A note on quadratic fields in which a fixed prime number splits completely. III

By Humio Ichimura

Department of Mathematics, Yokohama City University, 22–2 Seto, Kanazawa–ku, Yokohama, Kanagawa 236-0027

(Communicated by Shokichi Iyanaga, M. J. A., Nov. 12, 1999)

1. Introduction. Let p be a fixed prime number and $M(p)^+$ the set of all real quadratic fields in which p splits. For a quadratic field $K \in M(p)^+$, denote by $\delta_p^+(K)$ the order of the ideal class of K containing a prime ideal of K over p. Here, an ideal class is the one in the usual sense. We are concerned with the image of the map

$$\delta_p^+ : M(p)^+ \longrightarrow \boldsymbol{N}, \quad K \to \delta_p^+(K).$$

In the previous note [4], we showed that the image $\mathrm{Im}\,\delta_p^+$ of δ_p^+ contains 2^n for all $n \geq 0$ and any p. The purpose of this note is to show the following:

Theorem. *Assume that the abc conjecture holds.* (i) *Then, the complement* $\boldsymbol{N} \setminus \mathrm{Im}\,\delta_p^+$ *is a finite set for any prime number* p. (ii) *Further,* $\mathrm{Im}\,\delta_p^+$ *coincides with* $\boldsymbol{N}$ *for infinitely many* p.

The abc conjecture predicts that for any $\eta > 0$, there exists a positive constant $C = C_\eta$ depending only on η with which the inequality

$$(1) \qquad \max(|a|, |b|, |c|) < C \left(\prod_{\ell | abc} \ell \right)^{1+\eta}$$

holds for all nonzero integers a, b, c with $a + b = c$ and $(a, b, c) = 1$. Here, in the RHS of (1), ℓ runs over the prime numbers dividing abc. For more on the conjecture, confer Vojta [6, Chapter 5].

2. Lemma. Let d (> 1) be a square free integer and m (> 1) a natural number. Let (u, v) be an integral solution of the diophantine equation

$$(2) \qquad X^2 - dY^2 = \pm 4m.$$

We say that (u, v) is a trivial solution when $m = n^2$ is a square and $n|u$, $n|v$.

Lemma. *Let* d (> 1) *be a square free integer. Let* $\epsilon = (s + t\sqrt{d})/2$ *be a nontrivial unit of the real quadratic field* $K = \boldsymbol{Q}(\sqrt{d})$ *with* $\epsilon > 1$. *For a natural number* m (> 1), *if the equation* (2) *has a nontrivial integral solution, then we have*

$$m \geq \begin{cases} s/t^2, & \text{for } N(\epsilon) = -1, \\ (s-2)/t^2, & \text{for } N(\epsilon) = 1. \end{cases}$$

Here, $N(*)$ *denotes the norm map.*

This lemma was proved in Ankeny, Chowla and Hasse [1] and Hasse [2] when m is not a square. For the general case, see the author [3], and also Yokoi [8], Mollin [5].

3. Proof of Theorem. For a natural number n, we put $K = K_{(p,n)} = \boldsymbol{Q}(\sqrt{p^{2n} + 4})$. As is easily seen, $p^{2n} + 4$ is not a square. We see that

$$\epsilon = \frac{1}{2}\,(p^n + \sqrt{p^{2n} + 4})$$

is a nontrivial unit of the real quadratic field K with $N(\epsilon) = -1$.

First, we show the assertion (i) of the Theorem for the case $p \neq 2$. Let n be a natural number and $K = K_{(p,n)}$. We see that p splits in K, and let $\mathfrak{P}$ be a prime ideal of K over p. Let n_0 be the order of the ideal class $[\mathfrak{P}]$ of K containing $\mathfrak{P}$. We put $\alpha = 1 - \epsilon$. We have $N(\alpha) = -p^n$ and $Tr(\alpha) = 2 - p^n$, where $Tr(*)$ is the trace map. In particular,

$$(\alpha, \alpha') \supseteq (p^n, 2 - p^n) = 1$$

as $p \neq 2$. Here, α' is the conjugate of α. Therefore, we obtain

$$(3) \qquad (\alpha) = \mathfrak{P}^n,$$

and hence $n_0 | n$. We show, under the abc conjecture, that $n_0 = n$ when n is sufficiently large.

Write $p^{2n}+4 = f^2 d$ with d square free. Applying the inequality (1) for $(p^{2n}+4) - p^{2n} = 4$, we see that

$$f^2 d < c_1 \left(2p \prod_{\ell | p^{2n}+4} \ell \right)^{1+\eta} \leq c_1 (2pfd)^{1+\eta}$$

with $\eta = 1/100$ (say). Here, c_1 is a constant depending only on η, and ℓ runs over the prime numbers dividing $p^{2n} + 4$. From this, we obtain

$$f^{1-\eta} < c_2 p^{1+\eta} d^\eta = c_2 p^{1+\eta} \left(\frac{p^{2n}+4}{f^2} \right)^\eta,$$

Partially supported by Grant–in–Aid for Scientific Research (C), (No. 11640041), the Ministry of Education, Science, Sports and Culture of Japan.