3. Greatest Common Divisors

We began by discussing the homework from Monday:

**Question:** If \(d \mid a\) and \(d \mid b\), does \(d \mid ax + by\) for all integers \(x\) and \(y\)?

**Answer:** (Ryan) The answer is ’yes’. To see this, write \(a = du\) and \(b = dv\) for some integers \(u\) and \(v\). Then \(ax + by = dux + dvy = d(ux + vy)\). Since \(ux + vy \in \mathbb{Z}\), we see that \(d\) divides \(ax + by\).

**Question:** If \(d \mid a + b\) does \(d \mid a\) and \(d \mid b\)?

**Answer:** (Gabe) The answer is ’not always’. For example, let \(d = 5\), \(a = 2\) and \(b = 3\). Then \(5 \mid 2 + 3\) but \(5\) does not divide either \(2\) or \(3\). Of course, for some values of \(d\), \(a\), and \(b\), it does hold, for example when \(a = b = d\).

**Question:** If \(d \mid a + b\) and \(d \mid a\) does \(d \mid b\)?

**Answer:** (Sean) The answer is ‘yes’: As before, there are integers \(u\) and \(v\) such that \(a + b = du\) and \(a = dv\). Then \(b = (a + b) - b = du - dv = d(u - v)\). Since \(u - v\) is an integer, \(d\) divides \(b\).

Our next topic is greatest common divisors.

**Definition:** Let \(a\) and \(b\) be integers (not both zero). A **common divisor** of \(a\) and \(b\) is an integer \(d\) which divides both \(a\) and \(b\). The **greatest common divisor** of \(a\) and \(b\), denoted \(\gcd(a, b)\), is the largest common divisor of \(a\) and \(b\).

We remarked that if \(d\) is a divisor of a nonzero number \(a\), then \(|d| \leq |a|\). This means that the set of divisors of a nonzero integer is a finite set, since there are only finitely many integers between \(|a|\) and \(−|a|\).

Some examples:

**Example:** \(\gcd(4, 6) = 2\). To see this, one can list all divisors of both numbers. The divisors of 4 are \(-4, -2, -1, 1, 2,\) and 4, while the divisors of 6 are \(-6, -3, -2, -1, 1, 2, 3,\) and 6. Hence, the common divisors of 4 and 6 are \(-2, -1, 1,\) and 2, and the greatest of these is 2.

We observed the obvious fact that if \(d\) is a divisor of \(a\) then so is \(-d\). Thus, we only need to list out the positive divisors of each number to find the greatest common divisor.

**Example:** \(\gcd(7, 15) = 1\). The only divisors of 1 are 1 and \(-1\), both of which divide 15. The greatest common divisor is therefore 1.

**Example:** \(\gcd(-14, -21) = 7\).

We noted a couple of observations:

- If \(a \neq 0\) then \(\gcd(a, 0) = |a|\).
- \(\gcd(a, 1) = 1\).

As the numbers get bigger, it becomes more difficult to “eyeball” the \(\gcd\) of two integers. Is there a systematic procedure or method to find the \(\gcd\)? One method is the brute force approach of simply finding all common divisors as illustrated above. Of course, we don’t want to make an exhaustive list of all divisors of the two integers every time we want to find a \(\gcd\). (Try doing the brute force method for \(a = 144\) and \(b = 216\), for instance!) It turns
out there is a ‘fast’ way to find the gcd of two numbers, even if the are quite large. We will discuss this method in our next class.

We spent much of the rest of class contemplating the following question:

**Question:** Let $a, b$ be integers with $a \neq 0$. How do the integers $\gcd(a, b)$ and $\gcd(a, a + b)$ compare?

After a little experimentation with various numbers, most of the class quickly conjecture that $\gcd(a, b) = \gcd(a, a + b)$. Michael gave a proof of this:

**Theorem:** Let $a, b$ be integers with $a \neq 0$. Then $\gcd(a, b) = \gcd(a, a + b)$.

**Proof:** (Michael) Let $d = \gcd(a, b)$ and $e = \gcd(a, a + b)$. Since $d | a$ and $d | b$ we know $d | a + b$. Thus, $d$ is a common divisor of $a$ and $a + b$. Hence, $d \leq e$. Similarly, we have $e | a$ and $e | a + b$. Then $e | b$ (by the Homework problem from last week). So $e$ is a common divisor of $a$ and $b$, which means $e \leq d$. Since $d \leq e$ and $e \leq d$, we must have $d = e$. □

**Homework:**

1. Suppose $7 = ax + by$ where $a, b, x, y$ are integers. What are the possible values of $\gcd(a, b)$?
2. Suppose $a = bq + r$ where $a, b, q$, and $r$ are integers, and $b \neq 0$. Prove $\gcd(a, b) = \gcd(b, r)$.
3. Write down at least four positive and four negative numbers for each of the following sets of integers:
   - $4x$, for $x \in \mathbb{Z}$.
   - $4x + 1$, for $x \in \mathbb{Z}$.
   - $4x + 2$, for $x \in \mathbb{Z}$.
   - $4x + 3$, for $x \in \mathbb{Z}$.
   - $4x + 4$, for $x \in \mathbb{Z}$.
   - $4x - 1$, for $x \in \mathbb{Z}$.

Make as many observations and conjectures as you can about these lists of integers.