South Asian Journal of Mathematics 2013, Vol. 3 (1) : 91 ∼ 93
www.sajm-online.com ISSN 2251-1512 RESEARCH ARTICLE

Note on the divisibility of the class numbers of the imaginary quadratic fields $Q(\sqrt{3^{2e}-4k^n})$

K. Raja Rama Gandhi ①*

① Department of Mathematics, BITS-VIZAG, India
E-mail: editor126@gmail.com

Received: 11-15-2012; Accepted: 1-21-2013 *Corresponding author

Abstract In this paper, we apply an elementary approach to conclude the respected theorem(s)/lemma(s) of [1]. In the paper [1], the author studied the class number imaginary filed theory in more deeply and prepared manuscript in high order. However, this paper will increase the readability of the paper [1], and motivate to re-producing the work with additional features on the same area.

Key Words class number, equivalence classes, ring of integers, quadratic field

MSC 2010 11R11, 11R29

1 Introduction

In 1798 at the age of 21 Carl Friedrich Gauss wrote his classic number theory book Disquisitiones Arithmeticae, containing many results such as Legendre and Euler, along with many of his own contributions. Gauss addresses issues dealing with the behavior of binary quadratic forms, in particular, expressions that can be written as $ax^2 + 2bxy + cy^2$ with discriminant defined to be $b^2 - ac$. Of course, now we represent these forms as, with discriminant defined to be $b^2 - ac$. Of course, now we represent these forms as, $ax^2 + 2bxy + cy^2$ with discriminant defined to be $b^2 - 4ac$.

For more references, I would like to suggest studying the standard text books and recent paper [1] for more introductory material, especially the current research in this particular area. I have seen the paper [1] closely and I felt to produce a simple proof of theorem 4.2 of [1] and addendum at page number 25 of [1]. Also, the lemma 2.5 of page number 6 of [1]. This is not subsequent of paper [1] and there is no comparison of [1] with this paper, as [1] has its own importance.

2 Preliminaries

I would like to suggest, the readers to study [1] and the following preliminaries definitions and basic definitions for better understanding. I have seen the entire paper of [1] and it is quite interesting and I would like to add my own aroma to [1], see the third section and let me know the taste of the paper.

Citation: K. Raja Rama Gandhi, Note on the divisibility of the class numbers of the imaginary quadratic fields $Q(\sqrt{3^{2e}-4k^n})$, South Asian J Math, 2013, 3(1), 91-93.

Definition 2.1. *A binary quadratic form $f(x,y) = ax^2+bxy+cy^2$ is called positive definite if $f(x,y) \leqslant 0$ However, in the case of negative definite. To concern the positive definite form, we fix $a > 0$ with $\Delta = b^2 - 4ac < 0$ and by a simple square completion, we see*

$$ax^2 + bxy + cy^2 = a([x + \frac{by}{2a}]^2 - [\Delta][\frac{y}{2a}]^2).$$

Definition 2.2. *If $f_{x,y} = g_{m,n}$ with $(m,n) = L(x,y)$ for $L \in SL(2,Z)$ then we say $f_{x,y}$ and $g_{x,y}$are equivalent. In case, L has $\Delta = +1$, then f and g are properly equivalent.*

Example 2.3. Consider $\Delta = -20$ of

$$x^2 + 5y^2 \tag{1}$$

and

$$2x^2 + 2xy + 3y^2 \tag{2}$$

are not equivalent forms. Let the transform $() \in SL(2,Z)$ of x and y of (1) yields in $(5C^2 + A^2)x^2 + (2AB+10CD)xy+(5D^2+B^2)y^2$ where the coefficients will not match to the coefficients of (2) as A, B, C and D are in Z. However, to find these various points, we can see them only at $\{1, 9\}$ in $U(Z/20Z)$ for (1) and $\{3, 7\}$ for (2).

Definition 2.4. *A complex quadratic number field is a field $Q(\sqrt{d})$ where $d < 0$ is a square free.*

Example 2.5. Consider, $Q(\sqrt{-5})$ has ring of integers [2] $O_{-5} = Z\lfloor\sqrt{d}\rfloor$.

Observe that element 6 can be factorized in two differ ways, as $6 = 2.3 = (1-\sqrt{-5})(1+\sqrt{-5})$. Now the norm of any element of will be, $N(a+b\sqrt{-5}) = a^2 + 5b^2 \neq 2$ *or* 3. As elements of norm 6 is irreducible, and we see; $N(1+\sqrt{-5}) = 6 = N(1-\sqrt{-5})$ As and $N(2) = 2.2$, there is no solution of $l^2 + 5m^2 = 2$ in integers.

Theorem 2.6. *Any odd prime p can be written in the form of $x^2 + y^2$ when $p \equiv 1(\mathrm{mod}4)$.*

The above theorem is well known by Fermat. Let $L = (1,0,1)$ and L has $\Delta = -4$. If (a,b,c) is reduced representative of some equivalence class [3] with $\Delta \Rightarrow |b| \leqslant a \leqslant |c|$ and $\Delta = -4$. Thus $b^2 = 4(ac-1)$. Since $|ac| \geqslant b^2$, we should have $ac-1 = 0$. The only form of L is $(1,0,1)$. Thus $h(-4) = 1$ and p can be expressible by (1, 0, 1) if and only if $-4 \equiv \Delta(\mathrm{mod}4p)$. Similarly one can show that any odd prime p can be expressible in the form x^2+2y^2 when $p \equiv 1$ or 3 (mod 8). The above section is might be useful to realize [1].

3 Theorem(s) from [1]

In [1], (see page number 25). If n is even integer > 5, then the class number of $Q(\sqrt{3^{2e}-4k^n})$ (#) is divisible by n except $(k,n) = (13,8)$. The reason for this statement is quite unclear to readers. Let me discuss the reason behind this statement!

Let $\alpha = \sqrt{1-4k^n}$ and let $K = Q(\sqrt{\alpha})$. For $k > 1$, the minimal polynomial $\theta = \frac{1+\alpha}{2}$ of and it is $\theta^2 - \theta + k^n = 0$. Indeed, we even have $Z[\alpha]$ is the ring of integers of K. Let p be a prime dividing k.

Then p splits in K, as can be seen by factoring the polynomial above modulo p. Indeed, there is a unique such ideal which divides θ, namely $p = (p, \theta)$. Equally, every prime dividing θ also divides k. Since θ and $1 - \theta$ are co-prime, and since $\theta\overline{\theta} = \theta(1 - \theta) = k^n$, it follows that the exponent of p in θ is n-times the exponent of p in k. In particular, there exists an ideal a of norm k such that $a^n = \theta$. Suppose that is principal. Then

$$k^m = N(a) = a^2 + ab + b^2k^n = (a + \frac{b}{2})^2 + b^2(k^n - \frac{1}{4}) \geqslant k^n,$$

as long as b 0. Yet if $b = 0$, then $\theta^m = a^{mn} = a^n$, and then $\theta = \pm a^n$ (the only units in K are ± 1), which is nonsense. Hence and thus $m \geqslant n$ (using the fact that $k > 1$), and thus the order of a in the class group [4] is exactly n. It follows that the class number is divisible by n for any n. From the above proof, one can realize that, it is not only for $n = 2, 4, n = 1597$ and any other natural number.

The following theorem is drawn from [1] (see theorem 4.2 at [1]), however one can realize by my flavor.

Theorem 3.1. *Let n be a positive integer, l an odd prime number and e is a non-negative integer. If $(n, e) \neq (4, 0)$, then the class number of imaginary quadratic fields $Q(\sqrt{1 - 4(2l^e)^n})$ are divisible by n.*

Proof. let us take in the place of then our theorem reduced from $Q(\sqrt{1 - 4(2l^e)^n})$ to $Q(\sqrt{1 - 4k^n})$, which is very same as (#). Thus, the required proof is concluded. The following lemma 3.2 is lemma 2.5 of [1] at page 6. □

Lemma 3.2. (1) *The equation $x^4 - 2y^2 = 1$ has no positive integer solution (x, y).* (2) *The equation $x^4 - 2y^2 = -1$ has only one positive integer solution $(x, y) = (1, 1)$.*

Proof. The only integer solutions of $x^4 - 2y^2 = 1$ are $(1, 0)$ and $(-1, 0)$. For x has to be odd, re-write the equation as $(x^2 - 1)(x^2 + 1) = 2y^2$ with $(x^2 + 1, x^2 - 1) = 2$. Since $x^2 + 1$ is in the form of $8k + 2$ and it follows that $x^2 + 1 = 2m^2$ and $x^2 - 1 = n^2$ for some integers of m and n. Obviously, the only integer solutions of $x^2 - 1 = n^2$ are $(x, n) = (-1, 0), (1, 0)$, since 1 and 0 are the only perfect squares, which differ by 1. □

Acknowledgements I am heartily thankful to Mathematician Prof. J. Gopala Krishna and my well-wishers Smt. Sri Lakshmi (secretary and correspondent of BITS-Vizag), Dr. C.V. Gopinath, Akiko Ito and J. Moose.B, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

References

1 http://arxiv.org/pdf/1212.1733.pdf
2 Ronald S. Irving, 'Integers, Polynomials, and Rings', Springer Ver-lag Publication, 2004.
3 S. Shiral,'Number Theory' Indian Academy of Sciences, Universities Press (India)-2003.
4 Benson Farb, Dan Margalit,'A Primer on Mapping Class Groups', Princeton University Press-2012, USA.