4. The Division Theorem

We began class by discussing the third homework problem from Tuesday.

**Question:** What observations and conjectures can you make about the sets of integers $4x - 1$, $4x$, $4x + 1$, $4x + 2$, $4x + 3$, and $4x + 4$, where $x$ is an arbitrary integer?

The following observations were made:

- The set of integers of the form $4x$ is the same as the set of integers of the form $4x + 4$.
- The set of integers of the form $4x + 3$ is the same as the set of integers of the form $4x - 1$.
- (Shawn) If $n$ is an odd integer, then every integer in the sets $4x + n$ and $4x - n$ is odd.
- (Lisa A) If $n$ is an even integer, then every integer in the sets $4x + n$ and $4x - n$ is even.
- Every integer is in one of the sets $4x$, $4x + 1$, $4x + 2$, and $4x + 3$.
- No integer is in more than one set among $4x$, $4x + 1$, $4x + 2$, and $4x + 3$.

We made statements similar to the last two about the sets of integers of the form $6x$, $6x + 1$, $6x + 2$, $6x + 3$, $6x + 4$, and $6x + 5$. We think of $x$ as the “quotient” of an integer upon dividing by 6, and the other number (0, 1, 2, 3, 4, or 5) as the “remainder.” This brought us to the division theorem, which basically a statement that long division 'works'. The key axiom we need for the proof is that every non-empty set of nonnegative integers has a smallest element. (This is called the **Well-Ordering Axiom**.)

**Theorem:** (The Division Theorem) Let $a$, $b$ be integers with $b > 0$. Then there exist integers $q, r$ such that $a = bq + r$ and $0 \leq r < b$. Furthermore, for a given $a$ there is only one integer $q$ and one integer $r$ such that $a = bq + r$ and $0 \leq r < b$.

**Proof:** Let $S$ denote the set of all nonnegative integers of the form $a - bx$. As an example, if $a = 20$ and $b = 6$ then $S = \{2, 8, 14, 20, 26, \ldots \}$. We note that $S$ is non-empty. For, let $x$ be any integer less than or equal to $\frac{a}{b}$. Then $bx \leq a$, so $a - bx$ is in $S$. By the well-ordering axiom, $S$ must have a smallest element, call it $r$. As $r \in S$, $r \geq 0$. We claim that $r < b$. If not, then $r \geq b$. But then $r - b$ also in $S$ (if $r = a - bq$ then $r - b = a - b(q + 1)$; also $r - b \geq 0$), contradicting that $r$ is the smallest element in $S$. This means that we must have $r < b$ (to avoid the contradiction). Since $r = a - bq$, $a = bq + r$ and $0 \leq r < b$.

This proves the existence of the integers $q$ and $r$. Equally important is the uniqueness of $q$ and $r$. That is, there are no other integers $s$ and $t$ such that $a = bs + t$ with $0 \leq t < b$. We didn’t have time to prove this in class, but will discuss it later. □

Here are some examples:

**Example:** Let $a = 1150$ and $b = 12$. Then $q = 95$ and $r = 10$. That is, $1150 = 12(95)+10$.

**Example:** Let $a = -28$ and $b = 6$. Then $q = -5$ and $r = 2$. That is, $-28 = 6(-5)+2$.

We then returned to a discussion of the remaining homework problems:

**Question:** Suppose $7 = ax + by$ where $a, b, x, y$ are integers. What are the possible values of $\text{gcd}(a, b)$?

**Answer:** (Hui, Lisa A) Hui gave an example that $\text{gcd}(a, b) = 1$ is possible: namely, $a = 2$, $x = 1$, $b = 5$, $y = 1$. Then $(2)(1) + (5)(1) = 1$ and $\text{gcd}(2, 5) = 1$. Lisa showed that 7 is also
possible: \( a = -7, x = 0, b = 7, \) and \( y = 1. \) Then \((-7)(0) + (7)(1) = 7\) and \(\gcd(-7, 7) = 7.\)

Lisa also gave a proof that 1 and 7 are the only possibilities. Let \( d = \gcd(a, b). \) Then \( a = du \) and \( b = dv \) for some \( u, v \in \mathbb{Z}. \) Then \( 7 = ax + by = dux + dvy = d(ux + vy). \) This shows that \( d|7. \) Since \( d > 0, \) we must have \( d = 1 \) or \( d = 7. \)

We state the last homework problem as a theorem, as it will be used later in the Euclidean Algorithm:

**Theorem:** Suppose \( a = bq + r \) with \( b \neq 0. \) Then \( \gcd(a, b) = \gcd(b, r). \)

**Proof:** Let \( d = \gcd(a, b) \) and \( e = \gcd(b, r). \) Then \( a = dx \) and \( b = dy \) for some integers \( x, y. \) Then \( r = a - bq = dx - dyq = d(x - yq). \) This says that \( d|r, \) and thus \( d \) is a common divisor of \( b \) and \( r. \) Hence, \( d \leq e. \) On the other hand, we have \( b = eu \) and \( r = ev \) for some \( u, v \in \mathbb{Z}. \) Then \( a = bq + r = euq + ev = e(uq + v), \) so \( e|a. \) Thus, \( e \) is a common divisor of \( a \) and \( b, \) so \( e \leq d. \) Hence, \( e = d. \) \( \square \)

How might this theorem be helpful? Well, consider the problem of finding \( \gcd(1150, 12). \)

Dividing 12 into 1150 (using the division theorem), we have \( 1150 = (12)(95) = 10. \) By the theorem, \( \gcd(1150, 12) = \gcd(12, 10), \) which is easily seen to be 2. In fact, we could have repeated the process once more: 12 = (1)(10) + 2, so the same theorem gives that \( \gcd(12, 10) = \gcd(10, 2), \) which again is obviously 2. This suggests a method for calculating the \( \gcd \) of any two integers, called the Euclidean Algorithm: Let \( a \) and \( b \) be positive integers. Dividing \( b \) into \( a \) we get

\[
a = bq_1 + r_1
\]

with \( 0 \leq r_1 < b. \) If \( r_1 \) is not zero, we can divide \( r_1 \) into \( b:
\]

\[
b = r_1q_2 + r_2
\]

with \( 0 \leq r_2 < r_1. \) If \( r_2 \neq 0, \) we repeat the process:

\[
r_1 = r_2q_3 + r_3
\]

with \( 0 \leq r_3 < r_2. \) Eventually, we get down to a remainder of zero:

\[
r_{n-1} = r_nq_{n+1} + 0.
\]

For example, consider \( a = 3017 \) and \( b = 101:
\]

\[
3017 = 101(29) + 88 \\
101 = 88(1) + 13 \\
88 = 13(6) + 10 \\
13 = 10(1) + 3 \\
10 = 3(3) + 1 \\
3 = 1(3) + 0
\]

**Homework:**

1. Why do we eventually get a remainder of 0 in the Euclidean Algorithm?
2. Let \( r_n \) be the last nonzero remainder in the Euclidean Algorithm applied to the integers \( a \) and \( b. \) Show that \( r_n = \gcd(a, b). \)