Discrete Math HW 12: Learning goals N3–N5

due Monday, April 27

N3: I can compute the greatest common divisor of two natural numbers using the Euclidean Algorithm.

(*The problems for learning goal N3 in this section are the same problems from last week's homework, since we didn't make it as far last week as I thought we would. If you didn't have a chance to do them last week, you can do them now (but no need to complete them twice).*)

Exercise 1 Use the Euclidean Algorithm to compute each of the following. Be sure to show the steps of the process, not just the final result.

(a) $\gcd(1,5)$

(b) $\gcd(123,277)$

(c) $\gcd(78,104)$

(d) $\gcd(88,72)$

Exercise 2 Write a Disco function to find the GCD of two natural numbers using the Euclidean algorithm, by filling in the following template:

```
gcd : (N * N) -> N
gcd(a,0) = ???
gcd(a,b) = ???
```

Use your Disco function to find $\gcd(518303142726377580, 169429189188136020)$.

N4: I can compute Bézout coefficients and modular inverses using the Extended Euclidean Algorithm.

Exercise 3 For each pair of numbers a and b, compute integers s and t such that $sa + tb = \gcd(a,b)$.

(a) $a = 1$, $b = 5$

(b) $a = 123$, $b = 277$

(c) $a = 78$, $b = 104$

Exercise 4 For each a and m below, either find the multiplicative inverse of a modulo m, or state that it does not have one.

(a) $a = 7$, $m = 24$

(b) $a = 26$, $m = 39$

(c) $a = 922$, $m = 77$

N5: I can solve modular equivalences in one variable involving addition, subtraction, and multiplication by a constant.

Exercise 5 Solve each of the following equivalences for x. Express your answers in the form $x \equiv_m r$ where $0 \leq r < m$.

(a) $34x \equiv_{89} 77$

(b) $5x + 17 \equiv_{23} 2x - 10$

(c) $200x - 13 \equiv_{1001} 0$