SeMA (2015) 67:71–75
DOI 10.1007/s40324-014-0027-4

On generalized Mersenne Primes and class-numbers of equivalent quadratic fields and cyclotomic fields

Azizul Hoque · Helen K. Saikia

Received: 8 October 2014 / Accepted: 11 November 2014 / Published online: 25 November 2014

Abstract In this paper we define equivalent quadratic fields and prove that generalized Mersenne primes generate a family of infinitely many equivalent quadratic fields with equivalent index 2 and whose class numbers are divisible by 3. We also prove that the class-number of the cyclotomic field $\mathbb{Q}(\zeta_m)$, where $m \in \mathbb{N}$ and ζ_m is a primitive m-th root of unity, is divisible by a certain integer g.

Keywords Generalized mersenne prime · Equivalent quadratic field · Cyclotomic field · Class-number · Discriminant

Mathematics Subject Classification 11R29 · 11R11 · 11R18

1 Introduction

The class number problem of quadratic field and cyclotomic field is one of the most intriguing unsolved problems in algebraic number theory and it has been the object of attention of many years among researchers. It was proved by Nagel [6] that there are infinitely many quadratic number fields each with class number divisible by a given positive integer. Weinberger [10] showed that for all positive integers n, there are infinitely many real quadratic fields with class numbers divisible by n. Ankeny and Chowla [1] proved that there exist infinitely many imaginary quadratic fields each with class number divisible by g where g is any given rational integer. Hartung [3] constructed a family of infinitely many imaginary quadratic fields whose class number is divisible by 3. Ankeny et al.[2], Lang [5], Takeuchi [8] and Osada [7] independently proved that the class-number of the maximal real subfield of a cyclotomic field is greater than 1. Osada [7] also proved that this class-number is divisible by

A. Hoque (✉) · H. K. Saikia
Department of Mathematics, Gauhati University, Guwahati 781014, India
e-mail: ahoque.ms@gmail.com

H. K. Saikia
e-mail: hsaikia@yahoo.com

a certain integer n. Watabe [9] deduced some results on the divisibility of the class-numbers of certain cyclotomic fields. Recently, we generalized the results of Takeuchi [8] in one of our papers.

In this paper, we introduce the notion of equivalent quadratic fields. We denote by Δ_F and rad(F) respectively the discriminant and radicand of the quadratic field F. Two quadartic fields F_1 and F_2 are said to be equivalent if there exists an integer n satisfying $1 < n < \min\{|\text{rad}(F_1)|, |\text{rad}(F_2)|\}$ such that $\Delta_{F_1} \equiv \Delta_{F_2} (\text{mod } n)$. Such a smallest positive integer n is called the equivalent index of F_1 and F_2. We write $F_1 \triangleq F_2$ to represent F_1 is equivalent to F_2 or simply F_1 and F_2 are equivalent. Also by $(F_1 : F_2)$ we mean the equivalent index of $F_1 \triangleq F_2$. We show that generalized Mersenne primes generate a family of infinitely many equivalent quadratic fields with equivalent index 2 and whose class numbers are divisible by 3. We also establish that the class-number of the cyclotomic field $\mathbb{Q}(\zeta_m)$, where $m \in \mathbb{N}$ and ζ_m is a primitive m-th root of unity, is divisible by a certain integer g.

Example Consider the quadratic fields $F_1 = \mathbb{Q}(\sqrt{13})$, $F_2 = \mathbb{Q}(\sqrt{15})$ and $F_3 = \mathbb{Q}(\sqrt{21})$. Then $\text{rad}(F_1) = 13$, $\text{rad}(F_2) = 15$, $\text{rad}(F_3) = 21$, $\Delta_{F_1} = 13$, $\Delta_{F_2} = 60$ and $\Delta_{F_3} = 21$. Thus $F_1 \triangleq F_3$ with $(F_1 : F_3) = 2$ and $F_2 \triangleq F_3$ with $(F_2 : F_3) = 3$. But F_1 and F_2 are not equivalent.

2 Main results

The concept of generalized Mersenne Prime(GMP) was defined by Hoque and Saikia [4] as a prime of the form:

$$M_{p,q} = p^q - p + 1$$

where p and q are positive integers.

Throughout this paper we consider the GMP, $M_{p,q}$ with the restrictions: p is odd prime and q is odd integer.

We see that $M_{p,q} \equiv 1 (\text{mod } 3)$ and $M_{p,q} \equiv 1 (\text{mod } 4)$.

We consider the following trinomials:

$$f_1(x) = x^3 - M_{p,q}x + p$$
$$f_2(x) = x^3 - px + M_{p,q}$$

The discriminants of $f_1(x)$ and $f_2(x)$ are respectively $D(f_1) = 4M_{p,q}^3 - 27p^2$ and $D(f_2) = 4p^3 - 27M_{p,q}^2$. For all odd primes p and odd integers $q > 1$, we have $D(f_1) > 0$ and $D(f_2) < 0$. Now

$$f_1(x) \equiv x^3 - x \pm 1 \text{ (mod 3)}$$
$$f_2(x) \equiv x^3 \pm x + 1 \text{ (mod 3)}$$

We see both the trinomials in the right sides are irreducible mod 3. Thus both $f_1(x)$ and $f_2(x)$ are irreducible over $\mathbb{Q}$.

Theorem 2.1 *The class number of the real quadratic field $\mathbb{Q}(\sqrt{D(f_1)})$ and the imaginary quadratic field $\mathbb{Q}(\sqrt{D(f_2)})$ are divisible by 3.*

Proof Let $F_1(M_{p,q}) = \mathbb{Q}(\sqrt{D(f_1)}) = \mathbb{Q}(\sqrt{4M_{p,q}^3 - 27p^2})$ and $F_2(-M_{p,q}) = \mathbb{Q}(\sqrt{D(f_2)})$ $= \mathbb{Q}(\sqrt{4p^3 - 27M_{p,q}^2})$. Let K_i be the splitting field of $f_i(x)$ and G_i be the Galois group

of K_i $(i = 1, 2)$ over $\mathbb{Q}$. Since $f_1(x)$ and $f_2(x)$ are irreducible over $\mathbb{Q}$, G_1 and G_2 are isomorphic to S_3. Also $(2M_{p,q}, 3p) = 1$ and $(2p, 3M_{p,q}) = 1$. Thus by Proposition 1 in [12], K_i over F_i $(i = 1, 2)$ is unramified. Also the Galois group of K_i over F_i $(i = 1, 2)$ is cubic cyclic group. Thus K_i over F_i $(i = 1, 2)$ is cubic cyclic unramified extension. By class field theory, the Hilbert class field of F_i contains K_i $(i = 1, 2)$ and thus the class number of F_i $(i = 1, 2)$ is divisible by 3. □

Theorem 2.2 *There are infinitely many equivalent quadratic fields with index* 2 *whose class numbers are divisible by* 3.

Proof Since $D(f_1) = 4M_{p,q}^3 - 27p^2 \equiv 1 (\text{mod } 4)$, the discriminant of the real quadratic field is $\Delta_{F_1(M_{p,q})} = D(f_1)$.

Also, $D(f_2) = 4p^3 - 27M_{p,q}^2 \equiv 1 (\text{mod } 4)$ gives the discriminant of the imaginary quadratic field is $\Delta_{F_2(-M_{p,q})} = D(f_2)$.
Now

$$\Delta_{F_1(M_{p,q})} - \Delta_{F_2(-M_{p,q})} = 4\left(M_{p,q}^3 - p^3\right) + 27\left(M_{p,q}^2 - p^2\right) \equiv 0 (\text{mod } 2)$$

Thus the quadratic fields $F_1(M_{p,q}) \triangleq F_2(-M_{p,q})$ with $(F_1(M_{p,q}) : F_2(-M_{p,q})) = 2$.

Now we count the number of real quadratic fields of the form $F_1(M_{p,q})$.

Under the truth of the Conjecture 2.1 [4], we can find infinitely many GMPs such that $D(f_1)$'s are not perfect square and hence infinitely many quadratic fields of the form $F_1(M_{p,q}) = \mathbb{Q}(\sqrt{D(f_1)})$. Let S be the set of all $D(f_1)$'s which give rise to same fields more than once. We fix p. Let q_0 be give one member in S. Suppose $4M_{p,q_0}^3 - 27p^2 = a^2d$ for some fixed square-free integer d and an integer a. Then if $F_1(M_{p,q_0}) = F_1(M_{p,q})$, there exists an integer c such that $4M_{p,q}^3 - 27p^2 = c^2a^2d$. Thus $(M_{p,q},\ ca)$ is an integral solution of

$$4X^3 = dY^2 + 27p^2 \tag{1}$$

By Siegel's theorem, the algebraic curve given by the Diophantine equation (1) has only finite numbers of integral solutions. Thus $\#S$ is finite and hence there are infinitely many real quadratic fields of the form $F_1(M_{p,q})$. Also corresponding to each value of $M_{p,q}$ that contributes a real quadratic field of the form $F_1(M_{p,q})$, we get one imaginary quadratic field of the form $F_2(-M_{p,q})$. Thus there are infinitely many imaginary quadratic fields of the form $F_2(-M_{p,q})$. By the Theorem 2.1, we complete the proof. □

Yamaguchi [11] showed the following result.

Lemma 2.3 [11] *If* $\phi(m) > 4$, *then* $h(\mathbb{Q}(\sqrt{m}))|H(\mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}))$, *where* ϕ *stands for the Euler's function and* $m > 0$ *is an integer.*

Now from Theorem 2.1 and this lemma, we obtain the following result.

Theorem 2.4 *Let* $m = D(f_1)$ *such that* $\phi(m) > 4$. *Then* $3|H(\mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}))$.

Lemma 2.5 [9] *If* $u \geq 5$ *is a prime and* v *is a prime with* $v \equiv 1 (\text{mod } u)$, *then*

(i) $u^{\frac{u-3}{2}} \mid h(\mathbb{Q}(\zeta_{uv}))$.
(ii) $2^{\frac{u-3}{2}} \mid h\left(\mathbb{Q}\left(\sqrt{(-1)^{\frac{v-1}{2}}v}, \zeta_u\right)\right)$.
(iii) $2^{\frac{u-3}{2}} \mid h(\mathbb{Q}(\zeta_{uv}))$.

Applying this lemma we obtain the following result.

Theorem 2.6 *For any prime $u \geq 5$, the following statements hold:*

(i) $u^{\frac{u-3}{2}} \mid h(\mathbb{Q}(\zeta_{uM_{p,q}}))$.
(ii) $2^{\frac{u-3}{2}} \mid h\left(\mathbb{Q}\left(\sqrt{M_{p,q}}, \zeta_u\right)\right)$.
(iii) $2^{\frac{u-3}{2}} \mid h(\mathbb{Q}(\zeta_{uM_{p,q}}))$.

We now characterise units and irreducible elements in the real quadratic field $F_1(M_{p,q})$.

Theorem 2.7 *Let $D > 1$ be an square-free integer such that $D \equiv 1 (\mathrm{mod}\ 4)$. Let $\alpha = 1 \pm u$, where u is a unit in the real quadratic field $\mathbb{Q}(\sqrt{D})$. Then the following hold:*

(i) *If $N(u) = -1$, then α is irreducible if and only if u is expressible as $u = \frac{a+b\sqrt{D}}{2}$ such that a is an odd prime and b is an odd integer.*
(ii) *If $N(u) = 1$, then α is irreducible if and only if u is expressible as $u = \frac{a+b\sqrt{D}}{2}$ such that $a \pm 2$ is an odd prime and b is an odd integer.*

Proof (i) Since $D \equiv 1 (\mathrm{mod}\ 4)$ and u is a unit in $\mathbb{Q}(\sqrt{\mathrm{D}})$, u is of the form

$$\frac{a + b\sqrt{D}}{2}$$

where a and b are integers.
Now $N(\alpha) = \frac{(2\pm a)^2 - Db^2}{4} = N(u) \pm a + 1 = \pm a$.
For α to be irreducible in $\mathbb{Q}(\sqrt{\mathrm{D}})$, a should be a rational prime.
If $a = 2$, then $N(u) = -1$ gives a contradiction to D$\equiv$ 1(mod 4).
Thus α to be irreducible in $\mathbb{Q}(\sqrt{\mathrm{D}})$, a should be a rational odd prime.
Again, $N(u) = -1 \Rightarrow a^2 - db^2 = -4 \Rightarrow b \equiv 1 (\mathrm{mod}\ 2)$.
Thus b is a rational odd integer.
The converse part is obvious as $N(\alpha) = \pm a$, a rational odd prime.
Similarly we can prove (ii).
As a consequence we have the following result. □

Corollary 2.8 *Let u be a unit in $F_1(M_{p,n})$ and $\alpha = 1 \pm u$. Then the following hold:*

(i) *If $N(u) = 1$, then α is irreducible if and only if u is expressible as $u = \frac{a+b\sqrt{D(f_1)}}{2}$ such that a is a rational odd prime and b is a rational odd integer.*
(ii) *If $N(u) = 1$, then α is irreducible if and only if u is expressible as $u = \frac{a+b\sqrt{D(f_1)}}{2}$ such that $a \pm 2$ is a rational odd prime and b is a rational odd integer.*

Acknowledgments The first author acknowledges UGC for JRF Fellowship (No. GU/UGC/VI(3)/JRF/2012/2985).

References

1. Ankeny, N.C., Chowla, S.: On the divisibility of the class numbers of quadratic fields. Pac. J. Math. **5**, 321–324 (1955)
2. Ankeny, N.C., Chowla, S., Hasse, H.: On the class-number of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. **217**, 217–220 (1965)
3. Hartung, P.: Explicit construction of a class of infinitely many imaginary quadratic fields whose class number is divisible by 3. J. Number Theor. **6**, 279–281 (1974)

4. Hoque, A., Saikia, K.: On generalized Mersenne prime. SeMA. **66**, 1–7 (2014). doi:10.1007/s40324-014-0019-4
5. Lang, S.D.: Note on the class-number of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. **290**, 70–72 (1977)
6. Nagel, T.: Uber die Klassenzahl imaginr quadratischer zahlkorper. Abh. Math. Semin. Univ. Hamburg **1**, 140–150 (1922)
7. Osada, H.: Note on the class-number of the maximal real subfield of a cyclotomic field. Manuscr. Math. **58**, 215–227 (1987)
8. Takeuchi, H.: On the class-number of the maximal real subfield of a cyclotomic field. Can. J. Math. **33**(1), 55–58 (1981)
9. Watabe, M.: On class numbers of some cyclotomic fields. J. Reine Angew. Math. **301**, 212–215 (1978)
10. Weinberger, P.J.: Real Quadratic fields with Class number divisible by n. J. Number Theor. **5**, 237–241 (1973)
11. Yamaguchi, I.: On the class-number of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. **272**, 217–220 (1975)
12. Yamamoto, Y.: On unramified Galois extensions of quadratic number fields. Osaka J. Math. **7**, 57–76 (1979)