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 $0 \leq a < (1/2)u^2$.

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 $Q(\sqrt{p})$, and an estimate formula from below of the class-number of $Q(\sqrt{p})$ are given.

Throughout this paper, the following notation is used:

$N$: the set of all natural numbers

$Z$: the ring of all rational integers

$Q$: 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*

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

Received December 24, 1986