ON THE DISTRIBUTION OF QUADRATIC NON-RESIDUES AND THE EUCLIDEAN ALGORITHM IN REAL QUADRATIC FIELDS. I

BY

LOO-KENG HUA

1. **Introduction.** One of the aims of this paper is to establish an explicit upper bound for the least quadratic non-residue, mod p. The bound is not the best[1] which the author can obtain. The author gives such a result owing to the following facts: in the present procedure we may adopt some known results due to Rosser[2] and it is sufficient to establish some typical results in the study of the E.A. (abbreviation of Euclidean algorithm) of real quadratic fields[3].

As to the results in the study of the E.A., we have the following theorem.

THEOREM. *For $d>e^{250}$, there is no E.A. in the quadratic field $R(d^{1/2})$, where d is a square-free integer.*

There are three ways to sharpen the result, (i) by means of Euler's summation formula to improve an estimate of a sum, (ii) reconsideration of the estimate of certain character sums, and (iii) by means of higher order "average" of Riemann-Mangoldt's formula to smooth some results concerning distribution of primes[4].

2. **Lemmas quoted from Rosser's paper.**

LEMMA 1. *Let*

$$\vartheta(x) = \sum_{p\leqq x} \log p$$

Presented to the Society, October 28, 1944; received by the editors November 29, 1943.

[1] A better result has been obtained, for example, we may have $d>e^{160}$ in the theorem. But the proof of it is at least ten times more difficult than the present one.

[2] Amer. J. Math. vol. 63 (1941) pp. 211–232.

[3] As to a detailed description of the history of this problem, see a paper by A. Brauer, Amer. J. Math. vol. 62 (1940) pp. 697–713.

[4] When the paper mentioned in footnote 3 appeared, it was unknown only in the following cases whether the E.A. exists or not:

I. $d=p$ where p is a prime of form $8n+1$ or $p=61$ and 109.

II. $d=p_1p_2\equiv 1$ (mod 24) where p_1 and p_2 are primes and $p_1\equiv p_2\equiv 3$ (mod 4).

In both cases it was known that the algorithm does not exist if d is sufficiently large. But in the meantime it was proved by Rédei (*Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern,* Mat Fiz. Lapok vol. 47 (1940) pp. 78–90) that the algorithm does not exist in the case II. The paper of Rédei was unknown to the author; therefore he considered the cases I and II in the original version of this paper. But the case II is now without any interest. In order to accelerate the publishing under the present conditions this paper was changed a little without the knowledge of the author such that only the case I is considered. A. Brauer.

where p runs over all primes not greater than x. Then we have, for $x \geqq 1$,

$$\vartheta(x) < (1 + 0.0376)x$$

and, for $x \geqq 51^2$, $\vartheta(x) > (1-0.0393)x$.

Proof. (1) By (10) of Rosser, we have, for $x \geqq e^{13.8}$, $\vartheta(x) < (1+0.0376)x$. As to $x < e^{13.8}$, we have $\vartheta(x) < x < (1+0.0376)x$ by Theorem 2 of Rosser.

(2) By (10) of Rosser, we have, for $x \geqq e^{13.8}$, $\vartheta(x) > (1-0.0393)x$. For $71^2 \leqq x < e^{13.8}$, we have, by Theorem 7 of Rosser,

$$\vartheta(x) > x - 2.78x^{1/2} > (1 - 0.0393)x.$$

For $51^2 \leqq x < 71^2$, we have, by Theorem 5 of Rosser,

$$\vartheta(x) > x - 2x^{1/2} > (1 - 0.0393)x.$$

Lemma 2. *Let*

$$\pi(x) = \sum_{p \leqq x} 1, \qquad li\, x = \lim_{\epsilon \to 0} \left(\int_0^{1-\epsilon} + \int_{1+\epsilon}^x \right) \frac{dy}{\log y} \cdot$$

Then, for $x \geqq 2$, we have $\pi(x) < (1+0.0376)(li\ x + 1.85)$, and, for $x \geqq 51^2$, $\pi(x) > (1-0.0393) li\ x - 1.7$.

$$\pi(x) > (1 - 0.0393) li\, x - 1.7.$$

Proof. We have the identity

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(y)dy}{y \log^2 y} \cdot$$

(1) By Lemma 1, we have

$$\begin{aligned} \pi(x) &< 1.0376 \left(\frac{x}{\log x} + \int_2^x \frac{dy}{\log^2 y} \right) \\ &= 1.0376 \left(\int_0^x \frac{dy}{\log y} + \frac{2}{\log 2} - \int_0^2 \frac{dy}{\log y} \right) \\ &< 1.0376(li\, x + 1.85), \end{aligned}$$

using the value $li\ 2 = 1.04$.

(2) By the identity, we have, for $x \geqq K \geqq 51^2$,

$$\begin{aligned} \pi(x) - \pi(K) &= \frac{\vartheta(x)}{\log x} - \frac{\vartheta(K)}{\log K} + \int_K^x \frac{\vartheta(y)dy}{y(\log y)^2} \\ &> \frac{(1 - 0.0393)x}{\log x} - \frac{\vartheta(K)}{\log K} + (1 - 0.0393) \int_K^x \frac{dy}{(\log y)^2} \\ &= (1 - 0.0393)\left(li\, x + \frac{K}{\log K} - li\, K \right) - \frac{\vartheta(K)}{\log K} \cdot \end{aligned}$$

Thus

$$\pi(x) > (1 - 0.0393)(li\, x + K/\log K - li\, K) - (\vartheta(K)/\log K - \pi(K)).$$

Taking $K=51^2$, we have the lemma, since

$$\vartheta(K) = 2519.887, \qquad \pi(K) = 378, \qquad li\,(K) = 392.48.$$

LEMMA 3. *For* $x \geqq 2$,

$$\vartheta(x)/x \geqq 0.3465735.$$

Proof. For $x \geqq 16$, this follows from Lemma 1 and Rosser's Theorem 6. For $x \leqq 16$, the lemma is proved by the direct verifications

$$\vartheta(2)/2 = 0.3465735, \qquad \vartheta(3)/3 > \vartheta(4)/4 \geqq 0.44794,$$
$$\vartheta(5)/5 > \vartheta(6)/6 = 0.56686,$$
$$\vartheta(7)/7 > \vartheta(8)/8 > \vartheta(9)/9 > \vartheta(10)/10 = 0.53471,$$
$$\vartheta(11)/11 > \vartheta(12)/12 = 0.64542,$$
$$\vartheta(13)/13 > \vartheta(14)/14 > \vartheta(15)/15 > \vartheta(16)/16 = 0.64437.$$

3. A lemma concerning series.

LEMMA 4. *For* $q < A$,

$$\sum_{\nu=1}^{A/q} li\,\frac{A}{\nu} \leqq A \log\frac{\log A}{\log q} + \frac{A}{q}\, li\, q.$$

Proof. Since $d\, li(A/x)/dx \leqq 0$, we have

$$\sum_{\nu=1}^{A/q} li\,\frac{A}{\nu} \leqq \int_1^{A/q} li\,\frac{A}{x}\,dx + li\,A = \int_1^{A/q} dx \int_0^{A/x} \frac{dy}{\log y} + li\,A$$
$$= (A/q) li\, q + A \log\log A - A \log\log q.$$

REMARK. The inequality in the lemma may be sharpened by means of Euler's summation formula.

4. Lemmas concerning character sums.

LEMMA 5. *Let p be a prime and* $p \equiv 1 \pmod 4$. *Then, for $A < p$, we have*

$$\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right) \leqq \frac{1}{2} A p^{1/2}$$

where $(\frac{n}{p})$ *is Legendre's symbol.*

Proof. We may assume that $p < (A+1)^2$. For otherwise, we have

$$\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)\right| \leqq \sum_{a=1}^{A}\sum_{n=1}^{a} 1 = \frac{1}{2} A(A+1) \leqq \frac{1}{2} A p^{1/2}.$$

It is well known that

$$\sum_{r=1}^{p}\left(\frac{r}{p}\right)e^{2\pi irn/p}=\left(\frac{n}{p}\right)p^{1/2}.$$

We have

$$p^{1/2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)=\frac{1}{2}p^{1/2}\sum_{a=0}^{A}\sum_{n=-a}^{a}\left(\frac{n}{p}\right)=\frac{1}{2}\sum_{a=0}^{A}\sum_{n=-a}^{a}\sum_{r=1}^{p}\left(\frac{r}{p}\right)e^{2\pi irn/p}$$

$$=\frac{1}{2}\sum_{r=1}^{p}\left(\frac{r}{p}\right)\sum_{a=0}^{A}\sum_{n=-a}^{a}e^{2\pi irn/p}$$

$$=\frac{1}{2}\sum_{r=1}^{p}\left(\frac{r}{p}\right)\frac{\sin^2\pi r(A+1)/p}{\sin^2\pi r/p}.$$

Therefore, we obtain

$$p^{1/2}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)\right|\leqq\frac{1}{2}\sum_{r=1}^{p-1}\frac{\sin^2\pi r(A+1)/p}{\sin^2\pi r/p}=\frac{1}{2}\sum_{r=1}^{p-1}\sum_{a=0}^{A}\sum_{n=-a}^{a}e^{2\pi irn/p}$$

$$=p(A+1)/2-(A+1)^2/2\leqq pA/2.$$

LEMMA 6. *Let $r_1, r_2, \cdots, r_s$ be s distinct primes different from p. Then*

$$\left|\sum_{a=1}^{A}\sum_{n=1,(n,r_1r_2\cdots r_s)=1}^{a}\left(\frac{n}{p}\right)\right|\leqq 2^{s-1}Ap^{1/2}.$$

Proof. The sum may be written as

$$\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)-\sum_{\nu=1}^{s}\sum_{a=1}^{A}\sum_{n=1,r_\nu|n}^{a}\left(\frac{n}{p}\right)+\sum_{1\leqq\nu<\mu\leqq s}\sum_{a=1}^{A}\sum_{n=1,r_\nu r_\mu|n}^{a}\left(\frac{n}{p}\right)-\cdots+\cdots.$$

There are 2^s sums each of the form

$$\sum_{a=1}^{A}\sum_{n=1,m|n}^{a}\left(\frac{n}{p}\right).$$

Now we have

$$\left|\sum_{a=1}^{A}\sum_{n=1,m|n}^{a}\left(\frac{n}{p}\right)\right|=\left|\sum_{a=1}^{A}\sum_{\lambda=1}^{[a/m]}\left(\frac{m\lambda}{p}\right)\right|\ (^5)$$

$$=\left|\sum_{a=1}^{A}\sum_{\lambda=1}^{[a/m]}\left(\frac{\lambda}{p}\right)\right|\leqq m\left|\sum_{b=1}^{A/m}\sum_{\lambda=1}^{b}\left(\frac{\lambda}{p}\right)\right|$$

$$\leqq m\frac{A}{m}p^{1/2}/2=Ap^{1/2}/2$$

by Lemma 5. Thus we have the lemma.

[5] $[x]$ denotes the integral part of x.

LEMMA 7. *Let r_1, r_2 and r_3 be the least three positive primes which are quadratic non-residues* mod p. *Then*

$$r_1 \leqq p^{1/2}, \qquad r_2 \leqq \frac{2}{1-\dfrac{1}{r_1}}p^{1/2}, \qquad r_3 \leqq \frac{4}{\left(1-\dfrac{1}{r_1}\right)\left(1-\dfrac{1}{r_2}\right)}p^{1/2}.$$

Proof. The first inequality(6) follows immediately from Lemma 5, for otherwise, taking $A=p^{1/2}$,

$$\frac{1}{2}p \geqq \sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right) = \sum_{a=1}^{A}\sum_{n=1}^{a} 1 = \sum_{a=1}^{A} a = \frac{1}{2}A(A+1);$$

this is impossible.

We have, by Lemma 6, with $A=r_2-1$,

$$\sum_{a=1}^{A}\sum_{n=1,(n,r_1)=1}^{a} 1 \leqq Ap^{1/2}.$$

Consequently, we have

$$\left(1-\frac{1}{r_1}\right)\sum_{a=1}^{A} a \leqq Ap^{1/2},$$

that is,

$$(1-1/r_1)A(A+1)/2 \leqq Ap^{1/2},$$

$$r_2 \leqq \frac{2}{1-1/r_1}p^{1/2}.$$

The third inequality follows similarly, since

$$\left[\frac{a}{r_1}\right]+\left[\frac{a}{r_2}\right]-\left[\frac{a}{r_1r_2}\right] \leqq \frac{a}{r_1}+\frac{a}{r_2}-\frac{a}{r_1r_2}\cdot$$

5. The growth of the least quadratic non-residue.

LEMMA 8 (VINOGRADOV)(7). *Let $q_1, \cdots, q_s$ be all the primes not exceeding A which are quadratic non-residues* mod p. *Then, we have*

$$\frac{1}{2}\sum_{n=1}^{A}\left(1-\left(\frac{n}{p}\right)\right)-\frac{1}{2}\sum_{n=1,(n,p)\neq 1}^{A} 1 \leqq \sum_{\nu=1}^{s}\left(\frac{A}{q_\nu}\right).$$

Proof. The left-hand side is the number of non-residues $n \leqq A$. Evidently each such n is divisible by one of the q's.

[6] See A. Brauer, *Über den kleinsten quadratischen Nichtrest*, Math. Zeit. vol. 33 (1931) pp. 161–176.

[7] Trans. Amer. Math. Soc. vol. 29 (1927) pp. 216–226.

LEMMA 9. *Under the same assumption as in Lemma* 8, *we have*

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right)-\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}1\leqq\sum_{a=1}^{A}\sum_{q_1\leqq q_\nu\leqq a}\left[\frac{a}{q_\nu}\right].$$

Proof. Summing up the formula in Lemma 7, we have the above lemma immediately.

LEMMA 10. *We have*

$$\sum_{q_1\leqq q\leqq A}\left[\frac{A}{q}\right]=\sum_{\nu=1}^{[A/q_1]}\pi\left(\frac{A}{\nu}\right)-\left[\frac{A}{q_1}\right](\pi(q_1)-1)$$

where q runs over all primes satisfying the inequality

$$q_1\leqq q\leqq A.$$

Proof. We have

$$\begin{aligned}\sum_{q_1\leqq q\leqq A}\left[\frac{A}{q}\right]&=\sum_{A\geqq q>A/2}1+\sum_{A/2\geqq q>A/3}2+\cdots+\sum_{A/[A/q_1]\geqq q\geqq q_1}\left[\frac{A}{q_1}\right]\\&=\pi(A)-\pi(A/2)+2(\pi(A/2)-\pi(A/3))+\cdots\\&\quad+\left[\frac{A}{q_1}\right]\left(\pi\left(A\Big/\left[\frac{A}{q_1}\right]\right)-\pi(q_1)+1\right)\\&=\sum_{\nu=1}^{[A/q_1]}\pi\left(\frac{A}{\nu_1}\right)-\left[\frac{A}{q_1}\right](\pi(q_1)-1).\end{aligned}$$

LEMMA 11. *We have, for $q<A$,*

$$\sum_{a=1}^{A}\sum_{\nu=1}^{[a/q]}\pi\left(\frac{a}{\nu}\right)<1.0376\times A(A+1)/2\left(\log\frac{\log A}{\log q}+\frac{li\,q}{q}+\frac{1.85}{q}\right).$$

Proof. By Lemmas 2 and 4, we have, for $q<a<A$,

$$\begin{aligned}\sum_{\nu=1}^{a/q}\pi\left(\frac{a}{\nu}\right)&<1.0376\sum_{\nu=1}^{a/q}\left(li\frac{a}{\nu}+1.85\right)\\&<1.0376\left(a\log\frac{\log a}{\log q}+\frac{a}{q}li\,q+1.85\frac{a}{q}\right)\\&<1.0376\left(a\log\frac{\log A}{\log q}+a\frac{li\,q}{q}+1.85\frac{a}{q}\right).\end{aligned}$$

The inequality holds evidently for $q>a$. Thus

$$\sum_{a=1}^{A}\sum_{\nu=1}^{a/q}\pi\left(\frac{a}{\nu}\right)<\frac{1.0376}{2}A(A+1)\left(\log\frac{\log A}{\log q}+\frac{li\,q}{q}+\frac{1.85}{q}\right).$$

THEOREM 1. *Let q_1 be the least quadratic non-residue*, mod p. *Then, for $p \geqq e^{250}$, we have*

$$q_1 \leqq (60p^{1/2})^{0.625}.$$

Proof. (1) For $q_1 \leqq e^{80}$, we have

$$q_1 < (60e^{125})^{0.625} \leqq (60p^{1/2})^{0.625}.$$

(2) We suppose that $q_1 > e^{80}$. By Lemmas 9, 10, and 11, we have

$$\begin{aligned}\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right) &\leqq \sum_{a=1}^{A}\sum_{q_1\leqq q\leqq a}\left[\frac{a}{q}\right] \\ &= \sum_{a=1}^{A}\sum_{\nu=1}^{[a/q_1]}\pi\left(\frac{a}{\nu}\right)-\sum_{a=1}^{A}\left[\frac{a}{q_1}\right](\pi(q_1)-1) \\ &< 1.0376\,\frac{A(A+1)}{2}\left(\log\frac{\log A}{\log q_1}+\frac{li\, q_1}{q_1}+\frac{1.85}{q_1}\right) \\ &\quad -\frac{A(A+1)}{2}\left(\frac{1}{q_1}-\frac{2}{A+1}\right)(\pi(q_1)-1).\end{aligned}$$

By Lemmas 5 and 2, we have

$$\begin{aligned}\frac{1}{2}\left(\frac{A(A+1)}{2}-\frac{Ap^{1/2}}{2}\right) &< 1.0376\,\frac{A(A+1)}{2}\left(\log\frac{\log A}{\log q_1}+\frac{li\, q_1}{q_1}+\frac{1.85}{q_1}\right) \\ &\quad -\frac{A(A+1)}{2}\left(\frac{1}{q_1}-\frac{2}{A+1}\right)(0.9607\, li\, q_1-2.7).\end{aligned}$$

Therefore

$$\begin{aligned}\log\log q_1 < \log\log A &+ \frac{li\, q_1}{q_1}+\frac{1.85}{q_1}-\frac{1}{1.0376}\left(\frac{1}{2}-\frac{p^{1/2}}{2(A+1)}\right) \\ &-\frac{1}{1.0376}\left(\frac{1}{q_1}-\frac{2}{A+1}\right)(0.9607\, li\, q_1-2.7).\end{aligned}$$

Taking

$$A+1 = 60p^{1/2},$$

we deduce easily that

$$\begin{aligned}\log\log q_1 < \log\log A &+ 0.07412\, li\, q_1/q_1 + 4.453/q_1 \\ &- 0.48188 + 0.00804 \\ &+ 0.03115\, li\, q_1/p^{1/2} - 0.0546(1/p^{1/2}).\end{aligned}$$

Hence

$$\log\log q_1 < \log\log A - 0.472$$

for $e^{80} < q_1 < p^{1/2}$ and

$$0.07412\, li\, q_1/q_1 < 0.07412\, li\, e^{80}/e^{80} < 0.00095,$$

$$4.453/q_1 < 10^{-33},$$

$$0.03115\, li\, q_1/p^{1/2} < 0.03115\, li\, p^{1/2}/p^{1/2} < 0.03115/38 = 0.00082.$$

Therefore

$$q_1 < A^{e^{-0.472}} < A^{0.625}.$$

We have also:

THEOREM 2. *Let q_1, q_2 and q_3 be the least three prime quadratic non-residues,* mod p. *Then, for $p \geqq e^{250}$, we have*

$$q_2 \leqq (240 p^{1/2})^{0.625}$$

and

$$q_3 \leqq (720 p^{1/2})^{0.625}.$$

The proof of the theorem is similar to that of Theorem 1, but we start with the inequalities

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1,\, q_1 \nmid n}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqq \sum_{a=1}^{A}\left(\sum_{q_2 \leqq q \leqq a}\left[\frac{a}{q}\right] - \sum_{q_2 \leqq q \leqq a/q_1}\left[\frac{a}{q_1 q}\right]\right)$$

and

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1,\,(q_1q_2,n)=1}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqq \sum_{a=1}^{A}\left(\sum_{q_3 \leqq q \leqq a}\left[\frac{a}{q}\right] - \sum_{q_3 \leqq q \leqq a/q_1}\left[\frac{a}{q_1 q}\right] - \sum_{q_3 \leqq q \leqq a/q_2}\left[\frac{a}{q_2 q}\right] - \sum_{q_3 \leqq q \leqq a/q_1q_2}\left[\frac{a}{q_1 q_2 q}\right]\right),$$

respectively, instead of

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqq \sum_{a=1}^{A}\sum_{q_1 \leqq q \leqq a}\left[\frac{a}{q}\right].$$

The corresponding estimates are given in Lemma 6.

6. A necessary condition for the existence of E.A. in a quadratic field.

LEMMA 12[8]. *For a prime p of form $4n+1$, the E.A. cannot exist in $R(p^{1/2})$ if p can be written in the form*

$$p = q_1 n_1 + q_2 n_2,$$

where n_1, n_2, q_1, q_2 are all positive and quadratic non-residues (mod p), *and where the q_i are odd primes which divide $q_i n_i$ to an odd power for $i = 1, 2$.*

[8] P. Erdös and Ch. Ko, *Note on the Euclidean algorithm*, J. London Math. Soc. vol. 13 (1938) pp. 3–8.

Lemma 13. *Suppose that $s<q_1$. Let p_0 be the least prime not dividing s. Then*

$$p_0 \leqq (1/0.346) \log q_1.$$

Proof. By Lemma 3,

$$\vartheta((1/0.346) \log q_1) \geqq \log q_1 > \log s.$$

Thus, there is a prime not greater than $(1/0.346) \log q_1$ not dividing s.

Lemma 14. *Let p be a prime of form $4n+1$. Let q_1, q_2, and q_3 be the least three primes which are quadratic non-residues* mod p. *Suppose that $q_1>3$. If*

$$p > (1/0.346) q_1 q_2 q_3 \log q_1,$$

then we can find two positive numbers s and t such that

$$p = s q_2 q_3 + t q_1$$

where $(\frac{s}{p})=1$ *and* $(s, q_2q_3)=(t, q_1)=1$.

Proof. We have

$$p = s q_2 q_3 + t q_1, \qquad 0 < s < q_1$$

If $q_1 \nmid t$, the lemma follows from Lemma 12 since

$$s q_2 q_3 < q_1 q_2 q_3 < p.$$

The other conditions are evident.

If $q_1 | t$, let p_0 be the least prime not dividing s, then there exists an integer μ such that

$$s + \mu q_1 \equiv 0 \pmod{p_0}, \qquad 0 < \mu < p_0 < q_1.$$

Hence

$$p = ((s + \mu q_1)/p_0) p_0 q_2 q_3 + (t - \mu q_2 q_3) q_1.$$

Since

$$s + \mu q_1/p_0 < (1 + \mu) q_1/p_0 \leqq q_1$$

and, by Lemma 13,

$$((s + \mu q_1)/p_0) p_0 q_2 q_3 < p_0 q_1 q_2 q_3 < p,$$

we have the lemma by Lemma 12.

Lemma 15. *If $q_1>3$ and*

$$(1/0.346) q_1 q_2 q_3 \log q_1 < p,$$

then there is no E.A. in $R(p^{1/2})$.

Proof. The lemma is a consequence of Lemma 14.

LEMMA 16. *If $q_1=3$, there is no E.A. in $R(p^{1/2})$ providing that*

$$5q_2q_3 < p \quad for \quad \left(\frac{5}{p}\right) = 1,$$

and

$$40q_3 < p \quad for \quad \left(\frac{5}{p}\right) = -1.$$

Consequently Lemma 15 holds also for $q_1=3$.

Proof. (1) $(\frac{5}{p})=1$. We may write

$$p = sq_2q_3 + 3t, \quad \text{where} \quad s = 1 \text{ or } 2.$$

If $3\nmid t$, then this gives us a required decomposition; if $3|t$, then

$$p = (s+3)q_2q_3 + 3(t - q_2q_3)$$

will give us the same result.

(2) $(\frac{5}{p})=-1$. Then we may write

$$p = 5sq_3 + 3t, \quad \text{where} \quad s = 1 \text{ or } 2.$$

For $s=1$, the method in (1) gives us a required decomposition. If $s=2$ and $3|t$, we write

$$p = 40q_3 + 3(t - 10q_3).$$

7. Proof of the theorem for the E.A.

THEOREM 3. *For $d>e^{250}$ and square-free, there is no E.A. in the quadratic field $R(d^{1/2})$.*

Proof. According to the results which are already known, it is sufficient to consider the case $d=p\equiv 1 \pmod 4$. By Theorem 2 we have

$$(1/0.346)q_1q_2q_3 \log q_1 < (1/0.346)(60\cdot 240\cdot 720p^{3/2})^{0.625} \log (60p^{1/2})^{0.625} < p.$$

We have the theorem by Lemmas 15 and 16.

NATIONAL TSING HUA UNIVERSITY,
KUNMING, YUNNAN, CHINA.