BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 6, November 1973

EUCLID'S ALGORITHM IN GLOBAL FIELDS

BY CLIFFORD QUEEN

Communicated by Gian-Carlo Rota, April 23, 1973

1. **Introduction.** The purpose of this note is to announce some results regarding the relationship between principal ideal domains and euclidean domains which are subrings of global fields.

Let A be an integral domain. We shall say that A is a euclidean ring, or simply "A is euclidean", if there exists a map $\varphi : A - \{0\} \to N$, N the nonnegative integers, satisfying the following two properties:

(1) If $a, b \in A - \{0\}$, then $\varphi(ab) \geqq \varphi(a)$.

(2) If $a, b \in A$, $b \neq 0$, then there exists $q, r \in A$ such that $a = bq + r$, where $r = 0$ or $\varphi(r) < \varphi(b)$.

It is easy to see that condition (1) is an unnecessary restriction; i.e. if there is a map $\varphi : A - \{0\} \to N$ satisfying only condition (2), then there is always another map φ', derived from φ, such that φ' satisfies both (1) and (2). Further, it is apparently unknown whether one enlarges the class of euclidean integral domains by enlarging N to a well-ordered set of arbitrary cardinality, but this question will not concern us here except to say that whenever A has finite residue classes, i.e., A modulo any nonzero ideal is finite, then insisting on N as a set of values is no restriction. We refer the reader to an excellent paper by P. Samuel [7] in which all of the above and much more is exposed with great clarity.

Let A be as above. We define subsets A_n of A for $n \in N$ by induction as follows: $A_0 = \{0\}$ and if $n \geqq 1$, then $A'_n = \bigcup_{\alpha < n} A_\alpha$. Finally $A_n = \{b \in A |$ there is a representative in A'_n of every residue class of A modulo $bA\}$. Setting $A' = \bigcup_{n \in N} A_n$, A is euclidean if and only if $A' = A$ (see Motzkin [4]). Further when $A' = A$ we get a map $\varphi : A - \{0\} \to N$, where if $x \in A - \{0\}$ then there exists a unique $n \geqq 0$ such that $x \in A_{n+1} - A_n$ and $\varphi(x) = n$. Now not only does φ satisfy conditions (1) and (2) above, but if φ' is any other map satisfying condition (2), then $\varphi(x) \leqq \varphi'(x)$ for all $x \in A - \{0\}$. Hence Motzkin justifiably calls φ the minimal algorithm for A.

Let F be a global field; F is a finite extension of the rational numbers Q, or F is a function field of one variable over a finite field. Let S be a nonempty finite set of prime divisors of F such that S contains all infinite (i.e. archimedean) prime divisors. For each finite (i.e. nonarchimedean) prime divisor P we denote by O_P the valuation ring associated to P in F. Letting

AMS (MOS) subject classifications (1970). Primary 12A05; Secondary 12A05.
Key words and phrases. Euclid's algorithm, function fields.

P range over all prime divisors of F we get a ring for each such set S as follows:

$$O_S = \bigcap_{P \notin S} O_P.$$

For each such finite set S, O_S is a Dedekind ring with finite residue classes. It is known that there always exists such a finite set S such that O_S is a principal ideal domain or as we shall say "O_S is P.I.D." Further, as we have shown in [**6**], one can always find finite S so that O_S is euclidean. The question that concerns us here is: If S is a finite set of prime divisors, as above, and O_S is P.I.D., is it euclidean? That the answer to our question is not always yes is well known, but, as we shall see, there is excellent reason to believe that the only time the answer is no is in the finite number of examples already known.

In the next section we give an indication of the proof of the following: If F is a function field over a finite field and S is a nonempty finite set of prime divisors such that O_S is P.I.D., then O_S is euclidean if S contains at least two elements. Further we recall the evidence, due mostly to P. Weinberger (see [**9**]), that the above result is also true in the case when F is a number field. Full details of the proofs will appear elsewhere.

2. Let F be a global field and S a finite set of prime divisors of F such that S contains all infinite primes, the cardinality $|S|$ of S is at least 2 and O_S is P.I.D. Let F_S denote the group of S-units of F (see [**3**]) and let M_S denote the set of prime divisors P such that the nonzero residue classes of O_P modulo its maximal ideal I_P are representable by elements of F_S. Let P_0 be a prime divisor of F such that $P_0 \notin S \cup M_S$.

$\mathscr{P}_{P_0}$ denotes the rays modulo P_0, i.e. the group of principal ideals (α), $\alpha \in F$, with $|\alpha - 1|_{P_0} < 1$, $|\ \ |_{P_0}$ the usual normalized valuation associated with P_0;

I_S denotes the group of divisors of F involving only finite members of S;

$I(P_0)$ denotes the group of divisors prime to P_0.

Now we have a tower of subgroups $I(P_0) \supseteq H_S(P_0) \supseteq \mathscr{P}_{P_0}$, where $H_S(P_0) = I_S \cdot \mathscr{P}_{P_0}$. Thus according to class field theory (see [**1**]) we have an abelian extension E_{P_0} of F associated to $H_S(P_0)$ under the Artin reciprocity map.

THEOREM 1. *Let C be any divisor class of $I(P_0)$ modulo $H_S(P_0)$ and denote by M_C the set of prime divisors $P \in C$. If F is a function field (i.e. a function field of one variable over a finite field), then $M_S \cap M_C$ is an infinite set.*

INDICATION OF PROOF. Since $|S| \geqq 2$, there exists $t \in F - k$, k the exact field of constants, where $t \in F_S$. Let M_t denote the set of prime divisors P such that $P \notin S$ and t represents the generator of the multiplicative group of the field O_P/M_P (i.e. t is a primitive root modulo P). In [**2**] there is produced an exact computation of the Dirichlet density $\omega(M_t)$. It is shown that the density exists and $\omega(M_t) > 0$ modulo the generalized Riemann hypothesis.[1] Now in view of Weil [**8**], the generalized Riemann hypothesis holds for function fields over finite fields. Hence indeed $\omega(M_t)$ exists and is positive. Finally our procedure is to show that M_t and M_C are independent sets in the sense of Dirichlet density. Having shown that, we get at once that

$$\omega(M_t \cap M_C) = \omega(M_t)\omega(M_C).$$

By an extension of Dirichlet's Theorem on primes in an arithmetic progression we have that $\omega(M_C) = 1/n$, where $n = [E_{P_0}:F]$. Now, observing $M_t \cap M_C \subseteq M_S \cap M_C$ and that $\omega(M_t \cap M_C) > 0$, our result follows. Q.E.D.

THEOREM 2. *If F is a function field, then O_S is euclidean.*

INDICATION OF PROOF. Let $A = O_S$ and recall the notation A_0, A_1, $A_2, \ldots$ used in §1. We have that $A_0 = \{0\}$, $A_1 = \{0\} \cup F_S$ and $A_2 - A_1$ consists of all prime elements of A associated to the prime divisors of M_S. Further, in view of Theorem 1, every other prime element is contained in $A_3 - A_2$. Now if $0 \neq b \in A$, then b can be written uniquely, modulo elements of F_S, as a product of n_1 prime elements taken from A_2 and n_2 prime elements from $A_3 - A_2$. We use double induction on n_1 and n_2 to deduce that $b \in A'$ and thus show that $A' = A$.

REMARK. (1) If F is a function field, then the minimal algorithm φ_S on O_S, depends only on S and F, and lifts to a homomorphism from $F^* = F - \{0\}$ onto the rational integers Z. Further there are only finitely many Dedekind subdomains of function fields which are P.I.D. but not euclidean.

(2) Suppose now that F is a number field. The evidence is that all of the above results, including (1) above, are true in this case too. In fact a careful reading of [**9**] convinces one that all of the above is true modulo certain generalized Riemann hypotheses.

REFERENCES

1. E. Artin and J. Tate, *Class field theory*, Lecture Notes, Institute for Advanced Study, Princeton, N.J.

2. H. Belharz, *Primdivisoren mit Vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), 476–492.

3. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970. MR **44** #181.

[1] We choose t so that $t \notin F^n$ for n prime to characteristic of F.

4. T. Motzkin, *The Euclidean algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146. MR **11,** 311.

5. M. Madan and C. Queen, *Algebraic function fields of class number one*, Acta Arith. **20** (1972), 423–432.

6. C. Queen, *Euclidean subrings of global fields*, submitted for publication in the London Math. Soc. J.; also appears as Research Announcement in Bull. Amer. Math. Soc., (March 1973), paper #47.

7. P. Samuel, *About Euclidean rings*, J. Algebra **19** (1971), 282–301. MR **43** #6190.

8. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Indust., no. 1041, Publ. Inst. Math. Univ. Strasbourg 7, 1945, Hermann, Paris, 1948. MR **10,** 262.

9. P. Weinberger, *On Euclidean rings of algebraic integers*, Proc. Sympos. Pure Math., vol. 24, Amer. Math. Soc., Providence, R.I., 1973.

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PENNSYLVANIA 18015