REMARKS ON A PROBLEM OF EISENSTEIN

ROGER C. ALPERIN

ABSTRACT. The fundamental unit of $\mathbb{Z}[\sqrt{N}]$ for square-free $N = 5 \, mod \, 8$ is either ϵ or ϵ^3 where ϵ denotes the fundamental unit of the maximal order of $\mathbb{Q}(\sqrt{N})$. We give infinitely many examples for each case.

1. Introduction

For N square-free, the ring of integers $\mathcal{O}_N$ of a real quadratic field $\mathbb{Q}(\sqrt{N})$ has an infinite cyclic group of units of index 2. The generator ϵ for this subgroup is the fundamental unit. The ring of integers $\mathcal{O}_N$ has a subring $\mathcal{A}_N = \mathbb{Z}[\sqrt{N}]$; this is a proper subring if and only if $N = 1 \mod 4$. The subring also has an infinite cyclic subgroup of units generated by ϵ^e; it is easy to see that $e = 1$ or $e = 3$; the latter occurs only if $N = 5 \mod 8$.

Characterizing those N for which $e = 3$ is the problem of Eisenstein in the title of this article. By elementary methods we shall give infinitely many examples for each of the cases of $e = 1$ or $e = 3$. This problem has been addressed in [3] and [4] using other methods.

2. Main Examples

Basic properties of continued fractions and the relation of equivalence can be found in [2]. Equivalence of two continued fractions means that the periodic parts are equal or equivalently that the two real numbers are related by a linear fractional transformation.

The following examples are well-known [4, p. 297]:

Example 2.1. $\sqrt{a^2+4} = (a; \overline{\frac{a-1}{2}, 1, 1, \frac{a-1}{2}, 2a})$ *for any odd integer* $a > 1$.

Consider $a = 4b \mp 1$ and $N = a^2 + 4$ then

$$\frac{1}{\frac{\sqrt{N}\pm 1}{4} - b} = \frac{4}{\sqrt{N} - a}\frac{\sqrt{N}+a}{\sqrt{N}+a} = 4\frac{\sqrt{N}+a}{N - a^2} = \sqrt{N} + a$$

Proposition 2.2. *Suppose a is odd and greater than 1. For $N = a^2 + 4$, then $\frac{\sqrt{N}\pm 1}{4}$ is equivalent to $\sqrt{N}$.*

Proof. For $a = 4b \mp 1$ the floor of $\frac{\sqrt{N}\pm 1}{4}$ is b. ■

Example 2.3. *For any odd integer $a > 3$,* $\sqrt{a^2-4} = (a-1; \overline{1, \frac{a-3}{2}, 2, \frac{a-3}{2}, 1, 2a-2})$.

As a consequence one can easily show that

$$1+\frac{\sqrt{a^2-4}}{a-2}=(2;\overline{\frac{a-3}{2},1,2a-2,1,\frac{a-3}{2}}).$$

Let $N=a^2-4$ and put $a=4b\pm 1$. For $a=4b-1$ we have

$$\frac{1}{\frac{\sqrt{N}-1}{4}-(b-1)}=\frac{4}{\sqrt{N}-(a-2)}=\frac{\sqrt{N}+(a-2)}{a-2}.$$

For $a=4b+1$ we obtain

$$\frac{1}{\frac{\sqrt{N}+1}{4}-b}=\frac{4}{\sqrt{N}-(a-2)}=\frac{\sqrt{N}+(a-2)}{a-2}.$$

Proposition 2.4. *Suppose a is odd and greater than 3. For $N=a^2-4$ then $\frac{\sqrt{N}\pm 1}{4}$ is equivalent to $\sqrt{N}$.*

Proof. For $a=4b\pm 1$ we have $\frac{\sqrt{N}\pm 1}{4}$ is equivalent to $1+\frac{\sqrt{N}}{a-2}$ which is equivalent to $\sqrt{N}$. ■

Example 2.5. *For any integer $a>1$ $\sqrt{a^2+1}=(a;\overline{2a})$.*

Proposition 2.6. *For $N=4a^2+1$ where a is odd and greater than 3, then $\frac{\sqrt{N}\pm 1}{4}$ is not equivalent to $\sqrt{N}$.*

Proof. The numbers $u_\pm=(\frac{\sqrt{N}\pm 1}{4}-\lfloor\frac{\sqrt{N}\pm 1}{4}\rfloor)^{-1}$ are greater than 1 by definition. They are purely periodic ([2]) since the conjugates are negative and $-\frac{1}{\bar{u}_\pm}=\frac{\sqrt{N}\mp 1}{4}+\lfloor\frac{\sqrt{N}\pm 1}{4}\rfloor$ is greater than 1.

If $\frac{\sqrt{N}\pm 1}{4}$ is equivalent to $\sqrt{N}$ then $u_\pm$ has period length one also. Hence $u_\pm=(\overline{2a};)$. The continued fraction $(\overline{2a};)$ satisfies the equation $x^2-2ax-1$ which has the solutions $\sqrt{a^2+1}\pm a$; these can not be the same as $u_\pm$. This contradiction gives the desired result. ■

3. Relations of Units to Continued Fractions

We suppose that $N=5 \mod 8$ is square-free. It is an elementary exercise to see that the fundamental unit ϵ is a solution to $x^2-Ny^2=\pm 4$ with x, y odd if and only if $e=3$.

Let $\mathcal{A}=\mathcal{A}_N$ and $\mathcal{O}=\mathcal{O}_N$. Consider the ideals $I_\pm=[4,\sqrt{N}\pm 1]$ in $\mathcal{A}$. (the generators are a lattice basis). Extend these ideals to ideals $J_\pm=2[2,\frac{\sqrt{N}\pm 1}{2}]$ in $\mathcal{O}$; thus $J_\pm$ is principal since when $N=5 \mod 8$ the ideal (2) is maximal. An easy calculation shows that $[4,\sqrt{N}+1]^2=2[4,\sqrt{N}-1]$ so that $[4,\sqrt{N}+1]$ is an element of order 1 or 3 in the class group $Cl(\mathcal{A})$.

Lemma 3.1. *When $N=5 \mod 8$ the following are equivalent:*
(a) The equation $x^2-Ny^2=\pm 4$ has a solution with odd integers x,y.
(b) There is a non-integral element of norm ± 4 in $\mathcal{A}_N$.

(c) The ideals $I_\pm$ are principal.

(d) The elements $\frac{\sqrt{N}\pm 1}{4}$ are equivalent to $\sqrt{N}$.

Proof. It is easy to see that (a) and (b) are equivalent using $N = 5 \mod 8$. The conditions (b) and (c) are also easily seen to be equivalent since the ideals $I_\pm$ have norm 4. Conditions (c) and (d) are equivalent using the well-known description of the class group in terms of equivalence classes of elements according to their continued fractions. ■

If the elements $\frac{\sqrt{N}\pm 1}{4}$ are not on the principal cycle then the two continued fractions are the reverse of one another since the elements $[4, \sqrt{N} \pm 1]$ are inverses of one another in the class group of $\mathcal{A}$.

Theorem 3.2. *Suppose $N = 5 \mod 8$ is square-free. Consider the surjective natural homomorphism*

$$\phi : Cl(\mathcal{A}_N) \to Cl(\mathcal{O}_N).$$

(a) The homomomorphism ϕ is an isomorphism if and only if $e = 3$.

(b) The homomorphism ϕ has kernel generated by $[4, \sqrt{N} + 1]$ if and only if $e = 1$.

Proof. It is well-known that ϕ is surjective, that the kernel has order dividing three, and the order of the kernel is three if and only if condition (a) of the Lemma fails ([5]). Using Lemma 3.1 and this remark we see that the kernel of ϕ is the ideal class of $[4, \sqrt{N} + 1]$, and hence this class is an element of of order 3 if and only if $e = 1$. ■

4. Applications

Using a theorem of Erdŏs ([1]) it follows that there are infinitely many square-free integers $a^2 \pm 4$ or $4a^2 + 1$ for odd a .

Theorem 4.1. *For a odd and greater than 3. There are infinitely many square-free $N = 4a^2 + 1$ with $e = 1$.*

Proof. It follows from Proposition 2.6 that $\frac{\sqrt{N}\pm 1}{4}$ have cycle lengths greater 1 and hence are not equivalent to $\sqrt{N}$; thus the ideals $[4, \sqrt{N} \mp 1]$ of $\mathcal{A}_N$ are not principal and therefore there is no element of norm 4 so the fundamental unit ϵ does belong to $\mathcal{A}_N$; hence $e = 1$. ■

Theorem 4.2. *For a odd and greater than 3. There are infinitely many square-free $N = a^2 \pm 4$ with $e = 3$.*

Proof. The numbers $u_\pm = \frac{\sqrt{N}\pm 1}{4}$ are equivalent to $\sqrt{N}$. Consequently the ideal $[4, \sqrt{N} \mp 1]$ of $\mathcal{A}_N$ is principal and therefore the fundamental unit ϵ does not belong to $\mathcal{A}_N$; hence $e = 3$. ■

References

[1] P. Erdős, *Arithmetical propoertes of polynomials*, J. London Math. Soc., 28, 1953, 416-425.

[2] G. H. Hardy and E. M. Wright, **An Introduction to the Theory of Numbers**, Oxford, Fifth Edition, 1979.

[3] N. Ishii, P. Kaplan, K. S. Williams, *On Eisenstein's Problem*, Acta Arithmetica, 54, 1990, 323-345.

[4] W. Sierpinski, **Elementary Theory of Numbers**, Polish Academy of Sciences, Vol. 42, Warsaw, 1964.

[5] P. Stevenhagen, *On a Problem of Eisenstein*, Acta Arithmetica, 74, 3, 1995, 259-26.

MSC: 11R65,11R29

Department of Mathematics, San Jose State University, San Jose, CA 95192, USA

E-mail address: alperin@math.sjsu.edu