ON EUCLID'S ALGORITHM IN REAL QUADRATIC FIELDS

By Mr H. HEILBRONN, Trinity College

[*Received* 5 August, *read* 17 October 1938]

The object of this paper is to complete the proof of the

THEOREM. *Let* $P(\sqrt{d})$ *be the quadratic field of discriminant* $d > 0$. *Then Euclid's algorithm does not hold in* $P(\sqrt{d})$ *if* d *is sufficiently large.*

This was proved for even discriminants by Berg† in a surprisingly simple way.

The problem was further investigated by Behrbohm and Rédei‡, who proved the theorem in several special cases. In particular, they showed that unique factorization can only hold in $P(\sqrt{d})$ for odd d if d is either a prime or a product of two different primes $\equiv 3 \pmod 4$. Since unique factorization follows from Euclid's algorithm, we can restrict ourselves to these two cases.

For the first of these cases (d prime), the theorem was proved by Erdös and Ko§ in a recent paper. The method employed there is applied in the present paper to both cases, so that no knowledge of the former paper is required here.

Notation. All Latin letters except e denote positive rational integers; p, q and r always denote primes.

The discriminant d of our field $P(\sqrt{d})$ is either of the form

$$d = q_1, \quad q_1 \equiv 1 \pmod 4$$

or of the form $$d = q_1 q_2, \quad q_1 < q_2, \quad q_1 \equiv q_2 \equiv 3 \pmod 4.$$

The symbol O involves absolute constants only.

Let r_1, r_2, r_3 be the three smallest primes which satisfy

$$\left(\frac{d}{r_1}\right) = \left(\frac{d}{r_2}\right) = \left(\frac{d}{r_3}\right) = -1, \quad r_1 < r_2 < r_3.$$

LEMMA 1. *Let* r_1 *and* r_2 *divide* a_1 *and* a_2 *respectively, each to an odd power, where*

$$a_1 + a_2 = d.$$

Then Euclid's algorithm does not hold in $P(\sqrt{d})$ *if* a_1 *or* a_2 *is a quadratic residue* mod d *in the naive sense*||.

† *Kungl. Fysiogr. Sällskapeti Lund Förhandlingar*, 5 (1935), 5.

‡ *Journal für Math.* 174 (1936), 192–205.

§ *Journal London Math. Soc.* 13 (1938), 3–8.

|| We say that u is a quadratic residue mod v in the naive sense, if the congruence

$$y^2 \equiv u \pmod v$$

has a solution.

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press

Proof (indirect). Let us assume that Euclid's algorithm holds in $P(\sqrt{d})$ and that a_2 is a quadratic residue mod d.

Then we can find, for every integer z, an integer α in the field such that

$$z \equiv \alpha \pmod{\sqrt{d}},$$
$$|N(\alpha)| < |N(\sqrt{d})| = d.$$

The conjugate congruence $z \equiv \alpha' \pmod{\sqrt{d}}$

is also valid; hence we have $z^2 \equiv N(\alpha) \pmod{\sqrt{d}}$.

Since z^2 and $N(\alpha)$ are rational integers, and since d is quadratfrei, it follows that

$$z^2 \equiv N(\alpha) \pmod{d}.$$

We now choose z as a solution of the congruence

$$z^2 \equiv a_2 \pmod{d}.$$

Then we have an integer α satisfying

$$N(\alpha) \equiv a_2 \pmod{d},$$
$$|N(\alpha)| < d.$$

Hence, either $N(\alpha) = a_2$ or $N(\alpha) = a_2 - d = -a_1$.

But neither a_2 nor $-a_1$ can be the norm of a number of $P(\sqrt{d})$, since they are each divisible by a prime to an odd multiplicity for which d is a quadratic non-residue.

This contradiction proves the Lemma.

LEMMA 2. *If* $d \nmid m$, *then*

$$\sum_{\substack{n=1 \\ n \equiv 1 (m)}}^{x} \left(\frac{d}{n}\right) = O\{m^{\frac{1}{2}} d^{\frac{1}{2}} \log (md)\}.$$

Proof. It is well known that, for any non-principal character χ mod k,

$$\sum_{n=1}^{x} \chi(n) = O(k^{\frac{1}{2}} \log k).$$

Let ψ be any character mod m. Then $\psi(n)(d/n)$ is a character mod (md), and is not principal since $d \nmid m$.

Hence, if ψ runs through all characters mod m,

$$\sum_{\substack{n=1 \\ n \equiv 1 \pmod{m}}}^{x} \left(\frac{d}{n}\right) = \frac{1}{\phi(m)} \sum_{\psi} \sum_{n=1}^{x} \psi(n) \left(\frac{d}{n}\right)$$
$$= \frac{1}{\phi(m)} \sum_{\psi} O\{m^{\frac{1}{2}} d^{\frac{1}{2}} \log (md)\}$$
$$= O\{m^{\frac{1}{2}} d^{\frac{1}{2}} \log (md)\}.$$

LEMMA 3. $$r_3 = O(d^{\frac{1}{2}-\epsilon})$$

for a suitably chosen absolute constant $\epsilon > 0$.

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press

Proof†. We choose two absolute constants $\delta > 0$, $\epsilon > 0$, such that

$$\tfrac{1}{2}e^{-\frac{1}{2}+7\delta} + \epsilon = \tfrac{1}{3}, \quad \tfrac{1}{2} - 6\delta > 0.$$

We put
$$m = \prod_{\substack{e=1 \\ r_e < \delta^{-1}}}^{3} r_e \prod_{\substack{q \mid d \\ q < \delta^{-1}}} q$$

(so that m is bounded), and $x = [d^{\frac{1}{2}} \log^2 d]$.

We assume at once that d is large enough to satisfy the following conditions:

$$d > m, \tag{1}$$

$$x^{e^{-\frac{1}{2}+6\delta}} < d^{\frac{1}{2}e^{-\frac{1}{2}+7\delta}}. \tag{2}$$

Further we may assume that r_3 is so large that

$$\sum_{r_3 \leqslant p \leqslant x} \frac{1}{p} \leqslant \log_+\left(\frac{\log x}{\log r_3}\right) + \delta, \tag{3}$$

where $\log_+(\eta)$ denotes $\max(\log \eta, 0)$.

(1) shows that Lemma 2 is applicable. So we have

$$\sum_{\substack{n=1 \\ n \equiv 1 (m)}}^{x} \left(\frac{d}{n}\right) = O\{m^{\frac{1}{2}} d^{\frac{1}{2}} \log (md)\}$$
$$= O(d^{\frac{1}{2}} \log d). \tag{4}$$

On the other hand, $(d/n) = 1$ unless n is divisible by q_1, q_2, r_1, r_2 or a prime $\geqslant r_3$.

Hence
$$\sum_{\substack{n=1 \\ n \equiv 1 (m)}}^{x} \left(\frac{d}{n}\right) \geqslant \sum_{\substack{n=1 \\ n \equiv 1 (m)}}^{x} 1 - 2 \sum_{p}^{*} \sum_{\substack{n=1 \\ n \equiv 1 (m) \\ n \equiv 0 (p)}}^{x} 1,$$

where the star indicates that the summation is extended over all primes between r_3 and x, both inclusive, and over those of the primes q_1, q_2, r_1, r_2 which do not divide m and which are therefore greater than or equal to δ^{-1}.

Since
$$\sum_{\substack{n=1 \\ n \equiv 1 (m) \\ n \equiv 0 (p)}}^{x} 1 \leqslant \frac{x}{mp} + 1,$$

we have
$$\sum_{\substack{n=1 \\ n \equiv 1 (m)}}^{x} \left(\frac{d}{n}\right) \geqslant \frac{x}{m} - 2\left\{4\left(\frac{\delta x}{m} + 1\right) + \sum_{r_3 \leqslant p \leqslant x} \left(\frac{x}{mp} + 1\right)\right\}$$
$$\geqslant \frac{x}{m}\left\{1 - 8\delta - 2 \sum_{r_3 \leqslant p \leqslant x} \frac{1}{p}\right\} - 8 - \pi(x)$$
$$\geqslant \frac{x}{m}\left\{1 - 8\delta - 2\log_+\left(\frac{\log x}{\log r_3}\right) - 2\delta\right\} - 8 - \pi(x),$$

by (3).

† Vinogradov, *Trans. Amer. Math. Soc.* 29 (1927), 218–26 proved $r_1 = O(d^{\frac{1}{2}e^{-\frac{1}{2}+\epsilon}})$. His proof is easily generalized to obtain Lemma 3. See also Erdös and Ko, *loc. cit.* Lemma 3.

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press

Combining this inequality with (4), we have

$$\frac{x}{m}\left\{1-10\delta-2\log_+\left(\frac{\log x}{\log r_3}\right)\right\}\leqslant O\{\pi(x)+d^{\frac{1}{2}}\log d\},$$

i.e. dividing by x/m, $\quad 1-10\delta-2\log_+\left(\frac{\log x}{\log r_3}\right)\leqslant O\left(\frac{1}{\log d}\right).$

Hence, for sufficiently large d,

$$1-11\delta-2\log_+\left(\frac{\log x}{\log r_3}\right)\leqslant 0,$$

$$\log_+\left(\frac{\log x}{\log r_3}\right)\geqslant \tfrac{1}{2}-6\delta>0,$$

$$\log\frac{\log x}{\log r_3}\geqslant \tfrac{1}{2}-6\delta,$$

$$r_3\leqslant x^{e^{-\frac{1}{2}+6\delta}}$$

$$\leqslant d^{\frac{1}{2}e^{-\frac{1}{2}+7\delta}} \quad \text{(by (2))}$$

$$= d^{\frac{1}{2}-\epsilon}.$$

LEMMA 4. *If $r_1\geqslant 5$, $s<r_1$, we can find a prime p_0 not dividing s, which satisfies the inequalities*

$$p_0<r_1, \tag{5}$$

$$p_0\leqslant \log d, \text{ if } d \text{ is sufficiently large.} \tag{6}$$

Proof. Let p_0 be the least prime not dividing s. If $s\leqslant 2$, $p_0=s+1<r_1$; if $s>2$, no prime-divisor of $s-1$ exceeds s, hence $p_0\leqslant s-1<r_1$. This proves (5).

Further, by the prime number theorem, for large d

$$\sum_{p\leqslant \log d}\log p=\log d+o(\log d)$$

$$>\log r_3 \quad \text{(by Lemma 3)}$$

$$>\log r_1$$

$$>\log s.$$

This proves (6).

LEMMA 5. *If d is sufficiently large, then we can find two numbers s and t with the following properties:*

$$d=sr_2r_3+tr_1; \tag{7}$$

$$\left(\frac{d}{s}\right)\geqslant 0; \tag{8}$$

either $\quad (s, r_2r_3)=1 \tag{9}$

or $\quad (s, r_2^3r_3)=r_2^2; \tag{10}$

either $\quad (t, r_1)=1 \tag{11}$

or $\quad (t, r_1^3)=r_1^2. \tag{12}$

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press

Proof. We note, first, that (8) and (9) are automatically satisfied if every prime factor of s is less than r_1, in particular, if $s < r_1$.

We distinguish five cases.

First case. $r_1 \geqslant 5$. We choose d so large that Lemma 4 becomes applicable, and that

$$r_3^3(1+\log d) < d. \tag{13}$$

This is possible by Lemma 3.

We choose s as the smallest positive root of the congruence

$$r_2 r_3 s \equiv d \pmod{r_1}.$$

Then $$s < r_1, \quad s r_2 r_3 < r_3^3 < d$$

and we have a representation $$d = s r_2 r_3 + t r_1$$

which satisfies all conditions of our lemma with the possible exception of (11) and (12).

If $r_1 \mid t$, we denote by n the smallest positive root of the congruence

$$s + n r_1 \equiv 0 \pmod{p_0},$$

where p_0 is the prime in Lemma 4, and we consider the representation

$$d = \frac{s+nr_1}{p_0} p_0 r_2 r_3 + (t - n r_2 r_3) r_1,$$

where (11) is now satisfied since $n < p_0 < r_1$.

Further $$\frac{s+nr_1}{p_0} < \frac{(n+1)r_1}{p_0} \leqslant r_1,$$

so that (8) and (9) are satisfied and

$$\begin{aligned} \frac{s+nr_1}{p_0} p_0 r_2 r_3 &< r_1 p_0 r_2 r_3 \\ &< r_3^3 \log d \\ &< d \end{aligned}$$

by (13).

Second case. $r_1 = 3$. We have a representation

$$d = s r_2 r_3 + 3t$$

with $s \leqslant 2$, which satisfies (8) and (9). If $3 \mid t$ we replace it by

$$d = 4 s r_2 r_3 + 3(t - s r_2 r_3),$$

so that (11) is satisfied and we have, for large d,

$$t - s r_2 r_3 > 0.$$

Third case. $r_1 = 2$, $r_2 > 3$. We have a representation

$$d = r_2 r_3 + 2t,$$

and also $$d = 3 r_2 r_3 + 2(t - r_2 r_3)$$

and either t or $t - r_2 r_3$ is odd.

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press

Fourth case. $r_1 = 2, r_2 = 3, r_3 \equiv 1 \pmod 4$. If we write

$$d = 3r_3 + 2t,$$

then $t \equiv 1 \pmod 2$, since $d \equiv 1 \pmod 4$ and $3r_3 \equiv 3 \pmod 4$.

Fifth case. $r_1 = 2, r_2 = 3, r_3 \equiv -1 \pmod 4$. We have a representation

$$d = 3r_3 + 4t,$$

from which we deduce

$$d = 15r_3 + 4(t - 3r_3),$$
$$d = 27r_3 + 4(t - 6r_3),$$
$$d = 135r_3 + 4(t - 33r_3).$$

All these four relations satisfy (8). The first two satisfy (9) and the last two satisfy (10). Finally one of them satisfies (12) since the numbers t, $t - 3r_3$, $t - 6r_3$, $t - 33r_3$ run through a complete residue system mod 4, and therefore one of them must be even but not divisible by 4.

LEMMA 6. *If*

$$a_1 + a_2 = d,$$
$$\left(\frac{d}{a_1}\right) \geqslant 0,$$

then either a_1 or a_2 is a quadratic residue mod d *in the naive sense*†.

Proof. If $d = q_1$, it follows that $(a_1, q_1) = 1$,

$$\left(\frac{a_1}{q_1}\right) = 1,$$

and a_1 is a quadratic residue mod d in the ordinary sense.

If $d = q_1 q_2$, we note first that

$$\left(\frac{d}{a_1}\right) = \left(\frac{d}{a_2}\right) \geqslant 0;$$

hence, reducing the Kronecker symbols to Legendre symbols,

$$\left(\frac{a_1}{q_1}\right)\left(\frac{a_1}{q_2}\right) = \left(\frac{a_2}{q_1}\right)\left(\frac{a_2}{q_2}\right) \geqslant 0. \tag{14}$$

Since $q_1 \equiv q_2 \equiv 3 \pmod 4$, we have

$$\left(\frac{a_1}{q_1}\right) = -\left(\frac{a_2}{q_1}\right), \quad \left(\frac{a_1}{q_2}\right) = -\left(\frac{a_2}{q_2}\right).$$

Since $d \nmid a_1$, not all four Legendre symbols are zero. Hence at least one of them must be positive, say

$$\left(\frac{a_i}{q_j}\right) = 1,$$

and therefore by (14)

$$\left(\frac{a_i}{q_k}\right) \geqslant 0 \text{ for } k = 1 \text{ and } 2.$$

Hence a_i is a quadratic residue mod d in the naive sense.

PROOF OF THE MAIN THEOREM. Lemmas 1, 5 and 6.

† It may, of course, happen that a_1 and a_2 are both residues.

https://doi.org/10.1017/S030500410002051X Published online by Cambridge University Press