Exercises, week 12.

We recall the more general Bezout identity.

Theorem 1: Let $n, m \in \mathbb{Z}$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha n + \beta m = \gcd(n, m).$$

Exercise 1:

1. Find all the divisor of zero in $\mathbb{Z}/12\mathbb{Z}$.
2. Let $n \geq 2$. Find all the divisor of in $\mathbb{Z}/n\mathbb{Z}$.

Exercise 2: We define the

$$\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

1. Show that $\mathbb{Z}[\sqrt{2}]$ is a ring with the usual $\times$ and $+$ operation. In fact there is nothing special about 2: show that $\mathbb{Z}[\sqrt{n}]$ is a ring for all $n \in \mathbb{N}$.
2. Show that $3 + 2\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.

Exercise 3: Let R be a commutative ring. An element $x \in R$ is called *nilpotent* if there exists some $n \geq 1$ such that $x^n = 0$.

1. Let $\mathcal{N} := \{r \in R \mid r \text{ is nilpotent }\}$. Show that $\mathcal{N}$ is an ideal.
2. Let $r \in \mathcal{N}$. Show that $1 - r \in R^\times$.

Exercise 4:

1. Find the reminder of 37^{49} when divided by 7.
2. We want to find the reminder of $2^{2^{17}} + 1$ when divided by 19, we proceed in several steps.
   (a) Show that there exists some $q \in \mathbb{N}$ such that $2^{17} = 18q + 14$.
   (b) Deduce that $2^{2^{17}} + 1 \equiv 2^{14}\,[19]$
   (c) Conclude.

Exercise 5: Let p be a prime number.

1. Let $x, y \in \mathbb{Z}/p\mathbb{Z}$, such that $xy \equiv 0\,[p]$. Prove that $x = 0$ or $y = 0$.
2. Let $0 \leq k \leq p - 1$ such that $k^2 \equiv 1\,[p]$. Show that $k = 1$ or $k = p - 1$.

Exercise 6: Let X be a set, call 2^X its power set. Let $A \in 2^X$, we call $A^c := X \backslash A$. Let $A, B \in 2^X$, we define

$$A + B := (A \cap B^c) \cup (A^c \cap B),$$

and

$$A \cdot B := A \cap B.$$

Show that $(R, \cdot, +)$ is a ring, whose 0, 1, and additive inverse you will have to find.