"Divide each difficulty into as many parts as is feasible and necessary to resolve it." – Rene Descartes

LECTURE 6

DIVISIBILITY OF INTEGERS

ANDREW MISSELDINE

2.2. The Division Algorithm

Theorem 2.2.1 (The Division Algorithm)**.** *If $a, b \in \mathbb{Z}$ and if $b > 0$, then there are unique integers q and r such that*

$$a = qb + r$$

where $0 \leq r < b$

Proof. Let $S = \{a - bk \mid k \in \mathbb{Z}, a - kb \geq 0\}$, which is a subset of the natural numbers. If $a \geq 0$, then $a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \geq 0$. So, $a - b(2a) \in S$. In either case, S is not empty. By the well-ordering principle, there is a minimal element of S, call it r. Let q be an integer which obtains r, that is, $r = a - bq$.

We claim that $0 \leq r < b$. By definition of S, it must be that $r \geq 0$. Consider the number $a - b(q + 1)$, which is smaller than r. Since r is minimal in S, we can conclude that $a - b(q + 1) < 0$ which implies that $a - bq - b = r - b < 0$ or $r < b$. Therefore, there do exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

To show that these numbers are unique suppose that $a = bq + r$ and $a = bq' + r'$ with $0 \leq r, r' < b$. Without the loss of generality, assume that $r' \geq r$. Removing a from the system of equations, we get $bq + r = bq' + r'$, which implies that $b(q - q') = r' - r \geq 0$. Thus, $b \mid r' - r \leq r' < b$. But the only multiple less than b and greater than or equal to 0 is 0 itself. So, $r' - r = 0$, or $r' = r$. Consequently, $q = q'$ also. Therefore, the numbers q and r are unique. □

While we were able to prove the division algorithm from the well-ordering principle, unfortunately, this argument is a non-constructive proof, that is, although we know q and r exist we do not have any idea what these values are. Fortunately, the long division algorithm from grade school exists (hence the name of the theorem) to help us compute these integers.

Definition 2.2.2. Let a and b be integers. If $b = ak$ for some integer k, we write $a \mid b$. An integer d is called a **common divisor** of a and b if $d \mid a$ and $d \mid b$.

The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d' \mid d$. We say that two integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

Theorem 2.2.3 (Greatest Common Divisor Linear Combination)**.** *Let a and b be nonzero integers. Then there exist integers r and s such that*

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Again the greatest common divisor linear combination theorem can be proven using the well-ordering principle on the set $\{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$, but this proof is again non-constructive. Typically, the Euclidean algorithm is used to construct these values, as is demonstrated in the next example.

Example 2.2.4 (Euclidean Algorithm)**.** Write the greatest common divisor of $a = 945$ and $b = 2415$ as a linear combination of a and b.

The Euclidean algorithm begins by finding $\gcd(a, b)$, which is accomplished by repeated use of the division algorithm:

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0 \end{aligned}$$

Therefore, $\gcd(2415, 945) = 105$.

Next we can use the equations above to build 105 as a linear combination of a and b, working backward. We start at the second to last line.

$$\begin{aligned} 105 &= 525 - 420 \\ &= 525 - (945 - 525) = 2 \cdot 525 - 945 \\ &= 2 \cdot (2415 - 2 \cdot 945) - 945 = 2 \cdot 2415 - 5 \cdot 945 \end{aligned}$$

Therefore, $\boxed{105 = 2a - 5b}$. ■

Corollary 2.2.5. *Let a and b be two integers that are relatively prime. Then there exist integers r and s such that $ar + bs = 1$.*

Definition 2.2.6. Let p be an integer such that $p > 1$. We say that p is a **prime number** if the only positive numbers that divide p are 1 and p itself. An integer $n > 1$ that is not prime is said to be **composite**.

Lemma 2.2.7 (Euclid)**.** *Let a and b be integers and p be a prime number. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. Suppose that $p \nmid a$. Then $\gcd(p, a) = 1$, which implies there are integers r, s such that $ar + ps = 1$. Multiplying both sides by b, we get

$$b = (ab)r + p(bs).$$

Since p divides the RHS of the equation, we conclude that $p \mid b$. Therefore, $p \mid a$ or $p \mid b$. □

Euclid's lemma is one of the most powerful properties of prime numbers. The following two theorems are consequences of Euclid's lemma.

Theorem 2.2.8 (Euclid)**.** *There exist infinitely many prime numbers.*

Proof. Suppose that to the contrary there are only finitely many primes, $p_1, p_2, \ldots, p_r$. Let $q = p_1 p_2 \ldots p_r + 1$. If q is composite, then it must be divisible by some prime number by Euclid's lemma, say p_i. But this implies that $p_i \mid q - p_1 p_2 \ldots p_r = 1$, a contradiction. Thus, q must be a prime number which is larger than p_i for all i, another contradiction. Therefore, there are infinitely many prime numbers. □

Theorem 2.2.9 (Fundamental Theorem of Arithmetic)**.** *Let n be an integer such that $n > 1$. Then*

$$n = p_1 p_2 \ldots p_r,$$

where $p_1, \ldots, p_r$ are primes (not necessarily distinct). Furthermore, this factorization is unique; that is, if

$$n = q_1 q_2 \ldots q_s,$$

then $r = s$ and the q_i's are just the p_i's rearranged.

Homework:
Judson 2.4 : 15, Pick 4 from (16, 20, 22-27)