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 $\operatorname{Im}\delta_p^+$ 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 $\boldsymbol{N} \setminus \operatorname{Im}\delta_p^+$ is a finite set for any prime number p.* (ii) *Further, $\operatorname{Im}\delta_p^+$ 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

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

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

$$X^2 - dY^2 = \pm 4m. \tag{2}$$

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

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

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

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

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.

and hence

$$f < c_3 p(p^{2n}+4)^{\eta/(1+\eta)} < c_4 p^{x_n}$$

with

$$x_n = 1 + (2\eta/(1+\eta))n.$$

Here, c_2, c_3, c_4 are constants depending only on η (= 1/100). Therefore, we see that

$$f < p^{n/4} \tag{4}$$

when $n \geq 5$ and $p^{y_n} > c_4$ with

$$y_n = n/4 - x_n = 93n/404 - 1.$$

In particular, for each p (≥ 3), the inequality (4) holds for all sufficiently large n. Further, when p is sufficiently large, (4) holds for all n (≥ 5).

Assume that the inequality (4) holds for a given pair (p, n) with $n \geq 5$. We show that $n_0 = n$. We have $\epsilon = (p^n + f\sqrt{d})/2$ and $N(\epsilon) = -1$. Since n_0 is the order of the ideal class $[\mathfrak{P}]$, there exists a non-trivial solution for the equation (2) with $m = p^{n_0}$. Therefore, from the Lemma, we see that

$$p^{n_0} \geq p^n/f^2 > p^{n/2}.$$

Then, as $n_0 | n$, we obtain $n_0 = n$. The desired assertion follows from this. Moreover, from the above argument, we also obtain the following:

Proposition. *Assume that the abc conjecture holds. When p is sufficiently large,* $\mathrm{Im}\,\delta_p^+$ *contains all natural numbers n with $n \geq 5$.*

Next, we show the assertion (ii). It suffices to show that Im δ_p^+ contains 3 for infinitely many p because of the Proposition and the assertion of [4] recalled in Section 1. We use the same notation as above. Let $n = 3$. We assume that $p \equiv \pm 2 \mod 5$ and $p > 3$. Then, by Weinberger [7, Lemma 4], ϵ is a fundamental unit of $K = K_{(p,3)}$. We show that $n_0 = 3$ when p further satisfies

$$p \equiv 1 \bmod 3 \quad \text{and} \quad 2 \bmod p \notin (\boldsymbol{Z}/p\boldsymbol{Z})^{\times 3}.$$

We easily see that there are infinitely many p satisfying these conditions. Assume, on the contrary, that $n_0 \neq 3$. Then, as $n_0 | n = 3$, we have $n_0 = 1$, i.e., $\mathfrak{P}$ is principal. Hence, by (3),

$$\alpha = \pm\epsilon^a x^3 \tag{5}$$

for some integer a and some $x \in K^\times$. Let $\mathfrak{P}'$ be the conjugate of $\mathfrak{P}$. We see from $\mathfrak{P}'^3 = (\alpha')$ that $\sqrt{p^6+4} \equiv -2 \bmod \mathfrak{P}'$, and hence

$$\epsilon \equiv -1 \bmod \mathfrak{P}' \quad \text{and} \quad \alpha \equiv 2 \bmod \mathfrak{P}'.$$

Therefore, (5) is impossible since $2 \mod p$ is not a cube. Hence, we obtain $n_0 = 3$.

Finally, we show the assertion (i) for the case $p = 2$. Let $p = 2$, $n \geq 3$, $m = n - 2$ and $K = K_{(2,n)}$. Then, $(p^{2n}+4)/4$ is an integer congruent to 1 modulo 8. Hence, p splits in K. Let $\mathfrak{P}$ be a prime ideal of K over p, and m_0 the order of the ideal class $[\mathfrak{P}]$. Define an integer α of K by

$$\alpha = \frac{1}{2}\,(2^{n-1} + 1 + \sqrt{2^{2n-2}+1}).$$

Since $N(\alpha) = 2^m$ and $Tr(\alpha) = 2^{n-1}+1$, we see that $(\alpha) = \mathfrak{P}^m$, and hence $m_0 | m$. We can show, under the abc conjecture, that $m_0 = m$ for sufficiently large n by an argument similar to the case $p \neq 2$.

References

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

[2] H. Hasse: Über die mehrklassige, aber einegeschlechtige reell-quadratishe Zahlkörper. Elem. Math., **20**, 49–59 (1965).

[3] H. Ichimura: A note on quadratic fields in which a fixed prime number splits completely. Nagoya Math. J., **99**, 63–71 (1985).

[4] H. Ichimura: A note on quadratic fields in which a fixed prime number splits completely, II. Proc. Japan Acad., **75A**, 150–151 (1999).

[5] R. Mollin: On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud–Degert type. Nagoya Math. J., **105**, 39–47 (1987).

[6] P. Vojta: Diophantine Approximations and Value Distribution Theory. Lecture Notes in Math., vol. 1239, Springer, New York, pp. 1–132 (1987).

[7] P. Weinberger: Real quadratic fields with class numbers divisible by n. J. Number Theory, **5**, 237–241 (1973).

[8] H. Yokoi: Some relations among new invariants of prime number p congruent to 1 mod 4. in Investigation in Number Theory (ed. T. Kubota). Adv. Stud. Pure Math., vol. 13, Kinokuniya, Tokyo, pp. 493–501 (1988).