Section 2: Divisibility and Unique Factorization

In Section 1.1, we were introduced to the notion of divisibility. We say that a *divides* b (denoted by $a \mid b$) if there exists an integer c such that $ac = b$. So 2 divides 10, but not 11. Another idea closely related to divisibility is that of factorizations. If we represent a number by the product of all prime numbers that divide it, we are using the prime factorization of the number. For example, $10 = 2 \cdot 5$ and $16,500 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 11$. Of course we usually utilize exponents to make this less cumbersome, so that $16,500 = 2^2 \cdot 3 \cdot 5^3 \cdot 11$.

Theorem 1.2.1 If a, b, and d are integers, then $a \mid b$ if and only if $ad \mid bd$.

Proof: $(\Rightarrow)$ Suppose that $a \mid b$. Then there exists a natural number c such that $b = ac$. Then $bd = ac \cdot d = ad \cdot c$ also, which gives us $ad \mid bd$.

$(\Leftarrow)$ Suppose that $ad \mid bd$. Then there exists a natural number c such that $bd = ad \cdot c$. Dividing both sides by d yields the desired result. ■

Exercise 1.2.2 Let a, b, and d be integers.
(1) If $d \mid a$, then $d \mid ab$.
(2) If $d \mid a$ and $d \mid b$, then $d \mid (a \pm b)$.
(3) If $d \mid (a+b)$ and $d \mid a$, then $d \mid b$.

Given two integers, we often will want to know their ***greatest common divisor*** **(GCD).** We denote the greatest common divisor of a and b by $\gcd(a,b)$.

Theorem 1.2.3 Let a and b be integers. Then there exist integers x_0 and y_0 such that $\gcd(a,b) = ax_0 + by_0$.

In the proof that follows, I have left out some of the reasoning. In Exercise 1.2.4 you are asked to provide the missing reasons.

Proof: Define the set S to be the set of all positive linear combinations of the numbers a and b. In other words, define $S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$. This set is non-empty. (WHY?) Therefore, by the WOP, it has a smallest element. Call the smallest element d. Since $d \in S$, there exist integers x_0, y_0 such that $d = ax_0 + by_0$. We will show that $d = \gcd(a,b)$. Since d divides both a and b (WHY?), it is a common divisor of a and b. Now, let m be any other common divisor of a and b. Clearly m divides d (since m divides *every* element of S (WHY?)). Therefore, d is the *greatest* common divisor of a and b. (WHY?) ■

Exercise 1.2.4 There are four statements in the previous proof followed by "WHY?" Explain all four.

This last proof is an example of an existential proof. It proves that the integers x_0 and y_0 exist, but does not show how to find them. In fact, we have not yet seen a good method for finding the greatest common divisor of two numbers. One method for finding this requires writing each numbers prime factorization, but this can be a difficult task (especially if the numbers are very large). A second method, called the Euclidean Algorithm, often proves more useful. Indeed, it can even be used to find the integers x_0 and y_0 used in the linear combination of Theorem 1.2.3.

Theorem 1.2.5 (The Euclidean Algorithm) Let a and b be natural numbers with $a < b$. Let r_1 be the remainder obtained by dividing b by a, let r_2 be the remainder obtained by dividing a by r_1 (recall that $r_1 < a$), let r_3 be the remainder obtained by dividing r_1 by r_2, and so on. Then (1) this process must eventually end, i.e. $r_k = 0$ for some natural number k, and (2) the last non-zero remainder in the chain of remainders is $\gcd(a,b)$.

Proof: (1) Since the chain of remainders consists entirely of non-negative integers and is *strictly* decreasing, it must eventually be zero. This follows from a direct application of the Well-Ordering Principle.

(2) To see that the last non-zero remainder is $\gcd(a,b)$, we will use induction. Let $P(n)$ be the proposition: If $r_{n+1} = 0$, then $r_n = \gcd(a,b)$. Consider $n = 1$. We need to show if $r_2 = 0$, then $r_1 = \gcd(a,b)$. Suppose $r_2 = 0$. Then $b = aq_1 + r_1$ and $a = r_1 q_2$. If we make the substitution of $a = r_1 q_2$ in the first equation, we get $b = (r_1 q_2)q_1 + r_1$. So clearly r_1 divides both a and b. Therefore $r_1 \le \gcd(a,b)$. From $b = aq_1 + r_1$, we can also note that $b - aq_1 = r_1$. Since $\gcd(a,b)$ divides both a and b, it must then also divide r_1. So $\gcd(a,b) \le r_1$. Therefore, $r_1 = \gcd(a,b)$, and $P(1)$ is true.

Now assume that $P(k)$ is true, and consider $P(k+1)$. We will assume that $r_{k+2} = 0$ and show that $r_{k+1} = \gcd(a,b)$ follows. Notice that in this case, the algorithm extended $k+2$ iterations (for the division of b by a). Therefore, it extended $k+1$ iterations for the division of a by r_1. So, by our assumption of $P(k)$, we have that $r_{k+1} = \gcd(a, r_1)$. Now, since $b = aq_1 + r_1$, Exercise 1.2.2 implies that r_{k+1} must also divide b. Therefore, r_{k+1} is a common divisor of a and b. So as before we have $r_{k+1} \le \gcd(a,b)$. However, since $\gcd(a,b)$ divides r_1 (which is true since it divides both a and b, and $b = aq_1 + r_1$), we have $\gcd(a,b) \le \gcd(a, r_1) = r_{k+1}$. Therefore, $r_{k+1} = \gcd(a,b)$. ■

So now we have a method for finding the greatest common divisor of two numbers. Additionally, we can utilize the result of this algorithm to identify the integers x_0 and y_0. We will illustrate this with an example.

Example 1.2.6 Find $\gcd(3458, 7605)$ and the coefficients necessary to write it as a linear combination of 3458 and 7605.

Using the Euclidean Algorithm, we get:

$$\begin{aligned} 7605 &= 3458 \cdot 2 + 689 \\ 3458 &= 689 \cdot 5 + 13 \\ 689 &= 13 \cdot 53 + 0 \end{aligned}$$

Therefore, $13 = \gcd(3458, 7605)$. Working backwards through the algorithm, we see that:

$$\begin{aligned} 13 &= 3458 - 689 \cdot 5 \\ &= 3458 - (7605 - 3458 \cdot 2) \cdot 5 \\ &= 3458 - 7605 \cdot 5 + 3458 \cdot 10 \\ &= 3458 \cdot (11) + 7605 \cdot (-5) \end{aligned}$$

So $x_0 = 11$ and $y_0 = -5$ are the required integers.

Of course, with numbers of this size, we could have easily found $\gcd(3458, 7605)$ by using each numbers' prime factorization. Namely, $3458 = 2 \cdot 7 \cdot 13 \cdot 19$ and $7605 = 5 \cdot 9 \cdot 13^2$. From this we can clearly see that $\gcd(3458, 7605) = 13$. But then, we would not have the integral coefficients needed to write 13 as a linear combination of 3458 and 7605.

Exercise 1.2.7 Find the greatest common divisor of 233415 and 273273 and write it as a linear combination of the two numbers.

Writing out the prime factorizations also brings to mind one of the most important results in elementary number theory; the Fundamental Theorem of Arithmetic.

Theorem 1.2.8 (The Fundamental Theorem of Arithmetic - FTA) Every natural number (greater than 1) can be written as a product of primes uniquely, except for the order.

We will not prove this important result now, but I do want to spend a few moments (words, sentences, paragraphs, pages?) discussing *why* it is important. In order to understand this theorem, perhaps we should take a trip to a world of numbers where this property does *not* hold. Let's go visit Twozeeland.

Twozeeland is the set of all even integers. (Get it? $2\mathbb{Z}$ - land.) The set $2\mathbb{Z} = \{..., -6, -4, -2, 0, 2, 4, 6...\}$ is easily understood, but let's think about the following question: what are the "prime elements" in Twozeeland? Obviously since we can still add, subtract, and multiply numbers in Twozeeland (and the results remain in Twozeeland), we must be able to factor. What elements would be unfactorable and therefore prime? To determine this, we must understand what it means for one number to divide another in Twozeeland. We say that a divides b if there exists an element c (of Twozeeland) such that $ac = b$. So 6 divides 12 since $6 \cdot 2 = 12$. But 6 does not divide 18, since there is no element of Twozeeland that will multiply by 6 and yield 18.

So what numbers are prime in Twozeeland? Even integers are prime in Twozeeland if they are not divisible by any other even integer. Some examples are 2, 6, 30, and 174. Notice that numbers in Twozeeland are not even divisible by themselves! What a weird world. But here is the relevant weirdness; we lose unique factorization! Theorem 1.2.8 states that in $\mathbb{Z}$, numbers factor into primes uniquely. But in $2\mathbb{Z}$, notice that $60 = 6 \cdot 10$ (where 6 and 10 are both prime) and $60 = 2 \cdot 30$ (with 2 and 30 both prime). Two different factorizations of the same number. Weird.

So even though the FTA seems obvious and intuitive, it doesn't always hold in different number sets. Keep in mind that the fact that every number has a unique factorization into primes does not mean that such a factorization will be easy to find. Indeed, determining whether a given (large) number is prime or composite (and if composite, then factoring it) are very important topics in elementary number theory. We'll talk more about that later.

Exercise 1.2.9 Give an example to show that the division algorithm also fails in Twozeeland.