NUMBER THEORY	ASSIGNMENT 7.1
FALL 2023	DUE OCTOBER 18

Exercise 1. Textbook exercise 2.5.2.

Exercise 2. Textbook exercise 2.5.5.

Exercise 3. We can provide an alternate proof of Theorem 2.9 using a little linear algebra as follows. Let $a, b, c \in \mathbb{Z}$ with $ab \neq 0$. Bézout's Lemma implies that $ax + by = c$ has a solution $(x_0\ \ y_0)^T \in \mathbb{Z}^2$ if and only if $(a, b)|c$. Assume that this is the case.

a. The equation $ax + by = c$ can be written in matrix form as

$$\underbrace{(a\ \ b)}_{A}\underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{\mathbf{x}} = c.$$

A standard result from linear algebra states that the solutions $\mathbf{x} \in \mathbb{Q}^2$ to $A\mathbf{x} = c$ are given by

$$\mathbf{x} = \mathbf{x}_0 + \mathbf{z},$$

where $\mathbf{x}_0 = (x_0\ \ y_0)^T$ and $\mathbf{z} \in \mathbb{Q}^2$ is any vector in the nullspace of A. Use the Rank Theorem to show that the nullspace of A is 1-dimensional, and is $\mathbb{Q}$-spanned by $(-b\ \ a)^T$. Conclude that the solutions to $A\mathbf{x} = c$ with $\mathbf{x} \in \mathbb{Q}^2$ are given by

$$\mathbf{x} = \mathbf{x}_0 + t\begin{pmatrix} -b \\ a \end{pmatrix}, \quad t \in \mathbb{Q}.$$

b. Continuing part **a**, show that $\mathbf{x} \in \mathbb{Z}^2$ if and only if $t(-b\ \ a)^T \in \mathbb{Z}^2$ if and only if $at, bt \in \mathbb{Z}$ if and only if $t \in \frac{1}{(a,b)}\mathbb{Z}$. [*Suggestion.* Write $ra + sb = (a, b)$ with $r, s \in \mathbb{Z}$ and multiply both sides by t.]

c. Conclude that $A\mathbf{x} = c$ with $\mathbf{x} \in \mathbb{Z}^2$ if and only if

$$\mathbf{x} = \mathbf{x}_0 + \frac{\ell}{(a,b)}\begin{pmatrix} -b \\ a \end{pmatrix}, \quad \ell \in \mathbb{Z}.$$

Show that this is equivalent to the conclusion of Theorem 2.9.