface, and for finding a finite set of sections that contain a set of generators for the lattice [**10**]. We apply this algorithm to (2) to obtain the following.

Lemma 2.3. *If $k(t)$ is an irreducible square-free degree-four polynomial, then the structure of the Mordell-Weil lattice over $\mathbf{C}(t)$ of*

$y^2 = x^3 + k(t)$ is E_6^*, and the rank of the Mordell-Weil group over $\mathbf{C}(t)$ is 6.

Proof. To apply Shioda's algorithm, we must find the reducible bad fibers of the surface $y^2 = x^3 + k(t)$. Using Tate's algorithm [**11**], we find that the surface has bad reduction over the roots of $k(t)$. Here the reduction is of type II, which is an irreducible bad fiber. At $t = \infty$, after making the change of variables

$$t = \frac{1}{s}, \quad y = \frac{y}{s^3}, \quad x = \frac{x}{s^2}, \tag{3}$$

we find that the reduction is of type IV, which is a reducible bad fiber of multiplicity 3.

By Theorem 10.4 of Shioda [**10**] the root lattice is $T = A_2$, and so the structure of the surface is E_6^*, and the $\mathbf{C}(t)$-rank of the curve is 6. □

The following corollary is a special case of Theorem 10.6 of Shioda [**10**].

Corollary 2.4. *If $k(t)$ is an irreducible square-free degree-four polynomial, then there are exactly 54 points of the form $(A(t+B), Ct^2 + Dt + E)$ on $y^2 = x^3 + k(t)$ where $A, B, C, D, E \in \mathbf{C}$, and these 54 points contain a set of generators for the Mordell-Weil group over $\mathbf{C}(t)$.*

One can easily verify that $-4D_3(t)$ is a square-free, irreducible, degree-four polynomial, and so we can apply Lemma 2.3 and Corollary 2.4 to

$$y^2 = x^3 - 4D_3(t). \tag{4}$$

We compute the 54 points of the form $(A(t + B), Ct^2 + Dt + E)$ on the surface directly, in order to find the field of definition for $E(\mathbf{C}(t))$, which is the smallest field k such that $E(k(t)) = E(\mathbf{C}(t))$.

Proposition 2.5. *The field of definition for $E(\mathbf{C}(t))$ for the surface $y^2 = x^3 - 4D_3(t)$ is $\mathbf{Q}(\sqrt{-3})$.*

Proof. Substituting $x = A(t + B)$ and $y = Ct^2 + Dt + E$ into $y^2 = x^3 - 4D_3(t)$, we obtain the following five polynomial relations on the coefficients of a section (x, y).

$$\begin{aligned} C^2 &= -108, \\ 2CD &= A^3 + 296, \\ 2CE + D^2 &= 3A^3B - 336, \\ 2DE &= 3A^3B^2 + 192, \end{aligned}$$

and

$$E^2 = A^3B^3 - 48.$$

Using Maple to solve this system, we obtain the coefficients of the 54 points. Since all 54 points are defined over $\mathbf{Q}(\sqrt{-3})(t)$, and these points contain a set of generators for the Mordell-Weil group by Corollary 2.4, the result follows. □

We now wish to specialize an elliptic curve E over the function field $K(t)$ to elliptic curves over K via the specialization map

$$\sigma_{t_0} : E(K(t)) \to E_{t_0}(K), \tag{5}$$

which sends each section of E to the point on E_{t_0} obtained by setting $t = t_0 \in K$. We need the following theorem, which is Theorem III.11.4 of Silverman [**11**] for the case that we study.

Theorem 2.6. *If E is an elliptic curve over the function field $K(t)$ that is not $K(t)$-isomorphic to an elliptic curve defined over K, then the specialization map σ_{t_0} is injective for all but finitely many $t_0 \in K$.*

Since the elliptic curve (4) is not isomorphic to one defined over $\mathbf{Q}(\sqrt{-3})$ and the $\mathbf{Q}(\sqrt{-3})(t)$-rank of (4) is 6 by Lemma 2.3 and Proposition 2.5, Theorem 2.6 implies that the $\mathbf{Q}(\sqrt{-3})$-rank of $y^2 = x^3 - 4D_3(t_0)$ is at least 6 for all but a finite number of $t_0 \in \mathbf{Z}$.

Because they have complex multiplication by a cube-root of unity, we can relate the $\mathbf{Q}(\sqrt{-3})$-ranks of these elliptic curves to their ranks over $\mathbf{Q}$. The following is a well-known result whose proof is an easy exercise.

Proposition 2.7. *If $E : y^2 = x^3 + k$ is an elliptic curve defined over* $\mathbf{Q}$*, where k is not a square, then the rank of E over $\mathbf{Q}(\sqrt{-3})$ is twice the rank of E over* $\mathbf{Q}$*.*

The following corollary is now immediate.

Corollary 2.8. *The rank of $y^2 = x^3 - 4D_3(t_0)$ over* $\mathbf{Q}$ *is at least 3 for all but finitely many $t_0 \in \mathbf{Z}$.*

We will relate the ranks of the elliptic curves to the three-ranks of the number fields by appealing to results of Satgé [**6**]. If $E : y^2 = x^3 + k$ and $E' : \eta^2 = \xi^3 - 27k$, then we let $\psi : E \to E'$ denote the quotient map

$$\xi = \frac{y^2 + 3}{x^2} \quad \text{and} \quad \eta = \frac{y(x^3 - 8k)}{x^3}, \tag{6}$$

and let $\psi' : E' \to E$ denote its dual isogeny. We denote the Selmer groups of ψ and ψ' respectively by S^{ψ} and $S^{\psi'}$. The following two propositions are the contents of Satgé's Lemma 3.1, Proposition 3.2 and Proposition 3.3.[1]

Proposition 2.9. *Assume that k is a $6-$th-power-free integer such that the following two conditions on k are satisfied.*

(a) *If $p \neq 2, 3$ is a prime such that $v_p(k) = 2$ or 4, then $p \equiv 1 \pmod 3$ and $k/p^{v_p(k)}$ is not a square modulo p.*

(b) *If $v_2(k) = 0$ or 2 then $k/2^{v_2(k)} \equiv 3 \pmod 4$.*

If

(c) *$v_3(k) = 0$ and $k \equiv 1, 2, 4, 8 \pmod 9$, or if $v_3(k) = 1$ and $k/3 \equiv 1 \pmod 3$, or if $v_3(k) = 2$ and $k/9 \equiv 2 \pmod 3$, or if $v_3(k) = 3$ and $k/27 \equiv 2, 4 \pmod 9$,*

then

$$\dim_{\mathbf{F_3}} S^{\psi} = r_3(k).$$

If

(c′) *$v_3(k) = 2$ and $k/9 \equiv 1 \pmod 3$,*

then

$$\dim_{\mathbf{F_3}} S^{\psi} \leq r_3(k).$$

Proposition 2.10. *Assume that k is a sixth power-free integer satisfying conditions* (a) *and* (b) *of the previous proposition. Then,*

$$\dim_{\mathbf{F_3}} S^{\psi'} = \begin{cases} r_3(k)+1, & \text{if } k>0, \\ r_3(k), & \text{if } k<0, \end{cases}$$

if k is in case (c) *of the previous proposition. In addition,*

$$\dim_{\mathbf{F_3}} S^{\psi'} \leq \begin{cases} r_3(k)+2, & \text{if } k>0, \\ r_3(k)+1, & \text{if } k<0, \end{cases}$$

if k is in case (c') *of the previous proposition.*

To apply the results of Satgé to the elliptic curves $y^2 = x^3 - 4D_3(t_0)$ obtained from Series 3, we must verify the conditions of Proposition 2.9. Since the values in Series 3 are square-free, condition (a) holds. To verify condition (b), we note that $v_2(-4D_3(t_0)) = 2$ since $t_0 \equiv -1 \pmod 6$ implies that t_0 is odd. Therefore, we check that $-D_3(t_0) \equiv 3 \pmod 4$ when t_0 is odd. We note that $v_3(-4D_3(t_0)) = 0$ for $t_0 \equiv -1 \pmod 6$, since this implies that $t_0 \equiv 2 \pmod 3$. Therefore, we check that for $t_0 \equiv 2 \pmod 3$, $-4D_3(t_0) \equiv 1 \pmod 9$.

Thus Proposition 2.9 and Proposition 2.10 give us that

$$\dim S^{\psi} = r_3(-D_3(t_0)) \quad \text{and} \quad \dim S^{\psi'} = r_3(-D_3(t_0)) \tag{7}$$

for $t_0 \equiv -1 \pmod 6$. Since the sum of the dimensions of the Selmer groups is an upper bound for the $\mathbf{Q}$-rank of the elliptic curve, by Corollary 2.8 we have the inequality

$$3 \leq 2r_3(-D_3(t_0)). \tag{8}$$

Since the three-rank must be an integer, equation (8) gives

$$2 \leq r_3(-D_3(t_0)), \tag{9}$$

which is the result of Theorem 2.2 on the three-rank of the imaginary field.

Combining equation (9) with the classical theorem of Scholz [**7**] gives

$$1 \leq r_3(3D_3(t_0)) \tag{10}$$

for the values in Series 3. In fact, Shanks [**8**] verified that these fields are in the escalatory case of Scholz's theorem.

Remark 2.11. Actually, in the last few paragraphs we have been overstating things a bit. Shanks's theorem is actually stronger than what we have obtained. He proved the result of Theorem 2.2 for *all* fields in Series 3, whereas our method only proves the result for all but finitely many values of Series 3. The method of this paper seems unlikely to obtain the result for all fields, since it relies on the specialization theorem of Silverman. This theorem does not give an effectively computable constant for the maximal height of the rational numbers for which the specializations may not be injective.

3. Other known polynomials. Shanks exhibited three other polynomials which give rise to families of quadratic fields with nontrivial three-ranks [**8**]. These polynomials are

$$\Delta(w) = 9w^4 - 74w^3 + 252w^2 - 432w + 324, \tag{11}$$

$$\Delta_2(x) = 36x^4 - 148x^3 + 252x^2 - 216x + 81, \quad \text{and} \tag{12}$$

$$D_6(z) = 108z^4 - 148z^3 + 84z^2 - 24z + 3 \tag{13}$$

Definition 3.1. *Series* 1 consists of the square-free values of $\Delta(w)$. *Series* 2 consists of the square-free values of $\Delta_2(x)$. *Series* 6 consists of the square-free values of $D_6(z)$ evaluated at $z_0 \equiv 1 \pmod 3$.

The following theorems are all due to Shanks. We use Shanks's notation, which is $r = r_3(k)$ and $s = r_3(-3k)$, where k is a value in Series 1, 2, or 6.

Theorem 3.2. *For Series* 1 *we have* $r = s \geq 1$.

Theorem 3.3. *With the exception of* $\Delta_2(1) = 5$*, which has* $r = s = 0$*, all Series* 2 *fields have* $r = s \geq 1$*.*

Theorem 3.4. *With the exception of* $D_6(1) = 23$*, which has* $r = 0$ *and* $s = 1$*, all Series* 6 *fields have* $s = r + 1 \geq 2$*.*

These results can be obtained for all but finitely many values of Series 1, Series 2, and Series 6 using the methods of the previous section by looking at the surfaces $y^2 = x^3 + 4\Delta(w)$, $y^2 = x^3 + 16\Delta_2(x)$, and $y^2 = x^3 - 16\Delta_6(z)$. The next section will provide an infinite family of such series.

The exceptional cases $\Delta_2(1) = 5$ and $D_6(1) = 23$ fail because of the noninjectivity of the specialization map from the elliptic surface to the elliptic curves. The surface $y^2 = x^3 + 16\Delta_2(x)$ has $\mathbf{Q}(x)$-rank three, as can be seen via the methods of the previous section. On the other hand, one can easily verify by classical descent that the $\mathbf{Q}$-rank of $y^2 = x^3 + 16\Delta_2(1)$ is one.

Similarly, although the surface $y^2 = x^3 - 16D_6(t)$ has $\mathbf{Q}(t)$-rank three, the elliptic curve $y^2 = x^3 - 16D_6(1)$ has $\mathbf{Q}$-rank two.

The unfortunate drawback to our method is that the possible noninjectivity of the specialization at finitely many specializations means that we can only state the results for all but finitely many quadratic fields in a particular family.

As a final example, Buell and Ennola [**3**] consider the polynomial

$$d(t) = t^4 + 14t^3 + 67t^2 + 126t + 49. \tag{14}$$

They prove the following

Theorem 3.5. *For integers* $t \not\equiv 0 \pmod 7$ *and* $t > 0$*,* $r_3(d(t)) = r_3(-3d(t)) \geq 1$*.*

By considering the surface $y^2 = x^3 + 16d(t)$, we can obtain similar results with our method. In fact, we can slightly improve the restriction $t \not\equiv 0 \pmod 7$. For example, $d(21) = 7^3 \times 1039$. In this case the restriction of Theorem 2.9 does not come into play, and one can check that $r_3(1039) = r_3(-3 \times 1039) = 1$. Therefore, the best restriction

would be to say that if $v_7(d(t)) \equiv 2, 4 \pmod 6$, which will by the way only occur when $t \equiv 0 \pmod 7$, then $d(t)/7^{v_7(d(t))}$ is not a square modulo 7.

4. A two-parameter family of fields. Our goal in this section is to mirror our analysis of $D_3(t)$ to find an infinite family of degree-four polynomials in $\mathbf{Q}[t]$, such that every polynomial in the family yields infinitely many real quadratic number fields of non-trivial three-rank. As in the previous section, we study elliptic curves over $\mathbf{C}(t)$ of the form

$$y^2 = x^3 + k(t), \tag{15}$$

where $k(t) \in \mathbf{Q}[t]$ is a polynomial of degree four.

Top [**12**] analyzed Shanks's polynomial $D_3(t)$ via the surface $y^2 = x^3 + 108D_3(t)$. This has $\mathbf{Q}$-sections with $x = 6t$ and $x = 6t - 8$, respectively. Making the change of variables $t \mapsto \frac{t}{6}$ in the polynomial $108D_3(t)$ yields the polynomial

$$d_3(t) = \frac{9}{4}\,t^4 - 37t^3 + 252t^2 - 864t + 1296. \tag{16}$$

The elliptic surface $y^2 = x^3 + d_3(t)$ thus has sections with $x = t$ and $x = t - 4/3$. Hence, we search for curves of the form (15) with similar sections.

We first parametrize those elliptic curves with a rational section of the form $(t, a_0t^2 + a_1t + a_2)$, where $a_0, a_1, a_2 \in \mathbf{Q}$. If (15) has such a section, then the polynomial $k(t)$ must be

$$k(t) = a_0^2\,t^4 + (2a_0a_1 - 1)t^3 + (2a_0a_2 + a_1^2)t^2 + 2a_1a_2t + a_2^2, \tag{17}$$

where $a_0 \neq 0$.

Now we impose the additional condition that (15) has a section with $x = t + b$ for some nonzero $b \in \mathbf{Q}$. This will be true precisely when

$$\begin{aligned}(t+b)^3 + k(t) = \\ a_0^2t^4 + 2a_0a_1\,t^3 + (2a_0a_2 + a_1^2 + 3b)t^2 + (2a_1a_2 + 3b^2)t + (a_2^2 + b^3)\end{aligned} \tag{18}$$

is a square in $\mathbf{C}[t]$.

We need the following lemma, whose proof involves only elementary algebra.

Lemma 4.1. *The polynomial*

$$p(t) = \alpha t^4 + \beta t^3 + \gamma t^2 + \delta t + \varepsilon \in \mathbf{C}[t]$$

is a square in $\mathbf{C}[t]$ *if and only if the following relations on the coefficients are satisfied*:

$$\beta^3 - 4\alpha\beta\gamma + 8\alpha^2\delta = 0$$

and

$$\epsilon\beta^2 - \alpha\delta^2 = 0$$

Applying Lemma 4.1 to the polynomial (18) we obtain the conditions on the coefficients a_0, a_1, a_2, b given by

$$b^2 a_0^2 (9b^2 - 4a_1^2\, b + 12a_1 a_2) = 0, \tag{19}$$

and

$$24a_0^3\, b(a_0 b - a_1) = 0. \tag{20}$$

Since $a_0 \neq 0$ and $b \neq 0$, condition (20) implies that

$$b = \frac{a_1}{a_0}. \tag{21}$$

Therefore, we can substitute for b into condition (19) to obtain the relation on the a_is given by

$$9\left(\frac{a_1}{a_0}\right)^2 - 4a_1^2\,\frac{a_1}{a_0} + 12a_1 a_2 = 0. \tag{22}$$

Clearing denominators, we have

$$-a_1(4a_1^2 a_0 - 9a_1 - 12a_0^2 a_2) = 0. \tag{23}$$

Since $a_0 \neq 0$ and $b \neq 0$, condition (24) implies that $a_1 \neq 0$. Therefore, the conditions (19) and (20) taken together imply that

$$a_1 = \frac{9 \pm \sqrt{81 + 192a_0^3\, a_2}}{8a_0}. \tag{24}$$

Since $a_0, a_1, a_2 \in \mathbf{Q}$, condition (24) implies that $81 + 192a_0^3\, a_2 \equiv 0 \pmod{\mathbf{Q}^{*2}}$. Write

$$81 + 192a_0^3\, a_2 = r^2, \tag{25}$$

where $r \in \mathbf{Q}$. Then

$$a_2 = \frac{r^2 - 81}{192a_0^2}, \tag{26}$$

and by substituting (24), choosing the positive square root, and (26) into (17) we obtain a two-parameter family of polynomials given by

$$\begin{aligned} k_{r,a_0}(t) = a_0^2\, t^4 &+ \left(\frac{r+5}{4}\right)t^3 + \left(\frac{(5r+9)(r+9)}{192a_0^2}\right)t^2 \\ &+ \left(\frac{(r+9)^2(r-9)}{768a_0^4}\right)t + \left(\frac{(r+9)^2(r-9)^2}{36864a_0^6}\right). \end{aligned} \tag{27}$$

Now, the polynomial $d_3(t)$ must be a member of the family (27) for an appropriate choice of a_0 and r. By inspection we see that $a_0 = 3/2$ and $r = -153$.

Because, as we saw in Section 2, the surface given by Shanks's polynomial has rank equal to three over $\mathbf{Q}(t)$, and therefore produces interesting quadratic fields, let us fix $r = -153$ in (27) and study the one-parameter family of polynomials

$$k_{-153,a_0}(t) = a_0^2 t^4 - 37t^3 + \frac{567}{a_0^2}\, t^2 - \frac{4374}{a_0^4}\, t + \frac{59049}{4a_0^6}. \tag{28}$$

By making the change of variables

$$x \longmapsto \frac{x}{a_0^2}, \quad y \longmapsto \frac{y}{a_0^3}, \quad t \longmapsto \frac{t}{a_0^2} \tag{29}$$

we have that the elliptic surface

$$y^2 = x^3 + k_{-153,a_0}(t) \tag{30}$$

is isomorphic over $\mathbf{Q}$ to

$$y^2 = x^3 + 64t^4 - 2368t^3 + 36288t^2 - 279936t + 944784. \tag{31}$$

The polynomial $64t^4 - 2368t^3 + 36288t^2 - 279936t + 944784$ is square-free and irreducible with only positive outputs, therefore the polynomials of the form (28) are likewise.

As we did with $D_3(t)$, we use Maple to obtain the 54 sections of (31) of the form $(A(t+B), Ct^2 + Dt + E)$. As before, we see that all 54 sections are defined over $\mathbf{Q}(\sqrt{-3})$. As in Section 3.2, combining Lemma 2.3, Corollary 2.4 and Proposition 2.7, we have that all the surfaces

$$y^2 = x^3 + k_{-153,a_0}(t), \tag{32}$$

where $a_0 \in \mathbf{Q}$, have $\mathbf{Q}(t)$-rank equal to three. By Theorem 2.6, for each surface, all but finitely many specializations will yield elliptic curves with $\mathbf{Q}$-rank at least 3.

We would now like to apply the results from Propositions 2.9 and 2.10 to the elliptic curves we obtain through specialization to a pair $(a_0, t_0) \in \mathbf{Q} \times \mathbf{Z}$, in order to generate quadratic number fields with high three-rank. Since the result of specializing $k_{-153,a_0}(t)$ to such a pair may not necessarily be an integer, we first generalize the results of Propositions 2.9 and 2.10 to rational k.

Proposition 4.2. *All statements in Propositions* 2.9 *and* 2.10 *of the form* $v_p(k) = n$ *may be changed to* $v_p(k) \equiv n \pmod 6$ *without changing the conclusions of the propositions.*

Proof. The elliptic curve $y^2 = x^3 + k$ is isomorphic to $y^2 = x^3 + r^6 k$ for any $r \in \mathbf{Q}$. Clearly the fields $\mathbf{Q}(\sqrt{k})$ and $\mathbf{Q}(\sqrt{r^6 k})$ are the same. Therefore, the results of the propositions are valid up to any change to k by a sixth power in $\mathbf{Q}$. □

Notice that Propositions 2.9 and 2.10 fail to cover some congruence classes of k modulo $3^6 = 729$. Some of these cases can be treated via the isogenous curve, which is $E' : y^2 = x^3 - k/27$ or $E' : y^2 = x^3 - 27k$ according as $27|k$ or not, as will be seen below. The missing cases are then $k \equiv 6 \pmod 9$ and $k \equiv 0, 81 \pmod{243}$.

Now suppose we have $a_0 \in \mathbf{Q}$ and $t_0 \in \mathbf{Z}$, and for notational convenience denote by $k = k_{-153,a_0}(t_0)$. Recall that $k > 0$, and assume that conditions (a) and (b) of Proposition 2.9 are satisfied. We obtain estimates on $r_3(k)$ and $r_3(-3k)$ using the results of Satgé and this section. The analysis breaks down into three cases, depending upon the congruence class of k modulo 729.

In the first case, combining Proposition 2.9, Proposition 2.10 and Proposition 4.2, we have

$$\dim_{\mathbf{F_3}} S^{\psi} = r_3(k), \quad \text{and} \quad \dim_{\mathbf{F_3}} S^{\psi'} = r_3(k) + 1 \tag{33}$$

if $v_3(k) = 0$ and $k \equiv 1, 2, 4, 8 \pmod 9$, or if $v_3(k) = 1$ and $k/3 \equiv 1 \pmod 3$, or if $v_3(k) = 2$ and $k/9 \equiv 2 \pmod 3$, or if $v_3(k) = 3$ and $k/27 \equiv 2, 4 \pmod 9$.

In the second case,

$$\dim_{\mathbf{F_3}} S^{\psi} \le r_3(k), \text{ and } \dim_{\mathbf{F_3}} S^{\psi'} \le r_3(k) + 2 \tag{34}$$

if $v_3(k) = 2$ and $k/9 \equiv 1 \pmod 3$.

In the third case, we use the isogenous curve and the results of Satgé to obtain the bounds. If $k \equiv 5, 7 \pmod 9$, then $v_3(-27k) = 3$ and $-27k/27 \equiv 4, 2 \pmod 9$ respectively. Likewise, if $k \equiv 27, 135, 189, 216 \pmod{243}$, then $v_3(-k/27) = 0$ and $-k/27 \equiv 8, 4, 2, 1 \pmod 9$ respectively. Finally, if $k \equiv 162 \pmod{243}$, then $v_3(-k/27) = 1$ and $-k/81 \equiv 1 \pmod 3$. In all these cases, the results of Proposition 2.9 can be applied to the isogenous curve to obtain

$$\dim_{\mathbf{F_3}} S^{\psi} \le r_3(-3k), \quad \text{and} \quad \dim_{\mathbf{F_3}} S^{\psi'} \le r_3(-3k) \tag{35}$$

All but finitely many of the elliptic curves $y^2 = x^3 + k_{-153,a_0}(t_0)$ have $\mathbf{Q}$-rank at least 3. Therefore, in (33) we have

$$3 \le 2r_3(k) + 1. \tag{36}$$

Since $r_3(k)$ must be an integer we have that $r_3(k) \geq 1$, and hence by Scholz's theorem $r_3(-3k) \geq 1$. In (34) we have

$$3 \leq 2r_3(k) + 2. \tag{37}$$

Here again $r_3(k) \geq 1$ and $r_3(-3k) \geq 1$. Lastly in (35) we have

$$3 \leq 2r_3(-3k). \tag{38}$$

Therefore, $r_3(-3k) \geq 2$, and by Scholz's theorem $r_3(k) \geq 1$.

We have proved the following

Theorem 4.3. *For $a_0 \in \mathbf{Q}s$ and $t_0 \in \mathbf{Z}$, let $k = k_{-153,a_0}(t_0)$. Suppose that the following three conditions on k are satisfied.*

(a) *If $p \neq 2, 3$ is a prime such that $v_p(k) \equiv 2, 4 \pmod 6$, then $p \equiv 1 \pmod 3$ and $k/p^{v_p(k)}$ is not a square modulo p.*

(b) *If $v_2(k) \equiv 0, 2 \pmod 6$, then $k/2^{v_2(k)} \equiv 3 \pmod 4$.*

(c) *$k \not\equiv 6 \pmod 9$ and $k \not\equiv 0, 81 \pmod{243}$.*

Then for a fixed a_0, for all but finitely many t_0 we have

$$r_3(k) \geq 1 \quad \textit{and} \quad r_3(-3k) \geq 1.$$

Moreover, for certain congruence classes of k modulo 729, we can achieve

$$r_3(k) \geq 1 \quad \textit{and} \quad r_3(-3k) \geq 2.$$

Thus, we have achieved the stated goal of producing an infinite family of polynomials, each with the property that it produces fields with nontrivial three-rank for almost every integer input, and such that the family contains Shanks's polynomials as special cases. In Table 1 we include some sample fields arising via this method.

Finally, we notice that the best case is when we achieve the inequality (38). Here we obtain three-ranks of imaginary fields that are at least 2, which by the heuristic of Cohen and Lenstra [**4**] are somewhat rare. For a given $a_0 \in \mathbf{Z}$ not divisible by 3, we can restrict t to a specific congruence class modulo 9 in order that k is always in this case, as seen in the following proposition.

TABLE 1. Three-ranks generated from $k(t)$ when $a_0 = 1$.

t	$k(t)$	Δ	$r_3(k(t))$	$r_3(-3k(t))$
1	$2^{-2} \times 3^2 \times 23 \times 211$	23×211	1	1
2	$2^{-2} \times 32009$	32009	2	2
3	$2^{-2} \times 3^3 \times 863$	3×863	1	1
4	$2^{-2} \times 3 \times 5 \times 7^2 \times 23$	$3 \times 5 \times 23$	0	0
5	$2^{-2} \times 12269$	12269	1	2
6	$2^{-2} \times 3^3 \times 331$	3×331	1	1
7	$2^{-2} \times 3 \times 37 \times 59$	$3 \times 37 \times 59$	1	1
8	$2^{-2} \times 47 \times 103$	47×103	1	1

Proposition 4.4. *Suppose a_0 and t are integers. If $a_0 \equiv 1, 8 \pmod 9$, then $t \equiv 5 \pmod 9$ implies that $k \equiv 5 \pmod 9$. If $a_0 \equiv 2, 7 \pmod 9$, then $t \equiv 8 \pmod 9$ implies that $k \equiv 5 \pmod 9$. If $a_0 \equiv 4, 5 \pmod 9$, then $t \equiv 2 \pmod 9$ implies that $k \equiv 5 \pmod 9$.*

Proof. By obtaining a common denominator, we have

$$k = \frac{4a_0^8 t^4 - 148a_0^6 t^3 + 2268a_0^4 t^2 - 17496a_0^2 t + 59049}{4a_0^6}. \tag{39}$$

Now, $a_0^6 \equiv 1 \pmod 9$ for a_0 not divisible by 3. In addition, $4^{-1} \equiv 7 \pmod 9$. Therefore, $k \equiv a_0^8 t^4 - t^3 \pmod 9$. The results of the proposition are then easily verified by congruence arithmetic for the various combinations of a_0 and t modulo 9. □

By making the change of variables $t = 9x + 5$ in (27), we obtain

$$\begin{aligned} \hat{k}_1(x) &= 6561a_0^2 x^4 + (14580a_0^2 - 26973)x^3 \\ &\quad + \left(\frac{12150a_0^4 - 44955a_0^2 + 45927}{a_0^2}\right)x^2 \\ &\quad + \left(\frac{4500a_0^6 - 24975a_0^4 + 51030a_0^2 - 39366}{a_0^4}\right)x \\ &\quad + \left(\frac{2500a_0^8 - 18500a_0^6 + 56700a_0^4 - 87480a_0^2 + 59049}{4a_0^6}\right). \end{aligned} \tag{40}$$

Similarly, the substitution $t = 9x + 8$ yields

(41)
$$\begin{aligned}\hat{k}_2(x) &= 6561a_0^2\,x^4 + (23328a_0^2 - 26973)x^3 \\ &\quad + \left(\frac{31104a_0^4 - 71928a_0^2 + 45927}{a_0^2}\right)x^2 \\ &\quad + \left(\frac{18432a_0^6 - 63936a_0^4 + 81648a_0^2 - 39366}{a_0^4}\right)x \\ &\quad + \left(\frac{16384a_0^8 - 75776a_0^6 + 145152a_0^4 - 139968a_0^2 + 59049}{4a_0^6}\right).\end{aligned}$$

Likewise $t = 9x + 2$ yields

(42)
$$\begin{aligned}\hat{k}_4(x) &= 6561a_0^2\,x^4 + (5832a_0^2 - 26973)x^3 \\ &\quad + \left(\frac{1944a_0^4 - 17982a_0^2 + 45927}{a_0^2}\right)x^2 \\ &\quad + \left(\frac{288a_0^6 - 3996a_0^4 + 20412a_0^2 - 39366}{a_0^4}\right)x \\ &\quad + \left(\frac{64a_0^8 - 1184a_0^6 + 9072a_0^4 - 34992a_0^2 + 59049}{4a_0^6}\right).\end{aligned}$$

In the next lemma we show that condition (b) of Theorem 4.3 is automatically satisfied by any $k_{-153,a_0}(t_0)$ when $a_0, t_0 \in \mathbf{Z}$.

Lemma 4.5. *For any $a_0, t_0 \in \mathbf{Z}$, we have $v_2(k_{-153,a_0}(t_0)) \equiv 4 \pmod 6$.*

Proof. By writing k as in (39), we see that $v_2(k_{-153,a_0}(t_0)) = -2 - 6v_2(a_0)$. This is clearly congruent to 4 modulo 6. □

We then have the following theorem.

Theorem 4.6. *For $a_0 \equiv \pm i \pmod 9$ and $x \in \mathbf{Z}$, where $i \in \{1, 2, 4\}$, let $k = \hat{k}_i(x)$. Suppose that if $p \neq 2, 3$ is a prime such that $v_p(k) \equiv 2, 4 \pmod 6$, then $p \equiv 1 \pmod 3$ and $k/p^{v_p(k)}$ is not a square modulo p.*

Also suppose that $k \not\equiv 6 \pmod 9$ *and* $k \not\equiv 0, 81 \pmod{243}$. *Then for a fixed* a_0, *for all but finitely many* x *we have*

$$r_3(k) \geq 1 \quad \textit{and} \quad r_3(-3k) \geq 2.$$

In Tables 2, 3 and 4, we include some examples of fields obtained from these translated polynomials. In addition, a couple of fields of particularly high three rank were found by the author using $\hat{k}_1$ when $a_0 = 1$. For example, $\Delta = 4\hat{k}_1(1087) = 36575780952596681$, which is prime, has associated fields with three ranks $r_3(\Delta) = 4$ and $r_3(-3\Delta) = 5$. Similarly, $\Delta = 4\hat{k}_1(1437) = 111759971248983881 = 173 \times 977 \times 661219441661$ has associated fields with three ranks $r_3(\Delta) = 4$ and $r_3(-3\Delta) = 5$. By the heuristic of Cohen and Lenstra [**4**], the probability of finding a quadratic field with $r_3(d) = 5$ "at random" is on the order of 10^{-12}. The record for highest $r_3(d)$ seems to be six [**5**].

TABLE 2. Three-ranks generated from $\hat{k}_1(x)$ when $a_0 = 1$.

x	$\hat{k}_1(x)$	Δ	$r_3(\hat{k}_1(x))$	$r_3(-3\hat{k}_1(x))$
1	$2^{-2} \times 5 \times 1237$	5×1237	1	2
2	$2^{-2} \times 175061$	175061	1	2
3	$2^{-2} \times 7^2 \times 23801$	23801	0	1
4	$2^{-2} \times 43 \times 98999$	43×98999	1	2
5	$2^{-2} \times 17 \times 23 \times 71 \times 409$	$17 \times 23 \times 71 \times 409$	2	2
6	$2^{-2} \times 5 \times 761 \times 6569$	$5 \times 761 \times 6569$	2	2
7	$2^{-2} \times 48346121$	48346121	1	2
8	$2^{-2} \times 41 \times 2078149$	41×2078149	2	3

TABLE 3. Three-ranks generated from $\hat{k}_2(x)$ when $a_0 = 2$.

x	$\hat{k}_2(x)$	Δ	$r_3(\hat{k}_2(x))$	$r_3(-3\hat{k}_2(x))$
1	$2^{-8}\times 48346121$	43846121	1	2
2	$2^{-8}\times 5\times 64846741$	5×64846741	2	3
3	$2^{-8}\times 1172590409$	1172590409	2	2
4	$2^{-8}\times 131\times 271\times 87277$	$131\times 271\times 87277$	1	2
5	$2^{-8}\times 211\times 32075699$	211×32075699	1	2
6	$2^{-8}\times 131\times 229\times 433639$	$131\times 229\times 433639$	2	2
7	$2^{-8}\times 5\times 7^2\times 93099781$	5×93099781	0	1
8	$2^{-8}\times 37320079529$	37320079529	1	2

TABLE 4. Three-ranks generated from $\hat{k}_4(x)$ when $a_0 = 5$.

x	$\hat{k}_4(x)$	Δ	$r_3(\hat{k}_4(x))$	$r_3(-3\hat{k}_4(x))$
1	$2^{-2}\times 5^{-6}\times 4513\times 4423973$	4513×4423973	1	2
2	$2^{-2}\times 5^{-6}\times 232058311049$	232058311049	2	2
3	$2^{-2}\times 5^{-6}\times 7^2\times 373\times 57444137$	373×57444137	0	1
4	$2^{-2}\times 5^{-6}\times 3133163807849$	3133163807849	2	3
5	$2^{-2}\times 5^{-6}\times 7387521633749$	7387521633749	1	2
6	$2^{-2}\times 5^{-6}\times 397\times 37694480717$	397×37694480717	1	2
7	$2^{-2}\times 5^{-6}\times 1481\times 2437\times 7553617$	$1481\times 2437\times 7553617$	1	2
8	$2^{-2}\times 5^{-6}\times 367\times 2663\times 46990369$	$367\times 2663\times 46990369$	2	3

5. Concluding remarks. One could try to play the same game with the surface $y^2 = x^3 + 16d(t)$ associated with Buell and Ennola's polynomial (14). This surface is isomorphic over $\mathbf{Q}$ to the surface $y^2 = x^3 + 16d(-t/8)$. This latter surface has sections $(t, 1/16t^2 + 9/2t - 28)$ and $(-t + 56, 1/16t^2 - 23/2t + 420)$. Therefore, one could hope to parametrize the surfaces with sections satisfying $x = t$ and $x = -t + b$ for some nonzero $b \in \mathbf{Q}$. As in the previous section, one could then look for an infinite family of polynomials that give rise to quadratic number fields of high three-rank by determining a family of such surfaces that have as the field of definition for $E(\mathbf{C}(t))$ the field $\mathbf{Q}(\sqrt{-3})$.

As a final note, we remark that Bremner [**1**] has classified those elliptic surfaces of the form

$$y^2 = x^3 + k(t) \tag{43}$$

for $k(t) \in \mathbf{Q}[t]$ of degree less than or equal to three according to their rank over $\mathbf{Q}(t)$. If one could obtain a similar classification for $k(t)$ of degree 4, the methods of this paper show that the surfaces with $\mathbf{Q}(t)$-rank three would correspond to the polynomials that yield infinite families of quadratic fields of high three-rank.

ENDNOTE

1. There is a misprint in Lemma 3.1 and a misprint in Proposition 3.2. In 3.1 where Satgé writes $k/2^{v_2(k)} \equiv 3 \pmod 8$, he means $k/2^{v_2(k)} \equiv 3 \pmod 4$, as can be seen from the statement of his Lemma 1.13. In 3.2 where he writes $k/9 \equiv 2 \pmod 9$, he means $k/9 \equiv 2 \pmod 3$, as can be seen from the statement of his Theorem 1.14.

REFERENCES

1. A. Bremner, *Some simple elliptic surfaces of genus zero*, Manuscripta Math. **73** (1991), 5–37.

2. D.A. Buell, *Class groups of quadratic number fields*, Math. Comp. **30** (1976), 610–623.

3. D.A. Buell and V. Ennola, *On a parametrized family of quadratic and cubic fields*, J. Number Theory **54** (1995), 134–148.

4. H. Cohen and H.W. Lenstra, Jr., *Heuristics on class groups of number fields*, in *Number theory*, Noordwijkerhourt, 1983; Springer-Verlag, New York, 1984.

5. J. Quer. Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, C.R. Acad. Sci. Paris **305** (1987), 215–218.

6. P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory **23** (1986), 294–317.

7. A. Scholz, *Über die beziehung der klassenzahlen quadratischer körper zueinander*, J. Reine Angew Math. **166** (1932), 201–203.

8. D. Shanks, *New types of quadratic fields having three invariants divisible by* 3, J. Number Theory **4** (1972), 537–556.

9. D. Shanks and P. Weinberger, *A quadratic field of prime discriminant requiring three generators for its class group, and related theory*, Acta Arith. **21** (1972), 71–87.

10. T. Shioda, *On the Mordell-Weil lattices*, Comm. Math. Univ. Sancti Pauli **39** (1990), 211–240.

11. J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

12. J. Top, *Descent by* 3*-isogeny and* 3*-rank of quadratic fields*, in *Advances in number theory*, Oxford Univ. Press, Oxford, 1993.

Department of Mathematics, Taylor University, 236 W. Reade Ave., Upland, IN 46989
E-mail address: mtdelong@tayloru.edu