33. Prime Producing Quadratic Polynomials and Class-number One Problem for Real Quadratic Fields

By Masaki KOBAYASHI
Department of Mathematics, School of Science, Nagoya University

(Communicated by Shokichi IYANAGA, M. J. A., May 14, 1990)

Let $F=Q(\sqrt{m})$ ($m>0$: square-free integer) be a real quadratic field. Denote by $h=h(m)$ and $d=d(m)$ the class number in the wide sense and the discriminant of F, respectively. Recently the following theorem was obtained by Yokoi [4] and Louboutin [1]:

Theorem 1 (Yokoi-Louboutin). *Let p be an odd prime.*

In case $m=4p^2+1$, $h(m)=1$ if and only if $-n^2+n+p^2$ is prime for any integer n such that $1\leq n<p$.

In case $m=p^2+4$, $h(m)=1$ if and only if $-n^2+n+(p^2+3)/4$ is prime for any integer n such that $1\leq n\leq(p-1)/2$.

In case $m=p(p+4)$, $h(m)=1$ if and only if $-n^2+n+(p^2-1)/4$ is prime for any integer n such that $1\leq n\leq(p+1)/2$.

The purpose of this paper is to improve this theorem, especially concerning the sufficient condition for $h(m)=1$, by using "reduced quadratic irrational", and to prove the following:

Theorem 2. *In case $m=4p^2+1$, $h(m)=1$ if and only if $-n^2+n+p^2$ is prime for any integer n such that $\sqrt{p+1}\leq n\leq p-1$.*

In case $m=p^2+4$, $h(m)=1$ if and only if $-n^2+n+(p^2+3)/4$ is prime for any integer n such that $\sqrt{(p+5)/2}\leq n\leq(p-1)/2$.

In case $m=p(p+4)$, $h(m)=1$ if and only if $-n^2+n+p+(p^2-1)/4$ is prime for any integer n such that $\sqrt{(p+1)/2}\leq n\leq(p-1)/2$.

To prove Theorem 2, we need some preliminaries.

For two quadratic irrational numbers α, β, we say that they are *equivalent* to each other and denote $\alpha\sim\beta$ if and only if the periodic part in the expansion of α into a continued fraction is equal to that of β. Moreover, we say that α is *reduced* if and only if $\alpha>1>-\alpha'>0$, where α' is conjugate of α over Q. Then it is well-known that α is reduced if and only if the expansion of α into a continued fraction is purely periodic (cf. Perron [2]).

Put $R(m)=\{\alpha\in Q(\sqrt{m}): \alpha=(b+\sqrt{d})/2a\ (a, b\in N), \alpha \text{ is reduced}\}$. Then it is easily verified that $(d_0+\sqrt{d})/2$ belong to $R(m)$, if we choose $d_0\in N$ satisfying $d_0<\sqrt{d}<d_0+2$ and $d_0\equiv d \bmod 2$.

Now we can obtain the following three lemmas:

Lemma 1. *Set $(d_0+\sqrt{d})/2=[\overline{a_1, a_2, \cdots, a_n}]$, then $h(m)=1$ if and only if $R(m)=\{[\overline{a_i, a_{i+1}, \cdots, a_n, a_1, \cdots, a_{i-1}}]: 1\leq i\leq n\}$.*

Proof. This lemma follows easily from $h(m)=\#(R(m)/\sim)$ (cf. Yamamoto [3]).

Lemma 2. *A quadratic irrational* $(b+\sqrt{d})/2a$ *belongs to* $R(m)$ *if and only if* $4a|(d-b^2)$, $(b+\sqrt{d})/2>a>(-b+\sqrt{d})/2$, $b<\sqrt{d}$.

Proof. We put $\alpha=(b+\sqrt{d})/2a$ $(a, b \in N)$. Then $\alpha>1>-\alpha'>0$ is equivalent to $(b+\sqrt{d})/2>a>(-b+\sqrt{d})/2$, $b<\sqrt{d}$. On the other hand, if α is reduced, then a, b satisfy $4a|(d-b^2)$. Hence Lemma 2 follows from the definition of $R(m)$.

Now if $m=4t^2+1$ or t^2+4, $h(m)=1$ implies that m is prime and t is prime or one (cf. [4] Theorem 1), and in case $m=t(t+4)$, $h(m)=1$ implies that both t and $t+4$ are prime and $t\equiv 3 \bmod 4$ from genus theory. Therefore we have only to consider the cases $m=4p^2+1$, p^2+4 or $p(p+4)$ with an odd prime p.

Lemma 3. *In case* $m=4p^2+1$, $h(m)=1$ *if and only if* $R(m)=\{(2p-1+\sqrt{m})/2, (2p-1+\sqrt{m})/2p, (1+\sqrt{m})/2p\}$.

In case $m=p^2+4$, $h(m)=1$ *if and only if* $R(m)=\{(p+\sqrt{m})/2\}$.

In case $m=p(p+4)$, $h(m)=1$ *if and only if* $R(m)=\{(p+\sqrt{m})/2, (p+\sqrt{m})/2p\}$.

Proof. In case $m=4p^2+1$, we have $(d_0+\sqrt{d})/2=(2p-1+\sqrt{m})/2=[\overline{2p-1, 1, 1}]$, $(2p-1+\sqrt{m})/2p=[\overline{1, 1, 2p-1}]$, $(1+\sqrt{m})/2p=[\overline{1, 2p-1, 1}]$. In case $m=p^2+4$, we have $(d_0+\sqrt{d})/2=(p+\sqrt{m})/2=[\overline{p}]$ and in case $m=p(p+4)$, we have $(d_0+\sqrt{d})/2=(p+\sqrt{m})/2=[\overline{p, 1}]$, $(p+\sqrt{m})/2p=[\overline{1, p}]$. Hence the lemma follows from Lemma 1.

Now we can prove our main theorem.

Proof of Theorem 2. The necessity is clear from Theorem 1.

In case $m=4p^2+1$, assume that $-n^2+n+p^2$ is prime for any integer n satisfying $\sqrt{p+1}\leq n\leq p-1$. By Lemma 3, it is enough to show that if $(b+\sqrt{d})/2a \in R(m)$, then $(a, b)=(1, 2p-1)$, $(p, 2p-1)$ or $(p, 1)$.

If $(b+\overline{m})/2a$ belongs to $R(m)$, then $4|m-b^2$ holds, and hence b is odd because m is odd. Put $b=2n-1$; then we have $1\leq n\leq p$ and $m-b^2=4p^2+1-(2n-1)^2=4(-n^2+n+p^2)$, since $1\leq b<\sqrt{m}$. Now by Lemma 2, $(b+\sqrt{d})/2a$ belongs to $R(m)$ if and only if

$$a|(-n^2+n+p^2), \quad -n+p+1\leq a\leq n+p-1, \quad 1\leq n\leq p. \qquad (*)$$

Therefore it is enough to verify that (a, n)'s satisfying $(*)$ are exactly $(1, p)$, (p, p) and $(p, 1)$. In case $n=p$, $-n^2+n+p^2$ is equal to p. Hence if $n=p$, (a, n)'s satisfying $(*)$ are exactly $(1, p)$ and (p, p). For $n\leq p-1$, we have $-n^2+n+p^2>n+p-1$ and $-n+p+1>1$. In case $\sqrt{p+1}\leq n\leq p-1$, there does not exist any (a, n)'s satisfying $(*)$ by our assumption.

In case $n<\sqrt{p+1}$, put $a=p+x$. Then $-n+p+1\leq a\leq n+p-1$ implies $-n+1\leq x\leq n-1$. Since $-n^2+n+p^2=(p+x)(p-x)-n^2+n+x^2\equiv -n^2+n+x^2 \bmod (p+x)$, (a, n) satisfies $(*)$ if and only if $-n^2+n+x^2\equiv 0 \bmod (p+x)$. On the other hand, $p+x\geq p-n+1$ holds, and moreover $-n+1\geq -n^2+n+x^2\geq -n^2+n$, which implies $|-n^2+n+x^2|\leq n^2-n$. We see that $n<\sqrt{p+1}$ yields $n^2-n<p-n+1$, and hence $|-n^2+n+x^2|<p+x$. Therefore $-n^2+n$

$+x^2 \equiv 0 \bmod (p+x)$ implies $-n^2+n+x^2=0$. Finally, if $n \geq 2$, then $-n^2+n+x^2 < 0$, and if $n=1$, then $x=0$. Hence if $n<\sqrt{p+1}$, then (a, n) satisfying $(*)$ is just $(p, 1)$ only. Thus it follows that (a, n)'s satisfying $(*)$ are exactly $(1, p)$, (p, p) and $(p, 1)$.

We can also prove the second case and the third case in the same way.

References

[1] S. Louboutin: Prime producing quadratic polynomials and class-number of real quadratic fields. I (preprint).

[2] O. Perron: Die Lehre von den Kettenbrüchen. Teubner, Leipzig (1913).

[3] Y. Yamamoto: Real quadratic number fields with large fundamental units. Osaka J. Math., **8**, 261–270 (1971).

[4] H. Yokoi: Class-number one problem for certain kind of real quadratic fields. Proc. Int. Conf. on Class Number and Fundamental Units, Katata, Japan (1986).