JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Franz LEMMERMEYER

Binomial squares in pure cubic number fields

Tome 24, n° 3 (2012), p. 691-704.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_3_691_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 691-704

Binomial squares in pure cubic number fields

par Franz LEMMERMEYER

Résumé. Soit $K = \mathbb{Q}(\omega)$, avec $\omega^3 = m > 1$ un nombre entier, un corps de nombres cubique. Nous montrons que les éléments $\alpha \in K^\times$ avec $\alpha^2 = a - \omega$ (où a est un nombre rationnel) forment un groupe qui est isomorphe au groupe des points rationnels de la courbe elliptique $E_m : y^2 = x^3 - m$. Nous démontrons aussi comment utiliser cette observation pour construire des extensions quadratiques non ramifiées de K.

Abstract. Let $K = \mathbb{Q}(\omega)$, with $\omega^3 = m$ a positive integer, be a pure cubic number field. We show that the elements $\alpha \in K^\times$ whose squares have the form $a - \omega$ for rational numbers a form a group isomorphic to the group of rational points on the elliptic curve $E_m : y^2 = x^3 - m$. This result will allow us to construct unramified quadratic extensions of pure cubic number fields K.

Introduction

Let me begin by describing a method for solving certain diophantine equations invented by Euler and Lagrange. Euler, in his Algebra [7], showed that equations such as

$$x^2 + 2y^2 = z^3 \tag{0.1}$$

are easily solved by observing the following: set $x + y\sqrt{-2} = (p + q\sqrt{-2}\,)^3$; comparing real and imaginary parts shows that

$$x = p^3 - 6pq^2, \qquad y = 3p^2q - 2q^3,$$

and this provides us with infinitely many[1] solutions of Equation (0.1).

In [10, p. 532], read to the Academy two years before Euler's Algebra appeared[2], Lagrange exploits the same ideas (unlike Euler, however, Lagrange does not claim that his formulas would give all solutions), and extends them to algebraic numbers of degree > 2 in his theory of "fonctions semblables".

Thus for solving an equation of the form

$$r^3 - As^3 = p^2, \tag{0.2}$$

Manuscrit reçu le 7 octobre 2011, révisé le 15 décembre 2011.

[1]Euler realized that this parametrization does not always yield all possible solutions, but nevertheless used this technique for showing that certain diophantine equations do not have any nontrivial solutions.

[2]In [11], which appeared in 1774, Lagrange presented his "Additions" to Euler's Algebra.

Lagrange [10, p. 532] sets $p = t + ua\sqrt[3]{A} + xa^2\sqrt[3]{A^2}$ and observes that $p^2 = T + Va\sqrt[3]{A} + Xa^2\sqrt[3]{A^2}$ for

$$T = t^2 + 2Aux, \quad V = Ax^2 + 2tu, \quad X = u^2 + 2tx.$$

From $p^2 = r + s\sqrt[3]{A}$ he obtains $u^2 + 2tx = 0$. Solving for x and plugging the result into the other two equations gives

$$r = t^2 - \frac{Au^3}{t}, \quad s = -\frac{Au^4}{4t^2} - 2tu.$$

By giving T, U, V integral values, these formulas provide us with integral solutions of (0.2). In the case $A = 3$, for example, we find

t	u	x	r	s	p
1	2	-2	-23	-16	11
2	2	-1	25	-8	131

He then treats, in a similar way, the equation

$$r^3 - As^3 = p^3$$

and remarks

> Mais, comme nous ne nous proposons pas ici de traiter cette matière à fond, nous ne nous y arrètons pas davantage quant à présent;[3]

Lagrange had already remarked that his method, applied to the equation $r^n - As^n = p^n$, does not always give rational solutions when $n \geq 3$. At the end of his memoir he remarks that the equation $r^n + s^n = p^n$ was claimed to have no nonzero solution in rational numbers for $n > 2$ by Fermat, that Euler had shown this claim to be correct for the exponents $n = 3$ and $n = 4$ by a very ingenious analysis[4], and that the problem would deserve the highest attention by mathematicians.

A problem similar to (0.2) occurs when trying to solve the diophantine equation[5] $y^2 = x^3 + 1$ (or, equivalently, determining the integral points on this elliptic curve). The most direct way of attacking this equation probably is writing it in the form $(y-1)(y+1) = x^3$ and using unique factorization. If y is odd, one possibility we have to consider is $y - 1 = 2a^3$ and $y + 1 = 4b^3$ for integers a, b. This implies $a^3 - 2b^3 = -1$, which has the obvious solution $(a, b) = (1, 1)$, giving the solution $(x, y) = (2, 3)$ of the original equation. Showing that $a^3 - 2b^3 = -1$ does not have any other solution is

[3]But since we do not intend to treat this matter thoroughly here, we will not dwell any longer on this topic for now;

[4]Euler must have found a proof of Fermat's Last Theorem for the exponent $n = 3$ in 1753, as his correspondence with Goldbach (Aug. 4, 1753) shows. Euler mentioned this proof in E272, but it is not clear to me to which proof Lagrange is referring here. The case $n = 4$ was proved by Euler in E098.

[5]This was first solved by Euler; see [12].

a slightly technical task. A famous result due to Delaunay and Nagell (see [14]) tells us that equations $a^3 - mb^3 = 1$ for noncubes m have at most one integral solution. For proving this result one needs to study units of the form $a - b\sqrt[3]{m}$ in pure cubic number fields and show that these units, with a few exceptions, cannot be powers of other units.

In this article we shall investigate squares of the form $a + b\sqrt[3]{m}$ in pure cubic number fields and explain why their occurrence in diophantine problems related to elliptic curves is quite natural. We will also show how to apply our results to the construction of unramified quadratic extensions of pure cubic number fields; in particular, we will give these extensions for all values $2 \le m \le 113$ for which $K = \mathbb{Q}(\sqrt[3]{m})$ has even class number.

Each pure cubic number field $K = \mathbb{Q}(\sqrt[3]{m})$ contains binomial squares: trivial examples are $r^2 = r^2 + 0\sqrt[3]{m}$ and $\sqrt[3]{m^2}^2 = 0 + m\sqrt[3]{m}$. Finding nontrivial binomial squares is more challenging: in $\mathbb{Q}(\sqrt[3]{2})$, squares of the form $a - b\sqrt[3]{2}$ are

$$(1 - \sqrt[3]{2} - \sqrt[3]{4})^2 = 5 - \sqrt[3]{4},$$
$$(9 - 6\sqrt[3]{2} - 2\sqrt[3]{4})^2 = 129 - 100\sqrt[3]{2},$$
$$(16641 - 25800\sqrt[3]{2} - 20000\sqrt[3]{4})^2 = 2340922881 - 58675600\sqrt[3]{2},$$

where $58675600 = 7660^2$.

This abundance of examples in $\mathbb{Q}(\sqrt[3]{2})$ should not mislead the readers into thinking that this is a typical phenomenon; in fact, there are no nontrivial squares of the form $a - \sqrt[3]{3}$ at all in $\mathbb{Q}(\sqrt[3]{3})$.

1. The group law

Fix a cubefree integer m, let $K = \mathbb{Q}(\sqrt[3]{m})$ denote the corresponding pure cubic number field, and consider the set

$$S_m = \{\alpha \in K^\times : \alpha^2 = a - \sqrt[3]{m} : a \in \mathbb{Q}^\times\}.$$

Writing $\alpha = r + s\omega + t\omega^2$ with $\omega = \sqrt[3]{m}$ we find that the condition $\alpha^2 = a - \omega$ is equivalent to the system of equations

$$2rt + s^2 = 0, \tag{1.1}$$
$$2rs + mt^2 = -1, \tag{1.2}$$
$$2mst + r^2 = a. \tag{1.3}$$

Since $t = 0$ implies $s = 0$ and $a = r^2$ (which is the trivial solution), we may assume that $t \neq 0$; solving (1.1) for r and plugging the resulting equation $r = -s^2/2t$ into (1.2) we find $-s^3/t + mt^2 = -1$ which, after dividing through by $-t^2$ gives the point

$$P_\alpha = (x, y) = \Big(\frac{s}{t}, \frac{1}{t}\Big) \quad \text{on the elliptic curve } y^2 = x^3 - m.$$

The missing parameters a and r are given by $r/t = -\frac{1}{2}(s/t)^2$ and by (1.3).

Conversely, every affine point $(x,y) \in E_m(\mathbb{Q})$ gives a unique element of S_m via

$$t = \frac{1}{y}, \quad s = \frac{x}{y}, \quad r = \frac{x^2}{2y}, \quad \text{and} \quad a = \frac{x^4+8mx}{4y^2}. \tag{1.4}$$

Of course we make the point at infinity on $E_m(\mathbb{Q})$ correspond to the (class of the) trivial element $1 \in S_m$.

We have proved

Theorem 1. *Let m be an integer that is not a cube, let $K = \mathbb{Q}(\omega)$ with $\omega^3 = m$ denote the corresponding pure cubic field, and let E_m denote the elliptic curve $y^2 = x^3 - m$. There is a bijection between the rational points $(x,y) \in E_m(\mathbb{Q})$ and the elements $\alpha \in K^\times$ with $\alpha^2 = a - \omega$ for $a \in \mathbb{Q}^\times$. In fact, if $\alpha = r+s\omega+t\omega^2$ satisfies $\alpha^2 = a-\omega$, then $(x,y) \in E_m(\mathbb{Q})$ for $x = \frac{s}{t}$ and $y = \frac{1}{t}$. Clearly $\alpha = 1$ corresponds to the point at infinity on E, and multiplication by -1 in $K^\times$ corresponds to multiplication by -1 in $E_m(\mathbb{Q})$.*

Conversely, an affine point (x,y) corresponds to

$$\alpha = -\frac{x^2}{2y} + \frac{x}{y}\omega + \frac{1}{y}\omega^2 \quad \text{with } \alpha^2 = \frac{x^4+8mx}{4y^2} - \omega.$$

Multiplying through by $4y^2$ gives the simpler identity

$$(x^2 - 2x\omega - 2\omega^2)^2 = x^4 + 8mx - 4y^2\omega,$$

which can easily be verified directly.

Remark 1. If $\alpha = r + s\omega + t\omega^2$ with $\omega = \sqrt[3]{m}$ satisfies $\alpha^2 = a - \omega$ for some $a \in \mathbb{Q}^\times$, then $\alpha_1 = r - s\omega + t\omega^2$ has the property that $\alpha_1^2 = c - d\omega$ for suitable rational numbers c, d; this is due to the fact that Eqn. (1.1) remains invariant under $s \mapsto -s$.

Remark 2. The observation that rational points on elliptic curves without 2-torsion and elements of cubic number fields are related is classical. In fact, consider an elliptic curve $E : y^2 = f_3(x)$, where $f_3 \in \mathbb{Q}[x]$ is an irreducible polynomial, let ω denote a root of f_3, and set $K = \mathbb{Q}(\omega)$. Weil's proof of the Mordell-Weil theorem for such elliptic curves E uses a homomorphism $\alpha : E(\mathbb{Q}) \longrightarrow K^\times/K^{\times 2}$ defined by $\alpha(P) = (x-\omega)K^{\times 2}$, where $P = (x,y)$. This map α has kernel $2E(\mathbb{Q})$, giving us an injection $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow K^\times/K^{\times 2}$.

Theorem 1, on the other hand, gives a bijection between the group $E_m(\mathbb{Q})$ of rational points on an elliptic curve and a subset S_m of $K^\times/\mathbb{Q}^\times$, and the group structure on S_m is not the one inherited from $K^\times$.

Both results can be used to show that certain elements of $K^\times$ are not squares. The proof of Theorem 1 requires nothing beyond high school algebra and thus is a lot less deep than the exact sequence

$$0 \longrightarrow 2E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \xrightarrow{\alpha} K^\times/K^{\times 2}$$

coming from 2-descent on E, whose proof uses the addition law on $E(\mathbb{Q})$ as well as the arithmetic of ideals and units of the number field K.

Corollary 2. *If $E_m : y^2 = x^3 - m$ has no rational point except the point at infinity, then there are no squares of the form $a - \omega$ in $K = \mathbb{Q}(\omega)$ with $a \in \mathbb{Q}^\times$ and $\omega = \sqrt[3]{m}$.*

Remark. Torsion points of order 3 on E_m do not contribute significantly. In fact, the torsion points $(0, \pm k)$ on $y^2 = x^3 + k^2$ give rise to the trivial solutions $\sqrt[3]{k^2}^2 = k\sqrt[3]{k}$.

Some expressions occurring in Thm. 1 have a natural explanation in terms of the group law on elliptic curves.

The group law on E_m is given by the following formulas: given rational points (x_1, y_1) and (x_2, y_2), set

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_2 \neq x_1, \\ \frac{3x_1^2}{2y_1} & \text{if } x_2 = x_1. \end{cases}$$

Then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + y_1 - \lambda x_1.$$

The duplication formula for $P = (x, y)$ is given by

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

Comparing this formula with (1.4) we immediately get

Corollary 3. *The element $a - \omega$ is a square in K if and only if $a = x_{2P}$ for some point $P \in E_m(\mathbb{Q})$. In this case, $N(a - \omega) = y_{2P}^2$.*

The last claim is a simple calculation:

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

Example. Consider the element $\beta = 5 - \sqrt[3]{4}$ in $K = \mathbb{Q}(\sqrt[3]{2}\,)$, whose norm $5^3 - 4 = 11^2$ is a square. For deciding whether β is a square in K we observe that the point $P = (5, 11)$ on $y^2 = x^3 - 4$ is a multiple of 2 since $P = 2(2, -2)$. Thus $\beta = \alpha^2$ is a square, and the formulas above give $\alpha = -1 + \sqrt[3]{4} + \frac{1}{2}\sqrt[3]{16} = -1 + \sqrt[3]{2} + \sqrt[3]{4}$ as well as $N(\beta) = N(\alpha)^2 = 11^2$.

The example of Bachet-Fermat. Consider the curve $E_2 : y^2 = x^3 - 2$. The integral point $P = (3, 5)$ corresponds to

$$\alpha_P = -\frac{9}{10} + \frac{3}{5}\sqrt[3]{2} + \frac{1}{5}\sqrt[3]{4} \quad \text{with} \quad \alpha_P^2 = \frac{129}{100} - \sqrt[3]{2}.$$

Multiplying through by 10^2 shows that P gives rise to

$$(-9+6\sqrt[3]{2}+2\sqrt[3]{4}\,)^2 = 129-100\sqrt[3]{2}.$$

Observe that $2P = (\frac{129}{100}, \frac{383}{1000})$ corresponds to

$$\alpha_{2P} = -\frac{16641}{7660} + \frac{1290}{383}\omega + \frac{1000}{383}\omega^2$$

with $\alpha_{2P}^2 = \frac{2340922881}{58675600} - \omega$. Finally we remark that

$$3P = \Big(\frac{164323}{171^2}, -\frac{66234835}{171^3}\Big),$$
$$\alpha_{3P} = \frac{27002048329}{22652313570} - \frac{28099233}{66234835}\sqrt[3]{2} - \frac{5000211}{66234835}\sqrt[3]{4}.$$

2. Explicit multiplication formulas

Recall that we have constructed a bijection between elements $\alpha \in K^\times$ with $\alpha^2 = a-\omega$ and rational points on the elliptic curve $E_m : y^2 = x^3 - m$. The group structure on $E_m(\mathbb{Q})$ induces, by transport of structure, a group law on S_m. In this section we will give explicit formulas for the group law on S_m.

To this end assume that $\alpha_j = r_j + s_j\omega + t_j\omega^2$ $(j = 1, 2)$ are elements whose squares have the form $a_j - \omega$. Then these elements correspond to the points

$$P_j = \Big(\frac{s_j}{t_j}, \frac{1}{t_j}\Big)$$

on the elliptic curve $E_m : y^2 = x^3 - m$. The sum $P_3 = P_1 + P_2$ corresponds to an element $\alpha_3 \in K^\times$ with $\alpha_3^2 = a_3 - \omega$, and we can compute formulas for $\alpha_3 = \alpha_1 * \alpha_2$ by using the group law on elliptic curves. The "multiplication formulas" for the α_j have little if anything to do with multiplication in $K^\times$ and are rather complicated. It remains to be seen whether there is any geometric interpretation of these formulas.

If $\frac{s_1}{t_1} \ne \frac{s_2}{t_2}$, then we find

$$x_3 = \Big(\frac{\frac{1}{t_2}-\frac{1}{t_1}}{\frac{s_2}{t_2}-\frac{s_1}{t_1}}\Big)^2 - \frac{s_1}{t_1} - \frac{s_2}{t_2} = \Big(\frac{t_1-t_2}{t_1s_2-t_2s_1}\Big)^2 - \frac{s_1}{t_1} - \frac{s_2}{t_2},$$
$$y_3 = \frac{t_1-t_2}{t_1s_2-t_2s_1}\Big(x_3 - \frac{s_1}{t_1}\Big) + \frac{1}{t_1}.$$

From these values we can compute the coefficients of

$$\alpha_1 * \alpha_2 = \alpha_3 = r_3 + s_3\omega + t_3\omega^2.$$

For what it's worth, the corresponding values of s_3 and t_3 are given by

$$s_3 = \frac{x_3}{y_3} = \frac{\mathrm{num}(s)}{\mathrm{den}(s)}, \qquad t_3 = \frac{1}{y_3} = \frac{\mathrm{num}(t)}{\mathrm{den}(t)}$$

with

$$\begin{aligned}\operatorname{num}(s) &= (s_1t_2 - s_2t_1)((s_1t_2 + s_2t_1)(s_1t_2 - s_2t_1)^2 - t_1t_2(t_1 - t_2)^2)\\ \operatorname{den}(s) &= t_1t_2(t_1 - t_2)^3 + (s_1t_2 - s_2t_1)^2(s_1t_2^2 + 2(s_2 - s_1)t_2t_1 - s_2t_1^2)\\ \operatorname{num}(t) &= (s_2t_1 - s_1t_2)^3t_1t_2,\\ \operatorname{den}(t) &= t_1t_2(t_1 - t_2)^3 + (s_1t_2 - s_2t_1)^2(s_1t_2^2 + 2(s_2 - s_1)t_1t_2 - s_2t_1^2).\end{aligned}$$

Setting

$$S_- = s_1t_2 - s_2t_1, \quad S_+ = s_1t_2 + s_2t_1, \quad T_- = t_1 - t_2 \quad \text{and} \quad T_+ = t_1t_2,$$

as well as

$$\Sigma = s_1t_2^2 + 2(s_2 - s_1)t_1t_2 - s_2t_1^2 = (s_2 - s_1)T_+ - S_+T_-,$$

the multiplication formulas become

$$s_3 = \frac{S_-^3S_+ - S_-T_-^2T_+}{T_-^3T_+ + S_-^2\Sigma}, \qquad t_3 = -\frac{S_-^3T_+}{T_-^3T_+ + S_-^2\Sigma}.$$

Let us check these formulas by "multiplying" the elements

$$\alpha_1 = \frac{9}{10} - \frac{3}{5}\sqrt[3]{2} - \frac{1}{5}\sqrt[3]{4} \quad \text{and} \quad \alpha_2 = -\frac{16641}{7660} + \frac{1290}{383}\sqrt[3]{2} + \frac{1000}{383}\sqrt[3]{4}.$$

We find

$$\begin{aligned} s_1 &= -\frac{3}{5} & t_1 &= -\frac{1}{5} & S_- &= -\frac{342}{383} & T_+ &= -\frac{200}{383}\\ s_2 &= \frac{1290}{383} & t_2 &= \frac{1000}{383} & S_+ &= -\frac{858}{383} & T_- &= -\frac{5383}{1915}\\ \Sigma &= -\frac{6138414}{733445}\end{aligned}$$

This yields

$$s_3 = -\frac{28099233}{66234835}, \qquad t_3 = -\frac{5000211}{66234835}, \qquad r_3 = -\frac{s_3^2}{2t_3} = \frac{27002048329}{22652313570}$$

in perfect agreement with our calculations at the end of Section 1.

3. Squares of the form $a - b\omega$

Consider more generally the problem of classifying squares of the form $a - b\omega$ for some fixed value of $b \in \mathbb{Q}^\times$. Since $a - b\omega = a - \omega'$ for $\omega' = \sqrt[3]{mb^3}$ we find, by simply replacing m with mb^3 in Thm. 1, the following

Theorem 4. *Let m be an integer that is not a cube, let $K = \mathbb{Q}(\omega)$ with $\omega^3 = m$ denote the corresponding pure cubic field, and let E_m denote the elliptic curve $y^2 = x^3 - m$. There is a bijection between elements $\alpha \in K^\times$ with $\alpha^2 = a - b\omega$ for $a, b \in \mathbb{Q}$ and the rational points $(x, y) \in E'_m(\mathbb{Q})$, where $E'_m : y^2 = x^3 - mb^3$ is a quadratic twist of E_m.*

In fact, if $\alpha = r + s\omega + t\omega^2$ *satisfies* $\alpha^2 = a - b\omega$, *then* $(x, y) \in E'_m(\mathbb{Q})$ *for* $x = bs/t$ *and* $y = b^2/t$.

Conversely, an affine point $(x, y) \in E'_m(\mathbb{Q})$ *corresponds to*

$$\alpha = -\frac{x^2}{2y} + \frac{bx}{y}\omega + \frac{b^2}{y}\omega^2 \qquad \text{with } \alpha^2 = \frac{x^4 + 8mx}{4y^2} - b\omega.$$

In particular, $a - b\omega$ *is a square with* $N(a - b\omega) = y^2$ *if and only if* $(a, y) \in 2E'(\mathbb{Q})$.

Example. The unit

$$-19 + 7\sqrt[3]{20} = (1 + \sqrt[3]{20} - \sqrt[3]{50}\,)^2$$

is a well known example due to Nagell [14]; since $\sqrt[3]{50} = \frac{1}{2}\sqrt[3]{20}^2$, it comes from the point $P(-2, -2)$ on the quadratic twist $-7y^2 = x^3 - 20$ of the elliptic curve $y^2 = x^3 - 20$. The corresponding point on the elliptic curve $y^2 = x^3 + 7^3 \cdot 20$ is $P'(14, 98)$. Observe that $2P' = (-19, 1)$.

Corollary 5. *There is a binomial unit* $a - b\omega$ *that is a square in* K *if and only if there is an integral point* $(a, 1) \in 2E(\mathbb{Q})$ *on* $E' : y^2 = x^3 - mb^3$.

4. A homomorphism from $E(\mathbb{Q})$ to $\mathrm{Cl}(K)$

In this section we will define a map from $E(\mathbb{Q})$, the group of rational points on $E : y^2 = x^3 - m$ (where $m \not\equiv 0, \pm 1 \bmod 9$ is a cubefree integer), to the group $\mathrm{Cl}(K)[2]$ of ideal classes of order dividing 2 in $K = \mathbb{Q}(\sqrt[3]{m}\,)$, and show that this map is a homomorphism.

Remark. The condition $m \not\equiv \pm 1 \bmod 9$ occurring below also comes up in connection with integral bases in pure cubic fields: if $m = ab^2$ with a, b squarefree, then $1, \omega_1 = \sqrt[3]{ab^2}$ and $\omega_2 = \sqrt[3]{a^2b}$ form an integral basis of $\mathcal{O}_K$. The fact that this condition is relevant for comparing the ranks of elliptic curves and 2-class groups of pure cubic fields was noticed on a regular basis: see e.g. [3, 6, 4, 2] and the discussion in [13].

Theorem 6. *Let* $m \not\equiv 0, \pm 1 \bmod 9$ *be a cubefree integer, and consider the cubic number field* $K = \mathbb{Q}(\sqrt[3]{m}\,)$ *and the elliptic curve* $E : y^2 = x^3 - m$. *For any* $P = (x, y) \in E(\mathbb{Q}) \setminus \{\infty\}$, *set* $x = a/e^2$ *for coprime integers* a *and* e. *Then* $(a - e^2\omega) = \mathfrak{a}^2$, *and the map* $P \mapsto [\mathfrak{a}]$ *induces a homomorphism* $\kappa : E(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)[2]$.

Proof. Since $a^3/b^3 - m = y^2$ we find that $N(a - b\omega) = y^2b^3$. Since $b = e^2$ is a square (see [18, p. 68]), the norm of $\alpha = a - b\omega$ is a square. Thus (α) is the square of an ideal if and only if $a - b\omega$ is coprime to its conjugates $\alpha' = a - b\omega\rho$ and $\alpha'' = a - b\omega\rho^2$ in the normal closure L of $K/\mathbb{Q}$. Let $\mathfrak{d}$ be the greatest common ideal divisor of α and α'. Then $\mathfrak{d} \mid \alpha''$, hence $\mathfrak{d}$ divides

the trace $3a$ of α as well as the difference $\alpha - \alpha' = b\omega(1-\rho)$. Since a and b are coprime, $\mathfrak{d}$ is a product of ideals above 3.

Since we have assumed that $m \not\equiv \pm 1 \bmod 8$, we have $(3) = \mathfrak{q}^3$ in K (see e.g. [5] for the decomposition law in pure cubic number fields). Assume therefore that $\mathfrak{q} \mid (\alpha)$ (this implies that $\mathfrak{q} \mid (\alpha')$ since $\mathfrak{q}$ is totally ramified). If $3 \mid m$, then $3 \mid a$, and from $y^2 = a^3/b^3 - m$ we deduce that $3^2 \mid m$ contradicting our assumptions. If $3 \nmid m$, then $a^3 - mb^3 = y^2b^3$ is divisible by 3 if and only if it is divisibly by 9, and now $a^3 \equiv mb^3 \bmod 9$ implies that $m \equiv \pm 1 \bmod 9$, again contradicting our assumptions. Thus $(\alpha) = \mathfrak{a}^2$, and $[\mathfrak{a}] = \kappa(P)$ is an ideal class of order dividing 2 in K. It remains to show that κ is a homomorphism.

To this end, assume that $x_P = a/b$ and $x_Q = c/d$ for $P, Q \in E(\mathbb{Q})$. Set $\kappa(P) = [\mathfrak{a}]$ and $\kappa(Q) = [\mathfrak{b}]$. We have to show that $\kappa(P+Q) = [\mathfrak{ab}]$, which is equivalent to $\kappa(P)\kappa(Q)\kappa(R) \sim 1$ for collinear rational points $P, Q, R \in E(\mathbb{Q})$.

The Weil map $\alpha : E(K) \longrightarrow K^\times/K^{\times 2}$ defined by

$$\alpha(P) = \begin{cases} (x-\omega)K^{\times 2} & \text{if } P = (x,y),\ y \neq 0 \\ 3\omega K^{\times 2} & \text{if } P = (\omega, 0), \\ K^{\times 2} & \text{if } P = \mathcal{O} \end{cases}$$

(see e.g. [9, (4.2)]) is a homomorphism, and if we restrict α to $E(\mathbb{Q})$, then the second case cannot occur. This shows that $(x_P - \omega)(x_Q - \omega)(x_R - \omega)$ is a square in $K^\times$. Thus $(a - b\omega)(c - d\omega)(e - f\omega) = \beta^2$, where $x_R = e/f$, and $\mathfrak{a}^2\mathfrak{b}^2\mathfrak{c}^2 = (\beta)^2$. But this implies $\mathfrak{abc} = (\beta)$. □

We now discuss a few examples.

Example 1. Let $K = \mathbb{Q}(\sqrt[3]{26}\,)$ and $E : y^2 = x^3 - 26$. Then $E(\mathbb{Q})$ is generated by $P = (3,1)$ and $Q = (35, 207)$. The element $3 - \omega$ is a unit, and $(35 - \omega) = \mathfrak{3}_1^3\mathfrak{3}_2\mathfrak{q}^2$, where $(3) = \mathfrak{3}_1\mathfrak{3}_2^2$ and where $\mathfrak{q}$ is a prime ideal above 23. This shows that the condition $m \not\equiv \pm 1 \bmod 9$ cannot be dropped.

Example 2. Let $K = \mathbb{Q}(\sqrt[3]{47}\,)$ and $E : y^2 = x^3 - 47$. Then $E(\mathbb{Q})$ is generated by $P = (6, 13)$ and $Q = (12, 41)$; moreover, $P + Q = (34/9, -71/27)$. We have

$$(6 - \omega) = \mathfrak{p}_{13}^2, \quad (12 - \omega) = \mathfrak{p}_{41}^2, \quad (34 - 9\omega) = \mathfrak{p}_{71}^2.$$

The ideals $\mathfrak{p}_{13}$ and $\mathfrak{p}_{41}$ generate the ideal class of order 2, the ideal $\mathfrak{p}_{71}$ is principal.

Example 3. Let $m = 57$; then $P = (4873/36, -340165/216)$ generates $E(\mathbb{Q})$, $(4873 - 36\omega) = \mathfrak{a}^2$, and $\mathfrak{a}$ is principal. The elliptic curve $E' : y^2 = x^3 - 57^2$ has rank 0 according to `sage` [16] since $L(E', 1) \neq 0$, and has nontrivial Tate-Shafarevich group $\mathbf{Ш}(E')$.

This suggests the question whether there is any connection between the kernel of κ in $E(\mathbb{Q})$ and the Tate-Shafarevich group $\mathbf{Ш}(E')$ of E'.

Remark. If we consider the more general case of elliptic curves $y^2 = x^3 - mb^3$, then a point $(x, y) \in E(\mathbb{Q})$ with $x = a/e^2$ provides us with an element $\alpha = a - be^2\omega$ with square norm $N(\alpha) = a^3 - mb^3e^6 = (ye^3)^2$; yet (α) need not be a square of an ideal if $\gcd(a, b) \neq 1$. In fact, $(14, 44)$ is a rational point on $y^2 = x^3 - 2^3 \cdot 101$, and neither $(14 - 2\omega)$ nor $(7 - \omega)$ are squares of ideals in $K = \mathbb{Q}(\omega)$ with $\omega^3 = 101$.

On the other hand, the proof of Thm. 6 shows

Lemma 7. *Assume that m is a cubefree integer with $m \not\equiv 0, \pm 1 \bmod 9$, set $\omega = \sqrt[3]{m}$, and let $P = (x, y)$ be a rational point on $E : y^2 = x^3 - mb^3$ for some integer b. Write $x = a/e^2$; then $(a - be^2\omega)$ is a square of an ideal in K whenever $\gcd(a, b) = 1$.*

5. Hilbert 2-class fields

Let $K = \mathbb{Q}(\omega)$ with $\omega^3 = m$ be a cubic number field, where we assume that $m \not\equiv 0, \pm 1 \bmod 9$, and let $E : y^2 = x^3 - mb^3$ be a quadratic twist of E. If $\mathrm{q}P = (x, y) \in E(\mathbb{Q}) \setminus 2E(\mathbb{Q})$ is a rational point with $x = r/s^2$ and coprime integers r, s, then $\alpha = r - s^2b\omega \in K$ has norm $r^3 - ms^6b^6 = y^2(bs)^6$. Since α is not a square, $K_P = K(\sqrt{\alpha})$ is a quadratic extension. Next (α) is a square of an ideal by Lemma 7, hence the extension K_P/K can only ramify at the primes above 2 and ∞. If $2 \mid s$ and if r is chosen positive, then $r \equiv 1 \bmod 4$ since $r^3 \equiv 1 \bmod 4$, and in this case the extension K_P/K is unramified everywhere.

Table 5.1 lists the pure cubic number fields with even class number and $m \leq 113$, an elliptic curve E whose rational points provide us with unramified quadratic extensions $K(\sqrt{\alpha})$.

For $m = 113$, the three quadratic unramified extensions are generated by roots of the polynomials

$$f_1(x) = x^6 - 291x^4 + 28227x^2 - 717409$$
$$f_2(x) = x^6 - 130347x^4 + 5663446803x^2 - 34351825047849$$
$$f_3(x) = x^6 - 3771x^4 + 4740147x^2 - 1186320249$$

Since neither of the three points from which these extensions originate are in $2E(\mathbb{Q})$, these three extensions are pairwise distinct.

In the case of $m = 2351$, it can be checked that the three unramified (in all three cases, we have $\alpha > 0$, so there is no ramification at infinity) quadratic extensions generated by roots of the polynomials

$$f_1(x) = x^6 - 171x^4 + 9747x^2 - 4247721,$$
$$f_2(x) = x^6 + 1653x^4 + 910803x^2 - 92717641,$$
$$f_3(x) = x^6 + 261x^4 + 22707x^2 - 3404025$$

are independent.

m	$\mathrm{Cl}_2(K)$	E	x_P	α
11	2	$y^2 = x^3 - 11$	$9/4$	$9 - 4\omega$
15	2	$y^2 = x^3 + 15$	$1/4$	$1 + 4\omega$
39	2	$y^2 = x^3 + 39$	$217/4$	$217 + 4\omega$
43	4	$y^2 = x^3 - 43$	$1177/36$	$1177 - 36\omega$
47	2	$y^2 = x^3 + 47$	$17/4$	$17 - 4\omega$
57	2	$y^2 = x^3 - 57$	$4873/36$	$4873 - 36\omega$
58	2	$y^2 = x^3 - 58$	$5393/484$	$5393 - 484\omega$
61	2	$y^2 = x^3 - 61$	$929/100$	$929 - 100\omega$
63	2	$y^2 = x^3 + 63$	$9/4$	$9 + 4\omega$
65	2	$y^2 = x^3 + 27 \cdot 65$	$129/4$	$129 + 3 \cdot 4\omega$
66	2	$y^2 = x^3 + 66$	$1/4$	$1 + 4\omega$
67	2	$y^2 = x^3 - 67$	$17/4$	$17 - 4\omega$
76	2	$y^2 = x^3 - 76$	$17/4$	$17 - 4\omega$
79	2	$y^2 = x^3 + 27 \cdot 79$	$1921/100$	$1921 + 3 \cdot 100\omega$
83	2	$y^2 = x^3 - 83$	$33/4$	$33 - 4\omega$
89	2	$y^2 = x^3 - 89$	$153/4$	$153 - 4\omega$
101	2	$y^2 = x^3 - 101$	$6342921/1073296$	$6342921 - 1073296\omega$
105	2	$y^2 = x^3 - 105^2$	$16465/196$	$16465 - 196\omega^2$
106	2	$y^2 = x^3 - 106$	$8297/1024$	$8297 - 1024\omega$
113	$(2,2)$	$y^2 = x^3 - 27 \cdot 113$	$97/4$	$97 - 3 \cdot 4\omega$
			$43449/2500$	$43449 - 3 \cdot 2500\omega$
			$1257/64$	$1257 - 3 \cdot 64\omega$
2351	$(4,2,2)$	$y^2 = x^3 + 27m$	$57/4$	$57 + 3 \cdot 4\omega$
			$-551/16$	$-551 + 3 \cdot 16\omega$
			$-87/4$	$-87 + 3 \cdot 4\omega$

TABLE 5.1. Quadratic unramified extensions of pure cubic number fields

Our results suggest that every unramified quadratic extension of a pure cubic number field $K = \mathbb{Q}(\sqrt[3]{m})$ can be computed from a rational point on some quadratic twist of the elliptic curve $y^2 = x^3 - m$.

6. Binomial cubes in pure cubic fields

Cubes of the form $a + b\omega$ in pure cubic number fields defined by $\omega^3 = m$ also are related to rational points on elliptic curves. The equation

$$(r + s\omega + t\omega^2)^3 = a + b\omega$$

in $K = \mathbb{Q}(\omega)$ leads to

$$mst^2 + r^2t + rs^2 = 0.$$

Dividing through by s^3 and setting $T = t/s$ and $R = r/s$ gives $mT^2 + TR^2 + R = 0$. Multiplying through by T and setting $x = -T$ and $y = RT$ finally gives

$$E : y^2 + y = mx^3. \tag{6.1}$$

Thus if $\alpha = r + s\omega + t\omega^2$ satisfies $\alpha^3 = a + b\omega$, then $(x, y) = (-t/s, rt/s^2)$ is a rational point on the elliptic curve (6.1). Multiplying (6.1) through by m^2 and setting $Y = my$, $X = mx$ gives

$$Y^2 + mY = X^3.$$

Conversely, assume that $(x, y) \in E(\mathbb{Q})$ is a rational point on the affine part of E. Writing $x = -t/s$ for coprime integers s, t and setting $r = -sy/x$ produces rational numbers r, s, t such that $\alpha = r + s\omega + t\omega^2$ satisfies $\alpha^2 = a + b\omega$.

We have proved

Theorem 8. *Let m be a cubefree integer and let $K = \mathbb{Q}(\omega)$ with $\omega^3 = m$ denote a pure cubic number field. There is a bijection between classes in $K^\times/\mathbb{Q}^\times$ represented by elements $\alpha \in K^\times$ with $\alpha^2 = a + b\omega$ for $a, b \in \mathbb{Q}$, and rational points on the elliptic curve $E : y^2 + y = mx^3$.*

In fact, if the cube of $\alpha = r + s\omega + t\omega^2$ is binomial, then $(-t/s, rt/s^2) \in E(\mathbb{Q})$. Conversely, every affine rational point $(x, y) \in E(\mathbb{Q})$ gives us some α via $x = -\frac{t}{s}$ and $r = -sy/x$.

Example. Let $m = 6$; then $Y^2 + 6Y = X^3$ has the rational point $(-2, -2)$, hence $(x, y) = (-1/3, -1/3)$ is a rational point on $y^2 + y = 6x^3$. Thus we set $t = 1$, $s = 3$, $r = -3$ and find

$$(-3 + 3\sqrt[3]{6} + \sqrt[3]{6}^2)^3 = -153 + 189\sqrt[3]{6}.$$

Multiplying through by $\sqrt[3]{6}^3 = 6$ and cancelling $3^3 = 27$ gives

$$(2 - \sqrt[3]{6} + \sqrt[3]{6}^2)^3 = -34 + 42\sqrt[3]{6}.$$

Example. Let $m = 20$; then the Mordell-Weil group of $Y^2 + 20Y = X^3$ is generated by $P = (-4, -4)$. Thus $Q = (-\frac{1}{5}, -\frac{1}{5})$ generates the group $E(\mathbb{Q})$, where $E : y^2 + y = 20x^3$. This gives $r = -5$, $s = 5$, $t = 1$, and

$$(-5 + 5\sqrt[3]{20} + \sqrt[3]{20}^2)^3 = 225 + 1575\sqrt[3]{20}.$$

Multiplying through by 20 and cancelling 5^3 gives

$$(4 - \sqrt[3]{20} + \sqrt[3]{20}^2)^3 = -36 + 252\sqrt[3]{20}.$$

The elliptic curve E in (6.1) can also be given in short Weierstrass form $E_m : Y^2 = X^3 + 16m^2$. This curve has two rational points $(\pm 4m, 0)$ of order 3, corresponding to the points $(0, 0)$ and $(-1, 0)$ of order 3 on E, or to the trivial binomial cubes $(\pm\omega)^3 = \pm m$. The curve E_m is 3-isogenous

to the curve $Y^2 = X^3 - 432m^2$, which in turn is isomorphic to the cubic $E'_m : x^3 + y^3 = m$. In particular, E and E_m have the same rank as E'_m, and we have found

Corollary 9. *There exist nontrivial binomial cubes in $K = \mathbb{Q}(\sqrt[3]{m})$ if and only if m is a sum of two rational cubes.*

7. Open Problems and Questions

There are a lot of questions that deserve being investigated in detail; below I will list some of them.

(1) Is it possible to use the connection between binomial squares in pure cubic fields and elliptic curves for streamlining the proofs of the theorem of Delone and Nagell? The classical proof distinguishes between binomial squares, binomial cubes, and binomial powers of higher degree, so the first two cases essentially deal with elliptic curves.

(2) Eisenbeis, Frey & Ommerborn [6] showed that the 2-class group of pure cubic number fields $K = \mathbb{Q}(\sqrt[3]{k})$ and the Selmer group of elliptic curves $y^2 = x^3 \pm k$ are intimately related. These authors constructed unramified 2-extensions of K from the Selmer group of E; this is a group that "contains" both the group of rational points on E and the Tate-Shafarevich group $\mathbf{Ш}(E)$ of E. One may hope that a close investigation of their results will shed some light on some of the numerical observations on $\mathbf{Ш}(E)$ made above.

(3) The question whether all quadratic unramified extensions of pure cubic fields arise from elliptic curves is probably a quite difficult one. If $K = \mathbb{Q}(\sqrt[3]{m})$ has a class group with large 2-rank, and if the ranks of the twists of the elliptic curve E_m could be shown to be bounded (and small), then we could produce a counterexample to the conjecture that all quadratic unramified extensions of pure cubic number fields come from elliptic curves. But this seems rather unlikely, to say the least.

(4) Many questions concerning relations between binomial squares and the 2-class group of K can also be asked in connection with binomial cubes and the 3-class group of K. There is some sort of genus theory for the 3-class group of pure cubic number fields; see e.g. [1].

In particular it would be interesting to see whether certain parts of the 3-class field of pure cubic fields can be constructed with the help of elliptic curves. If $K = \mathbb{Q}(\sqrt[3]{m})$ and $p \equiv 1 \bmod 3$ is a prime dividing m, then the field of p-th roots of unity has a cubic subfield F, and Abhyankar's Lemma shows that FK/K is a cyclic cubic unramified extension. On the other hand, it is also known (see e.g. [1] and [8]) that K has class number divisible by 3 e.g. when

$m = p^2q$ for primes $p \equiv q \equiv 2 \bmod 3$ such that $p^2q \not\equiv \pm 1 \bmod 9$ (the smallest example is $m = 20$). In this case, there seems to be no way of constructing the corresponding 3-class group except by doing calculations in the 3-class group of the compositum Kk, where $k = \mathbb{Q}(\sqrt{-3}\,)$ is the field of cube roots of unity. I would expect that these class fields can also be constructed from the group of k-rational points on the elliptic curves $x^3 + y^3 = m$. Nontrivial results on the rank of such curves were obtained by Satgé [17].

(5) Similar results are to be expected by studying binomial squares in pure quartic number fields. This is currently being investigated.

Acknowledgements

It is my pleasure to thank the referee and the editors for helpful comments, and the developers of `pari` [15] and `sage` [16], with which all computations were done, for their efforts.

References

[1] P. Barrucand, H. Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*. J. Number Theory **2** (1970), 7–21.
[2] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*. ArXiv:1006.1002v2.
[3] G. Billing, *Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins*. Nova Acta Reg. Soc. Ups. (IV) **11** (1938).
[4] H. Cohen, J. Martinet, *Heuristics on class groups: some good primes are not too good*. Math. Comp. **63** (1994), no. 207, 329–334.
[5] H. Cohn, *A classical invitation to algebraic numbers and class fields*. Springer-Verlag, 1978.
[6] H. Eisenbeis, G. Frey, B. Ommerborn, *Computation of the 2-rank of pure cubic fields*. Math. Comp. **32** (1978), 559–569.
[7] L. Euler, *Vollständige Anleitung zur Algebra* (E387, E388). St. Petersburg, 1770.
[8] T. Honda, *Pure cubic fields whose class numbers are multiples of three*. J. Number Theory **3** (1971), 7–12.
[9] D. Husemöller, *Elliptic Curves*. 2nd ed., Springer-Verlag, 2004.
[10] J.-L. Lagrange, *Sur la solution des problèmes indéterminés du second degré*. Mem. Acad. Sci. Berlin, 1769.
[11] J.-L. Lagrange, *Additions à l'analyse indéterminée*. Lyon, 1774.
[12] F. Lemmermeyer, *A note on Pépin's counter examples to the Hasse principle for curves of genus* 1. Abh. Math. Sem. Hamburg **69** (1999), 335–345.
[13] F. Lemmermeyer, *Why is the class number of* $\mathbb{Q}(\sqrt[3]{11}\,)$ *even?* Math. Bohemica, to appear.
[14] T. Nagell, *Solution complète de quelques équations cubiques à deux indéterminées*. J. Math. Pures Appl. **4** (1925), 209–270.
[15] `pari`, available from `http://pari.math.u-bordeaux.fr`
[16] `sage`, available from `http://sagemath.org`
[17] P. Satgé, *Un analogue du calcul de Heegner*. Invent. Math. **87** (1987), 425–439.
[18] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.

Franz Lemmermeyer
Mörikeweg 1
73489 Jagstzell
Germany
E-mail: `hb3@ix.urz.uni-heidelberg.de`