85. On Fundamental Units of Real Quadratic Fields with Norm -1

By Shin-ichi KATAYAMA
College of General Education, Tokushima University

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1991)

1. There are many known results on explicit forms of the fundamental units of real quadratic fields of certain types (cf. [1], [2], [3], [5], [7], [8]). In this paper, we shall give a new explicit form of the fundamental units of real quadratic fields with norm -1. Let m be a positive integer which is not a perfect square and K be the real quadratic field $\boldsymbol{Q}(\sqrt{m})$. ε_0 denotes the fundamental unit of K, N the norm map from K to $\boldsymbol{Q}$. We put

$$R_-=\{K: \textit{real quadratic fields with } N\varepsilon_0=-1\},$$
$$E_-=\{\varepsilon: \textit{units of } K\in R_- \textit{ with } N\varepsilon=-1\}.$$

Then it is easy to see $R_-=\{\boldsymbol{Q}(\sqrt{a^2+4}): a\in \boldsymbol{N}\}$, where $\boldsymbol{N}$ is the set of all the natural numbers. Fix now a unit $\varepsilon=(t+u\sqrt{m})/2\in E_-$ $(t, u>0)$ for a while, and we denote $\varepsilon^n=(t_n+u_n\sqrt{m})/2$. $\bar{\varepsilon}$ denotes $(t-u\sqrt{m})/2$. Since $t_n=\varepsilon^n+\bar{\varepsilon}^n$, we have

$$t_{n+1}=\varepsilon^{n+1}+\bar{\varepsilon}^{n+1}=(\varepsilon^n+\bar{\varepsilon}^n)(\varepsilon+\bar{\varepsilon})+\varepsilon^{n-1}+\bar{\varepsilon}^{n-1}=tt_n+t_{n-1}\quad (n\geq 2).$$

Combining this recurrence and the fact $t_1=t$ and $t_2=t^2+2$, we get inductively $t\,|\,t_{2n+1}$ and $t_{2n+1}\geq t_3\geq 4t$ $(n\geq 1)$. Hence we have obtained the following elementary lemma.

Lemma 1. *With the above notation, we have*

(i) $t_{n+1}=tt_n+t_{n-1}$ $(n\geq 2)$ *and* $t_1=t$, $t_2=t^2+2$,

(ii) $t\,|\,t_{2n+1}$ and $t_{2n+1}\geq 4t$ $(n\geq 1)$.

From this lemma follows:

Lemma 2. *If t_{2n+1} is a prime, then $t=1$ and $2n+1$ is prime.*

Proof. If $t\geq 2$, t_{2n+1} can not be a prime by Lemma 1 (ii). Suppose now $2n+1$ decomposes into $2n+1=(2k+1)(2l+1)$, where $2k+1$, $2l+1>1$. Then, from (ii) of Lemma 1, $\varepsilon^{2n+1}=(\varepsilon^{2k+1})^{2l+1}$ implies $t_{2k+1}\,|\,t_{2n+1}$, $t_{2k+1}\geq 4$ and $t_{2n+1}/t_{2k+1}\geq 4$. Therefore t_{2n+1} can not be a prime.

Examine now the case $t=1$, From $N\varepsilon=-1$ and $t=1$ follows $u^2m=5$, so $u=1$, $m=5$. Thus t_n is nothing but *the nth Lucas number* $v_n=\{(1+\sqrt{5})/2\}^n+\{(1-\sqrt{5})/2\}^n$ (cf. [4]). Let $P_1=\{p$: primes such that $p=v_{2n+1}$, $n\geqq 1\}$. If the set P_1 is infinite or not is a famous open problem, but we shall consider the problem how the set P_1 is distributed in the set of all the primes.

For any $N>0$, we put

$$\rho_1(N)=\text{the number of primes } p \text{ such that } p\in P_1 \text{ and } p\leq N.$$

As usual we put

$$\pi(N)=\text{the number of primes } p \text{ such that } p\leq N.$$

For any $N>0$, ν denotes the real number $(\log_\varepsilon N-1)/2$, where $\varepsilon=(1+\sqrt{5})/2$, n denotes the largest integer in ν, that is, the only integer such that $n\leq\nu<n+1$. Then v_{2n+1} satisfies the inequality

$$v_{2n+1}=\varepsilon^{2n+1}+\bar{\varepsilon}^{2n+1}<\varepsilon^{2n+1}\leq\varepsilon^{2\nu+1}=N<\varepsilon^{2(n+1)+1}.$$

Hence, from Lemma 2, we have

$$\rho_1(N)\leq\pi(2n+1)\leq\pi(2\nu+1)=\pi(\log_\varepsilon N).$$

From the prime number theorem, we have

$$\pi(N)\sim\frac{N}{\log N},\qquad \pi(\log_\varepsilon N)\sim\frac{\log_\varepsilon N}{\log\log_\varepsilon N}.$$

Hence we have,

$$0<\lim_{N\to\infty}\frac{\rho_1(N)}{\pi(N)}\leq\lim_{N\to\infty}\frac{\pi(\log_\varepsilon N)}{\pi(N)}\leq\frac{1}{\log\varepsilon}\lim_{N\to\infty}\frac{(\log N)^2}{N\log\log_\varepsilon N}$$
$$\leq\frac{1}{\log\varepsilon}\lim_{N\to\infty}\frac{(\log N)^2}{N}=0.$$

Therefore, we have obtained the follwing proposition.

Proposition 1. *With the above notation,*

$$\lim_{N\to\infty}\frac{\rho_1(N)}{\pi(N)}=0.$$

Hence there are infinitely many primes $p\notin P_1$.

Let p be any prime $p\notin P_1$ and put $(p+\sqrt{p^2+4})/2=\varepsilon_1\in E_-$. Then from Lemma 2 follows that $\varepsilon_1=\varepsilon^{2n+1}$ has no solution with $\varepsilon\in E_-$. Obviously ε_1 can not be any square of $\varepsilon\in E_-$ as $N(\varepsilon^2)=1$. Hence $(p+\sqrt{p^2+4})/2$ is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p^2+4})$.

Theorem 1. *For any prime $p\notin P_1$, $(p+\sqrt{p^2+4})/2$ is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p^2+4})$.*

2. One can easily generalize this theorem as follows. Let k be a given positive integer. For this fixed k, we put

$$P_k=\{p: \text{primes such that } kp=\varepsilon^{2n+1}+\bar{\varepsilon}^{2n+1}\},$$

where n is a natural number and $\varepsilon=(t+\sqrt{t^2+4})/2$ $(t\in N)$. If $p\in P_k$, then $t\mid kp$. Hence $t=hp$ or $t=h$ or $t=k$, where $h\mid k$ $(1\leq h<k)$. We shall investigate the explicit forms of the primes $p\in P_k$.

(i) For the case $t=hp$, it follows $kp=t_{2n+1}\geq t_3=hp(h^2p^2+3)\geq p(p^2+3)$. Hence $k\geq p^2+3$. Therefore there are only finitely many primes $p\in P_k$ in this case.

(ii) For the case $t=h$, a denotes the minimal odd positive integer such that $k\mid t_a$. First we shall show any odd positive b such that $k\mid t_b$ is a multiple of a. Suppose b is an odd positive integer such that $k\mid t_b$ and $a\nmid b$. From the fact $\bar{\varepsilon}=-\varepsilon^{-1}$ follows

$$t_{b-2a}=\varepsilon^{b-2a}+\bar{\varepsilon}^{b-2a}=\varepsilon^b+\bar{\varepsilon}^b-(\varepsilon^a+\bar{\varepsilon}^a)(\varepsilon^{b-a}+\bar{\varepsilon}^{b-a})=t_b-t_at_{b-a}.$$

Hence $k\mid t_{b-2a}$. Therefore there exists an integer $r\geq0$ such that $a<b-2ra<2a$. Then $k\mid t_{2(r+1)a-b}=-t_{b-2(r+1)a}>0$ and $0<2(r+1)a-b<a$, which contradicts the assumption that a is minimal. Therefore any odd positive integer b such as $k\mid t_b$ is a multiple of a.

For each $h|k$, we denote the above minimal a by $a(h)$. Suppose $kp=t_b$, where p is prime. Then we have shown $a(h)|b$. Hence we have $k|t_{a(h)}|t_b=kp$. Since the case $t_{a(h)}=k$ is nothing but the following case (iii), we may assume $t_{a(h)}>k$. Then, from Lemma 1 (ii), t_b/k can not be a prime for any $b>a(h)$. Therefore $kp=t_b$ implies $b=a(h)$. Obviously there exist only finitely many h such that $h|k$, there are only finitely many primes p expressed in the form $p=t_{a(h)}/k$.

(iii) For the case $t=k$, in the same way as the proof of Lemma 2, the condition $t_{2n+1}=kp$ (p is a prime) implies that $2n+1$ is prime.

Combining above (i), (ii), (iii), almost all the primes $p\in P_k$ are expressed in the forms $p=(\varepsilon^{2n+1}+\bar{\varepsilon}^{2n+1})/k$, where $\varepsilon=(k+\sqrt{k^2+4})/2$ and $2n+1$ is prime. We put

$\rho_k(N)=$the number of primes such that $p\in P_k$ and $p\leq N$.

Then in the same way as the proof of the proposition, we have

$$\lim_{N\to\infty}\frac{\rho_k(N)}{\pi(N)}=0.$$

Theorem 2. *There are infinitely many primes $p\notin P_k$. For such prime p, $(kp+\sqrt{k^2p^2+4})/2$ is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{k^2p^2+4})$.*

Remark 1. If we put the set $R_0=\{\boldsymbol{Q}(\sqrt{5})\}$ and $R_k=\{\boldsymbol{Q}\sqrt{k^2p^2+4}):$ primes $p\notin P_k\}$. Then we have

$$R_-=\bigcup_{k=0}^{\infty}R_k.$$

Remark 2. If $k=2$, then $P_2=\{2\}\cup\{$*the NSW-primes* $S_{2n+1}\}$. Here *the NSW-primes* are the primes of the form

$$S_{2n+1}=\frac{(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}}{2}\quad(n\geq 1)$$

(see [4] Chapter 5).

References

[1] G. Degert: Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **22**, 92–97 (1958).

[2] M. Kutsuna: On the fundamental units of real quadratic fields. Proc. Japan Acad., **50**, 580–583 (1974).

[3] T. Nakahara: On the determination of the fundamental units of certain real quadratic fields. Mem. Fac. Sci., Kyushu Univ., **24**, 300–304 (1970).

[4] P. Ribemboim: The Book of Prime Number Records. Springer-Verlag, New York (1988).

[5] C. Richard: Sur la résolution des équations $x^2-Ay^2=+1$. Atti Accad. Pontif Nuovi Lincei, pp. 177–182 (1866).

[6] H. E. Rose: A Course in Number Theory. Clarenden Press, Oxford (1988).

[7] H. Yokoi: On real quadratic fields containing units with norm −1. Nagoya Math. J., **33**, 139–152 (1968).

[8] ——: The fundamental unit and class number one problem of real quadratic fields with prime discriminant. ibid., **120**, 51–59 (1990).