Math 412. Adventure sheet on the Euclidean Algorithm.

DEFINITION: The **greatest common divisor** or **GCD** of two integers a, b is the largest integer d such that $d|a$ and $d|b$. We often write (a, b) for the GCD of a and b.

THEOREM 1.2: Let a and b be integers, and assume that a and b are not both zero. There exist $r, s \in \mathbb{Z}$ such that $ra + sb = (a, b)$.

The **Euclidean algorithm** is a method to find the GCD of two integers, as well as a specific pair of numbers r, s such that $ra + sb = (a, b)$. We will say that an expression of the form $ra + sb$ with $r, s \in \mathbb{Z}$ is a **linear combination** of a and b.[1]

A. WARMUP:

(1) List all factors[2] of 18? List all factors of 24. Find $(18, 24)$.
(2) For $a \in \mathbb{Z}$, what is (a, a)? What is $(a, 7a)$? If $a > 0$, what is the GCD of a and 0?

B. Suppose we had two numbers a and b, and we did the division algorithm to get $a = bq + r$ for some $q, r \in \mathbb{Z}$.

(1) Show that if d is a common divisor of b and r, then d is a common divisor of a and b. What does this say about the relationship between (a, b) and (b, r)?
(2) Show that if d is a common divisor of a and b, then d is a common divisor of b and r. What does this say about the relationship between (b, r) and (a, b)?
(3) Show that $(a, b) = (b, r)$.
(4) How might (3) make the computation of (a, b) easier?

C. Consider the following computation, which you can assume is accurate:

(i)	$524 = 148 \cdot 3 + 80$	$0 \leq 80 < 148$
(ii)	$148 = 80 \cdot 1 + 68$	$0 \leq 68 < 80$
(iii)	$80 = 68 \cdot 1 + 12$	$0 \leq 12 < 68$
(iv)	$68 = 12 \cdot 5 + 8$	$0 \leq 8 < 12$
(v)	$12 = 8 \cdot 1 + 4$	$0 \leq 4 < 8$
(vi)	$8 = 4 \cdot 2 + 0$	

(1) What is going on on each individual line?
(2) How does each line relate to the previous one?
(3) Prove that

$$(524, 148) = (148, 80) = (80, 68) = (68, 12) = (12, 8) = (8, 4) = (4, 0) = 4.$$

D. Continuing this example...

(1) Use equation (i) to express 80 as a linear combination of 524 and 148.
(2) Use equation (ii) to express 68 as a linear combination of 148 and 80. Use this and the previous part to express 68 as a linear combination of 524 and 148.
(3) Express 12 as a linear combination of 524 and 148.
(4) Express $4 = (524, 148)$ as a linear combination of 524 and 148.

[1] Just like in linear algebra, except with integers instead of real number scalars and vectors.

[2] Factor is another word for divisor. Completely synonymous.

E. The computation in C is an example of the Euclidean algorithm applied to 524 and 148. Use the Euclidean algorithm to find $(1003, 456)$. Express $(1003, 456)$ as a linear combination of 1003 and 456.

F. Without formally writing a careful proof, discuss with your workmates how the Euclidean algorithm can be used to prove the Theorem at the top of the previous page. How is this different from the **non-constructive proof** in the textbook?