ACTA ARITHMETICA
178.2 (2017)

An explicit construction for unramified quadratic extensions of biquadratic fields

by

Debopam Chakraborty and Anupam Saikia (Guwahati)

1. Introduction. The class group of a number field K measures how far its ring of integers is from having unique factorization into irreducible elements. It is the quotient of the group of all fractional ideals of K by the subgroup of principal fractional ideals. It is well known from class field theory that the ideal class group is also the Galois group of the maximal unramified abelian extension of K.

Soleng [5] gave a construction of families of quadratic number fields from an elliptic curve having ideal class group isomorphic to the torsion group of the curve. A. Sato [4] constructed quadratic number fields with class number divisible by 5 from elliptic curves. Lemmermeyer [2] showed a method for constructing unramified quadratic extension of cubic fields using points on suitable elliptic curves. Drawing our inspiration from [2], we explicitly construct a quadratic unramified extension for each biquadratic field in an infinite family which originates from a non-torsion rational point on a suitably chosen elliptic curve.

The genus field of $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ has been discussed in detail by Ouyang Yi and Zhang Zhe [6], Sunghan Bae and Qin Yue [1] and Qin Yue [7] when at least one of a and b is a prime of the form 1 mod 4. Our results give quadratic unramified extension of infinitely many biquadratic fields $\mathbb{Q}(\sqrt{r}, \sqrt{m})$ where, if m is suitably chosen, both r and m will be composite or none of r and m will be a prime congruent to 1 mod 4. In Example 3.2, we apply our construction to infinitely many biquadratic fields $\mathbb{Q}(\sqrt{r_i}, \sqrt{3})$ where r_i's are square-free composite numbers.

Our main theorem is as follows.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11R29, 11R11.
Key words and phrases: elliptic curve, unramified extension.
Received 8 April 2016; revised 8 August 2016.
Published online 29 March 2017.

DOI: 10.4064/aa8493-10-2016

THEOREM 1.1. *Let $m \neq 0, 1$ be a square-free integer which is divisible by 3 if it is positive. Let $P_0 = (r_0/t_0^2, s_0/t_0^3)$ be any non-torsion point of the elliptic curve $y^2 = x^3 + m$ such that r_0 is odd and non-square. Let $(r_i/t_i^2, s_i/t_i^3) = 2^i P_0$ for each natural number i. Then the biquadratic field $K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{m})$ has an everywhere unramified quadratic extension $K_i(\sqrt{\beta_i})$, where β_i is either $\pm(s_i + t_i^3\sqrt{m})$ or $3(s_i + t_i^3\sqrt{m})$.*

We will identify the precise form of β_i later (see (2.8)). When r_0 is a square and t_0 is even, our construction gives an unramified extension of the quadratic field $\mathbb{Q}(\sqrt{m})$, but for the extension to be non-trivial we need to add an additional condition, for example, $0 < s < m$ (see Example 3.3). In order to prove Theorem 1.1, we carefully associate a non-torsion point P with a suitable element β in a biquadratic field K. We show that β generates the square of a fractional ideal. Then the extension $K(\sqrt{\beta})/K$ is unramified at all finite primes other than those lying above 2. If we can choose $\beta \equiv 1 \bmod 4$, then the primes above 2 are also unramified in $K(\sqrt{\beta})/K$. Finally, we consider the infinite primes and show that $K(\sqrt{\beta})/K$ is a quadratic extension which is unramified everywhere. These steps will be completed in §2. In §3, we show that the biquadratic fields K_i obtained from the multiples $2^i P_0$ of the initial non-torsion point P_0 are all distinct for distinct values $i = 1, 2, \ldots$.

2. Unramified quadratic extension from a non-torsion point. We fix the following notation for the rest of the article. For any square-free integer $m \neq 0, 1$, we consider the elliptic curve

$$E_m : \quad y^2 = x^3 + m. \tag{2.1}$$

We denote by P an arbitrary non-torsion rational point on E_m. Clearly, P can be written as $P = (r/t^2, s/t^3)$ where r, s and t are integers with $\gcd(r, t) = 1 = \gcd(s, t)$. We may take s and t to be positive, as we can replace P by its inverse $-P$ on E_m. On substitution, we find that

$$s^2 = r^3 + mt^6. \tag{2.2}$$

If s is not coprime to m then by (2.2) any common prime factor p will also divide r, and hence m will be divisible by p^2. Therefore $\gcd(s, m) = 1$. Similarly $\gcd(r, m) = 1$.

LEMMA 2.1. *Consider the duplication formula for $P = (r/t^2, s/t^3)$ on $y^2 = x^3 + m$:*

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(9r^3 - 8s^2)}{(2st)^2}, \frac{27r^6 - 36r^3s^2 + 8s^4}{(2st)^3}\right). \tag{2.3}$$

Suppose m is square-free and r is odd. If $3 \nmid s$, the fractions on the right hand side of (2.3) are already in their reduced form. When $s = 3s'$ the fractions

on the right hand side above reduce as follows:

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(r^3 - 8s'^2)}{(2s't)^2}, \frac{r^6 - 12r^3s'^2 + 24s'^4}{(2s't)^3}\right). \tag{2.4}$$

Proof. As m is square-free, it is clear from (2.2) that r and s are coprime, else the square of their common divisor will divide m. From the duplication formula (2.3) it is clear that the numerator $r(9r^3-8s^2)$ of $x(2P)$ is odd as r is odd. Now if p is a common prime divisor of t and the numerator $r(9r^3-8s^2)$ of $x(2P)$, then p divides $9r^3-8s^2$ as r and t are coprime. But $s^2 = r^3 + mt^6$ implies p also divides r^3-s^2, and hence p divides $9r^3-8s^2-8(r^3-s^2) = r^3$, which contradicts the fact that r and t are coprime. If p is a prime divisor of s and of the numerator of $x(2P)$, then p has to divide $9r^3 - 8s^2$ as r and s are coprime. Thus, p has to divide $9r^3$ and hence 9, as p cannot divide both r and s. So the only possibility for a common prime divisor of the numerator and the denominator of $x(2P)$ is $p = 3$, and in that case 3 divides s.

The y-coordinate $27r^6-36r^3s^2+8s^4$ of $2P$ in (2.3) is odd as r is odd. If p is a common prime divisor of t and $27r^6-36r^3s^2+8s^4$, then p also divides r^3-s^2 from (2.2). Hence p divides $27r^6 - 36r^3s^2 + 8s^4 - 27r^3(r^3-s^2) + 9s^2(r^3-s^2)$ $= -s^4$, which contradicts the fact that s and t are coprime. If p is a common prime divisor of s and $27r^6 - 36r^3s^2 + 8s^4$ then p must divide $27r^6$. But r and s are coprime, so $p = 3$ is the only possible common prime divisor of the numerator and the denominator of $y(2P)$, and in that case 3 divides s.

Therefore, when $3 \nmid s$ the fractions on the right hand side of (2.3) are in their reduced form. If $s = 3s'$, then we can cancel 3^2 for the $x(2P)$ and 3^3 for the $y(2P)$ and obtain the reduced form given in (2.4). ∎

From the duplication formula, it is also clear that if $r(P)$ is odd, then $t(2P)$ must be even, and hence $s(2P)$ must be odd. Hence from now on, we assume that $t = t(P)$ is even and $s = s(P)$ is odd without any loss of generality. We make the following assumption on the coordinates of the point $P = (r/t^2, s/t^3)$.

Assumption 2.2. (i) *r is odd,* (ii) *r is a non-square,* (iii) *t is even.*

It can be seen from the duplication formula that if $r = r(P)$ is odd, then so is $r(2P)$. If r is a non-square and $\gcd(r, s) = 1$, then $r(2P)$ is also a non-square. Thus Assumption 2.2 holds for $2P$ if it does for P.

If we allow r to be a square, then our construction gives an unramified quadratic extension of the quadratic field $\mathbb{Q}(\sqrt{m})$ under an additional condition ($0 < s < m$). We illustrate this point in Example 3.3 later.

With such a point P satisfying Assumption 2.2, we associate a biquadratic extension K and an element α as follows:

$$K = \mathbb{Q}(\sqrt{r}, \sqrt{m}), \quad \alpha = s + \sqrt{m}\, t^3 \in K. \tag{2.5}$$

As t is even, we note that

$$\alpha \equiv s \bmod 4. \tag{2.6}$$

The following lemma is crucial for the proof of the main theorem.

LEMMA 2.3. *Let $P = (r/t^2, s/t^3)$ be a non-torsion point of the elliptic curve E_m satisfying Assumption 2.2 with t even. Then α and its conjugate $\bar{\alpha}$ over $\mathbb{Q}(\sqrt{r})$ generate coprime ideals in the ring $\mathcal{O}_K$ of integers in K. Moreover, there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $\langle\alpha\rangle := \alpha\mathcal{O}_K = \mathfrak{a}^2$.*

Proof. Note that

$$N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) = \alpha\bar{\alpha} = (s + \sqrt{m}\,t^3)(s - \sqrt{m}\,t^3) = s^2 - mt^6 = r^3. \tag{2.7}$$

Now, suppose there exists some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\mathfrak{p}$ appears in the prime factorization of both the ideals $\langle\alpha\rangle$ and $\langle\bar{\alpha}\rangle$. Then $\alpha + \bar{\alpha} = 2s \in \mathfrak{p}$. But $r^3 = N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) \in \langle\alpha\rangle \subset \mathfrak{p}$, and r is odd under Assumption 2.2. Therefore, $2 \notin \mathfrak{p}$ and we must have $s \in \mathfrak{p}$. Similarly, $2\sqrt{m}\,t^3 = \alpha - \bar{\alpha} \in \mathfrak{p}$ implies either $t \in \mathfrak{p}$ or $m \in \mathfrak{p}$. Hence either both s and t belong to $\mathfrak{p}$, or both s and m belong to $\mathfrak{p}$. But this contradicts the fact that s is coprime to both m and t. Hence α and $\bar{\alpha}$ generate coprime ideals in $\mathcal{O}_K$.

Now $\alpha.\bar{\alpha} = N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) = (r\sqrt{r})^2$ implies $\langle\alpha\rangle = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$ in $\mathcal{O}_K$. ∎

For our subsequent argument, we need m to be divisible by 3 when $m > 0$ and $s \equiv 3 \bmod 4$. We can deduce a corollary of the above lemma in the case when the integer m is a positive multiple of 3. The corollary will be needed in §3 to show that at each stage of duplication of a non-torsion point we indeed get an unramified quadratic extension of a biquadratic field.

COROLLARY 2.4. *With the same notation as in the previous lemma, the element $3\alpha = 3(s + \sqrt{m}\,t^3)$ generates the square of an ideal in the ring of integers of $K = \mathbb{Q}(\sqrt{m}, \sqrt{r})$ if m is divisible by 3.*

Proof. If 3 divides the square-free integer m, then 3 generates the square of a prime ideal in $\mathbb{Q}(\sqrt{m})$, and hence it generates the square of an ideal in $\mathbb{Q}(\sqrt{m}, \sqrt{r})$. As α generates the square of some ideal by the previous lemma, the corollary follows. ∎

For the biquadratic extension $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ associated with the non-torsion point P, we want to construct a quadratic extension unramified at all finite as well as infinite primes of K. We consider the extension

$$K(\sqrt{\beta}), \quad \text{where} \quad \beta = \begin{cases} \alpha & \text{if } s \equiv 1 \bmod 4, \\ -\alpha & \text{if } s \equiv 3 \text{ modulo } 4 \text{ and } m < 0, \\ 3\alpha & \text{if } s \equiv 3 \text{ modulo } 4 \text{ and } m > 0. \end{cases} \tag{2.8}$$

Observe that $\beta \equiv 1 \bmod 4$ by (2.6). We first deal with the finite primes.

LEMMA 2.5. *The extension $K(\sqrt{\beta})$ over $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ is quadratic and unramified at all finite primes.*

Proof. First we prove that $K(\sqrt{\beta})$ is indeed a quadratic extension of K. Let us show this explicitly for $\beta = \alpha$. The cases $\beta = -\alpha$ or 3α are analogous. If possible, first assume that $\sqrt{\alpha} = a + b\sqrt{m}$ where $a, b \in \mathbb{Q}$. By comparing the coefficients of $\sqrt{m}$, we get $a^2 + mb^2 = s$ and $2ab = t^3$. Hence,

$$r^3 = s^2 - mt^6 = (a^2 + mb^2)^2 - 4a^2b^2m = (a^2 - mb^2)^2$$

implies that r is a square, which is a contradiction. Now consider $\sqrt{\alpha} = a + \sqrt{m}\, b$ where at least one of a and b is in $\mathbb{Q}(\sqrt{r}) - \mathbb{Q}$, say $a = u + v\sqrt{r}$ where $u,\ 0 \neq v \in \mathbb{Q}$. Comparing the coefficients of $\sqrt{m}$ in $\mathbb{Q}(\sqrt{r})$, we still obtain $2ab = t^3$, which means that b must be a rational multiple of the conjugate of a, i.e., $b = k\bar{a} = k(u - v\sqrt{r})$ for some $k \in \mathbb{Q}$. Then

$$a^2 + mb^2 = s \ \Rightarrow\ 2uv\sqrt{r}(1 - mk^2) = 0.$$

But $1 - mk^2 \neq 0$ as m is a square-free integer and k is a rational number. If $u = 0$ then $2ab = t^3$ will force $r = 1$. Therefore $\mathbb{Q}(\sqrt{r}, \sqrt{\alpha})$ is indeed a quadratic extension of K.

As $\beta \equiv 1 \bmod 4$, any prime over 2 in K is unramified in $K(\sqrt{\beta})/K$. By Lemma 2.3 and Corollary 2.4, we know that $\langle\beta\rangle = \mathfrak{a}^2$, hence no other finite primes can ramify in this extension. ∎

Now we consider whether the infinite primes can ramify in $K(\sqrt{\beta})/K$.

LEMMA 2.6. *The infinite primes do not ramify in $K(\sqrt{\beta})/K$.*

Proof. If $m < 0$ or $r < 0$ then the infinite prime already ramifies in the extension $K = \mathbb{Q}(\sqrt{m}, \sqrt{r})$ over $\mathbb{Q}$. If $m, r > 0$, then $\alpha = s + \sqrt{m}\, t^3 > 0$, as s and t are positive integers. Let $\alpha' = s - \sqrt{m}\, t^3$ be the conjugate of α. Then $\alpha\alpha' = N\alpha = r^3$ is positive as $r > 0$. Therefore $\alpha' > 0$ as well, i.e., α is totally positive, and hence so is β. Hence infinite primes do not ramify in $K(\sqrt{\beta})/K$. ∎

Thus, in this section we have explicitly constructed an everywhere unramified quadratic extension of a biquadratic field that we associate with a non-torsion rational point on the elliptic curve E_m where the coordinates of the point satisfy certain mild conditions. Note that we need m to be divisible by 3 only in the case when $s \equiv 3 \bmod 4$. As long as $s \equiv 1 \bmod 4$ for the point $P = (r/t^2, s/t^3)$ that satisfies Assumption 2.2, the field $\mathbb{Q}(\sqrt{m}, \sqrt{s + \sqrt{m}\, t^3})$ becomes an unramified quadratic extension of $\mathbb{Q}(\sqrt{m}, \sqrt{r})$.

We further study the unramified extension $L = \mathbb{Q}(\sqrt{\beta}, \sqrt{r}, \sqrt{m})$ over the base fields $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{rm})$, and obtain the following results.

PROPOSITION 2.7. *The extension $L = \mathbb{Q}(\sqrt{\beta}, \sqrt{r}, \sqrt{m})$ is Galois over $\mathbb{Q}$ with the dihedral group D_8 as the Galois group.*

Proof. It is enough to consider the case $\beta = \alpha$, as the arguments for the other two cases in (2.8) are identical. By Lemma 2.5, $[L : \mathbb{Q}(\sqrt{r}, \sqrt{m})] = 2$, and hence $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{r}, \sqrt{m})][\mathbb{Q}(\sqrt{r}, \sqrt{m}) : \mathbb{Q}] = 8$. The conjugates of $\sqrt{\alpha}$ over $\mathbb{Q}$ are $\pm\sqrt{\alpha}$ and $\pm\sqrt{\alpha'}$ where $\alpha' = s - \sqrt{m}\,t^3$. Now, $\sqrt{\alpha}\sqrt{\alpha'} = \sqrt{s^2 - mt^6} = r\sqrt{r}$. Therefore, $\sqrt{\alpha'} = r\sqrt{r}/\sqrt{\alpha} \in L$, and L is Galois over $\mathbb{Q}$.

Let $G = \mathrm{Gal}(L/\mathbb{Q})$. Now, $M = \mathbb{Q}(\sqrt{\alpha})$ is an extension of $\mathbb{Q}$ of degree 4. If M is Galois over $\mathbb{Q}$, then $\sqrt{\alpha'} \in M$ and hence $\sqrt{r} = \sqrt{\alpha}\sqrt{\alpha'}/r \in M$ and $\sqrt{m} \in M$. As $\mathbb{Q}(\sqrt{m}, \sqrt{r})$ is a subextension of M of degree 4, it must be M itself. But then $\sqrt{\alpha} \in \mathbb{Q}(\sqrt{r}, \sqrt{m})$, which contradicts Lemma 2.5. Therefore, L has a non-normal subextension, i.e., G is a group of order 8 with a non-normal subgroup. Therefore, G must be the dihedral group of order 8. ∎

Proposition 2.8. *The extension $L = \mathbb{Q}(\sqrt{\beta}, \sqrt{r}, \sqrt{m})$ is cyclic quartic over $\mathbb{Q}(\sqrt{rm})$.*

Proof. We use the following result which is a simple exercise in Galois theory.

Result 2.9 (see [3, §8.4]). Let $L/K/k$ be a tower of quadratic extensions of number fields and let σ denote the non-trivial automorphism of K/k. Let $L = K(\sqrt{\alpha})$. The extension L/k is normal if and only if $\alpha^{\sigma-1} = \alpha_\sigma^2$ for some $\alpha_\sigma \in K$. Moreover, L/k is a quartic cyclic extension if $\alpha_\sigma^{1+\sigma} = -1$, and a Klein-4-extension if $\alpha_\sigma^{1+\sigma} = 1$.

Now suppose $k = \mathbb{Q}(\sqrt{rm})$, $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ and $\alpha = s + \sqrt{m}\,t^3$. Let σ denote the non-trivial automorphism of K/k. Then $\alpha^{1+\sigma} = s^2 - mt^6 = r^3$, and hence

$$\alpha^{\sigma-1} = \frac{\alpha^{1+\sigma}}{\alpha^2} = \frac{r^3}{\alpha^2} = \left(\frac{r\sqrt{r}}{\alpha}\right)^2.$$

Thus L/k is normal, and we have $\alpha_\sigma = r\sqrt{r}/\alpha$; hence $\alpha_\sigma^{1+\sigma} = -r^3/r^3 = -1$, and therefore by Result 2.9, L/k is a quartic cyclic extension. ∎

3. The construction for an infinite family. In this section we show that we can start with a non-torsion point P_0 and repeat the procedure of the previous section for each multiple $P_i = 2^i P_0 = (r_i/t_i^2, s_i/t_i^3)$. It follows from the duplication formula (2.4) that if s_{i-1} is divisible by 3, then $s_i \equiv 1 \bmod 4$, and otherwise $s_i \equiv 3 \bmod 4$ from (2.3). Just as in (2.5), we associate with P_i a biquadratic extensions K_i and element α_i in K_i:

$$K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{m}), \qquad \alpha_i = s_i + \sqrt{m}\,t_i^3 \in K_i. \tag{3.1}$$

We obtain an everywhere unramified quadratic extension $K(\beta_i)$ (where $\beta_i = \pm\alpha_i$ or $3\alpha_i$ as in (2.8)). We now show that the biquadratic fields K_i are all distinct as i varies over the natural numbers.

LEMMA 3.1. *Suppose that the initial non-torsion point P_0 on E_m is such that*

(a) *r_0 is square-free and t_0 is even,*
(b) *if $r_0 \equiv 1 \bmod 4$, then r_0 has a prime factor $p \not\equiv 1, 3 \bmod 8$.*

Then the extensions $\mathbb{Q}(\sqrt{r_i})$ are distinct for distinct values of i.

Proof. First assume that $3 \nmid s_{i-1}$. From the duplication formula (2.3), we have $r_i = r_{i-1}(9r_{i-1}^3 - 8s_{i-1}^2)$. Hence r_i is odd for all i if r_0 is odd. As $\gcd(r_{i-1}, s_{i-1}) = 1$, we have $\gcd(r_{i-1}, 9r_{i-1}^3 - 8s_{i-1}^2) = 1$, and hence r_i is not a square if r_{i-1} is not a square. Moreover, if $r_0 \equiv 3 \bmod 4$, then $9r_0^3 - 8s_0^2 \equiv 3 \bmod 4$, and hence is not a square. Now suppose $r_0 \not\equiv 3 \bmod 4$. If $9r_0^3 - 8s_0^2$ is a square then -2 is a quadratic residue for any p dividing r_0, and hence r_0 only has prime factors congruent to 1 or 3 modulo 8, contradicting our assumption (b). As r_i is a multiple of r_0, this argument ensures that $9r_i^3 - 8s_i^2$ is never a square. r_i is obtained from r_{i-1} by multiplying with a coprime integer. So new prime factors of odd exponent get introduced at each step when we pass from r_i to r_{i+1}, and the result follows.

When $3 \mid s_{i-1}$, the same argument works by replacing $9r^3 - 8s^2$ with $r^3 - 8s'^2$ where $s' = s/3$ as in (2.4). ∎

EXAMPLE 3.2. Suppose we choose our curve to be $y^2 = x^3 + 3$. Now assuming $P_0 = (1, 2)$ we find that $2P_0$ is $(-23/16, 11/64)$. From the duplication formula (2.3) we find that $2^2P_0 = (2540833/88^2, 4050085583/88^3)$, and hence using our results we conclude that $\mathbb{Q}(\sqrt{2540833}, \sqrt{3}, \sqrt{\beta})$ is an unramified quadratic extension of $\mathbb{Q}(\sqrt{2540833}, \sqrt{3})$, where $\beta = 4050085583 + 88^3\sqrt{3}$.

From the duplication formula (2.3) we see that $23 \not\equiv 1, 3 \pmod 8$ is always a divisor of the numerator of the x-coordinate of 2^iP_0 for $i > 0$. We can conclude that the infinite family of biquadratic fields $K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{3})$ obtained from the rational points 2^iP_0 of the elliptic curve $y^2 = x^3 + 3$ has an unramified abelian quadratic extension given by $K_i(\sqrt{\beta_i})$ for each $i > 0$.

Next we consider examples of $(r/t^2, s/t^3)$ on $y^2 = x^3 + m$ where r is a square but $0 < s < m$. Then by our construction, $L = \mathbb{Q}(\sqrt{m}, \sqrt{s + t^3\sqrt{m}})$ is unramified over $K = \mathbb{Q}(\sqrt{m})$, and if $0 < s < m$ then $s + t^3\sqrt{m}$ cannot be a square in K so that L is a quadratic unramified extension of K.

EXAMPLE 3.3. Considering the point $(3^2/4, 133/8)$ on $y^2 = x^3 + 265$, we find that $133 < 265$, and hence $\mathbb{Q}(\sqrt{265}, \sqrt{133 + 8\sqrt{265}})$ is a quadratic unramified extension of $\mathbb{Q}(\sqrt{265})$.

The following corollary states that whenever r is a square as in the previous example, then β will also be a square in the genus field of the quadratic extension.

PROPOSITION 3.4. *Consider the elliptic curve $y^2 = x^3 + m$ where $m \equiv 1 \bmod 4$. If $(r/t^2, s/t^3)$ is a point on the curve such that r is a square then either β or $-\beta$ will always be a square in the genus field of $\mathbb{Q}(\sqrt{m})$.*

Proof. We first give the argument for $\beta = \pm\alpha$ in (2.8). Suppose that $(r^2/t^2, s/t^3)$ is on the curve $y^2 = x^3 + m$. By substituting in $y^2 = x^3 + m$, we find that $s^2 = r^6 + mt^6$, which implies $(s + r^3)(s - r^3) = mt^6$. Suppose d is a natural number dividing both $s + r^3$ and $s - r^3$. Then d divides $2s$ and $2r^3$. But s and r are coprime, hence d must divide 2, which implies $d = 2$. Hence the only common factor of $s + r^3$ and $s - r^3$ is 2. So we can write $t = 2pq$ where p divides $s + r^3$ and q divides $s - r^3$, and $m = ab$ where a divides $s + r^3$ and b divides $s - r^3$. We can now write $s + r^3 = 2^i p^6 a$ and $s - r^3 = 2^j q^6 b$ where $i + j = 6$. Hence, $2s = 2^i p^6 a + 2^j q^6 b$, so $s = 2^{i-1} p^6 a + 2^{j-1} q^6 b$. But s is coprime to t and t is even. Hence s is odd, and so either $i - 1 = 0$ or $j - 1 = 0$. Without loss of generality we assume that $i - 1 = 0$, and hence $i = 1$, $j = 5$ and $s = p^6 a + 16q^6 b$. Now the genus field of $K = \mathbb{Q}(\sqrt{m})$ is $F = K(\sqrt{p_i})$ where the p_i are the prime factors of m and $\pm p_i \equiv 1 \bmod 4$. Hence $m = ab \equiv 1 \bmod 4$ implies either $\sqrt{a}, \sqrt{b} \in F$ or $\sqrt{-a}, \sqrt{-b} \in F$. Therefore either

$$\beta = s + \sqrt{m}\, t^3 = p^6 a + 16q^6 b + 8\sqrt{ab}\, p^3 q^3 = (p^3\sqrt{a} + 4q^3\sqrt{b})^2,$$

or

$$-\beta = -(s + \sqrt{m}\, t^3) = -p^6 a - 16q^6 b - 8\sqrt{ab}\, p^3 q^3 = (p^3\sqrt{-a} - 4q^3\sqrt{-b})^2.$$

Hence either β or $-\beta$ will always be a square in the genus field of $\mathbb{Q}(\sqrt{m})$. In the case $\beta = 3\alpha$ in (2.8), we have m divisible by 3, and -3 is a square in the genus field of $\mathbb{Q}(\sqrt{m})$. ∎

We further observe that $\alpha = s + \sqrt{m}\, t^3$ will always be a product of a unit and a cube in $\mathbb{Q}(\sqrt{m})$ whenever the class number of $\mathbb{Q}(\sqrt{m})$ is coprime to 3. As $\alpha\alpha' = r^3$ and α, α' are coprime, hence α has to be the cube of some ideal I in $\mathbb{Q}(\sqrt{m})$. The ideal I will be either principal or of order 3 in the class group. When the class number of $\mathbb{Q}(\sqrt{m})$ is not divisible by 3, I has to be principal.

Acknowledgements. The authors are grateful to the anonymous referee for several valuable suggestions. In particular, Propositions 2.7, 2.8, 3.4 and the observation above have been included based on the suggestion of the referee.

References

[1] S. Bae and Q. Yue, *Hilbert genus fields of real biquadratic fields*, Ramanujan J. 24 (2011), 161–181.

[2] F. Lemmermeyer, *Why is the class number of* $\mathbb{Q}(\sqrt[3]{11})$ *even?* Math. Bohem. 138 (2013), 149–163.
[3] F. Lorenz und F. Lemmermeyer, *Algebra. 1. Körper und Galoistheorie*, Elsevier and Spektrum Akad. Verlag, 2007.
[4] A. Sato, *On the class numbers of certain number fields obtained from points on elliptic curves III*, Osaka J. Math. 48 (2011), 809–826.
[5] R. Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Number Theory 46 (1994), 214–229.
[6] O. Yi and Z. Zhe, *Hilbert genus fields of biquadratic fields*, Sci. China Math. 57 (2014), 2111–2122.
[7] Q. Yue, *Genus fields of real biquadratic fields*, Ramanujan J. 21 (2010), 17–25.

Debopam Chakraborty, Anupam Saikia
Department of Mathematics
Indian Institute of Technology Guwahati
Guwahati-781039, Assam, India
E-mail: c.debopam@iitg.ernet.in
a.saikia@iitg.ernet.in