Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 493–501

Some Relations Among New Invariants of Prime Number p Congruent to 1 mod 4

Hideo Yokoi

In this paper, we shall define some invariants (i.e. number theoretic function) of prime p congruent to 1 mod 4, and consider the problem to express the prime p by using those new invariants of p.

Namely, almost all such primes p are uniquely expressed as a polynomial of degree 2 of the first invariant n, which takes any value of natural numbers. Then, the coefficient of the term of degree 2 is the square of the second invariant u, which takes any value of natural numbers of the form $2^\delta \prod p_i^{e_i}$ ($\delta=0$ or 1, and prime $p_i \equiv 1 \bmod 4$). The coefficients $2a$ and b of terms of degree 1 and 0 respectively are invariants depending on u and satisfying the relations $a^2+4=bu^2$ and $0 \leqq a < (1/2)u^2$.

Moreover, with terms of these invariants, a necessary condition of solvability of the diophantine equation $x^2-py^2=\pm 4m$ for any natural number m, an explicit formula of the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$, and an estimate formula from below of the class-number of $\boldsymbol{Q}(\sqrt{p})$ are given.

Throughout this paper, the following notation is used:

$\boldsymbol{N}$: the set of all natural numbers

$\boldsymbol{Z}$: the ring of all rational integers

$\boldsymbol{Q}$: the rational number field

N: the absolute norm mapping

$(-)$: Legendre-Jacobi-Kronecker symbol.

Theorem. *Almost all rational prime p congruent to* 1 mod 4 *are uniquely expressed in the form*

$$p=u^2n^2 \pm 2an+b,$$

where

$$n \in \boldsymbol{N}^+ = \{0\} \cup \boldsymbol{N},$$

Received December 24, 1986

$$u \in U=\left\{2^{\delta} \prod_{i=1}^{r} p_i^{e_i};\ \delta=0 \text{ or } 1,\ e_i \geqq 1,\ \text{prime } p_i \equiv 1 \pmod 4\right\},$$

$$a \in A_u=\left\{\pm a_{\lambda};\ 0 \leqq a_{\lambda} < \frac{1}{2}u^2,\ \lambda=1, 2, \cdots, 2^{\delta+r-1}\right\},$$

which is a system of representatives of the residue classes of the solutions of $x^2 \equiv -4 \pmod{u^2}$ (*put* $a=0$ *in the case* $r=0$), *and*

$$b=\frac{a^2+4}{u^2} \quad (\text{i.e. } a^2+4=bu^2).$$

Moreover, then

(i) $$\varepsilon_p=\frac{1}{2}(u^2n \pm a+u\sqrt{p})>1$$

is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$.

(ii) *For a natural number* $m>1$, *if the diophantine equation* $x^2-py^2=\pm 4m$ *has at least one non-trivial integral solution, then* $m \geqq n$ *holds.*

(iii) *For the class-number* $h=h(p)$ *of* $\boldsymbol{Q}(\sqrt{p})$ *and the least prime* $q_0=q_0(p)$ *such that* $\left(\frac{p}{q_0}\right)=1$, *i.e.* q_0 *splits completely in* $\boldsymbol{Q}(\sqrt{p})$, *it holds*

$$h \geqq \frac{\log n}{\log q_0}.$$

To prove this theorem, we need two lemmas.

In a square-free integer $D>1$ and a natural number $m>1$, we say that an integral solution (u, v) of the diophantine equation $x^2-Dy^2=\pm 4m$ is *trivial* if and only if $m=n^2$ is a square and $u \equiv v \equiv 0 \pmod n$.

Lemma 1 (Davenport-Ankeny-Hasse-Ichimura). *Let* $D>1$ *be a square-free rational integer, and denote the fundamental unit of the real quadratic field* $\boldsymbol{Q}(\sqrt{D})$ *by*

$$\varepsilon_D=\frac{1}{2}(t+u\sqrt{D})>1.$$

Then, for any natural number $m>1$, *if the diophantine equation* $x^2-Dy^2=\pm 4m$ *has at least one non-trivial integral solution, it holds*

$$m \geqq \begin{cases} \dfrac{t}{u^2} & \cdots N\varepsilon_D=-1, \\[2mm] \dfrac{t-2}{u^2} & \cdots N\varepsilon_D=1. \end{cases}$$

Proof. For proofs in the case of no square m, see N. C. Ankeny, S. Chowla and H. Hasse [1] or H. Hasse [2]. For arbitrary natural number m, this lemma was first proved by H. Ichimura as follows in a letter to the author:

We prove this lemma in the case $N\varepsilon_D=-1$ only, because in another case it can be proved similarly. If there exists at least one non-trivial solution (x', y') of $x^2-Dy^2=\pm 4m$, then we know $y'\neq 0$ at once. Hence, let (x_0, y_0) be the non-trivial solution such that $x_0\geqq 0$ and $y_0>0$ is the smallest, then

$$N(x_0-y_0\sqrt{D})=\pm 4m$$

holds, and multiplying this by

$$N\left(\frac{t+u\sqrt{D}}{2}\right)=-1,$$

we obtain

$$N\left(\frac{x_0t-y_0uD}{2}+\frac{x_0u-y_0t}{2}\sqrt{D}\right)=\pm 4m,$$

and we see easily that both of

$$a=\frac{x_0t-y_0uD}{2} \quad \text{and} \quad b=\frac{x_0u-y_0t}{2}$$

are rational integers.

Here, we can verify that (a, b) is also a non-trivial integral solution of $x^2-Dy^2=\pm 4m$. For, if not, then there exists a positive integer n such that $m=n^2$, $a\equiv b\equiv 0 \pmod{n}$. Writing ε_D^{-1} as

$$\varepsilon_D^{-1}=\frac{1}{2}(t'+u'\sqrt{D}), \qquad (t', u' \in \boldsymbol{Z}),$$

and noting

$$\varepsilon_D(x_0-y_0\sqrt{D})=a+b\sqrt{D},$$

we obtain

$$x_0-y_0\sqrt{D}=\frac{t'a+u'bD}{2}+\frac{t'b+u'a}{2}\sqrt{D}.$$

Since ε_D^{-1} is an integer of $\boldsymbol{Q}(\sqrt{D})$ and D is square-free, we know $t'\equiv u' \pmod{2}$, and hence we obtain

$$x_0 = \frac{t'a+u'bD}{2} \equiv 0 \qquad (\text{mod } n),$$

$$-y_0 = \frac{t'b+u'a}{2} \equiv 0 \qquad (\text{mod } n).$$

This contradicts the assumption that (x_0, y_0) is non-trivial. Therefore, (a, b) and so $(|a|, |b|)$ is also a non-trivial solution of $x^2-Dy^2=\pm 4m$.

Finally, because of the minimum choice of y_0, we get

$$|b| = \left|\frac{x_0u-y_0t}{2}\right| \geqq y_0,$$

i.e.

$$x_0 \geqq \frac{t+2}{u} y_0 > 0 \quad \text{or} \quad 0 \leqq x_0 \leqq \frac{t-2}{u} y_0.$$

Hence, from $x_0^2-Dy_0^2=\pm 4m$, we obtain either

$$\underset{(-)}{+} 4m \geqq \left\{\left(\frac{t+2}{u}\right)^2 - D\right\} y_0^2 \geqq \frac{4t}{u}$$

or

$$\underset{(+)}{-} 4m \leqq \left\{\left(\frac{t-2}{u}\right)^2 - D\right\} y_0^2 \leqq -\frac{4t}{u^2}.$$

Therefore, in each case, we obtain $m \geqq t/u^2$ as asserted in the lemma.

Lemma 2. *Let $D>1$ be a square-free positive integer, and q be an odd prime. Then, the following two assertions are equivalent to each other*:

(i) *The number e is the smallest natural number such that the diophantine equation $x^2-Dy^2=\pm 4q^e$ has at least one integral solution.*

(ii) $\left(\dfrac{D}{q}\right)=1$ *and the natural number e is the order of prime factors $\mathfrak{q}_1 \neq \mathfrak{q}_2$ of q in $\boldsymbol{Q}(\sqrt{D})$ in the ideal class group.*

Proof. Let e_1 be the smallest natural number such that $x^2-Dy^2=\pm 4q^{e_1}$ is solvable, then $\left(\dfrac{D}{q}\right)=1$. On the other hand, for an odd prime q satisfying $\left(\dfrac{D}{q}\right)=1$, let e_2 be the order of prime factors $\mathfrak{q}_i$ $(i=1, 2)$ of q in $\boldsymbol{Q}(\sqrt{D})$ in the ideal class group. Moreover, put $\mathfrak{q}_1^{e_2}=(\omega)$, $\omega=\frac{1}{2}(u+v\sqrt{D})$, then we get

$$q^{e_2}=(N\mathfrak{q}_1)^{e_2}=|N(\omega)|=\left|\frac{1}{4}(u^2-Dv^2)\right|,$$

and so we have $u^2-Dv^2=\pm 4q^{e_2}$, which implies $e_2\geqq e_1$.

Conversely, for some (u, v), it holds $u^2-Dv^2=\pm 4q^{e_1}$, and so $u^2\equiv Dv^2$ (mod q), which implies $\left(\frac{D}{q}\right)=1$. Hence, putting $\frac{1}{2}(u+v\sqrt{D})=\omega$, $(\omega)=\mathfrak{A}$, and $q=\mathfrak{q}_1\cdot\mathfrak{q}_2$, we get

$$N\mathfrak{A}=|N(\omega)|=q^{e_1}=(\mathfrak{q}_1\mathfrak{q}_2)^{e_1}.$$

Then, we know $\mathfrak{A}=\mathfrak{q}_1^{e_1}$ or $\mathfrak{q}_2^{e_1}$, which implies $e_1\geqq e_2$.

For, putting $\mathfrak{A}=\mathfrak{q}_1^r\mathfrak{q}_2^{e_1-r}$ $(0\leqq r\leqq e_1)$, we get $\mathfrak{A}=q^{e_1-r}\mathfrak{q}_1^{2r-e_1}$ (resp. $q^r\mathfrak{q}_2^{e_1-2r}$) in the case $r\geqq e_1-r$ (resp. $r<e_1-r$). Hence, $\mathfrak{q}_1^{2r-e_1}$ (resp. $\mathfrak{q}_2^{e_1-2r}$) $=(\eta)$ is a principal ideal, and so putting $\eta=\frac{1}{2}(u_1+v_1\sqrt{D})$, we get

$$\pm q^{2r-e_1}(\text{resp. } \pm q^{e_1-2r})=N(\eta)=\frac{1}{4}(u_1^2-Dv_1^2),$$

which implies $u_1^2-Dv_1^2=\pm 4q^{2r-e_1}$ (resp. $\pm 4q^{e_1-2r}$). Hence, it follows from $2r-e_1\geqq e_1$ (resp. $e_1-2r\geqq e_1$) that $r=e_1$ (resp. $r=0$), i.e. $\mathfrak{A}=\mathfrak{q}_1^{e_1}$ (resp. $\mathfrak{q}_2^{e_1}$).

Proof of theorem. For any prime p congruent to 1 mod 4, let

$$\varepsilon_p=\frac{1}{2}(t_p+u_p\sqrt{p}), \qquad (t_p>0,\ u_p>0),$$

be the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$. Then, we get first

$$u_p=2^{\delta}\prod_{i=1}^{r}p_i^{e_i}, \qquad (\delta=0 \text{ or } 1, \text{ prime } p_i\equiv 1 \bmod 4),^{*)}$$

and

$$N\varepsilon_p=-1, \quad \text{i.e. } t_p^2-pu_p^2=-4.$$

Hence, $u=u_p$ is an invariant of p and belongs to $\boldsymbol{U}$.

Next, there is uniquely determined a number n_p of $\boldsymbol{N}^+$ by the inequality

$$\left|\frac{t_p}{n_p^2}-n_p\right|<\frac{1}{2}.$$

*) C.f. Yokoi [5], Lemma 1.

For, if $u_p=2$, then $p=\frac{1}{4}t_p^2+1\equiv 1 \pmod 4$ implies $t_p\equiv 0 \pmod 4$, and so $t_p/u_p^2=t_p/4 \in \boldsymbol{N}$. Hence, $n=n_p$ is also an invariant of p belonging to $\boldsymbol{N}^+$.

Moreover, if we put

$$t_p=nu^2\pm a, \quad (a\geqq 0),$$

then we get

$$0\leqq \frac{a}{u^2}=\left|\frac{t_p}{u^2}-n\right|<\frac{1}{2},$$

and hence $0\leqq a<\frac{1}{2}u^2$.

Here, $a=0$ if and only if $r=0$. For, if $a=0$, i.e. $t_p\equiv 0 \pmod{u_p^2}$, then it follows from $(t_p, u_p)=1$ or 2 that $u_p=1$ or 2. Conversely, if $r=0$, i.e. $u_p=1$ or 2, then it follows easily from $t_p^2-pu_p^2=-4$ that $t_p\equiv 0$ (mod u_p^2), i.e. $a=0$.

Furthermore, from

$$\begin{aligned} pu_p^2&=t_p^2+4=(nu_p^2\pm a)^2+4\\ &=n^2u_p^4\pm 2anu_p^2+a^2+4, \end{aligned}$$

we get $a^2+4\equiv 0 \pmod{u_p^2}$.

Hence, a is an invariant of p belonging to $\boldsymbol{A}$, and b defined by $a^2+4=bu^2$ is also an invariant of p, and consequently the prime p is expressed by those invariants of p in the form

$$p=u^2n^2\pm 2an+b.$$

Conversely, if a prime p congruent to 1 mod 4 is expressed in this form, then it is known by Yokoi-Nakahara**) that for almost all (i.e. except for finite number of) such primes p,

$$\varepsilon_p=\frac{1}{2}(u^2n\pm a+u\sqrt{p})$$

is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$. Hence, $u_p=u$ and $t_p=u^2n\pm a$, and moreover

$$\left|\frac{t_p}{u_p^2}-n\right|=\frac{a}{u_p^2}<\frac{1}{2}.$$

Therefore, u, n, a and b in $p=u^2n^2\pm 2an+b$ are uniquely determined by prime p.

**) C.f. Yokoi [5], Nakahara [3].

Furthermore, for a natural number m, if the diophantine equation $x^2 - py^2 = \pm 4m$ has at least one non-trivial integral solution, then by Lemma 1 we get $m \geqq t_p/u_p^2 = n \pm a/u_p^2$, and noting $0 \leqq a/u_p^2 < \frac{1}{2}$, we obtain $m \geqq n$.

Finally, for any rational prime q splitting completely in $Q(\sqrt{p})$, i.e. $\left(\frac{p}{q}\right) = 1$, by Lemma 2 we obtain

$$q^h \geqq n, \qquad \text{i.e. } h \geqq \frac{\log n}{\log q}.$$

Hence, in particular, for the least prime $q_0 = q_0(p)$ satisfying $\left(\frac{p}{q_0}\right) = 1$, $h \geqq \frac{\log n}{\log q_0}$ holds.

Example.

(1) The case of $u = 1$.

$$(a, b) = (0, 4). \quad \text{Hence } p = n^2 + 4.$$

For example,

$$(p, n; h) = (5, 1; 1), (13, 3; 1), (29, 5; 1), (53, 7; 1), (173, 13; 1), (293, 17; 1), (1373, 37; 3),$$

$$\varepsilon = \frac{1}{2}(n + \sqrt{p}).$$

(2) The case of $u = 2$.

$$(a, b) = (0, 1). \quad \text{Hence } p = 2^2 n^2 + 1.$$

For example,

$$(p, n; h) = (5, 1; 1), (17, 2; 1), (37, 3; 1), (101, 5; 1), (197, 7; 1), (677, 13; 1), (5477, 37; 3), \cdots$$

$$\varepsilon = 2n + \sqrt{p}.$$

(3) The case of $u = 5$.

$$(a, b) = (11, 5). \quad \text{Hence } p = 5^2 n^2 \pm 2 \cdot 11 n + 5.$$

For example,

$$(p, n; h)=(61, 2; 1), (317, 4; 1), (773, 6; 1),$$
$$(1429, 8; 5)\cdots p=5^2n^2-2\cdot 11n+5,$$
$$(p, n; h)=(149, 2; 1)\cdots p=5^2n^2+2\cdot 11n+5.$$

(4) The case of $u=10$.

$(a, b)=(36, 13)$. Hence $p=10^2n^2\pm 2\cdot 36n+13$.

For example,

$$(p, n; h)=(41, 1; 1), (269, 2; 1), (2153, 5; 5),$$
$$(3181, 6; 5), (4409, 7; 9)\cdots p=10^2n^2-2\cdot 36n+13.$$
$$(p, n; h)=(557, 2; 1), (1129, 3; 9), (1901, 4; 3),$$
$$(5417, 7; 7)\cdots p=10^2n^2+2\cdot 36n+13.$$

(5) The case of $p=1{,}009$.

$\varepsilon_p=540+17\sqrt{p}$. $h(p)=7$.
Hence $t_p=1{,}080$, $u_p=34$, $n=1$.
$(a, b)=(76, 5)$.

Therefore, $p=1{,}009=34^2\cdot 1^2-2\cdot 76\cdot 1+5$.

(6) The case of $p=2{,}677$.

$\varepsilon_p=\frac{1}{2}(3{,}777+73\sqrt{p})$. $h(p)=3$.
Hence $t_p=3{,}777$, $u_p=73$, $n=1$.
$(a, b)=(1552, 452)$.

Therefore, $p=2{,}677=73^2\cdot 1^2-2\cdot 1552\cdot 1+452$.

(7) The case of $p=5{,}273$.

$\varepsilon_p=944+13\sqrt{p}$. $h(p)=7$.
Hence $t_p=1{,}888$, $u_p=26$, $n=3$.
$(a, b)=(140, 29)$.

Therefore, $p=5{,}273=26^2\cdot 3^2-2\cdot 140\cdot 3+29$.

References

[1] N. C. Ankeny, S. Chowla and H. Hasse, On the class-number of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., **217** (1965), 217–220.

[2] H. Hasse, Über mehrklassige, aber eingeschlechitige reellquadratische Zahlkörper, Elemente der Mathematik, **20** (1965), 49–72.

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

[4] ——, On the fundamental units and an estimate of the class numbers of real quadratic fields, Reports Fac. Sci. & Eng., Saga Univ., **2** (1974), 1–13.

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

Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464
Japan