Worksheet 14

Problems marked with a $(*)$ are "key results".

1. $(*)$ Let $n > 1$ and let $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Consider the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $f([x]) = [a] \cdot [x]$.
   (a) What can you say about f? Is it injective? Surjective? Bijective?
   (b) Set $\mathrm{Im}(f) = \{f([x]) : [x] \in \mathbb{Z}/n\mathbb{Z}\}$, the set of outputs of the function f. How do the sets $\mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Im}(f)$ compare? Are they the same? Different?

2. Let $a, n \in \mathbb{Z}$ with $n > 1$ and $\gcd(a, n) = 1$. Prove there exists some positive integer k such that $a^k \equiv 1 \bmod n$. *(Hint: what happens if two different powers of a are the same mod n?)*

For $a, n \in \mathbb{Z}$ with $n > 1$ and $\gcd(a, n) = 1$, the **order of a mod n** is defined as the smallest positive integer k such that $a^k \equiv 1 \bmod n$. We denote this as $\mathrm{ord}_n(a)$. For example, $\mathrm{ord}_4(3) = 2$ because $3^2 \equiv 1 \bmod 4$ and 2 is the smallest positive integer with this property.
The above problem says that $\mathrm{ord}_n(a)$ always exists, and translated into a statement about $\mathbb{Z}/n\mathbb{Z}$, this says for any $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ we can find an integer k such that $[a]^k = [1]$ in $\mathbb{Z}/n\mathbb{Z}$. The smallest such positive integer k with this property is called the order of $[a]$, and we'll use the same notation to denote it.

3. (a) For $n = 7$, create a table of the different powers of $[a]$ for the various $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ and use your table to compute $\mathrm{ord}_n(a)$ for $a = [1], [2], [3], [4], [5], [6]$. What patterns do you notice? Any conjectures?
   (b) For $n = 8$, create a table of the different powers of $[a]$ for the various $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ and use your table to compute $\mathrm{ord}_n(a)$ for $a = [1], [3], [5], [7]$. What patterns do you notice? Any conjectures?
   (c) Do the same thing for any other values of n that your heart desires. General pattern finding advice: first see how things behave for various primes, then prime powers, then products of primes. You could spend a very long time making tables and finding different patterns – there are *a lot* of interesting ones that you could find by doing this!

4. $(*)$ Let $a, n \in \mathbb{Z}$ with $n > 1$ and $\gcd(a, n) = 1$. Prove that $a^k \equiv 1 \bmod n$ if and only if $\mathrm{ord}_n(a) \mid k$.

5. (a) Suppose you know for some integer $n > 1$ that $3^{2088} \equiv 1 \bmod n$ and $3^{4306} \equiv 1 \bmod n$. What can you say about $\mathrm{ord}_n(3)$?
   (b) Solve the equation $x^5 \equiv 2 \bmod 7$. Can you find a way to do this without just plugging in all elements of $\mathbb{Z}/7\mathbb{Z}$? (You might find your table from 3(a) to be useful here.)