Rep. Fac. Sci. Engrg.
Saga Univ., Math.,
30-1 (2001), 1~12

Reports of the Faculty of Science and Engineering,
Saga University, Mathematics, Vol.30, No.1, 2001

A CORRECTION OF NAKAHARA'S TABLE

BY
TORU KOMASTU

(Received September 11, 2000, revised June 27, 2001)

ABSTRACT. In this paper we will make a correction of Nakahara's table [N1] which contains data of the structure of 3-Sylow subgroups in the ideal class groups for real quadratic fields. We supply the correction by using algorithm in [K1] which enables us to see the 3-rank of the ideal class groups of real quadratic fields. We also provide a program of the algorithm written by PARI-GP.

0. Introduction.

In his paper [N1] Nakahara determines the structure of the 3-class group of a real quadratic field $\mathbb{Q}(\sqrt{D})$ whose class number is divisible by 9. By using an algorithm [K1, Theorem 0.5] we calculated the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{D})$ for the same range of D as in [N1], and found 121 errors in [N1]. For each of the 121 cases, we checked our result by making use of a function equipped in PARI-GP.

Remark 0.1. In his paper [N1] we obtain not only the structure of the 3-class group but also the class number in the wide sense, the number of reduced irrationals in the principal class, accordingly the norm of the fundamental unit of $\mathbb{Q}(\sqrt{D})$ and the number of the reduced irrationals in a real quadratic field $\mathbb{Q}(\sqrt{D})$ whose class number is divisible by 9.

I especially thank Professor Toru Nakahara for his valuable advice and suggestions. I am grateful to the referee for many helpful comments.

AMS subject classification: Primary 11R29, 11R11; secondary: 11Y16

1. Some remarks.

First we shall correct some mistakes in [N1]. At the Introduction in [N1], it is stated that the numbers of real quadratic fields $\mathbb{Q}(\sqrt{D})$ whose class numbers are divisible by 9 are 9386, 200, 300 and 400, when

(i) $1 \leq D \leq 1200000$, (ii) $2000000 \leq D \leq 2022589$,

(iii) $3000000 \leq D \leq 3029834$, (iv) $4000000 \leq D \leq 4033723$,

respectively. However,

Remark 1.1. The data for

(iv′) $4000000 \leq D \leq 4039891$

exist in [N1] disorderly. The data of $D = 4033666$, 4033718 and 4033723 are written doubly (for the details, see Remark 1.3 below). Hence the data for D greater than 4000000 listed in [N1] are not on 400 fields $\mathbb{Q}(\sqrt{D})$ such that $4000000 \leq D \leq 4033723$ but on 397 fields $\mathbb{Q}(\sqrt{D})$ such that $4000000 \leq D \leq 4039891$.

Remark 1.2. There is a correction that "exchange the pages 46 and 47" in the errata.

We call the lower and the upper tables of page m by pp.m.A and pp.m.B, respectively. The symbol $X.n$ means the nth line from the top on a table X.

Remark 1.3. The data in the tables pp.89.B, pp.90.A and pp.90.B are not arranged in the numerical order of D's. More precisely, the datum next to pp.89.B.49 is pp.90.A.35. The data from pp.89.B.50 to pp.90.A.34 must be connected to the next of pp.90.B.60. The data pp.90.B.61–63 are superfluous. In fact, they are the same as the data pp.89.B.50–52.

2. Main algorithm.

For our correction we utilize the following algorithm in [K1].

Theorem 2.1 (*algorithm to know all unramified cyclic cubic extensions of a real quadratic field and the* 3*-rank of the ideal class group* [K1, *Theorem* 0.5]).

First let d be a square-free positive integer such that $3 \nmid d$.

Step 1. *Put*

$$e = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ 2 & \text{otherwise.} \end{cases}$$

$$e^* = \frac{2}{e} \quad (e \cdot e^* = 2).$$

Step 2. *Find all triples* $(a,b,c) \in \mathbb{N}^3$ *which satisfy*

$$\begin{cases} \text{(A.1)} & \frac{1}{e^*}\sqrt[3]{e^*(27d+1)} \le c < e\sqrt{d}, \\ \text{(A.2)} & a^2 + 27db^2 = e^{*2}c^3, \\ \text{(A.3)} & \gcd(a,c) \mid \operatorname{lcm}(e, 3d), \\ \text{(A.4)} & v_3(a) \neq 2, \end{cases}$$

where $v_3(a)$ *is the greatest exponent* n *such that* $3^n \mid a$. *Let* W_d *be the set of all such triples. For each* $(a,b,c) \in W_d$, *there exists a unique integer* $s = s_{(a,b,c)}$ *which satisfies*

$$\begin{cases} \text{(A.5)} & -\frac{c}{e} < s < \frac{c}{e}, \\ \text{(A.6)} & 3bs \equiv a \pmod{e^*c}, \\ \text{(A.7)} & s^2 \equiv -3d \pmod{e^{*2}c}. \end{cases}$$

Let us define a subset $V_d\ (\subset W_d)$ *by*

$$V_d = \left\{ (a,b,c) \in W_d \;\middle|\; \left| \frac{s_{(a,b,c)} + \sqrt{-3d}}{e^*c} \right| > 1 \right\}.$$

Step 3. *For each* $(a,b,c) \in V_d$, *define a cubic polynomial* $f_{a,c}(Z)$ *by*

$$f_{a,c}(Z) = Z^3 - 3cZ - ea.$$

Put $n = \sharp V_d$ *and* $r = \log_3(2n+1) \in \mathbb{R}$.

Conclusion. Then the number r *is equal to the* 3*-rank of the ideal class group of the real quadratic field* $\mathbb{Q}(\sqrt{d})$. *For each* $(a,b,c) \in V_d$, *the minimal splitting field of* $f_{a,c}(Z)$ *over* $\mathbb{Q}$ *is an unramified cyclic cubic extension of* $\mathbb{Q}(\sqrt{d})$. *Conversely, every unramified cyclic cubic extension of* $\mathbb{Q}(\sqrt{d})$ *can be obtained in this way by a* *suitable* $(a,b,c) \in V_d$. *All splitting fields are different from each other. The integer* n *is equal to the number of unramified cyclic cubic extensions of* $\mathbb{Q}(\sqrt{d})$.

When $3 \mid d$, *let us change the conditions* (A.1) *to* (A.7) *in Step* 2 *as follows.*

$$\begin{cases} \text{(B.1)} \quad \dfrac{1}{3e^*}\sqrt[3]{9e^*(d+3)} \le c < \dfrac{e\sqrt{d}}{3}, \\ \text{(B.2)} \quad a^2 + \dfrac{d}{3}b^2 = e^{*2}c^3, \\ \text{(B.3)} \quad \gcd(a,c) \mid \operatorname{lcm}(e, \dfrac{d}{3}), \\ \text{(B.4)} \quad \max\{v_3(a^2e^2-d-4), v_3(a), v_3(b)\} \ge 2. \end{cases}$$

$$\begin{cases} \text{(B.5)} \quad -\dfrac{c}{e} < s < \dfrac{c}{e}, \\ \text{(B.6)} \quad bs \equiv a \pmod{e^*c}, \\ \text{(B.7)} \quad s^2 \equiv -\dfrac{d}{3} \pmod{e^{*2}c}. \end{cases}$$

And, put

$$V_d = \left\{ (a,b,c) \in W_d \;\middle|\; \left| \frac{s_{(a,b,c)} + \sqrt{-d/3}}{e^*c} \right| > 1 \right\}.$$

Then the conclusion is the same as in the case $3 \nmid d$.

Remark 2.2. Each calculation described in this theorem are carried out by finite steps. The polynomial $f_{a,c}(Z)$ is irreducible over $\mathbb{Q}$ for every $(a,b,c) \in V_d$.

We present a program of Theorem 2.1 written by PARI-GP. The first three programs "evalf", "maxabx" and "fnds" are supplymentary functions.

```
{evalf(x) = local(intgprt, frctprt, frc, zeros);
    intprt = floor(x); frctprt = frac(x);
    if( frctprt == 0
      ,frc = concat(".", 0);
      ,if( frctprt*10<1
        ,frctprt = frctprt*10; zeros = concat(".",0);
         while( frctprt*10<1, frctprt = frctprt*10; zeros = concat(zeros,0););
         frc = concat(zeros, floor(frctprt*10^3));
        ,frc = concat(".", floor(frctprt*10^3));
        );
      );
    concat(intprt, frc);}

{maxabx(a, b, e, d) = local();
    max(max(valuation(a,3), valuation(b,3)), valuation(a^2*e^2-d-4,3))}

{fnds(a, b, c, d0, e, est, ops) = local(b3, s, s0, estc, est2c);
    if( ops == 0, b3 = 3*b, b3 = b);
    estc = est*c; est2c = est^2*c;
    for( s = 0, floor(c/e),
        if( (s^2+d0)%est2c == 0
          ,if( (b3*s-a)%estc == 0, s0 = s; break,);
           if( (b3*s+a)%estc == 0 ,s0 = -s; break,);
          ,);
        );
    s0;}
```

```
{unram(d) =
  local(numVd, e, est, d27, lowbnd, uppbnd, d0, lcme, c, est2c3, b, a2, a, s, abst, rk);
    if( type(d) == "t_INT" && d>0
      ,if( issquarefree(d) == 1
        ,numVd = 0;
         if( d%4 == 1, e = 1, e = 2); est = 2/e;
         if( d%3>0
           ,d27 = 27*d;
            lowbnd = ceil((est*(d27+1))^(1/3)/est);
            uppbnd = floor(e*d^(1/2));
            d0 = d*3; lcme = lcm(e,d0);
            for( c = lowbnd, uppbnd,
                 est2c3 = est^2*c^3;
                 for( b = 1, floor(sqrt((est2c3-1)/d27)), a2 = est2c3-d27*b^2;
                       if( issquare(a2) == 1
                          ,a = round(sqrt(a2));
                           if( lcme%gcd(a,c) == 0 && valuation(a,3)<>2
                             ,s = fnds(a, b, c, d0, e, est, 0);
                              abst = abs((s+sqrt(-d0))/(est*c));
                              if( abst>1
                                ,print([a, b, c, s, evalf(abst), Z^3-3*c*Z-e*a]);
                                 numVd = numVd+1;
                                ,print([a, b, c, s, evalf(abst), " - "]);
                                );
                             ,);
                          ,);
                       );
                 );
```

```
        ,lowbnd = ceil((9*est*(d+3))^(1/3)/(3*est));
         uppbnd = floor(e*d^(1/2)/3);
         d0 = d/3; lcme = lcm(e,d0);
         for( c = lowbnd, uppbnd,
             est2c3 = est^2*c^3;
             for( b = 1, floor(sqrt((est2c3-1)/d0)), a2 = est2c3-d0*b^2;
                 if( issquare(a2) == 1
                   ,a = round(sqrt(a2));
                    if( lcme%gcd(a,c) == 0 && maxabx(a,b,e,d) >1
                      ,s = fnds(a, b, c, d0, e, est, 1);
                       abst = abs((s+sqrt(-d0))/(est*c));
                       if( abst>1
                         ,print([a, b, c, s, evalf(abst), Z^3-3*c*Z-e*a]);
                          numVd = numVd+1;
                         ,print([a, b, c, s, evalf(abst), " - "]);
                         );
                      ,);
                   ,);
                 );
             );
        );
      rk = valuation(2*numVd+1,3);
      if( 3^rk == 2*numVd+1
        ,print("3-rank of the ideal class group of Q(sqrt(", d ,")) = ", rk);
        ,print("error on the number of Vd  PLEASE REPORT!");
        );
      ,print(d ," is not square-free!");
      );
    ,print(d ," is not a positive integer!");
    );
}
```

For example, input "unram(23659);". Then the output is as follows.

$$[270, 2, 138, 45, "1.957", Z\hat{\ }3 - 414 * Z - 540]$$

$$[1837, 2, 181, -86, "1.546", Z\hat{\ }3 - 543 * Z - 3674]$$

$$[2998, 2, 226, -103, "1.263", Z\hat{\ }3 - 678 * Z - 5996]$$

$$[2872, 3, 241, -29, "1.111", Z\hat{\ }3 - 723 * Z - 5744]$$

$$[1862, 6, 298, -29, "0.899", " - "]$$

3-rank of the ideal class group of Q(sqrt(23659)) = 2

The 1st–3rd components a, b, c of each row mean a solution (a, b, c) which satisfies (A.1)–(A.4) of Theorem 2.1. The above data show $|W_{23659}| = 5$. The forth component is equal to $s_{(a,b,c)}$ determined by (A.5)–(A.7) of Theorem 2.1, and the fifth is equal to the absolute value $|(s_{(a,b,c)} + \sqrt{-3d})/(e^*c)|$. (The decimals are rounded off.) Thus $|V_{23659}| = 4$ and the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{23659})$ is equal to 2. Every unramified cyclic cubic extensions of $\mathbb{Q}(\sqrt{23659})$ is one of the minimal splitting fields over $\mathbb{Q}$ of $Z^3 - 414Z - 540$, $Z^3 - 543Z - 3674$, $Z^3 - 678Z - 5996$ and $Z^3 - 723Z - 5744$. It is known that 23659 is the smallest positive integer D such that the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{D})$ is greater than 1.

3. Some data.

Let us denote by $H3_{\rm N}$ 3-Sylow group of the ideal class group of $\mathbb{Q}(\sqrt{D})$ described in [N1], by $r_{\rm K}$ 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{D})$ obtained by using the algorithm in [K1], and by $\mathrm{Cl}_{\rm P}$ ideal class group of $\mathbb{Q}(\sqrt{D})$ calculated on PARI-GP. Here we take advantage of the function "`bnfinit`$(x^2 - D)$`.clgp`" in PARI-GP to see the ideal class group of $\mathbb{Q}(\sqrt{D})$. All calculations for $r_{\rm K}$ and $\mathrm{Cl}_{\rm P}$ are done on the version Ver.2.0.14 of PARI-GP. The following Tables 3.1–3.3 are the lists of data where $r_{\rm K}$ are contrary to $H3_{\rm N}$. We simply denote by $n_1 \times n_2 \times \cdots \times n_s$ a finite abelian group $\mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_s$.

Table 3.1 $(1 < D \leq 1000000)$

D	$H3_N$	r_K	Cl_P	D	$H3_N$	r_K	Cl_P
100014	3×3	1	18×2	729102	3×3	1	18×2
125310	3×3	1	18×2	738647	3×3	1	18×2
193610	3×3	1	18×2	743259	3×3	1	$18\times2\times2$
207026	3×3	1	36×2	751655	3×3	1	$18\times2\times2$
207879	3×3	1	$18\times2\times2$	751686	3×3	1	$18\times2\times2$
219894	3×3	1	36×2	757563	27	2	18×6
221527	3×3	1	36×2	757718	3×3	1	18×2
245010	3×3	1	18×2	762226	3×3	1	72×2
298447	27	2	18×3	786770	3×3	1	$18\times2\times2$
324915	3×3	1	18×2	796259	3×3	1	63
330635	3×3	1	18×2	801102	3×3	1	$18\times2\times2$
354039	3×3	1	$18\times2\times2$	816613	3×3	1	36
416111	27	2	18×3	829162	3×3	1	126
419487	3×3	1	18×2	837347	3×3	1	$18\times2\times2$
466990	3×3	1	$18\times2\times2$	841645	3×3	1	18×2
468951	3×3	1	$18\times2\times2$	851258	3×3	1	18×2
471511	3×3	1	72×2	858291	3×3	1	$18\times2\times2$
473258	27	2	18×3	865306	3×3	1	72×2
478587	3×3	1	18×2	868210	3×3	1	$18\times2\times2$
485342	3×3	1	18×2	876018	3×3	1	$18\times2\times2$
547563	3×3	1	36×2	895607	3×3	1	18×2
555026	27	2	36×3	911118	3×3	1	18×2
565598	3×3	1	18×2	928030	3×3	1	$36\times2\times2$
580771	3×3	1	90×2	940415	3×3	1	$18\times2\times2$
594435	3×3	1	$18\times2\times2$	940895	27	2	18×3
603507	3×3	1	36×2	943315	3×3	1	72×2
606395	3×3	1	18×2	949343	3×3	1	18×2
631230	3×3	1	$18\times2\times2$	950547	3×3	1	36×2
634283	3×3	1	18×2	950619	3×3	1	36×2
689495	3×3	1	18×2	950690	3×3	1	$18\times2\times2$
690938	3×3	1	18×2	960407	3×3	1	36
698918	3×3	1	36	961751	3×3	1	36
700010	3×3	1	18×2	968262	3×3	1	72
719051	3×3	1	90	970955	3×3	1	18×2
719106	27	2	18×3	972478	3×3	1	36×2
724110	3×3	1	18×2	973470	3×3	1	$36\times2\times2$

Table 3.2 $(1000000 < D \leq 1200000)$

D	$H3_N$	r_K	Cl_P	D	$H3_N$	r_K	Cl_P
1000002	27	2	18×3	1065018	3×3	1	36×2
1005951	3×3	1	$18 \times 2 \times 2$	1072731	3×3	1	36×2
1016070	3×3	1	$18 \times 2 \times 2$	1105310	3×3	1	18×2
1017759	3×3	1	$18 \times 2 \times 2$	1110854	3×3	1	$18 \times 2 \times 2$
1018018	27	2	18×6	1113838	3×3	1	36×2
1023891	3×3	1	$18 \times 2 \times 2 \times 2$	1119455	3×3	1	18×2
1024166	3×3	1	36×2	1138511	3×3	1	$18 \times 2 \times 2$
1025738	3×3	1	18×2	1146922	3×3	1	$36 \times 2 \times 2$
1030227	3×3	1	36×2	150435	3×3	1	$36 \times 2 \times 2$
1032510	3×3	1	$18 \times 2 \times 2$	1163490	3×3	1	18×2
1033170	3×3	1	18×2	1173003	3×3	1	$18 \times 2 \times 2$
1046526	3×3	1	36×2	1189686	3×3	1	90
1050082	3×3	1	36×2	1189810	3×3	1	18×2
1058862	3×3	1	$18 \times 2 \times 2$				

Table 3.3 (D satisfies (ii),(iii) or (iv′))

D	$H3_N$	r_K	Cl_P	D	$H3_N$	r_K	Cl_P
2002370	3×3	1	18×2	4009999	3×3	1	18×2
2012426	3×3	1	$18 \times 2 \times 2 \times 2$	4011114	27	2	18×6
2020487	3×3	1	18×2	4020827	27	2	18×6
2022242	3×3	1	72	4027826	3×3	1	90×2
3009182	3×3	1	$18 \times 2 \times 2$	4033135	3×3	1	144×2
3014443	3×3	1	72	4033718	3×3	1	18×2
3025906	3×3	1	18×2	4034371	3×3	1	18×2
4003951	3×3	1	18×2	4037867	3×3	1	72
4003999	3×3	1	171	4038241	3×3	1	18
4004506	3×3	1	18×2	4038295	3×3	1	18×2
4004674	3×3	1	18	4039483	3×3	1	90

Proposition 3.4. *For every case in the above tables, r_K agrees with* Cl_P.

Remark 3.5. The calculating ways of r_K and Cl_P are essentially distinct. The calculation for Cl_P is done in the real quadratic field $\mathbb{Q}(\sqrt{D})$ itself. On the other hand, that for r_K is done substantially in the imaginary quadratic field $\mathbb{Q}(\sqrt{-3D})$.

Remark 3.6. The datum for $D = 3025906$ in the page 406 of Nakahara's other paper [N2] is the same as the above $H3_N$. It also should be corrected.

For each $m = 0, 1, \ldots, 11$, let A_m be the set of all (square-free positive) integers

D in the tables of [N1] with $100000m + 1 \le D \le 100000(m+1)$. Let A_{20}, A_{30} and A_{40} be the set of all integers D in [N1] such that D satisfy (ii),(iii) and (iv′), respectively. Let B_m be the set of all integers which are contained in A_m and exist in Tables 3.1–3.3. We put $a_m = |A_m|$, $b_m = |B_m|$ and $p_m = (b_m/a_m) \times 100$.

Table 3.7 (the number of different results and its percentage)

m	0	1	2	3	4	5	6	7	8	9	10	11	0–11
a_m	550	702	742	832	813	804	771	821	819	825	920	787	9386
b_m	0	3	6	3	8	5	7	14	11	15	16	11	99
$p_m(\%)$	0.0	0.43	0.81	0.36	0.98	0.62	0.91	1.71	1.34	1.82	1.74	1.40	1.05

m	20	30	40	total
a_m	200	300	397	10283
b_m	4	3	15	121
$p_m(\%)$	2.00	1.00	3.78	1.18

Remark 3.8. The numbers p_m in Table 3.7 are rounded.

Remark 3.9. The percentage p_{40} is extremely bigger than others p_m. These phenomena intimate the limitation of double precision in calculation by Fortran 77 on the computers which were employed to construct the Nakahara's table.

Remark 3.10. One can obtain the program in § 2 written by PARI-GP at

http://www.comp.metro-u.ac.jp/~trkomatu/unram/algo.tar.gz

References

[K1] Komatsu, T., *On unramified cyclic cubic extensions of real quadratic fields*, (to appear in Japan. J. Math.).

[K2] Komatsu, T., *A family of infinite pairs of quadratic fields* $\mathbb{Q}(\sqrt{D})$ *and* $\mathbb{Q}(\sqrt{-D})$ *whose class numbers are both divisible by* 3, Acta Arith. **96** (2001), 213–221.

[N1] Nakahara, T., *The structure of* 3*-class groups in the real quadratic fields* $\mathbb{Q}(\sqrt{D})$ *for* D *less than* 1200000 *and for a few values of* D *between* 2000000 *and* 4033723, Rep. Fac. Sci. Engrg. Saga Univ. Math. **23** (1995), 9–90.

[N2] Nakahara, T., *Experiments on a problem of D. Shanks concerning quadratic fields*, Number Theory: Diophantine, Computational and Algebraic Aspect, (ed. by K. Győry/Pethő/Sós), Walter de Gruyter GmbH & Co. (1998), 401–408.

Department of Mathematics
Tokyo Metropolitan University
Minami-Ohsawa 1-1, Hachioji-shi
Tokyo 192-0397, JAPAN
E-mail address: trkomatu@comp.metro-u.ac.jp