MTH 505: Number Theory — Spring 2020
Homework 3 — Drew Armstrong

Problem 1. Chinese Remainder Theorem. Find all integers $x \in \mathbb{Z}$ satisfying the following system of simultaneous congruences:

$$\begin{cases} x & \equiv 3 \bmod 5, \\ x & \equiv 6 \bmod 9, \\ x & \equiv 8 \bmod 11. \end{cases}$$

Problem 2. Application of Bézout's Lemma. For any $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, Bézout's Lemma tells us that $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

(a) Prove the converse. That is, if $ax + by = 1$ for some $x, y \in \mathbb{Z}$, prove that $\gcd(a, b) = 1$.

(b) Apply Bézout and part (a) to prove that

$$\gcd(ab, c) = 1 \quad \Longleftrightarrow \quad \gcd(a, c) = 1 \quad \text{and} \quad \gcd(b, c) = 1.$$

Problem 3. GCD and LCM. Let $2 = p_1 < p_2 < p_3 < \cdots$ be the sequence of all primes. Then every positive integer $a \geqslant 2$ can be expressed in the form

$$a = p_1^{a_i} p_2^{a_2} p_3^{a_3} \cdots ,$$

and is uniquely determined by the sequence of exponents $a_1, a_2, a_3, \ldots$.

(a) Prove that $a|b$ if and only if $a_i \leqslant b_i$ for all i.

(b) Prove that $\gcd(a, b)_i = \min\{a_i, b_i\}$ for all i.

(c) Prove that $\operatorname{lcm}(a, b)_i = \max\{a_i, b_i\}$ for all i.

(d) Combine (b) and (c) to prove that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. [Hint: $(ab)_i = a_i + b_i$.]

Problem 4. RSA Cryptosystem. The following message has been encrypted using the RSA cryptosystem with public key $(n, e) = (55, 23)$:

$$[17, 1, 33, 15, 1, 13, 20, 20, 9, 39, 26, 2, 14, 49, 13, 8, 2, 15, 1, 11]$$

Decrypt the message. [Hint $A = 1$, $B = 2$, $C = 3$, etc.]