THE EUCLIDEAN ALGORITHM AND LINEAR EQUATIONS

DEFINITION: The **greatest common divisor** of two integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides a and b. Two integers a and b are **coprime** if $\gcd(a, b) = 1$.

The **Euclidean algorithm** is an algorithm to find the greatest common divisor of two integers $a \geq b \geq 1$. Here is how it works:

(I) Start with $a_0 := a$, $b_0 := b$, and $n = 0$.
(II) Apply long division / division algorithm to write $a_n := q_n b_n + r_n$ with $0 \leq r_n < b_n$.
(III) If $r_n = 0$, STOP; the greatest common divisor of a and b is b_n.
Else, set $a_{n+1} := b_n$, $b_{n+1} := r_n$, and return to Step (II).

It is a THEOREM from Math 310 that the Euclidean algorithm terminates and outputs the correct value.

An expression of the form $ra + sb$ with $r, s \in \mathbb{Z}$ is a **linear combination** of a and b.

COROLLARY: If a, b are integers, then $\gcd(a, b)$ can be realized as a linear combination of a and b. Concretely, we can use the Euclidean algorithm to do this.

(1) Warumup with GCDs:
  (a) Let a, b be nonzero integers. Explain why[1] that $\gcd(a, b) = \gcd(|a|, |b|)$.
  (b) Let a, b be nonzero integers and $d = \gcd(a, b)$. Show that a/d and b/d are coprime.
  (c) Given prime factorizations of two positive integers a and b, explain[2] how to find $\gcd(a, b)$ using the prime factorizations (not the Euclidean algorithm).

(2) The following calculations correspond to running the Euclidean algorithm with 524 and 148:

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

  (a) Identify the numbers a_n and b_n in the notation of the Euclidean algorithm as stated above.
  (b) What is the greatest common divisor of 524 and 148?

(3) Continuing this example. . .
  (a) Use equation (i) to express 80 as a linear combination of 524 and 148.
  (b) 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.
  (c) Express 12 as a linear combination of 524 and 148.
  (d) Express $4 = (524, 148)$ as a linear combination of 524 and 148.

(4) Use the Euclidean algorithm to find the GCD of 184 and 99, and to express this GCD as a linear combination of 184 and 99.

[1] Hint: How are the divisors of a and $|a|$ related?
[2] Explain how, but don't write a careful proof for now.

We now know everything we need to solve all equations of the form $ax + by = c$ over the integers! A equation of this form considered over $\mathbb{Z}$ is called a **linear Diophantine equation**.

THEOREM: Let a, b, c be integers. The equation

$$ax + by = c$$

has an integer solution if and only if c is divisible by $d := \gcd(a, b)$. If this is the case, there are infinitely many solutions. If (x_0, y_0) is a one particular solution, then the general solution is of the form

$$x = x_0 - (b/d)n, \quad y = y_0 + (a/d)n$$

as n ranges through all integers.

(4) Proof of the first sentence/finding one particular solution:
   (a) Explain why if $ax + by = c$ has an integer solution (x_0, y_0) then c is a multiple of d.
   (b) What technique[3] would you use to find a particular solution of $ax + by = d$?
   (c) Given an integer m how could you find a particular solution for $ax + by = md$?
   (d) Observe that you have proven the first sentence of the Theorem above.

(5) Find all integer solutions (x, y) of the following equations:
   - $21x + 56y = 222$.
   - $21x + 56y = 224$.

(6) A farmer wishes to buy 100 animals and spend exactly \$200. Cows are \$20, sheep are \$6, and pigs are \$1. Is this possible? If so, how many ways can he do this?

(7) Conclusion of the proof of the Theorem: Suppose that c is divisible by $d := \gcd(a, b)$ and that (x_0, y_0) is a particular solution to $ax + by = c$.
   (a) Show that, for any integer n, $(x_0 - (b/d)n, y_0 + (a/d)n)$ is also a solution.
   (b) Suppose that (x_1, y_1) is another solution. Show that $(x_0 - x_1, y_0 - y_1)$ is a solution to $ax + by = 0$.
   (c) Take the equation $a(x_0 - x_1) = -b(y_0 - y_1)$ and divide through by d. Show that a/d divides $y_0 - y_1$ and b/d divides $x_0 - x_1$. Conclude the proof of the Theorem.

---

(8) In the next few problems we outline how to solve linear equations

$$a_1x_1 + \cdots + a_nx_n = b \qquad (\dagger)$$

in multiple variables over $\mathbb{Z}$. First we deal with the easy cases.
   (a) Show that if $\gcd(a_1, \ldots, a_n)$ does not divide b, then ($\dagger$) has no solution.
   (b) Show that if $a_1 = 1$, then $x_2, \ldots, x_n$ can be chosen to be *any* integers, with x_1 determined uniquely by the other values.
   (c) Solve $6x_1 + 10x_2 + 12x_3 = 13$ over $\mathbb{Z}$.
   (d) Solve $x_1 + 7x_2 + 9x_3 = 3$ over $\mathbb{Z}$.

(9) Now we discuss how to reduce the general equation to the easy cases. We start with two examples:
   (a) Take the equation

$$5x_1 + 35x_2 + 45x_3 = 15.$$

   Divide through to get to a settled case.

[3] Just name the relevant algorithm for now.

(b) Take the equation:

$$3x + 7y + 8z + 9w = 10.$$

We replace x by $u = x + 2y$, so $x = u - 2y$. Rewrite the equation above in terms of u, y, z, w and solve. Then express (x, y, z, w) in terms of the free parameters u, y, z.

(c) Here's how to generalize the last example: if a_i is the coefficient with smallest absolute value (say it's positive) and a_j is another coefficient that is *not* a multiple of a_i, apply long division to write $a_j = qa_i + r$ with $0 \leq r < |a_i|$. Replace x_i with $x_i' := x_i + qx_j$. Show that the coefficient of x_j in the new system is smaller than $|a_i|$.

Repeating this step and dividing all coefficients through by a common factor keeps decreasing the smallest coefficient until it becomes 1*, or until it is clear there is no solution.*

(d) Solve the equation $4x + 11y + 9z = 35$ over $\mathbb{Z}$.

(e) Solve the equation $8x - 4y + 10z - 12w = 28$ over $\mathbb{Z}$.

(f) Challenge your neighbor with a multivariate linear Diophantine equation!

Key Points:

- Computing GCD and GCD as a linear combination by Euclidean Algorithm.
- How to solve linear equations over $\mathbb{Z}$.