ON EUCLID'S ALGORITHM IN CUBIC SELF-CONJUGATE FIELDS

By H. HEILBRONN

Received 11 October 1949

In a paper published in these *Proceedings*† I proved that there are only a finite number of quadratic fields in which Euclid's Algorithm (E.A.) holds. Recently Davenport‡ has found a new proof of this theorem based on the theory of the minima of the product of linear inhomogeneous forms.

He has also been able to extend his result to higher fields, namely, to non-totally real cubic fields and to totally complex quartic fields§. In other words, he has shown that E.A. holds only in a finite number of fields which possess one fundamental unit only.

His results made me take up the problem again, and I shall prove in this paper

THEOREM 1. *E.A. holds only in a finite number of cyclic cubic fields.*

The question of E.A. in totally real non-cyclic cubic fields is thus left open. Though I cannot prove any result in the opposite direction I should be surprised to learn that the analogue of Theorem 1 is true in this case.

In another paper I intend to investigate the case of cyclic fields of degree greater than 3.

If the discriminant of a cyclic cubic field is divisible by t different primes, then the class-number of the field is divisible by 3^{t-1}. Hence it suffices to prove Theorem 1 for fields whose discriminant is a power of a prime d. Actually, neglecting the single field of discriminant 81, we may assume that the discriminant equals d^2, where $d \equiv 1 \pmod 6$ is a prime.

A more detailed account of the most important properties of cyclic cubic fields is given in the Appendix.

We introduce the following conventions. Small italics, except e, i and o, denote positive rational integers; d, p, q always denote primes. The symbols O and o involve absolute constants only; unless otherwise stated the o-process refers to the limit as $d \to \infty$.

We assume $d \equiv 1 \pmod 6$, and denote by $\chi(n)$ a cubic character mod d. A, B, C denote the classes of integers for which $\chi(n) = 1$, $\chi(n) = \frac{1}{2}(-1+i\sqrt{3})$, $\chi(n) = \frac{1}{2}(-1-i\sqrt{3})$ respectively. A^* is the subclass of integers a in A which are of the form

$$a = bc, \quad (b,c) = 1, \quad b \text{ in } B, \quad c \text{ in } C.$$

$q_1 < q_2$ are the two smallest primes not in A; r is the smallest number in A^* prime to q_1.

† Vol. 34 (1938), 521–6.

‡ *Proc. London Math. Soc.* (in course of publication).

§ A preliminary account of the cubic case is given in *C.R. Acad. Sci., Paris*, 228 (1949), 883–5. Detailed proofs will appear in *Acta Mathematica*. I am indebted to Prof. Davenport for a private communication of his results.

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press

We introduce a number ϵ which may be arbitrarily small, and will be fixed later. We put

$$x = [d^{\frac{1}{4}+\epsilon}],$$

and define K as the set of numbers n which satisfy

$$d^{\frac{1}{4}-\epsilon} < n \leqslant x.$$

Symbols like KA, $B+C$, etc., have the meaning usually assigned to them in Boolean algebra.

We recall two well-known facts:

$$\sum_{p \leqslant \eta} p^{-1} = \log\log\eta + D + o(1) \quad \text{as} \quad \eta \to \infty, \tag{1}$$

where D is a constant.

If $\psi(n)$ is a non-principal character mod k, then

$$\sum_{n=1}^{y} \psi(n) = O(k^{\frac{1}{2}} \log k) \tag{2}$$

for all y.

LEMMA 1. *$q_1 r \leqslant d^{1-\epsilon}$ if d is sufficiently large.*

Proof. We distinguish three cases.

First case. $q_2 \leqslant d^{\frac{1}{4}-\epsilon}$. We assume without loss of generality that q_2 lies in B. Let c be the smallest number in C which is prime to $q_1 q_2$. Since $q_2 c$ is prime to q_1 and belongs to A^*, it follows that

$$r \leqslant q_2 c,$$

$$q_1 r \leqslant q_1 q_2 c \leqslant d^{\frac{1}{4}-2\epsilon} c;$$

and the lemma will be proved if we can show that

$$c \leqslant x. \tag{3}$$

If $q_1 \geqslant 7$ it follows from (2) with $k = d$ that there are

$$\tfrac{1}{3}x(1+o(1))$$

numbers not exceeding x which lie in C. Since there are at most

$$(q_1^{-1} + q_2^{-1})x < \tfrac{1}{3}x(1+o(1))$$

numbers not exceeding x which are not prime to $q_1 q_2$, (3) follows.

If $q_1 < 7 \leqslant q_2$ it follows from (2) with $k = q_1 d$ that there are

$$\tfrac{1}{3}(1-q_1^{-1})x(1+o(1)) \geqslant \tfrac{1}{6}x(1+o(1))$$

numbers not exceeding x which lie in C and are prime to q_1. Since there are at most

$$q_2^{-1}x \leqslant \tfrac{1}{7}x < \tfrac{1}{6}x(1+o(1))$$

numbers not exceeding x which are not prime to q_2, (3) follows again.

If $q_1 < q_2 < 7$ it follows from (2) with $k = q_1 q_2 d$ that there are

$$\tfrac{1}{3}(1-q_1^{-1})(1-q_2^{-1})x(1+o(1)) > 0$$

numbers not exceeding x which lie in C and are prime to $q_1 q_2$. This implies (3) again, and the lemma is established in the first case.

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press

Second case. $q_1 > d^{\frac{1}{3}-\epsilon}$. Then all primes $p \leqslant d^{\frac{1}{3}-\epsilon}$ belong to A and we have

$$\sum_{n=1}^{x} \chi(n) = \sum_{n=1}^{x} 1 + \sum_{p \text{ in } K} \sum_{\substack{n=1 \\ p/n}}^{x} (\chi(n)-1) + \sum_{p \text{ in } K} \sum_{p' \text{ in } K} \sum_{\substack{n=1 \\ pp'/n}}^{x} O(1).$$

Unless in the second sum on the right-hand side n/p is divisible by a prime p' in K, we have

$$\chi(n) - 1 = \chi(p) - 1;$$

hence

$$\begin{aligned}\sum_{n=1}^{x} \chi(n) &= x + \sum_{p \text{ in } K} (\chi(p)-1) \sum_{\substack{n=1 \\ p/n}}^{x} 1 + \sum_{p \text{ in } K} \sum_{p' \text{ in } K} \sum_{\substack{n=1 \\ pp'/n}}^{x} O(1) \\ &= x + \sum_{p \text{ in } K} (\chi(p)-1)\left[\frac{x}{p}\right] + \sum_{p \text{ in } K} \sum_{\substack{p' \text{ in } K \\ pp' \leqslant K}} O\left(\frac{x}{pp'}\right) \\ &= x + \tfrac{1}{2}(-3+i\sqrt{3})x \sum_{p \text{ in } KB} p^{-1} + \tfrac{1}{2}(-3-i\sqrt{3})x \sum_{p \text{ in } KC} p^{-1} \\ &\quad + O(\pi(x)) + O(x(\sum_{d^{\frac{1}{3}-\epsilon} < p \leqslant d^{\frac{1}{3}+\frac{1}{2}\epsilon}} p^{-1})^2).\end{aligned}$$

Dividing by x, and using (2) and (1), we get

$$o(1) = 1 + \tfrac{1}{2}(-3+i\sqrt{3}) \sum_{p \text{ in } KB} p^{-1} + \tfrac{1}{2}(-3-i\sqrt{3}) \sum_{p \text{ in } KC} p^{-1} + O(\epsilon^2),$$

whence

$$\sum_{p \text{ in } KB} p^{-1} = \tfrac{1}{3} + O(\epsilon^2), \quad \sum_{p \text{ in } KC} p^{-1} = \tfrac{1}{3} + O(\epsilon^2);$$

$$\sum_{p \text{ in } K(B+C)} p^{-1} = \tfrac{2}{3} + O(\epsilon_2).$$

Since by (1) for $0 < \alpha < \frac{1}{2}$

$$\sum_{d^{\alpha} < p \leqslant d^{\frac{1}{3}+\epsilon}} p^{-1} = \log((\tfrac{1}{2}+\epsilon)\alpha^{-1}) + o(1),$$

it follows for sufficiently large d that $K(B+C)$ contains at least two primes

$$q_1 < q_2 < d^{(\frac{1}{3}+\epsilon)\exp[-\frac{1}{3}+O(\epsilon)]}, \tag{4}$$

whilst KB and KC contain each at least two primes not exceeding

$$d^{(\frac{1}{3}+\epsilon)\exp[-\frac{1}{3}+O(\epsilon)]}.$$

Hence

$$q_1 < d^{(\frac{1}{3}+2\epsilon)\exp[-\frac{1}{3}]}, \quad r < d^{(\frac{1}{3}+2\epsilon)(\exp[-\frac{1}{3}]+\exp[-\frac{1}{2}])},$$

and the lemma follows for sufficiently small ϵ, since

$$e^{-\frac{1}{3}} + \tfrac{1}{2}e^{-\frac{1}{2}} < 1.$$

Third case. $q_1 \leqslant d^{\frac{1}{3}-\epsilon} < q_2$. We repeat the calculation as in the second case, except that n runs only through values prime to q_1. Then by (2)

$$\sum_{\substack{n=1 \\ (n,q_1)=1}}^{x} \chi(n) = \sum_{n=1}^{x} \chi(n) - \chi(q_1) \sum_{m \leqslant xq_1^{-1}} \chi(m) = O(d^{\frac{1}{3}} \log d).$$

In the evaluation of the right-hand side of the first formula each principal term will acquire a factor $1-q_1^{-1}$, which will cancel in the subsequent calculation. (4) is true again, and the remainder of the argument is the same as before.

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press

LEMMA 2. *d is representable as the sum of two numbers in A^*, if d is sufficiently large.*

Proof. We observe first that if a in A^*, p in A, then ap in A^*.

Since by Lemma 1, $q_1 r < d$, we can write

$$d = sr + tq_1, \quad s < q_1.$$

Since all prime divisors of s lie in A, sr lies in A^*. Since $\chi(tq_1) = \chi(-1)\chi(sr) = 1$, tq_1 will lie in A^* if $(t, q_1) = 1$. Since this condition is not automatically satisfied, we have to overcome the difficulty by consideration of three separate cases.

First case, $q_1 = 2$. We consider the representation

$$d = r + 2t, \quad d = 27r + 2(t - 13r).$$

r and $27r$ lie in A^*, and $2t$ or $2(t-13r)$ lie in A^* if t or $t-13r$ are odd. If they were both even, their difference $13r$ would be even, which is impossible since $(q_1, r) = 1$.

Second case. $q_1 = 3$. We consider the representations

$$d = sr + 3t, \quad d = 4sr + 3(t - sr),$$

where $s \leqslant 2$. Again sr and $4sr$ lie in A^*, and $3t$ or $3(t-sr)$ lie in A^* if t or $t-sr$ are not divisible by 3. If they were both divisible by 3, their difference sr would be divisible by 3, which is impossible since $(q_1, r) = 1$.

Third case. $q_1 \geqslant 5$. We start with the representation

$$d = sr + tq_1,$$

where $s < q_1$. Then we can find a prime p_0 such that†

$$p_0 < q_1, \quad (p_0, s) = 1, \quad p_0 = O(\log d).$$

Hence there exists an $l < p_0 < q_1$ such that

$$s + lq_1 \equiv 0 \pmod{p_0},$$

and we have

$$d = (s + lq_1)r + (t - lr)q_1.$$

Since $s + lq_1 < p_0 q_1$, every prime divisor of $s + lq_1$ lies in A, $(s + lq_1)r$ lies in A^* and tq_1 or $(t-lr)q_1$ lie in A^*, if t or $t-lr$ are not divisible by q_1. If they were both divisible by q_1, their difference lr would be divisible by q_1, which is impossible since $(q_1, r) = 1$, $l < q_1$.

Proof of Theorem 1 (indirect). We assume we have a cyclic cubic field of discriminant d^2 in which E.A. holds, and that d is so large that Lemma 2 applies. This implies that

$$d = a + a',$$

where

$$\chi(a) = 1,$$

and none of the four numbers $\pm a$, $\pm a'$ is norm of an integer in the field.

The ideal d splits up into a cube $(\delta)^3$ of a principal self-conjugate ideal (δ). Since E.A. holds we can find for each n an integer α in the field such that

$$n \equiv \alpha \pmod{\delta}, \quad |N(\alpha)| < |N(\delta)| = d.$$

† See Lemma 4 of paper referred to in the first footnote to p. 377.

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press

As the ideal (δ) is self-conjugate we have for each conjugate α' of α

$$n \equiv \alpha' \pmod{\delta},$$

and therefore $$n^3 \equiv N(\alpha) \pmod{\delta}, \quad n^3 \equiv N(\alpha) \pmod{d}.$$

We now fix n such that

$$n^3 \equiv a \pmod{d}, \quad N(\alpha) \equiv a \pmod{d}.$$

Since $$|N(\alpha)| < d,$$

this implies $$N(\alpha) = a \quad \text{or} \quad N(\alpha) = -a',$$

which is a contradiction.

APPENDIX

The principal theorem of class-field theory applied to cubic cyclic fields states†.

There is a one-one correspondence between cyclic cubic fields K and pairs of conjugate primitive cubic characters $\chi(n)$ and $\overline{\chi}(n) \pmod{d}$ such that:

(1) d^2 is the discriminant of the field K.

(2) Every rational prime divisor of d is the cube of a self-conjugate prime ideal in the field K.

(3) A prime p splits up into three different prime ideals if and only if $\chi(p) = \overline{\chi}(p) = 1$.

(4) All other rational primes remain primes in K.

It follows from (2), (3) and (4) that a rational integer

$$n = p_1^{l_1} \dots p_s^{l_s}$$

is norm of an ideal in K if and only if

$$\chi(p_j^{l_j}) \geqslant 0 \quad \text{for} \quad 1 \leqslant j \leqslant s.$$

Each primitive cubic character mod d is either a cubic character mod 9 or a cubic character mod p, where $p \equiv 1 \pmod{6}$, or the product of a finite number of distinct characters of this type.

Hence by (1) the discriminant of a cyclic cubic field K is either 81 or p^2, where $p \equiv 1 \pmod{6}$, or the product of a finite number of distinct factors of this type.

We now assume that

$$d = 9^u p_1 \dots p_{t-u}, \quad u = 0 \text{ or } 1, \quad t > 1,$$

so that the discriminant of K is divisible by t different primes. Let

$$3 < p = \mathfrak{p}^3$$

be such a divisor and α a number in K, not necessarily an integer (‡), which is prime to $\mathfrak{p}$. Then, since $\mathfrak{p}$ is a prime ideal of the first degree

$$\alpha \equiv a \pmod{\mathfrak{p}}$$

† We preserve the convention that small italics denote positive rational integers, but d need no longer be a prime. p continues to denote rational primes.

‡ We define $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{m}}$, if two integers β_1, β_2 exist such that $\beta_1 \equiv \beta_2 \equiv 1 \pmod{\mathfrak{m}}$ in the usual sense and $\alpha_1\beta_1 = \alpha_2\beta_2$. We call a number prime to d, if it is the quotient of two integers which are both prime to d.

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press

for some rational integer a, and since $\mathfrak{p}$ is self-conjugate we have for each conjugate α' of α

$$\alpha' \equiv a \pmod{\mathfrak{p}}, \quad N(\alpha) \equiv a^3 \pmod{\mathfrak{p}}, \quad N(\alpha) \equiv a^3 \pmod{p}.$$

Now let α be a number in K which is prime to d; then it follows that $N(\alpha)$ is a cubic residue mod d. We have already verified this for all prime divisors of d, and if $9/d$, it follows from (3) that $\chi(N(\alpha)) = 1$, and therefore $N(\alpha) \equiv \pm 1 \pmod{9}$.

In other words there are $3^{-t}\phi(d)$ residue classes mod d which contain the norms of all numbers in K which are prime to d. But by (3) and Dirichlet's theorem about the existence of primes in arithmetic progression it follows that there are exactly $\frac{1}{3}\phi(d)$ residue classes mod d, which contain the norm of an ideal in K prime to d. Hence, if we limit ourselves to ideals prime to d, the class group of K contains a subgroup of index 3^{t-1}, namely the group of all ideals whose norm is a cubic residue mod d.

Since each ideal class in K contains an ideal prime to d, it follows that the class group in the above-mentioned sense is isomorphic to the class group in the usual sense. This implies that 3^{t-1} divides the class number of K.

THE ROYAL FORT
BRISTOL 8

https://doi.org/10.1017/S0305004100025883 Published online by Cambridge University Press