

Descent by 3-isogeny and 3-rank of quadratic fields

Jaap Top

September 1991

Abstract

In this paper families of elliptic curves admitting a rational isogeny of degree 3 are studied. It is known that the 3-torsion in the class group of the field defined by the points in the kernel of such an isogeny is related to the rank of the elliptic curve. Families in which almost all the curves have rank at least 3 are constructed. In some cases this provides lower bounds for the number of quadratic fields which have a class number divisible by 3.

1 Introduction

By the 3-rank $r_3(K)$ of a number field K we will mean the dimension (as a vector space over the field with 3 elements \mathbf{F}_3) of the 3-torsion in the class group of K . As usual one writes $r_3(d) := r_3(\mathbf{Q}(\sqrt{d}))$. A remarkable classical result of Scholz says that the numbers $r_3(d)$ and $r_3(-3d)$ differ by at most 1. Most other literature on the function $r_3(d)$ concerns its possible values.

So far, the record seems to be $r_3(d) = 6$. In his thesis written in 1987, Quer exhibited 3 negative integers d for which this value is taken [Qu1],[Qu2]. The method exploited is that one can show that under certain conditions $2r_3(d) + 1$ is an upper bound for the rank of the group of \mathbf{Q} -rational points on the elliptic curve given by $y^2 = x^3 + d$. Given d such that this curve has rank 12, one obtains $r_3(d) \geq 6$.

By class field theory the 3-torsion in the class group of $\mathbf{Q}(\sqrt{d})$ corresponds to degree 3 Galois extensions of $\mathbf{Q}(\sqrt{d})$ which are unramified at all finite primes. Unramified extensions with –more generally– Galois group the alternating group A_n have been constructed by Fröhlich and by Uchida [Uch]. An example in case $n = 3$ (with in fact even more special properties) is given by the fields $\mathbf{Q}(\sqrt{-27m^2 - 4m})$, for any integer m which cannot be written in the form $n^3 - n^2$. This last example appears in a recent paper of Brinkhuis [Br].

From the example given above it follows easily that infinitely many fields $\mathbf{Q}(\sqrt{d})$ exist for which $r_3(d) \geq 1$. The same holds for $r_3(d) \geq 2$ (Shanks, [Sha]) and even

$r_3(d) \geq 4$ (Craig, [Cr]). We will discuss the weakest of such results, namely $r_3(d) \geq 1$. The reason to do this is that we hope it illustrates a general method, which is probably also of interest in other situations.

The method consists of studying the relation between the rank of certain elliptic curves and the 3-rank. Firstly it is shown that Quer's technique hinted at above applies more generally to any elliptic curve admitting a rational 3-isogeny. This puts classical work of Selmer and of Cassels and more recently of Satgé [Sat] and Nekovář [Ne] on rank calculations for elliptic curves with j -invariant 0 into a more general framework.

Next we construct families of elliptic curves for which this relation is valid. The rational points on the generic curve in such a family yield a group equipped with a well-understood quadratic form. Our examples will illustrate how the theory of these so-called Mordell-Weil lattices as developed by Shioda immediately gives a lot of useful information about the families under consideration.

Specializing the parameter in our families to a rational number now gives elliptic curves for which our theory works. Hence some lower bound (which may well be zero) for r_3 of the fields involved holds. The d 's obtained in this way are upto a square the values of some binary form. Using estimates of the number of square free values taken by binary forms (compare [St-T]) one can hope to obtain a density result for the number of quadratic fields with positive 3-rank. Unfortunately it seems that one has to put rather restrictive conditions on a family to obtain non-trivial bounds.

2 Results

To state the results of this paper some notation is needed. Let $E/\mathbf{C}(t)$ be an elliptic curve which is not isomorphic over $\mathbf{C}(t)$ to a curve already defined over \mathbf{C} . As in [Shi, 8.5 and 8.6] the finitely generated abelian group $E(\mathbf{C}(t))$ is equipped with a height pairing.

By A_2^* the lattice $\frac{1}{3}\sqrt{-3}\mathbf{Z}[-\frac{1}{2} + \frac{1}{2}\sqrt{-3}]$, with the quadratic form $\text{tr}(x\bar{y})$ is denoted. Alternatively one can describe it as the dual of the root lattice of the Lie group A_2 . Similarly one has A_1^* which is just \mathbf{Z} with the quadratic form $x^2/2$.

Theorem 2.1 *Let E be an elliptic curve given by $y^2 = x^3 + a(t)(x - b)^2$, in which $b \in \overline{\mathbf{Q}}^*$ and in which $a(t) \in \overline{\mathbf{Q}}[t]$ is a polynomial of degree 2.*

Assume that neither $a(t)$ nor $4a(t) + 27b$ is a square.

Then the Mordell-Weil lattice $E(\overline{\mathbf{Q}}(t))$ equipped with the height pairing is isomorphic to $A_1^ \oplus A_2^*$. The points with x -coordinate $x = b$ generate the A_1^* ; the remaining 6 points with constant x -coordinate correspond to the vectors with minimal norm in A_2^* (and hence they generate, too).*

Corollary 2.2 *With the notation from Theorem 2.1, let $a(t) = t^2 - (\beta^2 + \beta + 1)^3$ and $b = (\beta^2 + \beta)^2$, for a $\beta \in \mathbf{Q}$ with $\beta \neq 0, -1$.*

Then $E(\overline{\mathbf{Q}}(t)) = E(\mathbf{Q}(t)) \cong \mathbf{Z}^3$.

Concerning the relation between ranks of certain elliptic curves over \mathbf{Q} and 3-rank of quadratic fields the following general statement holds.

Theorem 2.3 Denote by $E_{a,b}/\mathbf{Q}$ the elliptic curve which is given by the equation $y^2 = x^3 + a(x - b)^2$ with $a, b \in \mathbf{Z}$, $a \neq 0, b \neq 0, 4a + 27b \neq 0$. Assume

1. $a \equiv 3 \pmod{4}$ and $b \equiv 1 \pmod{2}$ (or $a \equiv 1 \pmod{2}$ and $b \equiv 2 \pmod{4}$);
2. $a \equiv 2 \pmod{3}$;
3. a is square free.

Write s for the number of primes $p \geq 5$ such that $p|b$ and the Legendre symbol $(\frac{a}{p}) = 1$. Similarly let t denote the number of primes $p \geq 5$ for which $p|4a + 27b$ and $(\frac{-3a}{p}) = 1$.

Then

$$\text{rank } E_{a,b}(\mathbf{Q}) \leq r_3(a) + r_3(-3a) + s + t + 1.$$

3 Rational 3-isogenies

We recall some general facts about 3-isogenies. For the basic theory of elliptic curves Silverman's book [Sil] is an excellent reference.

Let K be a field of characteristic different from 2, 3. Suppose E/K is an elliptic curve and $T \subset E(\bar{K})$ is a subgroup of order 3 which is stable under the action of $\text{Gal}(K^{\text{sep}}/K)$. We can give E/K by an equation $y^2 = f(x)$ with f of degree 3. In these coordinates T consists of the point at infinity (the standard convention to take this point as the zero for the group law on E is used), plus two other points $P = (\alpha, \beta)$ and $2P = -P = (\alpha, -\beta)$. The Galois invariance implies $\alpha \in K$ and $\beta^2 \in K$. By a change of coordinates we can assume $\alpha = 0$. The curve is now given by an equation $y^2 = x^3 + ax^2 + cx + d$, and the point $(0, \sqrt{d})$ on this curve has order 3 precisely when $c^2 = 4ad$.

In case $c = 0$ our equation is $y^2 = x^3 + d$. In the other case $c \neq 0$ the equation can be written as $y^2 = x^3 + a(x - b)^2$.

Dividing out by the subgroup T yields another elliptic curve, which is again equipped with a rational subgroup of order 3. The function field of this curve is the subfield of $K(x, y)$ generated by the functions $x + \xi + \xi'$ and $y + \eta + \eta'$. Here (ξ, η) and (ξ', η') are the functions describing translation over the points $(0, \sqrt{d})$ and $(0, -\sqrt{d})$ respectively:

$$(\xi, \eta) = (x, y) + (0, \sqrt{d})$$

where '+' denotes addition in the group law on E .

One can choose coordinates on the new curve such that it is given in the same way as the original curve E . In particular, the rational subgroup on it (which corresponds to the 3-torsion points on E modulo T) is again given by points with first coordinate 0. A routine calculation reveals:

Case E : $y^2 = x^3 + a(x - b)^2$: The quotient curve E/T is given by the equation

$$\eta^2 = \xi^3 - 27a(\xi - 4a - 27b)^2$$

and the quotient map by

$$\xi = 9(2y^2 + 2ab^2 - x^3 - \frac{2}{3}ax^2)x^{-2} \text{ and } \eta = 27y(-4abx + 8ab^2 - x^3)x^{-3}.$$

Case E : $y^2 = x^3 + d$: The quotient curve E/T is given by the equation

$$\eta^2 = \xi^3 - 27d$$

and the quotient map by

$$\xi = (y^2 + 3d)x^{-2} \text{ and } \eta = y(x^3 - 8d)x^{-3}.$$

Repeating the process, i.e., taking the quotient by the new subgroup on the new curve, corresponds to taking the quotient by all 3-torsion on the original curve; this is just multiplication by 3.

Explicit formulas for isogenies as the one above can be obtained more generally (using the same ideas) from a paper of Vélu [Ve].

4 The Kummer sequence of a rational 3-isogeny

In this section the procedure for relating the rank of elliptic curves admitting a 3-isogeny as above to the 3-rank of certain quadratic fields is discussed. For the little bits of Galois cohomology needed, any textbook on the topic will suffice; we need nothing beyond the relevant Appendix in Silverman's book [Sil].

If one has to compute the rank of an elliptic curve E over a number field K , the usual strategy is to bound this rank from above by embedding a quotient $E(K)/nE(K)$ into a more understandable finite group. The relatively easy case where $K = \mathbf{Q}$, $n = 2$ and multiplication by 2 can be factored as a product of isogenies of degree 2 is well known; the first written account of it seems to be the Haverford Lectures by Tate which form the basis of Husemöller's book on elliptic curves. The next simplest case is the one to be discussed here. In Tate's situation the target group is a finite subgroup of $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Here following Quer we land in a finite subgroup of

$$\text{Kernel } K^*/K^{*3} \xrightarrow{\text{Norm}} \mathbf{Q}^*/\mathbf{Q}^{*3},$$

in which K/\mathbf{Q} is a quadratic extension. We start by introducing these subgroups and showing their relation to the class group of K .

Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic extension of \mathbf{Q} . The Norm homomorphism $N : K^* \rightarrow \mathbf{Q}^*$ given by $N(a + b\sqrt{d}) = a^2 - b^2d$ (for $a, b \in \mathbf{Q}$) induces a homomorphism $K^*/K^{*3} \rightarrow \mathbf{Q}^*/\mathbf{Q}^{*3}$ which will also be denoted N .

For a finite set of primes $p_1, \dots, p_t \in \mathbf{Z}$ which all split in K , write

$$H(p_1, \dots, p_t) := \{x \in \text{Ker}(N) ; v_\wp(x) \bmod 3 = 0 \ \forall \wp \in \mathcal{S} \text{ with } p_1 \cdot \dots \cdot p_t \notin \wp\}$$

in which \mathcal{S} denotes the set of all split primes of K/\mathbf{Q} . Decomposing the ideal of an $x \in K^*$ whose norm is a cube into prime ideals, and using that $v_\wp(x) + v_{\overline{\wp}}(x) \equiv 0 \bmod 3$, one obtains

Lemma 4.1

$$\dim_{\mathbf{F}_3} H(p_1, \dots, p_t) \leq r_3(d) + t + \dim_{\mathbf{F}_3} U/U^3.$$

Here U denotes the units in the ring of integers of K , hence the dimension of U/U^3 is 1 if d is positive or $K = \mathbf{Q}(\sqrt{-3})$ and 0 otherwise.

Suppose E/\mathbf{Q} is an elliptic curve admitting a rational 3-isogeny $\psi : E \rightarrow E'$. Write ψ' for the dual isogeny; so $\psi'\psi$ is multiplication by 3 on E . If one assumes that E has no point of order 3 defined over \mathbf{Q} , or equivalently that both the kernel of ψ and the kernel of ψ' contain no non-trivial rational point, then

$$\text{rank } E(\mathbf{Q}) = \dim_{\mathbf{F}_3} E(\mathbf{Q})/3E(\mathbf{Q}).$$

Moreover under our assumptions the group written on the right fits in the exact sequence

$$0 \rightarrow E'(\mathbf{Q})/\psi E(\mathbf{Q}) \xrightarrow{\psi'} E(\mathbf{Q})/3E(\mathbf{Q}) \longrightarrow E(\mathbf{Q})/\psi'E'(\mathbf{Q}) \rightarrow 0.$$

What remains to be done is estimating the dimensions on the left and the right in the above sequence. Here Galois cohomology comes in. Write $G_K = \text{Gal}(\overline{\mathbf{Q}}/K)$. In the preceding section it was shown that the kernel T of ψ consists of points which are rational over a field $\mathbf{Q}(\sqrt{d})$. The ‘Kummer sequence of our 3-isogeny’

$$0 \rightarrow T \rightarrow E(\overline{\mathbf{Q}}) \rightarrow E'(\overline{\mathbf{Q}}) \rightarrow 0$$

yields a long exact sequence

$$\dots \rightarrow E(\mathbf{Q}) \rightarrow E'(\mathbf{Q}) \rightarrow H^1(G_{\mathbf{Q}}, T) \rightarrow \dots$$

and therefore an injection

$$E'(\mathbf{Q})/\psi E(\mathbf{Q}) \longrightarrow H^1(G_{\mathbf{Q}}, T).$$

Let K be any quadratic extension of \mathbf{Q} and $\langle \tau \rangle = \text{Gal}(K/\mathbf{Q})$. From the inflation-restriction sequence one obtains an injection (in fact an isomorphism)

$$H^1(G_{\mathbf{Q}}, T) \longrightarrow H^1(G_K, T)^{\langle \tau \rangle}.$$

The action of $\langle \tau \rangle$ on $H^1(G_K, T)$ here is given on cocycles as ${}^\tau \xi(\sigma) = \tilde{\tau}(\xi(\tilde{\tau}\sigma\tilde{\tau}^{-1}))$ in which $\tilde{\tau}$ is any element of $G_{\mathbf{Q}}$ which acts on K by τ .

In the situation we consider it seems very natural to take the restriction to $G_{\mathbf{Q}(\sqrt{d})}$. This is what Satgé [Sat] does. The group $G_{\mathbf{Q}(\sqrt{d})}$ acts trivially on T , hence the H^1 consists of homomorphisms from $G_{\mathbf{Q}(\sqrt{d})}$ to $\mathbf{Z}/3\mathbf{Z}$, or equivalently of cubic cyclic extensions of $\mathbf{Q}(\sqrt{d})$. There is however a second restriction which appears helpful, namely the one to $G_{\mathbf{Q}(\sqrt{-3d})}$. We will use the latter restriction; it is also considered by Quer [Qu1].

One has $T \cong \mu_3$ as $G_{\mathbf{Q}(\sqrt{-3d})}$ -modules, hence using Hilbert 90 one obtains

$$H^1(G_{\mathbf{Q}(\sqrt{-3d})}, T) \cong H^1(G_{\mathbf{Q}(\sqrt{-3d})}, \mu_3) \cong \mathbf{Q}(\sqrt{-3d})^*/\mathbf{Q}(\sqrt{-3d})^{*3}.$$

Note that we deal with the $\langle \tau \rangle$ -invariants of the first group. It is clear that a lifting $\tilde{\tau}$ fixes all of T precisely when it acts by inversion on μ_3 . Hence the action induced on $\mathbf{Q}(\sqrt{-3d})^*/\mathbf{Q}(\sqrt{-3d})^{*3}$ is not the natural one, but the one given by ${}^\tau x = \tau(x)^{-1}$. In particular the invariants are given as the kernel of the norm map.

Summarizing, one obtains an injective homomorphism

$$E'(\mathbf{Q})/\psi E(\mathbf{Q}) \longrightarrow \text{Ker} (N : \mathbf{Q}(\sqrt{-3d})^*/\mathbf{Q}(\sqrt{-3d})^{*3} \rightarrow \mathbf{Q}^*/\mathbf{Q}^{*3}).$$

Using the explicit description of the morphism ψ as given in the previous section, and the definition of the various maps in cohomology it turns out that this injection can be given (upto a choice of an isomorphism $T \cong \mu_3$) as

$$(x, y) \mapsto (y + \sqrt{-27k}) \cdot \mathbf{Q}(\sqrt{-3k})^{*3}$$

in case E' is given by $y^2 = x^3 - 27k$, and

$$(x, y) \mapsto (y + (x - 4a - 27b)\sqrt{-27a}) \cdot \mathbf{Q}(\sqrt{-3a})^{*3}$$

in case E' is defined by an equation $y^2 = x^3 - 27a(x - 4a - 27b)^2$. However this explicit description will not be used.

The next task will be to bound the image of this injection. This is done by showing it is contained in a group $H(p_1, \dots, p_t)$ as defined above. Let $p \in \mathbf{Z}$ be a prime which splits in $K = \mathbf{Q}(\sqrt{-3d})$. Take $\wp|p$ in K . Assume $p \neq 3$; then for $x \in K^*/K^{*3}$ to have $v_\wp(x) \bmod 3 = 0$ precisely means that x maps to 1 under the composition

$$K^*/K^{*3} \longrightarrow \mathbf{Q}_p^*/\mathbf{Q}_p^{*3} \longrightarrow \mathbf{Q}_p^{\text{un}*}/\mathbf{Q}_p^{\text{un}*3}.$$

Here the first map is defined using φ and \mathbf{Q}_p^{un} denotes the maximal unramified extension of \mathbf{Q}_p . In virtue of the commutative diagram

$$\begin{array}{ccc} E'(\mathbf{Q})/\psi E(\mathbf{Q}) & \longrightarrow & K^*/K^{*3} \\ \downarrow & & \downarrow \\ E'(\mathbf{Q}_p)/\psi E(\mathbf{Q}_p) & \longrightarrow & \mathbf{Q}_p^*/\mathbf{Q}_p^{*3} \\ \downarrow & & \downarrow \\ E'(\mathbf{Q}_p^{\text{un}})/\psi E(\mathbf{Q}_p^{\text{un}}) & \longrightarrow & \mathbf{Q}_p^{\text{un}*}/\mathbf{Q}_p^{\text{un}*3} \end{array}$$

(in which all the horizontal arrows are injections) this means that the only primes $p \neq 3$ we need to consider are the ones that split in K , and moreover the map

$$E'(\mathbf{Q}_p)/\psi E(\mathbf{Q}_p) \longrightarrow E'(\mathbf{Q}_p^{\text{un}})/\psi E(\mathbf{Q}_p^{\text{un}})$$

is not the zero map.

Note that the prime $p = 3$ of course needs special attention. However, by assuming 3 does not split in K this can be completely avoided. Let $p \neq 3$ be given; we assume that the equations defining E and E' are both minimal at p and that both curves have either good reduction at p or reduction of type II or I_ν^* for some $\nu \geq 0$. For $p = 2$ this can be achieved with the curve given by $y^2 = x^3 + a(x - b)^2$ by demanding $a \equiv 3 \pmod{4}, b \equiv 1 \pmod{2}$, or $a \equiv 1 \pmod{2}, b \equiv 2 \pmod{4}$. In both these situations E and E' have reduction of type II. For $p \geq 5$ one has good reduction if $p \nmid ab(4a + 27b)$; type II reduction if $p \mid a, p \nmid b(4a + 27b)$ and type I_ν^* reduction if $p \mid a, p \mid b$. Recall the standard notation [Sil, Chapter VII] or [ModFu IV, pp. 41–46] $E_0(\mathbf{Q}_p)$ is the group of points which reduce mod p to points in the smooth part $E_0(\mathbf{F}_p)$ of $E(\mathbf{F}_p)$, and $E_1(\mathbf{Q}_p)$ is the kernel of the reduction map $E_0(\mathbf{Q}_p) \rightarrow E_0(\mathbf{F}_p)$.

By the minimality assumption ψ maps E_i to E'_i . Moreover the assumption on the reduction implies that the quotients $E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)$ and $E'(\mathbf{Q}_p)/E'_0(\mathbf{Q}_p)$ are isomorphic to groups of order 1, 2 or 4. Hence the Kernel-Cokernel sequence of the commutative diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & E_0(\mathbf{Q}_p) & \longrightarrow & E(\mathbf{Q}_p) & \longrightarrow & (*) \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & E'_0(\mathbf{Q}_p) & \longrightarrow & E'(\mathbf{Q}_p) & \longrightarrow & (*) \rightarrow 0 \end{array}$$

yields $E'(\mathbf{Q}_p)/\psi E(\mathbf{Q}_p) \cong E'_0(\mathbf{Q}_p)/\psi E'_0(\mathbf{Q}_p)$.

To compute the latter quotient (or rather its image over \mathbf{Q}_p^{un}) one uses the same technique applied to the diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & E_1(\mathbf{Q}_p^{\text{un}}) & \longrightarrow & E_0(\mathbf{Q}_p^{\text{un}}) & \longrightarrow & E_0(\overline{\mathbf{F}_p}) \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & E'_1(\mathbf{Q}_p^{\text{un}}) & \longrightarrow & E'_0(\mathbf{Q}_p^{\text{un}}) & \longrightarrow & E'_0(\overline{\mathbf{F}_p}) \rightarrow 0. \end{array}$$

The vertical arrow on the left is an isomorphism since multiplication by 3 defines an isomorphism on both E_1 and E'_1 ([Sil, IV.2.3 and VII.2.2]). The vertical arrow on the right

is surjective, hence it follows that the image of $E'(\mathbf{Q}_p)/\psi E(\mathbf{Q}_p)$ in $E'(\mathbf{Q}_p^{\text{un}})/\psi E(\mathbf{Q}_p^{\text{un}})$ is zero.

Note that in fact the above argument is only needed in case $p = 2$ and in case $p \geq 5$ such that E has good reduction at p . In the remaining cases p does not split in K , hence we can ignore it. Note also that the argument applies verbatim to the dual isogeny ψ' .

The proof of Theorem 2.3 is now almost complete. Assume the conditions mentioned in 2.3. By the argument given above, the group $E_{a,b}(\mathbf{Q})/\psi'E_{a,b}'(\mathbf{Q})$ injects into $H(p_1, \dots, p_t)$, where the p_i are all primes such that $(\frac{a}{p_i}) = 1$ and $E_{a,b}$ has multiplicative reduction at p_i . Assume p is such a prime, then working over \mathbf{Q}_p^{un} we have two cases:

1. If $p^n \mid 4a + 27b$ and $n > 0$ then one obtains a commutative diagram with exact rows and columns

$$\begin{array}{ccccccc} 0 \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0 \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \rightarrow & 0 & \rightarrow & E'_0(\mathbf{Q}_p^{\text{un}}) & \rightarrow & E_0(\mathbf{Q}_p^{\text{un}}) \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \rightarrow & \mathbf{Z}/3\mathbf{Z} & \rightarrow & E'(\mathbf{Q}_p^{\text{un}}) & \rightarrow & E(\mathbf{Q}_p^{\text{un}}) \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \rightarrow & \mathbf{Z}/3\mathbf{Z} & \rightarrow & \mathbf{Z}/3n\mathbf{Z} & \rightarrow & \mathbf{Z}/n\mathbf{Z}. \end{array}$$

It follows that $E(\mathbf{Q}_p^{\text{un}})/\psi'E'(\mathbf{Q}_p^{\text{un}}) \cong E_0(\mathbf{Q}_p^{\text{un}})/\psi'E'_0(\mathbf{Q}_p^{\text{un}})$. Since ψ' induces isomorphisms on the first and third group in the sequence

$$E'_1(\mathbf{Q}_p^{\text{un}}) \longrightarrow E'_0(\mathbf{Q}_p^{\text{un}}) \longrightarrow \overline{\mathbf{F}_p}^*$$

we conclude that the quotient we are computing is zero in this case.

2. The remaining case is $p \mid b$. Here the analogous argument shows that the quotient over \mathbf{Q}_p^{un} is cyclic of order 3, and the quotient one obtains over \mathbf{Q}_p surjects onto it. Hence these primes can not be avoided in general.

A similar argument shows that for the dual isogeny precisely the primes p of multiplicative reduction and $p \mid 4a + 27b$ and $(\frac{b}{p}) = 1$ have to be taken. Since $(\frac{-3a}{p}) = (\frac{b}{p})$ for $p \mid 4a + 27b$ this finishes the proof of Theorem 2.3. \square

5 Some applications of the rank estimate

We will briefly discuss an attempt to prove the existence of many quadratic fields with a high 3-rank. First, note that e.g. Brinkhuis's example mentioned in the introduction already yields using the sieving results from [St-T]

$$\# \{d \in \mathbf{Z} ; |d| < T \text{ \& } r_3(d) \neq 0\} \geq C \cdot T^{1/2}$$

for a positive constant C .

The simplest way to obtain positive 3-rank via our approach seems to be to look for elliptic curves of moderately high rank, such that by the method described above one obtains an estimate $r_3(d) + r_3(-3d) > 0$. Since it appears hard to find curves with very high rank, one may look for curves with rank 2 or 3, such that the invariants s and t appearing in the statement of Theorem 2.3 are 0.

An example is provided by the curves given as $E_a : y^2 = x^3 + 7a(x + a)^2$ in which a is a non-zero square free integer satisfying $a \equiv 5 \pmod{12}$. This curve is the quadratic twist over $\mathbf{Q}(\sqrt{a})$ of the one given by $y^2 = x^3 + 7(x + 1)^2$. For any such a the estimate

$$\text{rank } E_a(\mathbf{Q}) \leq 1 + r_3(7a) + r_3(-21a)$$

holds. Under the assumption of a parity conjecture which claims that this rank equals modulo 2 the order of vanishing of a certain L -series, one can show following Mazur and Gouv  a that indeed we obtain the ‘density exponent’ $1/2$ already given above. Note however that this is not unconditional! An account on the problem of finding many twists with high rank is given in [St-T].

A second example is given by the family $E_d : y^2 = x^3 + 16d^3$. From Satg  ’s paper [Sat] or from Quer’s thesis [Qu1] or using a computation analogous to the one given in the preceding section one shows that for every square free d one has

$$\text{rank } E_d(\mathbf{Q}) \leq 1 + r_3(d) + r_3(-3d).$$

These are quadratic twists of the curve given by $y^2 + y = x^3$.

One could hope to use the following idea to get better density exponents. Suppose given a curve $E : y^2 = x^3 + a(t)(x - b)^2$ over the function field $\mathbf{Q}(t)$, in which b is a constant and $a(t)$ a polynomial of degree 2. Suppose moreover that the rank of $E(\mathbf{Q}(t))$ is ‘high’. Then for almost all specializations of t to a rational number c/d , the rank remains at least as high. The specialization can be given by an equation $y^2 = x^3 + d^2a(c/d)(x - bd^2)^2$, hence writing

$$A(c, d) = d^2a(c/d)$$

(which is a binary quadratic form), we deal with the family of fields $\mathbf{Q}(\sqrt{A(c, d)})$. Although this defines indeed a set of discriminants which has density exponent 1, it seems hard to control the ‘error terms’ s and t appearing in Theorem 2.3 for all curves in such a family. In the remaining two sections of this paper a construction of such pairs $a(t), b$ will be given.

One can try to describe constructions appearing in the literature on 3-rank using the language of elliptic curves as above. To illustrate this, consider Shanks’s polynomial $D_3(t) = 27t^4 - 74t^3 + 84t^2 - 48t + 12$ (or an other polynomial dealt with by him as, e.g., $D_6(t)$ defined by $4D_6(t) = D_3(2t)$). Shanks has proven in [Sha] that many of the fields

$\mathbf{Q}(\sqrt{-D_3(t_0)})$ have 3-rank at least 2. In order to relate this result to elliptic curves, consider $E_{D_3}/\mathbf{Q}(t)$ given by $y^2 = x^3 + 108D_3(t)$. Using the results from § 10 in Shioda's paper [Shi] it follows that this curve has $\overline{\mathbf{Q}}(t)$ -rank 6. Since the Mordell-Weil group is a module over the endomorphism ring of the curve one deduces from this that the $\mathbf{Q}(t)$ -rank is at most 3. Moreover, again using [Shi], one finds a set of generators among the 18 points $(\rho x_1, \pm y_1)$, $(\rho x_2, \pm y_2)$, $(\rho x_3, \pm y_3)$ in which $\rho^3 = 1$ and x_i is a polynomial of degree 1. The points with x -coordinates $x = 6t$ and $x = 6t - 8$ yield such generators, hence $\text{rank } E_{D_3}(\mathbf{Q}(t)) \geq 2$. Apparently Shanks's result can be interpreted as the statement that under certain congruence conditions on $t_0 \in \mathbf{Z}$, these points map to independent elements in the class group part of $H^1(G_{\mathbf{Q}}, T)$.

A similar example, which is one of many given in a paper of Buell [Bu], is the curve

$$E : y^2 = 4x^3 + t^4 + 10t^3 - 305t^2 - 416946t - 3321607.$$

From the theory of Mordell-Weil lattices it follows that the $\mathbf{Q}(t)$ -rational points with x -coordinates $4t+94$, $2t+252$ and $-6t+538$ generate $E(\overline{\mathbf{Q}}(t))$ as a module over $\text{End}(E)$.

6 Families of rational 3-isogenies and Mordell-Weil lattices

In this section we will work over an algebraically closed field K of characteristic 0. Suppose an elliptic curve E over $K(t)$ is given, satisfying the conditions of Theorem 2.1. Multiplying the x and y function by a scalar and changing t to $\alpha t + \beta$ we may assume E is given by an equation

$$y^2 = x^3 + (t^2 + c)(x - 1)^2$$

in which $c \in K$ satisfies $c \neq 0$ and $4c + 27 \neq 0$.

From the work of Kodaira (compare [Shi]) it follows that one can regard $E/K(t)$ as the generic fibre of an elliptic surface $f : S \rightarrow \mathbf{P}^1$, which is called the Kodaira-Néron model of $E/K(t)$. Moreover, in our case this surface is rational, as is e.g. explained in [Shi, 10.13-10.14]. A result of Oguiso and Shioda [Og-Shi] implies that the structure of the Mordell-Weil lattice $E(K(t))$ in this situation is usually completely determined by the singular fibres of $f : S \rightarrow \mathbf{P}^1$.

An algorithm for determining these bad fibres and their respective types is given by Tate in [ModFu IV]. One finds fibres of type II over the zeroes of $t^2 + c = 0$ and fibres of type I₁ over the t 's satisfying $4t^2 + 4c + 27 = 0$. The only remaining bad fibre is over $t = \infty$. To compute it, change coordinates

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

The equation becomes $\eta^2 = \xi^3 + (cs^2 + 1)(\xi - s^2)^2$ and one concludes easily that over $t = \infty$, which corresponds to $s = 0$ one has a fibre of type I₆.

The Main Theorem in [Og-Shi] immediately implies that $E(K(t)) \cong A_1^* \oplus A_2^*$ which proves part of Theorem 2.1. What remains to be proven is that the points with constant x -coordinate yield the desired generators. We first compute these points. If a point with $x = \alpha$ is on the curve, then $(t^2 + c)(\alpha - 1)^2 + \alpha^3$ has to be a square in $K[t]$. In case $\alpha = 1$ this defines a constant, hence a square. In case $\alpha \neq 1$ we deal with a polynomial of degree 2. If it is a square then a square root must be of the form $(\alpha - 1)t + \beta$. One checks $\beta = 0$ and α is a zero of $X^3 + c(X - 1)^2$.

Next we compute the height $h(P)$ of these points. An explicit formula for it appears in [Shi, 8.12]. Using the notations from that paper, one has

$$h(P) = 2 + 2(PO) - \text{contr}_\infty(P).$$

Here (PO) is the intersection number of the sections in S defined by the point P and the point at infinity O . Since $P = (\alpha, *)$ it is clear that these sections do not intersect over any finite value of t . Over $t = \infty$ one uses the ξ, η, s -coordinates given above to conclude that also here is no intersection. Hence $(PO) = 0$.

The remaining term $\text{contr}_\infty(P)$ appearing in the formula for the height is a bit more subtle. Recall that at $t = \infty$ we have a special fibre of type I_6 , which is a 6-gon. The term we have to compute depends on which of the components of this 6-gon the section defined by P meets. If it meets the same one as the zero-section, then the contribution is 0. If it meets a component next to this one we have contribution $5/6$. The components ‘two steps away’ from the identity component yield value $4/3$, and the one opposite to it $3/2$.

Locally the section defined by P is given by $x = \alpha, y = \beta t + \gamma$. Hence in the ξ, η, s -coordinates by $\xi = \alpha s^2, \eta = \beta s^2 + \gamma s^3$. The Kodaira-Néron model is obtained by repeatedly blowing up the singularities of the surface we have, and normalizing. Hence we have to do this process and inspect what happens with the given section. Most of the geometry we need is explained in [HAG, pp. 28–29].

In \mathbf{A}^3 with coordinates ξ, η, s the only singularity of the surface defined locally by $y^2 = \xi^3 + (cs^2 + 1)(\xi - s^2)^2$ becomes visible as the point $\xi = \eta = s = 0$. The blow up of \mathbf{A}^3 in this point is locally described in $\mathbf{A}^3 \times \mathbf{A}^2$ by the equations $ux = vy, x = vs, y = us$. Hence the strict transform of our surface is given by $u^2 = v^3 s + (cs^2 + 1)(v - s)^2$. The fibre over $s = 0$ becomes a triangle, of which one sees only two sides using our coordinates. The section we study becomes $v = \alpha s, u = \beta s + \gamma s^2$ and it is clear that in the special fibre we obtain precisely the singular point of the new surface. Since this singularity $u = v = s = 0$ is also the intersection point of the two new components meeting the identity component, it follows that $0 \neq \text{contr}_\infty(P) \neq 5/6$.

We blow up once more by introducing new coordinates w, z satisfying $u = vw, uz = ws, s = zv$. The new equation is $w^2 = v^2 z + (cz^2 v^2 + 1)(1 - z^2)^2$. Our section is now given by $1 = \alpha z, w = \beta z + \gamma z^2 v$. The point $w = v = 0, z = 1$ is the only singularity of this surface. The part of the special fibre not meeting this singularity is in the $z = 0$ -plane. The ‘new’ part, contained in the plane given by $v = 0$, contains the section we

study. One checks that if $\alpha \neq 1$ then the point we obtain in the special fibre is not the singular point. Hence in this case our section meets a component ‘two steps away from the identity component’, so $\text{contr}_\infty(P) = 4/3$. In case $\alpha = 1$ we do get the singular point, hence our section meets the component which shows up in the next blow up, and which is opposite to the identity component.

It follows that the points with $x = 1$ have height $1/2$ and the remaining ones with constant x -coordinate height $2/3$. Hence these are precisely the points with minimal norm in the Mordell-Weil lattice. This proves Theorem 2.1.

7 Examples with all sections defined over \mathbf{Q}

From Theorem 2.1 it is obvious how to deduce Corollary 2.2. Hence it seems to be more interesting to show how one obtains such examples. We will now give a construction of elliptic curves E over $\mathbf{Q}(t)$ of the kind studied in the previous section, such that all the points in $E(\overline{\mathbf{Q}}(t))$ are already $\mathbf{Q}(t)$ -rational.

Let $a(t) \in \mathbf{Q}[t]$ be a polynomial of degree 2 and $b \in \mathbf{Q}^*$. Assume neither $a(t)$ nor $4a(t) + 27b$ has a double zero. Write $E : y^2 = x^3 + a(t)(x - b)^2$ as before. The Galois group $G_{\mathbf{Q}} = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the Mordell-Weil lattice $E(\overline{\mathbf{Q}}(t)) \cong A_1^* \oplus A_2^*$. The $G_{\mathbf{Q}}$ -invariants $E(\mathbf{Q}(t))$ can therefore be decomposed as the ones coming from A_1^* and the ones coming from A_2^* . The first group is infinite cyclic, hence the invariants are either (0) or all of the group. A generator is given by $(x = b, y = b\sqrt{b})$. hence we have invariants here precisely when b is a square.

The generators of A_2^* are the points whose x -coordinate satisfy a certain cubic relation. Hence the $G_{\mathbf{Q}}$ -action here is also easily determined. Without loss of generality we may assume $a(t)$ is of the form $a(t) = ct^2 + d$. In order to have invariants among the generators one certainly needs c to be a square. If this is the case, we may as well assume $c = 1$. What remains is that zeroes of $X^3 + d(X - b)^2$ have to be rational.

The number of rational zeroes of the polynomial above is the same as the number of rational points of order 2 on the elliptic curve given by $y^2 = x^3 + d(x - b)^2$. This is exactly a curve as is studied in this paper, namely one which admits a rational isogeny of degree 3. It turns out to be possible to write down a family of elliptic curves having both properties (in fact, the moduli space of elliptic curves having these properties is rational). An example of such a family shows up in a classical problem investigated by Fermat (compare [Za]). Namely, for a parameter β , consider the curve defined by the equations

$$1 + \beta^2 x = u^2, \quad 1 + (\beta + 1)^2 x = v^2, \quad 1 + x = w^2.$$

This defines an elliptic curve; choosing a zero, the group of rational points over $\mathbf{Q}(\beta)$ is in fact $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. Using the classical methods of writing such a curve in Weierstrass

form (as explained e.g. in [Weil, pp. 135-139]) one obtains the equation

$$Y^2 = X^3 + (\beta^2 + \beta + 1)^2 \left(X + \frac{\beta^2(\beta + 1)^2}{\beta^2 + \beta + 1} \right)^2.$$

Since we prefer a term $(X - b)^2$ in which b is a square we now twist this curve over the field $\mathbf{Q}(\beta, \sqrt{-\beta^2 - \beta - 1})$, which yields precisely the constants listed in the statement of Corollary 2.2.

As a last remark, note how subtle it seems to obtain fields with positive 3-rank using the family of curves just constructed. Namely, for every specialization we have a curve $y^2 = x^3 + a(x - b)^2$ in which b is a square. Hence the condition b is a square mod p is satisfied for all primes p . This means that the ‘error term’ $s+t$ appearing in Theorem 2.3 seems very hard to avoid.

References

- [ModFu IV] B. J. Birch and W. Kuyk, *Modular Functions of One Variable IV*, Springer-Verlag, LNM 476 (1975).
- [Br] J. Brinkhuis, *Normal integral bases and the Spiegelungssatz of Scholz*, preprint, Erasmus University Rotterdam (1990).
- [Bu] D.A. Buell, *Class groups of quadratic fields*, Math. of Comp., **30** (1976), pp. 610–623.
- [Cr] M. Craig, *A construction for irregular discriminants*, Osaka J. Math., **14** (1977), pp. 365–402.
- [HAG] R. Hartshorne, *Algebraic Geometry*. Springer Verlag, New York - Berlin - Heidelberg - Tokyo (1977).
- [Ne] J. Nekovář, *Class numbers of quadratic fields and Shimura’s correspondence*, Math. Ann., **287** (1990), pp. 577–594.
- [Og-Shi] K. Oguiso and T. Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, preprint, 1991.
- [Qu1] J. Quer, *Sobre el 3-rang dels Cossos Quadràtics i la Corba El·lítica $Y^2 = X^3 + M$* , Ph.D. thesis, 1987.
- [Qu2] J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C.R. Acad. Sci. Paris, **305** (1987), pp. 215–218.

- [Sat] Ph. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory, **23** (1986), pp. 294–317.
- [Sha] D. Shanks, *New types of quadratic fields having three invariants divisible by three*, J. Number Theory, **4** (1972), pp. 537–556.
- [Shi] T. Shioda, *On the Mordell-Weil Lattices*, Comm. Math. Univ. Sancti Pauli, **39** (1990), pp. 211–240.
- [Sil] J. Silverman, *The Arithmetic of Elliptic Curves*. Springer Verlag, New York - Berlin - Heidelberg - Tokyo (1986).
- [St-T] C. Stewart and J. Top, *On twists of elliptic curves having rank at least two*, in preparation.
- [Uch] K. Uchida, *Unramified extensions of quadratic number fields II*, Tôhoku Math. J., **22** (1970), pp. 220–224.
- [Ve] J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris, **273** (1971), pp. 238–241.
- [Weil] A. Weil, *Number Theory*. Birkhäuser, Boston - Basel - Stuttgart (1983).
- [Za] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jber. d. Dt. Math. Verein., **92** (1990), pp. 58–76.

Erasmus University Rotterdam,
Econometric Institute,
P.O. Box 1738,
3000 DR Rotterdam,
the Netherlands.