Repeating our method for all other prime power factors of e instead of u^t, we get our theorem.

When the class number of k is relatively prime to n, we can delete the condition on q that it splits into principal k-primes and state the theorem in the following manner:

THEOREM 2. *Let $(k: Q) = n$ and let the class number of k be relatively prime to n. Let e be a positive integer such that*

$$(e, n/e) = 1 \quad \text{and} \quad e \mid (g_q, e_p, p-1).$$

Then

$$e \mid c(p-1)/\mathrm{ord}_p q$$

where $c = 1$ if e is odd or $p \equiv 1 \bmod 2e$ and $c = 2$ otherwise.

Proof. Let K be the Hilbert class field of k and let $(K: k) = h$. Then $(h, n) = 1$ and $(K: Q) = nh$. Let e_l^K and g_l^K denote the ramification index of a K-prime lying above the rational prime l and the number of distinct K-primes lying above l respectively. Then, we can easily see that

$$(e, n/e) = 1 \quad \text{implies} \quad (e, nh/e) = 1$$

and

$$e \mid (g_q, e_p, p-1) \quad \text{implies} \quad e \mid (g_q^K, e_p^K, p-1).$$

Taking K for k in Theorem 1, we see that e satisfies the required conditions and so the theorem follows since every k-prime splits into principal K-primes.

Received on 20. 8. 1973 (444)

ACTA ARITHMETICA
XXVI (1974)

Arithmetic euclidean rings

by

CLIFFORD QUEEN (Bethlehem, Penn.)

1. Introduction. 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 φ: $A-\{0\} \to N$, N the non-negative integers, satisfying the following two properties:

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

2) If $a, b \in A$, $b \neq 0$, then there exist $q, r \in A$ 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 φ: $A - \{0\} \to N$ 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 non-zero 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 [8] 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 $n \geqslant 1$, then $A'_n = \bigcup_{a<n} A_a$. Finally $A_n = \{b \in A \mid$ 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 [6]). Further when $A' = A$ we get a map φ: $A - \{0\} \to N$, where if $x \in A - \{0\}$ then there exists a unique $n \geqslant 0$ 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 $\varphi(x) \leqslant \varphi'(x)$ for all $x \in A - \{0\}$. Hence Motzkin justifiably calls φ the minimal algorithm for A.

Let F be a global field, so 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 non-empty finite set of prime divisors of F such that S contains all infinite (i.e. archimedean) prime divisors. For each finite (i.e. non-archimedean) prime divisor P, we denote by O_P the valuation ring associated to P in F. Letting 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 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 [7], 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 Section 2 we prove an essential lemma using transcendental techniques. In Section 3 we prove the following: If F is a function field over a finite field and S a finite non-empty set of prime divisors of F such that O_S is P.I.D., then O_S is euclidean if S contains at least two elements. Further we display the evidence, due mostly to P. Weinberger (see [11]), that the above result is also true in the case when F is a number field.

2. Let F be a global field and S a finite non-empty set of prime divisors of F such that S contains all infinite primes of F and has cardinality at least two. Assume further that O_S is P.I.D. Let F_S denote the group of S-units of F and denote by M_S the set of finite prime divisors P of F such that $P \notin S$ and the non-zero residue classes of O_P modulo its maximal ideal I_P are represented by elements of F_S. We shall say that an integral divisor D is prime to the elements of S if for finite P in S, $V_P(D) = 0$, where for any finite prime divisor P of F, V_P denotes the additive normalized valuation associated with P. We establish notation as follows: Let D be an integral divisor of F prime to the elements of S.

R_D — denotes the rays of F modulo D, i.e., the group of principal divisors (x), where $x \in F^* = F - \{0\}$ and $V_P(x-1) \geqslant V_P(D)$ for all finite P such that $V_P(D) > 0$;

I_D — denotes the group of divisors of F prime to the set of finite prime divisors P such that $V_P(D) > 0$;

I_S — denotes the group of divisors generated by finite members of S.

Now let D be any integral divisor of F prime to the elements of S and consider the tower of subgroups $I(D) \supseteq H_S(D) \supseteq R_D$, where $H_S(D) = I_S \cdot R_D$. Because $S \neq \emptyset$, $H_S(D)$ has finite index in $I(D)$ and thus by classfield theory (see [1]) there is a finite abelian extension E_D of F which is classfield to $H_S(D)$. Let C range over the classes of $I(D)$ modulo $H_S(D)$. For each C we set K_C equal to the set of prime divisors P such that $P \notin S$ and $P \in C$. Our objective in this section is to investigate the sets $M_S \cap K_C$. To that end we record some definitions and results regarding the idea of Dirichlet density (we follow [2] and [3]). Letting P range over all finite prime divisors of F, we set

$$\xi(\sigma, F) = \prod_P \left(1 - \frac{1}{N(P)^\sigma}\right)^{-1},$$

where $N(P)$ denotes the absolute norm of P and $\sigma > 1$ is to take on real values. We note that $\xi(\sigma, F)$ is absolutely convergent for $\sigma > 1$ and it is called the real zeta-function of F. If M is a set of finite prime divisors of F, we define a real valued continuous function ($\sigma > 1$)

$$\omega(\sigma, M) = \left(\sum_{P \in M} \frac{1}{N(P)^\sigma}\right)(\log \xi(\sigma, F))^{-1}.$$

Next

$$\lim_{\sigma \to 1+0} \omega(\sigma, M) = \omega(M)$$

is called the Dirichlet density of M, when the limit exist. Evidently M is an infinite set if $\omega(M) > 0$. Of particular interest to us, for later application, is the following:

TCHEBOTAREV'S THEOREM. *Let E be a finite galois extension of F with galois group G. Let P' be a finite prime divisor of E such that P' does not ramify over F. Then the Frobenius map $(P', E/F)^*$ determines a conjugacy class Δ in G. If Δ is a conjugacy class in G and K_Δ the set of prime divisors P of F such that there exists P' of E with $P'|P$ and $(P', E/F)^* \in \Delta$, then $\omega(K_\Delta) = \left|\dfrac{\Delta}{G}\right|$, where $|\ |$, denotes the cardinality of a finite set.*

THEOREM 1. *If F is a function field (i.e. a function field of one variable over a finite field), then for any class C of $I(D)$ modulo $H_S(D)$*

$$M_S \cap K_C$$

is an infinite set.

Proof. Let k be the exact field of constants of F and set $q = |k|$. If F_S denotes the group of S-units of F, then, because $|S| \geqslant 2$, there exists $t \in F_S$ such that $t \notin F^m$ for any positive integer m, where $(m, q) = 1$. We denote by T the set of prime divisors $P \in M_S$ such that t represents the generator of the multiplicative group of the field O_P/I_P, i.e. t is a primitive root modulo P. Following Bilharz [2], we discuss the existence and positivity of $\omega(T)$. To that end let P be a prime divisor of F such that $P \notin S \cup T$. There exists a rational prime p such that $p \nmid q$, $N(P) \equiv 1 \bmod p$ and $t^{\frac{N(P)-1}{p}} \equiv 1 \bmod I_P$ in O_P. If m is a positive integer, $(m, q) = 1$, we denote by $\mathscr{S}(L_m)$ the set of prime divisors P such that $P \notin S$ and P splits completely in $L_m = F(\sqrt[m]{1}, \sqrt[m]{t})$. For convenience we shall also denote by $\mathscr{S}(L_1)$ the set of prime divisors of F not in S. Now if p is a rational prime, $p \nmid q$, then $P \in \mathscr{S}(L_p)$ if and only if $P \notin S$, $N(P) \equiv 1 \bmod p$ and $t^{\frac{N(P)-1}{p}} \equiv 1 \bmod I_P$. Thus letting p range over all rational primes we have

$$T = \bigcap_{p \nmid q} \overline{\mathscr{S}(L_p)},$$

where $\overline{\mathscr{S}(L_p)} = \mathscr{S}(L_1) - \mathscr{S}(L_p)$. We note that $\mathscr{S}(L_m) = \bigcap_{p|m} \mathscr{S}(L_p)$ if m is a square free positive integer. Hence setting $T_n = \bigcap_{p \leqslant n} \overline{\mathscr{S}(L_p)}$, $n \geqslant 1$, we obtain T_n as an algebraic sum of sets (see [2])

$$T_n = \sum_{m|m_n} \mu(m) \mathscr{S}(L_m),$$

where $m_n = \prod_{\substack{p \nmid q \\ p \leqslant n}} p$. The significance of writting T_n as an algebraic sum of sets is that it gives us $\omega(\sigma, T_n)$ in terms of the $\omega(\sigma, \mathscr{S}(L_m))$, namely

$$\omega(\sigma, T_n) = \sum_{m|m_n} \mu(m) \omega(\sigma, \mathscr{S}(L_m)).$$

Since $T_{n+1} \subseteq T_n$, $n \geqslant 1$, we have (for $\sigma > 1$)

(1) $$\omega(\sigma, T_n) \geqslant \omega(\sigma, T_{n+1}).$$

Further because $T_n - T \subseteq \bigcup_{\substack{p > n \\ p \nmid q}} \mathscr{S}(L_p)$,

(2) $$0 \leqslant \omega(\sigma, T_n) - \omega(\sigma, T) \leqslant \sum_{\substack{p > n \\ p \nmid q}} \omega(\sigma, \mathscr{S}(L_p)).$$

Now for each positive integer m, $(m, q) = 1$, we have by Tchebotarev's theorem that

$$\omega(\mathscr{S}(L_m)) = \lim_{\sigma \to 1+0} \omega(\sigma, \mathscr{S}(L_m)) = \frac{1}{n(m)},$$

where $n(m) = [L_m : F]$. Next in view of [2]

$$\lim_{n\to\infty} \omega(T_n) = \sum_{(m,q)=1} \mu(m) \omega(\mathscr{S}(L_m)) = \sum_{(m,q)} \frac{\mu(m)}{n(m)} > 0.$$

We would have that

$$\lim_{n\to\infty} \omega(\sigma, T_n) = \omega(\sigma, T) \quad \text{and} \quad \omega(T) = \sum_{(m,q)=1} \frac{\mu(m)}{n(m)} > 0,$$

in view of (1) and (2), if the following held:

(3) $\sum_{p \nmid q} \omega(\sigma, \mathscr{S}(L_p))$ is uniformly convergent in any interval

$$1 < \sigma \leqslant \sigma_0, \ \sigma_0 > 1.$$

Bilharz shows in [2] that (3) is true modulo the Riemann Hypothesis for function fields over finite fields. According to Weil [10], the Riemann Hypothesis holds for function fields and thus indeed

$$\omega(T) = \sum_{(m,q)=1} \frac{\mu(m)}{n(m)} > 0.$$

Now let C be any class in $I(D)$ modulo $H_S(D)$. Let E_D be classfield to $H_S(D)$ and for any positive integer m, consider $E_D \cap L_m$. Since D is prime to the elements of S and only elements of S can ramify in L_m, we have that $E_D \cap L_m$ is an unramified extension of F. Since $E_D \cap L_m$ is unramified over F and contained in E_D, we have $H_S(D) \cdot R(D) \subseteq H$, where $R(D)$ denotes the group of principal divisors of F prime to D and H denotes the divisor group in $I(D)$ to which $E_D \cap L_m$ is classified. Since $R_D \subseteq R(D)$, $H_S(D) \cdot R(D) = I_S \cdot R(D)$ and because O_S is P.I.D., $I_S \cdot R(D) = I(D)$. Thus $H = I(D)$, i.e. $E_D \cap L_m = F$. Now if H_D is the galois group of E_D over F, H_m that of L_m over F and G that of $L_m \cdot E_D$ over F,

$$G \cong H_m \times H_D.$$

There exists unique $\sigma_C \in H_D$ such that $(C, E_D/F) = \sigma_C$, where $(\ , E_D/F)$ denotes the Artin reciprocity map. Now if P' is a prime of $L_m \cdot E_D$ which does not ramify over F and $(P', L_m, E_D/F)^* = (1, \sigma_C)$, then $P \in \mathscr{S}(L_m) \cap K_C$ if $P' | P$ and $P \notin S$. Conversely if $P \in \mathscr{S}(L_m) \cap K_C$ then $P \notin S$, P does not ramify in $L_m \cdot E_D$ and there exists a prime divisor P' of $L_m \cdot E_D$, such that $P' | P$ and $(P', L_m \cdot E_D/F)^* = (1, \sigma_C)$. So because $(1, \sigma_C)$ is in the center of G, we have by Tchebotarev's theorem

(1′) $$\omega(\mathscr{S}(L_m) \cap K_C) = \omega(\mathscr{S}(L_m)) \cdot \omega(K_C).$$

Next

$$\omega(T_n \cap K_C) = \sum_{m|m_n} \mu(m) \omega(\mathscr{S}(L_m)) \omega(K_C)$$

and

$$\omega(\sigma, T_n \cap K_C) = \sum_{m|m_n} \mu(m) \omega(\sigma, \mathscr{S}(L_m) \cap K_C).$$

Since

$$T_{n+1} \cap K_C \subseteq T_n \cap K_C \quad \text{and} \quad T_n \cap K_C - T \cap K_C \subseteq \bigcup_{\substack{p \nmid q \\ p > n}} \mathscr{S}(L_p),$$

(2′) $$\omega(\sigma, T_n \cap K_C) \geqslant \omega(\sigma, T_{n+1} \cap K_C),$$

and

$$(3') \qquad 0 \leqslant \omega(\sigma, T_n \cap K_C) - \omega(\sigma, T \cap K_C) \leqslant \sum_{\substack{p \nmid q \\ p > n}} \omega(\sigma, \mathscr{S}(L_p)).$$

Finally (1′), (2′), (3′) and (3) yield

$$\omega(T \cap K_C) = \lim_{n\to\infty} \omega(T_n \cap K_C) = \omega(T)\,\omega(K_C),$$

and since $\omega(K_C) = 1/d$, $d = [E_D : F]$, and $T \cap K_C \subseteq M_S \cap K_C$, we have

$$\omega(M_S \cap K_C) > 0.$$

Q.E.D.

3. Let F be a global field and S a finite non-empty set of prime divisors such that S contains all infinite primes and $|S| \geqslant 2$. Consider the homomorphism θ_S from the group I of all divisors of F into the rational integers Z, determined on finite prime divisors P as follows: $\theta_S(P) = 0$ if $P \in S$, $\theta_S(P) = 1$ if $P \in M_S$ and $\theta_S(P) = 2$ if $P \notin S \cup M_S$. We have an exact sequence

$$0 \to I_S \to I \xrightarrow{\theta_S} Z.$$

Remark 1. If F is a function field, then by [2] θ_S is surjective. If F is a number field then there is good reason to believe that θ_S is also surjective and we will have more to say about that later.

Definition. We define a homomorphism $\varphi_S\colon F^* \to Z$ as follows: If $x \in F^*$, we denote by (x) the principal divisor in I associated to x and set $\varphi_S(x) = \theta_S((x))$. We have an exact sequence

$$1 \to F_S \to F^* \xrightarrow{\varphi_S} Z,$$

and further φ_S restricted to $O_S - \{0\}$ takes on only non-negative values in Z.

Theorem 2. *If F is a function field and $|S| \geqslant 2$, then O_S is P.I.D. if and only if O_S is euclidean with respect to φ_S.*

Proof. Since very euclidean integral domain is P.I.D., we need only show that P.I.D. implies euclidean. To that end assume that O_S is P.I.D. and denote by $I(O_S)$ the group of divisors of F with respect to O_S. We have an exact sequence

$$1 \to I_S \to I \to I(O_S) \to 1.$$

Now if $0 \neq b \in O_S$, we set $D_b = \prod_{P \notin S} P^{V_P((b))}$. Next $D_b I_S / I_S = (b) I_S / I_S$. Further if D is an integral divisor of F such that D is prime to elements of S, then since O_S is P.I.D. there exists $0 \neq b \in O_S$ such that $D = D_b$. Now if D is an integral divisor of F prime to the elements of S and $c, d \in O_S - \{0\}$ such that $(c), (d) \in I(D)$, then $(c)H_S(D) = (d)H_S(D)$ if and only if $V_P((cd^{-1}-1)) \geqslant V_P(D)$ for $P \notin S$ and $V_P(D) > 0$, i.e. $V_P((c-d)) \geqslant V_P(D)$ for $P \notin S$, since $V_P(d) = 0$ for all $P, P \mid D$. Thus $(c)H_S(D) = (d)H_S(D)$ if and only if there exists $u \in F_S$ such that $c \equiv ud \bmod bO_S$, where $D = D_b$, $b \in O_S$. So in particular if $0 \neq \pi \in O_S$ such that the non-zero residue classes of O_S modulo πO_S are representable by elements of F_S then $D_\pi = P \in M_S$ and conversely. Let $a, b \in O_S - \{0\}$ such that $(a, b) = 1$, then the principal divisor (a) of F represents a divisor class C_a of $I(D_b)$ modulo $H_S(D_b)$. By Theorem 1 there exists $P \in M_S$ such that $P \in C_a$ hence there exists $\pi \in O_S$ such that $D_\pi = P$ and there exists $u \in F_S$ such that $a = u\pi \bmod bO_S$.

We set $A = O_S$ and recall the notation of Section 1, $A_0, A_1, A_2, \ldots$ What we have shown above is the following

(A) $\pi \in A_2 - A_1$ if and only if $D_\pi \in M_S$.

(B) If $a, b \in A - \{0\}$ such that $(a, b) = 1$, then there exists $x \in A_2$ such that

$$a \equiv x \bmod bA.$$

Our objective is to show that if $0 \neq b \in A$ and $a \in A$, then $a \equiv 0 \bmod bA$ or $a \equiv x \bmod bA$, where $\varphi_S(x) < \varphi_S(b)$. Now if $\varphi_S(b) \leqslant 1$, then $b \in A_2$ and our result is immediate. So assume $\varphi_S(b) > 1$. If $a \in A$ and $a \equiv 0 \bmod bA$ or $(a, b) = 1$, we have by (B) that there exists $x \in A_2$ such that $a \equiv x \bmod bA$, where $x = 0$ or $\varphi_S(x) \leqslant 1 < \varphi_S(b)$. So assume that $a \not\equiv 0 \bmod bA$ and $(a, b) = b_0$, where $\varphi_S(b_0) > 0$. We can now write $a = a_0 b_0$ and $b = b_0 b_1$, with $(a_0, b_1) = 1$ and $\varphi_S(b_1) \geqslant 1$. If $\varphi_S(b_1) = 1$, then by (A) there exists $u \in F_S$ such that $a_0 \equiv u \bmod b_1 A$ and thus $a \equiv ub_0 \bmod bA$, where $\varphi_S(ub_0) = \varphi_S(b_0) < \varphi_S(b)$. Finally if $\varphi_S(b_1) > 1$, then there exists $x \in A_2$ such that $x \neq 0$ and $a \equiv xb_0 \bmod bA$, with $\varphi_S(xb_0) = \varphi_S(b_0) + \varphi_S(x) \leqslant \varphi_S(b_0) + 1 < \varphi_S(b)$. Q.E.D.

Corollary 1. *Let F be a function field and S a finite non-empty set of prime divisors such that $|S| \geqslant 2$ and O_S is P.I.D. We claim that φ_S is the minimal algorithm on O_S.*

Proof. Let $A = O_S$ and recall the notation of Section 1, $A_0, A_1, A_2, \ldots$ Since O_S is euclidean $\bigcup_{n=0}^{\infty} A_n = A$ and the minimal algorithm φ is defined on A as follows: for each $n \geqslant 0$, we have $A_n \subseteq A_{n+1}$ and if $0 \neq x \in A$, then there exists unique $n \geqslant 0$ such that $x \in A_{n+1} - A_n$, where $\varphi(x) = n$. Next if $0 \neq \pi \in A$ and πA is a prime ideal, we have two cases, $D_\pi \in M_S$ or $D_\pi \notin M_S$. If $D_\pi \in M_S$, then by (A) of Theorem 2, $\pi \in A_2 - A_1$ and since $\varphi_S(\pi) = \theta_S(D_\pi) = 1$, $\varphi(\pi) = \varphi_S(\pi)$. Next if $D_\pi \notin M_S$, then by (B) of Theorem 2, $\pi \in A_3 - A_2$ and again $\varphi(\pi) = \varphi_S(\pi)$. Finally suppose $0 \neq b \in A$ and let $b = \pi_1\pi_2 \ldots \pi_r$ be a prime factorization of b. By [8], pp. 291, we have $\varphi(b) \geqslant \varphi(\pi_1) + \varphi(\pi_2) + \ldots + \varphi(\pi_r)$ and since $\varphi_S(\pi_i) = \varphi(\pi_i)$ for $1 \leqslant i \leqslant r$, $\varphi(b) \geqslant \varphi_S(b)$. However since φ is minimal algorithm on A and

A is euclidean with respect to φ_S, $\varphi(b) \leqslant \varphi_S(b)$ for all $b \in A$ such that $b \neq 0$. Q.E.D.

THEOREM 3. *Let F be a function field and S a finite non-empty set of prime divisors of F such that O_S is P.I.D., but not euclidean. Let k denote the exact field of constants of F and g_F the genus of F, then F is isomorphic to one of the following fields: $k(x, y)$, where $x \notin k$ and*

1) $|k| = 2$, $g_F = 1$ *and* $y^2+y = x^3+x+1$, *or*
2) $|k| = 3$, $g_F = 1$ *and* $y^2 = x^3+2x+2$, *or*
3) $|k| = 4$, $g_F = 1$ *and* $y^2+y = x^3+\eta$, *where η is a generator of the multiplicative group of k, or*
4) $|k| = 2$, $g_F = 2$ *and* $y^2+y = x^5+x^3+1$.

Further in each case $O_S = k[x, y]$.

Proof. In view of Theorem 2, $|S| = 1$. Further if $S = \{P\}$, then by a relation of F. K. Schmidt (see [9]), $(\deg P)h \mid h_S$, where h is the class number of F. Thus because $h_S = 1$, we have $h = \deg P = 1$. Further $g_F > 0$, since otherwise O_S would be isomorphic to the polynomial ring in one variable over k which is clearly euclidean. Thus according to [4], F must be isomorphic to one of the 4 fields mentioned in the statement of the theorem. Now if P_∞ denotes the pole divisor of x in F, $S = \{P_\infty\}$, since F can have only one prime of degree one. Thus the only possibility, in each case, is that $O_S = k[x, y]$. Now since the $k[x, y]$ are evidently P.I.D. it remains to show that they are not euclidean. To that end set $A = k[x, y]$. What we have seen above is that A has no prime ideal of degree one, but the units of A are evidently $k^* = k-\{0\}$. Hence $A_0 = \{0\}$, $A_1 = k$, but $A_2 - A_1 = \emptyset$ and thus $A' = \bigcup_{n=0}^{\infty} A_n \neq A$. Q.E.D.

Remark 2. Now let F be a number field. The evidence is that Theorem 1 and 2 are true in this case. In fact the arguments in [11] seem to generalize easily and give both theorems modulo the generalized Riemann Hypothesis. Given the truth of Theorem 1 an analogue of Theorem 3 is that the only O_S which are P.I.D. but not euclidean are the rings of integers in the imaginary quadratic number fields $Q(\sqrt{-19})$, $Q(\sqrt{-43})$, $Q(\sqrt{-67})$ and $Q(\sqrt{-163})$.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Lecture Notes, Institute for Advanced Study.

[2] H. Bilharz, *Primdivisoren mit Vorgegebener Primitivwurzel*, Math. Ann. 114 (1937), pp. 476–492.

[3] S. Lang, *Algebraic Number Theory*, 1970.

[4] J. R. Leitzel, M. Madan, and C. Queen, *Algebraic function fields of small class number*, to appear in Journal of Number Theory.

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

[6] T. Motzkin, *The Euclidean Algorithm*, Bull. Amer. Math. Soc. 55 (1949), pp. 1142–1146.

[7] 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.

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

[9] F. K. Schmidt, *Analytische Zahlentheorie in Korpern der Charakteristik p*, Math. Zeitschr. 33 (1931), pp. 1–32.

[10] A. Weil, *Sur les courbes algebriques et les variétés ques s'en deduisent*, Actual. Scientif. Industr., 1041 (1948).

[11] P. Weinberger, *On Euclidean Rings of Algebraic Integers*, A. M. S. Proceedings of Symposium on Analytic Number Theory, #24 (1973).

DEPARTMENT OF MATHEMATICS
LEHIGH UNIVERSITY
Bethlehem, Pennsylvania

Received on 8. 9. 1973 (450)