Investigations on Calculating and Using the GCD
Pre-class, Week 3

For the justification questions in this activity, you do not need to worry about official proofs. If a question asks for a justification, just think about how you would convince someone. If you can think of a general explanation (possibly using specific numbers, but an explanation which can be generalized), that's great. If you cannot think of a general explanation, then try to explain why it works for specific numbers. Maybe try specific numbers in two different ways. We will make things more general and official during class.

1. Justify why any factor of a and b should be a factor of a and $a - b$. (For example, any factor of 6799 and 6789 should be a factor of 6799 and 10.)

$f | a \quad f | b$

So $a = fi \quad b = fj \longrightarrow a - b = fi - fj = f(i-j) \rightarrow f | a, \; f | a-b$

2. Justify why any factor of a and $a - b$ should be a factor of a and b. (For example, any factor of 6799 and 10 should be a factor of 6799 and 6789.)

$f | a \quad f | a-b$

So $a = fi \quad a-b = fj \longrightarrow b = a - fj = fi - fj = f(i-j) \rightarrow f | a, \; f | b$

3. Why would the first two problems above imply $\gcd(a, b) = \gcd(a, a - b)$?

$\gcd(a,b)$ is a common factor of a & $a-b$ so $\gcd(a,b) \leq \gcd(a,a-b)$

$\gcd(a,a-b)$ is a common factor of a & b so $\gcd(a,a-b) \leq \gcd(a,b)$

Thus $\gcd(a,b) = \gcd(a,a-b)$

4. Using $\gcd(a, b) = \gcd(a, a - b)$, find $\gcd(123456, 123476)$.

$= \gcd(123456, 20)$

$20 \nmid 123456, \; 10 \nmid 123456, \; 5 \nmid 123456, \; 4 | 123456$

5. Using a similar idea to what you used for problems 1 and 2, explain why $\gcd(a, b) = \gcd(b, r)$ if $a = bq + r$ and $0 \leq r < b$ (i.e. r is the remainder when a is divided by b).

$r = a - bq$

$$\left.\begin{aligned} \gcd(a,b) &= \gcd(a, a-b) \\ &= \gcd(a, a-2b) \\ &= \cdots \\ &= \gcd(a, r) \end{aligned}\right\} q \text{ times}$$

Over →

6. Use $\gcd(a, b) = \gcd(b, r)$ where r is the remainder when a is divided by b to find $\gcd(23024709, 188727)$?

$23024709 \% 188727 = 15$ $\quad = gcd(15, 12)$

$188727 \% 15 = 12$ $\quad = 3$

or: $15 \nmid 188727$, $5 \nmid 188727$, $\underline{3 \mid 188727}$

7 a. If we apply the formula $\gcd(a, b) = \gcd(b, r)$ to find $\gcd(527176, 35039)$, is the resulting gcd easy enough? In other words, can we find that gcd without too many trial errors?

$= gcd(35039, 1591)$

I'd rather not 1591's factors

b. Can we apply the formula $\gcd(a, b) = \gcd(b, r)$ once more to the resulting gcd? If so, does this new gcd look easy enough?

$= gcd(1591, 37)$

$= 37$

A *Diophantine equation* (named after the Greek mathematician Diophantus of Alexandria) is an equation for which we are interested only in integer solutions. Fermat's Last Theorem deals with one such famous equation: $x^n + y^n = z^n$ where x, y, z, n are all integers. We will not be as ambitious as to try to prove Fermat's Last Theorem in this course. Instead we will focus on *linear* Diophantine equations. These are equations of the form $ax + by = c$.

8. Find, if possible, at least one solution to each of the following linear Diophantine equation. If not possible, explain why. (Note: x and y can be any integers, positive, negative, or 0.)

a. $2x + 3y = 8$ $\quad (x, y) = (1, 2)$

b. $2x + 3y = 13$ $\quad (x, y) = (-1, 5)$

c. $2x + 3y = c$ $\quad (x, y) = (-c, c)$

$ax + by = c$ $\quad f = gcd(a, b)$

$f(\frac{a}{f}x + \frac{b}{f}y) = c$ $\quad \frac{a}{f}, \frac{b}{f} \in \mathbb{Z}$

$\exists (x,y) \in \mathbb{Z}^2 \mid ax + by = c$ if $gcd(a, b) \mid c$

d. $2x + 4y = 105$ $\rightarrow 2(x + 2y) = 105$, impossible, even = odd

e. $6x + 9y = 24$ $\rightarrow 3(2x + 3y) = 24$, $2x + 3y = 8$, $(x, y) = (1, 2)$

f. $6x + 9y = 11$ $\rightarrow 3(2x + 3y) = 11$, impossible, $3 \nmid 11$