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).

(a) The divisors of a are exactly the same as the divisors of $|a|$, and likewise with b. The conclusion is then clear.
(b) Suppose that n divides a/d and b/d. Write $a/d = na'$ and $b/d = nb'$, so $a = nda'$ and $b = ndb'$. If $n > 1$, then $nd > d$ is a common divisor of a/d and b/d, which contradicts the definition of GCD.
(c) For each prime factor p_i of a and b, take the minimum of the multiplicity of p_i in the factorization of a and the multiplicity of p_i in the factorization of b; the product of the p_i's to these powers is the GCD.

(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?

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

$a_0 = 524$, $b_0 = a_1 = 148$, $b_1 = a_2 = 80$, $b_2 = a_3 = 68$, $b_3 = a_4 = 12$, $b_4 = a_5 = 8$, $b_5 = 4$. The GCD is 4.

(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.

$$\begin{aligned}
80 &= 1 \cdot 524 - 3 \cdot 148 \\
68 &= 1 \cdot 148 - 1 \cdot 80 = 1 \cdot 148 - 1 \cdot (1 \cdot 524 - 3 \cdot 148) \\
&= -1 \cdot 524 + 4 \cdot 148 \\
12 &= 1 \cdot 80 - 1 \cdot 68 = 1 \cdot (1 \cdot 524 - 3 \cdot 148) - 1 \cdot (-1 \cdot 524 + 4 \cdot 148) \\
&= 2 \cdot 524 - 7 \cdot 148 \\
8 &= 1 \cdot 68 - 5 \cdot 12 = 1 \cdot (-1 \cdot 524 + 4 \cdot 148) - 5 \cdot (2 \cdot 524 - 7 \cdot 148) \\
&= -11 \cdot 524 + 39 \cdot 148 \\
4 &= 1 \cdot 12 - 1 \cdot 8 = 1 \cdot (2 \cdot 524 - 7 \cdot 148) - 1 \cdot (-11 \cdot 524 + 39 \cdot 148) \\
&= 13 \cdot 524 - 46 \cdot 148.
\end{aligned}$$

(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.

$$\begin{aligned}
184 &= 1 \cdot 99 + 85 \\
99 &= 1 \cdot 85 + 14 \\
85 &= 6 \cdot 14 + 1 \\
14 &= 14 \cdot 1 + 0
\end{aligned}$$

so the GCD is 1.

$$\begin{aligned}
85 &= 1 \cdot 184 - 1 \cdot 99 \\
14 &= 1 \cdot 99 - 1 \cdot 85 = 1 \cdot 99 - 1 \cdot (1 \cdot 184 - 1 \cdot 99) = -1 \cdot 184 + 2 \cdot 99 \\
1 &= 1 \cdot 85 - 6 \cdot 14 = 1 \cdot (1 \cdot 184 - 1 \cdot 99) - 6 \cdot (-1 \cdot 184 + 2 \cdot 99) = 7 \cdot 184 - 13 \cdot 85.
\end{aligned}$$

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.

(a) We can write $a = a'd$ and $b = b'd$. Then $c = ax_0 + by_0 = a'dx_0 + b'dy_0 = d(a'x_0 + b'y_0)$ is a multiple of d.
(b) The Euclidean algorithm!
(c) Take s, t such that $as + bt = d$. Then $a(ms) + b(mt) = md$.
(d) OK!

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

- First we use the Euclidean algorithm to find the GCD of 21 and 56:
$$56 = 2 \cdot 21 + 14$$
$$21 = 1 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$
it is 7. Since 222 is not a multiple of 7 there is no solution.
- Now that 224 is a multiple of 7, we know that there is a solution. We find a particular solution by running the Euclidean algorithm backwards.
$$14 = 1 \cdot 56 - 2 \cdot 21$$
$$7 = 1 \cdot 21 - 1 \cdot 14 = 1 \cdot 21 - 1 \cdot (1 \cdot 56 - 2 \cdot 21) = -1 \cdot 56 + 3 \cdot 21^{\cdot}$$
Then since $224 = 32 \cdot 7$, we have
$$224 = 32(7) = 32(-1 \cdot 56 + 3 \cdot 21) = -32(56) + 96(21),$$
so $(-32, 96)$ is a particular solution. The general solution is then $(-32 - 8n, 96 + 3n)$ by the formula.

(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?

The system of equations is
$$c + s + p = 100, 20c + 6s + p = 200.$$
Substituting $p = 100 - c - s$ we obtain
$$20c + 6s + 100 - c - s = 200$$
$$19c + 5s = 100.$$
As $\gcd(19, 5) = 1$ this equation will have infinitely many integer solutions. We can find one by the Euclidean Algorithm.
$$19 = 3 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$4 = 1 \cdot 19 - 3 \cdot 5$$
$$1 = 1 \cdot 5 - 1 \cdot 4 = 1 \cdot 5 - 1 \cdot (1 \cdot 19 - 3 \cdot 5) = -1 \cdot 19 + 4 \cdot 5.$$

[3] Just name the relevant algorithm for now.

Then we multiply through:

$$100 = -100 \cdot 19 + 400 \cdot 5.$$

Hence $c = -100, s = 400$ is one integer solution. By the Theorem, all solutions are of the form

$$c = -100 - 5n, s = 400 + 19n.$$

Since we are looking for nonnegative integer solutions, we see that

$$-100 - 5n \geq 0 \quad \text{and} \quad 400 + 19n \geq 0.$$

This yields $-20 \geq n$ and $-21 \leq n$, hence $n = -21$ and $n = -20$ give the only nonnegative solutions. This yields

$$c = 5, s = 1, p = 94 \qquad \text{and} \qquad c = 0, s = 20, p = 80.$$

(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.

(a) Plug in and check.
(b) Plug in and check.
(c) Recall that a/d and b/d are coprime. Since $a/d(x_0 - x_1) = -b/d(y_0 - y_1)$, by the lemma, a/d divides $y_0 - y_1$; write $y_0 - y_1 = na/d$. Then $a(x_0 - x_1) = -b(y_0 - y_1) = -nab/d$, so $x_0 - x_1 = -nb/d$. Putting things back in place, this gives the formula the statement.

---

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

$$a_1x_1 + \cdots + a_nx_n = b \tag{†}$$

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 (†) 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 $\mathbb{Z}$.

(a) If d is this GCD, then d would divide the LHS but not the RHS.
(b) Take $x_1 = b - a_2x_2 - \cdots - a_nx_n$.
(c) No solution: LHS is even, RHS is odd.
(d) $(x_1, x_2, x_3) = (3 - 7x_2 - 9x_3, x_2, x_3)$ is the general solution.

(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.
  (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!

(a)

$$x_1 + 7x_2 + 9x_3 = 3.$$
$$(x_1, x_2, x_3) = (3 - 7x_2 - 9x_3, x_2, x_3)$$

(b) Take the equation:

$$3x + 7y + 8z + 9w = 10.$$
$$3(u - 2y) + 7y + 8z + 9w = 10 \qquad x = u - 2y$$
$$3u + y + 8z + 9w = 10 \qquad x = u - 2y$$
$$(u, y, z, w) = (u, 10 - 3u - 8z - 9w, z, w) \qquad x = u - 2y$$
$$(x, y, z, w) = (u - 2y, 10 - 3u - 8z - 9w, z, w)$$
$$(x, y, z, w) = (u - 2(10 - 3u - 8z - 9w), 10 - 3u - 8z - 9w, z, w)$$
$$(x, y, z, w) = (-20 + 7u + 16z + 18w, 10 - 3u - 8z - 9w, z, w)$$

(c) The coefficient is r, since plugging in we get

$$a_i(x_i' + qx_j) + a_jx_j + \cdots = a_ix_i' + (a_j - qa_i)x_j + \cdots = a_ix_i' + rx_j + \cdots.$$

(d) Take $u = x + 2y$, so we get

$$4u + 3y + 9z = 35.$$

Then take $v = y + u$, so we get

$$u + 3v + 9z = 35.$$

Then v and z are free variables and

$$u = 35 - 3v - 9z,$$

so the general solution, at least in terms of u, v, z, is

$$(u, v, z) = (35 - 3v - 9z, v, z).$$

We need to express y and x in terms of u, v, z (and then v, z) to get the solution. Since $v = y + u$, we have

$$y = v - u = v - (35 - 3v - 9z) = -35 + 4v + 9z.$$

Then, since $u = x + 2y$, $x = u - 2y$, so

$$x = (35 - 3v - 9z) - 2(-35 + 4v + 9z) = 3(35) - 11v - 27z.$$

Thus, the general solution is

$$(x, y, z) = (105 - 11v - 27z, -35 + 4v + 9z, z), \quad v, z \in \mathbb{Z}.$$

(e),(f): Left for you.

Key Points:

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