Can. J. Math., Vol. XXXIII, No. 1, 1981, pp. 55–58

ON THE CLASS-NUMBER OF THE MAXIMAL REAL SUBFIELD OF A CYCLOTOMIC FIELD

HIROSHI TAKEUCHI

Let p be an integer and let $H(p)$ be the class-number of the field

$$K = \mathbf{Q}\,(\zeta_p + \zeta_p^{-1})$$

where ζ_p is a primitive p-th root of unity and $\mathbf{Q}$ is the field of rational numbers. It has been proved in [**1**] that if $p = (2qn)^2 + 1$ is a prime, where q is a prime and $n > 1$ an integer, then $H(p) > 1$. Later, S. D. Lang [**2**] proved the same result for the prime number $p = ((2n + 1)q)^2 + 4$, where q is an odd prime and $n \geqq 1$ an integer. Both results have been obtained in the case $p \equiv 1 \pmod 4$.

In this paper we shall prove the similar results for a certain prime number $p \equiv 3 \pmod 4$.

We designate by $h(p)$ the class-number of the real quadratic field

$$k = \mathbf{Q}\,(\sqrt{p}).$$

We prove the following theorem.

THEOREM 1. *If* $12m + 7$ *and* $p = (3(8m + 5))^2 - 2$ *are primes, where* $m \geqq 0$ *is an integer, then* $h(p) > 1$.

To prove this theorem we need the next lemma.

LEMMA. *The conditions on* p *and* m *being the same as in Theorem* 1, *the equation*

$$u^2 - pv^2 = \pm 3$$

has no solution in integers u, v.

Proof. To prove this lemma, it is convenient to divide the discussion into three cases as follows,

Case I. $u^2 - pv^2 = 3$,
Case II. $u^2 - pv^2 = -3$ and $v^2 = 1$,
Case III. $u^2 - pv^2 = -3$ and $v^2 > 1$.

First in Case I, if there exists a pair of integers u, v, we obtain

$$u^2 \equiv 3 \pmod p.$$

Received April 24, 1979.

Since $p \equiv 3 \pmod 4$ we have by the Legendre symbol

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2\cdot(3-1)/2} = -1$$

and from $p \equiv -2 \pmod 3$

$$\left(\frac{p}{3}\right) = \left(\frac{-2}{3}\right) = 1.$$

So we obtain

$$\left(\frac{3}{p}\right) = -1.$$

This is a contradiction.

Next in Case II, if the equation holds for an integer u, then we have

$$u^2 = p - 3.$$

Hence

$$\begin{aligned} u'^2 &= 144m^2 + 180m + 55 \\ &= (12m + 7)^2 + (12m + 7) - 1, \end{aligned}$$

for an integer m, where $2u' = u$.

So

$$u'^2 \equiv -1 \pmod{12m + 7}.$$

Since

$$\left(\frac{-1}{12m + 7}\right) = (-1)^{6m+3} = -1,$$

this is impossible.

In Case III, there is no loss of generality in assuming that $u > 0$ and $v > 1$. Among all representation of -3 by the form

$$u^2 - (l^2 - 2)v^2, \text{ where } u > 0,\ v > 1 \text{ and } l = 3(8m + 5),$$

choose u_0, v_0 with the smallest value v_0. Thus

$$-3 = u_0^2 - (l^2 - 2)v_0^2.$$

Writing this equation as norm representation

$$-3 = N(u_0 - v_0\sqrt{l^2 - 2})$$

and multiplying by

$$1 = N((l^2 - 1) + l\sqrt{l^2 - 2}),$$

we obtain

$$-3 = N(u_0(l^2 - 1) - l(l^2 - 2)v_0 - ((l^2 - 1)v_0 - lu_0)\sqrt{l^2 - 2}).$$

https://doi.org/10.4153/CJM-1981-006-8 Published online by Cambridge University Press

By the definition of v_0, we have

$$|(l^2 - 1)v_0 - lu_0| \geqq v_0.$$

Hence either $lv_0 \leqq u_0$ or $(l^2 - 2)v_0 \geqq lu_0$. So either

$$-3 = u_0^2 - (l^2 - 2)v_0^2 \geqq l^2v_0^2 - (l^2 - 2)v_0^2 = 2v_0^2$$

or

$$-3l^2 = l^2u_0^2 - l^2(l^2 - 2)v_0^2 \leqq (l^2 - 2)^2v_0^2 - l^2(l^2 - 2)v_0^2 = -2(l^2 - 2)v_0^2.$$

Both inequalities contradict $v_0 > 1$ and $l > 2$.

This completes the proof of the lemma.

Proof of Theorem 1. A prime p satisfies $p \equiv -2 \pmod 3$. Hence

$$\left(\frac{p}{3}\right) = \left(\frac{-2}{3}\right) = 1.$$

Therefore, by the law of decomposition in quadratic fields, 3 splits in k into a prime divisor $\mathfrak{Q}$ of degree one and its conjugate, and hence is its absolute norm

$$3 = N(\mathfrak{Q}).$$

Suppose $h(p) = 1$. Then $\mathfrak{Q}$ is a principal divisor, i.e.,

$$\mathfrak{Q} \cong (\omega) = (u + v\sqrt{p})$$

with rational integers u, v ($\cong$ denotes the divisor equality). Hence

$$N(\mathfrak{Q}) = |N(\omega)| = |u^2 - pv^2|.$$

Thus

$$u^2 - pv^2 = \pm 3.$$

This contradicts the lemma. Hence $h(p) > 1$.

Similarly we obtain the following:

THEOREM 2. *If* $12m + 11$ *and* $p = (3(8m + 7))^2 - 2$ *are primes, where* $m \geqq 0$ *is an integer, then* $h(p) > 1$.

Proof. It is sufficient to prove that $u^2 \neq p - 3$ for all integers u.

Now if $u^2 = p - 3$ for some integer u, then we obtain the equation

$$u'^2 = (12m + 11)^2 - (12m + 11) - 1,$$

where $u = 2u'$. So we have

$$u'^2 \equiv -1 \pmod{12m + 11}.$$

This contradicts the fact that

$$\left(\frac{-1}{12m + 11}\right) = -1.$$

https://doi.org/10.4153/CJM-1981-006-8 Published online by Cambridge University Press

I. Yamaguchi [3] has proved the following:

THEOREM A. *If $\varphi(p) > 4$, then $h(p)|H(4p)$, where $\varphi(p)$ stands for the Euler function and $p > 0$ is an integer.*

By this theorem, we have the following theorems.

THEOREM 3. *If $12m + 7$ and $p = (3(8m + 5))^2 - 2$ are primes, where $m \geqq 0$ is an integer, then $H(4p) > 1$.*

Proof. Since p is a prime number, the value of the Euler function is $\varphi(p) = p - 1$. And $p - 1 = 576m^2 + 720m + 222$. Hence $\varphi(p) > 4$. This proves the assertion of theorem.

THEOREM 4. *If $12m + 11$ and $p = (3(8m + 7))^2 - 2$ are primes, where $m \geqq 0$ is an integer, then $H(4p) > 1$.*

Proof. Since $p - 1 = 576m^2 + 1008m + 438$, it follows that $\varphi(p) > 4$. This completes the proof.

Examples.

Type of Theorem 1	Type of Theorem 2
$m = 0; p = 223, \ h(p) = 3$ $m = 2; p = 3967, h(p) = 5$	$m = 0; p = 439, h(p) = 5$

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. S. D. Lang, *Note on the class-number of the maximal real subfield of a cyclotomic field*, J. reine angew. Math. *290* (1977), 70–72.
3. I. Yamaguchi, *On the class-number of the maximal real subfield of a cyclotomic field*, J. reine angew. Math. *272* (1975), 217–220.
4. I. Yamaguchi and K. Oozeki, *On the class-number of the real quadratic field*, T R U (Tokyo Rika University) Mathematics *8* (1972), 13–14.

Tokyo Metropolitan Agricultural Senior High School,
Tokyo, Japan