Canadian Mathematical Society
Conference Proceedings
Volume 7 (1987)

THE EUCLIDEAN ALGORITHM FOR S-INTEGERS

Rajiv Gupta*, M. Ram Murty* and V. Kumar Murty*

1. INTRODUCTION. Let $m, n \in \mathbb{Z}$, $n \neq 0$. Following Euclid, there are $q, r \in \mathbb{Z}$ such that $m = qn + r$ with $r = 0$ or $0 < |r| < |n|$. The analogous assertion for number fields has received considerable attention over the years. To formulate it precisely, let K be a number field and S a finite set of places of K containing the infinite places S_∞. Let $\mathcal{O}_S$ denote the ring of S-integers of K (i.e., elements x of K with $\mathrm{ord}_\mathfrak{p} x \geq 0$ for all primes $\mathfrak{p}$ of K not in S).

DEFINITION. $\mathcal{O}_S$ is <u>Euclidean</u> if there is a function

$$\psi : \mathcal{O}_S - \{0\} \longrightarrow \mathbb{Z} \geq 0$$

such that for all $\alpha, \beta \in \mathcal{O}_S$, $\beta \neq 0$, there are $q, r \in \mathcal{O}_S$ satisfying

$$\alpha = q\beta + r$$

and $r = 0$ or $\psi(r) < \psi(\beta)$.

Such a function ψ will be called a <u>Euclidean algorithm</u> for $\mathcal{O}_S$. It is well known that if $\mathcal{O}_S$ is Euclidean, then it is a principal ideal domain. In general, the converse is false. For example, if we take $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ which is the ring of integers in $K = \mathbb{Q}(\sqrt{-19})$, then $\mathcal{O}$ is a principal ideal domain. (One easily checks this from the Minkowski bound [9, p. 119] and the fact that 2 and 3 remain prime in K). If ψ is a Euclidean algorithm for $\mathcal{O}$, take $\alpha_0 \in \mathcal{O}$ satisfying

$$\psi(\alpha_0) = \min \psi(\alpha)$$

where the minimum is over all $\alpha \in \mathcal{O}$ with $\psi(\alpha) \neq 0$. Thus, every residue class mod α_0 is represented by 0 or an element $\alpha \in \mathcal{O}$ with $\psi(\alpha) = 0$. Since $\psi(\alpha) = 0$ implies that α is a unit, we deduce that $N(\alpha_0) \leq 3$. By the fact stated above about 2 and 3, we get a contradiction. Note that in this example $|S| = |S_\infty| = 1$.

* Research partially supported by NSERC grants A8910, U0237 and U0373.

On the other hand, Lenstra [10] and Weinberger [19] have shown that if $\mathcal{O}_S$ is a principal ideal domain and $|S| \geq 2$, then the Riemann Hypothesis for all Dedekind zeta functions implies that $\mathcal{O}_S$ is Euclidean. Our main result here is to show that the assumption of the Riemann Hypothesis may be removed if we insist on a larger set S. More precisely, let us define

$$g \stackrel{df}{=} GCD\,[(N_{k/\mathbb{Q}}(\mathfrak{P}) - 1) : \mathfrak{P} \in S - S_\infty] .$$

THEOREM. Suppose that K is Galois over $\mathbb{Q}$ and that

a) $|S| \geq \max(5, 2[K:\mathbb{Q}]-3)$

b) K has a real embedding or $\zeta_g \in K$.

If $\mathcal{O}_S$ is a principal ideal domain, then it is Euclidean.

The idea of the proof is to combine a method used by the first two authors [4] in their work on the Artin primitive root conjecture with a result of the second two authors [15] on the Bombieri-Vinogradov theorem. We would like to heartily thank Lenstra for suggesting that the methods of [4] be developed in this direction.

The study of Euclidean rings of integers before the work of Lenstra and Weinberger proceeded along quite different lines, and in the next section we briefly review the history of the problem and recall the known results. In section 3, we give a technical lemma which is essential in our arguments. In section 4, we give the proof of the Theorem. In section 5, we return to the Artin primitive root conjecture and give a slight refinement of [4].*

Finally, we remark that where $\mathcal{O}_S$ is proved Euclidean by the Theorem, the algorithm provided is <u>not</u> the norm function. These are the first such examples.

2. A BRIEF HISTORY. The problem of deciding which rings $\mathcal{O}_S$ are Euclidean has been studied extensively, but mostly in the case $S = S_\infty$ and ϕ the norm function. We give a brief survey of known results, referring the reader to Samuel [18], Lenstra [10,11] and Narkiewicz [16] for further references. When $S = S_\infty$, we shall write $\mathcal{O}_K$ (or simply $\mathcal{O}$) for $\mathcal{O}_S$.

If $[K:\mathbb{Q}] = 2$, there are two cases to consider. If $K = Q(\sqrt{-d})$ is imaginary quadratic, $\mathcal{O}$ has class number 1 for

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Of these, $\mathcal{O}$ is Euclidean only for the first five, and in this case, the norm serves as an algorithm (cf. [18, Prop. 13]). If $K = \mathbb{Q}(\sqrt{d})$ is real quadratic,

* After this paper was written, we learned that R. Heath-Brown has made further refinements. See also M. Ram Murty and S. Srinivasan, "Some remarks on Artin's conjecture", to appear.

it is conjectured that $\mathcal{O}$ has class number 1 for infinitely many d. Heilbronn [6] showed, however, that the norm can be a Euclidean algorithm only for finitely many d. It is classical (cf. [5, ch. 14]) that the norm is an algorithm for the sixteen values

$$d = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73 \ .$$

Combining work of Hua, Davenport, Inkeri and Chatland, it is known that the above list is complete (see [16] for further references). Thus, $\mathbb{Z}[\sqrt{14}]$, for example, is not Euclidean for the norm.

Write $n_K = [K:\mathbb{Q}] = r+2s$, where r is the number of real embeddings and s is the number of non-conjugate complex embeddings of K. For $\mathcal{O}$ to be Euclidean for the norm means that given any $\alpha \in K^*$, there exists $\beta \in \mathcal{O}$ so that $N_{K/\mathbb{Q}}(\alpha - \beta) < 1$. The norm $N_{K/\mathbb{Q}}$ is a homogeneous form of degree n_K in n_K variables. Given a general homogeneous form (over $\mathbb{R}$) f of degree n in n variables, we define for each point $P \in \mathbb{R}^n$,

$$M(f,P) = \inf |f(Q)|$$

where the infimum is over all $Q \in \mathbb{R}^n$ so that $Q-P \in \mathbb{Z}^n$. We also set

$$M(f) = \sup M(f,P)$$

over all $P \in \mathbb{R}^n$. Then, $M(f)$ is called the inhomogeneous minimum of f. When f is the norm form, $\mathcal{O}$ is Euclidean if and only if $M(f) < 1$.

There is an extensive literature on estimates for $M(f)$, mostly in the case $n=2$. Cassels [1] showed that if $n \leq 4$ and f can be factored into linear forms with the number of factors (counting conjugate factors only once) at most 2, then

$$M(f) > \frac{|\Delta|}{\gamma}$$

where Δ is the discriminant of f, and $\gamma = 420$ if $n=3$, $\gamma = 5300$ if $n=4$. Applying this to f, the norm form, it follows that if $r+s \leq 2$, there are only finitely many K for which $\mathcal{O}$ is Euclidean for the norm.

Another technique for determining whether the norm is a Euclidean algorithm was developed by Lenstra [11]. He defines a constant

$$M = M(K) = \sup \{ m : \text{there exist } \alpha_1,\ldots,\alpha_m \in \mathcal{O} \text{ such that } \alpha_i - \alpha_j \text{ is a unit for } 1 \leq i < j \leq m \} \ .$$

If we have the bound

$$M > n! n^{-n} (4/\pi)^s |d_K|^{\frac{1}{2}}$$

where $n = n_K$ and d_K is the discriminant of K, then $\mathcal{O}$ is Euclidean for the norm. The proof uses ideas from packing theory. Let $U \subseteq \mathbb{R}^n$ be a bounded measurable set with positive Lebesgue measure $\mu(U)$. If $\{a_i\}$ is a

sequence of points in $\mathbb{R}^n$ which are "sufficiently well distributed", and $\mu(U)$ is sufficiently large then the system $\{U+a_i\}$ is not a packing of U in the sense that there are i,j with $i \neq j$ and $(U+a_i) \cap (U+a_j) \neq \phi$ (see [11] for a precise statement). Lenstra uses

$$U = \{(x_j) \in \mathbb{R}^n \times \mathbb{C}^s : \sum_{j=1}^{r} |x_j| + 2 \sum_{j=r+1}^{r+s} |x_j| < \tfrac{1}{2} n_K\} \quad .$$

This set has the property that for $u = (x_j)$, $v = (y_j) \in U$,

$$N(u-v) \overset{df}{=} \prod_{j=1}^{r} |x_j - y_j| \prod_{j=r+1}^{r+s} |x_j - y_j|^2 < 1 \quad .$$

Let $\alpha_1, \ldots, \alpha_M \in \mathcal{O}$ be such that the difference of any two is a unit, and for $x \in K^*$, consider the sequence $\{\alpha_i x + \alpha\}$ as α ranges over all of $\mathcal{O}$ and $1 \leq i \leq M$. The above bound on M is what is needed to guarantee that $(U+\alpha_i x+\alpha) \cap (U+\alpha_j x+\beta) \neq \phi$ for some $1 \leq i < j \leq M$ and $\alpha, \beta \in \mathcal{O}$. Then

$$x = \frac{\beta-\alpha}{\alpha_i-\alpha_j} + \frac{u-v}{\alpha_i-\alpha_j}$$

for some $u, v \in U$. As $(\alpha_i-\alpha_j)$ is a unit, $\gamma = (\beta-\alpha)/(\alpha_i-\alpha_j) \in \mathcal{O}$ and $N(x-\gamma) < 1$ by the choice of U. Using this method, Lenstra produces 132 examples of Euclidean fields (i.e., K for which $\mathcal{O}$ is Euclidean for the norm) with $4 \leq n_K \leq 8$.

Using a variety of methods, several authors have studied the case of cyclotomic fields $K = \mathbb{Q}(\zeta_m)$. It is known that $\mathbb{Q}(\zeta_m)$ has class number 1 for precisely the following thirty values of m (cf. Masley and Montgomery [13]):

$$m = 1,3,4,5,7,8,9,11,12,13,15,16,17,19,20,$$
$$21,24,25,27,28,32,33,35,36,40,44,45,48,60,84.$$

It is known that $\mathbb{Z}[\zeta_m]$ is Euclidean for the following values:

m	Reason
1, 3, 4	$\phi(m) \leq 2$
5, 7	Lenstra [11, §3.1]
8	Lakein [8]
9, 11, 12, 15	Lenstra (loc. cit.)
16, 20, 24	Ojala [17] .

Finally, we mention that variants of the Euclidean condition have been studied by Cooke [2] and applied by Cooke and Weinberger [3] to study the existence of division chains in number fields.

We return to consider the general case of $\mathcal{O}_S$. Define a sequence of sets

$$E_{-1} = \{0\}$$
$$E_0 = \{0\} \cup \mathcal{O}_S^*$$
$$n \geq 1 \qquad E_n = \{\alpha \in \mathcal{O}_K : \text{every residue class mod } \alpha\mathcal{O}_S \text{ has a representative in } E_{n-1}\} \cup E_{n-1} .$$

Then, Motzkin [14] proved that $\mathcal{O}_S$ is Euclidean if and only if

$$\mathcal{O}_S = \bigcup_{n \geq -1} E_n .$$

Moreover, when $\mathcal{O}_S$ is Euclidean, the function ψ given by

$$\psi(E_n - E_{n-1}) = n \quad (n \geq 0)$$

is a Euclidean algorithm. Motzkin also introduced the notion of a minimal algorithm. Precisely, if $\{\psi_\alpha\}$ is a family of algorithms, with α ranging over some indexing set A, then

$$\psi_A = \min_{\alpha \in A} \psi_\alpha$$

is also an algorithm. In particular, there is a "smallest" algorithm $\psi_{\min}$ (say). As Samuel [18] showed, this algorithm satisfies

$$\psi_{\min}(xy) \geq \psi_{\min}(x) + \psi_{\min}(y)$$

if $xy \neq 0$. (Notice that in particular, $\psi_{\min}(xy) \geq \psi_{\min}(x)$ if $y \neq 0$. In earlier works, this was sometimes imposed as an axiom to be satisfied by any algorithm. That the class of rings which are Euclidean is the same whether we include this axiom or not seems to be due to Veldkamp (cf. [16, p. 114])). It follows that for any $x \in \mathcal{O}_S - \{0\}$,

$$\psi_{\min}(x) \geq \sum_{\mathfrak{P} \notin S} \operatorname{ord}_{\mathfrak{P}}(x) \cdot \psi_{\min}(\pi)$$

where in the sum, π is a generator of $\mathfrak{P}$. Note that by the semi-additivity, $\psi_{\min}(\pi)$ does not depend on the choice of generator π. Define

$$n_{\mathfrak{P}} = \begin{cases} 1 & \text{if } \mathcal{O}_S^* \longrightarrow (\mathcal{O}_S/\mathfrak{P})^* \text{ is surjective} \\ 2 & \text{otherwise,} \end{cases}$$

and set

$$\theta(x) = \sum_{\mathfrak{P} \notin S} \operatorname{ord}_{\mathfrak{P}}(x) \cdot n_{\mathfrak{P}} .$$

Then certainly, $\psi_{\min} \geq \theta$. Samuel studied this function and was led to observe that the condition $n_{\mathfrak{P}} = 1$ was similar in spirit to Artin's primitive root conjecture.

This was formalized by Weinberger [19] and in a refined form by Lenstra [10], who showed the following.

THEOREM. Suppose that $|S| \geq 2$ and all Dedekind zeta functions satisfy the Riemann Hypothesis. Then $\mathcal{O}_S$ is a principal ideal domain if and only if

$\mathcal{O}_S$ is Euclidean. When $\mathcal{O}_S$ is Euclidean, θ is the minimal algorithm. As was observed in [10] and [19], the difficulty in proving that θ is an algorithm lies entirely at $\beta \in \mathcal{O}_S$ with $\theta(\beta) = 2$. Indeed, let $\alpha, \beta \in \mathcal{O}_S$, $\beta \neq 0$. We want to produce $q, r \in \mathcal{O}_S$ such that $\alpha = q\beta + r$ and $r = 0$ or $\theta(r) < \theta(\beta)$. By the additivity of θ, we may suppose that $(\alpha, \beta) = \mathcal{O}_S$. If $\theta(\beta) = 0$, then $\beta \in \mathcal{O}_S^*$ so $r = 0$. If $\theta(\beta) = 1$, then from the definition of θ, (β) is a prime ideal and $\mathcal{O}_S^*$ surjects on $\mathcal{O}_S/(\beta)$. Thus, we may choose $r = 0$ or an r with $\theta(r) = 0 < \theta(\beta)$. If $\theta(\beta) \geq 3$, then by Dirichlet's theorem on arithmetic progressions in number fields, every coprime residue class mod(β) contains a prime element π (say). Then $\theta(\pi) \leq 2 < \theta(\beta)$.

When $\theta(\beta) = 2$, we need $r \in \mathcal{O}_S$, $r \equiv \alpha \pmod{\beta}$ and $r \in \mathcal{O}_S^*$ or (r) is a prime ideal and $n_{(r)} = 1$. Let us write

$$\varphi : \mathcal{O}_S^* \longrightarrow (\mathcal{O}_S/\beta\,\mathcal{O}_S)^*$$

for the natural reduction map, and consider the S-ray class field F/K of conductor dividing $\beta\,\mathcal{O}_S$. Thus F is the maximal abelian extension of K whose conductor divides $\beta\,\mathcal{O}_S$ and in which every prime in S splits completely. Moreover, if $K \subseteq M \subseteq F$ and M/K is everywhere unramified, then $M = K$. Such an extension exists and is unique by class field theory, and we have

$$\mathrm{Gal}(F/K) \simeq (\mathcal{O}_S/\beta\,\mathcal{O}_S)^*/\varphi(\mathcal{O}_S^*) .$$

We denote by C the element in $\mathrm{Gal}(F/K)$ corresponding to $\alpha \pmod{\beta}$ under the above isomorphism. The existence of r as above is equivalent to the existence of a prime ideal $\mathfrak{P}$ of K satisfying

$$(\mathfrak{P}, F/K) = C$$
$$n_{\mathfrak{P}} = 1$$

where $(\ ,\ )$ denotes the Artin symbol. We discuss the existence of such primes in section 4. In the next section, we give a technical lemma which is crucial in what follows.

3. A TECHNICAL LEMMA. We will require some notation. Let E_1/E_2 be a Galois extension and D a subset of $\mathrm{Gal}(E_1/E_2)$ stable under conjugation (a conjugacy subset for short). We define

$$d = d(E_1/E_2, D)$$

to be the largest integer such that $\mathbb{Q}(\zeta_d) \subseteq E_1$ and $D\big|_{\mathbb{Q}(\zeta_d)} = 1$. Let $E/\mathbb{Q}$ be a Galois extension with group G, and C any conjugacy class of G. We define

$$\eta^*(C) = \min_H \max_\omega \frac{|H|}{|H|}\omega(1)$$

where the minimum is over subgroups $H \subseteq G$ satisfying

(i) $H \cap C \neq \emptyset$

(ii) for every non-trivial irreducible character ω of H with $\omega|_{H\cap C} \neq 0$, and every Dirichlet character χ, the Artin L-series $L(s,\omega \otimes \chi)$ is entire,

and the maximum is taken over irreducible non-trivial characters ω of H with $\omega|_{H\cap C} \neq 0$. We also define

$$\eta = \eta(C) = \max(4, 2\eta^*(C)-2) .$$

We can now state the technical lemma.

LEMMA. Let $\epsilon > 0$. There is a constant $\delta_1 > 0$ and $\geq \delta_1 x(\log x)^{-2}$ primes $p \leq x$, satisfying

(i) $(p,E/\mathbb{Q}) \subset C$

(ii) $t \mid (p-1)$, t prime $\Longrightarrow t \mid d(E/\mathbb{Q},C)$ or $t > p^{(1/\eta)-\epsilon}$.

PROOF. This follows from the lower bound sieve method using the twisted Bombieri-Vinogradov theorem of [15, Theorem 7.3].

4. PROOF OF THE THEOREM. We recall our assumptions:

(a) $|S| \geq \max(5, 2n_K-3)$

(b) either K has a real embedding or $\zeta_g \in K$ where $g = \mathrm{GCD}(N_{K/\mathbb{Q}}\mathfrak{P}-1 : \mathfrak{P} \in S-S_\infty)$.

By the discussion of section 2, it suffices to prove the following result Let $\beta \in \mathcal{O}_S$ with $\theta(\beta) = 2$. Let F/K denote the S-ray class field of conductor $\beta\mathcal{O}_S$, and fix $1 \neq C \in \mathrm{Gal}(F/K)$.

PROPOSITION. There are infinitely many primes $\mathfrak{P}$ of K satisfying $(\mathfrak{P},F/K) = C$ and $n_\mathfrak{P} = 1$.

The proof will require several lemmas. For any prime ℓ, let L_ℓ denote the Kummer extension of K obtained by adjoining the ℓ-th roots of all elements of $\mathcal{O}_S^*$. (In particular, $\zeta_\ell \in L_\ell$). Let L denote the compositum $F\prod L_\ell$, the product taken over prime divisors ℓ of $d(F/K,C)$, and set

$$C' = [\sigma \in \mathrm{Gal}(L/K) : \sigma|_F = C \text{ and } \sigma|_{L_\ell} \neq 1 \text{ for } \ell \mid d(F/K,C)] .$$

By Lenstra [10, pp. 221-223], C' is not empty.

LEMMA 1. $d(L/K,C') = d(F/K,C)$.

PROOF. First, we note that if $\ell \mid d(F/K,C)$, then $\zeta_\ell \in K$. Indeed, $F \supseteq K(\zeta_\ell) \supseteq K$ and so every prime in S splits completely in $K(\zeta_\ell)$. If K has a real embedding, this forces $\ell = 2$ so $\zeta_\ell \in K$. Otherwise, $\ell \mid g$ and so (b) above implies $\zeta_\ell \in K$ in this case also. From this, it follows that L/K is abelian. Now take a prime t dividing $d(L/K,C')$. If $K(\zeta_t)$ is contained in F, then t divides $d(F/K,C)$ also. So suppose $\zeta_t \notin F$. Let $H = \mathrm{Gal}(L/F)$, $J = \mathrm{Gal}(L/K(\zeta_t))$ and for each $\ell \mid d(F/K,C)$, set $H_\ell = \mathrm{Gal}(L/L_\ell)$. Since

$$\sigma_0 H - \bigcup_{\ell \mid d} (\sigma_0 H \cap H_\ell) \subseteq C' \subseteq J \cap \sigma_0 H$$

(for some fixed σ_0 in C'), we have

$$(*) \qquad |H| - \sum_{\ell \mid d} |H \cap H_\ell| \leq |J \cap \rho_0 H| \leq \tfrac{1}{2}|H| \quad .$$

Now,

$$|H \cap H_\ell| = |\mathrm{Gal}(L/L_\ell F)| = |H| / |\mathrm{Gal}(L_\ell/(L_\ell \cap F))| \quad .$$

Note that L_ℓ/K is of degree a power of ℓ and is ramified at most at primes dividing ℓ and at the primes in S. On the other hand, there are no extensions intermediate between F and K which are everywhere unramified over K. Now, suppose that $L_\ell \cap F \neq K$. Then, there is a prime $\mathfrak{L}$ of K dividing ℓ with

$$\mathfrak{L} \notin S, \quad n_{\mathfrak{L}} = 1 \quad \text{and} \quad \mathfrak{B}\, \mathcal{O}_S = \mathfrak{L}^2 \quad .$$

We use an argument of Lenstra [10, p. 222] to deduce that $F \subseteq L_\ell$. Briefly, since $n_{\mathfrak{L}} = 1$, and $\mathrm{Gal}(F/K) \simeq (\mathcal{O}_S/\mathfrak{B}\,\mathcal{O}_S)^*/\varphi(\mathcal{O}_S^*)$, $[F:K]$ is a power of ℓ and so, by Kummer theory, $F = K(x_1^{1/\ell}, \ldots, x_s^{1/\ell})$ for some $x_i \in K^*$, $x_i \in K^{*\ell}$ and $1 \leq s \in \mathbb{Z}$. Since F is unramified outside $\mathfrak{L}$, we have $\mathrm{ord}_{\mathfrak{P}} x_i \equiv 0 \pmod{\ell}$ for all $\mathfrak{P} \neq \mathfrak{L}$. As $\mathcal{O}_S$ is a principal ideal domain, we can adjust the x_i by ℓ-th powers so that $\mathrm{ord}_{\mathfrak{P}} x_i = 0$ for all $\mathfrak{P} \notin S \cup \{\mathfrak{L}\}$. By a local discriminant calculation and the fact that the conductor of F/K divides $\mathfrak{L}^2$, we can also ensure that $\mathrm{ord}_{\mathfrak{L}} x_i = 0$. Hence, $x_i \in \mathcal{O}_S^*$ so that $F \subseteq L_\ell$.

Hence, we deduce that in any case,

$$|\mathrm{Gal}(L_\ell/(L_\ell \cap F))| \geq [L_\ell:K]/[F:K] \geq \ell^r / N_{K/\mathbb{Q}}\,\mathfrak{L} \geq \ell^{r-n_K} \quad .$$

Thus, $|H \cap H_\ell| \leq |H|/\ell^{r-n_K}$. Using this in (*), we find

$$\tfrac{1}{2} \leq \sum_{\ell \mid d} \frac{1}{\ell^{r-n_K}} \leq \sum_{\ell=2}^{\infty} \ell^{n_K - r}$$

$$\leq (r-n_K-1)^{-1}$$

which contradicts (a). Thus $\zeta_t \in F$ and t divides $d(F/K,C)$. On the other hand, we clearly have $d(F/K,C) \mid d(L/K,C')$. This proves the lemma.

Now let $\tilde{L}$ denote the normal closure of L over $\mathbb{Q}$. Let C'' denote the inverse image of C' in $\mathrm{Gal}(\tilde{L}/K)$ and let $C^* = \cup g^{-1}C''g$ where g ranges over $\mathrm{Gal}(\tilde{L}/\mathbb{Q})$.

LEMMA 2. $d(\tilde{L}/\mathbb{Q},C^*) = d(L/K,C')$.

PROOF. Clearly, $d(\tilde{L}/\mathbb{Q},C^*) = d(L/K,C')$. Now suppose that t is a prime divisor of $d(\tilde{L}/K,C'')$. Then $C'\big|_{K(\zeta_t)\cap L} = C''\big|_{K(\zeta_t)\cap L} = 1$. If $K(\zeta_t) \neq K(\zeta_t)\cap L$, then there exist primes $\mathfrak{P}$ of K such that $\mathfrak{P}$ does not split completely in $K(\zeta_t)$ and $(\mathfrak{P},L/K) \subset C'$. The latter is equivalent to the condition $(\mathfrak{P},\tilde{L}/K) \subset C''$. This contradicts $t \mid d(\tilde{L}/K,C'')$. Hence, $K(\zeta_t)$ is contained in L and $C'\big|_{K(\zeta_t)} = 1$. Thus, t divides $d(L/K,C')$. Conversely, it is easily seen that $d(L/K,C')$ divides $d(\tilde{L}/K,C'')$. This proves the lemma.

LEMMA 3. Let $n = \max(4, 2n_K - 4)$. There is a constant $\delta_2 > 0$ and $\geq \delta_2 x/(\log x)^2$ primes $\mathfrak{P}$ of K satisfying

(i) $N_{K/\mathbb{Q}}(\mathfrak{P}) = p \leq x$

(ii) $(\mathfrak{P},F/K) = C$

(iii) $(\mathfrak{P},L_\ell/K) \neq 1$ for each ℓ dividing $d(F/K,C)$

(iv) $t \mid (p-1)$, t prime $\Longrightarrow t \mid d(F/K,C)$ or $t > p^{(1/n)-\epsilon}$.

PROOF. For any prime p which is unramified in $\tilde{L}$ that satisfies $(p,\tilde{L}/\mathbb{Q}) \subset C^*$, take a prime $\mathfrak{B} \mid p$ in $\tilde{L}$. Then, for some g in $\mathrm{Gal}(\tilde{L}/\mathbb{Q})$, $(\mathfrak{B}^g,\tilde{L}/\mathbb{Q})$ lies in C'' and hence in $\mathrm{Gal}(\tilde{L}/K)$. If $\mathfrak{P}$ is a prime of K below $\mathfrak{B}^g$, then $\mathfrak{P}$ is of degree 1 and $(\mathfrak{P},L/K) \subset C'$. Thus, such a $\mathfrak{P}$ satisfies (i)-(iii).

Now, we recall that L/K is abelian, by our assumption (b). Also, as $K/\mathbb{Q}$ is Galois, it follows that $\tilde{L}$ is also abelian over K. Moreover, the characteristic function of C^* can be written as a linear combination of inductions of (abelian) characters of $\mathrm{Gal}(\tilde{L}/K)$. In the notation of section 3, $\eta^*(D) \leq n_K$ for any conjugacy class D in C^*, and $\eta(D) \leq n$ (as we see by taking $H = \mathrm{Gal}(\tilde{L}/K)$). Now, the lemma of section 3 shows that there are $\gg x/(\log x)^2$ primes $p < x$ satisfying $(p,L/\mathbb{Q}) \subset C^*$ and

$$t \mid (p-1),\ t \text{ prime} \Longrightarrow t \mid d(\tilde{L}/\mathbb{Q},C^*) \text{ or } t > p^{(1/n)-\epsilon}.$$

By Lemmas 1 and 2, $d(\tilde{L}/\mathbb{Q},C^*) = d(F/K,C)$. This proves the lemma.

For any prime $\mathfrak{P}$ of K, we denote by $k(\mathfrak{P})$ the residue field mod $\mathfrak{P}$. If $\mathfrak{P} \notin S$, we also define the map $\varphi_{\mathfrak{P}} : \mathcal{O}_S^* \longrightarrow k(\mathfrak{P})^*$ which is reduction mod $\mathfrak{P}$.

LEMMA 4. Let $s = |S| - 1$. Then, the number of primes $\mathfrak{P}$ of K for which $|\varphi_{\mathfrak{P}}(\mathcal{O}_S^*)| < y$ is $\ll y^{(s+1)/s}$.

PROOF. This is proved in exactly the same way as Lemma 2 or [4]. We have only to note that the rank of $\mathcal{O}_S^*$ is s and that if $\beta \in K$, then $\beta^b - 1$ has $\underline{O}(b)$ prime divisors (counted with multiplicity). Here, the implied constant depends on β and on $[K:\mathbb{Q}]$.

PROOF OF THE PROPOSITION. We consider the primes $\mathfrak{P}$ of K satisfying conditions (i)-(iv) of Lemma 3. For such a prime, we have that either $|\varphi_{\mathfrak{P}}(\mathcal{O}_S^*)| < p^{(n-1)/n+\epsilon}$ or all prime divisors of the index $[k(\mathfrak{P})^* : \varphi_{\mathfrak{P}}(\mathcal{O}_S^*)]$ divide $d(F/K,C)$. By Lemma 4, the number of $\mathfrak{P}$ with $N_{K/\mathbb{Q}}\mathfrak{P} \leq x$ satisfying the first condition is $\ll x^{1-\epsilon}$ as $s \geq n$. Thus, we can discard those primes. Also, a prime ℓ divides the index $[k(\mathfrak{P})^* : \varphi_{\mathfrak{P}}(\mathcal{O}_S^*)]$ if and only if $\mathfrak{P}$ splits completely in L_ℓ. But this contradicts (iii) of Lemma 3. Hence, the index must be 1 and this proves the result.

5. PRIMITIVE ROOTS. Let q, r, s be three distinct integers such that $\omega(q)$, $\omega(r)$ and $\omega(s)$ are odd and such that the group $\Gamma = [q^a r^b s^c : a,b,c \in \mathbb{Z}]$ has rank 3. (Here ω denotes the total number of prime divisors.) By the method of proof of Lemma 3, we find that there are at least $\gg x/(\log x)^2$ primes $p \leq x$ satisfying

(i) $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$

(ii) $\varphi_p(\Gamma) = \mathbb{F}_p^*$

(iii) $t \mid (p-1)$, t prime $\Longrightarrow t = 2$ or $t > p^{\frac{1}{4}+\epsilon}$.

We refine the result of [4].

THEOREM. There is a constant $\delta_1 > 0$ such that one of the numbers of the set

$$\{q, r, s, q^2r, qr^2, q^2s, qs^2\}$$

is a primitive root for $> \delta_1 x/(\log x)^2$ of the primes p x.

PROOF. Let T denote the set of primes p satisfying (i)-(iii). Let $\langle q \rangle$ denote the subgroup of $\mathbb{F}_p^*$ generated by q, and let d denote its order. We note that

$$\#\{p<x : p \text{ prime}, d<y\} \leq \Sigma\omega(q^b-1) \leq \Sigma b\log q \ll y^2 .$$

The implied constant of course depends on q. If we choose $y = x^{1/2}/(\log x)^{1+\epsilon}$, we see that by throwing out $o(x/(\log x)^2)$ of the $p < x$, we may assume that $d > p^{1/2}/(\log p)^{1+\epsilon}$ for all $p \in T$. We know that d is even by (ii). This and (i) implies that

$$\omega(d) \leq \omega(p-1) < \omega(d) + 1 .$$

If $\omega(p-1) = \omega(d)$, then $\langle q\rangle = \mathbb{F}_p^*$, so suppose $p-1 = dt$, t prime. Write d' for the order of the subgroup $\langle q,r\rangle$ of $\mathbb{F}_p^*$ generated by q and r. Write d'' for the order of $\langle q,s\rangle$. Then $d', d'' \equiv 0 (\text{mod } d)$, i.e., $d', d'' = d$ or dt. If either of d' or d'' is equal to dt, this means $\langle q,r\rangle$ or $\langle q,s\rangle = \mathbb{F}_p^*$. If $d' = d'' = d$, this means $\langle q\rangle = \langle q,r,s\rangle = \mathbb{F}_p^*$ contradicting $p-1 = dt$. Suppose now that $\langle q,r\rangle = \mathbb{F}_p^*$. Then, one of $\{r, q^2r, qr^2\}$ is a primitive root. Indeed, let g be a primitive root mod p. Say $q = g^a$, $r = g^b$ (mod p). Because of (ii), the elements of $S = \{b, 2a+b, a+2b\}$ are all odd. Also, $(p-1, ab) = 1$ and $t \mid a$, so t does not divide any element of S. Moreover the vectors $(1,0), (1,2)$ and $(2,1)$ are pairwise linearly independent modulo any prime larger than 3. Hence, any other odd prime divisor t' of $(p-1)$ divides at most one element of S, for p sufficiently large. We conclude that at least one element of S is relatively prime to $p-1$, as required.

REMARKS. 1) The lower bound $x/(\log x)^2$ can be improved to $x(\log\log\log x)/(\log x)^2$ by allowing $p-1$ to have prime divisors $< \log\log p$. To ensure that these primes do not appear in the index $[\mathbb{F}_p^* : \varphi_p(\Gamma)]$, we have to replace (ii) by the condition that p does not split completely in any of the Kummer extensions $\mathbb{Q}(\zeta_\ell, q^{1/\ell})$ for $\ell < \log\log x$. This number is estimated using the effective Chebotarev density theorem.

2) The proof also shows that for infinitely many primes p, two of q, r, s are sufficient to generate $\mathbb{F}_p^*$.

3) It is possible to produce a set of 7 elements directly by the methods of [4]. Indeed, by the same reasoning, there are at least $\delta_1 x/(\log x)^2$ primes $p \leq x$ satisfying (i)-(iii) above. Consider any such prime. If g is a primitive root mod p, then

$$q = g^\alpha , \quad r = g^\beta , \quad s = g^\gamma \quad (\text{mod } p)$$

where $(p-1, \alpha, \beta, \gamma) = 1$ and because of (ii), α, β, γ are all odd. Now if $v = (v_1, v_2, v_3) \in \mathbb{Z}^3$, $v_i \geq 0$, then $(q,r,s)^v = q^{v_1} r^{v_2} s^{v_3}$ is a primitive root mod p if and only if $(p-1, \lambda, v) = 1$ where $\lambda = (\alpha, \beta, \gamma)$. Consider

$$\tilde{S} = \{(1,2,0), (2,1,0), (1,0,2), (2,0,1), (0,1,2), (0,2,1), (1,2,2)\} .$$

Using, for example, cross products, it is easy to check that any three elements of S are linearly independent. Thus, if the odd prime divisors of $(p-1)$ are sufficiently large, then for each odd prime t dividing $(p-1)$, at most two of $\{\lambda.v, v \in \tilde{S}\}$ are divisible by t (as $\lambda \not\equiv 0 \pmod{t}$). As $p-1$ has at most three odd prime divisors, for some $v_0 \in S$, $\lambda.v_0$ is not divisible by any odd prime dividing $p-1$. But $\lambda.v$ is odd for any $v \in S$ and so $(p-1, \lambda.v_0) = 1$ as desired. This proves that one of

$$\{qr^2, q^2r, qs^2, q^2s, rs^2, r^2s, qr^2s^2\}$$

is a primitive root (mod p) for at least $\gg x(\log x)^{-2}$ primes $p \leq x$.

4) Replacing condition (ii) by the condition $(\frac{q}{p}) = -1$ yields the result that one of the set

$$\{qr^2, qs^4, qr^2s^2, qr^4s^2, q^3r^2, q^3s^2, q^3r^2s^2\}$$

is a primitive root (mod p) for $\geq \delta\, x/(\log x)^2$ primes $p \leq x$. This is true for any three integers q, r, s such that q is not a square and q, r, s generate a subgroup of $\mathbb{Q}^*$ of rank 3.

5) The above method has an interesting corollary. One can deduce that almost all elements of the form $q^a r^b s^c$ are primitive roots. To be more precise, let q, r, s be as before. Then there is a $\delta > 0$ such that the number of elements of

$$\{q^a r^b s^c : 0 \leq a, b, c \leq N,\ (a, b, c) \not\equiv (0, 0, 0) \bmod 2\}$$

which are not primitive roots (mod p) for at least $\delta\, x/(\log x)^2$ of the primes $p \leq x$ is $O(N^2)$.

To see this let $u \in \mathbb{F}_2^3 - \{0\}$, and set

$$S_N^u = \{(a, b, c) \in \mathbb{Z}^3 : 0 \leq a, b, c \leq N,\ (a, b, c) \equiv u \pmod 2\}.$$

By replacing (ii) by the condition $(q/p) = -1$, we can get at least $\delta_1 x/(\log x)^2$ primes $p \leq x$ such that for any seven 3-wise linearly independent elements of S_N^u, at least one gives a primitive root mod p. Let M be the minimum number of 3-wise linearly independent elements $v_1, \ldots, v_M$ of S_N^u such that for each $1 \leq i \leq M$, the number of primes $p \leq x$ for which $(q, r, s)^{v_i}$ is a primitive root (mod p) is $\leq \delta_1 x/(\log x)^2$. Then $M \leq 6$. Suppose $v \in S_N^u$ is such that $(q, r, s)^v$ is a primitive root mod p for $< \delta_1 x/(\log x)^2$ primes $p \leq x$. Then v must be in the span of $\{v_i, v_j\}$ for some i, j with $1 \leq i, j \leq M$, and the number of such v is at most

$$\binom{M}{2}\left[\frac{N+1}{2}\right]^2 \leq 15\left[\frac{N+1}{2}\right]^2.$$

Letting u range over the seven elements of $\mathbb{F}_2^3 - \{0\}$, we get at most $105(N+1)^2/4$ exceptions as claimed. It is thus clear that there is an infinite variation on the seven numbers formed with q, r, s.

REFERENCES

1. J.W.S. Cassels, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, Proc. Camb. Phil. Soc. 48 (1952) 72-86, 519-520.
2. G. Cooke, A weakening of the Euclidean property for integral domains and applications to algebraic number theory, I, II, J. Reine und Angew. Math. 282 (1976) 133-156, 283/284 (1976) 71-85.
3. G. Cooke and P. Weinberger, On the construction of division chains in algebraic number fields with applications to SL_2, Comm. Alg. 3 (1975) 481-524.
4. R.Gupta and M. Ram Murty, A remark on Artin's conjecture, Inv. Math. 78 (1984) 127-130.
5. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 5th ed., Oxford University Press, Oxford, 1979.
6. H. Heilbronn, On Euclid's algorithm in real quadratic fields, Proc. Camb. Phil. Soc. 34 (1938) 521-526.
7. H. Iwaniec, Rosser's sieve, Acta Arith. 36 (1980) 174-202.
8. R. B. Lakein, Euclid's algorithm in complex quartic fields, Acta Arith. 20 (1972) 393-400.
9. S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, 1970.
10. H.W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields, Inv. Math. 42 (1977) 201-224.
11. H.W. Lenstra, Jr., Euclidean number fields of large degree, Inv. Math. 38 (1977) 237-254.
12. H.W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, J. London Math. Soc. 10 (1975) 457-465.
13. J. Masley and H. Montgomery, Cyclotomic fields with unique factorization, J. Reine und Angew. Math. 286/287 (1976) 248-256.
14. Th. Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55 (1949) 1142-1146.
15. M. Ram Murty and V. Kumar Murty, A variant of the Bombieri-Vinogradov Theorem, these proceedings.
16. W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Polish Scientific Publishers, Warszawa, 1974.
17. T. Ojala, Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$, Math. Comp. 31 (1977) 268-273.
18. P. Samuel, About Euclidean rings, J. Algebra 19 (1971) 282-301.
19. P. Weinberger, On Euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (1973) 321-332.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER

DEPARTMENT OF MATHEMATICS, McGILL UNIVERSITY, MONTREAL

DEPARTMENT OF MATHEMATICS, CONCORDIA UNIVERSITY, MONTREAL