J. reine angew. Math. **459** (1995), 151—162

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1995

The Euclidean algorithm for Galois extensions of $\mathbb{Q}$

By *David A. Clark* at Montréal and Essen, and *M. Ram Murty* at Montréal

A Euclidean algorithm for an integral domain R is a map

$$\phi : R\backslash\{0\} \to \mathbb{N}_0,$$

the set of nonnegative integers, such that for all a, $b \in R$, $b \neq 0$, there exist q, $r \in R$ with $a = qb + r$ and either $\phi(r) < \phi(b)$ or $r = 0$. One important property of integral domains satisfying this condition is that all their ideals are principal. An integral domain equipped with a Euclidean algorithm is called a Euclidean domain. Often we shall say that a field is Euclidean if its ring of integers is a Euclidean domain. For algebraic number fields the Euclidean algorithm that has usually been studied is the absolute value of the norm. We will refer to such fields as being norm-Euclidean.

Introduction

Dedekind showed in Supplement XI to Dirichlet's *Vorlesungen über Zahlentheorie* that $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean for $d = -1, -2, -3, -7, -11, 2, 3, 5, 13$. He also noted that while the ring of integers of $\mathbb{Q}(\sqrt{-19})$ is a principal ideal domain it is not Euclidean for the norm (this is also true for $d = -43$, -67, and -163). Hasse [5] asked if it is possible to define Euclidean algorithms other than the norm when the ring of integers is a principal ideal domain. Motzkin [9] showed that the ring of integers of $\mathbb{Q}(\sqrt{-19})$ is not Euclidean for any algorithm, thus giving a negative answer to this question in general. Previously, no examples of rings of integers of algebraic number fields were known which were Euclidean but not norm-Euclidean.

Motzkin [9] constructed a special kind of Euclidean algorithm. Given a nonempty collection of Euclidean algorithms ϕ_α on R, the map defined by

$$\phi(r) = \min_\alpha \phi_\alpha(r)$$

is also a Euclidean algorithm on R. To check this, let $a, b \in R$, $b \neq 0$. Choose an α_1 such that $\phi(b) = \phi_{\alpha_1}(b)$. Since

$$\phi(r) \leqq \phi_{\alpha_1}(r) < \phi_{\alpha_1}(b) = \phi(b),$$

ϕ is Euclidean. If the minimum is taken over all the Euclidean algorithms of the ring R, the resulting algorithm E is called the minimal algorithm.

Let $E_n = \{0\} \cup \{r \in R : E(r) \leqq n\}$. One can show that E_0 is the set consisting of 0 and the units of R. If $b \in E_{n+1}$ and $a + Rb$ is any reside class mod Rb, then there exist $q, r \in R$ with $a = qb + r$ and $E(r) < E(b)$ so that $r \in E_n$. Thus, $E_n \to R/Rb$ is surjective. Conversely, consider $b \in R$ such that $E_n \to R/Rb$ is surjective. If $E(b) > n + 1$ then a new map E' could be defined by $E'(r) = E(r)$, for $r \neq b$ and $E'(b) = n + 1$. To see that E' is an algorithm it suffices to consider the cases when b occurs as either a divisor or a remainder. Since $E_n \to R/Rb$ is surjective, every residue class $a + Rb$ has a representative such that $a = qb + r, r \in E_n$ which implies $E'(r) < n + 1 = E'(b)$. If $a = qc + b$ with $E(b) < E(c)$, then trivially $E'(b) < E(b) < E(c) = E'(c)$.

The importance of the sets E_n is that they can be constructed in any ring. If

$$R' = \bigcup_{n \geqq 0} E_n = R, \tag{1}$$

then R is Euclidean with algorithm defined by

$$\phi(r) = \min\{n : r \in E_n\}.$$

On the other hand, if R is Euclidean then every element of R is in some E_n. So the condition (1) is necessary and sufficient for R to be a Euclidean domain. Now it is easy to see why $\mathbb{Q}(\sqrt{-19})$ is not Euclidean for any algorithm, the only units are ± 1 and every nontrivial ideal has norm greater than 4 so the construction of the sets E_n stops at E_0. The same proof works for the other three cases noted above.

Samuel [11] noted a similarity between the success of the construction of the minimal algorithm and Artin's Primitive Root Conjecture. Namely, if there are infinitely many primes π such that a unit is a primitive root modulo π, then E_1 contains these primes. In particular, Samuel asked whether $\mathbb{Q}(\sqrt{14})$ is Euclidean for some algorithm other than the norm. ($\mathbb{Q}(\sqrt{14})$ is not Euclidean for the norm.)

Weinberger [12] made the connection with Artin's conjecture more precise and showed how the conditional proof of Artin's conjecture by Hooley [6] could be modified to show that under the assumption of the Generalized Riemann Hypothesis for Dedekind zeta functions (GRH), the ring of integers of an algebraic number field with at least one fundamental unit is Euclidean if and only if it is a principal ideal domain. That is, assuming the GRH, if K is an algebraic number field which is not an imaginary quadratic field and the ring of integers is a principal ideal domain, then it is a Euclidean domain. Thus, conjecturally, Hasse's question can be answered affirmatively, with only the four exceptions noted above. Lenstra [8] generalized this result to rings of S-integers, $|S| \geqq 2$, where S is a set of primes containing the infinite primes. R. Gupta, K. Murty, and R. Murty [4] removed the dependence on the Generalized Riemann Hypothesis from Lenstra's result for large enough $|S|$.

Statement of the Theorem

In this paper we prove the following result.

Theorem. *Let R be a principal ideal domain whose quotient field K is a totally real Galois extension of $\mathbb{Q}$ of degree n_K. Suppose that a collection S of $m = |n_K - 4| + 1$ non-associate prime elements $\pi_1, \pi_2, \dots, \pi_m$ of R can be found so that for all nonnegative integers a_i, $i = 1, \dots, m$, the unit group of R maps onto $(R/(\pi_1^{a_1} \cdots \pi_m^{a_m}))^*$, then R is a Euclidean domain.*

Since the unit group is the product of n_K cyclic groups, one expects to be able to find n_K prime elements π_i, $i = 1, \dots, n_K$ satisfying the condition stated in the theorem. Hence, this theorem should apply to rings such that $n_K \geqq 3$.

In the special case of totally real quartic Galois fields, to show that the ring of integers is a Euclidean domain requires only the existence of a single prime element π such that the unit group maps onto $(R/(\pi^m))^*$ for all nonnegative integers m. This case was treated in detail by Clark [3]. Call these prime elements Wieferich primes. We conjecture, by analogy to Artin's Primitive Root Conjecture, that there is a positive density of Wieferich primes. Computations support the validity of this conjecture.

In Clark [3], Wieferich primes were found in each of the 165 totally real quartic Galois fields of class number one with discriminant less than one million, which were determined by Buchmann, Ford, Pohst, and von Schmettow [1], [2], and the required primes were also found for the real cubic Galois fields with discriminant less than 500,000 with class number one. Some examples will be given in the last section.

Proof of the Theorem

Let S be a set of prime elements of K. In analogy to the minimal algorithm, we define the S-minimal algorithm as follows. Let U_S be the multiplicative monoid generated by the units and the prime elements in S. Define sets E_n^S inductively as follows,

$$E_0^S = \{0\} \cup U_S, \quad \text{and} \quad E_{n+1}^S = E_n^S \cup \{a : E_n^S \to R/(a) \text{ is onto}\}\,.$$

Define the S-minimal algorithm as we did earlier for the minimal algorithm. In general, the S-minimal algorithm is not a Euclidean algorithm. However we have:

Lemma 1. *If each prime element of R is contained in E_2^S, and if, for each $u \in U_S$, the units map onto the prime residue class group $(R/uR)^*$, then R is a Euclidean domain.*

Proof. (i) $E_0^S \subseteqq R'$: For $a \in U_S$, let $v(a)$ denote the sum of the exponents in the prime factorization of a. Then $v(a) = 0$ iff a is a unit, in which case clearly $a \in R'$. Otherwise we proceed by induction on $v(a) = n > 0$. By hypothesis, each $a' \in U_S$ satisfying $v(a') < n$ is in R'. Consider an arbitrary residue class $b + aR$ modulo a; we need to show that it contains an element of R'. This is clear for the class $0 + aR$ and for the invertible residue classes, each of which contains a unit of R by assumption. In the remaining case, $d = \gcd(a, b)$ (it does not matter which of the pairwise associate greatest common divisors is selected) lies in U_S

and satisfies $0 < v(d) < v(a)$, and the invertible residue class $(b/d) + (a/d)R$ modulo $a/d \in U_S$ contains a unit u; therefore $b + aR = du + aR$ with $du \in R'$ by the inductive hypothesis.

(ii) The difference set $E_1^S \backslash E_0^S$ consists of prime elements: For any element a of this set, the nonzero residue classes mod a form a multiplicative monoid which is an epimorphic image of U_S.

(iii) All the primes of R are contained in R': This is clear for the primes $\pi \in S$; for $\pi \in E_1^S \backslash E_0^S$ it follows from (i) and (ii), and any prime not in E_1^S is in E_2^S by assumption and thus has all its residue classes represented by elements of E_1^S, but we know at this point that $E_1^S \subseteqq R'$.

Now let $v(a)$, for arbitrary nonzero $a \in R$, denote the sum of the exponents of primes $\pi \in S$ in the factorization of a (as above), and $v'(a)$ and $v''(a)$ the sums of the exponents of the prime factors in $E_1^S \backslash E_0^S$ and in $E_1^S \backslash E_1^S$, respectively; furthermore, put $w(a) = v'(a) + v''(a)$. The remainder of the proof proceeds by induction on the lexicographically ordered triples $(w(a), v(a), v''(a))$.

(iv) Assume contrary to the assertion of the lemma that $R \backslash R'$ is nonempty. Select those of its members for which $w(a)$ is minimal, pass to the subset of this set for which $v(a)$ is minimal, and pick from the latter subset an element a for which $v''(a)$ is minimal. If every residue class mod a had a representative in R', then a would be in R'; therefore we can pick a residue class $b + aR$ which does not intersect R'. By (iii), this class contains no prime elements, and obviously it is not the zero class. Nor can it be an invertible class – these contain primes by the Čebotarev density theorem. Put again $d = \gcd(a, b)$; we then have $v(d) \leqq v(a)$, $w(d) \leqq w(a)$ and even $0 < v(d) + w(d) < v(a) + w(a)$. Decompose $a = da'$ and $b = db'$, then a' and b' are coprime.

If now $w(a') = 0$, i.e. $a' \in U_S$, the residue class $b' + a'R$ would contain a unit u, implying $du \in (b + aR) \cap R'$ by inductive hypothesis (that is to say, by our minimal choice of a), contradicting the choice of b. Thus $w(a') > 0$.

Appealing again to the Čebotarev density theorem, we can find a prime $\pi \in b' + a'R$ and such that π is not among the finitely many primes of S. The product $d\pi$ is in $(b + aR) \backslash R'$. By the inductive hypothesis,

$$w(d\pi) \geqq w(a) = w(d) + w(a'),$$

$$v(d\pi) = v(d) \geqq v(a) = v(d) + v(a'),$$

showing that $w(\pi) = w(a') = 1$ and $v(a') = 0$. Therefore, a' is a prime element in E_2^S, not in E_0^S, and it cannot be in E_1^S either, since this would imply that $b' + a'R$ contained some $u \in U_S$, entailing $w(du) = w(d) < w(a)$ and $du \in d(b' + a'R) \cap R' \neq \emptyset$.

We thus arrive at $v''(a') = 1$. By definition of E_2^S, this means that π can actually be chosen in E_1^S. This gives $w(d\pi) = w(a)$, $v(d\pi) = v(a)$ and $v''(d\pi) = v''(d) < v''(da')$. The inductive hypothesis now yields the final contradiction, $d\pi \in (b + aR) \cap R'$. This concludes the proof of Lemma 1.

The method for proving the theorem is similar to that used by R. Gupta, K. Murty and R. Murty [4]. First, we interpret the problem in terms of class field theory. Let π be a prime element not in S, we want to show that π is contained in E_2^S.

Let F be the ray class field of modulus (π). That is, F is the largest extension field of K (in some algebraic closure) with the properties

(i) F/K is abelian,

(ii) the conductor of F/K is equal to (π) (since R is a pid),

(iii) $\mathrm{Gal}(F/K) \cong (R/(\pi))^*/\psi(U)$,

where U is the unit group of K and ψ is the map $R \to R/(\pi)$ sending an element to its reduction modulo π. To show that π is contained in E_2^S it is sufficient to find, for each $a \in R$ not congruent modulo π to 0 or to an element of U_S, a prime element ϖ having Artin symbol $(\varpi, F/K) = \sigma$, where σ is the element of $\mathrm{Gal}(F/K)$ corresponding to $a + R\pi$ under the isomorphism (iii), and such that the map $U_S \to (R/\varpi R)^*$ is onto.

Fix π, F, a, and σ for the remainder of the proof. We are going to need a couple of notations. Let F_2 be a finite Galois extension of some number field F_1 and D a union of conjugacy classes of $\mathrm{Gal}(F_2/F_1)$. Denote by $t(F_2/F_1, D)$ the set of rational primes ℓ such that $\mathbb{Q}(\zeta_\ell) \subseteq F_2$ and $\tau|_{\mathbb{Q}(\zeta_\ell)} = 1$ for all $\tau \in D$. Let K_ℓ denote the extension of K formed by adjoining the ℓ^{th} roots of a set of representatives of U/U^ℓ, the field $L = K_2$ will be an abelian (Kummer) extension of K. Let L_1 be the compositum of L and F and let L_2 be the Galois closure of L_1 over $\mathbb{Q}$. Then let

$$C_1 = \{\tau \in \mathrm{Gal}(L_1/K) : \tau|F = \sigma, \tau|_L \neq 1\},$$

let C_2 be the inverse image of C_1 in $\mathrm{Gal}(L_2/K)$, and let C_2^* be the smallest subset of $\mathrm{Gal}(L_2/\mathbb{Q})$ containing C_2 closed under conjugation.

First, we show that $L \cap F = K$. The primes of K which ramify in L are all divisors of 2, while π is the only prime of K which ramifies in F. Since K has no unramified proper abelian extensions, $L \cap F$ cannot be larger than K unless π is itself a divisor of 2. But in this case $[F:K]$, which divides $N\pi - 1$, is odd, while $[L:K]$ is a power of 2. This implies that $L \cap F = K$ and, furthermore, that C_1 is nonempty.

Let us show that $t(L_1/K, C_1) = \{2\}$: The group $\mathrm{Gal}(L_1/K)$ is isomorphic to the direct product of the elementary abelian 2-group $\mathrm{Gal}(L/K)$, which has at least four elements unless $K = \mathbb{Q}$ (in which case there is nothing to prove), and the group $\mathrm{Gal}(F/K)$ of order dividing $N\pi - 1$. If ℓ were an odd prime in $t(L_1/K, C_1)$, the field L_1 would contain a root of unity ζ_ℓ of that order, fixed by all automorphisms $(\tau, \sigma) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$ with $\tau \neq 1$. But then ζ_ℓ is also fixed by $(1, \sigma)$, since the identity element of an elementary 2-group of order at least four can always be written as a product of $N\pi \geqq 2$ nonidentity elements. Then $(1, \sigma^{-1})$ also fixes ζ_ℓ, and so does $(\tau, 1) = (\tau, \sigma) \circ (1, \sigma^{-1})$ for each $\tau \in \mathrm{Gal}(L/K)$. By Galois theory, this would force $K(\zeta_\ell)$ to be contained in F, which is absurd since F is totally real.

Furthermore, $t(L_1/K, C_1) \subseteqq t(L_2/K, C_2) = t(L_2/\mathbb{Q}, C_2^*)$. In fact, we have equality throughout: If ℓ is an odd prime such that L_2 contains a root of unity $\zeta_\ell \notin L_1$ of order ℓ, the group $\mathrm{Gal}(L_2/K)$ must contain automorphisms fixing L_1 and moving ζ_ℓ (because $\zeta_\ell \notin L_1$), and therefore also elements inducing any prescribed automorphism of L_1/K and still not fixing ζ_ℓ. In particular, it is impossible that all elements of C_2 fix ζ_ℓ. Thus 2 is still the only member of $t(L_2/\mathbb{Q}, C_2^*)$.

Now we can apply sieve methods to the problem of finding prime elements ϖ in K with Artin symbol $(\varpi, F/K) = \sigma$. Let $\mathscr{A}$ be a finite sequence of integers, $\mathscr{P}$ a sequence of rational primes, z a real number greater than 2, and

$$P(z) = \prod_{\substack{p<z \\ p\in\mathscr{P}}} p,$$

then

$$S(\mathscr{A}, \mathscr{P}, z) = |\{a \in \mathscr{A} : (a, P(z)) = 1\}|$$

is the number of elements of $\mathscr{A}$ whose prime factors which belong to $\mathscr{P}$ are all greater than z. For d a square-free integer define

$$\mathscr{A}_d = \{a \in \mathscr{A} : a \equiv 0 \pmod{d}\}.$$

If we are given a quantity X which approximates $|\mathscr{A}|$, the number of elements in $\mathscr{A}$, and for each prime $p \in \mathscr{P}$ a number $\omega(p)$ such that $(\omega(p)/p)X$ approximates $|\mathscr{A}_p|$, then the error of this approximation is measured by the numbers

$$R_d = |\mathscr{A}_d| - \frac{\omega(d)}{d} X,$$

where we have put $\omega(1) = 1$ and $\omega(p) = 0$ for primes $p \notin \mathscr{P}$, and finally, for arbitrary square-free integers d,

$$\omega(d) = \prod_{p|d} \omega(p).$$

Let

$$W(z) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right).$$

We also require the functions

$$F(u) = \frac{2e^\gamma}{u}, \quad f(u) = 0, \quad 0 < u \leqq 2,$$

where γ is Euler's constant. For $u > 2$, F, f are solutions to the differential-difference equations

$$(uF(u))' = f(u-1), \quad (uf(u))' = F(u-1).$$

In particular, f is defined by

$$f(u) = \frac{2e^{\gamma}}{u} \log(u-1),$$

for $2 \leqq u \leqq 4$.

We will use the linear sieve in the form given by Iwaniec [7].

Lemma 2. *Assume that $0 < \omega(p) < p$ and that there is a constant $A \geqq 2$ such that for all $z > w \geqq 2$,*

$$\prod_{w \leqq p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)\left(1 + \frac{K}{\log w}\right),$$

then for $\xi^2 \geqq z$ there is the lower bound

$$S(\mathscr{A}, \mathscr{P}, z) \geqq XW(z)\left\{f\left(\frac{\log \xi^2}{\log z}\right) - \frac{B}{(\log \xi)^{1/3}}\right\} - \sum_{\substack{d < \xi^2 \\ d \mid P(z)}} |R_d|,$$

where B is some positive constant.

We apply this lemma to sequences $\mathscr{A} = \{p - 1 \leqq x : (p, L_2/\mathbb{Q}) \in C_2^*\}$. For this case, we have

$$|R_d| \leqq R_\sigma(x, d) = \max_{(a,d)=1} \max_{y \leqq x} \left| \pi_\sigma(y, d, a) - \frac{|C_2^*|}{[L_2 : \mathbb{Q}]\,\phi(d)} li(y) \right|,$$

where $\pi_\sigma(y, d, a)$ is the number of primes $p \leqq y$ such that p is congruent to a modulo d and $(p, L_2/\mathbb{Q}) \in C_2^*$. As customary, we obtain estimates using the function $\psi_\sigma(y, d, a) = \sum_{p^n \leqq y} \log p$, where the sum extends over powers of the primes p counted by π_σ, and then estimate the remainder terms by partial summation.

We use a variant of the Bombieri-Vinogradov theorem given by K. Murty and R. Murty [10], Theorem 7.3.

Lemma 3. *For every $\varepsilon > 0$ and $A > 0$,*

$$\sum_{d \leqq Q}{}' \max_{(a,d)=1} \max_{y \leqq x} \left| \psi_\sigma(y, d, a) - \frac{|C_2^*|}{[L_2 : \mathbb{Q}]\,\phi(d)} y \right| \ll \frac{x}{\log^A x},$$

where $Q = x^{\frac{1}{\eta} - \varepsilon}$, $\eta = \max(n_K - 2, 2)$.

Lemma 3 is the only place we use the assumption that $K/\mathbb{Q}$ is Galois. Lemmas 2 and 3 yield the following

Lemma 4. *For any $\varepsilon > 0$ there exists a positive constant δ_1 depending on ε such that there are more than*

$$\delta_1 x / (\log x)^2$$

rational primes p with the properties

(1) $p \leqq x$,

(2) $(p, L_2/\mathbb{Q}) \in C_2^*$,

(3) *if* $\ell \mid (p-1)$, *then* $\ell \in t(L_2/\mathbb{Q}, C_2^*)$ *or* $\ell > x^{1/2\eta-\varepsilon}$.

Proof. Consider the sequence $\mathscr{A}$ with $\mathscr{P}$ the set of odd primes. The Čebotarev density theorem suggests the choices $X = |C_2^*|/[L_2 : \mathbb{Q}]\, li(x)$ and $\omega(p) = 1$. The first condition of Lemma 2 is obvious, and the second condition is well-known. Since

$$|R_d| \leqq \max_{(a,d)=1} \max_{y \leqq x} \left| \psi_\sigma(y, d, L_2/\mathbb{Q}) - \frac{|C_2^*|}{[L_2 : \mathbb{Q}]\,\phi(d)}\, y \right|,$$

Lemma 3 implies that

$$\sum_{\substack{d < x^{1/\eta - \varepsilon} \\ d \mid P(z)}} |R_d| \ll x/(\log x)^3 .$$

Choose $z = x^{1/2\eta-\varepsilon}$ and $\xi^2 = x^{1/\eta-\varepsilon}$. Apply Lemma 2 to obtain

$$S(\mathscr{A}, \mathscr{P}_d, z) \geqq X W(z) \left\{ f\left(\frac{\log \xi^2}{\log z}\right) - \frac{B}{(\log \xi)^{1/3}} \right\} - O\left(\frac{x}{(\log x)^3}\right).$$

Lemma 5. *For every* $\varepsilon > 0$ *and for a suitable positive constant* δ_2 *depending on* ε, *there are more than*

$$\delta_2\, x/(\log x)^2$$

prime elements ϖ *of* K *with the properties*

(1) $N\varpi = p \leqq x$ *for some rational prime* p,

(2) $(\varpi, F/K) = \sigma$,

(3) $(\varpi, K_\ell/K) \neq 1$ *for all* $\ell \in t(F/K, \sigma)$,

(4) *if* $\ell' \mid (p-1)$, *then* $\ell' \in t(F/K, \sigma)$ *or* $\ell' > x^{1/2\eta-\varepsilon}$.

Proof. Consider the rational primes p found in Lemma 4. Choose a prime element Π of L_2 lying above p. For some $\tau \in \mathrm{Gal}(L_2/\mathbb{Q})$, $(\Pi^\tau, L_2/\mathbb{Q}) \in C_2$. If ϖ is a prime element of K lying below Π^τ, then ϖ has properties (2) and (3). The automorphism $(\Pi^\tau, L_2/\mathbb{Q})$ fixes K pointwise, which means that K is contained in the decomposition field of Π^τ. Thus, ϖ has residue class degree one over p, which gives properties (1) and (4).

The last lemma we require states that there are many prime elements ϖ so that $\psi_\varpi(U_S)$ is large.

Lemma 6. *Let* $s = |S| + n_K - 1$, *then the number of prime elements* ϖ *of* K *for which* $|\psi_\varpi(U_S)| < y$ *is* $\ll y^{(s+1)/s}$.

Proof. The number of integer s-tuples $(a_1, a_2, \ldots, a_s)$ with

$$|a_1| + |a_2| + \cdots + |a_s| \leqq y^{1/s} \tag{3}$$

is less than $\dfrac{s+1}{s} y$. If $|\psi_\varpi(U_S)| \leqq y$, then

$$\omega_1^{a_1} \omega_2^{a_2} \cdots \omega_s^{a_s} \equiv \omega_1^{b_1} \omega_2^{b_2} \cdots \omega_s^{b_s} (\operatorname{mod} \varpi),$$

for some pair of s-tuples satisfying (3) with the ω_i either units or prime elements in S. Then, ϖ divides the numerator of

$$\omega_1^{a_1 - b_1} \omega_2^{a_2 - b_2} \cdots \omega_s^{a_s - b_s} - 1 .$$

The number of primes dividing each such element is bounded by a constant times $y^{1/s}$, where the constant is independent of y. Thus, the total number of primes ϖ such that $|\psi_\varpi(U_S)| \leqq y$ is bounded by a constant times $y^{(s+1)/s}$.

Now, to prove the theorem, consider the primes ϖ found in Lemma 5. For these primes either $|\psi_\varpi(U)| < x^{1 - 1/2\eta + \varepsilon}$ or the only divisors of

$$|(R/R\varpi)^*/\psi_\varpi(U)| \tag{4}$$

are powers of 2, since this index, if nontrivial, must be divisible by a prime divisor of $p - 1$. For similar reasons, the same alternative holds with U_S in place of U. Our choice of s implies

$$\left(1 - \frac{1}{2\eta} + \varepsilon\right)\left(\frac{s+1}{s}\right) < 1 ,$$

assuming ε is chosen small enough. Putting $y = x^{1 - 1/2\eta + \varepsilon}$ in the previous lemma, we see that the primes ϖ satisfying $|\psi_\varpi(U_S)| < y$ may be disregarded as $x \to \infty$. On the other hand, for any prime ℓ dividing the group index in formula (4), ϖ must be fully decomposed from K to K_ℓ, since $(R/R\varpi)^*$ is cyclic and the residue field extension is generated by ℓ^{th} roots of members of the subgroup of index ℓ, which exist already in the field $R/R\varpi$. This cannot happen, however, with the prime $\ell = 2$, because $(\varpi, L_1/K) \in C_1$ restricts to a nontrivial automorphism of L and thus the decomposition field cannot contain L. Thus the index

$$|(R/R\varpi)^*/\psi_\varpi(U_S)| , \tag{5}$$

which divides the index (4), must be odd. Hence, for each of the infinitely many nonassociate primes ϖ which have $|\psi_\varpi(U_S)|$ larger than the upper bound, the index (5) equals one i.e. $\varpi \in E_1^S$, which completes the proof of the theorem.

Examples

The following proposition is helpful for verifying that the unit group maps onto

$$(R/(\pi_1^{a_1}\cdots\pi_m^{a_m}))^*,$$

for all nonnegative integers a_i, $i=1,\dots,m$.

Proposition. *Suppose that $\pi_1,\dots,\pi_s$ are non-ramified prime elements of residue class degree one in R not lying above 2. If a multiplicative submonoid M of R maps onto $(R/(\pi_1^2\pi_2^2\cdots\pi_s^2))^*$, then M maps onto $(R/(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_s^{a_s}))^*$ for any choice of nonnegative integers a_i, $i=1,\dots,s$.*

Proof. Suppose the claim has been proved for all products $\pi_1^{m_1}\cdots\pi_s^{m_s}$, such that $m_i\leqq n_i$ for $i=1,\dots,s$ with at least one of the inequalities strict. Use the inductive assumption to find an element ε_1 of M, ε_1 such that $\varepsilon_1\equiv 1(\operatorname{mod}\pi_i^{n_i})$ for $i=2,\dots,s$ and ε_1 has order $p_1^{n_1-2}(p_1-1)$ modulo $\pi_1^{n_1-1}\pi_2^{n_2}\cdots\pi_s^{n_s}$, where $N\pi_1=p_1$. Then,

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)}=1+k\pi_1^{n_1-2}\pi_2^{n_2}\cdots\pi_s^{n_s},$$
$$\varepsilon_1^{p_1^{n_1-2}(p_1-1)}\equiv 1+k'\pi_1^{n_1}(\operatorname{mod}\pi_1^{n_1-1}\pi_2^{n_2}\cdots\pi_s^{n_s})$$

where $\pi_1\not\mid k$, k' which implies that $\varepsilon_1$has order $p_1^{n_1-1}(p_1-1)$ modulo $\pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$. Similarly, elements $\varepsilon_i\in M$ can be found such that $\varepsilon_i\equiv 1(\operatorname{mod}\pi_j^{n_j})$ for $j\neq i$ and ε_i has order $p_i^{n_i-1}(p_i-1)$ modulo $\pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$. Then the multiplicative group generated by $\varepsilon_1,\dots,\varepsilon_s$ maps onto the coprime residue classes modulo $\pi_1^{n_1}\cdots\pi_r^{n_s}$.

Remark. A similar result holds for prime elements lying above 2 and prime elements with residue class degree greater than one. In these cases $(R/(\pi^n))^*$, $n\geqq\dfrac{p}{p-1}$, is the product of $f+1$ or f cyclic groups, according as R does or does not contain the p^{th} roots of unity, where $N\pi=p^f$ with p a rational prime. Thus, this more general result is less useful for applications of our theorem.

Our first example is K, the splitting field of x^4-18x^2+4 of discriminant 616^2. K has an integral basis $\{1,\alpha,\alpha^2/2,\alpha^3/2\}$, where α is a root of the polynomial. The unit group of K is generated by

$$-9+\alpha^2/2,\quad 1-2\alpha-\alpha^2/2,\quad 30+63\alpha-3\alpha^2/2-7\alpha^3/2.$$

We consider the prime ideals of K with norm less than or equal to 7. Compute the factorizations of x^4-18x^2+4 modulo p for $p\leqq 7$.

$$\begin{aligned}x^4-18x^2+4&\equiv x^4(\operatorname{mod}2)\\&\equiv(x^2+x+2)(x^2+2x+2)(\operatorname{mod}3)\\&\equiv(x^2+3x+3)(x^2+2x+3)(\operatorname{mod}5)\\&\equiv(x+3)^2(x+4)^2(\operatorname{mod}7).\end{aligned}$$

Using these factorizations, we can determine the image of the unit group modulo the prime ideal $(7, \alpha + 3)$.

$$-9 + \alpha^2/2 \equiv -2 + \alpha^2/2 + 7\alpha^2/2 \equiv -2 + 4\alpha^2 \equiv -2 + 2\alpha \equiv -1 (\mathrm{mod}\,(7, \alpha + 3)),$$

$$1 - 2\alpha - \alpha^2/2 \equiv 1 - 2\alpha + 3\alpha^2 \equiv 1 - 11\alpha \equiv 1 - 4\alpha \equiv -1 (\mathrm{mod}\,(7, \alpha + 3)),$$

$$30 + 63\alpha - 3\alpha^2/2 - 7\alpha^3/2 \equiv 2 - 3\alpha^2/2 \equiv 2 + 2\alpha^2 \equiv 2 + \alpha \equiv -1 (\mathrm{mod}\,(7, \alpha + 3)).$$

Therefore, the image of the unit group modulo $(7, \alpha + 3)$ is $\{\pm 1\}$. There is only one nontrivial ideal of norm less than 7, namely $(2, \alpha) = (\alpha)$ of norm 4. Only the classes ± 1, ± 3 modulo $(7, \alpha + 3)$ contain elements of norm less than 7. Hence, the norm ist not a Euclidean algorithm for the ring of integers of K. But, since

$$-9 + \alpha^2/2 \equiv 102 (\mathrm{mod}(13, \alpha + 12)^2),$$

and 102 is a primitive root modulo 13^2, the theorem implies that the ring of integers of K is Euclidean.

Next, consider the field with generating polynomial $x^3 - x^2 - 24x + 27$ and discriminant 73^2. An integral basis is $1, \alpha, \gamma = (-15 - \alpha + \alpha^2)/3$. The unit group is generated by $41 - 10\alpha + 6\gamma$ and $31 + 16\alpha + 10\gamma$. As above, one can show that the ring of integers is not Euclidean for the norm by considering the residue classes modulo the ideal (2). Let $\pi_1 = 8 - \alpha - 3\gamma$ of norm 7 and $\pi_2 = 1 + 3\alpha + \gamma$ of norm 83. The unit group maps onto $(R/(\pi_1^2 \pi_2^2))^*$. Hence, the theorem implies that R is Euclidean.

We cannot apply the theorem to $\mathbb{Z}[\sqrt{14}]$; however, for p a rational prime which does not split in $K = \mathbb{Q}(\sqrt{14})$, consider the ring $R = \mathbb{Z}[\sqrt{14}][1/p]$. We will choose p later on. The positive fundamental unit of K is $\varepsilon = 15 + 4\sqrt{14}$. Let $\pi_1 = 5 - \sqrt{14}$ of norm 11, $\pi_2 = 27 + 7\sqrt{14}$ of norm 43, and $\pi_3 = 3 - 2\sqrt{14}$ of norm 47. ε has order 110 modulo π_1^2, order 1806 modulo π_2^2, and order 1081 modulo π_3^2. $-\varepsilon$ has order 55 modulo π_1^2, order 903 modulo π_2^2, and order 2162 modulo π_3^2. Thus, one can verify that the image of the multiplicative group generated by $\pm\varepsilon$ in $(R/(\pi_1^2 \pi_2^2 \pi_3^2))^*$ has index 2. The residue class 310417515 of order 2 modulo $\pi_1^2 \pi_2^2 \pi_3^2$ is not contained in the image of the units. Now choose $p = 1298852237$ which is contained in this residue class and does not split in $\mathbb{Q}(\sqrt{14})$, then the units of $\mathbb{Z}[\sqrt{14}][1/p]$ map onto $(R/(\pi_1^2 \pi_2^2 \pi_3^2))^*$. To see that R is not Euclidean for the norm, note that up to multiplication by units, there is only one element of norm less than 4, $4 + \sqrt{14}$. The units all map to 1 modulo (2). The residue class $1 + \sqrt{14}$ modulo (2) contains no elements of norm less than 4; hence, R is not Euclidean for the norm.

Acknowledgements. We would like to thank Rajiv Gupta, Michael Zieve, and the referees for their careful reading of earlier versions of this paper.

References

[1] *J. Buchmann* and *D. Ford*, On the Computation of Totally Real Quartic Fields of Small Discriminant, Math. Comp. **52** (1989), 161–174.

[2] *J. Buchmann*, *M. Pohst* and *J. v. Schmettow*, On the Computation of Unit Groups and Class Groups of Totally Real Quartic Fields, Math. Comp. **53** (1989), 387–397.

[3] *D. Clark*, The Euclidean Algorithm for Galois Extensions of the Rational Numbers, Ph. D. Thesis, McGill University, Montréal 1992.

[4] *R. Gupta*, *M.R. Murty* and *V.K. Murty*, The Euclidean Algorithm for S-integers, Conf. Proc. CMS **7** (1987), 189–201.

[5] *H. Hasse*, Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen, J. reine angew. Math. **159** (1928), 3–12.

[6] *C. Hooley*, On Artin's Conjecture, J. reine angew. Math. **225** (1967), 209–220.

[7] *H. Iwaniec*, Rosser's Sieve, Acta Arith. **36** (1980), 171–202.

[8] *H. W. Lenstra, Jr.*, On Artin's Conjecture and Euclid's Algorithm in Global Fields, Invent. Math. **42** (1977), 201–224.

[9] *T. Motzkin*, On the Euclidean Algorithm, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.

[10] *M.R. Murty* and *V.K. Murty*, A Variant of the Bombieri-Vinogradov Theorem, Conf. Proc. CMS **7** (1987), 243–271.

[11] *P. Samuel*, About Euclidean Rings, J. Algebra **19** (1971), 282–301.

[12] *P. Weinberger*, On Euclidean Rings of Algebraic Integers, Proc. Symp. Pure Math. **24** (1973), 321–332.

Department of Mathematics, McGill University, Montréal, Québec, H3A 2K6, Canada

Institut für Experimentelle Mathematik, Universität GHS Essen, Ellernstraße 29, 45326 Essen, Germany

Eingegangen 2. April 1993, in revidierter Fassung 18. Juli 1994