

## Some notes on relative primality

written by rapha on Functor Network

original link: <https://functor.network/user/2593/entry/1045>

---

Recall that one may define relative primality of a pair of elements in full generality: let  $M$  be a monoid, and let  $f$  and  $g$  be two elements of  $M$ . We say  $f$  and  $g$  are **relatively prime** if all common divisors of  $f$  and  $g$  are units. Formally:  $\forall d \in M, d \mid f \wedge d \mid g \Rightarrow d \in M^\times$ .

However, we will work in the more restricted setting of a commutative ring  $A$  with identity. As we get more and more specialized types of rings, we get better and better characterizations of relative primality.

**In integral domains.** In this setting, the divisibility relation is more meaningful, and we have: two elements  $f$  and  $g$  are relatively prime if, and only if, for any element  $d$ , the containment  $(f, g) \leq (d)$  implies  $(d) = (1)$ . In effect, this says the ideal  $(f, g)$  generated by  $f$  and  $g$  is “bigger” than any non-trivial principal ideal in the ring.

**In GCD domains.** Recall that a GCD domain is an integral domain where a greatest common divisor for any pair of elements is guaranteed to exist. In other words, there is always a unique minimal principal ideal containing  $(f, g)$ . Together with the previous characterization in integral domains, this yields: two elements  $f$  and  $g$  are relatively prime if, and only if, a greatest common divisor of  $f$  and  $g$  is 1.

**In unique factorization domains.** Two elements  $f$  and  $g$  are relatively prime if, and only if, for every *irreducible* element  $h$ , we fail to have the containment  $(f, g) \leq (h)$ . For this to work, we in fact only need the existence of at least one irreducible factor for every non-zero non-unit element, so this characterization could work in more general types of rings.

**In principal ideal domains.** Now the situation is maybe as good as it gets, theoretically speaking. Two elements  $f$  and  $g$  are relatively prime if, and only if, the two ideals  $(f)$  and  $(g)$  are comaximal, i.e.  $(f) + (g) = (1)$ . This is a strengthening of the previous characterization on GCD domains (recall that every PID is a UFD, hence is a GCD domain). Of course,  $(f) + (g)$  is just a fancier way of writing  $(f, g)$ . Most of the time, the equation  $(f) + (g) = (1)$  is called *Bézout’s Identity*.