"ON THE NUMBER OF REMAINDERS IN EUCLIDEAN DOMAINS"

RAJ K. MARKANDA

§1) INTRODUCTION: The purpose of this note is to discuss two classes of euclidean domains, namely: those in which the number of remainders is always finite and those in which the number is always infinite. It is well known that in the polynomial ring $k[x]$, over any field k, the remainder is always unique and that in the ring of integers Z one always gets exactly two remainders. Indeed, these rings are characterized by these properties as shown by Jodeit [2] and Galovich [1]. In Theorem 2.1 we show that in the ring of integers of the complex euclidean quadratic fields $Q(\sqrt{-d})$, the number of remainders is less than or equal to 4. As a corollary to Theorem 2.3, we show that the number of remainders is always infinite in the ring of integers of any euclidean field different from the fields of Theorem 2.1. We connect this result with the existence of an infinite number of solutions of a certain type of diophantine equations. In section 3, we show that one always gets an infinite number of remainders in any ring of fractions of a euclidean domain with respect to a non-trivial multiplicative subset.

§2) Let A be a domain with a multiplicative function $\phi: A \to \{0\} \cup \mathbb{N}$. Let K be the quotient field of A. Then

ϕ can be extended to K by setting $\phi_1 (\frac{a}{b}) = \frac{\phi(a)}{\phi(b)}$ for all $\frac{a}{b}$ in K with a,b in A and $a \neq 0$. We set $\phi_1(0) = \phi(0) = 0$. The following is a well known result:

LEMA 2.1. The domain A is euclidean with respect to ϕ if and only if given $\frac{a}{b}$ in K there exists q in A such that $\phi_1 (\frac{a}{b} - q) < 1$.

We use this to prove the following.

THEOREM 2.1. Let A be the ring of integers of the euclidean complex field $\mathbb{Q}(\sqrt{-d})$. Then the maximum number of remainders in the euclidean algorithm of A is 4.

PROOF. Case (i) $A = \mathbb{Z}[\sqrt{-d}]$ and d = 1 or 2. Then A is euclidean for the multiplicative function $\phi(m+n\sqrt{-d}) = m^2 + dn^2$. Let a,b be in A with $b \neq 0$ and such that b dues not divide a. Then, by lemma 2.1, there exists q in A such that

$$\phi_1(\frac{a}{b} - q) < 1 .$$

Set

(1) ..... $C = \frac{a}{b} - q = s+t\sqrt{-d}$

Then $\phi_1(s+t\sqrt{-d}) = s^2 + t^2 d < 1$ and $bc = r$ is a remainder in the division of a by b. Let r_1 be any other remainder in the division of a by b i.e.

there exists q_1 in A such that

$$a = bq_1 + r_1$$

with $\phi(r_1) < \phi(b)$. Set

(2) ..... $C_1 = \frac{r_1}{b} = \frac{a}{b} - q_1$

From (1) and (2) we get

$$\begin{aligned} C_1 &= (q - q_1) + C \\ &= (q - q_1) + s + t\sqrt{-d} \\ &= (x + s) + (y + t)\sqrt{-d} \end{aligned}$$

where $q-q_1 = x + y\sqrt{-d}$ is in $Z|\sqrt{-d}|$.

Then $\phi_1(C_1) < 1$ implies that

(3) ...... $(x + s)^2 + d(y + t)^2 < 1$

There are only 4 possible solutions of (3) with x and y in Z, for example, if $s > 0$ and $t < 0$ then the only possible solutions are $x = 0$, $y = 0$; $x = -1$, $y = 0$; $x = 0$, $y = 1$; $x = -1$, $y = 1$. Now the result follows from this observation.

Case (ii) $A = Z\left[1, \frac{1+\sqrt{-d}}{2}\right]$ with $d = 3$, 7 or 11. The proof is similar to case (i).

Theorem 2.2. Let A be a euclidean domain with respect to ϕ such that $\phi(a) = \phi(ua)$ for every a in A and every unit u of A.

(i) Let r be a remainder in a division by an element $b \neq 0$ of A. Let u be a unit of A such $1 \equiv u$ (mod b). Then ur is also a remainder in a division by b.

(ii) Let a,b be in A, $b \neq 0$ and such that a and b are relatively primes. Let u be a unit of A and r be a remainder in a division of a by b. Then ur is also a remainder in the division of a by b if and only if $1 \equiv u$ (mod b).

PROOF: Let a,q be in A such that

$$a = bq + r$$

with $\phi(r) < \phi(b)$. Let u be a unit of A such that $1 - u = bc$. For some c in A. Then $r - ur = bc$ and

$$\begin{aligned} a &= bq + r \\ &= bq + bc + ru \\ &= bq + bc + ru \\ &= b(q + c) + ru \end{aligned}$$

with $\phi(ur) = \phi(r) < \phi(b)$.

Thus ur is also a remainder in a division by b.

(2) The if part follows from part (i). Now suppose that

$$a = bq + r$$

and $$a = bq + ur$$

With $\phi(r) = \phi(ur) < \phi(b)$.

Since $r \equiv a(\text{mod } b)$, r is prime to b and from $(1-u)\, r \equiv 0(\text{mod } b)$, it follows that $1 \equiv u(\text{mod } b)$.

COROLLARY 2.1. Let A be a euclidean domain with respect to a multiplicative algorithm ϕ. Let a,b be in A with $b \neq 0$ and so that b does not divide a. Let g.c.d. $(a,b) = d$. Set $a = a_1 d$, $b=b_1 d$ and let u be a unit of A and r be a remainder in the division of a by b. Then ur is also a remainder in the division of a by b if and only if $1 \equiv u(\text{mod } b_1)$.

PROOF: Similar to part (2) of Theorem 2.2.

Now we give sufficient conditions for the existence of an infinite number remainders.

THEOREM 2.3. Let A be a euclidean domain such that A^*, the group of units of A, is infinite and $A/_{Ab}$ is finite for all $b \neq 0$ in A. Then the number of remainders in the division algorithm of A is always infinite.

PROOF: The set $\{ u \in A^*: \ u \equiv 1 \ (\text{mod } b)\}$

= Kernel of the group homomorphism $A^* \to (\frac{A}{Ab})^*$ is infinite and whence the result follows from Theorem 2.2, (1).

<u>COROLLARY 2.2</u>. Let A be a euclidean ring of integers of a number field such that the number of units of A is infinite (this is always true except for the 5 cases of Theorem 2.1). Then one always gets an infinite number of remainders in A. In particular, one always gets an infinite number of remainders in A if

(i) $A = Z[\sqrt{d}]$ for $d = 2,3,6,7,11,19$

(ii) $A = Z[1, \frac{1+\sqrt{d}}{2}]$ for $d = 5,13,17,21,29,33,37,41,57,73$

<u>PROOF</u>: Recall that for $b \neq 0$ in A,

$$\#(A/_{Ab}) = \text{norm}\ (b)$$

and now apply Theorem 2.3.

<u>COROLLARY 2.3</u>. Let $r \geq 2$ be any integer. Let a and b be any two integers such that r does not divide $a + b\sqrt{d}$ or $a + b.\frac{1+\sqrt{d}}{2}$ according as $d \equiv 2,3 \pmod 4$ or $d \equiv 1 \pmod 4$. Then

(i) for $d = 2,3,6,7,11,19$

the diophantine equation

(4) .... $(rx + a)^2 - d(ry + b)^2 = k$

has an infinite number of solutions for some k in Z such that $|k| < r^2$.

(ii) for $d = 5,13,17,21,29,33,37,41,57,73$ the diophantine equation

5) ..... $(r(2x + y) - (2a + b))^2 - d\,(y + b)^2 = 4k$

has an infinite number of solutions for some k in Z with $|k| < r^2$.

Conversely, existence of solutions of (4) or (5) for any $r \geq 2$, a,b in Z such that r does not divide $a + b\sqrt{d}$ or $a + b\frac{1 + \sqrt{d}}{2}$ implies that $Z[\sqrt{d}]$ or $Z[1, \frac{1 + \sqrt{d}}{2}]$ is euclidean for the norm function.

PROOF: Existence of a solution of (4) or (5) is equivalent to the euclideaness of $Z[\sqrt{d}]$ or $Z[1, \frac{1 + \sqrt{d}}{2}]$. Now the solutions of (4) are just the remainders in the division of $a + b\sqrt{d}$ by r and hence (4) has an infinite number of solutions by corollary 2.2. Similarly one can reason for (5).

NOTE 2.1. (i) If the number of remaindrs in a euclidean domain A is always infinite then necessarily A^* is infinite. To show this let P be a prime of A such that remainders in any division by P are always units. Now consider the division of P^2+1 by P. Then $P^2+1 \equiv u \pmod{P}$ for an infinite number of units u of A.

(ii) Let $a = 4 + 3.\sqrt{2}$ and $b = 3$. Then $r_1 = 1$ and $r_2 = 4 + 3.\sqrt{2}$ are two remainders in the division of a by b but r_{1}/r_{2} is not a unit in $Z[\sqrt{2}]$.

§3) Let B be a euclidean domain euclidean for the function ϕ such that $\phi(a) + \phi(b) \leq \phi(ab)$ for all a,b in B with $ab \neq 0$. Let S be a multiplicatively closed saturated subset of B such that S contains atleast one prime p of B. Then the ring $A = \{s^{-1}a: s \in S, a \in B\}$ of fractions of B with respect to S is euclidean for the function ϕ' defined as follows: write any x in A as $x = \frac{s}{t}a$ with s,t in S and a in B such that a is prime to all elements of S. Set $\phi'(x) = \phi(a)$. Notice that a is uniquely determined upto units in B as it is a unique factorisation domain.

<u>THEOREM 3.1.</u> The ring A is euclidean for algorithm ϕ' and one always gets an infinite **number** of remainders.

<u>PROOF</u>. Let x,y be in A with $y \neq 0$ such that y does not divide x. We can write $x = \frac{s}{t}a$ and $y = \frac{s_1}{t_1}b$ for some s, t, s_1, t_1 in S and a,b in B prime to all elements of S. Let $m \geq 0$ be any integer. Then $p^m a$ and b are in B and thus there exist q'_m and r'_m in B such that

$$p^m a = q'_m b + r'_m$$

with $r'_m \neq 0$ and $\phi(r'_m) < \phi(b)$.

Thus

$$x = \frac{sa}{t} = \frac{t_1 \ sq_m'}{p^m \ s_1 t} \cdot \frac{s_1 \ b}{t_1} + \frac{sr_m'}{t \ p^m}$$

$$= q_m \ y + r_m$$

where $q_m = \dfrac{t_1 \ sq_m'}{p^m \ s_1 t}$, $r_m = \dfrac{sr_m'}{t \ p^m}$

and $\phi'(r_m) \leq \phi(r_m') < \phi(b) = \phi'(y)$. Thus A is euclidean for ϕ'.

Now we show that for a given $m \geq 0$ there exists $n > m$ such that $r_n \neq r_m$ and thus the number of remainders in A is always infinite. Suppose that $r_n = r_m$ for all $n > m$. Then $\dfrac{sr_n'}{tp^n} = \dfrac{sr_m'}{tp^m}$ i.e. $r_n' = p^{n-m} r_m'$ for all $n > m$

But then

$$\phi(r_m') + (n-m)\phi(p) \leq \phi(p^{n-m} r_m') = \phi(r_n') < \phi(b) \text{ for all } n > m$$

which is a contradiction as $\phi(b)$ is finite. In fact we have proved that if m_o is the least integer such that $m_o \ \phi(p) \geq \phi(b)$ then $\{r_{km_\theta}\}_{k \geq 0}$ is an infinite set of distinct remainder in a division of a by b.

ACKNOWLEDGEMENTS. We are thankful to J.J. Hiblot for suggesting Theorems 2.2(i) and 2.3. We would also like to thank Pierre Samuel for encouragement and many improvements in the preliminary version of this paper.

R E F E R E N C E S

(i) S.GALOVICH. "A characterization of the integers among euclidean domains" A.M.M. 85 (1978), 572-575.

(ii) N.A. JODEIT, " Uniqueness in the division algorithm" A.M.M.74 (1967) 835-836.

UNIVERSIDAD DE LOS ANDES

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICA

MERIDA - VENEZUELA