NOTE ON THE EUCLIDEAN ALGORITHM

PAUL ERDÖS *and* CHAO KO*

[*Extracted from the Journal of the London Mathematical Society, Vol.* 13, 1938.]

1. The E.A. (Euclidean Algorithm) holds for a quadratic field $R(\sqrt{m})$, when, for any two integers α, β in $R(\sqrt{m})$ with $\beta \neq 0$, a third integer γ in $R(\sqrt{m})$ can be so determined that

$$|N(\alpha-\beta\gamma)| < |N(\beta)| \quad \text{or} \quad |N(\alpha/\beta-\gamma)| < 1. \tag{1}$$

The existence of the E.A. is undecided in the following cases, p, q denoting primes:†

I. $m=p=13+24n \quad (n>1)$;

II. $m=p=1+8n \quad (n>7)$;

III. $m=pq$ with $p \equiv q \equiv 3$ or $p \equiv q \equiv 7 \pmod 8$, and $pq>57$.

In this paper, we show that *the* E.A. *does not exist for large p in the first two cases*, *i.e.* it can exist only in a finite number of quadratic fields $R(\sqrt{p})$.

The integers in $R(\sqrt{p})$, where $p \equiv 1 \pmod 4$, are given by $\frac{1}{2}(x+y\sqrt{p})$, where x, y are rational integers and $x \equiv y \pmod 2$. Instead of (1), we can write

$$\left|N\left(a+b\sqrt{p}-\tfrac{1}{2}(x+y\sqrt{p})\right)\right| = |(a-\tfrac{1}{2}x)^2-p(b-\tfrac{1}{2}y)^2| < 1,$$

where a, b, denote rational numbers, *i.e.*

$$|(x-2a)^2-p(y-2b)^2| < 4. \tag{2}$$

* Received 12 March, 1937; read 18 March, 1937.

† Behrbohm and Rédei, "Der E. A. in quadratischen Körpern", *Journal für Math.*, 174 (1936), 193–205; Hofreiter, "Quadratische Körper mit und ohne E. A.", *Monatshefte für Math. und Phys.*, 42 (1935), 397–400.

LEMMA 1. *(Behrbohm and Rédei.) The E.A. does not exist in $R(\sqrt{p})$. $p \equiv 1$ (mod 4), if there exists a quadratic residue r of p, where $0 < r < p$, such that each of the equations*

$$px^2 - Y^2 = -4r, \quad px^2 - Y^2 = 4(p-r) \tag{3}$$

is impossible in integers x, Y.

For suppose that $z^2 \equiv r \pmod{p}$. Take $a = 0$, $b = z/p$. Then, from (2),

$$|px^2 - (py-2z)^2| < 4p.$$

Since the term on the left under the modulus sign is congruent to $-4z^2$ (mod $4p$), the result follows by putting $Y = py - 2z$.

Now, by special choice of r, we have

LEMMA 2. *The E.A. does not exist in $R(\sqrt{p})$ for $p \equiv 1$ (mod 4), if p can be expressed in the form*

$$A_1 Q_1 + A_2 Q_2, \quad (A_i > 0,\ Q_i > 0,\ i = 1,\ 2)$$

where Q_1, Q_2 are odd primes, A_1, Q_1, Q_2 are quadratic non-residues mod p, and A_1, A_2 are not divisible by odd powers of Q_1, Q_2 respectively.

Since $(A_1 Q_1/p) = (A_1/p)(Q_1/p) = 1$, we can take $r = A_1 Q_1$ in Lemma 1, and then (3) becomes

$$px^2 - Y^2 = -4A_1 Q_1, \quad px^2 - Y^2 = 4A_2 Q_2. \tag{4}$$

Since $(p/Q_i) = (Q_i/p) = -1$, and A_i is not divisible by odd powers of $Q_i (i = 1,\ 2)$, both equations in (4) are not solvable and so the Lemma follows.

The proof of the main theorem requires also the following Lemma, of which the proof is given in § 2.

LEMMA 3. *Let q_1, q_2, q_3 be the least three odd prime quadratic non-residues of p. Then, for large p, $p > p(\eta)$,*

$$q_1 q_2 q_3 < p^{1-\eta},$$

where $\eta < \cdot 001$ is an arbitrary positive constant.

THEOREM. *The E.A. does not exist in $R(\sqrt{p})$ for large p, when*

$$p \equiv 13 \pmod{24} \quad or \quad p \equiv 1 \pmod{8}.$$

I. When $p \equiv 13$ (mod 24),

$$(2/p) = -1, \quad (3/p) = 1.$$

Let q_1, q_2 be the two least odd prime quadratic non-residues of p. Define B_1, B_2 by

$$p = 3q_1 q_2 + 2B_1, \quad p = q_1 q_2 + 2B_2.$$

Since $p = 3B_2 - B_1$, one of the B's must be odd. Suppose first that B_1 is odd; by Lemma 3, $B_1 > 0$. Since

$$(2B_1/p) = (-3q_1 q_2/p) = (-1/p)(3/p)(q_1/p)(q_2/p) = 1,$$

we have
$$(B_1/p) = (2/p) = -1,$$

and so B_1 contains an odd prime factor, say q_3, such that $(q_3/p) = -1$ and B_1/q_3 is not divisible by an odd power of q_3. Hence, by Lemma 2 with $Q_1 = q_1$, $A_1 = 3q_2$, $Q_2 = q_3$, the E.A. cannot exist. A similar proof holds when B_2 is odd.

II. When $p \equiv 1 \pmod 8$,

$$(2/p) = 1.$$

Let q_1, q_2, q_3 be the three least prime quadratic non-residues of p.

Suppose first that $q_1 \leqslant p^{\epsilon}$ $(\epsilon \leqslant \eta)$. The congruence

$$p - q_2 q_3 x \equiv 0 \pmod{q_1} \quad (0 < x < q_1)$$

is always solvable, and, by Lemma 3, $p - xq_2 q_3 > 0$. By the definition of q_1, $(x/p) = 1$. If

$$p - q_2 q_3 x \not\equiv 0 \pmod{q_1^2},$$

we can express p in the form of Lemma 2 with $Q_1 = q_2$, $A_1 = q_3 x$, $Q_2 = q_1$, and so the theorem is proved. Otherwise, we can replace x by $(1+q_1)x$ to make

$$p - (1+q_1)xq_2 q_3 \not\equiv 0 \pmod{q_1^2}.$$

Obviously Lemma 2 applies, since, by Lemma 3,

$$(1+q_1)xq_2 q_3 < q_1^2 q_2 q_3 < p \quad \text{for} \quad \epsilon \leqslant \eta.$$

Suppose next that $q_1 > p^{\epsilon}$. The argument above shows that the theorem is proved if x exists such that $0 < x < q_1$ and

$$p - q_2 q_3 x \equiv 0 \pmod{q_1} \quad \text{but} \quad \not\equiv 0 \pmod{q_1^2}.$$

Suppose then that

$$p - q_2 q_3 x \equiv 0 \pmod{q_1^2};$$

we prove that there exists at least one quadratic residue of p among the integers

$$x+q_1, \quad x+2q_1, \ldots, x+[2\log q_1].q_1.$$

By the prime number theorem, the product of the primes not exceeding $2\log q_1$ is

$$e^{2\log q_1+o(\log q_1)} > q_1 > x.$$

Thus there exists a prime $q_0 \leqslant 2\log q_1 < q_1$, *i.e.* $(q_0/p)=1$, and $q_0 \nmid x$. Since q_0 is a divisor of one of the set $x, x+q_1, x+2q_1, \ldots, x+(q_0-1)q_1$, say $x+yq_1$, $y>0$, $x+yq_1=q_0 s$, $s<q_1$. Hence $x+yq_1$ is a quadratic residue mod p, since $(s/p)=1$, and

$$p-q_2q_3(x+yq_1) \not\equiv 0 \pmod{q_1^2}.$$

Also, by Lemma 3,

$$q_2q_3(x+yq_1)=q_0sq_2q_3 < 2q_1(\log q_1).q_2q_3 < 2p^{1-\eta}\log p < p,$$

and hence, by Lemma 2, the theorem is proved.

2. It remains now to prove Lemma 3. This requires the following lemma, the proof of which is similar to that of the well-known Satz 494 of Landau's *Zahlentheorie*, Bd. 2, S. 178.

LEMMA 4. *For* $1 \leqslant f < (p-c)/d$,

$$\left|\sum_{n=1}^{f}\chi(c+nd)\right| < \sqrt{p}\log p,$$

where c, d *are rational integers,* p *is an odd prime and* χ *is any character mod* p *except the principal one.*

Let $q_1, q_2, \ldots, q_z$ be the odd prime quadratic non-residues mod p up to $p^{\frac{1}{2}+\epsilon_1}$ $(0\cdot 01 > \epsilon_1 > 0)$. By the prime number theorem, $z < 2p^{\frac{1}{2}+\epsilon_1}/\log p$. Let k be the number of odd quadratic non-residues mod p up to $p^{\frac{1}{2}+\epsilon_1}$. Then

$$k < \tfrac{1}{2}p^{\frac{1}{2}+\epsilon_1}\sum_{i=1}^{z}\frac{1}{q_i}+z < \tfrac{1}{2}p^{\frac{1}{2}+\epsilon_1}\sum_{i=1}^{z}\frac{1}{q_i}+2\frac{p^{\frac{1}{2}+\epsilon_1}}{\log p}, \tag{5}$$

since each odd non-residue must contain at least one q_i. If h denotes the number of odd quadratic residues mod p up to $p^{\frac{1}{2}+\epsilon_1}$, then

$$h+k \geqslant \tfrac{1}{2}p^{\frac{1}{2}+\epsilon_1}-1.$$

From Lemma 4, we have

$$|h-k| < p^{\frac{1}{2}}\log p;$$

hence $$2k > p^{\frac{1}{2}+\epsilon_1}(\tfrac{1}{2}-\log p/p^{\epsilon_1})-1.$$

Thus, by (5),

$$\tfrac{1}{2}p^{\frac{1}{2}+\epsilon_1}\sum_{i=1}^{z}\frac{1}{q_i}+2\frac{p^{\frac{1}{2}+\epsilon_1}}{\log p} > \tfrac{1}{2}p^{\frac{1}{2}+\epsilon_1}(\tfrac{1}{2}-\log p/p^{\epsilon_1})-\tfrac{1}{2};$$

hence

$$\sum_{i=1}^{z}\frac{1}{q_i} > \tfrac{1}{2}-\epsilon_2, \tag{6}$$

with $0 < \epsilon_2 = \epsilon_2(p, \epsilon_1) < 2 \, . \, 10^{-5}$.

Suppose first that $q_1 \leqslant p^{\epsilon_3}$ $(0 < \epsilon_3 \leqslant \frac{1}{2}\eta)$. Then, since $q_1 \geqslant 3$,

$$\sum_{i=2}^{z} 1/q_i > 1/6-\epsilon_2.$$

If $q_2 \neq 5$, $$\sum_{i=3}^{z} 1/q_i > 1/6-\epsilon_2-1/7 > 1/43.$$

From the prime number theorem,

$$\sum_{P \leqslant y} 1/P = \log\log y + C + o(1),$$

where P denotes a prime, and C is a constant. Hence

$$\sum_{p^{\frac{1}{2}-\epsilon_4} \leqslant P \leqslant p^{\frac{1}{2}+\epsilon_1}} 1/P = \log\log p^{\frac{1}{2}+\epsilon_1} - \log\log p^{\frac{1}{2}-\epsilon_4} + o(1) < 1/43,$$

by choice of $\epsilon_4 > 0$. We see also that we can take $\epsilon_4 > \frac{3}{4}\eta$. Hence

$$q_3 < p^{\frac{1}{2}-\epsilon_4},$$

and so

$$q_1 q_2 q_3 < q_1 q_3^2 < p^{\epsilon_3+1-2\epsilon_4} \leqslant p^{1+\frac{1}{2}\eta-\frac{3}{2}\eta} = p^{1-\eta}.$$

If $q_2 = 5$, by Lemma 4, with $c = 1$, $d = 30$, there exists at least one quadratic non-residue among the positive integers of the form $30n+1$ up to $p^{\frac{1}{2}+\epsilon_1}$, since $p^{\frac{1}{2}+\epsilon_1} > \sqrt{p}\log p$, and so

$$q_3 < p^{\frac{1}{2}+\epsilon_1} \quad \text{and} \quad q_1 q_2 q_3 = 15 q_3 < p^{1-\eta}.$$

Suppose next that $q_1 > p^{\epsilon_3}$. Since $q_2 > q_1 > p^{\epsilon_3}$, from (6), we get

$$\sum_{i=3}^{z} 1/q_i > \tfrac{1}{2}-\epsilon_2', \tag{7}$$

where $0 < \epsilon_2' < 10^{-5}$. Since, by choice of ϵ_5 $(0{\cdot}008 > \epsilon_5 > 0{\cdot}007)$,

$$\sum_{p^{(1/2\sqrt{e})+\epsilon_4} \leqslant P \leqslant p^{\frac{1}{2}+\epsilon_1}} 1/P = \log\log p^{\frac{1}{2}+\epsilon_1} - \log\log p^{1/2\sqrt{e}+\epsilon_5} < \tfrac{1}{2}-\epsilon_2',$$

we have*, from (7),

$$q_3 < p^{1/2\sqrt{e}+\epsilon_3}.$$

Hence $$q_1 q_2 q_3 < p^{3/2\sqrt{e}+3\epsilon_3} < p^{1-\eta}.$$

This proves the lemma.

We should like to thank Prof. L. J. Mordell for his help with our manuscript.

The University of Manchester.

* Vinogradov proved that the least quadratic non-residue mod p is less than

$$p^{1/2\sqrt{e}}(\log p)^2.$$

See J. M. Vinogradov, " Sur la distribution des résidus et des non-résidus des puissances ", *Journ. Physico-Math. Soc. of Perm*, 1 (1919), 94–98; or " On the bound of the least non-residue of n-th powers ", *Trans. American Math. Soc.*, 29 (1927), 218–226.

Printed by C. F. Hodgson & Son, Ltd., Newton St., London, W.C.2.