Discrete Math HW 9: Learning goals N2–N4 (solutions)

due Monday, April 28

N2: I can compute the greatest common divisor of two natural numbers using the Euclidean Algorithm.

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) $\gcd(1,5) = \gcd(5,1) = \gcd(1,0) = 1$

(b) $\gcd(123,277) = \gcd(277,123) = \gcd(123,31) = \gcd(31,30) = \gcd(30,1) = \gcd(1,0) = 1$

(c) $\gcd(78,104) = \gcd(104,78) = \gcd(78,26) = \gcd(26,0) = 26$

Exercise 2 Write a Disco function to find the GCD of two natural numbers using the Euclidean algorithm.

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

$$\gcd(518303142726377580, 169429189188136020) = 8580$$

N3: 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) $a = 1$, $b = 5$

$s = 1$, $t = 0$ works!

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

s	t	$123s + 277t$	q
0	1	277	
1	0	123	2
-2	1	31	3
7	-3	30	1
-9	4	1	

Hence $-9 \cdot 123 + 4 \cdot 277 = 1$.

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

s	t	$78s + 104t$	q
0	1	104	
1	0	78	1
-1	1	26	3
4	-3	0	1

Hence the GCD is $\gcd(78, 104) = 26$, and $104 - 78 = 26$.

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

7 is its own multiplicative inverse modulo 24: $7 \cdot 7 = 49 \equiv_{24} 1$.

(b) $a = 26$, $m = 39$ $\gcd(a, m) = 13 \neq 1$, so a does not have a multiplicative inverse modulo 39.

(c) $a = 922$, $m = 77$ $922 \equiv_{77} 75$, and we can compute its inverse via the extended Euclidean algorithm:

s	t	$77s + 75t$	q
1	0	77	
0	1	75	1
1	-1	2	37
-37	38	1	

Hence 38 is the modular inverse of $75 \equiv_{77} 922$. We can double-check that $922 \cdot 38 = 35036 \equiv_{77} 1$.

N4: 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) $34x \equiv_{89} 77$

The modular inverse of 34 modulo 89 is 55. Multiplying both sides by 55 thus cancels the 34:

$$
\begin{array}{ll}
\quad 34x \equiv_{89} 77 & \\
\to & \{ \quad \text{multiply both sides by 55} \quad \} \\
\quad x \equiv_{89} 4235 & \\
\to & \{ \quad \text{reduce mod 89} \quad \}
\end{array}
$$

$x \equiv_{89} 52$

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

$5x + 17 \equiv_{23} 2x - 10$
$\rightarrow$ { subtract $2x$ from both sides }
$3x + 17 \equiv_{23} -10$
$\rightarrow$ { subtract 17 from both sides }
$3x \equiv_{23} -27$
$\rightarrow$ { reduce modulo 23 }
$3x \equiv_{23} -4$
$\rightarrow$ { $3 \cdot 8 \equiv_{23} 1$ }
$x \equiv_{23} -32$
$\rightarrow$ { reduce modulo 23 }
$x \equiv_{23} 14$

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

$200x - 13 \equiv_{1001} 0$
$\rightarrow$ { add 13 to both sides }
$200x \equiv_{1001} 13$
$\rightarrow$ { multiply both sides by -5, the modular inverse of 200 }
$x \equiv_{1001} -65$
$\rightarrow$ { reduce modulo 1001 }
$x \equiv_{1001} 936$