Journal of Number Theory 155 (2015) 46–62

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Primitive generators of certain class fields

Ick Sun Eum [a], Ja Kyung Koo [a], Dong Hwa Shin [b,*,1]

[a] *Department of Mathematical Sciences, KAIST, Daejeon 305-701, Republic of Korea*
[b] *Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 449-791, Republic of Korea*

ARTICLE INFO

Article history:
Received 15 December 2014
Received in revised form 5 March 2015
Accepted 17 March 2015
Available online 6 May 2015
Communicated by David Goss

MSC:
primary 11R37
secondary 11F03, 11G16

Keywords:
Class field theory
Modular functions

ABSTRACT

We find primitive generators of certain class fields of imaginary quadratic fields as real algebraic integers which arise from the study of some quadratic Diophantine equations.

1. Introduction

Let n and N be positive integers, and p be an odd prime not dividing nN. Recently, Cho showed in [1] that there exists a unique finite abelian extension L of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$, which is also Galois over $\mathbb{Q}$, for which

* Corresponding author.
E-mail addresses: zandc@kaist.ac.kr (I.S. Eum), jkkoo@math.kaist.ac.kr (J.K. Koo), dhshin@hufs.ac.kr (D.H. Shin).

[1] Supported by Hankuk University of Foreign Studies Research Fund of 2015.

http://dx.doi.org/10.1016/j.jnt.2015.03.011
0022-314X/

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \text{ satisfying } x \equiv 1 \pmod{N} \text{ and } y \equiv 0 \pmod{N}$$
$$\Longleftrightarrow p \text{ splits completely in } L.$$

Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of a real algebraic integer which generates L over K. He further claimed by making use of class field theory [2, Proposition 5.29] that if p does not divide the discriminant of $f(X)$, then

$$p \text{ splits completely in } L$$
$$\Longleftrightarrow (-n/p) = 1 \text{ and } f(X) \equiv 0 \pmod{p} \text{ has an integer solution.}$$

His work extends the classical one for $N = 1$ [2, Theorem 9.2], however, he did not present any algorithm how to construct a primitive generator of such field L over K.

In this paper we shall first show that L is in fact the compositum of the ring class field of the order $\mathcal{O} = [N\sqrt{-n}, 1]$ and the ray class field modulo $N\mathcal{O}_K$ (Theorem 3.5). Then, we shall theoretically construct a primitive generator of L over K as a real algebraic integer by combining two classical generators (Theorem 4.6 and Corollary 4.7). To this end we shall make use of some consequences of the main theorem of complex multiplication and Shimura's reciprocity law. Lastly, we shall give several concrete examples on these Diophantine equations in terms of the special values of primitive generators of the function fields of some modular curves (Examples 4.12, 4.13 and 4.14).

2. Modular functions

Let N be a positive integer and Γ be one of the following congruence subgroups

$$\Gamma_1(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \pmod{N}\},$$
$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \pmod{N}\}.$$

Then the group $\overline{\Gamma} = \langle \Gamma, \pm I_2 \rangle / \{\pm I_2\}$ acts on the complex upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ by fractional linear transformations, and the orbit space

$$X(\Gamma) = \overline{\Gamma} \backslash (\mathbb{H} \cup \mathbb{Q} \cup \{i\infty\})$$

for the left action of $\overline{\Gamma}$ can be given the structure of a compact Riemann surface [10, Chapter 1]. We call $X(\Gamma)$ the *modular curve* for Γ and also denote it by $X_1(N)$ or $X(N)$ according as $\Gamma = \Gamma_1(N)$ or $\Gamma(N)$. If $\mathbb{C}(X(\Gamma))$ denotes the field of all meromorphic functions on $X(\Gamma)$, then we have the inclusion $\mathbb{C}(X_1(N)) \subseteq \mathbb{C}(X(N))$. Observe that every function in $\mathbb{C}(X(\Gamma))$ has the Fourier expansion with respect to $q^{1/N}$, where $q = e^{2\pi i\tau}$ [10, §2.1]. In particular, since $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma_1(N)$, every function in $\mathbb{C}(X_1(N))$ has the Fourier expansion with respect to q. We further let $\mathbb{Q}(X(\Gamma))$ be the field of all functions in $\mathbb{C}(X(\Gamma))$ whose Fourier expansions with respect to $q^{1/N}$ have rational coefficients.