A. GRYTCZUK and J. KACIERZYNSKI

ON FACTORIZATION IN REAL QUADRATIC NUMBER FIELDS

ABSTRACT: This paper investigates uniqeness of factorization in quadratic number fields. It is proved by elementary method, that under certain conditions, the ring R_k of a field K is the ring with nonuique factorization.

1. Introduction. Using class-field theory C. S. Herz [1] proved the following result:
Let $K = Q(\sqrt{d})$ be given quadratic number field with the discriminant D which has t distinct prime divisors. Then the class group $H(K)$ of K hast $t-1$ even invariants, except the case when K is real and at least one prime $p \equiv 3 \pmod 4$ is ramified, in this case $H(K)$ has $t-2$ even invariants.
From this result we can deduce that if $h = H(K) = 1$ where $K = Q(\sqrt{d})$ and $d > 0$ then

(1.1) $d = p, 2q$

or qr where p is prime and $q \equiv r \equiv 3 \pmod 4$ are primes.

In this paper we prove by simple elementary method without using class-field theory the following.

Theorem. Let Z_s denote the set of all square-free integers and $L_d = \{d : d = p, 2q \text{ or } qr, q \equiv r \equiv 3 (\text{mod } 4)\}$
and let $K = Q(\sqrt{d})$, $d > 0$ and $d \in Z_s \setminus L_d$.
Then the ring R_K of K is the ring with nonuniqueness of factorization.
It is easy to see that from our Theorem follows also the corollary which follows from Herz's result.

Let Z_s denote the set of all squarefree positive integers and
(2.1) $L_d = \{d = p', 2q' \text{ or } q'r'; q' \equiv r' \equiv 3(\text{mod } 4), p', q', r' \text{ are primes}\}$

Then we can prove the following
Lemma 1. For every $d \in Z_s \setminus L_d$ there exist the odd primes p, q, q^* such that

(2.2) $p|d$, $q|d$ (may be $p = q$)

and

(2.3.) $\left(\frac{d}{q^*}\right) = 1$, $\left(\frac{q^*}{q}\right) = \left(\frac{-q^*}{p}\right) = -1$.

Proof. Since $d \in Z_s \setminus L_d$ thus it suffice to consider the following four cases:
1° $d = 2p$, $p \equiv 1 (\text{mod } 4)$ is a prime.

2° $d = 2^\alpha pp_1 \dots p_k$, $p \equiv 1 (\mathrm{mod}\, 4)$; $\alpha = 0$ or 1,
p and p_i are odd distinct primes.

3° $d = 2p_1 p_2 \dots p_k$, $k \geq 2$, $p_i \equiv 3 (\mathrm{mod}\, 4)$ for $i = 1,2,\dots,k$..

4° $d = p_1 p_2 \dots p_k$, $k \geq 3$, $p_i \equiv 3 (\mathrm{mod}\, 4)$ for $i = 1,2,\dots,k$.

Consider the case 1°. Let r denote the quadratic nonresidue for prime $p \equiv 1 (\mathrm{mod}\, 4)$. Hence $\left(\frac{r}{p}\right) = -1$. Suppose that m_0 is a positive integer such that

(2.4) $pm_0 + r \equiv 5 (\mathrm{mod}\, 8)$.

We note that m_0 satisfying (2.4.) exist since the number $pj + r$ for $j = 1,2,\dots,8$ gives distinct residues modulo 8. Let

(2.5) $r_m = p(8m + m_0) + r = 8pm + (pm_0 + r)$, $m = 1,2,\dots$.

From (2.4) it follows that $(8p, pm_0 + r) = 1$.
Therefore by Dirichlet's theorem we obtain from (2.5) that for some m

(2.6) $q^* = r_0$ where q^* is a prime number.

On the other hand by (2.4) it follows that $pm_0 + r = 8k + 5$ thus by (2.5) and (2.6) we obtain

(2.7) $q^* = 8t + 5$.

Since $r_m = q^* = p(8m+m_0)+r$ thus by well-known property of Legendre's symbol we have

(2.8) $$\left(\frac{q^*}{p}\right)=\left(\frac{r}{p}\right)=-1$$

By reciprocity law of Gauss in our case $q^* \equiv 5 \pmod 8$, $p = 4k+1$ we get

(2.9) $$\left(\frac{p}{q^*}\right)=-1 \quad \text{and} \quad \left(\frac{2}{q^*}\right)=-1$$

Thus by (2.9) we have

(2.10) $$\left(\frac{d}{q^*}\right)=\left(\frac{2p}{q^*}\right)=\left(\frac{2}{q^*}\right)\cdot\left(\frac{p}{q^*}\right)=+1.$$

By (2.8) and property of Legendre's symbol we have

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

and the case 1° is proved.

For the proof of case 2° suppose that r, s are the residues for p and p_1 and $r_2, r_3, \ldots, r_k$ are non residues for modulo $p_2, p_3, \ldots, p_k$. Since $(p, p_i) = (p_i, p_j) = 1$ for $i \neq j$ thus by Chinese remainder theorem we obtain, that there exists positive integer u such that

(2.11) $u \equiv r \pmod p$, $u \equiv s \pmod{p_1}$, $u \equiv r_i \pmod{p_i}$; $i = 2, \ldots, k$.

Let m_0 denote the positive integer such that

(2.12) $pp_1 \dots p_k m_0 + u \equiv (\mathrm{mod}\, 8)$.

It is easy to see that such m_0 exist, because the number $pp_1 \dots p_1 j + u$ gives distinct residues (mod 8). Let

(2.13) $r_m = pp_1 \dots p_k (8m + m_0) + u = 8pp_1 \dots p_k m + (pp_1 \dots p_k m_0 + u)$ $m = 1, 2 \dots$. Since $(8pp_1 \dots p_k, pp_1 \dots p_k m_0 + u) = 1$ then by Dirichlet's Theorem we have for some m

(2.14) $q^* = r_m$ where q^* is a prime number.

It is easy to see that by (2.12) it follows that $q \overset{*}{\equiv} 1 (\mathrm{mod}\, 8)$. Therefore similarly as in the case 1° we obtain

(2.15) $$\left(\frac{q^*}{p}\right) = \left(\frac{u}{p}\right) = \left(\frac{r}{p}\right) = -1, \quad \left(\frac{q^*}{p_1}\right) = \left(\frac{u}{p_1}\right) = \left(\frac{s}{p_1}\right) = -1$$

and

(2.16) $$\left(\frac{q^*}{p_i}\right) = \left(\frac{u}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = 1 \qquad \text{for } i = 2, 3, \dots, k.$$

From (2.15), (2.16) and reciprocity law of Gauss we get

$$\left(\frac{p}{q^*}\right) = \left(\frac{p_1}{q^*}\right) = -1, \quad \left(\frac{p_i}{q^*}\right) = 1 \text{ for } i = 2, 3, \dots, k$$

and therefore we have $\left(\frac{d}{q^*}\right) = 1$, $\left(\frac{q^*}{p}\right) = -1$ and $\left(\frac{-q^*}{p}\right) = -1$.

Consider the case 3°. Let $\left(\frac{r_1}{p_1}\right)=+1$ and $\left(\frac{r_i}{p_i}\right)=-1$ for $i=2,3,\ldots,k$. Since $(p_i,p_j)=1$ for $i\neq j$ thus by Chinese remainder theorem we obtain that there exists a positive integer u such that $u\equiv r_i \pmod{p_i}$, for $i=1,2,\ldots,k$.
Similarly as in the case 2°, let m_0 denote the number statisfying $p_1\ldots p_k m_0+u\equiv 3 \pmod 8$ and let

$$r_m = 8p_1\ldots p_k m+(p_1\ldots p_k m_0+u).$$

Thus we obtain for some m, $q\doteq r_m$ and $q^*\equiv 3 \pmod 8$.
Therefore we obtain

(2.17) $\left(\frac{q^*}{p_1}\right)=\left(\frac{u}{p_1}\right)=\left(\frac{r_1}{p_1}\right)=1$ and $\left(\frac{q^*}{p_i}\right)=\left(\frac{u}{p_i}\right)=\left(\frac{r_i}{p_i}\right)=-1$

for $i=2,3,\ldots,k$. By (2.17) and reciprocity law of Gauss it follows that $\left(\frac{p_1}{q^*}\right)=-1$, $\left(\frac{p_i}{q^*}\right)=1$ for $i=2,3,\ldots,k$ and $\left(\frac{2}{q^*}\right)=-1$.

Therefore we obtain $\left(\frac{d}{q^*}\right)=1$, $\left(\frac{-q^*}{p_1}\right)=-1$, $\left(\frac{q^*}{p_2}\right)=-1$, and the case 3° is proved.
For the proof the case 4° we suppose that

$$\left(\frac{r_1}{p_1}\right)=\left(\frac{r_2}{p_2}\right)=1 \text{ and } \left(\frac{r_i}{p_i}\right)=-1 \text{ for } i=3,4,\ldots,k.$$

Since $(p_i,p_j)=1$ for $i\neq j$ thus by Chinese remainder theorem we obtain that there exists a positive integer u such

that $u \equiv r_i \pmod{p_i}$, for $i = 1,2,\ldots,k$. Let m_0 denote the number such that

$$p_1 p_2 \ldots p_k m_0 + u \equiv 3 \pmod 4$$

and

$$r_m = 4p_1 \ldots p_k m + (p_1 \ldots p_k m_0 + u),$$

$m = 1,2,\ldots$ then we have

$$(4p_1 \ldots p_k, p_1 \ldots p_k m_0 + u) = 1$$

and for some m,

$$r_m = q^* \equiv 3 \pmod 4.$$

Since $p_i \equiv 3 \pmod 4$ for $i = 1,2,\ldots,k$ thus we have

$$\left(\frac{q^*}{p_i}\right) = \left(\frac{u}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = \begin{cases} 1 & \text{for } i = 1,2, \\ -1 & \text{for } i = 3,4,\ldots \end{cases}$$

By Gauss theorem we get

$$\left(\frac{p_i}{q^*}\right) = \begin{cases} -1 & \text{for } i = 1,2, \\ 1 & \text{for } i = 3,4,\ldots k. \end{cases}$$

Therefore $\left(\frac{d}{q^*}\right) = 1, \left(\frac{-q^*}{p_3}\right) = -1, \left(\frac{-q^*}{p_1}\right) = -1$

and proof the case 4° and our Lemma is finished.

Lemma 2. Let R_k denote the ring of all integers of $K = Q(\sqrt{d})$, $d > 0$. If R_k is the ring with uniqueness of factorization then the Diophantine equation

(2.18) $x^2 - dy^2 = \pm 4^\alpha p$

has a solution in positive integers x, y for every prime p such that $\left(\frac{d}{p}\right) = +1$, where

$$\alpha = \begin{cases} 0 & \text{if } d \equiv 2,3 \pmod 4 \\ 1 & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Proof. From the assumption that $\left(\frac{d}{p}\right) = +1$ it follows that there exists a positive integer x such that $x^2 \equiv d \pmod p$.
From this follows that

(2.19) $p | x^2 - d = \left(x - \sqrt{d}\right)\left(x + \sqrt{d}\right)$

Suppose that the number p is an irreducible element of R_k. Since the ring R_k is the ring with uniqueness factorization we get that the number p is also prime number in R_k.
The by (2.19) it follows that

(2.20) $p | x - \sqrt{d}$ or $p | x + \sqrt{d}$

it is impossible, because the elements $\frac{x - \sqrt{d}}{p}$ and are no elements of R_k.
Therefore we obtain

(2.21) $p = \left(\frac{x_1 + y_1\sqrt{d}}{2^\alpha}\right) \cdot \left(\frac{x_2 + y_2\sqrt{d}}{2^\alpha}\right)$

where

(2.22) $\alpha = \begin{cases} 0 & d \equiv 2,3 \pmod 4 \\ 1 & d \equiv 1 \pmod 4 \end{cases}$

and the elements $\frac{x_1 + y_1\sqrt{d}}{2^\alpha}$ and $\frac{x_2 + y_2\sqrt{d}}{2^\alpha}$ are noninvertible.

Hence by (2.21) we have

$$(2.23)\quad p^2 = N\left(\frac{x_1 + y_1\sqrt{d}}{2^\alpha}\right)\cdot N\left(\frac{x_2 + y_2\sqrt{d}}{2^\alpha}\right)$$

From (2.23) it follows that the equation

$$|x^2 - dy^2| = 4^\alpha p$$

has a solution in integers, x, y and proof of Lemma 2 is complete.

Result.

We can prove the following

Theorem. Let $K = Q(\sqrt{d})$, $d > 0$, $d \in Z_s \setminus L_d$. Then the ring R_k of K is the ring with nonuniqueness of factorization.

Proof. Suppose that for some $0 < d \in Z_s \setminus L_d$ the ring R_k is the ring with uniqueness of factorization. By Lemma 1 it follows that there are odd primes p, q, q^* such that $p|d$, $q|d$ and

$$(3.1.)\quad \left(\frac{d}{q^*}\right) = 1 \quad , \quad \left(\frac{q^*}{p}\right) = -1 \quad , \quad \left(\frac{-q^*}{p}\right) = -1$$

From (3.1) and Lemma 2 it follows that the equation

$$(3.2)\quad |x^2 - dy^2| = 4^\alpha q^*$$

has a solution in integers x, y. From (3.2) we have

$$(3.3)\quad x^2 - dy^2 = 4^\alpha q^* \qquad \text{or} \qquad x^2 - dy^2 = -4^\alpha q^*.$$

From (3.3) it follows that for $p|d$ and $q|d$ we have

$$(3.4.)\quad \left(\frac{4^\alpha q^*}{p}\right) = 1 \quad \text{or} \quad \left(\frac{-4^\alpha q^*}{q}\right) = 1.$$

But on the other hand from (3.1) we obtain

$$\left(\frac{4^{\alpha}q^{*}}{p}\right)=\left(\frac{q^{*}}{p}\right)=-1 \quad \text{and} \quad \left(\frac{-4^{\alpha}q^{*}}{q}\right)=\left(\frac{-q^{*}}{q}\right)=-1$$

so contrary to (3.4). The proof is complete.

From our Theorem we get the following

Corollary. Let $K=Q(\sqrt{d})$, $d>0$. If R_k of K is the ring with uniquenes of factorization then

$d \in L_d=\{d: d=p, 2q$ or qr, $q \equiv r \equiv 3 \pmod 4$, p,q,r are primes$\}$.

REFERENCES

[1] C. S. Herz, *Construction of class fields* in: Seminar on Complex Multiplication Lectures Notes in Math. Springer-Verlag 21, 1966.

Institute of Mathematics
Departament of Algebra and Number Theory
Pedagogical University of Zielona Góra
Zielona Góra, Poland