12. Class Number Calculation and Elliptic Unit. I

Cubic Case

By Ken NAKAMULA

Department of Mathematics, Tokyo Metropolitan University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1981)

Let \( K \) be a real cubic number field with the discriminant \( D < 0 \). In the following, an effective algorithm will be given, to calculate the class number \( h \) and the fundamental unit \( \varepsilon_i \) of \( K \) at a time.

Angell [1] has given a table of \( h \) and \( \varepsilon_i \) of \( K \) for \( D > -20000 \). In the special case when \( K = \mathbb{Q}(\sqrt[3]{m}) \), a pure cubic number field, Dedekind [5] has given an analytic method to calculate \( h \). In such a pure cubic case, Dedekind’s method has been improved by several authors, see [3] and [13]. In all these algorithms, however, it is necessary to compute \( \varepsilon_i \) by Voronoi’s algorithm, see [6, pp. 232–230], before the calculation of \( h \).

Our method does not need Voronoi’s algorithm, and \( h \) and \( \varepsilon_i \) are calculated at a time. The starting point of the method is the index formula on elliptic units given by Schertz, see [11] and [12], and the idea of the algorithm is learned from G. Gras and M.-N. Gras [8]. There is a similar algorithm to compute the class number and fundamental units of a real quartic number field which is not totally real and contains a quadratic subfield, see the author’s [10]. The author expects that such an algorithm will be generalized to calculate the class number of a non-galois number field whose galois closure is an abelian extension over an imaginary quadratic number field.

§ 1. Illustration of algorithm. The class number \( h \) of \( K \) is given by the index of the subgroup generated by the so called “elliptic unit” \( \eta_\varepsilon \) of \( K \), of which the definition will be given in § 4, in the group of positive units of \( K \), see [11]:

\[
\eta_\varepsilon = \varepsilon_i^h, \quad \text{i.e.} \quad h = \langle \varepsilon_i \rangle : \langle \eta_\varepsilon \rangle.
\]

Our method consists of the following steps:

(i) to compute an approximate value of \( \eta_\varepsilon \) (§ 4),
(ii) to compute the minimal polynomial of \( \eta_\varepsilon \) over \( \mathbb{Q} \) (Lemma 2),
(iii) for any unit \( \xi(>1) \) of \( K \), to give an explicit upper bound \( B(\xi) \) of \( \langle \varepsilon_i \rangle : \langle \xi \rangle \) (Proposition 1),
(iv) for any unit \( \xi(>1) \) of \( K \) and for a natural number \( \mu \), to judge whether a real number \( \sqrt[3]{\xi} \) is an element to \( K \) or not, and to compute the minimal polynomial of \( \sqrt[3]{\xi} \) over \( \mathbb{Q} \) if it is an element of \( K \).
Now, the computation of $h$ and $\varepsilon_1$ goes as follows. Determine the minimal polynomial of $\eta_e$ over $\mathbb{Q}$ by (i) and (ii). Put $h(\eta_e) = 1$ and compute $B(\eta_e)$ by (iii). Put $\xi = \eta_e$, and test whether the set

$$S(\xi) := \{p \mid p : \text{prime number, } p \leq B(\xi), \sqrt[\xi]{\xi} \in K\}$$

is empty or not by (iv). If $S(\xi)$ is empty, then $\varepsilon_1 = \xi$ and $h = h(\xi)$. If $S(\xi)$ is not empty, take the smallest prime $p$ in $S(\xi)$, and let $\xi = \sqrt[\xi]{\xi}$, $B(\xi) = B(\xi)/p$ and $h(\xi) = p h(\xi)$. The minimal polynomial of $\xi$ over $\mathbb{Q}$ can be calculated by (iv). Next, put $\xi = \varepsilon$ and repeat the above procedure for $\xi$ by using (iv). Then $S(\xi)$ becomes an empty set in a finite number of steps.

§ 2. Upper bound of $h$. The following Artin's lemma essentially gives an upper bound of the index of a subgroup of the group of units of $K$.

**Lemma 1 (Artin [2]).** Let $\varepsilon(>1)$ be a unit of $K$. Then the absolute value of the discriminant $D(\varepsilon)$ of $\varepsilon$ is smaller than $4\varepsilon^2 + 24$, i.e. $|D(\varepsilon)| < 4\varepsilon^2 + 24$.

Note that $D(\varepsilon)$ is a non-zero multiple of the discriminant $D$ of $K$ since $\varepsilon$ is irrational. It is easy to see that $(|D(\varepsilon)| - 24)/4 > 1$. Then we have

**Proposition 1.** Let $\xi(>1)$ be a unit of $K$. Then

$$\langle \xi \rangle : \langle \xi \rangle < 3 \log(\xi)/\log((|D| - 24)/4).$$

On account of (1), we have

**Corollary.** Let $\eta_e$ be the elliptic unit of $K$. Then the class number $h$ of $K$ satisfies

$$h < 3 \log(\eta_e)/\log((|D| - 24)/4).$$

§ 3. $\mu$-th root of units. For any positive unit $\xi$ of $K$, we denote by $s(\xi)$ and $t(\xi)$ the absolute trace of $\xi$ and $1/\xi$ respectively. The following lemma enables us to calculate the minimal polynomial of a unit of $K$ over $\mathbb{Q}$ from an approximate value of the unit.

**Lemma 2.** Let $\xi(>1)$ be a unit of $K$. Then $s(\xi)$ is a rational integer such that $|s(\xi) - \xi| < 2/\sqrt[\xi]{\langle \xi \rangle}$ and $1/\xi + s(\xi)/\xi$ is a rational integer, and $t(\xi)$ is given by $t(\xi) = 1/\xi + s(\xi)/\xi$.

For any rational integers $s$ and $t$, define $r_\mu = r_\mu(s, t) (\mu = 1, 2, 3, \cdots)$ as follows:

\[
\begin{align*}
r_1 & = s, \quad r_2 = s^2 - 2t, \quad r_3 = s^3 - 3st + 3, \\
r_\mu & = s r_{\mu-1} - t r_{\mu-2} + r_{\mu-3} \quad \text{ if } \mu \geq 4.
\end{align*}
\]

Then we have

**Proposition 2.** Let $\xi(>1)$ be a unit of $K$ and $\mu$ be a natural number. Put $\varepsilon = \sqrt[\xi]{\xi}(>1)$. The real number $\varepsilon$ belongs to $K$ if and only if there exists a rational integer $u$ such that

$$|u - \varepsilon| < 2/\sqrt[\xi]{\langle \xi \rangle},$$

and $r_\mu(u, \varepsilon)$ and $r_\mu(v, u) = t(\xi)$.\]
where \( v \) is the nearest rational integer to \( 1/\varepsilon + \varepsilon(u - \varepsilon) \). If \( \varepsilon \) belongs to \( K \), then
\[
s(\varepsilon) = u \quad \text{and} \quad t(\varepsilon) = v.
\]
This proposition gives us an effective method to judge whether the \( \mu \)-th root of a unit \( \xi(>1) \) of \( K \) is an element of \( K \) or not. It only uses \( s(\xi) \), \( t(\xi) \) and an approximate value of \( \xi \).

§ 4. Elliptic unit. In order to define the elliptic unit \( \eta_e \) of \( K \), let us prepare some notations. Let the imaginary quadratic number field \( \Sigma = \mathbb{Q}(\sqrt{D}) \) and the discriminant of \( \Sigma \) be \(-d\). Then the galois closure of \( K/Q \) is the composite field \( L = K\Sigma \), which is dihedral of degree 6 over \( Q \) and cyclic cubic over \( \Sigma \). The abelian extension \( L/\Sigma \) has a rational conductor \( (f) \) with a natural number \( f \), and \( D = -f^3d \). Moreover, \( L \) is contained in the ring class field \( \Sigma, \) modulo \( f \) over \( \Sigma \). All these facts are known in Hasse [9]. Let \( \mathfrak{N}(f) \) be the ring class group of \( \Sigma \) modulo \( f \). By the classical theory of complex multiplication, see Deuring [7], the ring class field \( \Sigma_f = \Sigma(j(f)) \) for \( f \in \mathfrak{N}(f) \), where \( j(f) \) is the ring class invariant as usual, and there is the canonical isomorphism
\[
\lambda : \mathfrak{N}(f) \cong \text{Gal} (\Sigma_f/\Sigma); \quad j(f^{(T)}) = j(f^{(T)}_{f^{-1}}) \quad \text{for } f, f' \in \mathfrak{N}(f).
\]
Let \( \mathfrak{u} = \lambda^{-1}(\text{Gal} (\Sigma_f/L)) \), take and fix a class of \( f \) which does not belong to \( \mathfrak{u} \). For \( f \in \mathfrak{N}(f) \), denote by \( \gamma_f \) a complex number with its imaginary part positive such that \( Z \gamma_f + Z \in f \). Then the elliptic unit \( \eta_e \) of \( K \) is defined, independent of the choice of \( \gamma_f \) and \( \gamma_{f'} \), by the following:
\[
(2) \quad \eta_e := \prod_{f \in \mathfrak{u}} \sqrt{\text{Im} (\gamma_f)/\text{Im} (\gamma_{f'})} |\eta(\gamma_f) / \eta(\gamma_{f'})|^{|f|/2}.
\]
Here \( \eta(z) \) is the Dedekind eta-function:
\[
\eta(z) = \exp (\pi i z/12) \prod_{v=1}^{\infty} (1 - \exp (2\pi ivz)).
\]
Now we should see how an approximate value of \( \eta_e \) is computed. Suppose that \( \mathfrak{N}(f) \) and \( \mathfrak{u} \) have been given already. Then, since we can take \( \gamma_f \) so that \( \text{Im} (\gamma_f) \geq \sqrt{3}/2 \) as in [4], we can compute \( \eta_e \) by (2), using the following lemma for example.

**Lemma 3.** Let \( z = x + iy \) be a complex number with the imaginary part \( y > 0 \), and put
\[
R_N(z) := -\pi y/6 + \sum_{v=1}^{N-1} \log |1 - \exp (2\pi ivz)|^2.
\]
Then
\[
|\log |\eta(z)|^2 - R_N(z)| < \frac{(2 - \exp (-2\pi Ny))(\exp (-2\pi Ny))}{(1 - \exp (-2\pi Ny))(1 - \exp (-2\pi y))}.
\]
If the discriminant \( D \) of \( K \) is given, it is easy to compute \( f \). Then we can count out explicitly every subgroup \( \mathfrak{u} \) of \( \mathfrak{N}(f) \) which may correspond to \( K \) as in Hasse [9]. Thus the class numbers and the fundamental units of all cubic number fields with the same discriminant.
$D$ can be computed as described above. In pure cubic case, i.e. $K = \mathbb{Q}(\sqrt[3]{m})$ with a cube free natural number $m$, the corresponding subgroup $\alpha$ of $\mathfrak{N}(f)$ is perfectly determined from the value $m$, see [5].

References