Math 412. 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?

ANSWER:
(1) The factors of 18 are $\{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18\}$.
The factors of 24 are $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}$. The GCD is 6.
(2) $(a, a) = |a|$, $(a, 7a) = |a|$ and $(a, 0) = |a|$.

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?

ANSWER:
(1) Let d be a common factor of b and r. So there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = dk_1$ and $r = dk_2$. Substitute $a = bq + r = dk_1q + dk_2 = d(k_1q + k_2)$.

[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.

Since $k_1 q + k_2 \in \mathbb{Z}$, we have $d|a$. Thus d is a common factor of a and b. We conclude that $(b, r) \leq (a, b)$ since the *greatest* common factor of b and r is at least some common factor of a and b, but not necessarily the greatest.

(2) Let d be a common factor of b and a. So there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = dk_1$ and $ra = dk_2$. Substitute $r = a - bq = dk_1 - dk_2 q = d(k_1 - k_2 q)$. So similarly, $d|r$. Thus d is a common factor of r and b. By a similar argument, we conclude that $(b, r) \geq (a, b)$

(3) This follows from (1) and (2), since both $(b, r) \geq (a, b)$ and $(b, r) \leq (a, b)$.

(4) The integers a and b may have an out-of-control number of digits, but assuming (without loss of generality) that $a > b$, then we know that the pair b, r will be "smaller". So instead we can compute the GCD (b, r), which is the same as the one we started with (a, b).

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

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

ANSWER: This shows several applications of the technique in B. We use repeated instances of the division algorithm to replace each pair (a, b) with a more manageable pair (b, r) where b is the smaller of the two original integers and r is the remainder upon dividing the larger by the smaller. We keep doing this until the remainder becomes 0. This eventually tells us that the GCD is of 524 and 148 is 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.

ANSWER:

(1) $80 = 524 - 3 \times 148$.

(2) $68 = 148 - 80$. So $68 = 148 - (524 - 3 \times 148) = -524 + 4 \times 148$

(3) $12 = 80 - 68 = 524 - 3 \times 148 - (-524 + 4 \times 148) = 2 \times 524 - 7 \times 148$

(4) $4 = 12 - 8 = 12 - (68 - 5 \times 12) = -68 + 6 \times 12 = -(-524 + 4 \times 148) + 6 \times (2 \times 524 - 7 \times 148) = 13 \times 524 - 46 \times 148$

E. The computation above 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.

ANSWER:

$$\begin{aligned} 1003 &= 2 \times 456 + 91 \text{ so } (1003, 456) = (456, 91). \\ 456 &= 91 \times 5 + 1 \text{ so } (456, 91) = (91, 1). \\ 91 &= 91 \times 1 + 0 \text{ so } (91, 1) = (1, 0) = 1 \end{aligned}$$

So $(1003, 456) = 1$. Note that we could have stopped one step earlier, since obviously $(91, 1) = 1$.

$1 = -5 \times 1003 + 11 \times 456$

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?

ANSWER: This proof gives a recipe for actually finding the desired linear combination, whereas the proof in the book does not. Rather, the book "finds" a linear combination by summoning the smallest element in some enormous set.