138 (2013) MATHEMATICA BOHEMICA No. 2, 149–163

WHY IS THE CLASS NUMBER OF $\mathbb{Q}(\sqrt[3]{11})$ EVEN?

F. Lemmermeyer, Jagstzell

(Received September 15, 2011)

Abstract. In this article we will describe a surprising observation that occurred in the construction of quadratic unramified extensions of a family of pure cubic number fields. Attempting to find an explanation will lead us on a magical mystery tour through the land of pure cubic number fields, Hilbert class fields, and elliptic curves.

Keywords: class number, pure cubic field, elliptic curve

MSC 2010: 11R16, 11G05

Euler was one of the (if not the) most prolific writers in mathematics. Yet few if any of the articles appearing today are modeled after Euler's way of writing; Euler often explained how he attacked a problem even if the attack ultimately proved unsuccessful: before showing that an equation such as $x^3+y^3=z^3$ is not solvable in integers he would try out one method of solving diophantine equations after another. Gauss's motto "pauca sed matura" places him at the other end of the spectrum: Gauss did not care very much about conveying the motivation behind his proofs or about sketching the paths that led him there, and Landau later wrote a whole series of textbooks that consisted of little more than definitions, theorems and proofs.

Today, articles written in Euler's style have almost disappeared from the literature for obvious economic (and other) reasons. Here I would like to revive the Eulerian tradition and describe in some detail the development from a curious observation on class numbers to the results in Section 8. What happened was that I numerically tested a result I wanted to use as an exercise for [10]; it turned out that the family of pure cubic number fields $\mathbb{Q}(\sqrt[3]{m}\,)$ for cubefree values of $m=8b^3+3$ with $1\leqslant b<89$ had even class numbers, but that the class number was odd for $b=89$.

1. An exercise in class field theory

Consider pure cubic number fields $K = \mathbb{Q}(\sqrt[3]{m})$ with $m = a^3 + 3$, and assume that m is cubefree. The element $a - \omega$, where $\omega = \sqrt[3]{m}$, has norm $N(a-\omega) = a^3 - m = -3$. Since $m \equiv 2, 3, 4 \bmod 9$, the prime 3 is ramified completely in $K/\mathbb{Q}$. Thus $(a-\omega)^3 = (3)$, and the element $\varepsilon = -\frac{1}{3}(a-\omega)^3 = 1 + a^2\omega - a\omega^2$ must be a unit in the ring of integers $\mathcal{O}_K$.

If $a \equiv 0 \bmod 4$, this unit is positive and congruent to 1 mod 4, hence $K(\sqrt{\varepsilon})/K$ is an unramified quadratic extension of K.

Proposition 1.1. *Let $a > 0$ be an integer and assume that $m = a^3+3$ is cubefree. If $4 \mid a$, then the class number of $K = \mathbb{Q}(\sqrt[3]{m})$ is even.*

It only remains to show that the unit ε is not a square:

Lemma 1.2. *Let $a > 0$ be an integer and assume that $m = a^3 + 3$ is cubefree. Then $\varepsilon = 1 + a^2\omega - a\omega^2$ is not a square in $K = \mathbb{Q}(\sqrt[3]{m})$.*

Proof. From $\varepsilon = \frac{1}{3}(\omega - a)^3$ we see that if ε is a square in $\mathcal{O}_K$, then $3\omega - 3a = \beta^2$ is a square in K. With $\beta = r + s\omega + t\omega^2$ we find the equations

$$r^2 + 2stm = -3a, \quad 2rs + mt^2 = 3 \quad \text{and} \quad s^2 + 2rt = 0.$$

Since $m > 3$, these equations imply $st < 0$, $rs < 0$ and $rt < 0$: but this is clearly impossible. □

If $a \equiv 2 \bmod 4$, let us write $a = 2b$ and $m = 8b^3 + 3$; the unit $\varepsilon = 1 + 4b^2\omega - 2b\omega^2$ is not congruent to a square modulo 4, but computing the class numbers of a few fields $K_b = \mathbb{Q}(\sqrt[3]{m})$ produces the following results:

b	1	3	5	7	9	11	13
m	11	$3 \cdot 73$	$17 \cdot 59$	$41 \cdot 67$	$3 \cdot 5 \cdot 389$	10651	17579
$h(K_b)$	2	18	54	168	240	564	920

Although these class numbers are all even, searching for a family of explicit generators of unramified quadratic extensions of these cubic fields was unsuccessful.

Continuing this table shows that $h(K_b)$ is odd for $b = 19$; but here $m = 54875 = 5^3 \cdot 439$ is not cubefree. The calculations have to be extended considerably before something surprising happens:

b	85	86	87	88	89
m	$619 \cdot 7937$	$23^2 \cdot 9619$	$3 \cdot 1756009$	5451779	$5 \cdot 11 \cdot 41^2 \cdot 61$
$h(K_b)$	153954	6000	151200	186860	3375

Thus the class number of K_b for $b = 89$ is odd, although it is even for all 87 values less than 89 for which $m = 8b^3 + 3$ is squarefree. This clearly cannot be an accident; but how can we explain this phenomenon?

2. Elliptic curves

Let $m = 8b^3 + 3$ for integers $b \geqslant 1$, assume that m is cubefree, and let $K_b = \mathbb{Q}(\omega)$ denote the pure cubic number field defined by $\omega = \sqrt[3]{m}$.

We now consider the family of elliptic curves $E_b\colon\ y^2 = x^3 - m$. A rational point on a curve E_b has the form[1] $x = r/t^2$ and $y = s/t^3$, and clearing denominators shows that such rational points correspond to solutions of the equation $s^2 = r^3 - mt^6$. In other words: the norm of the element $r - t^2\omega \in K_b$ is a square. If this element is coprime to its conjugates, then there must be an ideal $\mathfrak{a}$ with $(r - t^2\omega) = \mathfrak{a}^2$, and if $\mathfrak{a}$ is not principal, then the class number of K_a will be even.

Computing a couple of rational points on these curves E_b produces the following table of selected points (here we have included even values of b):

b	1	2	3	4	5
P	$(3, 4)$	$(17/4, 25/8)$	$(55/9, 82/27)$	$(129/16, 193/64)$	$(251/25, 376/125)$

These points all have the form $(f(b)/b^2, g(b)/b^3)$ for some (yet) unknown functions f and g. Computing the differences we find

$$\begin{array}{ccccccccccc}
3 & & 17 & & 55 & & 129 & & 251 & & 433 \\
& 14 & & 38 & & 74 & & 122 & & 182 & \\
& & 24 & & 36 & & 48 & & 60 & & \\
& & & 12 & & 12 & & 12 & & &
\end{array}$$

The fact that the third differences seem to be constant and equal to $12 = 2 \cdot 3!$ suggests that $f(b) = 2b^3 +$ terms of lower order, and then it is easy to guess that

$$P_b\Big(\frac{2b^3 + 1}{b^2}, \frac{3b^3 + 1}{b^3}\Big) \tag{2.1}$$

is a family of rational points on the elliptic curves E_b. Since torsion points must be integral, we find:

Let $a > 0$ be an integer and assume that $m = a^3 + 3$ is cubefree. The elliptic curves $E_b\colon\ y^2 = x^3 - m$ have rank at least 1, and the rational points in (2.1) *have infinite order.*

[1] For standard results on the arithmetic of elliptic curves we refer to [15] for a first introduction.

Thus all curves E_b have rank at least 1. Does this explain the fact that the class numbers of K_b tend to be even? Before we return to this question, let us describe an approach that could have predicted the family of rational points P_b.

3. Quadratic fields

The points $P_b = (x, y)$ from (2.1) satisfy $y^2 = x^3 - m$; clearing denominators then gives

$$(3b^3 + 1)^2 + b^6 m = (2b^3 + 1)^3. \tag{3.1}$$

Since the elements $\tau = 3b^3 + 1 + b^3\sqrt{-m}$ and $\tau' = 3b^3 + 1 - b^3\sqrt{-m}$ generate coprime ideals in $k_b = \mathbb{Q}(\sqrt{-m})$, there must be an integral ideal $\mathfrak{a}$ in k_b with $(\tau) = \mathfrak{a}^3$. This suggests that the class numbers of the quadratic number fields k_b should have a tendency to be divisible by 3. Numerical experiments, however, reveal that this is not correct. In fact, the element τ with norm $(2b^3 + 1)^3$ is a cube since

$$3b^2 + 1 + b^3\sqrt{-m} = \Big(\frac{1 + \sqrt{-m}}{2}\Big)^3. \tag{3.2}$$

Thus we have seen:

The element $\tau = 3b^3 + 1 + b^3\sqrt{-m}$ in $\mathbb{Q}(\sqrt{-m}\,)$ is a cube. In particular, the ideal $\mathfrak{a}$ with $(\tau) = \mathfrak{a}^3$ is principal.

This also means that the rational points P_b on the family of elliptic curves E_b could have been constructed in a rather trivial way: for $m = 8b^3 + 3$, taking the cube of the element[2] $\frac{1}{2}(1 + \sqrt{-m})$ immediately gives (3.2) and thus the points P_b.

The ideal classes $[\mathfrak{a}]$ of order dividing 3 in the quadratic number fields k_b are all trivial. This begs the question whether the ideal classes of order dividing 2 in the number fields K_b deduced from (3.1) are also trivial. This is what we will look into next.

[2] To be honest, this only worked because the coefficient of $\sqrt{-m}$ is a cube; taking the third power of $\frac{1}{2}(3 + \sqrt{-m}\,)$, for example, does not work since its cube is $-9b^3 + (3 - b^3)\sqrt{-m}$.

4. Pure cubic fields

Let us now write the equation (3.1) in the form

$$(3b^3+1)^2 = (2b^3+1)^3 - b^6 m = N(2b^3+1-b^2\omega).$$

The element $\alpha = 2b^3+1-b^2\omega$ has square norm; if it is the square of a principal ideal, it will not explain our observations on class numbers. Playing around with elements of small norm leads us to the observation[3] that

$$(4b^3+1)^3 - b^3 \cdot m^2 = 3b^3+1,$$

which shows that

$$N(\beta) = 3b^3+1 \quad \text{for } \beta = 4b^3+1-b\omega^2.$$

Thus there exist elements of norm $3b^3+1$; but is $\beta^2 = \alpha$? The answer is no because

$$\beta^2 = 16b^6 + 8b^3 + 1 + b^2(8b^3+3)\omega - (8b^4+2b)\omega^2.$$

A simple calculation, however, shows that

$$\varepsilon\alpha = \beta^2,$$

where $\varepsilon = 1 + 4b^2\omega - 2b\omega$ is the unit in K_b we have started with. Thus (α) is the square of the principal ideal (β), and so the ideal classes coming from the rational points P_b are all trivial. It seems that we are back to square one.

5. Back to elliptic curves

The family of points P_b on the elliptic curves E_b shows that these curves all have rank $\geqslant 1$. In fact, the curves E_b for small values of b all have rank $\geqslant 2$: in fact, the Mordell-Weil rank is 2 for $1 \leqslant b \leqslant 90$ except for

- ▷ the values $b = 9, 17, 18, 20, 25, 53, 54, 67, 82, 87$ for which the rank is 4;
- ▷ the value $b = 13$ for which the computation of the rank is complicated by the likely presence of a nontrivial Tate-Shafarevich group; here the rank is bounded by $2 \leqslant r \leqslant 4$, and the 2-Selmer rank is even;
- ▷ the values $b = 77$ and $a = 80$, for which the Selmer rank is 2, but the second generator has large height;

[3] Observe that $(4b^2+1)^3 = 64b^6 + 48b^4 + 12b^2 + 1$ and $m^2 = 64b^6 + 48b^3 + 9$; in order to make the second terms vanish we only have to adjust the coefficients slightly.

▷ the values $b = 44$ and $a = 89$, for which the rank is 1;

▷ the values $b = 56, 68, 69, 86$, for which the rank is 3.

These results show that trying to construct two independent families of points on E_b is bound to fail since there are examples of curves with rank 1. We therefore should show that the ranks of the curves E_b have a tendency to be even. This can be accomplished with the help of the parity conjecture.

Parity conjectures. For formulating the various statements connected with the name partiy conjectures, let r denote the Mordell-Weil rank of an elliptic curve, and R the analytic rank, that is, the order of vanishing of the L-series of E at $s = 1$. The conjecture of Birch and Swinnerton-Dyer predicts that $r = R$.

The functional equation of the L-series of E connects the values at s and $2 - s$; the completed L-series L^* satisfies the functional equation

$$L_E^*(2 - s) = w(E)L^*(s),$$

where $w(E) \in \{\pm 1\}$ is called Artin's root number. If $w(E) = -1$, then setting $s = 1$ in the functional equation implies $L(1) = 0$, and the Birch and Swinnerton-Dyer Conjecture predicts that E has rank $\geqslant 1$. More generally, the parity conjecture states that $(-1)^r = w(E)$. Performing a p-descent on an elliptic curve provides us with the p-Selmer rank r_p of E, and this rank differs from the rank r of E by an even number if the Tate-Shafarevich group of E is finite.

Theorem 5.1. *If $Ш(E)$ is finite, then the parity conjecture $(-1)^r = w(E)$ holds.*

The root number for elliptic curves with j-invariant 0 was computed by Birch and Stephens; for our curves E_b we find that (see Liverance [11])

$$w(E) = \prod_{p^2 | m} \Big(\frac{-3}{p}\Big).$$

Thus we expect that the rank r_b of E_b is even whenever m is squarefree, and that it is odd if r_b is divisible by the square of a unique prime $p \equiv 2 \bmod 3$. The values $b < 200$ for which this happens are

$$b = 44,\ 56,\ 68,\ 69,\ 86,\ 89,\ 94,\ 119,\ 169,\ 177,\ 194,$$

which agrees perfectly with our computations above. Observe that the class number for $b = 419$ is even, and that $m = 5^2 \cdot 11^2 \cdot 227 \cdot 857$ is divisible by the square of two primes $p \equiv 2 \bmod 3$.

The only examples of pure cubic fields K_b with odd class numbers for $b < 1630$ and cubefree m are

$$b = 89,\ 119,\ 169,\ 177,\ 209,\ 369,\ 369,\ 503,\ 615,\ 661,\ 719,\ 787,$$
$$903,\ 1069,\ 1145,\ 1219,\ 1319,\ 1365,\ 1387,\ 1419,\ 1629.$$

For all these b, the number $m = 8b^3+3$ is divisible by exactly one prime $p \equiv 2 \bmod 3$. The many values of b ending in 19 are explained by the observation that m is divisible by 5^2 if $m \equiv 19, 69 \bmod 100$.

Nothing so far prevents a pure cubic field K_b from having an odd class number if the rank of E_b is even: the rational points on E_b give rise to ideals $\mathfrak{a}$ in K_b whose squares are principal, but there is no guarantee that $\mathfrak{a}$ is not principal. Yet all available numerical evidence points towards the following

Conjecture 1. *Let $b \geqslant 1$ be an integer and assume that $m = 8b^3 + 3$ is cubefree. If the class number of $K_b = \mathbb{Q}(\sqrt[3]{m})$ is odd, then the rank of the elliptic curve $E_b\colon\ y^2 = x^3 - m$ is 1.*

This conjecture implies, by the parity conjecture, the following, which does not even mention elliptic curves:

Conjecture 2. *Let $b \geqslant 1$ be an integer and assume that $m = 8b^3 + 3$ is cubefree. If the class number of $K_b = \mathbb{Q}(\sqrt[3]{m}\,)$ is odd, then m is divisible by an odd number of squares of primes $p \equiv 2 \bmod 3$.*

A weaker formulation of the conjecture would be that the class number of K_b is even whenever m is squarefree. Even this weaker conjecture is unlike anything I would have expected. After all, the primes with exponent 1 and 2 in the prime factorization of m change their roles when m is replaced by m^2 (observe that $\mathbb{Q}(\sqrt[3]{m}\,) = \mathbb{Q}(\sqrt[3]{m^2}\,)$).

6. Nobody expects the Spanish inquisition

In the conjectures above, the condition that m be squarefree seemed quite surprising at first. This condition also occurs in the computation of an integral basis of pure cubic fields: it is well known that the ring of integers in $\mathbb{Q}(\sqrt[3]{m}\,)$ is given by $\mathbb{Z}[\sqrt[3]{m}]$ (such cubic fields are called monogenic) if and only if $m \not\equiv \pm 1 \bmod 9$ is squarefree. If, on the other hand, m is divisible by the square of a prime p, then $p^{-1}\sqrt[3]{m^2}$ is integral, and the field is not monogenic.

But what should the form of an integral basis have to do with the parity of the class number? Ten years ago, just about any number theorist you would have asked probably would have answered "nothing!" and would have quoted the heuristics of Cohen, Lenstra and Martinet as supporting evidence. In fact, Cohen and Lenstra [3] gave an explanation of the numerical evidence for the distribution of class numbers of quadratic number fields based on certain heuristics; the main idea was that it's not the actual size of a class group that matters but rather the size of its automorphism group. It is clear that the prime 2 behaves differently in quadratic extensions k since the 2-class group $\mathrm{Cl}_2(k)$ is far from being random: Gauss's genus theory predicts its rank, and even the invariants divisible by 4.

Cohen and Martinet [4] then extended this project to class groups of extensions of higher degree. As in the case of quadratic extensions there were "bad primes" p for which the behaviour of the p-class group $\mathrm{Cl}_p(k)$ was not believed to be random; in [4], the prime 2 was considered to be good for nonnormal cubic extensions k although it divides the degree of the normal closure of $k/\mathbb{Q}$. In particular, the probability that the class number of k is even was predicted to be about $p = 0.25932$. In [5, Sect. 4], however, the authors cast some doubt on their earlier conjectures and asked whether the prime 2 actually was bad in this case.

Finally Bhargava and Shankar [1, Thm. 1.9, 1.10] proved the following result: the average size of the 2-class groups of complex cubic number fields ordered by discriminant (or height) is smaller than the corresponding average for monogenic cubic fields. Their result agrees with the Cohen-Martinet prediction based on the assumption that the prime 2 is good for nonnormal cubic fields.

An observation suggesting a relation between monogenic rings and the distribution of class groups can actually already be found in the article [7], where the authors computed the 2-rank of pure cubic number fields $\mathbb{Q}(\sqrt[3]{m})$ by studying the elliptic curves $E\colon\ y^2 = x^3 \mp m$ and remarked ([7, p. 567]):

> The primes[4] $p \equiv \pm 1 \bmod 9$ have relatively small 2-class numbers.
> It seems that the reason for this is the fact that $A_k\colon\ y^2 = x^3 + k$ has a point of order 2 in $\mathbb{Q}_3$ iff $k^2 \equiv 1 \bmod 9\ldots$

Let me add the remark that the fact that the 2-class groups of the fields K_b do not seem to be random does, of course, not imply that the prime 2 is bad in the sense of Cohen-Martinet because the family of fields K_b has density 0.

[4] More precisely: the fields $\mathbb{Q}(\sqrt[3]{p})$.

7. Why the class number of $\mathbb{Q}(\sqrt[3]{11})$ is even

Since we have started our tour with the question why the class number of $\mathbb{Q}(\sqrt[3]{11})$ is even it is about time we provide an answer.

Consider the elliptic curve $E\colon\ y^2 = x^3 - m$ for some cubefree integer $m \equiv 3 \bmod 4$, and let $K = \mathbb{Q}(\omega)$ denote the pure cubic number field defined by $\omega = \sqrt[3]{m}$. If $P = (r/t^2, s/t^3)$ is a rational point with $t \equiv 0 \bmod 2$, then $s^2 = r^3 - mt^6$ shows that $\alpha = r - t^2\omega \in K$ is congruent to 1 mod 4; moreover, (α) is, as we will see below, an ideal square. Thus the field $K(\sqrt{\alpha})$ is a quadratic unramified extension of K, and by class field theory, K has even class number.

Computing the generators of the Mordell-Weil group $E(\mathbb{Q})$ of the elliptic curve $E\colon\ y^2 = x^3 - 11$ we find the two points $P = (3, 4)$ and $Q = (15, 58)$. The sum $P + Q = (9/4, -5/8)$ has the desired form, hence $\alpha = 9 - 4\omega$ works. The minimal polynomial of $\sqrt{\alpha}$ is $f(x) = x^6 - 27x^4 + 243x^2 - 25$, and the discriminant of the number field generated by a root of f is $3^6 11^4$; a "smaller" polynomial generating the same number field is $g(x) = x^6 - 3x^5 + 9x^4 - 1$. Thus $K = \mathbb{Q}(\sqrt[3]{11})$ has the unramified quadratic extension $K(\sqrt{9 - 4\omega})$.

point		α	$\mathfrak{a}_P$	$[\mathfrak{a}_P]$
$(3, 4)$	P	$3 - \omega$	$\mathfrak{2}_1^2$	1
$(15, 58)$	Q	$15 - \omega$	$\mathfrak{2}_1 \cdot \mathfrak{29}$	$[\mathfrak{2}]$
$(\frac{9}{4}, -\frac{5}{8})$	$P + Q$	$9 - 4\omega$	$\mathfrak{5}$	$[\mathfrak{2}]$
$(\frac{345}{64}, -\frac{6179}{512})$	$2P$	$345 - 64\omega$	$\mathfrak{37}_3 \cdot \mathfrak{167}$	1
$(\frac{51945}{13456}, \frac{10647157}{1560896})$	$2Q$	$51945 - 13456\omega$	$\mathfrak{37}_1 \cdot \mathfrak{83} \cdot \mathfrak{3467}$	1
$(\frac{861139}{23409}, \frac{799027820}{3581577})$	$3P$	$861139 - 23409\omega$	$\mathfrak{2}_1^2 \cdot \mathfrak{5} \cdot \mathfrak{23} \cdot \mathfrak{1737017}$	1

The prime 2 splits into two prime ideals in K, namely $\mathfrak{2}_1$ with norm 2 and $\mathfrak{2}_2$ with norm 4. The squares of these ideals are principal: we have $\mathfrak{2}_1^2 = (5 + 2\omega + \omega^2)$ and $\mathfrak{2}_2 = (3 + \omega - \omega^2)$.

The prime number 37 splits into three prime ideals in K; the prime ideals in the decomposition $(37) = \mathfrak{37}_1\mathfrak{37}_2\mathfrak{37}_3$ are determined by the congruences $\omega \equiv -9 \bmod \mathfrak{37}_1$, $\omega \equiv -12 \bmod \mathfrak{37}_2$, and $\omega \equiv -16 \bmod \mathfrak{37}_3$. The first two ideals are nonprincipal, whereas $\mathfrak{37}_3$ is generated by $5 - 2\omega$. This is compatible with our construction of the Hilbert class field of K: a computation of the quadratic residue symbols shows that

$$\Big[\frac{9 - 4\omega}{\mathfrak{37}_1}\Big]_2 = \Big(\frac{45}{37}\Big) = -1, \quad \Big[\frac{9 - 4\omega}{\mathfrak{37}_2}\Big]_2 = \Big(\frac{57}{37}\Big) = -1, \quad \Big[\frac{9 - 4\omega}{\mathfrak{37}_3}\Big]_2 = \Big(\frac{73}{37}\Big) = +1.$$

Thus only $\mathfrak{37}_3$ splits in the Hilbert class field.

Without going into details we remark that $\mathfrak{a}_{3Q}$ belongs to the ideal class [2]. This is compatible with the conjecture that the map $P \to [\mathfrak{a}_P]$ is a homomorphism from $E(\mathbb{Q})$ to $\mathrm{Cl}(K)[2]$.

Similarly, for $b = 3$ and $m = 219$, the curve $E_3(\mathbb{Q})$ is generated by $P = (55/9, 82/27)$ and $Q = (283/9, 4744/27)$, and the sum $P + Q$ provides us with the quadratic unramified extension $K(\sqrt{\alpha})$ for $\alpha = 115657 - 12996\omega$. The minimal polynomial of $\sqrt{\alpha}$ is $f(x) = x^6 - 346971x^4 + 40129624947x^2 - 1066391672856409$, a "smaller" polynomial whose root generates the same number field is $g(x) = x^6 - 3x^5 + 21x^4 - 37x^3 + 126x^2 - 108x - 3$.

8. Hilbert class fields via elliptic curves

We will now show that this construction works whenever E has rank $\geqslant 2$:

Theorem 8.1. *Let b be an odd integer such that $m = 8b^3 + 3$ is squarefree. Then the class number of $\mathbb{Q}(\sqrt[3]{m})$ is even whenever $E\colon y^2 = x^3 - m$ has rank $\geqslant 2$. If the parity conjecture holds, then the class number is even for all squarefree values of m.*

This theorem will be proved by showing that if there is a point $P = (r/t^2, s/t^3)$ on $E(\mathbb{Q}) \setminus 2E(\mathbb{Q})$ with $2 \mid t$, then the extension $H = K(\sqrt{\alpha})$ of K is a quadratic unramified extension.

For showing that H/K is unramified we have to verify the following claims:

- $\alpha > 0$, which implies that the extension H/K is unramified at the infinite primes;
- $\alpha \equiv 1 \bmod 4$, which implies that H/K is unramified above 2;
- $(\alpha) = \mathfrak{a}^2$ is an ideal square, which implies that H/K is unramified at all finite primes not dividing 2.

The first claim is trivial since $N\alpha = s^2 > 0$, and the second claim follows from the assumption $2 \mid t$. It remains to show that (α) is an ideal square:

Lemma 8.2. *Let $P = (r/t^2, s/t^3)$ be a rational point on $E_b\colon y^2 = x^3 - m$ for a squarefree value of $m = 8b^3 + 3$. Assume as above that $\gcd(r, t) = \gcd(s, t) = 1$. Then the ideal (α) for $\alpha = r - t^2\omega$ is the square of an ideal $\mathfrak{a}$ in K_b.*

Proof. The ideal (α) is a square if $N\alpha$ is a square and $(\alpha, \alpha') = (1)$ in $K_b' = \mathbb{Q}(\sqrt{-3}, \omega)$. In our case, $N\alpha = s^2$, and any ideal divisor of α and α' divides the difference $\alpha - \alpha' = (1 - \varrho)t^2\omega$. Since $\gcd(s, t) = 1$, this ideal must divide $(1 - \varrho)\omega$. Any prime ideal dividing ω and s also divides r, so its norm divides both r and s, hence the square of its norm divides mt^6. Since $\gcd(r, t) = 1$, it must divide m, and this contradicts the assumption that m be squarefree.

Thus the only possibilities for $\mathfrak{d} = (\alpha, \alpha')$ are $\mathfrak{d} = (1)$ and $\mathfrak{d} = \mathfrak{z}$, where $\mathfrak{z}$ is the prime ideal above 3 (recall that $m \equiv 2, 3, 4 \bmod 9$, hence $3\mathcal{O}_K = \mathfrak{z}^3$). The second case is only possible if $3 \mid s$, but this leads quickly to a contradiction, since in this case r and t are not divisible by 3, and $r^2 - mt^6$ is not divisibly by 9 in this case. Thus $(\alpha) = \mathfrak{a}^2$ is an ideal square. □

For showing that H/K is a quadratic extension we need to know when α is square in K. To this end let us first characterize the points on E that give rise to squares:

Lemma 8.3. *Let m be a cubefree integer, $K = \mathbb{Q}(\omega)$ the corresponding pure cubic number field with $\omega^3 = m$, and $E\colon\ y^2 = x^3 - m$ an elliptic curve. Every rational affine point $P \in E(\mathbb{Q})$ can be written in the form $P = (r/t^2, s/t^3)$ for integers r, s, t with $\gcd(r, t) = \gcd(s, t) = 1$.*

The map $\alpha\colon\ E(\mathbb{Q}) \longrightarrow K^\times/K^{\times 2}$ defined by $\alpha(P) = (r - t^2\omega)K^{\times 2}$ is a group homomorphism whose kernel contains $2E(\mathbb{Q})$; more exactly $\alpha(2P)$ is represented by the square of $\beta = (r - t^2\omega)^2 - 3(t^2\omega)^2$.

Finally if $P \in \ker\alpha$ and t is even, then $P = 2Q$ for some $Q \in E(\mathbb{Q})$.

P r o o f. For a proof that we may assume $\gcd(r, t) = \gcd(s, t) = 1$ see [15, p. 68].

Performing a 2-descent on the elliptic curve $E\colon\ y^2 = x^3 - m$ means studying the Weil map $E(K) \longrightarrow K^\times/K^{\times 2}$ which sends a K-rational point $P = (x, y)$ to the coset represented by $x - \omega$. The fact that the Weil map is a homomorphism is classical (see e.g. [15]); in particular, the restriction of the Weil map to $E(\mathbb{Q})$ is also a homomorphism.

Since the target group is $K^\times$ modulo squares, the Weil map can be defined by $\alpha(P) = (r - t^2\omega)K^{\times 2}$.

Now assume that $\alpha(P) = (r - t^2\omega)K^{\times 2}$ and set $\beta = \alpha(P)^2 - 3t^4\omega^2$. Then

$$\beta^2 = (r^2 - 2rt^2\omega - 2t^4\omega^2)^2 = r^4 + 8rt^6m - 4t^2\omega(r^3 - mt^6).$$

On the other hand, the group law on E gives

$$2(x, y) = \Big(\frac{9x^4}{4y^2} - 2x, -\frac{27x^6}{8y^3} + \frac{9x^3}{2y} - y\Big) = \Big(\frac{x^4 + 8mx}{(2y)^2}, \frac{x^6 - 20mx^3 - 8m^2}{(2y)^3}\Big).$$

Thus

$$x_{2P} = \frac{x^4 + 8mx}{(2y)^2} = \frac{x^4 + 8mx}{4x^3 - 4m} = \frac{r^4/t^8 + 8mr/t^2}{4r^3/t^6 - 4m} = \frac{r^4 + 8rmt^6}{4t^2(r^3 - mt^6)},$$

and this implies the claim.

Finally assume that $\alpha(P) \in K^{\times 2}$ for $P = (x, y)$. Since

$$y^2 = x^3 - m = (x - \omega)(x - \varrho\omega)(x - \varrho^2\omega),$$

we find that

$$x^2 + x\omega + \omega^2 = (x - \varrho\omega)(x - \varrho^2\omega) \in K^{\times 2}.$$

The ideals $(x - \varrho\omega)$ and $(x - \varrho^2\omega)$ are coprime in $L = K(\sqrt{-3})$ by the proof of Lemma 8.2, hence

$$r - \varrho\omega t^2 = \eta\beta^2 \tag{8.1}$$

for some unit η in L. Now we need a variant of Kummer's Lemma for L:

Proposition 8.4. *If η is a unit in L with $\eta \equiv \xi^2 \bmod 4$, then η is a square.*

Since the left hand side of (8.1) is congruent to 1 mod 4, Prop. 8.4 implies that η is a square. But then $r - \varrho\omega t^2$ (and therefore also $r - \varrho^2\omega t^2$) is a square. By [6, Prop. 1.7.5], we have $P = (x_P, y_P) = 2Q$ for some point $Q \in E(\mathbb{Q})$ on $E\colon\ y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$ if and only if $x_P - e_j$ is a square in $\mathbb{Q}(e_j)$ for $j = 1, 2, 3$. This implies our claims[5]. □

If E has rank $\geqslant 2$, let P and Q denote two generators of $E(\mathbb{Q})$. If one of them has the desired form, we are done. If not, then we claim that $P + Q$ works:

Lemma 8.5. *If P and Q are independent points with odd denominators, then $P + Q = (r/t^2, s/t^3)$ with $\gcd(r, t) = \gcd(s, t) = 1$ and $2 \mid t$.*

P r o o f. This is a direct consequence of the addition formulas. In fact, we find $x_3 = \mu^2 - x_1 - x_2$ for $\mu = (y_2 - y_1)/(x_2 - x_1)$. Now $(y_1 - y_2)(y_1 + y_2) = y_1^2 - y_2^2 = x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2)$; we know by assumption that $x_1 \equiv x_2 \equiv 1 \bmod 2$, hence the right hand side is divisible by 2. Since the second bracket on the right side is odd, the whole power of 2 is contained in $x_1 - x_2$. On the left hand side, the power of 2 is split among the factors $y_1 - y_2$ and $y_1 + y_2$, both of which are even. This implies that the denominator of μ must be even. In particular, the denominator of $x_3 = \mu^2 - x_1 - x_2$ must also be even, which is what we wanted to prove. □

It remains to give a

[5] A simpler proof that $P = 2Q$ in this case can be found in [9].

P r o o f of Prop. 8.4. We start by determining the unit group of L. We know that $E_K = \langle -1, \varepsilon\rangle$; it is easy to verify that $E = \langle -\varrho, \varepsilon, \varepsilon'\rangle$ has finite index in E_L (for example by showing that the regulator of this group is nonzero), where $\varepsilon' = 1 + 4b^2\varrho\omega - 2b\varrho^2\omega^2$ is the conjugate of ε over K. We first show that $E = E_L$.

- ▷ The units $\pm\varepsilon$ are not squares in L. In fact, if $\pm\varepsilon$ is a square in L, then $L = K(\sqrt{\pm\varepsilon})$. This implies that L/K is unramified outside 2∞, which contradicts the fact that L/K is ramified above 3.
- ▷ The units $\pm\varrho^c\varepsilon$ are not squares in L: this follows from above by noting that ϱ is a square in L.
- ▷ The units $\pm\varrho^c\varepsilon'$ and $\pm\varrho^c\varepsilon''$ are not squares in L: this follows by applying a suitable automorphism of $\mathrm{Gal}(L/\mathbb{Q})$.
- ▷ The units $\pm\varrho^c\varepsilon'\varepsilon''$ are not squares in L: this follows from the above by observing that $\varepsilon'\varepsilon'' = 1/\varepsilon$.

This shows that E has odd index in E_L. The fact that the index must then be 1 follows by applying the norm $N_{L/K}$ to any relation of the form $(-\varrho)^a\varepsilon^b\varepsilon'^c = \eta^p$.

Now assume that $\eta \equiv \xi^2 \bmod 4$ for some unit $\eta \in E_L$. Since ϱ is a square, we may assume that $\eta = (-1)^a\varepsilon^b\varepsilon'^c$ with $a, b, c \in \{0, 1\}$. We know that $\eta \equiv 1 \bmod 2$; if $\eta \equiv \xi^2 \bmod 4$, we must have $\eta \equiv 1 \bmod 4$. Checking the finitely many possibilities we easily deduce that $a = b = c = 0$, and this implies the claim. □

This completes the proof of Theorem 8.1. As a matter of fact, we can prove something stronger:

Theorem 8.6. *Let b be an odd integer such that $m = 8b^3 + 3$ is squarefree. Then the 2-rank s of the class group $\mathrm{Cl}_2(K)$ of $K = \mathbb{Q}(\sqrt[3]{m})$ and the rank r of the Mordell-Weil group $E(\mathbb{Q})$ of E: $y^2 = x^3 - m$ satisfy the inequality*

$$r \leqslant s + 1. \tag{8.2}$$

P r o o f. Let $P_1, \ldots, P_k$ denote the generators of $E(\mathbb{Q})$ with even denominators, and $P_{k+1}, \ldots, P_r$ those with odd denominators. Then the points $P_1, \ldots, P_k$, $P_{k+1} + P_r, \ldots, P_{r-1} + P_r$ are independent points in $E(\mathbb{Q}) \setminus 2E(\mathbb{Q})$ with even denominators; by what we have proved, the pure cubic field K has $r - 1$ independent unramified quadratic extensions. □

In the only case where we have been unable to compute the rank of the curve E_b, namely for $b = 13$, we find $s = 3$ and therefore $r \leqslant 4$. This does not improve on the bound coming from the Selmer rank, but it suggests that the rank r of $E(\mathbb{Q})$ in the preceding theorem may perhaps be replaced by some Selmer rank.

An inequality similar to (8.2) for general elliptic curves was given by Billing (see [6, Sect. 3.7]). For curves $E\colon\ y^2 = x^3 - m$, Billings bound was

$$r \leqslant \begin{cases} s+1 & \text{if } m \not\equiv \pm 1 \bmod 9, \\ s+2 & \text{if } m \equiv \pm 1 \bmod 9. \end{cases}$$

The main difference between Billing's result applied to E_b and ours is that Billing proved $r \leqslant s+1$, whereas we proved $s \geqslant r-1$ by more or less explicitly exhibiting generators of the quadratic unramified extensions of K.

Additional remarks and open problems

The explanation that the fields K_b tend to have even class numbers could have been giving by simply citing the parity conjecture and Billing's bound. We have shown more by using rational points on elliptic curves for constructing subfields of Hilbert class fields. It remains to be studied how much of Billing's bound can be proved in a similar way.

Instead of using the curves $E_m\colon\ y^2 = x^3 - m$ we could also investigate the family $E_{-m}\colon\ y^2 = x^3 + m$; in this case, the root number is $w(E_{-m}) = -w(E_m)$, so we expect that its rank is odd whenever m is squarefree. For the curves with rank 1, the generator seems to have even denominator in most cases. It also seems that the curves E_{-m} more often have nontrivial Tate-Shafarevich groups than the curves E_m, but this might be a general feature of families of elliptic curves with root number -1 when compared with families of curves with rank $\geqslant 1$ and positive root number.

I would like to call the attention of the readers to the fact that Soleng [16] has constructed a homomorphism from the group of rational points on elliptic curves to the class groups of certain quadratic number fields. Our map sending the points $P = (r/t^2, s/t^3)$ with even t to the ideal class $[\mathfrak{b}]$, where $(s + t^3\sqrt{-m}\,) = \mathfrak{b}^2$, does not seem to be a special case of Soleng's construction. Is this map also a homomorphism? How are these maps related to the group structure on Pell surfaces $y^2 + mz^2 = x^3$ studied in [8]?

Our calculations in the Mordell-Weil group of $y^2 = x^3 - 11$ and the corresponding pure cubic field $K = \mathbb{Q}(\sqrt[3]{11})$ paired with a strong belief in the prestabilized harmony of algebraic number theory suggest the following: If $P = (x, y)$ with $x = r/t^2$ is a rational point on the elliptic curve $E\colon\ y^2 = x^3 - m$, then under suitable conditions on m, the ideal $(r - t^2\omega) = \mathfrak{a}_P^2$ is an ideal square in $K = \mathbb{Q}(\sqrt[3]{m}\,)$, and the map sending P to the ideal class of $\mathfrak{a}_P$ is a homomorphism from $E(\mathbb{Q})$ to the 2-class group $\mathrm{Cl}(K)[2]$ of the pure cubic field K; this is in fact true, and will be proved in [9].

Here is one more question: Paul Monsky gave a proof that the class number of $\mathbb{Q}(\sqrt[4]{p})$ is even for primes $p \equiv 9 \bmod 16$ based on the parity conjecture in [13]; an unconditional proof of this fact can be found in [14]. Is it possible to give an unconditional proof of the results on the parity of the class numbers of the pure cubic fields K_b?

A c k n o w l e d g e m e n t. I thank Dror Speiser [12] for reminding me of the approach using elliptic curves and for pointing out the relevance of [11]. Paul Monsky kindly sent me an unpublished manuscript [13] in which he studied connections between the parity of class numbers of pure quartic fields and elliptic curves. All calculations were done with `pari` and `sage`.

References

[1] *M. Bhargava, A. Shankar*: Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. arXiv:1006.1002v2.
[2] *B. J. Birch, N. M. Stephens*: The parity of the rank of the Mordell-Weil group. Topology *5* (1966), 295–299. zbl
[3] *H. Cohen, H. W. Lenstra*: Heuristics on class groups of number fields. Number theory, Noordwijkerhout 1983, Proc. Journ. Arithm. Lect. Notes Math. 1068, Springer, Berlin, 1984, pp. 33–62. zbl
[4] *H. Cohen, J. Martinet*: Étude heuristique des groupes de classes des corps de nombres. J. Reine Angew. Math. *404* (1990), 39–76. (In French.) zbl
[5] *H. Cohen, J. Martinet*: Heuristics on class groups: some good primes are not too good. Math. Comp. *63* (1994), 329–334. zbl
[6] *I. Connell*: Elliptic Curves Handbook. 1996; see `http://www.math.mcgill.ca/connell/public/ECH1/`.
[7] *H. Eisenbeis, G. Frey, B. Ommerborn*: Computation of the 2-rank of pure cubic fields. Math. Comp. *32* (1978), 559–569. zbl
[8] *S. Hambleton, F. Lemmermeyer*: Arithmetic of Pell Surfaces. Acta Arith. *146* (2011), 1–12. zbl
[9] *F. Lemmermeyer*: Binomial squares in pure cubic number fields. J. Théor. Nombres Bordx. *24* (2012), 691–704.
[10] *F. Lemmermeyer, C. Snyder*: Exercises in Class Field Theory. In preparation.
[11] *E. Liverance*: A formula for the root number of a family of elliptic curves. J. Number Th. *51* (1995), 288–305. zbl
[12] Math Overflow, Question 70024.
[13] *P. Monsky*: A remark on the class number of $\mathbb{Q}(p^{1/4})$. Unpublished manuscript, 1991.
[14] *P. Monsky*: A result of Lemmermeyer on class numbers. arXiv 1009.3990.
[15] *J. Silverman, J. Tate*: Rational Points on Elliptic Curves. Springer, New York, 1992. zbl
[16] *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. zbl

Author's address: *F. Lemmermeyer*, Mörikeweg 1, 73489 Jagstzell, Germany, e-mail: `hb3@ix.urz.uni-heidelberg.de`.