Math 261 — Fall 2022
Number Theory
https://sites.aub.edu.lb/kmakdisi/
Problem set 1, due Friday, September 9 at the beginning of class

Exercise 1.1: a) Find the prime factorizations of 1001, 14784, 10001, 93933, 99939, and 14853960. Feel free to use a calculator in this and in subsequent exercises.

b) Use the prime factorization to find the following GCDs (we will redo these later using the Euclidean algorithm):

$$\gcd(14784, 14853960), \qquad \gcd(93933, 99939), \qquad \gcd(10001, 100001).$$

Exercise 1.2: (A proof of Euclidean division with remainder.) Given $a, b \in \mathbf{Z}$ with $b \neq 0$. Our goal is to show the existence of q, r with $a = bq + r$ and $0 \leq r < |b|$ using the well-ordering principle. We will do this by considering the set

$$T = \{x \in \mathbf{Z} \mid \exists q \in \mathbf{Z} \text{ s.t. } x = a - bq\}.$$

Informally, $T = \{a - bq \mid q \in \mathbf{Z}\}$.

a) Show that $T \cap \mathbf{N}_0 \neq \emptyset$. (Hint: choose a q with the opposite sign to b, and which is "large" compared to a. Try to write an explicit formula for q in terms of a and b.)

b) Let r be the smallest element of $T \cap \mathbf{N}_0$. Show that $0 \leq r < |b|$. This concludes our proof, because this r is of the form $a - bq$ for some q. (Hint: what would happen if the smallest element r satisfied $r \geq |b|$? Show that one would be able to produce an even smaller element of $T \cap \mathbf{N}_0$ in that case.)

c) Since we got this far, show also that the quotient q and remainder r that we obtain from division with remainder are both unique. This means that if $a = bq + r = bq' + r'$ with $0 \leq r, r' < |b|$, show that $r = r'$ and $q = q'$.

Exercise 1.3: Let $a, b, n \geq 1$. Give two different proofs of the identity

$$\gcd(na, nb) = n \gcd(a, b),$$

the first using prime factorization, and the second using the fact that $\gcd(a, b)$ is the smallest element of $I \cap \mathbf{N}$, where $I = \{r \in \mathbf{Z} \mid \exists x, y \in \mathbf{Z} \text{ s.t. } r = ax + by\}$ is the set of "$\mathbf{Z}$-linear combinations" of a and b.

Exercise 1.4: Let $a, b \in \mathbf{Z}$ be relatively prime, which means that $\gcd(a, b) = 1$. Show that $\gcd(a + b, a - b)$ is either 1 or 2.

Exercise 1.5: The least common multiple (LCM). Given $a, b \in \mathbf{N}$, we define the least common multiple $\operatorname{lcm}(a, b) = [a, b]$ to be the smallest positive number that is simultaneously a multiple of a and of b. For example, the LCM of 15 and 6 is $[15, 6] = 30$.

a) Express $[a, b]$ in terms of the prime factorizations of a and of b. Use this to conclude that if n is **any** common multiple of a and of b, then n is a multiple of $[a, b]$.

b) One can similarly define the least common multiple of several numbers; for example, $[15, 6, 7] = 210$. Find the **prime factorization** of the least common multiple $[1, 2, 3, 4, \ldots, 30]$ of all numbers between 1 and 30 (inclusive). (Please do not multiply out the prime factors! The LCM in question is approximately 2.3×10^{12}.)

c) Show that $[a, b] \gcd(a, b) = ab$. In other words, show that the product of the GCD and the LCM of two (positive) numbers is equal to the product of those two numbers.