ACTA ARITHMETICA
163.4 (2014)

Another look at real quadratic fields of relative class number 1

by

Debopam Chakraborty and Anupam Saikia (Guwahati)

1. Introduction. A real quadratic field K is necessarily of the form $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ for some square-free natural number m. The discriminant d of K is m if $m \equiv 1 \pmod 4$, otherwise $d = 4m$. In the former case, the ring $\mathcal{O}_K$ of integers of K is $\{a + b(1 + \sqrt{m})/2 \mid a, b \in \mathbb{Z}\}$, and in the latter case, $\mathcal{O}_K = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. By Dirichlet's Unit Theorem, the units of $\mathcal{O}_K$ are given by $\pm\xi_m^i$ $(i \in \mathbb{Z})$ where ξ_m is called the *fundamental unit*. The relative class number of K for a conductor f is the ratio $H_d(f)$ of the class numbers of $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ and $\mathcal{O}_K$. It was Dirichlet who obtained a nice formula for the relative class number (see [1]):

Result 1.1. *Let $\theta(f)$ be the smallest positive integer such that $\xi_m^{\theta(f)} \in \mathcal{O}_f$ and*

$$\psi(f) = f \prod_{q \mid f} \left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right),$$

where $\left(\frac{d}{q}\right)$ denotes the "Kronecker residue symbol" of d modulo a prime q. Then the relative class number for conductor f is given by

$$H_d(f) = \frac{\psi(f)}{\theta(f)}. \tag{1.1}$$

Recall that the Kronecker residue symbol $\left(\frac{d}{q}\right)$ is the same as the Legendre symbol when q is an odd prime. For $q = 2$ and d odd, $\left(\frac{d}{q}\right)$ is 1 if $d \equiv \pm 1 \pmod 8$, and -1 if $d \equiv \pm 3 \pmod 8$. The relative class number is always an integer (see [1]), hence $\theta(f)$ always divides $\psi(f)$. We will always write the fundamental unit of $\mathcal{O}_K$ as

$$\xi_m = \alpha_0 + \beta_0\sqrt{m}, \qquad 2\alpha_0, 2\beta_0 \in \mathbb{Z}.$$

2010 *Mathematics Subject Classification*: Primary 11R11; Secondary 11R65.
Key words and phrases: relative class number, fundamental unit.

DOI: 10.4064/aa163-4-5

It is well known that $\xi_m^3 \in \mathbb{Z}[\sqrt{m}]$ and, when $m \not\equiv 5 \pmod 8$, α_0 and β_0 are integers. For the rest of the paper, we will use the following notation:

$$\tilde{\beta_0} = \beta_0,\ \tilde{\alpha}_0 = \alpha_0 \quad \text{if } \xi_m \in \mathbb{Z}[\sqrt{m}], \qquad \tilde{\beta_0} = 2\beta_0,\ \tilde{\alpha}_0 = 2\alpha_0 \quad \text{if } \xi_m \notin \mathbb{Z}[\sqrt{m}].$$

Observe that if $\tilde{\beta_0}$ is divisible by a prime q, then $\theta(q) = 1$. When the square-free integer m does not divide $\tilde{\beta_0}$, there exists a prime q dividing m such that $\tilde{\beta_0}$ is not divisible by q. Taking $f = q$ in Dirichlet's formula, we find that $\psi(q) = q$ and $\theta(q) \neq 1$ is a factor of $\psi(q)$. Hence $\theta(q) = \psi(q) = q$, and $H_d(q) = 1$. Now we consider $m = 1817$ and $f = 2$. As $1817 \equiv 1 \pmod 8$, we find that $H_d(2) = 1$. But m divides $\tilde{\beta_0}$ in this case (see [4]). In other words, non-divisibility of $\tilde{\beta_0}$ by m is a sufficient condition for existence of f such that $H_d(f) = 1$ but it is not a necessary condition. Later, we will obtain a necessary and sufficient condition for existence of f with $H_d(f) = 1$ when ξ_m has norm 1. We will mostly consider prime conductors $f = p$, and try to determine the smallest exponent $\theta(p)$ that takes the fundamental unit ξ_m of $\mathbb{Q}(\sqrt{m})$ into the order $\mathcal{O}_p$ of conductor p.

2. Powers of ξ_m in $\mathcal{O}_p$. The fundamental unit $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ has norm either 1 or -1, and accordingly, we have $\xi_m^{-1} = \alpha_0 - \beta_0\sqrt{m}$ or $\xi_m^{-1} = -(\alpha_0 - \beta_0\sqrt{m})$. In the following two sections we assume that ξ_m has norm 1. We need the next two propositions.

Proposition 2.1. *If ξ_m has norm 1, then $\xi_m^{(p-(\frac{d}{p}))/2} \in \mathcal{O}_p$ for any odd prime p not dividing m.*

In fact, one can obtain the following sharper result.

Proposition 2.2. *Let p be an odd prime not dividing m. If 2^s divides $p - \left(\frac{d}{p}\right)$ and ${\xi_m}^{(p-(\frac{d}{p}))/2^{s-1}} \equiv 1 \pmod p$ then $\xi_m^{(p-(\frac{d}{p}))/2^s} \in \mathcal{O}_p$.*

The propositions above can be derived easily by considering congruence. The essential idea lies in the following lemma.

Lemma 2.3. *$\xi_m^{p-(\frac{d}{p})} \equiv 1 \pmod p$ for any odd prime p not dividing m.*

Proof. Modulo $p\mathcal{O}_K$ we have

$$\xi_m^p \equiv \alpha_0^p + \beta_0^p m^{(p-1)/2}\sqrt{m} \equiv \alpha_0 + \left(\frac{m}{p}\right)\beta_0\sqrt{m} = (\alpha_0 + \beta_0\sqrt{m})^{(\frac{m}{p})} = \xi_m^{(\frac{m}{p})}.$$

As ξ_m is a unit and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right)$, it follows that $\xi_m^{p-(\frac{d}{p})} \equiv 1 \bmod p\mathcal{O}_K$. ∎

Proof of Proposition 2.1. Let $\xi_m^{(p-(\frac{d}{p}))/2} = \alpha_1 + \beta_1\sqrt{m}$. It is obvious that $\xi_m^{-(p-(\frac{d}{p}))/2} = \alpha_1 - \beta_1\sqrt{m}$. Now,

$$2\beta_1\sqrt{m} = \xi_m^{-(p-(\frac{d}{p}))/2}\big(\xi_m^{p-(\frac{d}{p})} - 1\big) \in p\mathcal{O}_K.$$

When $\left(\frac{m}{p}\right) = -1$, $p\mathcal{O}_K$ is a prime ideal. As m is not divisible by p, $\sqrt{m}$ does not belong to $p\mathcal{O}_K$. Therefore, $2\beta_1 \in p\mathbb{Z}$, i.e.,

$$\xi_m^{(p-(\frac{d}{p}))/2} = \alpha_1 + \beta_1\sqrt{m} \in \mathbb{Z} + p\mathcal{O}_K = \mathcal{O}_p.$$

When $\left(\frac{m}{p}\right) = 1$, $p\mathcal{O}_K$ splits as a product $\wp_1\wp_2$ of two prime ideals. As m is not divisible by p, $\sqrt{m} \notin \wp_i$ and therefore $2\beta_1 \in \wp_i$ $(i = 1, 2)$. Consequently, $2\beta_1 \in p\mathbb{Z}$, and $\xi_m^{(p-(\frac{d}{p}))/2} \in \mathcal{O}_p$ in this case too. ∎

Proof of Proposition 2.2. Let $p - \left(\frac{d}{p}\right) = l2^s$ and $\xi_m^l = \alpha_l + \beta_l\sqrt{m}$. From $\xi_m^{2l} - 1 \in p\mathcal{O}_K$ we can conclude that $4(\alpha_l^2 + m\beta_l^2 - 1)$ and $4\alpha_l\beta_l$ are in $p\mathbb{Z}$, noting that α_l and β_l can be half-integers when $m \equiv 5 \pmod 8$. If p divides $2\beta_l$ we are done with our proof. If not, then p must divide $2\alpha_l$ from the second condition. But p also divides $4(\alpha_l^2 + m\beta_l^2 - 1)$. Hence $4m\beta_l^2 \equiv 4 \pmod p$. On the other hand, ξ_m^l has norm 1 as ξ_m has norm 1. Therefore $4(\alpha_l^2 - m\beta_l^2) = 4$ and $4m\beta_l^2 \equiv -4 \pmod p$. This means p divides 8, which is a contradiction. Therefore we have our desired result. ∎

3. Fundamental unit of norm -1. In this section we assume that the fundamental unit $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ of $\mathbb{Q}(\sqrt{m})$ has norm -1, and obtain information about the relative class number for odd prime conductors that do not divide m. We will show that if d is a quadratic non-residue modulo a Mersenne prime f, then the conductor f has relative class number 1. Finally, we will show that if f is a Sophie Germain prime such that d is a quadratic residue modulo $2f+1$, then the conductor $2f+1$ has relative class number 1. Note that we now have $\xi_m^{-1} = -(\alpha_0 - \beta_0\sqrt{m})$. The following lemma is almost obvious.

Lemma 3.1. ${\xi_m}^{p-\left(\frac{d}{p}\right)} \equiv \left(\frac{d}{p}\right) \pmod p$ *for any odd prime p not dividing m.*

Proof. We have

$$\xi_m^p \equiv \alpha_0^p + \beta_0^p m^{(p-1)/2}\sqrt{m} \equiv \alpha_0 \pm \beta_0\sqrt{m} \equiv \left(\frac{d}{p}\right)\xi_m^{\left(\frac{d}{p}\right)} \pmod{p\mathcal{O}_K},$$

As ξ_m is a unit in $\mathcal{O}_K$, the lemma follows. ∎

Proposition 3.2. *If p is an odd prime not dividing m then $p \equiv 1 \pmod 4$ if and only if $\xi_m^{(p-(\frac{d}{p}))/2} \in \mathcal{O}_p$.*

Proof. We can assume that the fundamental units ξ_m are in $\mathbb{Z}[\sqrt{m}]$, as the argument is exactly similar for the case $2\xi_m \in \mathbb{Z}[\sqrt{m}\,]$ for an odd prime p.

First assume that $p \equiv 1 \pmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$. Now $\xi_m^{(p-1)/2} = \alpha_1 + \beta_1\sqrt{m}$ has norm 1 as $(p-1)/2$ is even, so its inverse is $\xi_m^{-(p-1)/2} =$

$\alpha_1 - \beta_1\sqrt{m}$. By Lemma 3.1,

$$2\beta_1\sqrt{m} = \xi_m^{(p-1)/2} - \xi_m^{-(p-1)/2} = \xi_m^{-(p-1)/2}(\xi_m^{p-1} - 1) \in p\mathcal{O}_K.$$

From $2\beta_1\sqrt{m} \in p\mathcal{O}_K$ it follows that $2m\beta_1 = \sqrt{m}\cdot 2\beta_1\sqrt{m} \in p\mathcal{O}_K$. Hence, $2m\beta_1 \in p\mathbb{Z}$, so $p \mid \beta_1$, since $2m$ is invertible modulo p.

Now let $p \equiv 1 \pmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$, so $p\mathcal{O}_K$ is a prime ideal. Then $\xi_m^{(p+1)/2} = \alpha_2 + \beta_2\sqrt{m}$ has norm -1 as $(p+1)/2$ is odd, so $\alpha_2^2 - m\beta_2^2 = -1$. By Lemma 3.1,

$$\xi_m^{p+1} + 1 = (\xi_m^{(p+1)/2})^2 + 1 \in p\mathcal{O}_K \;\Rightarrow\; \alpha_2^2 + m\beta_2^2 + 1 + 2\alpha_2\beta_2\sqrt{m} \in p\mathcal{O}_K.$$

If p does not divide β_2 then p divides α_2 and $m\beta_2^2 = 1 + \alpha_2^2 \equiv 1 \pmod p$ contradicts $\left(\frac{m}{p}\right) = -1$. Hence, $p \mid \beta_2$ and $\xi_m^{(p+1)/2} \in \mathcal{O}_p$.

Assume in turn that $p \equiv 3 \pmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$ so that $\xi_m^{p+1} \equiv -1 \pmod{p\mathcal{O}_K}$. Now $\xi_m^{(p+1)/2} = \alpha_2 + \beta_2\sqrt{m}$ has norm 1 as $(p+1)/2$ is even, so $\alpha_2^2 - m\beta_2^2 = 1$. If $\xi_m^{(p+1)/2} \in \mathcal{O}_p$, then

$$p \mid \beta_2 \;\Rightarrow\; -1 \equiv \xi_m^{p+1} \equiv \alpha_2^2 \equiv 1 \pmod{p\mathcal{O}_K} \;\Rightarrow\; p = 2.$$

Next assume that $p \equiv 3 \pmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$ so that $\xi_m^{p-1} \equiv 1 \pmod{p\mathcal{O}_K}$. Now $\xi_m^{(p-1)/2} = \alpha_2 + \beta_2\sqrt{m}$ has norm -1 as $(p-1)/2$ is odd, so $\alpha_2^2 - m\beta_2^2 = -1$. Then $\xi_m^{p-1} = \alpha_2^2 + m\beta_2^2 + 2\alpha_2\beta_2\sqrt{m} \equiv 1 \pmod{p\mathcal{O}_K}$, so p divides $2\alpha_2\beta_2$. If $\xi_m^{(p-1)/2} \in \mathcal{O}_p$ then

$$p \mid \beta_2 \;\Rightarrow\; 1 \equiv \xi_m^{p-1} \equiv \alpha_2^2 \equiv -1 \pmod{p\mathcal{O}_K} \;\Rightarrow\; p = 2. \blacksquare$$

The following corollaries now follow immediately from Dirichlet's formula.

Corollary 3.3.

(i) *If $p \equiv 1 \pmod 4$ is an odd prime not dividing m, then the relative class number for conductor p is not* 1.
(ii) *If $p \equiv 3 \pmod 4$ is an odd prime not dividing m, then the relative class number for conductor p is odd.*

Proposition 3.4. *When $\mathbb{Q}(\sqrt{m})$ has fundamental unit of norm -1, the relative class number for conductor* 3 *must be* 1.

Proof. If the fundamental unit of $\mathbb{Q}(\sqrt{m})$ has norm -1 then -1 will be a quadratic residue modulo any odd prime dividing d. Hence only odd primes dividing m must be of the form $4k+1$. In particular, 3 cannot divide m, and $\psi(3) = 2$ or 4. By the second part of the above corollary, $H_d(3)$ is odd. The only odd factor of 2 or 4 is 1, hence $H_d(3) = 1$. $\blacksquare$

Corollary 3.5. *There are infinitely many real quadratic fields of relative class number* 1 *for the conductor* 3.

Proof. If m is a prime which is congruent to 1 modulo 4, it is an easy exercise to show that the fundamental unit of $\mathbb{Q}(\sqrt{m})$ has norm -1. By Dirichlet's theorem on primes in arithmetic progression, there are infinitely many such primes m. Hence the corollary follows from Proposition 3.4. ∎

PROPOSITION 3.6. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field with fundamental unit ξ_m of norm -1. If d is a quadratic non-residue modulo a Mersenne prime f, then the relative class number for conductor f is* 1.

Proof. Let $\xi_m = \alpha_0 + \beta_0\sqrt{m}$. Suppose there exists a Mersenne prime $f = 2^p - 1$ for some prime p such that $\left(\frac{d}{f}\right) = -1$. Now,

$$\psi(f) = f\left(1 - \left(\frac{d}{f}\right)\frac{1}{f}\right) = 1 + f = 2^p.$$

By Corollary 3.3, $H_d(f)$ is an odd divisor of 2^p, hence it must be 1. ∎

A prime f is said to be a *Sophie Germain prime of the first kind* if $2f+1$ is also a prime. We can deduce the following result.

PROPOSITION 3.7. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field with fundamental unit ξ_m of norm -1. If d is a quadratic residue modulo $2f+1$ where f is a sufficiently large Sophie Germain prime of the first kind, then the relative class number for the conductor $2f+1$ is* 1.

Proof. Let $\xi_m = \alpha_0 + \sqrt{m}\,\beta_0$. Suppose f is a Sophie Germain prime such that d is a quadratic residue modulo the prime $2f+1$ and $2f+1$ does not divide $\tilde{\alpha}_0\tilde{\beta}_0$. Then

$$\psi(2f+1) = (2f+1)\left(1 - \left(\frac{d}{2f+1}\right)\frac{1}{2f+1}\right) = 2f.$$

Now, $2f+1$ not dividing $2m\tilde{\alpha}_0\tilde{\beta}_0$ implies $\phi(f) \neq 2$. By Proposition 3.2,

$$2f+1 \equiv 3 \pmod 4 \;\Rightarrow\; \theta(f) \neq f \;\Rightarrow\; \theta(f) = 2f.$$

Therefore,

$$H_d(2f+1) = \frac{\psi(2f+1)}{\theta(2f+1)} = 1. \;∎$$

The following corollary follows directly from the previous two propositions.

COROLLARY 3.8. *Suppose $\mathbb{Q}(\sqrt{m})$ has only finitely many prime conductors of relative class number* 1. *Then*

(i) *There are only finitely many Mersenne primes with d as quadratic non-residue.*
(ii) *There are only finitely many Sophie Germain primes of the first kind with d as quadratic residue.*

4. A criterion for non-existence of conductor of relative class number 1. The main result of this section is the following criterion for non-existence of a conductor f for which the relative class number of $\mathbb{Q}(\sqrt{m})$ is 1. As before, we have $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ as the fundamental unit and d is the discriminant of $\mathbb{Q}(\sqrt{m})$. In view of Proposition 3.4, ξ_m must have norm 1.

THEOREM 4.1. *There does not exist any conductor f for which the relative class number of $\mathbb{Q}(\sqrt{m})$ is 1 if and only if*

(i) *m divides $\tilde{\beta_0}$, and*
(ii) *if m is odd then $m \neq 1 \pmod 8$ and $\tilde{\beta_0}$ is an even integer.*

Proof. Let us first prove the sufficiency. If p is an odd prime dividing m, then p divides $\tilde{\beta_0}$. So $\xi_m \in \mathcal{O}_p$ and $\theta(p) = 1$. But

$$\psi(p) = p\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) = p > 1.$$

If p is an odd prime not dividing m then by Proposition 2.1 we have $\xi_m^{(p-(\frac{d}{p}))/2} \in \mathcal{O}_p$. Therefore, $\theta(p) \leq (p - (\frac{d}{p}))/2$. Now by the formula (1.1) of Dirichlet,

$$\psi(p) = p\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) \;\Rightarrow\; H_d(p) = \frac{\psi(p)}{\theta(p)} \geq 2.$$

The only remaining prime is $p = 2$ when m is odd. Under the given conditions, $\psi(2) = 2\big(1 - \big(\frac{d}{2}\big)\frac{1}{2}\big) = 3$ or 2 (when $d \equiv -3 \pmod 8$), and $\theta(2) = 1$ as $\tilde{\beta_0}$ is even. Therefore, $H_d(2) > 1$. For any non-prime conductor f, our theorem follows from the fact that $H_d(g)$ divides $H_d(f)$ if g divides f (see [1]).

Conversely, suppose there does not exist any f with $H_d(f) = 1$. Any prime q that divides m but does not divide $\tilde{\beta_0}$ will give $H_d(q) = \psi(q)/\theta(q) = 1$. Hence m must divide $\tilde{\beta_0}$. Also, $H_d(2) \neq 1$ implies that

$$\psi(2) = 2\left(1 - \left(\frac{d}{2}\right)\frac{1}{2}\right) = 2 \text{ or } 3,$$

and hence m must be of the form $m \not\equiv 1 \pmod 8$ if m is odd. In that case, $\theta(2) = 1$ and hence $\tilde{\beta_0}$ must be an even integer. ∎

EXAMPLE. Consider $m = 46$. It is well known that $\beta_0 = 3588$ (see [2]), which is divisible by 46. Hence $\mathbb{Q}(\sqrt{46})$ does not have relative class number 1 for any conductor.

Acknowledgements. We would like to thank the anonymous referee for his/her valuable comments.

References

[1] H. Cohn, *A numerical study of the relative class numbers of real quadratic integral domains*, Math. Comp. 16 (1962), 127–140.
[2] H. Davenport, *The Higher Arithmetic*, 8th ed., Cambridge Univ. Press, 2008.
[3] R. A. Mollin, *Proof of relative class number one for almost all real quadratic fields and a counterexample for the rest*, Gen. Math. Notes 17 (2013), no. 2, 81–90.
[4] A. J. Stephens and H. C. Williams, *Some computational results on a problem concerning powerful numbers*, Math. Comp. 50 (1988), 619–632.

Debopam Chakraborty, Anupam Saikia
Department of Mathematics
Indian Institute of Technology, Guwahati
Guwahati 781039, Assam, India
E-mail: c.debopam@iitg.ernet.in
a.saikia@iitg.ernet.in

Received on 8.10.2013
and in revised form on 19.3.2014 (7607)