NUMBER THEORY
FALL 2023

ASSIGNMENT 11.1
DUE NOVEMBER 15

**Exercise 1.** Let $d, n \in \mathbb{N}$ with $d|n$. In class we showed that the rule $a + n\mathbb{Z} \mapsto a + d\mathbb{Z}$ yields a well-defined function

$$R : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times.$$

Show that $R$ is surjective as follows.

- **a.** Let $a, k \in \mathbb{Z}$ with $(a, d) = 1$. Show that if a prime $p$ divides $(a + kd, n)$, then $p|n$ and $p \nmid d$.
- **b.** Let $p_1, p_2, \ldots, p_r$ be the primes dividing $n$ that don't divide $d$. Use the CRT to show that there is a $k \in \mathbb{Z}$ so that $dk \equiv 1 - a \pmod{p_i}$ for all $i$.
- **c.** With $k \in \mathbb{Z}$ chosen as above, show that $(a + kd, n) = 1$. [*Suggestion:* Use parts **a** and **b** to show that $(a + kd, n)$ has no prime divisors.]
- **d.** Parts **a** - **c** show that for any $a \in \mathbb{Z}$ with $(a, d) = 1$, there exists $k \in \mathbb{Z}$ so that $(a + kd, n) = 1$. Use this to conclude that $R$ is surjective.

**Exercise 2.** Textbook exercise 7.2.1.

**Exercise 3.** Textbook exercise 7.2.14.

**Exercise 4.** Textbook exercise 7.3.1c.

**Exercise 5.** Textbook exercise 7.3.4.

**Exercise 6.** Textbook exercise 7.3.5.

**Exercise 7.** Textbook exercise 7.3.9.