We started talking about linear combinations last time, and given integers \( a \) and \( b \), I told you that the GCD\((a, b)\) is equal to the smallest positive linear combination
\[
(1) \quad sa + tb.
\]
Note that since GCD\((a, b)\) divides both \( a \) and \( b \), it will divide any linear combination of \( a \) and \( b \). This tells us that the smallest positive linear combination can be no smaller than GCD\((a, b)\). Is it possible that smallest positive linear combination is bigger than GCD\((a, b)\)? We’ll investigate that today. Let’s start with the following.

**Remainder Theorem.** Let \( m \in \mathbb{Z} \) and let \( n > 0 \in \mathbb{Z} \). There exists \( q, r \in \mathbb{Z} \) with \( 0 \leq r < n \) such that
\[
m = qn + r.
\]
This theorem states what we expect when we do a long division problem. In other words, if we divide an integer \( n \) into another integer \( m \), it either divides evenly or we get a remainder smaller than \( n \).

“Proof.” As an illustration of what we already know, the integers will lay out
\[
(2) \quad \ldots, -2, -1, 0, 1, 2, \ldots, n - 1, n, n + 1, n + 2, \ldots, n + n - 1, 2n, 2n + 1, \ldots, 2n + n - 1, 3n, \ldots
\]
In particular, the multiples of \( n \) will be evenly spaced along the number line
\[
(3) \quad \ldots, -2n, \ldots, -n, \ldots, 0, \ldots, n, \ldots, 2n, \ldots
\]
At each multiple of \( n \), we’ll have a sequence of \( n \) consecutive integers
\[
(4) \quad qn, qn + 1, qn + 2, \ldots, qn + (n - 1)
\]
In other words, every integer is either a multiple of \( n \) or a multiple of \( n \) plus something less than \( n \).

**Euclidean Algorithm.** Next, we’ll look at a seemingly goofy way to find the GCD of two integers. It’s called the *Euclidean algorithm*. I’ll explain it with an example (taken from *Discrete Mathematical Structures*, by Kolman, Busby, and Ross). We’ll be finding GCD\((273, 98)\).

The process repeats the same basic steps until we can’t go any further. In particular, we will divide the smaller integer into the larger, and then look at the remainder. If we divide 98 into 273, we’ll see that it goes in twice and leaves 77 as the remainder. In other words,
\[
(5) \quad 273 = 2 \cdot 98 + 77.
\]
Since GCD\((273, 98)\) divides both 273 and 98, it must also divide 77. Next, we’ll divide 77 into 98, and we get
\[
(6) \quad 98 = 1 \cdot 77 + 21.
\]
Again, GCD\((273, 98)\) divides both 98 and 77, so it must also divide 21. Now divide 21 into 77. We get
\[
(7) \quad 77 = 3 \cdot 21 + 14,
\]
and GCD\((273, 98)\) divides 14. Next,
\[
(8) \quad 21 = 1 \cdot 14 + 7,
\]
and GCD\((273, 98)\) must divide 7. Finally,
\[
(9) \quad 14 = 2 \cdot 7 + 0.
\]
this last equation tells us that 7 divides 14. If we work backwards, we can see that 7 must also divide 21. Similarly, 7 must also divide 77, 98, and 273, and so 7 is a common divisor of 273 and 98, which means
that \(7 \leq \text{GCD}(273, 98)\). We just saw that \(\text{GCD}(273, 98)\) divides 7, so \(\text{GCD}(273, 98) \leq 7\). It follows that \(\text{GCD}(273, 98) = 7\).

**Basic Principle 1.** This example used two specific positive integers, but any two positive integers would yield a similar result. We would always get a sequence of remainders that get smaller and smaller, eventually hitting zero. The GCD must divide all the remainders, and the last non-zero remainder must divide all previous remainders, as well as the original two numbers. That last non-zero remainder must always be the GCD.

**The smallest linear combination.** The Euclidean algorithm also tells us how to express the GCD as a linear combination. In the example above, we can just work up from the bottom. The second to last equation tells us that

\[
(10) \quad 7 = 21 - 1 \cdot 14.
\]

The next equation tells us that

\[
(11) \quad 14 = 77 - 3 \cdot 21,
\]

and if we substitute that into the previous equation, we get

\[
(12) \quad 7 = 21 - 1 \cdot (77 - 3 \cdot 21) = 2 \cdot 21 - 1 \cdot 77.
\]

**Quiz 05A**

1. Express 21 as a linear combination of 77 and 98.

2. Use your answer to Problem 1 to get 7 as a linear combination of 77 and 98.

3. Now get 7 as a linear combination of 98 and 273.

4. Do the Euclidean algorithm on 175 and 245.

5. Use the results of Problem 4 to express \(\text{GCD}(175, 245)\) as a linear combination of 175 and 245.

**Basic Principle 2.** Note that the steps illustrated with these examples will always work, so while we might not need to use the Euclidean algorithm in practice, it shows that the GCD is always the smallest positive linear combination.

**Basic Principle 3.** Note also that the GCD is the largest common divisor, and it is also the smallest positive linear combination.

**If you want a proof**

**Theorem 1.** Show that if \(a\) and \(b\) are positive integers, then there are integers \(s\) and \(t\) such that \(\text{GCD}(a, b) = sa + tb\).

**Proof.** Let \(a\) and \(b\) be positive integers with \(a > b\). There is an integer 0 \(\leq r_1 < b\) such that

\[
(13) \quad a = n_1 b + r_1.
\]

If \(r_1 = 0\), then we’re done, because \(\text{GCD}(a, b) = b = 0 \cdot a + 1 \cdot b\). Otherwise, we can divide \(r_1\) into \(b\) to get

\[
(14) \quad b = n_2 r_1 + r_2.
\]

If \(r_2 \neq 0\), divide \(r_2\) into \(r_1\) to get

\[
(15) \quad r_2 = n_3 r_2 + r_3.
\]

Since \(b > r_1 > r_2 > r_3 > \cdots \geq 0\), our basic knowledge of integers tells us that we must eventually get a remainder of zero. Since \(\text{GCD}(a, b)\) divides both \(a\) and \(b\), it must also divide \(r_1\) (basic algebra). Similarly, \(\text{GCD}(a, b)\) must divide every \(r_i\), and in particular, the last non-zero \(r_i\), which we’ll call \(d\). I won’t go through the details, but like we did in the example, we can express \(d\) as a linear combination of \(a\) and \(b\). This tells us
that \( \gcd(a, b) \) divides \( d \). Note also that \( d \), equal to the last non-zero remainder, must divide the previous remainder, and every other remainder. Therefore, \( d \) divides both \( a \) and \( b \), and so must divide \( \gcd(a, b) \). Two integers that divide each other must be equal (basic algebra).

**Homework 05**

1. Suppose we have five integers related by the equation \( c = sa + tb \).
   
   a. If an integer \( d \) divides both \( a \) and \( b \), must \( d \) also divide \( c \)?
   
   b. If \( d \) divides both \( c \) and \( a \), must \( c \) divide \( tb \)?
   
   c. If \( d \) divides both \( c \) and \( a \), \( c \) might not divide \( b \). Find a counter example.

2a. Use the Euclidean algorithm on \( 8 \) and \( 5 \).

2b. Use the results of Part a to express \( \gcd(8, 5) \) as a linear combination of \( 8 \) and \( 5 \).

3. Do the same with \( 168 \) and \( 60 \).

Answers on next page.
1a) Yes. b) Yes. c) Example: \( d = 6 \) and \( 72 = 5 \cdot 12 + 4 \cdot 3 \).

2) \( 8 = 1 \cdot 5 + 3, 5 = 1 \cdot 3 + 2, 3 = 1 \cdot 2 + 1, 2 = 2 \cdot 1 + 0 \). GCD = 1.
   b) \( 1 = 3 + (\neg 1) \cdot 2 = 3 + (\neg 1) \cdot (5 + (\neg 1) \cdot 3) = 2 \cdot 3 + (\neg 1) \cdot 5 = 2 \cdot (8 + (\neg 1) \cdot 5) + (\neg 1) \cdot 5 = 2 \cdot 8 + (\neg 3) \cdot 5 \).

3) \( 168 = 2 \cdot 60 + 48, 60 = 1 \cdot 48 + 12, 48 = 4 \cdot 12 + 0 \). GCD = 1.
   b) \( 12 = 60 + (\neg 1) \cdot 48 = 60 + (\neg 1) \cdot (168 + (\neg 2) \cdot 60) = 3 \cdot 60 + (\neg 1) \cdot 168 \).