ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 4, 2006

THE MINIMAL GENERATING SETS OF THE MULTIPLICATIVE MONOID OF A FINITE COMMUTATIVE RING

DAVID E. DOBBS AND BRIAN C. IRICK

ABSTRACT. For any finite commutative multiplicative monoid S with an element 0 such that $S0 = \{0\} \neq S$, some decompositions of S are given as the disjoint union of a submonoid of S and some prime ideals of some submonoids of S. These decompositions lead to an algorithm producing all the minimal generating sets of S in terms of semigroup-theoretic generating sets of minimal prime ideals of some submonoids of S and minimal generating sets of the group of invertible elements of S. This algorithm is applied in case S is the multipicative monoid of a finite nonzero commutative ring R. For any such R, each application of the algorithm terminates in the same number of steps, namely, the number of prime ideals of R, that is, the number of minimal prime ideals of S.

1. Introduction. All rings considered below are commutative with identity; all semigroups and monoids considered below are commutative. Our interest is in developing some semigroup- and monoid-theoretic results that have applications to ring theory. Perhaps the most useful monoid associated to a ring R is the *multiplicative monoid* of R, i.e., the structure consisting of the underlying set of R and its binary operation of multiplication. One sees this topic in the current *renaissance* in factorization theory, but it was already apparent in Jacobson's approach to unique factorization domains via Gaussian monoids [**7**, pp. 115–127].

In dealing with the semigroup-ring interface, one must exercise caution, as the semigroup-theoretic ideal theory of S may differ from the ring-theoretic ideal theory of R. A result of Aubert [**3**] characterizes the rings R such that each (semigroup-theoretic) ideal of S is an (ring-theoretic) ideal of R. One such class of rings consists of the special principal ideal rings, or SPIRs; this follows from a well-known factorization result [**10**, Example, p. 245]. (Recall from [**10**, p. 245] that a ring R is called an SPIR in the case where R is a quasilocal principal ideal

Received by the editors on July 7, 2003, and in revised form on May 19, 2004.