Commun. Korean Math. Soc. **21** (2006), No. 3, pp. 577–586

ON THE PUBLIC KEY CRYPTOSYSTEMS OVER CLASS SEMIGROUPS OF IMAGINARY QUADRATIC NON-MAXIMAL ORDERS

YONGTAE KIM AND CHANG HAN KIM

ABSTRACT. In this paper we will propose the methods for finding the non-invertible ideals corresponding to non-primitive quadratic forms and clarify the structures of class semigroups of imaginary quadratic orders which were given by Zanardo and Zannier [8], and we will give a general algorithm for calculating power of ideals/classes via the Dirichlet composition of quadratic forms which is applicable to cryptography in the class semigroup of imaginary quadratic non-maximal order and revisit the cryptosystem of Kim and Moon [5] using a Zanardo and Zannier [8]'s quantity as their secret key, in order to analyze Jacobson [7]'s revised cryptosystem based on the class semigroup which is an alternative of Kim and Moon [5]'s.

1. Introduction

Gauss [4] classified the quadratic forms with rational coefficients using theory of composition without mentioning the relation between ideals and forms. Cox [2] proved that there is an isomorphism between the form class group and the ideal class group of the non-maximal order using the Dirichlet composition of quadratic forms. He, however, didn't explain the class semigroup of non-maximal order. Zanardo and Zannier [8] have given the structure of the class semigroup of non-maximal order as finitely disjoint union of groups with some quantities which was discussed by Kim [6] and Jacobson [7] on the quantities. Buchmann [1] proposed a public key cryptosystem making use of ideals of the maximal orders in quadratic fields which may pave the way for a public key cryptosystem using imaginary quadratic non-invertible ideals as generators.

Received May 18, 2005.
2000 Mathematics Subject Classification: 11Y40, 94A60.
Key words and phrases: class semigroup, power of ideals, key exchange system.

In this paper we discuss the methods for finding non-invertible ideals corresponding to non-primitive quadratic forms, and we will constitute the explicit formulas calculating power of ideals/classes in the class semigroup of imaginary quadratic non-maximal order. Chapter 2 contains some preliminaries necessary to this paper. Chapter 3 consists of a lemma concerning the methods for constructing invertible or non-invertible ideals and a corollary to the lemma involving the contents for certain type of idempotent class in the class semigroup. In particular, we will give a theorem for clarifying the structures of class semigroup. In chapter 4, we establish the explicit formulas for powering ideals/classes via the Dirichlet composition which are applicable to cryptography (e.g. Diffie-Hellman cryptosystem [3]) in imaginary quadratic non-maximal order. We will revisit the cryptosystem of Kim and Moon [5] and analyze Jacobson [7]'s revised cryptosystem based on class semigroups in chapter 5.

2. Preliminaries

In this chapter, we introduce some facts concerning class semigroup in imaginary quadratic field. Throughout this paper, most of the terminologies are due to Gauss [4] and notations and some preliminaries are due to Cox [2] and Zanardo and Zannier [8] and the notations O, $\mathcal{Z}$ and $\mathcal{Q}$ denote the imaginary quadratic non-maximal order, the ring of integers and the field of rational numbers respectively. Let $D_1 < 0$ be a square free rational integer and set $D = 4D_1/r^2$, where $r = 2$ if $D_1 \equiv 1 \bmod 4$ and $r = 1$ if $D_1 \equiv 2, 3 \bmod 4$. Then $K = \mathcal{Q}(\sqrt{D_1})$ is an imaginary quadratic field of discriminant D. Note that $K = \mathcal{Q}(\sqrt{D})$. If $\alpha, \beta \in K$, we denote by $[\alpha, \beta]$ the set $\alpha\mathcal{Z} + \beta\mathcal{Z}$. Then an order in K having conductor f with discriminant $D_f = f^2 D$ is denoted by $O = [1, f\omega]$, where $\omega = (D + \sqrt{D})/2$. An (integral) ideal A of O is a subset of O such that $\alpha + \beta \in A$ and $\alpha\lambda \in A$ whenever $\alpha, \beta \in A, \lambda \in O$. For $\alpha \in K, \alpha', N(\alpha)$ and $Tr(\alpha)$ denote the complex conjugate, norm and trace of α respectively. Let $\gamma = f\omega$. Then any ideal A of O (any O-ideal) is given by $A = [a, b + c\gamma]$, where $a, b, c \in \mathcal{Z}$, $a > 0, c > 0$, $c \mid a, c \mid b$ and $ac \mid N(b + c\gamma)$. If $c = 1$, then A is called primitive, which means that A has no rational integer factors other than 1. Then $A = [a, b + \gamma]$ is O-ideal if and only if a divides $N(b + \gamma)$. We say that A and B are equivalent ideals of O and denote $A \sim B$ if there exist non-zero $\alpha, \beta \in K$ such that $(\alpha)A = (\beta)B$ (this relation actually is equivalent relation). We denote the equivalence class of an ideal A by

$\overline{A}$. Let $I(O)$ be the set of non-zero fractional ideals of O and $P(O)$ the set of non-zero principal ideals of O. Then $Cls(O) = I(O)/P(O)$ will be the class semigroup of the order O.

3. Structure of $Cls(O)$

In this chapter we discuss some generalizations of the facts, discussed by Gauss [4] and Cox [2], for quadratic forms, orders and ideals. For convenience, we will set the positive definite quadratic form $u(x,y) = ax^2 + bxy + cy^2$ as (a,b,c) for brevity, and call η the root of $u(x,y)$ if $u(\eta,1) = 0$ and η lies in the upper half plane $\mathcal{H}$. We begin with introducing a lemma due to Cox [2].

LEMMA 3.1. (Confer [2, Proposition 7.4]) *Let O be an order in a imaginary quadratic field K, and let A be a fractional O-ideal. Then*

$$\{\beta \in K \mid \beta A \subset A\} = O$$

if and only if A is invertible.

We now generalize Theorem 7.7 in [2] in order to apply quadratic non-invertible ideals to some cryptography.

LEMMA 3.2. *Let $u(x,y) = (a,b,c)$ be a positive definite quadratic form with discriminant D_f, where $k = \gcd(a,b,c)$. Let η be the root of $u(x,y)$. Then the ideal $[a,a\eta]$ is invertible ideal if $k = 1$ and is non-invertible if $k > 1$ in the order $O = [1,\gamma]$ of K.*

PROOF. Firstly, we note that $[1,a\eta]$ is an order of K, since $a\eta$ is an algebraic integer. Now, we can show whether $[a,a\eta]$ is a invertible ideal or not in $[1,a\eta]$ according to $k = 1$ or not. For a given $\beta \in K$, $\beta[a,a\eta] \subset [a,a\eta]$ is equivalent to $\beta a \in [a,a\eta]$ and $\beta(a\eta) \in [a,a\eta]$. Since $a\beta$ belongs to $[a,a\eta]$, we then have $a\beta = ma+n(a\eta)$, that is , $\beta = m+n\eta$ for some rational integers m and n.

Conversely, for any rational integers m and n, $a(m+n\eta)$ clearly belongs to $[a,a\eta]$. For the second, note that

$$\beta(a\eta) = ma\eta + na\eta^2 = ma\eta + n(-b\eta - c) = -nc + (ma - nb)\eta.$$

Thus, $\beta(a\eta) \in [a,a\eta]$ if and only if $a \mid nc$ and $a \mid nb$ and m is arbitrary. If $k = 1$, then $a \mid n$. However if $k > 1$, then $\gcd(a,b)$ and $\gcd(a,c) \geq k$. There thus exist an non-trivial divisor s of a and arbitrary rational integer m such that $a\eta(m+s\eta) \in [a,a\eta]$. These facts tell us,

$$\{\beta \in K \mid \beta[a,a\eta] \subset [a,a\eta]\} = [1,a\eta]$$

if and only if $k = 1$. Therefore $[a, a\eta]$ is invertible in $[1, a\eta]$ if $k = 1$ and non-invertible if $k > 1$ by Lemma 3.1. Since f is the conductor of O with discriminant D_f, $a\eta = -(b + fD)/2 + \gamma$. Since fD and b have the same parity, we have $(b + fD)/2 \in \mathcal{Z}$. It follows that $[1, a\eta] = [1, \gamma]$ and thus $[a, a\eta] = [a, -(b + fD)/2 + \gamma]$ is an O-ideal. □

In particular, if $a = k$, then we denote the ideal $[k, k\eta]$ by E_k. For a quadratic form $u(x, y) = (a, b, c)$, we define $\gcd(u(x, y)) = \gcd(a, b, c)$, $u_1(x, y) = 1/\gcd(u(x, y))u(x, y)$, $\gcd(I) = \gcd(a, Tr(b+\gamma), N(b+\gamma)/a)$ and $Tr(b+\gamma)^2 - 4N(b+\gamma)$, the discriminant of I, for a non-zero O-ideal $I = [a, b + \gamma]$.

COROLLARY 3.3. *For any divisor $k \mid f$, we have $E_k = [k, \gamma]$.*

PROOF. Let $u(x, y) = (k, kb_1, kc_1)$ with discriminant D_f , where $f = kd$. Then $k\eta - \gamma \in k\mathcal{Z}$ since b_1 and dD are same parity. Therefore $[k, k\eta] = [k, \gamma]$. □

To clarify the structure of $Cls(O)$, we need the following two Lemmas.

LEMMA 3.4. ([8, Theorem 10]) *Let $I = [a, b+\gamma]$ be a non-zero O-ideal and $\gcd(I) = k$. Then we have $E_k^2 = kE_k, II' = aE_k, IE_k = kI$.*

LEMMA 3.5. *Suppose I and J are O-ideals with same discriminant D_f such that $\gcd(I) = k_1, \gcd(J) = k_2$. Then $\gcd(IJ) = lcm(k_1, k_2)$.*

PROOF. Suppose that $u(x, y)$ and $v(x, y)$ be positive definite quadratic forms with discriminant D_f corresponding to I and J respectively. Let $u(x, y) = k_1u_1(x, y)$ and $v(x, y) = k_2v_1(x, y)$, where $k_1 = \gcd(u(x, y))$ and $k_2 = \gcd(v(x, y))$. Then if $f = k_1d_1 = k_2d_2$ by Lemma 3.4, then $u_1(x, y)$ and $v_1(x, y)$ are primitive with discriminant d_1^2D and d_2^2D respectively. From Gauss[4, art.236], the direct composition $U_1(x, y)$ of $u_1(x, y)$ and $v_1(x, y)$ has the discriminant d^2D, where $d = \gcd(d_1, d_2)$. Then from elementary number theory $f = kd$, where $k = lcm(k_1, k_2)$. Therefore if we denote $U(x, y)$ the direct composition of $u(x, y)$ and $v(x, y)$, then $\gcd(U(x, y)) = k$. This completes the proof. □

Here we need to prove an important property of $\gcd(I)$.

LEMMA 3.6. (See also [8, Proposition 13]). *If $I = [a, b + \gamma]$ is a non-zero primitive O-ideal, then $\gcd(I)$ divides f.*

PROOF. Let $k = \gcd(I)$ for brevity. Since I is an primitive -ideal, a divides $N(b+\gamma)$, and thus k divides a and $k^2 \mid N(b+\gamma)$ and $k|Tr(b+\gamma)$. If we choose an element $\theta = 1/k(b+\gamma) \in K$, then $Tr(\theta) = 1/kTr(b+\gamma)$

and $N(\theta) = 1/k^2 N(b+\gamma)$, which are both rational integers, since $k^2 \mid N(b+\gamma)$ and $k \mid Tr(b+\gamma)$. Therefore θ is an algebraic integer and thus is contained in the maximal order $[1, \omega]$. Consequently k divides both b and f. □

For the structure of $Cls(O)$, Michael [7] proposed [7, Proposition 2.3] instead of [8, Proposition 14]. [7, Proposition 2.3] is right, however, the proof is somewhat ambiguous. Because, [8, Proposition 14] says only that $G_\alpha G_\beta$ contained in G_δ,where $\delta = lcm(\alpha, \beta)$(Corollary 3.5 of this paper is equivalent to that). So, we will need a necessary and sufficient condition for clarifying the group G_δ. It is well-known that the cardinality of $Cls(O)$ is finite. Thus we have the following.

THEOREM 3.7. *The class semigroup* $Cls(O) = \cup_{k|f} G_{\overline{E_k}}$, *where* $G_{\overline{E_k}}$ *is the set of all classes containing* O*-ideals* A*'s such that* $\gcd(A) = k$.

PROOF. From Lemma 3.4, we have $Cls(O)$ is a commutative Clifford semigroup. Equivalently $Cls(O)$ is a finitely disjoint union of groups of the form G_e's, where e is an idempotent element of $Cls(O)$, and there exists a homomorphism between groups. It is well-known that $G_{\overline{E_k}} = \{\overline{A} \mid \overline{AE_k} = \overline{A}$ and $\overline{AB} = \overline{E_k}$ for some $\overline{B} \in Cls(O)\}$ since $Cls(O)$ is the Clifford algebra. We claim that $G_{\overline{E_k}}$ is the set of all classes containing O-ideal A's such that $\gcd(A) = k$. In fact; For any O-ideal A, $\gcd(A)$ divides f by Lemma 3.6. Suppose that $\gcd(A) = k$, then $\overline{A} \in G_{\overline{E_k}}$ by Lemma 3.4. Conversely suppose that $\overline{B} \in G_{\overline{E_k}}$ with $\gcd(B) = h$. Then $\overline{BB'} = \overline{E_k}$ by Lemma 3.4. Note that $\gcd(A) = \gcd(A')$. Therefore $\gcd(AA') = \gcd(A)$ by Lemma 3.5. Consequently $h = \gcd(B) = \gcd(BB') = \gcd(E_k) = k$. This completes the proof □

In Kim [6, Remark 3.9(a)], we can find an explicit counterexample for [8, Proposition 12]. Combining Lemma 3.5 and Theorem 3.7, we have the following.

COROLLARY 3.8. *If two ideal classes* $\overline{A}$ *and* $\overline{B}$ *belong to* $G_{\overline{E_k}}$ *and* $G_{\overline{E_h}}$ *respectively, then* $\overline{AB}$ *belongs to* $G_{\overline{E_l}}$, *where* $l = lcm(k, h)$.

4. Powering ideals/classes via the Dirichlet composition

In this chapter, we will calculate power of an ideal via the Dirichlet decomposition which is applicable to public key cryptosystems directly. From Gauss' work [4], we notice that if two primitive quadratic forms $u(x, y)$ and $v(x, y)$ are positive definite with discriminant D_f, then their

Dirichlet composition $U(x,y)$ will be positive definite of discriminant D_f and moreover, $U(x,y)$ is the direct composition(in the sense of Gauss) of $u(x,y)$ and $v(x,y)$ of discriminant D_f. We now give an efficient method for powering an ideal/class in O, which is the generalization of Cox [2, Theorem 7.7].

THEOREM 4.1. *Let $u(x,y) = (a,b,c) = (ka_1, kb_1, kc_1)$ be a positive definite quadratic form with $k = \gcd(u(x,y))$, discriminant D_f and $\gcd(a_1,b_1) = 1$. Let I be an O-ideal corresponding to $u(x,y)$. Then, for any natural number x, we have $I^x = k^{x-1}[ka_1^x, \mu]$, where $\mu = (-kW + f\sqrt{D})/2$ for a unique rational integer W modulo $2a_1^x$ and the ideal class containing I^x is $\overline{[ka_1^x, \mu]}$.*

PROOF. Note that $\overline{I} \in G_{\overline{E_k}}$ and thus $\overline{I}^x \in G_{\overline{E_k}}$ by Corollary 3.8 and the Dirichlet composition of a primitive quadratic form is primitive with the same discriminant as the quadratic form. Let's denote $U_1^{x+1}(x,y)$ the Dirichlet composition of $u_1(x,y)$ with itself x times for any natural number x and $U^x(x,y) = kU_1^x(x,y)$. We will prove the theorem using mathematical induction on the exponent x. Let $u_1(x,y) = (a_1,b_1,c_1)$ and $f = kd$, since $k \mid f$ by Lemma 3.6. Then $u_1(x,y)$ is primitive with discriminant d^2D. Therefore we can calculate the Dirichlet composition of $u_1(x,y)$ with itself. In fact, we can find the unique rational integer T modulo $2a_1^2$ satisfying the following system of congruences (confer [2, Lemma 3.2])

$$\begin{aligned} T &\equiv b_1 \bmod 2a_1 \\ T^2 &\equiv d^2D \bmod 4a_1^2, \end{aligned} \tag{1}$$

since $\gcd(a_1,b_1) = 1$. Then $U_1^2(x,y) = (a_1^2, T, C)$ and $U^2(x,y) = (ka_1^2, kT, kC)$, where $C = (T^2 - d^2D)/4a_1^2$ and $\gcd(a_1, (b_1+T)/2) = 1$ since $\gcd(a_1,b_1) = 1$. Note that the discriminants of $U_1^2(x,y)$ and $U^2(x,y)$ are d^2D and D_f respectively. Multiplying each congruence of (1) by k or k^2, we obtain the following

$$\begin{aligned} kT &\equiv b \bmod 2a \\ k^2T^2 &\equiv D_f \bmod 4a^2. \end{aligned} \tag{2}$$

Let τ_1 and τ_2 be the roots of $u_1(x,y)$ and $U_1^2(x,y)$ respectively. Then the ideals corresponding to $u_1(x,y)$ and $U_1^2(x,y)$ are $[a_1, a_1\tau_1]$ and $[a_1^2, \tau]$ respectively, where $\tau = a_1^2\tau_2$, by Lemma 3.2. Note that $[a_1, a_1\tau_1]^2 = [a_1^2, \tau]$ (confer [2,Theorem 7.7]). Similarly, the ideals corresponding to $u(x,y)$ and $U^2(x,y)$ are $[a, a\tau_1]$ and $[ka_1^2, k\tau]$ respectively by Lemma 3.2.

Simple calculation shows that $[a, a\tau_1] = [a, k\tau]$ and $(k\tau)^2 = -k^2T\tau \bmod a^2$ by the system of congruences (2). Thus

$$[a, a\tau_1]^2 = [a, k\tau]^2 = [a^2, ak\tau, -k^2T\tau] = [a^2, k^2\tau] = k[ka_1^2, k\tau],$$

since $\gcd(a_1, T) = 1$. Let S modulo $2a_1^3$ be the unique rational integer satisfying the following system of congruences

$$\begin{aligned} S &\equiv b_1 \bmod 2a_1 \\ S &\equiv T \bmod 2a_1^2 \\ S^2 &\equiv d^2D \bmod 4a_1^3. \end{aligned} \tag{3}$$

Then $U_1^3(x, y) = (a_1^3, S, C)$ and $U^3(x, y) = (ka_1^3, kS, kC)$ with discriminant d^2D and D_f respectively, where $C = (S^2 - d^2D)/4a_1^2$ and $\gcd(a_1, (b_1 + S)/2) = 1$. Let μ_1 be the root of $U_1^3(x, y)$ and $\mu = a_1^3\mu_1$. Then the corresponding ideal to $U_1^3(x, y)$ is $[a_1^3, \mu]$. Therefore

$$[a, a\tau_1]^3 = [a, a\tau_1][a, a\tau_1]^2 = k^3[a_1, \mu][a_1^2, \mu] = k^2[ka_1^3, k\mu].$$

Inductively $U_1^x(x, y) = (a_1^x, W, C)$ with discriminant d^2D and $U^x(x, y) = (ka_1^x, kW, kC)$ with discriminant D_f, where $C = (W^2 - d^2D)/4a_1^x$ and $\gcd(a_1, (b_1 + W)/2) = 1$ and W is uniquely determined by the system of congruences similar to (3). If we set θ the root of $U_1^x(x, y)$, then we can obtain $[a, a\tau]^x = k[ka_1^x, ka_1^x\theta]$ by the same procedure above. This completes the proof. □

Slight modification of [2, Theorem 2.8] tells us that every positive definite form is properly equivalent to the unique reduced form, and thus every O-ideal can be transformed to a unique reduced O-ideal of the form $I = [a, b + \gamma]$. From these facts, commutativity, associativity of Dirichlet composition(see also [4, art. 240, 241]) and Theorem 3.6, we have the following.

COROLLARY 4.2. *Suppose that $u(x, y)$ is the quadratic form as defined in Theorem 4.1. Then $(\overline{u(x, y)}^x)^y = (\overline{u(x, y)}^y)^x$ and thus $(\bar{I}^x)^y = (\bar{I}^y)^x$ for any O-ideal I.*

The facts above can be applicable to public key crpytosystems based on the quadratic non-maximal order by choosing non-invertible ideals as generators.

5. Analyses of some public key cryptosystems

In this chapter, we discuss some facts concerning the secret key chosen by Kim and Moon [5, p.492] and the analysis of Kim and Moon [5]'s cryptosystem proposed by Michael [7].

(a) Analysis of Kim and Moon's key-exchange system by Kim [6]

In [6, Lemma 3.9(b)], Kim [6] attacks Kim and Moon [5]'s cryptosystem as follows.

The class $\overline{I}$ of the generator I in Kim and Moon's system belongs to $G_{\overline{E_k}}$ for some divisor k of f(confer Theorem 3.7). Then $\gcd(I) = k$. However, any power of I is equivalent to a unique reduced ideal T with the same $\gcd(T) = k$ since $\overline{T}$ belongs to $G_{\overline{E_k}}$ by Corollary 3.8. Therefore their cryptosystem can be broken trivially since they use their secret key as $\gcd(I)$.

(b) Analysis of Jacobson [7]'s revised cryptosystem

To analyze the revised cryptosystem, we introduce the following theorem due to Zanardo and Zannier [8].

THEOREM 5.1. (Confer [8, Theorem 16]) *Let $E_k = [k, \gamma]$, where $k \mid f$, and let I be an O-ideal such that $\overline{I} \in G_{\overline{E_k}}$. Then $JE_k = kI$ for some invertible ideal J.*

In [7], Jacobson analyze Kim and Moon [5]'s cryptosystem by finding out the same misconceptions as Kim [6]'s, and propose the revised cryptosystem as follows(confer [7, chapter 4]).

1. Revised cryptosystem

Given ideals I_1, I_2 with $\overline{I}_1, \overline{I}_2 \in G_{\overline{E_k}}$, find $x \in \mathcal{Z}$ such that $I_2 \sim I_1^x$.

To find preimages of $\overline{I}_1$ and $\overline{I}_2$ under ϕ_k - invertible ideals J_1 and J_2 such that $\phi_k(\overline{J}_1) = \overline{I}_1$ and $\phi_k(\overline{J}_2) = \overline{I}_2$. If there exists $y \in \mathcal{Z}$ such that $J_1 \sim J_2^y$ in $G_{\overline{E_1}}$, then because ϕ_k is a homomorphism $I_1 = I_2^y$, i.e., y is also a solution of the discrete logarithm problem in $G_{\overline{E_k}}$. Theorem 16 of [8] describes an algorithm for computing the required preimages given only a representative of an ideal class in $G_{\overline{E_k}}$ and k. In general, $| G_{\overline{E_k}} | < | Cl(D_f) |$ means that the preimages J_1 and J_2 are not unique. It is thus possible that J_1 does not have a discrete logarithm with respect to J_2. The procedure for computing preimages by changing under ϕ_k can be randomized by changing the representative of the ideal equivalence class. If the first chosen preimages does not yield discrete logarithm, the process is simply repeated until it is found. Therefore computing discrete

logarithm in $Cls(O)$ is no harder than computing discrete logarithm in $Cl(O)$.

2. Analysis

The algorithm in Theorem 5.1, however, ensures the only one preimage under the algorithm of a representative ideal, and this is seriously different from the facts claimed by Jacobson [7]. In fact, Zanardo and Zannier [8] prove the theorem only to claim the surjectivity of a homomorphism. So, the algorithm of Theorem 5.1 can calculate a particular preimage in $G_{\overline{E}_1}$ of a given ideal in $G_{\overline{E}_k}$, that is, it can not find all the preimages of a given representative ideal. Thus the preimages under this algorithm of the other representative ideal can fall into the same class of preimages of a given representative. On the other hand, the "preimages of ϕ_k" mentioned by Jacobson means the whole set of preimages of ϕ_k. This is the difference between the algorithm of Theorem 5.1 and ϕ_k. If we, therefore, want to find the whole preimages under ϕ_k of a representative ideal, then we have to test all the ideals in $Ker(\phi_k)$ in the worst case. Since the class number of the order D_f is generally larger that of the order D_1, the size of $Ker(\phi_k)$ may not be sufficiently small. In other word, there is no known efficient algorithm for finding all the preimages under ϕ_k of a given representative ideal using Theorem 5.1. So, his claim on the comparison of securities between $Cls(O)$ and $Cl(O)$ will not be correct.

References

[1] J. Buchmann and H. C. Williams, *A key-exchange system based on imaginary quadratic fields*, J. Cryptology **1** (1988), 107–118.

[2] D. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, New York, 1989.

[3] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. on Inform. Theory **22** (1976), 472–492.

[4] C. F. Gauss, *Disquisitiones Arithmeticae* , translated by Clarke A. A., Springer-Verlag, New York, 1986.

[5] H. Kim and S. Moon, *Public-Key Cryptosystems based on Class Semigroups of Imaginary Quadratic Non-maximal Orders*, ASISP 2003, LNCS 2727 (2003), 488–497.

[6] Y. Kim, *On the structures of class semigroups of quadratic non-maximal orders*, Honam Mathematical Journal **26** (2004), no. 3, 247–256.

[7] Michael J. Jacobson, Jr., *The security of cryptosystems based on class semigroups of imaginary quadratic non-maximal orders* ASISP 2004, LNCS 3108 (2004), 149–156.

[8] P. Zanardo and U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Camb.Phil. Soc. **115** (1994), 379–391.

Yongtae Kim
Department of Mathematics Education
Gwangju National University of Education
Gwangju 500-703, Korea
E-mail: ytkim@gnue.ac.kr

Chang Han Kim
Department of Information Security
Semyung University
Chungbuk 390-711, Korea
E-mail: chkim@semyung.ac.kr