MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 33 Nos. 1-2 (2010) pp. 1-6

The quadratic fields with discriminant divisible by exactly three primes and with subgroup of ideal class group isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$

CHRISTOPHER F. SANTOS
Institute of Mathematics
University of the Philippines Diliman
Quezon City, Philippines
cfsantos@math.upd.edu.ph

JULIUS M. BASILLA
Institute of Mathematics
University of the Philippines Diliman
Quezon City, Philippines
jbasilla@math.upd.edu.ph

Abstract

Let m be a square-free integer and let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with discriminant d divisible by exactly three distinct primes. Results on elementary Gauss-genus theory implies that the Sylow 2-subgroup of the ideal class group H^+ in the narrow sense of K is isomorphic to $\frac{\mathbb{Z}}{2^k\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2^l\mathbb{Z}}$ for some nonnegative integers k and l. In this paper, we give sufficient and necessary conditions under which H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$.
Keywords: Gauss Genus Theorem, ideal class group, quadratic field

1 Review of Related Literature

Let m be a square-free integer and K be the quadratic field $\mathbb{Q}(\sqrt{m})$ with discriminant d and let $\mathcal{O}_K$ denote its ring of integers. For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, we write $\mathfrak{a} \cong \mathfrak{b}$, if there exists nonzero integers α and β in $\mathcal{O}_K$ with norm $N(\alpha\beta) > 0$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. It can be shown that $\cong$ is an equivalence relation of ideals in $\mathcal{O}_K$ and the equivalence classes induced by this relation forms an abelian group H^+ called the narrow ideal class group of K([7, 8, 9]). The order h^+ of H^+ is called the narrow class number of K.

For brevity, we write $\mathfrak{a} \cong \square$ if there exist an ideal $\mathfrak{b}$ such that $\mathfrak{a} \cong \mathfrak{b}^2$.

The study of the Sylow 2-subgroup G of the narrow ideal class group of K can be traced back to Gauss([6]). Hasse ([7]) proposed a method for computing G using Legendre theorem but the method requires decomposition of many integers to its prime factorization([2, 9]). Shanks([15]), Bosma and Stevenhagen ([1]) calculated G using Gauss' ternary quadratic form but they did not use the ideal theory directly so they were not able to calculate G in the wide sense. Basilla and Wada([5]) proposed a faster method for computing G.

Using class field theory, Redei and Reichard ([13]) were able to show the necessary and sufficient conditions for the narrow class number of a quadratic field with discriminant divisible by exactly 2 primes say p and q to be divisible by 4. Scholz([14]) and Kaplan([10]),

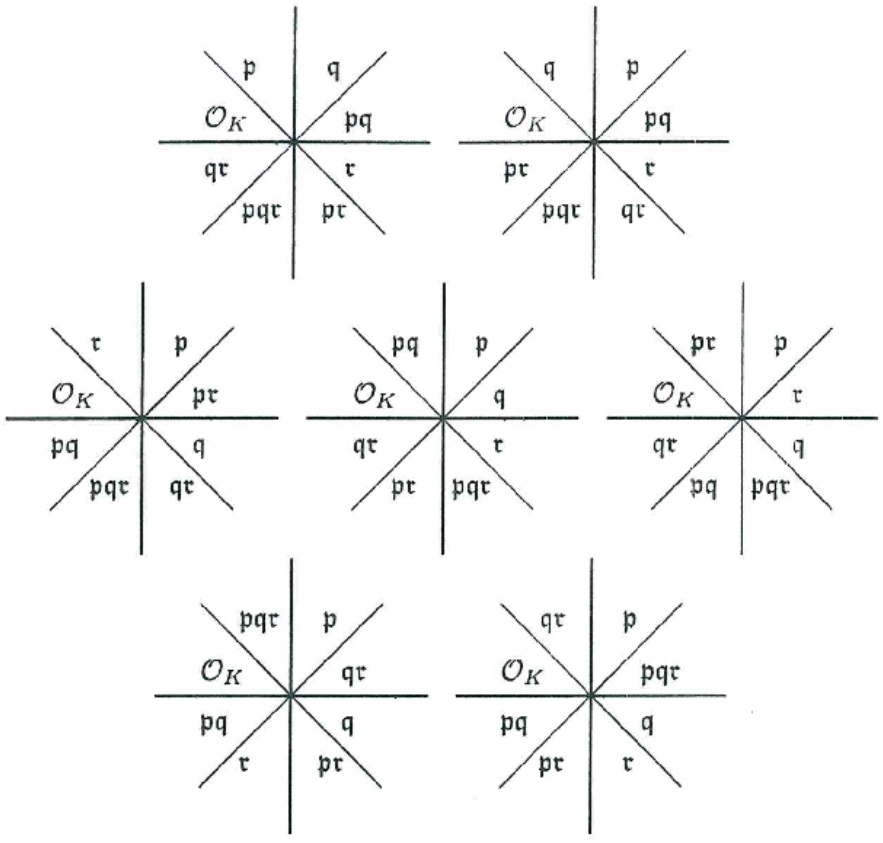
working separately and applying different methods, have extended these results by arriving at a sufficient and necessary conditions so that the narrow class number of a field with discriminant divisible by exactly 2 primes will be divisible by 8.

Nemenzo([11]) and Basilla([3]) were able to verify the results of Scholz using Ideal Theory and Legendre's theorem on the solvability of the Diophantine equation $ax^2 + by^2 = z^2$([9]).

In this paper, we extend these results to the case where the discriminant is divisible by exactly three primes following the approaches of Nemenzo, Basilla and Wada.

2 A note on quadratic fields with discriminant divisible by exactly three primes

Let $K = \mathbb{Q}(\sqrt{m})$, m a square-free integer, be quadratic field with discriminant d divisible by exactly three distinct primes p, q, r. We denote the prime ideals lying over p, q and r by $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ respectively. Then the eight ambiguous primitive ideals in $\mathcal{O}_k$ are $\mathcal{O}_K$, $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, $\mathfrak{pq}$, $\mathfrak{pr}$, $\mathfrak{qr}$, $\mathfrak{pqr}$ and these eight primitive ambiguous ideals are segregated into four ambiguous classes with each ambiguous class containing two primitive ambiguous ideals (cf. [12]). We therefore have the following seven possibilities.



The diagrams above mean that primitive ideals belonging to the same quadrant are equivalent in the narrow sense, or are in the same ambiguous class. For instance the upper leftmost diagram means that $\mathcal{O}_K \cong \mathfrak{p}$,$\mathfrak{q} \cong \mathfrak{pq}$, $\mathfrak{r} \cong \mathfrak{pr}$ and $\mathfrak{pqr} \cong \mathfrak{qr}$.

The ambiguous ideal classes are precisely the elements of the ideal class group of order 2 ($x^2 \equiv 1$). By repeatedly taking the square roots of each of the primitive ambiguous

ideals $\mathcal{O}_K$, $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, $\mathfrak{pq}$, $\mathfrak{pr}$, $\mathfrak{qr}$ and $\mathfrak{pqr}$, we can determine the largest power of 2 dividing the narrow class number of $\mathbb{Q}(\sqrt{m})$ and the distribution of the primitive ambiguous ideals on the ambiguous ideal classes (cf. [5]). In order to determine the sufficient and necessary condition for the narrow class number to be divisible by a power of 2, we need to count how many times we can take the square roots iteratively of the primitive ambiguous ideals.

In addition, the principal ideal $(\sqrt{m})$ is among these eight primitive ambiguous ideals. If the norm of the fundamental unit is -1, the equivalence classes in the wide sense and in the narrow sense coincides. This forces $(\sqrt{m}) \cong \mathcal{O}_K$. Hence, if $(\sqrt{m}) \ncong \mathcal{O}_K$, we conclude that the norm of the fundamental unit is 1. Also for imaginary quadratic fields ($m < 0$), the equivalence classes in the wide sense and in the narrow sense always coincides. Hence, we always have $(\sqrt{m}) \cong \mathcal{O}_K$. This makes the imaginary cases simpler than the real cases as we shall see for the remainder of the paper.

3 Sufficient and necessary conditions for an ideal to be equivalent to a square

We now determine sufficient and necessary conditions under which the ideals $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ will be equivalent to a square. Thus we need a criterion for an ideal to be equivalent to a square. This fact is taken care of by following theorem:

Theorem 1. *Let $\mathfrak{a} = [a, b+\omega]$ be an ideal in $\mathbb{Q}(\sqrt{m})$ and let a_1 denote the square-free part of a. Then $\mathfrak{a} \cong \square$ if and only if for all odd prime p dividing m, we have*

$$\left(\frac{a_1}{p}\right) = 1 \text{ if } p \nmid a_1 \quad \text{and} \quad \left(\frac{-a_1 m/p^2}{p}\right) = 1 \text{ if } p \mid a_1 \text{ (cf. [4]).}$$

We obtain the following corollaries.

Corollary 2. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with discriminant d divisible by a prime p and let $\mathfrak{p}$ be a prime ideal lying over p. Then $\mathfrak{p} \cong \square$ if and only if $\left(\frac{-\frac{m}{p}}{p}\right) = 1$ and for all odd prime q dividing d and $q \neq p$,we have $\left(\frac{p}{q}\right) = 1$.*

Corollary 3. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with and even discriminant d and let $\mathfrak{p}$ be the prime ideal lying over 2. Then $\mathfrak{p} \cong \square$ if and only if for all odd prime p dividing d, $\left(\frac{2}{p}\right) = 1$.*

4 Main Results

We now give a sufficient and necessary criteria for the narrow class number H^+ to contain a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$, when the discriminant d is divisible by 3 distinct primes, say p, q and r. This calls for establishing a sufficient and necessary criterion for the primes lying over p, q and r to be equivalent to the square of some ideal.

Proposition 4. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with discriminant $d \equiv 1 \pmod 4$ and divisible by exactly 3 distinct primes p, q and r. Then H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$ if and only if $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$ and at least two of p, q and r are congruent 1 modulo 4.*

Proof. If $m = pqr$, the ideal $\mathfrak{p} \cong \square$ if and only if $\left(\frac{-qr}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1$. Likewise, the ideal $\mathfrak{q} \cong \square$ if and only if $\left(\frac{-pr}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{q}{r}\right) = 1$ and the ideal $\mathfrak{r} \cong \square$ if and only if $\left(\frac{-pq}{r}\right) = \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Hence, if the ideals $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ are all equivalent to a square, we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = \left(\frac{q}{r}\right) = \left(\frac{r}{q}\right) = 1$. It also follows that at least two of p, q and r are conguent to 1 modulo 4. On the other hand, if at least 2 of p, q and r are congruent to 1 modulo 4, say $p \equiv q \equiv 1 \pmod 4$, and $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$, we obtain $\left(\frac{-qr}{p}\right) = 1$ and $\left(\frac{-pr}{q}\right) = 1$. Since $d \equiv 1 \pmod 4$, it follows that $r \equiv 1 \pmod 4$ and therefore $\left(\frac{-pq}{r}\right) = 1$.

If $m = -pqr$ then $r \equiv 3 \pmod 4$. In this case, the ideal $\mathfrak{p} \cong \square$ if and only if $\left(\frac{qr}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1$. Likewise, the ideal $\mathfrak{q} \cong \square$ if and only if $\left(\frac{pr}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{q}{r}\right) = 1$ and the ideal $\mathfrak{r} \cong \square$ if and only if $\left(\frac{pq}{r}\right) = \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Hence, if the ideals $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ are all equivalent to a square, we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = \left(\frac{q}{r}\right) = \left(\frac{r}{q}\right) = 1$. Conversely, if at least 2 of p, q and r is congruent to 1 modulo 4, say $p \equiv q \equiv 1 \pmod 4$, and $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$, we obtain $\left(\frac{qr}{p}\right) = 1$, $\left(\frac{pr}{q}\right) = 1$ and $\left(\frac{pq}{r}\right) = 1$. □

We now consider the case where 2, p and q are the distinct primes dividing d. If $\mathfrak{r}$ is a prime lying over 2, $\mathfrak{r} \cong \square$ if and only if $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1$. Hence, $\mathfrak{r} \cong \square$ if and only if $p \equiv 1$ or $7 \pmod 8$ and $q \equiv 1$ or $7 \pmod 8$.

Proposition 5. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with $m \equiv 3 \pmod 4$ and m divisible by exactly two distinct odd primes p and q. Then H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$ if and only if $m = -pq$, $p \equiv q \equiv 1 \pmod 8$, $\left(\frac{p}{q}\right) = 1$.*

Proof. Let $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ be the primes lying over p, q and 2 respectively. The ideal $\mathfrak{p} \cong \square$ if and only if $\left(\frac{\frac{-m}{p}}{p}\right) = \left(\frac{p}{q}\right) = 1$ and $\mathfrak{q} \cong \square$ if and only if $\left(\frac{\frac{-m}{q}}{q}\right) = \left(\frac{q}{p}\right) = 1$. Since $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$ and $\left(\frac{-p}{q}\right) = \left(\frac{-q}{p}\right) = 1$, then $p \equiv q \equiv 1 \pmod 4$. Hence, $m = pq$ is not possible. Thus $m = -pq \equiv 1 \pmod 4$. In view of the discussion preceding the proposition, $p \equiv q \equiv 1 \pmod 8$.

Conversely if $p \equiv q \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = 1$, we can show that $\left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1$. Thus $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ are all congruent to squares.

□

Proposition 6. *Let $K = \mathbb{Q}(\sqrt{m})$, $m = 2pq$ where p and q are distinct odd primes. Then H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$ if and only if $p \equiv q \equiv 1 \pmod 8$, $\left(\frac{p}{q}\right) = 1$.*

Proof. Let $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ be the primes lying over p, q and 2. The ideals $\mathfrak{p}$ and $\mathfrak{q}$ are equivalent to the square of some ideals if and only if $\left(\frac{-2q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{-2p}{q}\right) = 1$. Hence, at least one of p and $q \equiv 1 \pmod 4$.

Again, from the discussion preceding proposition 5, we must have $p \equiv 1$ or $7 \pmod 8$ and $q \equiv 1$ or $7 \pmod 8$. Without loss of generality, we assume that $p \equiv 1 \pmod 8$. Since $\mathfrak{q} \cong \square$, we have $\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{p}{q}\right) = 1$. Hence, $\left(\frac{-1}{q}\right) = 1$. Thus equivalently $q \equiv 1 \pmod 8$.

Conversely, if $p \equiv q \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = 1$ we have $\mathfrak{r} \cong \square$. Also, $\left(\frac{-2q}{p}\right) = \left(\frac{p}{q}\right) = 1$, so $\mathfrak{p} \cong \square$. Likewise, $\mathfrak{q} \cong \square$. Therefore, H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$. $\square$

Proposition 7. *Let $K = \mathbb{Q}(\sqrt{m})$, $m = -2pq$ where p and q are distinct odd primes. Then H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$ if and only if*

i. $p \equiv 1$,

ii. $q \equiv \pm 1 \pmod 8$, *and*

iii. $\left(\frac{p}{q}\right) = 1$.

Proof. Let $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ be the prime ideals lying over p, q and 2, respectively. The ideals $\mathfrak{p}$ and $\mathfrak{q}$ are equivalent to the square of some ideals if and only if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Thus, $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$. Without loss of generality we can assume $p \equiv 1 \pmod 4$. From the discussion preceding Proposition 5, we must have $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1$. It follows that $p \equiv 1 \pmod 8$.

Conversely, if the conditions $p \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = 1$ imply $\left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) = 1$ while the condition $q \equiv \pm 1 \pmod 8$ implies $\left(\frac{2}{q}\right) = 1$.

Thus, $\mathfrak{r} \cong \square$, $\mathfrak{p} \cong \square$, and $\mathfrak{q} \cong \square$; hence H^+ contains a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$. $\square$

These exhaust the quadratic fields with discriminant divisible by exactly three primes and with ideal class group containing a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$.

References

[1] W. Bosma and P. Stevenhagen, On the computation of quadratic 2-class groups, *J. Theorie des Nombres*, **8**(1996), 283-313.

[2] J.M. Basilla, On the solution of $x^2 + dy^2 = m$, *Proc. Japan Acad.*, **80A**(2004), 40-41.

[3] J.M. Basilla, The quadratic fields with discriminant divisible by exactly two primes and with "narrow" class number divisible by 8, *Proc. Japan Acad.*, **80A**(2004), 187-190.

[4] J.M. Basilla, On the Sylow 2-subgroup of the ideal class groups of quadratic fields and related Diophantine equations, Dissertation Sophia University Tokyo Japan, 2005.

[5] J.M. Basilla. and H. Wada, On efficient computation of the 2-parts of the ideal class groups of quadratic field, *Proc. Japan Acad.*, **80A**(2004), 191-193.

[6] C.F. Gauss, *Disquisitiones Arithmiticae*, Gerhard Fleischer, Leipzig, 1801.

[7] H. Hasse, An algorithm for determining the structure of the Sylow 2-subgroup of the divisor class group of a quadratic field, Symposia Mathematica **XV** (Convegno di Strutture in Corpi Algebrice) INDAM, Roma 1973, Acad. Press London 1975, pp. 341-352.

[8] E. Hecke, *Lectures on the theory of Algebraic Number Theory. Grad. Text in Math.*, Springer-Verlag, New York, 1981.

[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics 84*, Springer-Verlag, New York (1990), pp. 272-275.

[10] P. Kaplan, Divisibilité par 8 du nombr des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, *J. Math. Soc. Japan*, **25** (4), 596-608.

[11] F.R. Nemenzo, On a Theorem of Scholz on the class number of quadratic fields, *Proc Japan Acad*, **80A**(2004), 9-11.

[12] T. Ono, *An introduction to Algebraic Number Theory, 2 ed.*, Plenum Press, New York, 1990.

[13] L. Rédei and H. Reichard, Die Anzahl der durch 4 teilbaren invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.*, **170**(1934), 69-74.

[14] A. Scholz, Über die Lösbarket der Gleichung $t^2 - Du^2 = -4$, *Math Z*, **39**(1934), 95-111.

[15] D. Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, *Math. Comp. 25*, **116**(1971), 837-853.