On efficient computation of the 2-parts of ideal class groups of quadratic fields

By Julius M. Basilla and Hideo Wada

Department of Mathematics, Sophia University
7-1 Kioicho, Chiyoda-ku, Tokyo 102-8554
(Communicated by Shigefumi Mori, m. j. a., Dec. 13, 2004)

Abstract: We shall show a relation between Gauss' ternary quadratic form and an ideal of a quadratic field. Using this relation, we can compute rapidly the 2-part of ideal class group of a quadratic field in narrow sense and in wide sense.

Key words: Ternary quadrartic form; quadratic field; ideal class group; 2-part.

1. Introduction. Let K be a quadratic field $\mathbf{Q}(\sqrt{m})$, where m is a square free integer and $m \not\equiv 1 \pmod 4$. Let Cl_2^+ and Cl_2 be the 2-part of ideal class group in narrow sense and in wide sense respectively. When two ideals $\mathbf{A}$, $\mathbf{B}$ belong to the same ideal class in narrow sense, we write $\mathbf{A} \cong \mathbf{B}$. Conjugate of $\theta \in K$ and ideal $\mathbf{A}$ are denoted by $\bar{\theta}$, $\bar{\mathbf{A}}$ respectively. $N\theta$, $N\mathbf{A}$ mean $\theta\bar{\theta}$, $\mathbf{A}\bar{\mathbf{A}}$ respectively. Hasse [4] proposed how to calculate Cl_2^+ using Legendre theorem. But we must decompose many integers to prime factors (cf. [1, 5]). So this method is not efficient. Shanks [8] and Bosma, Stevenhagen [2] calculated Cl_2^+ very efficiently using Gauss' ternary quadratic form. But they did not use ideal theory directly. So they could not calculate Cl_2. We shall show an ideal interpretation of Gauss' ternary quadratic form.

2. Square root of ideal class. When $\mathbf{A}$, $\mathbf{B}$ are primitive ideals such that

$$\mathbf{A} = [a,\, b+\sqrt{m}\,], \quad \mathbf{B} = [z,\, u+\sqrt{m}\,], \quad \mathbf{A} \cong \mathbf{B}^2$$

where $a = N\mathbf{A} > 0$. Then for some $\rho(\rho\bar{\rho} > 0)$, $\mathbf{A} = \rho\mathbf{B}^2$. So $\mathbf{A}$ contains $\theta = \rho z^2$ and

$$\frac{\theta\bar{\theta}}{a} = \frac{\rho\bar{\rho}z^4}{\rho\bar{\rho}z^2} = z^2$$

(cf. [7]). Put $\theta = ax + (b+\sqrt{m})y$. Then

$$(1) \quad ax^2 + 2bxy + cy^2 = z^2, \quad \text{where} \quad b^2 - m = ac.$$

Conversely if $\mathbf{A}$ contains $\theta = ax + (b+\sqrt{m})y$ such that $N\theta = az^2$ for some integer z, then we may assume $\gcd(x, y) = 1$. So there exists primitive ideal $\mathbf{C}$ such that $(\theta) = \mathbf{AC}$, $\mathbf{C}\bar{\mathbf{C}} = z^2$. All prime factors of z must be decomposed and we have

$$\mathbf{C} = \prod_{p|z} \mathbf{P}^2 = \left(\prod_{p|z} \mathbf{P}\right)^2$$

$$\text{where} \quad (p) = \mathbf{P}\bar{\mathbf{P}}, \quad \mathbf{P} \neq \bar{\mathbf{P}}.$$

So we have

$$\mathbf{A} \cong z^2\mathbf{A} = \mathbf{A}\mathbf{C}\bar{\mathbf{C}} = \theta\bar{\mathbf{C}} \cong \bar{\mathbf{C}}$$

(cf. [7]). Put $\mathbf{B} = \prod_{p|z} \bar{\mathbf{P}}$. Then we have $\mathbf{A} \cong \mathbf{B}^2$. We can compute $\mathbf{B}$ from $\mathbf{A}$ and θ as follows:

$$(\theta)\bar{\mathbf{A}} = \mathbf{A}\bar{\mathbf{A}}\mathbf{C} = a\mathbf{C},$$

$$\mathbf{B}^2 = \bar{\mathbf{C}} = \frac{1}{a}\bar{\theta}\mathbf{A} = [z^2,\, u+\sqrt{m}\,] = [z,\, u+\sqrt{m}\,]^2.$$

As $az^2 = \theta\bar{\theta} = (ax+by)^2 - my^2$ we have integer solutions U, V, W such that $aU^2 + mV^2 = W^2$. We may assume $\gcd(U, V) = 1$. For an odd prime divisor p of m, if $p \nmid a$ then $p \nmid U$ because m is square free. If $p|a$ then $p|W$, $p^2 \nmid a$, $p \nmid U$, $p \nmid V$ because $b^2 - ac = m$. So we have the local conditions (cf. [6]) $\chi_p(a) = 1$ for all odd prime divisors p of m where $\chi_p(a)$ is

$$\chi_p(a) = \begin{cases} \left(\dfrac{a}{p}\right) & p \nmid a \\[2ex] \left(\dfrac{-am/p^2}{p}\right) = \left(\dfrac{c}{p}\right) & p|a. \end{cases}$$

If we have a prime decomposition of m, we can examine these local conditions and if these local conditions are satisfied, Gauss ([3], 286) showed a very rapid algorithm for computing the global solution of (1). We shall explain Gauss' method.

2000 Mathematics Subject Classification. Primary 11E20, 11R29; Secondary 11R11, 11Y16.

We can compute rapidly X, Y such that

$$\begin{aligned} a &\equiv X^2 \pmod m \\ -b &\equiv XY \pmod m \\ c &\equiv Y^2 \pmod m \end{aligned}$$

(cf. [2]). Let $L \in M_3(\mathbf{Z})$ be

$$L = \begin{pmatrix} (Y^2-c)/m & (XY+b)/m & Y \\ (XY+b)/m & (X^2-a)/m & X \\ Y & X & m \end{pmatrix}.$$

Then $|L| = -1$ and $M = L^{-1}$ is of the form (cf. [2])

$$M = \begin{pmatrix} a & b & * \\ b & c & * \\ * & * & * \end{pmatrix}, \quad {}^tM = M, \quad |M| = -1.$$

We can find rapidly $S \in SL_3(\mathbf{Z})$ such that

$$(2) \qquad {}^tSMS = \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}$$

(cf. [3], 277). Let F be the right hand of (2) and put

$$S = \begin{pmatrix} * & * & * \\ * & * & * \\ A & B & C \end{pmatrix}, \quad S^{-1} = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$$

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = S^{-1} \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \alpha' x + \beta' y \\ \alpha'' x + \beta'' y \end{pmatrix}.$$

Then we have

$$(3) \qquad A = \begin{vmatrix} \alpha' & \beta' \\ \alpha'' & \beta'' \end{vmatrix}, \quad -B = \begin{vmatrix} \alpha & \beta \\ \alpha'' & \beta'' \end{vmatrix}.$$

$$(4) \qquad M = {}^tS^{-1}FS^{-1}, \quad c = \beta'^2 + 2\beta\beta''.$$

$$(5) \qquad L = M^{-1} = SF{}^tS, \quad m = B^2 + 2AC.$$

And we have the quadratic forms

$$ax^2 + 2bxy + cy^2 = (x, y, 0) M \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}$$

$$= (X, Y, Z) \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = Y^2 + 2XZ.$$

When $\gcd(\alpha'', \beta'') = d$, we put $x = \beta''/d$, $y = -\alpha''/d$. Then $Z = 0$, $X = -B/d$, $Y = A/d$ and

$$ax^2 + 2bxy + cy^2 = Y^2, \ \gcd(x, y) = 1.$$

Namely we get the global solution of (1) and $N\mathbf{B} = |Y|$.

From (4) we have

$$\begin{pmatrix} ax+by \\ bx+cy \\ * \end{pmatrix} = M \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} = {}^tS^{-1}FS^{-1} \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}$$

$$= {}^tS^{-1} \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} X \\ Y \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha' Y + \alpha'' X \\ \beta' Y + \beta'' X \\ * \end{pmatrix},$$

$$\begin{aligned} \mathbf{B}^2 &= \frac{\bar\theta}{a}\mathbf{A} = \frac{ax + (b-\sqrt{m})y}{a}[a,\, b+\sqrt{m}\,] \\ &= [ax + (b-\sqrt{m})y,\ (b+\sqrt{m})x + cy] \\ &= [\alpha' Y + \alpha'' X - \sqrt{m}y,\ \beta' Y + \beta'' X + \sqrt{m}x] \\ &= [\alpha' Y - (-B+\sqrt{m})y,\ \beta' Y + (-B+\sqrt{m})x]. \end{aligned}$$

As $\mathbf{B} \ni Y$ and $\gcd(x, y) = 1$, we have $\mathbf{B} \ni (-B + \sqrt{m})$, namely $\mathbf{B} = [Y, -B+\sqrt{m}\,]$. From (3), (5) we have $d|m$, $A|B^2 - m$. Therefore we get

$$\mathbf{A} \cong \left[\frac{A}{d}, -B+\sqrt{m}\right]^2 \cong [A, -B+\sqrt{m}\,]^2.$$

3. The case $m \equiv 1 \pmod 4$. When square free integer $m \equiv 1 \pmod 4$, then we must make a few modifications. We start from the following forms:

$$\mathbf{A} = \left[a, \frac{b+\sqrt{m}}{2}\right], \quad \mathbf{B} = \left[z, \frac{u+\sqrt{m}}{2}\right]$$

$$b^2 - m = ac, \ 4|c, \quad \theta = ax + \frac{b+\sqrt{m}}{2}y.$$

Then we have the quadratic form

$$(6) \qquad z^2 = \frac{\theta\bar\theta}{a} = ax^2 + bxy + \frac{c}{4}y^2, \quad \gcd(x, y) = 1.$$

Multiplying 4, we get

$$a(2x)^2 + 2b(2x)y + cy^2 = (2z)^2.$$

If we have a solution x_0, y_0, z_0 such that

$$ax_0^2 + 2bx_0y_0 + cy_0^2 = z_0^2, \quad \gcd(x_0, y_0) = 1$$

then there are two cases.

Case 1. $x_0 =$ even. Put $x = x_0/2$, $y = y_0$, $z = z_0/2$.

Case 2. $x_0 =$ odd. Put $x = x_0$, $y = 2y_0$, $z = z_0$.

Then we have a solution of (6). From (4), β' must be even. So we have

Case 1. $\beta'' =$ even,

$$\mathbf{B}^2 = \left[ax + \frac{b-\sqrt{m}}{2}y, \frac{b+\sqrt{m}}{2}x + \frac{c}{4}y\right]$$

$$= \left[\frac{ax_0 + by_0}{2} - \frac{\sqrt{m}}{2}y, \frac{bx_0 + cy_0}{4} + \frac{\sqrt{m}}{2}x\right]$$
$$= \left[\alpha'\frac{Y}{2} - \frac{-B+\sqrt{m}}{2}y, \frac{\beta'}{2}\frac{Y}{2} + \frac{-B+\sqrt{m}}{2}x\right]$$
$$= \left[\frac{Y}{2}, \frac{-B+\sqrt{m}}{2}\right]^2.$$

From

$$\frac{Y}{2} = \frac{1}{d}\frac{A}{2}, \quad \frac{A}{2} \,\Big|\, \frac{B^2-m}{4}$$

we have

$$\mathbf{A} \cong \left[\frac{Y}{2}, \frac{-B+\sqrt{m}}{2}\right]^2 \cong \left[\frac{A}{2}, \frac{-B+\sqrt{m}}{2}\right]^2.$$

Case 2. $\beta'' =$ odd,

$$\mathbf{B}^2 = \left[\alpha' Y - \frac{-B+\sqrt{m}}{2}y, \frac{\beta'}{2}Y + \frac{-B+\sqrt{m}}{2}x\right]$$
$$= \left[Y, \frac{-B+\sqrt{m}}{2}\right]^2.$$

From

$$d|m, Y = \frac{1}{d}A, \quad 2Y \,\Big|\, \frac{B^2-m}{2}, \quad A \,\Big|\, \frac{B^2-m}{2},$$

we have $d =$ odd,

$$(2Y, A) = Y, \quad 2A \,\Big|\, \frac{B^2-m}{2}$$

and

$$\mathbf{A} \cong \left[Y, \frac{-B+\sqrt{m}}{2}\right]^2 \cong \left[A, \frac{-B+\sqrt{m}}{2}\right]^2.$$

Using these we can find a system of generators of Cl_2^+ (cf. [2]). So we can find the relation between $(\sqrt{m})$ and the generators. Therefore we can compute Cl_2. When

$$m = 433(10^{100}+949)(10^{100}+1293)(10^{100}+2809) \times (10^{100}+6637)(10^{100}+22261)$$

we get

$$Cl_2^+ = (2,4,4,4,64) \text{ type}$$
$$Cl_2 = (2,2,4,4,64) \text{ type}$$

(cf. [2]). It took only 2 seconds using a personal computer. We made the program using Ubasic.

References

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

[2] Bosma, W., and Stevenhagen, P.: On the computation of quadratic 2-class groups. J. Théor. Nombres Bordeaux, **8**, 283–313 (1996).

[3] Gauss, C. F.: Disquisitiones Arithmeticae. Gerhard Fleischer, Leipzig (1801).

[4] Hasse, H.: An algorithm for determining the structure of the 2-Sylow-subgroup of the divisor class group of a quadratic number field. Symposia Mathematica (Convegno di Strutture in Corpi Algebrici, INDAM, Roma 1973), vol. XV, Academic Press, London, pp. 341–352 (1975).

[5] Ireland, K., and Rosen, M.: A Classical Introduction to Modern Number Theory. Grad. Texts in Math., 84, Springer-Verlag, New York, pp. 272–275 (1982).

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

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

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