Divisibility of Products

1. First Result

The following result is a weaker version of a standard result involving greatest common divisors. We will prove the stronger result at the end of these notes.

Proposition 1.1. *Suppose that a and b are integers which have the property that if $d \in \mathbb{N}$ and d divides a and d divides b then $d = 1$. Then there are integers x and y such that:*

$$ax + by = 1$$

It should be pointed out that it is not the case that $a = 0$ and $b = 0$, otherwise every integer divides a and b.
Proof: Since $a^2 + b^2$ is a positive integer, the set

$$S = \{ax + by \mid x \in \mathbb{Z}, y \in \mathbb{Z} \text{ and } ax + by > 0\}$$

is non-empty. The well-ordering principle guarantees that there is a least element d in S. Using the division algorithm, we can write

$$a = qd + r$$

where $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, d - 1\}$. Then

$$a - r = qd.$$

Since $d = ax + by$ for some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,

$$qd = qax + qby$$

So

$$a - r = qax + qby$$

$$a - qax - qby = r$$

$$a(1 - qax) + b(-qy) = r$$

Since $r < d$, and d is a least element of S, the only possible value for r is $r = 0$. In particular, d divides a. Repeating this same argument with b in place of a shows that d divides b. Therefore, by the hypothesis, $d = 1$.
$\square$

Proposition 1.2. *Suppose that a and b are integers which have the property that if $d \in \mathbb{N}$ and d divides a and d divides b then $d = 1$. If c is an integer and a divides bc, then a divides c.*

Proof: From the proposition above, there are integers x and y such that $ax + by = 1$. Then $axc + byc = c$. So $(xc)a = c - (y)bc$. In particular, a divides $c - (y)bc$. Since a divides bc, a must divide c. $\square$

corollary 1.3. *Suppose that x and y are integers and that p is a prime such that p divides xy. Then p divides x or p divides y.*

Proof: If p divides x then the result is true, so we may assume that p does not divide x. Then p and x satisfy the conditions for a and b, respectively of the previous proposition. In particular, p must divide y ($y = c$ in the referenced proposition). $\square$

2. General Result

Definition 2.1. *Suppose that a and b are integers. We say that the whole number d is a* **common divisor** *of a and b if d divides a and b. We say that d is the* **greatest common divisor** *of a and b if*

(1.) *d is a common division of a and b and*

(2.) *if c is any common divisor of a and b then c divides d.*

At this point, there is no guarantee that $\gcd(a, b)$ exists for any pair of integers a and b.

Proposition 2.2. *Let a and b be integers. Then*

(1.) *There exists a whole number $d = \gcd(a, b)$.*

(2.) *There exists integers x and y such that $ax + by = \gcd(a, b)$.*

The proof of this theorem is nearly identical to the first proposition in these notes, with the exception that we are working with whole numbers rather than natural numbers.

Proof: Since $a^2 + b^2$ is a non-negative integer, the set

$$S = \{ax + by \mid x \in \mathbb{Z}, y \in \mathbb{Z} \text{ and } ax + by \geq 0\}$$

is non-empty. The well-ordering principle guarantees that there is a least element d in S. Using the division algorithm, we can write

$$a = qd + r$$

where $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, d - 1\}$. Then

$$a - r = qd.$$

Since $d = ax + by$ for some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,

$$qd = qax + qby$$

So

$$a - r = qax + qby$$

$$a - qax - qby = r$$

$$a(1 - qax) + b(-qy) = r$$

Since $r < d$, and d is a least element of S, the only possible value for r is $r = 0$. In particular, d divides a. Repeating this same argument with b in place of a shows that d divides b. We have now shown that d is a common factor of a and b. Now suppose that c is any integer that divides both a and b. Then c divides $ax + by$ so c divides d. Thus $d = \gcd(a, b) = ax + by$. $\square$