Section 4.3: Relatively Prime Integers

Let a and b be integers, not both zero (so $\gcd(a,b)$ exists). Let $d = \gcd(a,b)$ and let

$$S = \{\, c \in \mathbf{Z} \,|\, \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \,\}.$$

We have seen, in Theorem 5 of Section 4.2, that $c \in S$ if and only if d divides c; that is, S consists of all integer multiples of d. Thus, an alternate description of S is

$$S = \{\, md \,|\, m \in \mathbf{Z} \,\}.$$

The following theorem is an immediate consequence of this observation.

Theorem 1: Let a and b be integers, not both zero. Let $d = \gcd(a,b)$ and let

$$S = \{\, c \in \mathbf{Z} \,|\, \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \,\}.$$

Then d is the smallest positive integer in S.

Example 1: Let a and b be integers, not both zero. Suppose there exist integers m and n such that $15 = ma + nb$. What are the possibilities for $\gcd(a,b)$.

Solution: If $d = \gcd(a,b)$ then, by Theorem 5 of Section 4.2, d is a positive divisor of 15. Thus, the choices for d are 1, 3, 5, and 15.

Exercise 1: Let a and b be integers, not both zero. Suppose $\gcd(a,b) < 10$ and there exist integers m and n such that $17 = ma + nb$. What are the possibilities for $\gcd(a,b)$.

Definition 1: Let a and b be integers, not both zero. Then a and b are **relatively prime** provided $1 = \gcd(a,b)$.

Example 2: The integers 15 and 22 are relatively prime and $1 = (-2)22 + (3)15$.

Theorem 2: Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers m and n such that $1 = ma + nb$.

Proof: Note that Theorem 2 is an equivalence, so two proofs are required.

First, let a and b be integers, not both zero, and suppose a and b are relatively prime. Then $1 = \gcd(a, b)$ so, by Theorem 4 of Section 4.2, there exist integers m and n such that $1 = ma + nb$.

In the other direction, let a and b be integers, not both zero, and suppose there exist integers m and n such that $1 = ma + nb$. If $S = \{ c \in \mathbf{Z} \mid \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \}$ then we are assuming that $1 \in S$. Let $d = \gcd(a, b)$. By Theorem 1, d is the smallest positive integer in S. Clearly 1 is the smallest positive integer there is. Since $1 \in S$ and d is the smallest positive integer in S, it follows that $d = 1$.

Exercise 2: Determine whether the following statement is true or false:

For all integers a, b, and c, if a divides bc then either a divides b or a divides c.

Theorem 3: For all integers a, b, and c, if a divides bc and $\gcd(a, b) = 1$, then a divides c.

Proof: Let a, b, and c be integers. Suppose that a divides bc and $\gcd(a, b) = 1$. Since a divides bc, there exists an integer k such that $bc = ak$. Since $\gcd(a, b) = 1$, by Theorem 2 (or by Theorem 4 of Section 4.2), there exist integers m and n such that $1 = ma + nb$. Multiplying by c gives $c = mac + nbc$. This gives

$$c = mac + nbc = mac + nak = (mc + nk)a; \text{ that is, } c = qa \text{ where } q = mc + nk.$$

This proves that a divides c.

Example 3: Let k be an integer such that 12 divides $35k$. Since 12 and 35 are relatively prime, it follows from Theorem 3 that 12 divides k.

Exercise 3: Let a be an integer and let p be a prime integer. List all possibilites for $\gcd(a, p)$.

Theorem 4: Let a be an integer and let p be a prime integer. Then either p divides a and $p = \gcd(a, p)$ or a and p are relatively prime.

Proof: Let a be an integer and let p be a prime integer. Set $d = \gcd(a, p)$. Then d is a positive integer divisor of p so either $d = p$ or $d = 1$. If $d = p$ then it follows that p divides a (since d divides a). If $d = 1$ then a and p are relatively prime.

Exercise 4: Let n be a positive integer such that 7 divides $3n$ and $25 \leq 3n \leq 60$. Determine the value of $3n$.

Theorem 5: Let a and b be integers. If p is a prime integer such that p divides ab, then either p divides a or p divides b.

Proof: We will prove the equivalent formulation:

If p is a prime integer such that p divides ab and p does not divide a, then p divides b.

Thus, assume that p divides ab and p does not divide a. By Theorem 4, a and p are relatively prime. By Theorem 3, p divides b.

Exercise 5: Let p and q be distinct prime integers such that $15p = 35q$. Find values for p and q and prove that those are the only values possible.

Section 4.3. EXERCISES

4.3.1. Let a and b be integers, not both 0, and let d be a positive integer that divides both a and b. Then there exists integers a_1 and b_1 such that $a = a_1 d$ and $b = b_1 d$.

Prove that $d = \gcd(a, b)$ if and only if $1 = \gcd(a_1, b_1)$.

4.3.2. Let a, b, and n be integers such that $1 = \gcd(a, n)$ and $1 = \gcd(b, n)$. Prove that $1 = \gcd(ab, n)$.

4.3.3. Let p be a prime integer. Prove by induction that for every integer $n \geq 2$, if a_1, a_2, $\ldots$, a_n are integers such that p divides the product $a_1 a_2 \cdots a_n$ then there exists an integer i such that $1 \leq i \leq n$ and p divides a_i.