5. Linear Combinations

We recalled the Euclidean Algorithm from last class: Let a and b be two integers (assume $b \neq 0$). 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:

$$b = r_1 q_2 + r_2$$

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

$$r_1 = r_2 q_3 + r_3$$

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

$$r_{n-1} = r_n q_{n+1} + 0.$$

The first homework question was, why do we eventually get to a remainder of zero? In other words, why must the Euclidean Algorithm terminate? Megan explained that since the remainders are getting smaller and are always nonnegative, eventually we must reach a remainder of zero. In other words, since we have a sequence of nonnegative integers $b > r_1 > r_2 > r_3 > \cdots$, we must have $r_1 \leq b - 1$, $r_2 \leq b - 2$, $r_3 \leq b - 3$ so that the process must terminate in at most b steps.

The next homework problem was to explain why the last nonzero remainder in the Euclidean Algorithm is $\gcd(a, b)$. The answer is given by the theorem we proved on September 4th: If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$. Applying this to each step in the Euclidean Algorithm above, we have

$$\begin{aligned}
\gcd(a, b) &= \gcd(b, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\cdots \\
&\cdots \\
&= \gcd(r_n, 0) \\
&= r_n
\end{aligned}$$

Example: Find $\gcd(141, 120)$:

$$\begin{aligned}
141 &= 120(1) + 21 \\
120 &= 21(5) + 15 \\
21 &= 15(1) + 6 \\
15 &= 6(2) + 3 \\
6 &= 3(2) + 0
\end{aligned}$$

This means that

$$\gcd(141, 120) = \gcd(120, 21) = \gcd(21, 15) = \gcd(15, 6) = \gcd(6, 3) = \gcd(3, 0) = 3.$$

The Euclidean Algorithm provides a fast way to compute gcds of pairs of even very large integers.

We spent the rest of class discussing "linear combinations" of integers:

Definition: Let a, b be integers. Any expression of the form $ax+by$ where $x, y \in \mathbb{Z}$ is called a **linear combination** of a and b.

Example: Let $a = 4$ and $b = 7$. Some of the linear combinations of 4 and 7 we found were:

$$\begin{aligned}
0 &= 4(0) + 7(0) \\
4 &= 4(1) + 7(0) \\
7 &= 4(0) + 7(1) \\
11 &= 4(1) + 7(1) \\
15 &= 4(2) + 7(1) \\
1 &= 4(2) + 7(-1) \\
-3 &= 4(-2) + 7(1) \\
-4 &= 4(-1) + 7(0)
\end{aligned}$$

We noted that since 1 is a linear combination of 4 and 7 then *every* integer is a linear combination of 4 and 7: Let m be an integer. Then multiplying the equation $1 = 4(2)+7(-1)$ by m, we have $m = 4(2m) + 7(-m)$, showing that m is indeed a linear combination of 4 and 7.

We also remarked that if d is a linear combination of a and b then so is $-d$, just by multiplying the equation by -1. So from now on, we will only be interested in positive integers which are linear combinations of a and b.

We considered another example:

Example: Let $a = 8$ and $b = 12$. Some of the linear combinations of 8 and 12 we found were:

$$\begin{aligned}
8 &= 8(1) + 12(0) \\
12 &= 8(0) + 12(1) \\
20 &= 8(1) + 12(1) \\
4 &= 8(-1) + 12(1)
\end{aligned}$$

In this example, we wondered what the smallest positive linear combination of 8 and 12 is. Since this quantity will come up again, we made a definition:

Definition: Let a, b be integers. We define $\text{splc}(a, b)$ to be the smallest positive integer which is a linear combination of a and b.

In our first example, clearly $\text{splc}(4, 7) = 1$ since 1 is a linear combination of 4 and 7 and 1 is the smallest positive integer. In our second example, the smallest positive integer anyone could write as a linear combination of 8 and 12 was 4. Is this indeed the smallest? Or is it possible that 1, 2, or 3 is a linear combination? Hui pointed out that since $8x$ and $12y$ are even, and since the sum of two even integers is even, every linear combination of 8 and 12 must be even. Thus, $\text{splc}(8, 12)$ is either 2 or 4. Nick gave an argument that 2 is not a linear combination. For, suppose $2 = 8x + 12y$. Dividing by 2, we get $1 = 4x + 6y$. But this says that 1 is the sum of two even numbers, which is clearly a contradiction. Hence, 2 cannot be a linear combination of 8 and 12. We can thus safely conclude that $\text{splc}(8, 12) = 4$.

At this point, Gabe was ready to make a conjecture!

Conjecture: (Gabe) Let a and b be integers (not both zero). Then $\text{splc}(a, b) = \gcd(a, b)$.

We tested this conjecture on another example:

Example: Let $a = 12$ and $b = 30$. Find $\text{splc}(12, 30)$.

Answer: We quickly noted that $6 = 12(3) + 30(-1)$, so $\text{splc}(12, 30) \leq 6$. How do we eliminate 1 through 5 as possibilities. Again, we noted that $12x$ and $30y$ are both even, so $\text{splc}(12, 3)$ must be even. However, we can eliminate all the numbers 1 through 5 simultaneously by noting that $12x + 30y = 6(2x + 5y)$, so any linear combination of 12 and 30 is a multiple of 6. Since 6 is clearly the smallest positive multiple of 6, we conclude that $\text{splc}(12, 30) \geq 6$. Thus, $\text{splc}(12, 30) = 6 = \gcd(12, 30)$.

The solution to this example suggested the following theorem.

Theorem: Let a and b be two integers (not both zero). Then any linear combination of a and b is a multiple of $\gcd(a, b)$. In particular, $\text{splc}(a, b) \geq \gcd(a, b)$.

Proof: (Michael) Let $d = \gcd(a, b)$. Then $a = dp$ and $b = dq$ for some integers p and q. Let m be a linear combination of a and b. Then $m = ax + by$ for some $x, y \in \mathbb{Z}$. Then $m = ax + by = dpx + dqy = d(px + qy)$, which shows d divides m. This proves the first statement. For the second statement, since $\text{splc}(a, b)$ is a linear combination of a and b, the first statement says that $\text{splc}(a, b)$ is a multiple of d. Since the smallest positive multiple of d is d, this shows that $\text{splc}(a, b) \geq d$.

Homework: Use the Euclidean algorithm to find the following greatest common divisors:

(1) $\gcd(7696, 4144)$
(2) $\gcd(1721, 378)$