Euclidean Algorithm
Class activity, Week 3

In the pre-class activity, you were asked to consider:
Claim: $\gcd(a, b) = \gcd(b, r)$ where r is the remainder when a is divided by b.

proof: To show this equality, it is enough to show that
d is a factor of a and b if and only if d is a factor of b and r.

Suppose d is a factor of a and b. Since $r = a - bq$, $d|r$ as well. Hence d is a factor of b and r.

Suppose now d is a factor of b and r. Since $a = bq + r$, $d|a$ as well. Hence d is a factor of a and b.
□

Euclidean algorithm uses this claim to find the greatest common divisor of two numbers efficiently. Specifically, we find the greatest common divisor of two numbers by recursively reducing to an easier case. Here's an example of the algorithm in action:

Finding $\gcd(1419, 1254)$ (where $a = 1419$, $b = 1254$) is equivalent to finding $\gcd(1254, 165)$ by the above claim.

Again, finding $\gcd(1254, 165)$ is equivalent to finding $\gcd(165, 99)$, which is equivalent to finding $\gcd(99, 66)$, which is equivalent to finding $\gcd(66, 33)$.

At this point we recognize that $33|66$, hence $\gcd(66, 33) = 33 = \gcd(1419, 1254)$.

In the above work, we actually did not need to keep writing gcd as we were only interested in the numbers and remainders. So we can compactify the amount of writing by focusing only on the remainder calculations. We also keep track of the remainders and quotients in each step as will see that reversing this process helps us express the greatest common divisor as a linear combination.

$$\begin{aligned}
1419 &= 1254 \cdot 1 + 165 \\
1254 &= 165 \cdot 7 + 99 \\
165 &= 99 \cdot 1 + 66 \\
99 &= 66 \cdot 1 + 33 \\
66 &= 33 \cdot 2
\end{aligned}$$

In the algorithmic calculation, we continue quotient-remainder calculations until the remainder becomes 0, in which case the greatest common divisor is found to be the last non-zero remainder.

1. Apply the Euclidean algorithm to find $\gcd(2093, 5005)$.

$5005 = 2093 \cdot 2 + 819 \quad = \gcd(2093, 819)$

$2093 = 819 \cdot 2 + 455 \quad = \gcd(819, 455)$

$819 = 455 \cdot 1 + 364 \quad = \gcd(455, 364)$

$455 = 364 \cdot 1 + 91 \quad = \gcd(364, 91)$

$364 = 91 \cdot 4 + 0 \quad = 91$

We will now reverse the Euclidean algorithm to express the $\gcd(1419, 1254)$ as a linear combination of 1419 and 1254, in other words the dividend and the divisor of the first equation in the Euclidean algorithm. Note that from the fourth equation where the greatest common divisor is the remainder, we can express the greatest common divisor as a linear combination of the dividend and the divisor in that equation: $33 = 99 - 66$.

Now, we can use the previous equation to express the greatest common divisor as a linear combination of the dividend and the divisor of the previous step:

$$33 = 99 - 66 = 99 - (165 - 99) = 2 \cdot 99 - 165$$

Then, using the second equation, we get

$$33 = 2 \cdot 99 - 165 = 2(1254 - 165 \cdot 7) - 165 = 2 \cdot 1254 - 15 \cdot 165$$

Finally, using the first equations, we have

$$33 = 2 \cdot 1254 - 15(1419 - 1254) = 17 \cdot 1254 - 15 \cdot 1419$$

2. Reverse your Euclidean algorithm calculation from problem 1 to express $\gcd(2093, 5005)$ as a linear combination of 2093 and 5005.

$$\begin{aligned} 91 &= 455 - 364 \\ &= 455 - (819 - 455) \\ &= 455 \cdot 2 - 819 \\ &= (2093 - 819 \cdot 2) \cdot 2 - 819 \\ &= 2 \cdot 2093 - 5 \cdot 819 \\ &= 2 \cdot 2093 - 5(5005 - 2093 \cdot 2) = 12 \cdot 2093 - 5 \cdot 5005 \end{aligned}$$

3. (If time) Find $\gcd(180557, 145673)$ using the Euclidean algorithm. Then, reverse your calculations to express the greatest common divisor as a linear combination of these two numbers.

Recall: A *Diophantine equation* is an equation for which we are interested only in integer solutions. A *linear* Diophantine equation is an equation of the form $ax + by = c$.

4. Find a solution for each of the following equations, if possible:

a. $5x + 10y = 1234$ $\longrightarrow 5(x+2y) = 1234$ impossible

b. $5x - 4y = 2$ $(x,y) = (2,2)$

c. $5x - 4y = 1234$ $(x,y) = (246,-1)$

Theorem 1: The linear Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides c.

proof: Prove the easy direction.

if $ax+by=c$ has a solution then $\gcd(a,b) \mid c$.

$f = \gcd(a,b)$ $\qquad \underbrace{f}_{\mathbb{Z}}\underbrace{\left(\frac{a}{f}x + \frac{b}{f}y\right)}_{\mathbb{Z}} = c$ $\qquad \frac{a}{f}, \frac{b}{f} \in \mathbb{Z}$

so $f \mid c$

To prove the other direction, assume $\gcd(a,b) \mid c$. By definition of divisibility, we have $c = k \cdot \gcd(a,b)$ for some int k. By the GCD as a linear combination result, we have $c = k(ax+by)$. Multiplying both sides by _____ and rearranging terms, we obtain

$$c = akx + bky$$

which shows that there is a solution to the given Diophantine equation.

□

5 a. Use your result from problem 2 to solve the following Diophantine equation:

$$2093 \cdot x + 5005 \cdot y = 9191$$

$$2093 \cdot 1212 + 5005(-505) = 9191$$

b. Check that $x = 1322$ and $y = -551$ is a possible solution. Are your x and y values different than these?

it is & they are different

Over →

c. Show that for any k, $x = 1322 + 5005 \cdot k$ and $y = -551 - 2093 \cdot k$ also works as solution.

$2093(1322 + 5005 \cdot k) + 5005(-551 - 2093 \cdot k)$

all k's cancel

$= 9191$

d. Show that $x = 1322 + 55 \cdot k$ and $y = -551 - 23 \cdot k$ also works.

$2093(1322 + 55 \cdot k) + 5005(-551 - 23 \cdot k)$

all k's cancel

$= 9191$

Theorem 2: Suppose x_0 and y_0 is a solution to the Diophantine equation $ax + by = c$. Let $d = \gcd(a, b)$. Then the general solution to this equation is given by

$$x_k = x_0 + \frac{kb}{d} \ , \ y_k = y_0 - \frac{ka}{d}$$

where $k = 0, \pm 1, \pm 2, \ldots$.

proof: Your work in part d of problem 5 generalizes to show that if x_k and y_k are as given, then they are solutions to the given Diophantine equation.

To show any solution must be of this form, consider a solution x' and y', i.e. $ax' + by' = c$. Since x_0 and y_0 is also a solution, we also have $ax_0 + by_0 = c$. Subtracting the second equation from the first, we find that

$$a(x' - x_0) + b(y' - y_0) = 0 \quad \longrightarrow \quad a(x' - x_0) = b(y_0 - y')$$

Since d divides both a and b, we can divide both sides of the right equation by d to get

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we have $\frac{a}{d} | y_0 - y'$, hence $y_0 - y' = k\frac{a}{d}$ for some k. Rearranging, we find that $y' = y_0 - k\frac{a}{d}$, which is what the theorem claims. Plugging this into

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

we find the formula for x' to be the same as in the theorem.