Number Theory I
Spring 2018

Assignment 2.1
Due January 24

Exercise 1. Use the Euclidean Algorithm to compute the following GCDs. Express each GCD as a linear combination of its arguments.

- **a.** (455,1235)
- **b.** (1248, 8421)
- **c.** (27182, 31415)

Exercise 2. Prove the following extension of Euclid's Lemma. If p is prime, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and $p | a_1 a_2 \cdots a_n$, then $p | a_i$ for some $1 \leq i \leq n$. [*Suggestion:* Induct on n.]

Exercise 3. Let $a, b \in \mathbb{Z}$. Prove that

$$\{n(a,b) \,|\, n \in \mathbb{Z}\} = \{ra + sb \,|\, r, s \in \mathbb{Z}\},$$

i.e. that the set of multiples of (a,b) is the same as the set of $\mathbb{Z}$-linear combinations of a and b.

Exercise 4. Let $a, b, n \in \mathbb{Z}$. Prove that $(na, nb) = |n|(a,b)$. [*Suggestion:* Use Bézout's Lemma and the preceding exercise to show that the two sides of the equation divide each other. Why is this sufficient?]