NUMBER THEORY I
SPRING 2018

ASSIGNMENT 6.2
DUE FEBRUARY 21

Exercise 1. Let $n_1, n_2, \dots, n_r \in \mathbb{N}$ be pairwise relatively prime and set $N = n_1 n_2 \cdots n_r$. Recall the function from the proof of the CRT:

$$\begin{aligned} \rho : \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ a + N\mathbb{Z} &\mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \dots, a + n_r\mathbb{Z}). \end{aligned}$$

Prove that CRT implies ρ is a bijection.

Exercise 2. Let $m, n \in \mathbb{N}$ be relatively prime. Prove that

$$x = an^{\varphi(m)} + bm^{\varphi(n)}$$

provides a solution to the system

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}. \end{aligned}$$

Exercise 3. Use exercise 2 and the CRT to solve the system

$$\begin{aligned} x &\equiv 1 \pmod{11}, \\ x &\equiv 4 \pmod{12}. \end{aligned}$$