ACTA ARITHMETICA
146.4 (2011)

# A geometric proof of Kummer's reciprocity law for seventh powers

by

R. Clement Fernández, J. M. Echarri Hernández and E. J. Gómez Ayala (Bilbao)

**1. Introduction.** The use of elliptic curves to give proofs of reciprocity laws has a long history which goes back to Eisenstein, who proved the cubic and the biquadratic reciprocity laws by considering the values of elliptic functions at torsion points ([Le]). Other landmarks in this history were the proofs by Fueter ([F]) in 1927 of quadratic reciprocity over all imaginary quadratic fields and by Kubota ([K1]) in 1961 of cubic and biquadratic reciprocity using the theory of elliptic curves with complex multiplication. We refer the reader to the commentaries and references in [G4] for more about this fascinating topic.

Following the tracks of this rich tradition, Grant derived in [G2] Kummer's reciprocity law for fifth powers from the main theorems of complex multiplication of abelian varieties applied to the jacobian of the curve $y^2 = x^5 + 1/4$, which is a genus 2 curve and a rational image of the quintic Fermat curve, and asked whether other power reciprocity laws could be deduced in a similar way. In [G4] he himself gave a remarkable answer to this question, by proving Kummer's general reciprocity law for any regular prime and of Eisenstein's reciprocity law which rest on the arithmetical properties of the jacobians of rational images of the Fermat curves. Although the main idea is essentially the same in both papers, in [G2] a particular embedding of the jacobian in a projective space—which was constructed in [G1]—plays a central role, whereas in [G4] the chief tools are the theory of abelian varieties in arbitrary characteristics and the theory of formal groups. However, the strategy followed in [G4] does not seem to provide any method to tackle the complementary laws of Kummer's reciprocity.

2010 *Mathematics Subject Classification*: Primary 11G10, 11A15; Secondary 11G30, 11R18, 14K22.
*Key words and phrases*: Fermat jacobians, complex multiplication, Kummer's reciprocity law, complementary laws, formal group.

DOI: 10.4064/aa146-4-1  

According to Grant, the idea that formal groups could be used to prove higher reciprocity laws is due to Childress. The knowledge of the existence of a formal group whose points can be identified with the kernel of reduction seems to go back to Mattuck's thesis ([M]), which was supervised by Artin and completed in 1954.

In this paper we prove Kummer's reciprocity law for seventh powers making use of the theory of complex multiplication applied to the jacobian $J$ of the curve $y^2 = x^7 + 1/4$, which is a genus 3 curve and a rational quotient of the seventh Fermat curve. The main idea for the proof of the general law is, as in [G2], to reverse an argument of Kubota, who in [K2] derived facts about products of functions at torsion points using the reciprocity law. More precisely, we consider a number in the cyclotomic field of seventh roots of unity which is described as the product of a function of $J$ at torsion points and whose seventh roots lie in a division field of $J$ and deduce its factorization up to seventh powers using the theory of formal groups. This factorization, together with Gauss's lemma, provides the desired proof. Since we do not know an explicit embedding of $J$ in a projective space, the definition of this number differs from the one given by Grant in [G2].

A cornerstone of our proof of the complementary laws is the explicit knowledge of some 7-torsion points of $J$. The computation of these points is a somewhat delicate task that has been carried out in [C-E-G], taking advantage of the insights of Greenberg in [Gr]. It is possible that there is something deep in the relationship between Greenberg's work and our own that should be investigated in more detail. Moreover, along the way we obtain some interesting units as values of a rational function at torsion points, which perhaps deserve a closer look.

In Section 2 we gather some facts necessary to understand Kummer's reciprocity law for seventh powers and we state this law. In Section 3 we introduce the curve $x^7 + y^2 + y = 0$ (which coincides with the curve $y^2 = x^7 + 1/4$ after a linear change of variables) and its jacobian $J$, we study the formal group of $J$ at the origin and prove several results concerning $J$ and its torsion. In Section 4 we prove the general law and we conclude in Section 5 with the proof of the complementary laws.

Finally we want to point out that this work coincides essentially with the content of the second author's Ph.D. in the University of the Basque Country ([E]), which was completed in March 2006.

**2. Kummer's reciprocity law.** Let $\zeta$ denote a primitive seventh root of unity in $\mathbb{C}$ and let $F = \mathbb{Q}(\zeta)$. Let $\mathfrak{O}$ be the ring of integers of $F$, that is, $\mathfrak{O} = \mathbb{Z}[\zeta]$; recall that $\mathfrak{O}$ is a principal ideal domain. We set $\lambda = 1 - \zeta$, so that $\lambda\mathfrak{O}$ is the unique prime ideal of $\mathfrak{O}$ lying above 7. Let $\mu_1 = \zeta + \zeta^{-1}$ and $\mu_2 = \zeta^2 + \zeta^{-2}$; it can be shown that $\{\mu_1, \mu_2\}$ is a fundamental set of units

of $\mathfrak{O}$, so that every unit of $\mathfrak{O}$ can be written in a unique way as $\pm\zeta^i\mu_1^j\mu_2^k$ with $0 \le i \le 6$ and $j$ and $k$ in $\mathbb{Z}$. For every integer $i$, $1 \le i \le 6$, let $\sigma_i$ be the automorphism of $F$ defined by $\zeta^{\sigma_i} = \zeta^i$; then $\mathrm{Gal}\,(F/\mathbb{Q}) = \{\sigma_i \mid 1 \le i \le 6\}$. If $\sigma_i \in \mathrm{Gal}\,(F/\mathbb{Q})$, for any $\alpha \in F$ and any ideal $\mathfrak{a}$ of $\mathfrak{O}$, we shall denote by $\alpha_i$ and $\mathfrak{a}_i$, respectively, the images of $\alpha$ and $\mathfrak{a}$ under the action of $\sigma_i$.

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and let $\mathbf{N}(\mathfrak{p})$ be its norm. For any $\nu \in \mathfrak{O}$, $\nu \notin \mathfrak{p}$, the symbol $\left(\frac{\nu}{\mathfrak{p}}\right)$ is defined by $\left(\frac{\nu}{\mathfrak{p}}\right) = \zeta^j$, where $j$ is determined modulo 7 by the congruence $\zeta^j \equiv \nu^{(\mathbf{N}(\mathfrak{p})-1)/7} \bmod \mathfrak{p}$.

For every $\alpha \in \mathfrak{O}$, there is a unique sequence $\{a_n\}_{n\ge 0}$ of integers such that $0 \le a_n \le 6$ for every $n \ge 0$ and $\alpha \equiv a_0 + a_1\lambda + \cdots + a_i\lambda^i \bmod \lambda^{i+1}$ for every $i \ge 0$; as usual, we shall call $a_0 + a_1\lambda + a_2\lambda^2 + \cdots$ the *$\lambda$-adic expansion* of $\alpha$. A nonzero element $\mu \in \mathfrak{O}$ is said to be *primary* if $\mu$ is prime to $\lambda$ and there are rational integers $r$ and $s$ such that $\mu \equiv r \bmod \lambda^2$ and $\mu\overline{\mu} \equiv s \bmod 7$, where $\overline{\mu}$ is the complex conjugate of $\mu$. For any $n \in \mathbb{Z}$, let $[n]$ denote the unique integer such that $0 \le [n] \le 6$ and $[n] \equiv n \bmod 7$. If $\alpha \in \mathfrak{O}$ and $a + b\lambda + c\lambda^2 + d\lambda^3 + e\lambda^4 + \cdots$ is the $\lambda$-adic expansion of $\alpha$, it can be shown that $\alpha$ is primary if and only if $a \ne 0$, $b = c = 0$ and $e = [5d]$.

Since the quotient of two associated primary elements of $\mathfrak{O}$ is the seventh power of a unit of $\mathfrak{O}$, the following definition makes sense. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}$, prime to $\mathfrak{p}$ and to $\lambda\mathfrak{O}$; then we put

$$\left(\frac{\mathfrak{a}}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{p}}\right),$$

where $\nu$ is a primary generator of $\mathfrak{a}$. If $\alpha \in \mathfrak{O}$ is primary, we shall say that $\alpha$ is *normalized* when $\alpha \equiv 1 \bmod \lambda$. It is not difficult to prove that any nonzero ideal $\mathfrak{a}$ of $\mathfrak{O}$, prime to $\lambda\mathfrak{O}$, has a normalized primary generator.

We can now state Kummer's reciprocity law, together with its complementary laws.

THEOREM 2.1 (Kummer's general reciprocity law). *Let $\mathfrak{p}$ and $\mathfrak{q}$ be two nonzero distinct prime ideals of $\mathfrak{O}$, both different from $\lambda\mathfrak{O}$. Then*

$$\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right).$$

THEOREM 2.2 (Complementary laws). *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and let $\pi$ be a normalized primary generator of $\mathfrak{p}$ with $\lambda$-adic expansion $1 + a\lambda^3 + [5a]\lambda^4 + c\lambda^5 + d\lambda^6 + e\lambda^7 + \cdots$. Then*

$$\left(\frac{\zeta}{\mathfrak{p}}\right) = \zeta^{-a+3a^2+c+d},\ \left(\frac{\mu_1}{\mathfrak{p}}\right) = \zeta^{-2a-c},\ \left(\frac{\mu_2}{\mathfrak{p}}\right) = \zeta^{3a+3c},\ \left(\frac{\lambda}{\mathfrak{p}}\right) = \zeta^{-2a^2-e}.$$

**3. The curve $C$ and its jacobian $J$.** Let $C$ be the nonsingular model of the curve defined by the affine equation $X^7 + Y^2 + Y = 0$. Then $C$ is a hyperelliptic curve of genus 3 whose points can be identified with the

points of the affine curve $X^7 + Y^2 + Y = 0$ together with the point at infinity $(0:1:0)$, which will be denoted by $\infty$. The involution $I$ of $C$ is the automorphism of $C$ defined by

$$I(x,y) = (x, -1-y), \quad I(\infty) = \infty.$$

If we put

$$\zeta(x,y) = (\zeta x, y), \quad \zeta\infty = \infty, \tag{3.1}$$

then $\zeta$ defines an automorphism of $C$. Let us denote by $J$ the jacobian of $C$ and if $d$ is a divisor of $C$ of degree 0, let $[d]$ be its class in $J$. If $\Theta$ is the Theta divisor of $J$ corresponding to the Abel–Jacobi embedding $C \to J$ defined by $A \mapsto [A - \infty]$, then every element of $J$ outside $\Theta$ can be written in a unique way up to order as $[A + B + D - 3\infty]$ with $A, B$ and $D$ affine points of $C$ such that $B \neq I(A)$, $D \neq I(A)$ and $D \neq I(B)$, while every nonzero element of $\Theta$ can be written as $[A - \infty]$ with $A$ an affine point of $C$ or as $[A + B - 2\infty]$ with $A$ and $B$ affine points of $C$. In any case, every element of $J$ can be written as $[A + B + D - 3\infty]$ with $A$, $B$ and $D$ points of $C$.

One can easily check that for any $w = [A + B + D - 3\infty]$ in $J$, one has

$$-w = [I(A) + I(B) + I(D) - 3\infty]. \tag{3.2}$$

The jacobian $J$ is an abelian variety with complex multiplication by the ring of integers $\mathfrak{O}$ of the cyclotomic field $F$ (see [S-T]). Indeed, the automorphism of $C$ given by (3.1) induces an automorphism $[\zeta]$ of $J$ defined by

$$[\zeta][A + B + D - 3\infty] = [\zeta A + \zeta B + \zeta D - 3\infty]. \tag{3.3}$$

From (3.2), (3.3) and $\mathbb{Z}$-linearity one easily deduces the effect of any endomorphism of the form $[\alpha]$ with $\alpha \in \mathfrak{O}$ on any element of $J$.

Notice that statements similar to the above hold when one takes as base point for the Abel–Jacobi embedding a point of $J$ different from $\infty$, as we shall do below to investigate the formal group at the origin.

We remark as well that the CM-type of $J$ is $\Phi = \{\sigma_1, \sigma_2, \sigma_3\}$; then, since $(F, \Phi)$ is simple ([L]), the reflex type of $J$ is

$$\Phi' = \{\sigma_1^{-1}, \sigma_2^{-1}, \sigma_3^{-1}\} = \{\sigma_1, \sigma_4, \sigma_5\}.$$

The following proposition is not hard to prove.

PROPOSITION 3.1. *The curve $C$ and hence its jacobian $J$ both have good reduction at $\mathfrak{p}$ over $F$ for every nonzero prime ideal $\mathfrak{p}$ of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and everywhere good reduction over $K = F(\sqrt[7]{2}, \sqrt{\lambda})$.* ∎

Let us now consider the formal group of $J$ at the origin. Let $C^{(3)}$ denote the symmetric product of three copies of $C$ and write $(P_1, P_2, P_3)_{\mathrm{sym}}$ for the class of a triple $(P_1, P_2, P_3)$. The Abel–Jacobi injection $C \to J$ given by $P \mapsto [P - (0,0)]$ induces the birational equivalence $C^{(3)} \to J$ defined

by $(P_1, P_2, P_3)_{\mathrm{sym}} \mapsto [P_1 + P_2 + P_3 - 3(0,0)]$. This means that the rational functions on $J$ are simply the symmetric functions on triples of points of $C$.

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$ be three points of $C$, let $P$, $Q$ and $R$ be the rational functions on $J$ determined respectively by the symmetric polynomials $x_1 + x_2 + x_3$, $x_1x_2 + x_1x_3 + x_2x_3$ and $x_1x_2x_3$, and let $\hat{\mathfrak{O}}_{J,0}$ denote the completion of the local ring of $J$ at the origin. Then there is an isomorphism of $F$-algebras

$$\hat{\mathfrak{O}}_{J,0} \simeq F[[P, Q, R]].$$

The formal group of $J$ at the origin is the translation, via this isomorphism, of the mapping induced by the group law $J \times J \to J$ which maps $(z, w)$ to $z+w$. The computation, with *Mathematica*, of the first terms of the expansions of $P(z+w)$, $Q(z+w)$ and $R(z+w)$ in $F[[P(z), Q(z), R(z), P(w), Q(w), R(w)]]$, though tedious, massive and quite involved, is not seriously difficult. We write them in the next proposition, in which, to simplify notation, we have set $P(z) = P_1$, $P(w) = P_2$, $Q(z) = Q_1$, $Q(w) = Q_2$, $R(z) = R_1$ and $R(w) = R_2$.

PROPOSITION 3.2. *The formal group of $J$ at the origin with respect to the system of parameters $P$, $Q$ and $R$ has coefficients in $\mathbb{Z}$. Moreover, the first terms of the expansions for $P(z+w)$, $Q(z+w)$ and $R(z+w)$ are the following:*

$$\begin{aligned}
&P(z+w)\\
&= P_1 + P_2 + 2(R_1^2Q_2 + Q_1R_1^2) + 4(Q_1R_1R_2 + Q_2R_1R_2)\\
&\quad - 3(Q_1^2Q_2^2 + P_2^2R_1^2 + P_1^2R_2^2) - 2(Q_1^3Q_2 + Q_1Q_2^3) - 4(P_1P_2R_1^2 + P_1P_2R_2^2)\\
&\quad - 8(P_1Q_1Q_2R_1 + P_2Q_1Q_2R_1 + P_1Q_1Q_2R_2 + P_2Q_1Q_2R_2 + P_1P_2R_1R_2)\\
&\quad - 2(P_2Q_1^2R_1 + P_1Q_2^2R_1 + P^2Q_1^2R_2 + P_1Q_2^2R_2) - 6(P_2Q_2^2R_1 + P_1Q_1^2R_2\\
&\quad + P_1^2R_1R_2 + P_2^2R_1R_2) + 2(P_2^2Q_1^2Q_2 + P_1^2Q_1Q_2^2) + 6(P_1^2Q_1^2Q_2 + P_2^2Q_1Q_2^2)\\
&\quad + 8(P_2^3Q_2R_1 + P_1^3Q_1R_2) + 2(P_2^3Q_1R_1 + P_1^3Q_2R_1 + P_2^3Q_1R_2 + P_1^3Q_2R_2)\\
&\quad + 4(P_1P_2Q_1^2Q_2 + P_1P_2Q_1Q_2^2 + P_1P_2^2Q_1R_1 + P_1^2P_2Q_2R_1 + P_1P_2^2Q_1R_2\\
&\quad + P_1^2P_2Q_2R_2) + 6(P_1^2P_2Q_1R_1 + P_1P_2^2Q_2R_1 + P_1^2P_2Q_1R_2 + P_1P_2^2Q_2R_2)\\
&\qquad\qquad + 4(R_1^3R_2^2 + R_1^2R_2^3) + 2(R_1^4R_2 + R_1R_2^4) + \cdots,\\
&Q(z+w)\\
&\quad = Q_1 + Q_2 + P_1P_2 + 2(R_1^2R_2 + R_2^2R_1) - 2(Q_1^3R_2 + Q_2^3R_1) - 6(Q_1^2Q_2R_1\\
&\qquad + Q_1Q_2^2R_1 + Q_1^2Q_2R_2 + Q_1Q_2^2R_2) - 4(P_2Q_1R_1R_2 + P_1Q_2R_1R_2)\\
&\qquad - 8(P_1Q_1R_1R_2 + P_2Q_2R_1R_2) - 2(P_1Q_2R_1^2 + P_2Q_1R_2^2) - 4(P_2Q_1R_1^2\\
&\qquad + P_2Q_2R_1^2 + P_1Q_1R_2^2 + P_1Q_2R_2^2) + 3(P_1Q_1^2Q_2^2 + P_2Q_1^2Q_2^2)
\end{aligned}$$

$$+ 4(P_1Q_1^3Q_2 + P_2Q_1Q_2^3) - (P_1P_2^2R_1^2 + P_1^2P_2R_2^2) + (P_2^3R_1^2 + P_1^3R_2^2)$$
$$+ 6(P_2^2Q_2^2R_1 + P_1^2Q_1^2R_2) + 4(P_1P_2Q_1^2R_1 + P_1^2Q_1Q_2R_1 + P_2^2Q_1Q_2R_1$$
$$+ P_1^2Q_1Q_2R_2 + P_2^2Q_1Q_2R_2 + P_1P_2Q_2^2R_2) - 2(P_1P_2Q_2^2R_1 + P_1P_2Q_1^2R_2$$
$$+ P_1^2P_2R_1R_2 + P_1P_2^2R_1R_2) + 2(P_1^3R_1R_2 + P_2^3R_1R_2)$$
$$+ 2(P_1^2P_2R_1^2 + P_1P_2^2R_2^2) + \cdots,$$

$$R(z+w)$$
$$= R_1 + R_2 + P_1Q_2 + Q_1P_2 - 2(R_1^3P_2 + P_1R_2^3) - (R_1^2Q_2^2 + Q_1^2R_2^2)$$
$$- 4(Q_1R_1^2Q_2 + P_1R_1^2R_2 + R_1^2P_2R_2 + P_1R_1R_2^2 + R_1P_2R_2^2 + Q_1Q_2R_2^2)$$
$$- 2(Q_1^2R_1R_2 + R_1Q_2^2R_2) - 4Q_1R_1Q_2R_2 + 4(P_1Q_1R_1^2P_2 + P_1Q_1^2R_1Q_2$$
$$+ Q_1P_2Q_2^2R_2 + P_1P_2Q_2R_2^2) - 4(Q_1^2R_1P_2Q_2 + P_1Q_1R_1Q_2^2 + Q_1^2P_2Q_2R_2$$
$$+ P_1Q_1Q_2^2R_2) - (Q_1R_1^2P_2^2 + P_1^2Q_2R_2^2) + 2(P_1^2R_1^2Q_2 + Q_1P_2^2R_2^2)$$
$$- 2(Q_1R_1P_2Q_2^2 + Q_1R_1R_2P_2^2 + P_1Q_2R_2Q_1^2 + P_1^2R_1Q_2R_2)$$
$$+ 3(R_1^2P_2^2Q_2 + P_1^2Q_1R_2^2) - (Q_1^3Q_2^2 + Q_1^2Q_2^3) - 2(P_1R_1Q_2^3 + P_2R_2Q_1^3)$$
$$+ 6(P_1^2Q_1R_1R_2 + P_2^2R_1Q_2R_2) + \cdots,$$

*where the dots mean terms of total degree* $\geq 6$. ∎

Since $\mathfrak{O} = \mathbb{Z}[\zeta]$, repeated application of Proposition 3.2 together with the fact that $P([\zeta]z) = \zeta P(z)$, $Q([\zeta]z) = \zeta^2 Q(z)$ and $R([\zeta]z) = \zeta^3 R(z)$, yields explicitly the first terms of the action of any $\alpha \in \mathfrak{O}$ on the formal group. Namely, one gets the following proposition, in which, to simplify notation, $P(z)$, $Q(z)$ and $R(z)$ are denoted $P$, $Q$ and $R$, respectively.

PROPOSITION 3.3. *Let* $\alpha \in \mathfrak{O}$. *Then:*

(1) *The coefficients of the monomials of total degree* $\leq 5$ *in the expansion of* $P([\alpha]z)$ *are zero, except perhaps the coefficients of* $P$, $QR^2$, $Q^4$, $P^2R^2$, $PQ^2R$, $P^2Q^3$, $P^3QR$ *and* $R^5$. *Moreover, the coefficients of* $P$, $QR^2$, $Q^4$ *and* $R^5$ *are* $\alpha$, $2(\alpha_2\alpha_3^2 - \alpha)$, $-\frac{1}{2}(\alpha_2^4 - \alpha)$ *and* $\frac{2}{5}(\alpha_3^5 - \alpha)$, *respectively.*

(2) *The coefficients of the monomials of total degree* $\leq 4$ *in the expansion of* $Q([\alpha]z)$ *are zero, except perhaps the coefficients of* $Q$, $P^2$, $R^3$, $Q^3R$ *and* $PQR^2$. *Moreover the coefficients of* $Q$ *and* $R^3$ *are* $\alpha_2$ *and* $\frac{2}{3}(\alpha_3^3 - \alpha_2)$, *respectively.*

(3) *The homogeneous linear part of the expansion of* $R([\alpha]z)$ *is* $\alpha_3 R$. ∎

Next we shall describe some facts related to Frobenius endomorphisms. For any $\alpha \in \mathfrak{O}$, let $J[\alpha]$ denote the kernel of the endomorphism $[\alpha]$ of $J$ and, for any ideal $\mathfrak{a}$ of $\mathfrak{O}$, put $J[\mathfrak{a}] = \bigcap_{\alpha\in\mathfrak{a}} J[\alpha]$.

PROPOSITION 3.4. *Let* $\mathfrak{p}$ *be a nonzero prime ideal of* $\mathfrak{O}$, *different from* $\lambda\mathfrak{O}$, *let* $\pi$ *be a generator of* $\mathfrak{p}$ *such that* $\pi \equiv 1 \bmod \lambda^3$ *and let* $\tilde{J}$ *be the*

*reduction of $J$ modulo $\mathfrak{p}$. Then the Frobenius endomorphism of $\tilde{J}$ is the reduction modulo $\mathfrak{p}$ of the endomorphism $[\pi\pi_4\pi_5]$ of $J$.*

*Proof.* There is a unique $\alpha \in \mathfrak{O}$ such that the Frobenius endomorphism $\mathrm{Fr}_\mathfrak{p}$ of $\tilde{J}$ is the reduction modulo $\mathfrak{p}$ of the endomorphism $[\alpha]$. Moreover, since the reflex type of $J$ is $\Phi' = \{\sigma_1, \sigma_4, \sigma_5\}$, we can assert that there is a unit $u$ of $\mathfrak{O}$ such that $\alpha = u\pi\pi_4\pi_5$ and in fact $u$ is a root of unity of $\mathfrak{O}$ (see [L] or [S-T]). Since $\pi\pi_4\pi_5 \equiv 1 \bmod \lambda^3$, in order to prove that $u = 1$, it is enough to show that $\alpha \equiv 1 \bmod \lambda^3$. The first assertion of Proposition 3.1 and the fact that $J[\lambda^3]$ is rational over $F$ (see [Gr]) imply that $7^3$ divides the cardinality of $\tilde{J}(\mathfrak{O}/\mathfrak{p})$. But it is known that

$$\mathrm{Card}(\tilde{J}(\mathfrak{O}/\mathfrak{p})) = \deg(1 - \mathrm{Fr}_\mathfrak{p}) = \mathbf{N}(1 - \alpha).$$

Hence $7^3$ divides $\mathbf{N}(1-\alpha)$ and therefore $\alpha \equiv 1 \bmod \lambda^3$. ∎

It follows from Hecke's theorem ([C, Theorem 10.2.9]) that $\lambda\mathfrak{O}$ is totally ramified in $K = F(\sqrt[7]{2}, \sqrt{\lambda})$. Let $\Lambda$ be the only prime ideal of the ring of integers of $K$ lying above $\lambda\mathfrak{O}$ and let $\hat{J}$ denote the reduction of $J$ modulo $\Lambda$. Let $\sqrt{-7}$ denote the square root of $-7$ with imaginary part $> 0$, that is, $\sqrt{-7} = \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6$. In the next proposition we give a description of the Frobenius endomorphism of $\hat{J}$ that will be used in Section 5.

Proposition 3.5. *Let $\hat{J}$ be the reduction of $J$ modulo $\Lambda$. Then the Frobenius endomorphism of $\hat{J}$ is the reduction modulo $\Lambda$ either of the endomorphism $[\sqrt{-7}]$ or of the endomorphism $[-\sqrt{-7}]$ of $J$.*

*Proof.* We make an extensive use of [L, Chapter 4] and the notation thereof. There is a unique $\alpha \in \mathfrak{O}$ such that the Frobenius endomorphism $\mathrm{Fr}_\Lambda$ of $\hat{J}$ is the reduction modulo $\Lambda$ of the endomorphism $[\alpha]$. Moreover $(\alpha) = N_{\Gamma'}(\Lambda)$, where $\Gamma'$ is an extension to $K$ of the reflex type $\Phi'$ of $J$ over $F$. Since

$$N_{\Gamma'}(\Lambda) = N_{\Phi'} \circ N_{K/F}(\Lambda)$$

and $\Lambda$ is totally ramified in $K/F$, it follows that

$$(\alpha) = N_{\Phi'}((\lambda)) = (\lambda\lambda_4\lambda_5).$$

One also knows that $|\alpha| = \sqrt{\mathbf{N}(\lambda)} = \sqrt{7}$ for any archimedean absolute value on $F$; therefore $\alpha = u\lambda\lambda_4\lambda_5$, where $u = \pm\zeta^j$ for some $j$, $0 \le j \le 6$. Hence

$$\alpha = \pm\zeta^j(1-\zeta)(1-\zeta^4)(1-\zeta^5) = \pm\zeta^{j-2}\sqrt{-7}.$$

It is not difficult to prove that all 2-torsion points of $J$ are rational over $K$. This fact, together with the fact that $\mathrm{Card}(\hat{J}[2]) = \mathrm{Card}(J[2]) = 2^6$, implies that $2^6$ divides $\mathrm{Card}(\hat{J})$. Since $\mathrm{Card}(\hat{J}) = \deg(1 - \mathrm{Fr}_\Lambda) = \mathbf{N}(1-\alpha)$, it follows that $2^6$ divides $\mathbf{N}(1-\alpha)$. Let $\epsilon = \zeta + \zeta^2 + \zeta^4$; then $2 = \epsilon\bar{\epsilon}$. Thus $\epsilon^6$ divides $\mathbf{N}(1-\alpha)$ and therefore $\alpha \equiv \pm 1 \bmod \epsilon$. This implies, taking into account the equality $\sqrt{-7} = 2\epsilon + 1$, that $j = 2$. ∎

In what follows we shall prove some further properties of $J$ that will be needed later. For any ideal $\mathfrak{a}$ of $\mathfrak{O}$, let $F(J[\mathfrak{a}])$ denote the extension of $F$ generated by the coordinates of the points of $J[\mathfrak{a}]$.

PROPOSITION 3.6. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$. Any nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, $\mathfrak{p}$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$, is unramified in the extension $F \subseteq F(J[\mathfrak{p}])$.*

*Proof.* For the sake of simplicity, write $E$ instead of $F(J[\mathfrak{p}])$. Since $J$ has complex multiplication by $\mathfrak{O}$, the extension $F \subseteq E$ is abelian and $E = F(z)$ for any primitive $\mathfrak{p}$-torsion point $z$ of $J$. Let $\mathfrak{q}$ be a nonzero prime ideal of $\mathfrak{O}$ different from $\lambda\mathfrak{O}$, $\mathfrak{p}$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$, and let $\mathfrak{Q}$ be a prime ideal of the ring of integers of $E$ lying above $\mathfrak{q}$. Denote by $\hat{E}_{\mathfrak{Q}}$ the completion of $E$ with respect to $\mathfrak{Q}$ and by $J_{\hat{E}_{\mathfrak{Q}}}$ the jacobian of $C$ over $\hat{E}_{\mathfrak{Q}}$; then, invoking the first claim of Proposition 3.1, for any $\sigma$ in the inertia group of $\mathfrak{Q}$, $z^\sigma - z$ can be viewed as an element of $J_{\hat{E}_{\mathfrak{Q}}}$ contained in the kernel $N$ of the reduction morphism $J_{\hat{E}_{\mathfrak{Q}}} \to J_{\mathbb{F}_q}$, where $J_{\mathbb{F}_q}$ is the reduced jacobian over the residue field $\mathbb{F}_q$ of the local field $\hat{E}_{\mathfrak{Q}}$. If $\pi$ is a generator of $\mathfrak{p}$, obviously $\pi$, $\pi_2$ and $\pi_3$ are units in $\hat{E}_{\mathfrak{Q}}$; hence $\pi$ induces an isomorphism on the maximal ideal $M_{\mathfrak{Q}}$ of $\hat{E}_{\mathfrak{Q}}$ endowed with the group structure given by the formal group of $J$ at the origin with respect to the parameters $P$, $Q$ and $R$. Since $M_{\mathfrak{Q}}$ is isomorphic to $N$ (see [H-S]), we deduce that there is no nontrivial $\mathfrak{p}$-torsion element in $N$. Therefore $z^\sigma - z = 0$ and the proposition follows. ∎

Invoking the second claim of Proposition 3.1, one obtains quite similarly the following result.

PROPOSITION 3.7. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and let $\Lambda$ be the unique prime ideal of the ring of integers of $K = F(\sqrt[7]{2}, \sqrt{\lambda})$ lying above $\lambda\mathfrak{O}$. Then $\Lambda$ is unramified in the extension $K \subseteq K(J[\mathfrak{p}])$.* ∎

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and write as before $E$ to denote $F(J[\mathfrak{p}])$. Let $\mathfrak{P}$ be a prime ideal of the ring of integers of $E$ lying above $\mathfrak{p}$, let $\hat{E}_{\mathfrak{P}}$ be the completion of $E$ at $\mathfrak{P}$, and let $\mathbb{F}_q$ be its residue field, so that we have the reduction morphism

$$\varphi\colon J_{\hat{E}_{\mathfrak{P}}} \to J_{\mathbb{F}_q}.$$

For every $\alpha \in \mathfrak{O}$, let $\widetilde{[\alpha]}$ denote the endomorphism of $J_{\mathbb{F}_q}$ induced by $[\alpha]$.

PROPOSITION 3.8. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$ and of degree one or two. Then $J[\mathfrak{p}]$ is contained in the kernel of the reduction morphism $\varphi$ defined above.*

*Proof.* Let $\pi$ be a generator of $\mathfrak{p}$ such that $\pi \equiv 1 \bmod \lambda^3$. It follows from Proposition 3.4 that the Frobenius endomorphism of $J_{\mathbb{F}_q}$ is just $\widetilde{[\pi\pi_4\pi_5]}$,

which coincides with the composition $\widetilde{[\pi]}\circ\widetilde{[\pi_4]}\circ\widetilde{[\pi_5]}$. But the degree of $\mathfrak{p}$ being one or two, $\pi_4$ and $\pi_5$ are both units modulo $\mathfrak{p}$, and this implies that $\widetilde{[\pi_4]}$ and $\widetilde{[\pi_5]}$ are both automorphisms of $J_{\mathbb{F}_q}$. Since the Frobenius endomorphism of $J_{\mathbb{F}_q}$ is purely inseparable, $\widetilde{[\pi]}$ is also purely inseparable and this implies that $J[\mathfrak{p}]$ is indeed contained in the kernel of the reduction morphism $\varphi$. ∎

**4. The number $A(\mathfrak{p})$ and the general law.** Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$ and of degree one or two, and let $J[\mathfrak{p}]' = J[\mathfrak{p}] - \{0\}$. It can be shown (see [A] or [G3]) that the rational functions $P$, $Q$ and $R$ are defined at every point of $J[\mathfrak{p}]'$, so that in particular we can consider the algebraic number $A(\mathfrak{p})$ defined as follows:

$$A(\mathfrak{p}) = \prod_{z\in J[\mathfrak{p}]'} P(z). \tag{4.1}$$

First of all, it is easily seen that the Galois group of the algebraic closure of $\mathbb{Q}$ over $F$ fixes $A(\mathfrak{p})$ and hence $A(\mathfrak{p}) \in F$. Our proof of Kummer's reciprocity law relies essentially on the prime factorization, up to seventh powers, of the number $A(\mathfrak{p})$ in the cyclotomic field $F$.

PROPOSITION 4.1. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$ and of degree one or two. Then* $\operatorname{ord}_{\mathfrak{p}}(A(\mathfrak{p})) = 1$, $\operatorname{ord}_{\mathfrak{p}_2}(A(\mathfrak{p})) = 4$ *and* $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p})) \equiv 5 \bmod 7$.

*Proof.* Write as before $E$ to denote $F(J[\mathfrak{p}])$. Let $\mathfrak{P}$ be a prime ideal of the ring of integers of $E$ lying above $\mathfrak{p}$, let $\hat{E}_{\mathfrak{P}}$ be the completion of $E$ at $\mathfrak{P}$, and let $M_{\mathfrak{P}}$ be the corresponding maximal ideal. Let $\pi$ be a generator of $\mathfrak{p}$ such that $\pi \equiv 1 \bmod \lambda^3$. From Proposition 3.8 it follows that the homomorphism of $\mathfrak{O}$-modules

$$\psi\colon J[\mathfrak{p}] \to M_{\mathfrak{P}} \times M_{\mathfrak{P}} \times M_{\mathfrak{P}}$$

defined by $z \mapsto (P(z), Q(z), R(z))$ identifies $J[\mathfrak{p}]$ with a submodule of the kernel of the endomorphism induced by $[\pi]$ in the formal group. Therefore, for every $z \in J[\mathfrak{p}]$, one has

$$[\pi](P(z), Q(z), R(z)) = (0, 0, 0). \tag{4.2}$$

Hence from Proposition 3.3 we get

$$0 = \pi P(z) + \cdots, \quad 0 = \pi_2 Q(z) + \cdots, \quad 0 = \pi_3 R(z) + \cdots \tag{4.3}$$

where the dots mean terms of total degree $\geq 2$. Since $\pi_2$ and $\pi_3$ are units in the completion $\hat{\mathfrak{O}}_{\mathfrak{p}}$ of $\mathfrak{O}$ at $\mathfrak{p}$, we can express $Q(z)$ and $R(z)$ as power series in $\hat{\mathfrak{O}}_{\mathfrak{p}}[[P(z)]]$. Again from Proposition 3.3 one has

$$P([\pi\pi_4\pi_5]z) = \pi\pi_4\pi_5 P(z) + \cdots \tag{4.4}$$

where the dots mean terms of total degree $\geq 2$. Since, by Proposition 3.4, $[\pi\pi_4\pi_5]$ induces the Frobenius endomorphism modulo $\mathfrak{p}$, replacing $Q(z)$ and $R(z)$ by their corresponding series expansions in $P(z)$, we obtain a power series $H(P(z))$ in $\hat{\mathfrak{O}}_{\mathfrak{p}}[[P(z)]]$ such that

$$H(P(z)) \equiv P(z)^{\mathbf{N}(\mathfrak{p})} \bmod \mathfrak{p}\hat{\mathfrak{O}}_{\mathfrak{p}}$$

and such that $H(P(z)) = 0$, because (4.2) ensures that $P([\pi\pi_4\pi_5]z) = 0$. Applying the Weierstrass preparation theorem one obtains

$$H(P(z)) = S(P(z))u(P(z))$$

with

$$S(P(z)) = a_1P(z) + a_2P(z)^2 + \cdots + a_{\mathbf{N}(\mathfrak{p})}P(z)^{\mathbf{N}(\mathfrak{p})}$$

where $a_1 = \pi\pi_4\pi_5$, $a_i \equiv 0 \bmod \mathfrak{p}\hat{\mathfrak{O}}_{\mathfrak{p}}$ $(1 \leq i \leq \mathbf{N}(\mathfrak{p}) - 1)$ and $a_{\mathbf{N}(\mathfrak{p})} \equiv 1 \bmod \mathfrak{p}\hat{\mathfrak{O}}_{\mathfrak{p}}$. Notice that the roots of the polynomial $S(X)/X$ are exactly the numbers $P(z)$ when $z$ runs through $J[\mathfrak{p}]'$. Therefore

$$A(\mathfrak{p}) = \frac{\pi\pi_4\pi_5}{a_{\mathbf{N}(\mathfrak{p})}}.$$

But $\pi_4$ and $\pi_5$ are units in $\mathfrak{O}_{\mathfrak{p}}$ and since $a_{\mathbf{N}(\mathfrak{p})} \equiv 1 \bmod \mathfrak{p}\hat{\mathfrak{O}}_{\mathfrak{p}}$, $a_{\mathbf{N}(\mathfrak{p})}$ is also a unit in $\hat{\mathfrak{O}}_{\mathfrak{p}}$, hence indeed $\mathrm{ord}_{\mathfrak{p}}(A(\mathfrak{p})) = 1$.

In order to compute $\mathrm{ord}_{\mathfrak{p}_2}(A(\mathfrak{p}))$ we slightly modify the above argument. Consider the equalities (4.3) in the completion $\hat{\mathfrak{O}}_{\mathfrak{p}_2}$ of $\mathfrak{O}$ at $\mathfrak{p}_2$; now $\pi$ and $\pi_3$ are units in $\hat{\mathfrak{O}}_{\mathfrak{p}_2}$, so that $P(z)$ and $R(z)$ can be written as power series of $\hat{\mathfrak{O}}_{\mathfrak{p}_2}[[Q(z)]]$. Substituting these series in

$$Q([\pi\pi_2\pi_3]z) = \pi_2\pi_4\pi_6Q(z) + \cdots$$

one obtains a power series $I(Q(z))$ in $\hat{\mathfrak{O}}_{\mathfrak{p}_2}[[Q(z)]]$ such that $I(Q(z)) = 0$ and

$$I(Q(z)) = \pi_2\pi_4\pi_6Q(z) + \cdots$$

where the dots mean terms of total degree $\geq 2$. Since $[\pi\pi_2\pi_3]$ induces the Frobenius endomorphism modulo $\mathfrak{p}_2$ we obtain as before

$$I(Q(z)) = T(Q(z))v(Q(z)) \quad \text{with} \quad T(Q(z)) = b_1Q(z) + \cdots + b_{\mathbf{N}(\mathfrak{p})}Q(z)^{\mathbf{N}(\mathfrak{p})},$$

where $b_1 = \pi_2\pi_4\pi_6$, $b_i \equiv 0 \bmod \mathfrak{p}_2\hat{\mathfrak{O}}_{\mathfrak{p}_2}$ $(1 \leq i \leq \mathbf{N}(\mathfrak{p}) - 1)$ and $b_{\mathbf{N}(\mathfrak{p})} \equiv 1 \bmod \mathfrak{p}_2\hat{\mathfrak{O}}_{\mathfrak{p}_2}$. The roots of the polynomial $T(X)$ are the numbers $Q(z)$ with $z$ running through $J[\mathfrak{p}]$, and $T(X)/X$ is an Eisenstein polynomial of degree $\mathbf{N}(\mathfrak{p}) - 1$. Therefore $F_{\mathfrak{p}_2} \subseteq F_{\mathfrak{p}_2}(J[\mathfrak{p}])$ is a totally ramified extension and $Q(z)$ is for any $z \in J[\mathfrak{p}]$ a uniformizing parameter of $F_{\mathfrak{p}_2}(J[\mathfrak{p}])$. Since the power series obtained above for $P(z)$ in terms of $Q(z)$ is given by

$$P(z) = \frac{1}{2\pi}(\pi_2^4 - \pi)Q(z)^4 + \cdots$$

where the dots mean terms of total degree $\geq 5$, it follows that $\operatorname{ord}_{\mathfrak{m}_2}(P(z)) = 4$ for any $z \in J[\mathfrak{p}]'$, where $\mathfrak{m}_2$ is the maximal ideal in $F_{\mathfrak{p}_2}(J[\mathfrak{p}])$. Therefore

$$\operatorname{ord}_{\mathfrak{m}_2}(A(\mathfrak{p})) = \operatorname{ord}_{\mathfrak{m}_2}\Big(\prod_{z\in J[\mathfrak{p}]'} P(z)\Big) = \sum_{z\in J[\mathfrak{p}]'} \operatorname{ord}_{\mathfrak{m}_2}(P(z)) = 4(\mathbf{N}(\mathfrak{p})-1)$$

and this implies indeed that $\operatorname{ord}_{\mathfrak{p}_2}(A(\mathfrak{p})) = 4$.

Finally, in order to compute $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p}))$ we consider the equalities (4.3) in the completion $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$ of $\mathfrak{O}$ at $\mathfrak{p}_3$; now $\pi$ and $\pi_2$ are units in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$, so that $P(z)$ and $Q(z)$ can be written as power series in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}[[R(z)]]$. The power series for $P(z)$ is

$$P(z) = \frac{2}{15\pi\pi_2}(7\pi_2\pi_3^5 - 13\pi\pi_2 + 10\pi_2^2\pi_3^2 + 10\pi\pi_3^3)R(z)^5 + \cdots \tag{4.5}$$

where the dots mean terms of total degree $\geq 6$. Since 3 and 5 are inert in $\mathfrak{O}$, and the prime ideals of $\mathfrak{O}$ lying over 2 are of degree three while $\mathfrak{p}_3$ is of degree one or two, it follows that $\mathfrak{p}_3$ is prime to 2, 3 and 5. Hence 2, 3 and 5 are units in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$.

Now, if 13 is a unit in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$, it is easy to check that the coefficient of $R(z)^5$ in (4.5) is a unit in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$; therefore the order of $P(z)$ in $F_{\mathfrak{p}_3}(J[\mathfrak{p}])$ is 5. Arguing as in the previous case one gets $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p})) = 5$.

If 13 is not a unit in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$, since 13 is a product of three prime ideals in $\mathfrak{O}$, necessarily $\mathfrak{p}_3$ is one of them and consequently $\mathbf{N}(\mathfrak{p}_3) = 13^2$. In this case the order of the coefficient of $R(z)^5$ in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$ is 1; thus, its order in $F_{\mathfrak{p}_3}(J[\mathfrak{p}])$ is $\mathbf{N}(\mathfrak{p}_3) - 1 = 13^2 - 1 = 168$. Since $R(z)$ is a uniformizer in $F_{\mathfrak{p}_3}(J[\mathfrak{p}])$, it follows that the order of $P(z)$ in $F_{\mathfrak{p}_3}(J[\mathfrak{p}])$ is $168 + 5 = 173$. Let $\mathfrak{m}_3$ denote the maximal ideal of $F_{\mathfrak{p}_3}(J[\mathfrak{p}])$. Then

$$\operatorname{ord}_{\mathfrak{m}_3}(A(\mathfrak{p})) = \operatorname{ord}_{\mathfrak{m}_3}\Big(\prod_{z\in J[\mathfrak{p}]'} P(z)\Big) = \sum_{z\in J[\mathfrak{p}]'} \operatorname{ord}_{\mathfrak{m}_3}(P(z)) = 173\cdot 168.$$

Since $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p})) = \operatorname{ord}_{\mathfrak{m}_3}(A(\mathfrak{p}))/168$, we get $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p})) = 173$. In any case, whether 13 is a unit in $\hat{\mathfrak{O}}_{\mathfrak{p}_3}$ or not, $\operatorname{ord}_{\mathfrak{p}_3}(A(\mathfrak{p})) \equiv 5 \bmod 7$ as announced. ∎

PROPOSITION 4.2. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$ and of degree one or two, let $\pi$ be a primary normalized generator of $\mathfrak{p}$ with $\lambda$-adic expansion $1 + a\lambda^3 + [5a]\lambda^4 + c\lambda^5 + d\lambda^6 + \cdots$, and let $m = [-2a - a^2 + 2c + 2d]$. Then:*

(a) *The extension $F \subseteq F(\sqrt[7]{2^m A(\mathfrak{p})})$ has degree seven and is unramified at $\lambda\mathfrak{O}$.*
(b) *There exists $D(\mathfrak{p}) \in F^*$ such that $A(\mathfrak{p}) = \pi\pi_2^4\pi_3^5 D(\mathfrak{p})^7$.*

*Proof.* Let $M$ be a 7-section of $J[\mathfrak{p}]'$, that is, a subset $M$ of $J[\mathfrak{p}]'$ with $(\mathbf{N}(\mathfrak{p})-1)/7$ elements such that

$$J[\mathfrak{p}]' = M \cup \zeta M \cup \cdots \cup \zeta^6 M.$$

We define

$$B(\mathfrak{p}) = \prod_{z \in M} P(z). \tag{4.6}$$

Of course, $B(\mathfrak{p})$ depends also on $M$, but for the sake of simplicity let us forget this in the notation. Clearly $B(\mathfrak{p}) \in F(J[\mathfrak{p}])$ and $B(\mathfrak{p})^7 = A(\mathfrak{p})$; hence $F(\sqrt[7]{A(\mathfrak{p})}) \subseteq F(J[\mathfrak{p}])$. It follows from Proposition 3.6 that $F \subseteq F(\sqrt[7]{A(\mathfrak{p})})$ is a Kummer extension of degree 7 ramified, at most, at the primes $\lambda\mathfrak{O}$, $\mathfrak{p}$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$. Thus, by Hecke's theorem ([C, Theorem 10.2.9]), there is a unit $u$ in $\mathfrak{O}$, an element $D(\mathfrak{p}) \neq 0$ in $F$ and an integer $l \geq 0$ such that

$$A(\mathfrak{p}) = u\lambda^l \pi \pi_2^4 \pi_3^5 D(\mathfrak{p})^7.$$

Furthermore, there are integers $i$, $j$ and $k$ such that $u = \pm\zeta^i \mu_1^j \mu_2^k$; hence

$$A(\mathfrak{p}) = \pm\zeta^i \mu_1^j \mu_2^k \lambda^l \pi \pi_2^4 \pi_3^5 D(\mathfrak{p})^7. \tag{4.7}$$

Consider the following diagram of fields and field extensions:

$$\begin{array}{ccccc}
F(\sqrt[7]{2}, \sqrt{\lambda}) & \xrightarrow{7} & F(\sqrt[7]{2}, \sqrt{\lambda}, B(\mathfrak{p})) & \longrightarrow & F(\sqrt[7]{2}, \sqrt{\lambda}, J[\mathfrak{p}]) \\
\uparrow 2 & & \uparrow & & \uparrow \\
F(\sqrt[7]{2}) & \xrightarrow{7} & F(\sqrt[7]{2}, B(\mathfrak{p})) & \longrightarrow & F(\sqrt[7]{2}, J[\mathfrak{p}]) \\
\uparrow 7 & & \uparrow & & \uparrow \\
F & \xrightarrow{7} & F(B(\mathfrak{p})) & \longrightarrow & F(J[\mathfrak{p}])
\end{array}$$

The prime $\lambda\mathfrak{O}$ is totally ramified in the extension $F \subseteq F(\sqrt[7]{2}, \sqrt{\lambda})$; let $\Lambda$ be the lone prime of $F(\sqrt[7]{2}, \sqrt{\lambda})$ lying above $\lambda\mathfrak{O}$. It follows from Proposition 3.7 that $\Lambda$ is unramified in $F(\sqrt[7]{2}, \sqrt{\lambda}) \subseteq F(\sqrt[7]{2}, \sqrt{\lambda}, B(\mathfrak{p}))$. Let $\mathcal{L}$ denote the prime of $F(\sqrt[7]{2})$ lying above $\lambda\mathfrak{O}$; then the ramification index of $\mathcal{L}$ in $F(\sqrt[7]{2}) \subseteq F(\sqrt[7]{2}, \sqrt{\lambda}, B(\mathfrak{p}))$ is 2. Therefore the ramification index of $\lambda\mathfrak{O}$ in $F \subseteq F(\sqrt[7]{2}, B(\mathfrak{p}))$ is 7.

Let $L$ be the inertia field of $\lambda\mathfrak{O}$ in $F \subseteq F(\sqrt[7]{2}, B(\mathfrak{p}))$; then $L$ is a cyclic extension of $F$ of degree 7 and $\lambda\mathfrak{O}$ is unramified in $F \subseteq L$. By elementary Galois theory, there exists a nonnegative integer $n$ such that

$$L = F(\sqrt[7]{2^n A(\mathfrak{p})}).$$

It then follows from (4.7) and Hecke's theorem that $l \equiv 0 \bmod 7$ and that there exists $x \in F$ such that

$$x^7 \equiv 2^n \zeta^i \mu_1^j \mu_2^k \pi \pi_2^4 \pi_3^5 \bmod \lambda^7. \tag{4.8}$$

Looking at the $\lambda$-adic expansions one deduces that

$$2^n\zeta^i\mu_1^j\mu_2^k\pi\pi_2^4\pi_3^5 \equiv 2^{n+j+k} \bmod \lambda. \tag{4.9}$$

Making in (4.8) the change of variables $x = z + 2^{n+j+k}$ and using (4.9) one concludes that $\lambda^7$ divides $2^{7(n+j+k)} - 2^m\zeta^i\mu_1^j\mu_2^k\pi\pi_2^4\pi_3^5$. From this fact and after some elementary manipulations with the $\lambda$-adic expansions, one finds easily that $i \equiv j \equiv k \equiv 0 \bmod 7$, which proves (b), and also that

$$n \equiv -2a - a^2 + 2c + 2d \bmod 7,$$

which proves (a). ∎

The proof of the following generalized Gauss lemma is quite straightforward (see for example [K2] or [Le]).

LEMMA 4.3. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, $\alpha$ an element of $\mathfrak{O}$ outside $\mathfrak{p}$, and $M$ a 7-section of $J[\mathfrak{p}]'$. Then*

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \frac{\prod_{z\in M} P([\alpha]z)}{\prod_{z\in M} P(z)}. \ \blacksquare$$

THEOREM 4.4. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be nonzero prime ideals of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$ and such that $\mathfrak{p}$ is of degree one or two and different from $\mathfrak{q}$, $\mathfrak{q}_2$ and $\mathfrak{q}_3$. Then*

$$\left(\frac{\mathfrak{q}\mathfrak{q}_2\mathfrak{q}_3}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}\mathfrak{q}_2\mathfrak{q}_3}\right).$$

*Proof.* Let $\pi$ be a primary normalized generator of $\mathfrak{p}$, $B(\mathfrak{p})$ and $D(\mathfrak{p})$ the numbers appearing in Proposition 4.2, and $\mathrm{Fr}_{\mathfrak{q}_2}$ the Frobenius automorphism of $\mathfrak{q}_2$ in the abelian extension $F \subseteq F(J[\mathfrak{p}])$. The definition of the symbol, Proposition 4.2(b) and the fact that $D(\mathfrak{p}) \in F$ give rise to the equalities

$$\left(\frac{\mathfrak{p}\mathfrak{p}_2^4\mathfrak{p}_3^5}{\mathfrak{q}_2}\right) = \left(\frac{\pi\pi_2^4\pi_3^5}{\mathfrak{q}_2}\right) = \frac{(B(\mathfrak{p})/D(\mathfrak{p}))^{\mathrm{Fr}_{\mathfrak{q}_2}}}{B(\mathfrak{p})/D(\mathfrak{p})} = \frac{B(\mathfrak{p})^{\mathrm{Fr}_{\mathfrak{q}_2}}}{B(\mathfrak{p})}.$$

Let $q$ denote a primary normalized generator of $\mathfrak{q}$. Now the definition of $B(\mathfrak{p})$, Proposition 3.4, Lemma 4.3 and the definition of the symbol produce consecutively the following equalities:

$$\frac{B(\mathfrak{p})^{\mathrm{Fr}_{\mathfrak{q}_2}}}{B(\mathfrak{p})} = \frac{\prod_{z\in M} P(z^{\mathrm{Fr}_{\mathfrak{q}_2}})}{\prod_{z\in M} P(z)} = \frac{\prod_{z\in M} P([qq_2q_3]z)}{\prod_{z\in M} P(z)} = \left(\frac{qq_2q_3}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{q}\mathfrak{q}_2\mathfrak{q}_3}{\mathfrak{p}}\right).$$

Therefore on the one hand one has

$$\left(\frac{\mathfrak{p}\mathfrak{p}_2^4\mathfrak{p}_3^5}{\mathfrak{q}_2}\right) = \left(\frac{\mathfrak{q}\mathfrak{q}_2\mathfrak{q}_3}{\mathfrak{p}}\right)$$

and on the other hand it follows from elementary facts that

$$\left(\frac{\mathfrak{p}\mathfrak{p}_2^4\mathfrak{p}_3^5}{\mathfrak{q}_2}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}_2}\right)\left(\frac{\mathfrak{p}_2}{\mathfrak{q}_2}\right)^4\left(\frac{\mathfrak{p}_3}{\mathfrak{q}_2}\right)^5 = \left(\frac{\mathfrak{p}}{\mathfrak{q}_2}\right)\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)\left(\frac{\mathfrak{p}}{\mathfrak{q}_3}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}\mathfrak{q}_2\mathfrak{q}_3}\right).$$

This finishes the proof of the theorem. ∎

Now we can proceed to prove Kummer's reciprocity law, which was stated above as Theorem 2.1. Taking into account the action of $\mathrm{Gal}(F/\mathbb{Q})$ on the Kummer symbol, which rules out the various settings in which Theorem 2.1 is indeed trivial, it is not difficult to establish that it suffices to prove the theorem in the following two cases: when the ideals $\mathfrak{p}$ and $\mathfrak{q}$ are not conjugate and at least one of them has degree one or two, and when $\mathfrak{p}$ and $\mathfrak{q}$ are conjugate and have degree one.

Consider the first case. Suppose that $\mathfrak{p}$ has degree one or two. If $\mathfrak{q}$ also has degree one or two, applying Theorem 4.4 to the ordered pairs $(\mathfrak{p},\mathfrak{q})$, $(\mathfrak{p},\mathfrak{q}_2)$, $(\mathfrak{p},\mathfrak{q}_3)$, $(\mathfrak{p},\mathfrak{q}_4)$, $(\mathfrak{q},\mathfrak{p})$ and $(\mathfrak{q},\mathfrak{p}_2)$ one gets a multiplicative system of six linear homogeneous equations in the variables $x_i = \left(\frac{\mathfrak{p}}{\mathfrak{q}_i}\right)/\left(\frac{\mathfrak{q}_i}{\mathfrak{p}}\right)$ $(1 \le i \le 6)$ with nonzero determinant in $\mathbb{F}_7$, which implies that $x_1 = 1$. If $\mathfrak{q}$ has degree three and one writes $x = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)/\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)$ and $y = \left(\frac{\mathfrak{p}}{\mathfrak{q}_3}\right)/\left(\frac{\mathfrak{q}_3}{\mathfrak{p}}\right)$, applying Theorem 4.4 to the ordered pairs $(\mathfrak{p},\mathfrak{q})$ and $(\mathfrak{p},\mathfrak{q}_3)$ one gets $x^2y = 1$ and $xy^2 = 1$ and thus $x = 1$. Finally, if $\mathfrak{q}$ is of degree 6, since $\mathfrak{q}_1 = \mathfrak{q}_2 = \mathfrak{q}_3$, applying Theorem 4.4 to the ordered pair $(\mathfrak{p},\mathfrak{q})$ one gets $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)^3 = \left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)^3$ and therefore $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)$.

Consider now the second case. Applying Theorem 4.4 to the ordered pairs $(\mathfrak{p}_2,\mathfrak{p}_4)$, $(\mathfrak{p}_3,\mathfrak{p}_4)$, $(\mathfrak{p}_6,\mathfrak{p}_4)$, $(\mathfrak{p},\mathfrak{p}_6)$ and $(\mathfrak{p},\mathfrak{p}_3)$ one gets a multiplicative system of five linear homogeneous equations in the variables $z_i = \left(\frac{\mathfrak{p}}{\mathfrak{p}_i}\right)/\left(\frac{\mathfrak{p}_i}{\mathfrak{p}}\right)$ $(2 \le i \le 6)$ with nonzero determinant in $\mathbb{F}_7$, which implies that $z_i = 1$ $(2 \le i \le 6)$.

**5. The complementary laws.** The purpose of this section is to prove the complementary laws of Kummer's reciprocity for seventh powers, which was stated above as Theorem 2.2. We skip the computation of the symbol $\left(\frac{\zeta}{\mathfrak{q}}\right)$ since it follows immediately from its definition without any further consideration. We shall first compute the symbols for $\mu_1$ and $\mu_2$ and conclude with the computation of the symbol for $\lambda$.

In order to compute the symbols for $\mu_1$ and $\mu_2$, we shall consider a certain rational function $Y$ on $J$ whose values at 7-torsion points of $J$ are related on the one hand to $\mu_1$ and $\mu_2$ and, on the other hand, to the values of a seventh power of another rational function on $J$.

As at the beginning of Section 3, take $\infty$ as base point for the Abel–Jacobi embedding. Recall that via this embedding the rational functions on $J$ are simply the symmetric functions on triples of points of $C$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$ be three points of $C$; as above, we denote by $P$, $Q$ and $R$ the rational functions on $J$ determined respectively by the symmetric polynomials $x_1 + x_2 + x_3$, $x_1x_2 + x_1x_3 + x_2x_3$ and $x_1x_2x_3$.

We define $Y$ to be the rational function on $J$ determined by the symmetric polynomial $y_1y_2y_3$.

Let us say momentarily that a polynomial expression $h$ in the indeterminates $X_1$, $Y_1$, $X_2$, $Y_2$, $X_3$, $Y_3$ with coefficients in a ring $A$ is *symmetric* whenever

$$h(X_{\sigma(1)}, Y_{\sigma(1)}, X_{\sigma(2)}, Y_{\sigma(2)}, X_{\sigma(3)}, Y_{\sigma(3)}) = h(X_1, Y_1, X_2, Y_2, X_3, Y_3)$$

for every permutation $\sigma$ in the symmetric group $S_3$. If $P$ is a point in the affine plane, let as usual $x_P$ denote its first coordinate and $y_P$ its second coordinate.

LEMMA 5.1. *There is an open set $\mathcal{U} \subset J$ such that for every $u, v \in \mathcal{U}$ such that $u = [A + B + C - 3\infty]$ and $v = [D + E + F - 3\infty]$ one has*

$$R(u)^7 R(v)^7 Y(u+v) = -e(u,v)^7 Y(u) Y(v)$$

*where $e(u,v)$ is a quotient of symmetric polynomial expressions with coefficients in $\mathbb{Z}[x_A, x_B, x_C, y_A, y_B, y_C]$ evaluated at $x_D, x_E, x_F, y_D, y_E, y_F$ and also a quotient of symmetric polynomial expressions with coefficients in $\mathbb{Z}[x_D, x_E, x_F, y_D, y_E, y_F]$ evaluated at $x_A, x_B, x_C, y_A, y_B, y_C$.*

*Proof.* We confine ourselves here to giving a quick sketch of the proof. Write $u + v = [J + K + L - 3\infty]$. By the Riemann–Roch theorem, there is a rational function $g = ax^4 + bx^3 + cx^2 + dx + e + fy - xy$ whose divisor is

$$J + K + L + I(A) + I(B) + I(C) + I(D) + I(E) + I(F) - 9\infty.$$

Thus clearly all the coefficients of $g$, and in particular $e$, are expressions with the symmetry property described in the statement of the lemma. Moreover, the resultant of $g$ and the curve $C$ yields

$$(y_A + 1)(y_B + 1)(y_C + 1)(y_D + 1)(y_E + 1)(y_F + 1) y_J y_K y_L = -e^7$$

so that

$$y_A(y_A+1) y_B(y_B+1) y_C(y_C+1) y_D(y_D+1) y_E(y_E+1) y_F(y_F+1) Y(u+v) = -e^7 Y(u) Y(v)$$

and the lemma follows. ∎

PROPOSITION 5.2. *There is a rational function $G$ on $J$ with coefficients in $F$ such that $G^7 = Y \circ [\lambda]$.*

*Proof.* Recall that $[\lambda]z = z - [\zeta]z$ for any $z \in J$. Thus, applying Lemma 5.1 to $u = z$ and $v = -[\zeta]z$ one gets

$$R(z)^7 R(-[\zeta]z)^7 Y([\lambda]z) = -e(z, -[\zeta]z)^7 Y(z) Y(-[\zeta]z). \tag{5.1}$$

Using the equalities $Y(-[\zeta]z) = Y(-z)$, $Y(z)Y(-z) = R(z)^7$ and $R(-[\zeta]z)^7 = R(z)^7$, it follows from (5.1) that

$$R(z)^7 Y([\lambda]z) = -e(z, -[\zeta]z)^7. \tag{5.2}$$

We define

$$G(z) = -\frac{e(z, -[\zeta]z)}{R(z)}.$$

From the properties of $e$ stated in Lemma 5.1, it is clear that $G$ is a rational function on $J$ with coefficients in $F$. Moreover, (5.2) implies that $G^7 = Y \circ [\lambda]$. ∎

PROPOSITION 5.3. *Let $\omega_1 = [(0,0) - \infty] \in J$. There is an open set $\mathcal{V} \subset J$ such that for any $z \in \mathcal{V}$ one has*

$$G(z + \omega_1) = \zeta^4 G(z).$$

*Proof.* It follows from Proposition 5.2 and the fact that $[\lambda]\omega_1 = 0$ that

$$G(z + \omega_1)^7 = Y([\lambda](z + \omega_1)) = Y([\lambda]z) = G(z)^7.$$

Hence for some $i$, $0 \le i \le 6$, the quotient $G(z + \omega_1)/G(z)$ is the constant function $\zeta^i$. Evaluating this quotient at a suitable point $z$ one concludes that $i = 4$. ∎

The strategy now is to evaluate the function $Y$ at several 7-torsion points of $J$. Actually it is a rather difficult task to compute nontrivial torsion points of $J$ explicitly. However, all the $\lambda^3$-torsion points and some $\lambda^4$-torsion and $\lambda^5$-torsion points of $J$ were computed in [C-E-G]. In particular, we have determined in [C-E-G] four points $\omega_2$, $\omega_3$, $\omega_4$ and $\omega_5$ such that

$$[\lambda]\omega_5 = \omega_4, \quad [\lambda]\omega_4 = \omega_3, \quad [\lambda]\omega_3 = \omega_2, \quad [\lambda]\omega_2 = \omega_1. \tag{5.3}$$

Let us remark that in the notation of [C-E-G], $\omega_2$ is $\omega_{1,4}$ and $\omega_3$ is $\omega_{1,4,0}$. Let $s$ be the unique real seventh root of $\mu_1^3\mu_2$. It was proved in [C-E-G] that

$$Y(\omega_3) = -\mu_1^3\mu_2, \tag{5.4}$$

$$Y(\omega_5) = \mu_2\tau^7, \tag{5.5}$$

where $\tau$ is a unit in the ring of integers of $F(s)$ defined explicitly by

$$\begin{aligned}\tau = \frac{1}{7}(&1 - 3\zeta^2 - \zeta^3 - \zeta^4 - 3\zeta^5 + (5\zeta + \zeta^2 + 2\zeta^3 + \zeta^4 + 5\zeta^5)s \\ &+ (-4 - 5\zeta - 3\zeta^2 - 5\zeta^3 - 4\zeta^4)s^3 + (2 - 4\zeta - 4\zeta^2 + 2\zeta^3 - 3\zeta^5)s^4 \\ &+ (3 + 4\zeta + 3\zeta^2 + 2\zeta^4 + 2\zeta^5)s^5 + (-6 - 6\zeta - 2\zeta^3 - 5\zeta^4 - 2\zeta^5)s^6).\end{aligned}$$

From (5.4) and previous results one obtains the following proposition.

PROPOSITION 5.4. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and let $\pi$ be a normalized primary generator of $\mathfrak{p}$ such that $\pi \equiv 1 + a\lambda^3 \bmod \lambda^4$. Then*

$$\left(\frac{\mu_1^3\mu_2}{\mathfrak{p}}\right) = \zeta^{4a}.$$

*Proof.* Let $\mathrm{Fr}_{\mathfrak{p}}$ denote the Frobenius automorphism of $\mathfrak{p}$ in the abelian extension $F \subseteq F(s)$. Notice that Proposition 5.2 combined with the second

statement of (5.3) implies that $G(\omega_4)^7 = Y(\omega_3)$. This fact, together with Proposition 3.4, the equalities in (5.3) and Proposition 5.3, gives rise to the following chain of equalities:

$$\left(\frac{\mu_1^3\mu_2}{\mathfrak{p}}\right) = \frac{G(\omega_4)^{\mathrm{Fr}_\mathfrak{p}}}{G(\omega_4)} = \frac{G(\omega_4^{\mathrm{Fr}_\mathfrak{p}})}{G(\omega_4)} = \frac{G([\pi\pi_4\pi_5]\omega_4)}{G(\omega_4)}$$
$$= \frac{G([1+a\lambda^3+\alpha\lambda^4]\omega_4)}{G(\omega_4)} = \frac{G(\omega_4+a\omega_1)}{G(\omega_4)} = \zeta^{4a},$$

where $\alpha$ denotes a certain element of $\mathfrak{O}$. ∎

Notice that Corollary 2 of [C-E-G] means that we cannot go any further using $\lambda^3$-torsion points and that to be successful, it is actually necessary to get some essentially new data coming from other torsion points. Indeed, with the help of Proposition 5.4 and (5.5), we can now prove the complementary laws for $\mu_1$ and $\mu_2$. Let us denote by $\rho$ the inverse of the unit $\tau$ defined above, let $E = F(s)$ and let $M = E(\sqrt[7]{\mu_2}) = F(\sqrt[7]{\mu_1}, \sqrt[7]{\mu_2})$. Let $\mathrm{Fr}_{M/F}(\mathfrak{p})$ and $\mathrm{Fr}_{E/F}(\mathfrak{p})$ be the Frobenius automorphisms of $\mathfrak{p}$ in the corresponding extensions; of course, $\mathrm{Fr}_{M/F}(\mathfrak{p})$ coincides with $\mathrm{Fr}_{E/F}(\mathfrak{p})$ when restricted to $E$. If $\omega_6$ is any of the seven points of $J$ such that $[\lambda]\omega_6 = \omega_5$, we have

$$\left(\frac{\mu_2}{\mathfrak{p}}\right) = \left(\frac{Y(\omega_5)\rho^7}{\mathfrak{p}}\right) = \frac{(G(\omega_6)\rho)^{\mathrm{Fr}_{M/F}(\mathfrak{p})}}{G(\omega_6)\rho} = \frac{G(\omega_6)^{\mathrm{Fr}_{M/F}(\mathfrak{p})}}{G(\omega_6)} \cdot \frac{\rho^{\mathrm{Fr}_{E/F}(\mathfrak{p})}}{\rho}.$$

Let us look at the two factors above. On the one hand, Proposition 5.4 says that $s^{\mathrm{Fr}_{E/F}(\mathfrak{p})} = \zeta^{4a}s$ and from this it follows easily that $\rho^{\mathrm{Fr}_{E/F}(\mathfrak{p})}/\rho$ is a unit of the ring of integers of $M$ depending only on $a$. On the other hand, Proposition 3.4, the equalities in (5.3) and Proposition 5.3 yield

$$\frac{G(\omega_6)^{\mathrm{Fr}_{M/F}(\mathfrak{p})}}{G(\omega_6)} = \frac{G([\pi\pi_4\pi_5]\omega_6)}{G(\omega_6)} = \frac{G([1+a\lambda^3+[5a]\lambda^4-c\lambda^5+\beta\lambda^6]\omega_6)}{G(\omega_6)}$$
$$= \frac{G(\omega_6+a\omega_3+[5a]\omega_2-c\omega_1)}{G(\omega_6)} = \zeta^{3c}\frac{G(\omega_6+a\omega_3+[5a]\omega_2)}{G(\omega_6)}$$

where $\beta$ is some element in $\mathfrak{O}$. Since $G(\omega_6+a\omega_3+[5a]\omega_2)/G(\omega_6)$ depends only on $a$, we can write

$$\frac{G(\omega_6+a\omega_3+[5a]\omega_2)}{G(\omega_6)} \cdot \frac{\rho^{\mathrm{Fr}_{E/F}(\mathfrak{p})}}{\rho} = \zeta^{\phi(a)}$$

where $\phi(a)$ is an integer depending only on $a$. Summing up, one has

$$\left(\frac{\mu_2}{\mathfrak{p}}\right) = \zeta^{3c+\phi(a)}. \tag{5.6}$$

Combining (5.6) with Proposition 5.4 gives

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) = \zeta^{-a-5\phi(a)-c}. \tag{5.7}$$

Since $\pi_2 \equiv 1 + a\lambda^3 + 5a\lambda^4 + 4c\lambda^5 \bmod \lambda^6$, the same argument leading to (5.6) yields

$$\left(\frac{\mu_2}{\mathfrak{p}_2}\right) = \zeta^{12c+\phi(a)}. \tag{5.8}$$

Now, using

$$\left(\frac{\mu_1^2}{\mathfrak{p}}\right) = \left(\frac{\mu_1}{\mathfrak{p}}\right)^{\sigma_2} = \left(\frac{\mu_2}{\mathfrak{p}_2}\right)$$

together with (5.7) and (5.8), we get

$$\zeta^{2(-a-5\phi(a)-c)} = \zeta^{12c+\phi(a)},$$

which ensures that $\phi(a) \equiv 3a \bmod 7$, and this proves the complementary laws for $\mu_1$ and $\mu_2$.

Finally we tackle the complementary law for $\lambda$. Since we already have formulas for $\left(\frac{\zeta}{\mathfrak{p}}\right)$, $\left(\frac{\mu_1}{\mathfrak{p}}\right)$ and $\left(\frac{\mu_2}{\mathfrak{p}}\right)$, the equality

$$\sqrt{-7} = -\lambda^3\zeta^2\mu_1^{-1}\mu_2^{-2}$$

shows that to determine $\left(\frac{\lambda}{\mathfrak{p}}\right)$ it is enough to compute $\left(\frac{\sqrt{-7}}{\mathfrak{p}}\right)$. Here again the facts stated in Proposition 4.2 play a central role.

PROPOSITION 5.5. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{O}$, different from $\lambda\mathfrak{O}$, and let $\pi$ be a normalized primary generator of $\mathfrak{p}$ with $\lambda$-adic expansion $1 + a\lambda^3 + [5a]\lambda^4 + c\lambda^5 + d\lambda^6 + e\lambda^7 + \cdots$. Then*

$$\left(\frac{\sqrt{-7}}{\mathfrak{p}}\right) = \zeta^{a-3c+2d-3e}.$$

*Proof.* Suppose that $\mathfrak{p}$ has degree one or two. Let $K = F(\sqrt[7]{2}, \sqrt{\lambda})$, let $m = [-2a - a^2 + 2c + 2d]$ and let $A(\mathfrak{p})$ be the number defined in (4.1). Consider the following diagram of fields and field extensions:

$$\begin{array}{ccc} K & \longrightarrow & K(J[\mathfrak{p}]) \\ \uparrow & & \uparrow \\ F & \longrightarrow & F(\sqrt[7]{2^m A(\mathfrak{p})}) \end{array}$$

It is known from Proposition 4.2(a) that $\lambda\mathfrak{O}$ is unramified in the abelian extension $F \subseteq F(\sqrt[7]{2^m A(\mathfrak{p})})$; let $\mathrm{Fr}_\lambda$ denote the Frobenius automorphism of $\lambda\mathfrak{O}$ in this extension. Recall that $\lambda\mathfrak{O}$ is totally ramified in $F \subseteq K$; let $\Lambda$ be the only prime of $K$ lying above $\lambda\mathfrak{O}$. We know from Proposition 3.7 that $\Lambda$ is unramified in the abelian extension $K \subseteq K(J[\mathfrak{p}])$; let $\mathrm{Fr}_\Lambda$ denote the Frobenius automorphism of $\Lambda$ in this extension.

Let $B(\mathfrak{p})$ be the number defined in (4.6). On the one hand, from the definition of $B(\mathfrak{p})$, Proposition 3.5 and Lemma 4.3 it follows that

$$\frac{B(\mathfrak{p})^{\mathrm{Fr}_\Lambda}}{B(\mathfrak{p})} = \frac{(\prod_{z\in M} P(z))^{\mathrm{Fr}_\Lambda}}{\prod_{z\in M} P(z)} = \frac{\prod_{z\in M} P(z^{\mathrm{Fr}_\Lambda})}{\prod_{z\in M} P(z)} = \frac{\prod_{z\in M} P([\pm\sqrt{7}i]z)}{\prod_{z\in M} P(z)}$$
$$= \left(\frac{\sqrt{-7}}{\mathfrak{p}}\right).$$

On the other hand, since $B(\mathfrak{p})$ is a seventh root of $A(\mathfrak{p})$ and $\sqrt[7]{2}$ belongs to $K(J[\mathfrak{p}])$, one has

$$\frac{B(\mathfrak{p})^{\mathrm{Fr}_\Lambda}}{B(\mathfrak{p})} = \frac{(\sqrt[7]{A(\mathfrak{p})})^{\mathrm{Fr}_\Lambda}}{\sqrt[7]{A(\mathfrak{p})}} = \frac{(\sqrt[7]{2^m A(\mathfrak{p})})^{\mathrm{Fr}_\lambda}}{\sqrt[7]{2^m A(\mathfrak{p})}}.$$

Hence

$$\left(\frac{\sqrt{-7}}{\mathfrak{p}}\right) = \frac{(\sqrt[7]{2^m A(\mathfrak{p})})^{\mathrm{Fr}_\lambda}}{\sqrt[7]{2^m A(\mathfrak{p})}}.$$

Recall now that following Proposition 4.2(b) there is a number $D(\mathfrak{p}) \in F^*$ such that $A(\mathfrak{p}) = \pi\pi_2^4\pi_3^5 D(\mathfrak{p})^7$. Write $T(\mathfrak{p}) = 2^m A(\mathfrak{p})(2^m D(\mathfrak{p}))^{-7}$; then for any root $x$ of the polynomial $X^7 - T(\mathfrak{p})$, we have $F(\sqrt[7]{2^m A(\mathfrak{p})}) = F(x)$ and

$$\left(\frac{\sqrt{-7}}{\mathfrak{p}}\right) = \frac{x^{\mathrm{Fr}_\lambda}}{x}.$$

Suppose $x^{\mathrm{Fr}_\lambda}/x = \zeta^j$ and let us compute $j$. Writing $x = 1 + \lambda y$ we have

$$\lambda^7 y^7 + 7\lambda^6 y^6 + 21\lambda^5 y^5 + 35\lambda^4 y^4 + 21\lambda^2 y^2 + 7\lambda y + 1 - T(\mathfrak{p}) = 0.$$

Denote by $R$ the ring of integers of $F(\sqrt[7]{2^m A(\mathfrak{p})})$. Using the fact, easy to prove, that $\lambda^7$ divides $1 - T(\mathfrak{p})$, it follows from the last equality that $y^7 + uy - N \equiv 0 \bmod \lambda R$, where $N = -a + 3c - 2d + 3e$ and $u = (1+\zeta)(1+\zeta+\zeta^2)\cdots(1+\zeta+\cdots+\zeta^5)$. Thus, since $u \equiv -1 \bmod \lambda$, we have $y^7 - y - N \equiv 0 \bmod \lambda R$. From this fact, using the relations $y^7 \equiv y^{\mathrm{Fr}_\lambda} \bmod \lambda R$ and $\zeta^j = (1+\lambda y)^{\mathrm{Fr}_\lambda}/(1+\lambda y)$, one can deduce that

$$\zeta^j \equiv 1 + N\lambda \bmod \lambda^2.$$

But obviously $\zeta^j \equiv 1 - j\lambda \bmod \lambda^2$, hence $j \equiv -N \bmod 7$, and this proves the proposition when $\mathfrak{p}$ has degree one or two. When $\mathfrak{p}$ has degree three or six, the proof of the proposition is a consequence of already known facts and therefore is left as an exercise for the reader. ∎

**Acknowledgements.** The third author has been supported by research project EHU 07/09 "Topics in Number Theory" from the University of the Basque Country.

## References

[A] G. W. Anderson, *Torsion points on the Jacobians of quotients of Fermat curves and p-adic soliton theory*, Invent. Math. 118 (1994), 475–492.

[C-E-G] R. Clement, J. M. Echarri, E. J. Gómez Ayala, *Torsion points on the jacobian of a Fermat quotient*, J. Pure Appl. Algebra 213 (2009), 1489–1500.

[C] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, 2000.

[E] J. M. Echarri, *The jacobian of a hyperelliptic quotient of the Fermat curve and the reciprocity law for seventh powers*, Ph.D. thesis, University of the Basque Country, 2006 (in Spanish).

[F] R. Fueter, *Reziprozitätsgesetze in quadratisch-imaginären Körpern*, Gött. Nachr. 1927, 336–346, 427–445.

[G1] D. Grant, *Formal groups in genus 2*, J. Reine Angew. Math. 411 (1990), 96–121.

[G2] —, *A proof of quintic reciprocity using the arithmetic of* $y^2 = x^5 + 1/4$, Acta Arith. 75 (1996), 321–337.

[G3] —, *Torsion on theta divisors of hyperelliptic Fermat Jacobians*, Compos. Math. 140 (2004), 1432–1438.

[G4] —, *Geometric proofs of reciprocity laws*, J. Reine Angew. Math. 586 (2005), 91–124.

[Gr] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compos. Math. 42 (1981), 345–359.

[H-S] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer, 2000.

[K1] T. Kubota, *Reciprocities in Gauss's and Eisenstein's number fields*, J. Reine Angew. Math. 208 (1961), 35–50.

[K2] —, *An application of the power residue theory to some abelian functions*, Nagoya Math. J. 27 (1966), 51–54.

[L] S. Lang, *Complex Multiplication*, Springer, 1983.

[Le] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer, 2000.

[M] A. Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. 62 (1955), 92–119.

[S-T] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan, 1961.

R. Clement Fernández, E. J. Gómez Ayala
Departamento de Matemáticas
Facultad de Ciencia y Tecnología
Universidad del País Vasco
Apartado 644
48080 Bilbao, Spain
E-mail: rosario.clement@ehu.es
eugeniojesus.gomez@ehu.es

J. M. Echarri Hernández
Departamento de Economía Aplicada IV
Facultad de Ciencias Económicas
y Empresariales
Universidad del País Vasco
Apartado 644
48080 Bilbao, Spain
E-mail: josemiguel.echarri@ehu.es

*Received on 16.10.2008*
*and in revised form on 15.7.2009* (5828)