On a theorem of Scholz on the class number of quadratic fields

By Fidel R. Nemenzo

Department of Mathematics, University of the Philippines
Diliman, Quezon City, 1101, Philippines
(Communicated by Shokichi Iyanaga, m. j. a., Feb. 12, 2004)

Abstract: Let p and q be distinct primes such that $p \equiv q \pmod 4$ and consider the quadratic field $K = \mathbf{Q}(\sqrt{pq})$. In this paper, we shall investigate the class group and determine the exact power of 2 dividing the class number of K using the theory of ideals and a theorem on the solvability of $ax^2 + by^2 = z^2$.

Key words: Quadratic fields; class number; residue characters.

1. Preliminaries. Let p and q be distinct primes congruent modulo 4 and K be the quadratic field $\mathbf{Q}(\sqrt{pq})$, with integer ring $\mathcal{O}_K$. Let H and H^+ denote the ordinary ideal class group and the "narrow" ideal class group of K, with class numbers h and h^+, respectively. The class numbers h and h^+ are equal whenever the fundamental unit ϵ of K has norm $N(\epsilon) < 0$. On the other hand, if $N(\epsilon) > 0$ then $2h = h^+$.

In [5], Scholz used class field theory to look at the structure of the class group of K and proved the following theorem.

Theorem 1.1. *Let p and q be distinct primes with $p \equiv q \pmod 4$ and h^+, h (in the narrow and wide sense, respectively) of the quadratic field $\mathbf{Q}(\sqrt{pq})$. Then:*

a) *If $p \equiv q \equiv 3 \pmod 4$ then $h^+ \equiv 2 \pmod 4$ and h is odd.*

b) *If $p \equiv q \equiv 1 \pmod 4$ and $(p/q) = (q/p) = -1$ then $h^+ = h$ and $h \equiv 2 \pmod 4$.*

c) *Let $p \equiv q \equiv 1 \pmod 4$ and $(p/q) = (q/p) = 1$.*

1) *If $(p/q)_4 = -(q/p)_4$ then $h^+ \equiv 4 \pmod 8$ and $h \equiv 2 \pmod 4$.*

2) *If $(p/q)_4 = (q/p)_4 = -1$ then $h^+ = h$ and $h \equiv 4 \pmod 8$.*

3) *If $(p/q)_4 = (q/p)_4 = 1$ then $h^+ \equiv 0 \pmod 8$. Furthermore, $h \equiv 0 \pmod 8$ if $N(\epsilon) = -1$ and $h \equiv 0 \pmod 4$ if $N(\epsilon) = 1$.*

In this paper, we shall give an elementary proof of Scholz's theorem using ideal theory and Legendre's theorem on the solvability of the Diophantine equation $ax^2 + by^2 = z^2$.

2000 Mathematics Subject Classification. Primary 11R29, Secondary 11R11.

In the general sense, the problem is that of determining the Sylow 2-group of H^+. The idea is to find sufficient and necessary conditions under which a given ideal is equivalent to the square of some ideal. Let $(H^+)^2$ be the set of squares among the classes of H^+. If $\operatorname{ord} C = 2$ and $C \in (H^+)^2$ then $C = C_1^2$ for some $C_1 \in H^+$, with $\operatorname{ord} C_1 = 4$. Now if $C_1 \in (H^+)^2$, then $C = C_2^4$ for some $C_2 \in H^+$ and $\operatorname{ord} C_2 = 8$. We continue this process and find the smallest i such that $C_i \notin (H^+)^2$. Then $\operatorname{ord} C_i = 2^{i+1}$. The narrow class group H^+ has a cyclic subgroup of order 2^{i+1} and the class number h^+ is divisible by 2^{i+1}.

Let m and n be non-zero rational integers. Whenever n is a square modulo m, we write nRm. The following classical result is due to Legendre. An interesting proof by induction can be found in [1].

Lemma 1.2. *If a and b are positive square-free integers, then the equation $ax^2 + by^2 = z^2$ has non-trivial integer solutions x, y and z if and only if aRb, bRa and $(-ab/(a,b)^2)R(a,b)$.*

Lemma 1.3. *Let A be an ideal. Then $A \cong B^2$ for some ideal B if and only if there is a non-zero rational integer z and $\alpha \in A$ such that $z^2 = (N(\alpha)/NA)$, where NA is the norm of A, i.e., the number of elements in $\mathcal{O}_K/A$* (c.f. [4]).

Let A be a primitive ideal with norm $NA = a = kn^2$, with k square-free. A has an integral basis of the form $A = [a, (b + \sqrt{d}/2)]$ where $d = pq$ is the discriminant of K and $a \mid N(b + \sqrt{d}/2)$. Therefore there is some rational integer c such that $d = b^2 - 4ac$.

To show that $A \cong B^2$ for some ideal B, we need to find $z \in \mathbf{Z}$ and $\alpha = ax + (b + \sqrt{d}/2)y$ such that $z^2 = (N(\alpha)/NA)$. This is equivalent to

$$N(\alpha) = az^2$$

$$\left(ax + \frac{b+\sqrt{d}}{2}y\right)\left(ax + \frac{b-\sqrt{d}}{2}y\right) = az^2$$

$$(2ax+by)^2 = k(2nz)^2 + dy^2.$$

Putting $x = n\bar{z} - bn\bar{y}$, $y = 2an\bar{y}$ and $z = a\bar{x}$, the problem reduces to finding whether there are integers $\bar{x}$, $\bar{y}$ and $\bar{z}$ such that $k\bar{x}^2 + d\bar{y}^2 = \bar{z}^2$. Using the previous lemmas, we have

Lemma 1.4. *Let A be an ideal and $NA = kn^2$, with k square-free. The $A \cong B^2$ for some ideal B if and only if kRd, dRk and $(-kd/(k,d)^2)R(k,d)$.*

2. Proof of theorem. We begin with a few standard definitions and facts. Let σ be the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$. An ambiguous ideal is an ideal A such that $A = A^\sigma$. The only primitive ambiguous ideals are the unit ideal and those whose prime factors divide the discriminant of K. An ambiguous ideal class is a class C such that $C = C^\sigma$.

The primes p and q ramify in K, hence there are prime ideals P and Q such that $(p) = P^2$ and $(q) = Q^2$. The only primitive ambiguous ideals are the unit ideal $I = \mathcal{O}_k$, P, Q and $PQ = (\sqrt{d})$. K has two ambiguous ideal classes, each containing two primitive ambiguous ideals. These ideals can be distributed among the two classes in three possible ways:

$$\begin{aligned} P &\cong Q \not\cong I \cong (\sqrt{d}),\\ P &\cong I \not\cong Q \cong (\sqrt{d}),\\ P &\cong (\sqrt{d}) \not\cong Q \cong I. \end{aligned}$$

Let the integral basis of P be $[p, (p+\sqrt{d}/2)]$ and apply Lemma 1.4. Then $P \cong P_1^2$ for some ideal P_1 if and only if $(p/q) = (-q/p) = 1$.

Now we apply Lemma 1.4 to $(\sqrt{d}) = [d, (d+\sqrt{d}/2)]$. There is an ideal D_1 such that $(\sqrt{d}) \cong D_1^2$ if and only if $-1Rd$ or $-1Rpq$. The Chinese Remainder Theorem and the quadratic reciprocity law reduce this condition to $p \equiv q \equiv 1 \pmod 4$.

We treat the following cases separately:

a) If $p \equiv q \equiv 3 \pmod 4$, then without loss of generality, assume $(p/q) = 1$. Then

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

$$\Rightarrow P \cong P_1^2 \cong I$$

$$\Rightarrow P \cong I \not\cong Q \cong (\sqrt{d})$$

$$\Rightarrow N(\epsilon) = 1, \quad 2 \| h^+ \text{ and } h \text{ is odd.}$$

b) If $p \equiv q \equiv 1 \pmod 4$ and $(p/q) = (q/p) = -1$ we get $P \cong Q \not\cong I \cong (\sqrt{d})$ and $N(\epsilon) = -1$ and $2 \| h^+ = h$.

c) If $p \equiv q \equiv 1 \pmod 4$ and $(p/q) = (q/p) = 1$ then each of the four ambiguous ideals are equivalent to squares. In order to find out how they are distributed into the two ambiguous classes, we need to know the conditions under which each ideal is equivalent (in the narrow sense) to the fourth power of some ideal. These are given by the following lemma.

Lemma 2.1. *There is an ideal P_2 such that $P \equiv P_2^4$ if and only if q is a biquadratic residue modulo p. Similarly, $Q \equiv Q_2^4$ for some ideal Q_2 if and only if p is a biquadratic residue modulo q.*

Proof. Consider the ideal P_1 where $P \cong P_1^2$. We can assume that P_1 is primitive and has integral basis $P_1 = [a_p, (b_p + \sqrt{d}/2)]$, where $NP_1 = a_p = \prod p_i^{m_i}$ divides the norm of $(b_p + \sqrt{d}/2)$ and $(a_p, d) = 1$. All the prime divisors p_i of a_p split in $\mathcal{O}_k$. Hence, for odd prime divisors p_j, $(d/p_j) = 1$. If a_p is even then $(2/d) = 1$.

From Lemma 1.4, $P_1 \cong P_2^2$ for some ideal P_2 if and only if a_pRd, dRa_p and $(-a_pd/(a_p,d)^2)R(a_p,d)$. The last two conditions are trivially satisfied because $a_p \mid N(b_p + \sqrt{d}/2)$ and $(a_p, d) = 1$.

Writing $a_p = 2^m a_p'$, we have

$$\left(\frac{a_p}{p}\right)\left(\frac{a_p}{q}\right) = \left(\frac{2}{d}\right)^m \left(\frac{a_p'}{d}\right)$$

$$= \left(\frac{a_p'}{d}\right) = \left(\frac{d}{a_p'}\right) = \left(\frac{b_p^2}{a_p'}\right) = 1.$$

Thus $(a_p/p) = (a_p/q)$. By the Chinese Remainder Theorem, we have $P_1 \cong P_2^2$ if and only if $(a_p/p) = 1$.

Let $(p/q)_4$ be the biquadratic residue character, which takes on values 1 or -1, according as p is a biquadratic residue or a biquadratic nonresidue modulo q. Since $P \cong P_1^2$, there exists $\alpha = px + (p + \sqrt{d}/2)y \in P$ such that $(x, y) = 1$ and $(N\alpha/NP) = a_p^2$. Thus $4a_p^2 \equiv -qy^2 \pmod p$.

From this follows

$$\left(\frac{2}{p}\right)\left(\frac{a_p}{p}\right) \equiv (2a_p)^{(p-1/2)}$$

$$\equiv (4a_p^2)^{(p-1/4)}$$

$$\equiv (-qy^2)^{(p-1/4)} \pmod p$$

$$= \left(\frac{-1}{p}\right)_4 \left(\frac{q}{p}\right)_4 \left(\frac{y}{p}\right).$$

But $(2/p) = (-1/p)_4$, so to prove the lemma, it suffices that we show that $(y/p) = 1$.

Let $y = 2^k y_1$, where y_1 is odd. Then

$$\left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{y_1}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{p}{y_1}\right).$$

Since $4a_p^2 \equiv p(2x+y)^2 \pmod{y_1}$, we get

$$1 = \left(\frac{4a_p^2}{y_1}\right) = \left(\frac{p}{y_1}\right)\left(\frac{2x+y}{y_1}\right)^2,$$

and so $(p/y_1) = 1$ and $(y/p) = (2/p)^k$. If y is odd then $(y/p) = 1$. Let y be even and consider the equation $a_p^2 = px^2+pxy+(p-q/4)y^2$. Since $(x,y) = 1$, x and a_p are odd, and thus $pxy \equiv 0 \pmod 4$. It follows that $y \equiv 0 \pmod 4$ and $k \geq 2$.

If $p \equiv 1 \pmod 8$ then $(2/p) = 1$ and $(y/p) = 1$. If $p \equiv 5 \pmod 8$, we look at $a_p^2 = px^2 + pxy + (p-q/4)y^2$ modulo 8. Since x and a_p are odd, we get $1 \equiv 5 + 5xy \pmod 8$ and $k = 2$. □

Finally we consider the three subcases of c):

c-2) If $(p/q)_4 = (q/p)_4 = -1$ then $P \ncong P_2^4$; $Q \ncong Q_2^4$
$\Rightarrow\ P \equiv Q \ncong (\sqrt{d}) \cong I$
$\Rightarrow\ N(\epsilon) = -1,\ \ 4 \| h^+ = h.$

c-1) If $(p/q)_4 = -(q/p)_4 = 1$ then $P \ncong P_2^4$; $Q \cong Q_2^4$
$\Rightarrow\ P \cong (\sqrt{d}) \ncong Q \cong I$
$\Rightarrow\ N(\epsilon) = 1,\ \ 4 \| h^+ = 2h,\ \ 2 \| h.$
If $(p/q)_4 = -(q/p)_4 = -1$ then $P \cong P_2^4$; $Q \ncong Q_2^4$
$\Rightarrow\ P \cong I \ncong Q \cong (\sqrt{d})$
$\Rightarrow\ N(\epsilon) = 1,\ \ 4 \| h^+ = 2h,\ \ 2 \| h.$

c-3) If $(p/q)_4 = (q/p)_4 = 1$ then all four ideals are fourth powers. The distribution of ideals therefore takes into account the conditions under which an ideal is an eight power. In this case, $8|h^+$. Therefore $8|h$ if $N(\epsilon) = -1$, and $4|h$ if $N(\epsilon) = 1$.

The proof is complete.

References

[1] Ireland, K., and Rosen, M.: A classical introduction to modern number theory. 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York (1990).

[2] Lemmermeyer, F.: Reciprocity Laws From Euler to Eisenstein. Springer-Verlag, Berlin (2000).

[3] Nemenzo, F.: Quadratic forms, genus groups and rational reciprocity laws. Masteral Thesis, Sophia University (1991).

[4] Nemenzo, F., and Wada, H.: An elementary proof of Gauss' genus theorem. Proc. Japan Acad., **68A**, 94–95 (1992).

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