Worksheet 17

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

1. $(*)$ Let a, n, k be integers with $n > 1$ and $k \geq 1$. Prove that $\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{\gcd(\mathrm{ord}_n(a),k)}$.

2. (a) Create a table of all elements of $(\mathbb{Z}/61\mathbb{Z})^\times$ and their orders. Does every possible order appear as the order of some element? How many element of each order are there?

   (b) Do the same thing for $(\mathbb{Z}/90\mathbb{Z})^\times$. What's different? The same?

   (c) Repeat this for any other values of n that your heart desires. See if you can find any patterns!

The next few problems concern themselves with polynomials. Recall that when R is one of the sets of numbers we care about ($\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}$, etc.) that $R[x]$ denotes the set of all polynomials with coefficients in R in the variable x. The **degree** of a polynomial $f(x) \in R[x]$ is denoted by $\deg(f)$ and defined to be the largest exponent of the non-zero terms in the polynomial. Polynomials add and multiply together in the way you are familiar with from middle school.

3. Let $f(x), g(x) \in (\mathbb{Z}/5\mathbb{Z})[x]$ with $f(x) = [4]x^3 + [2]x^2 + x + [3]$ and $g(x) = [3]x^4 + [3]x^3 + [3]x^2 + x + [4]$. Compute $f(x) + g(x)$ and $f(x)g(x)$. Do the same thing but now view $f(x), g(x) \in (\mathbb{Z}/6\mathbb{Z})[x]$.

4. (a) $(*)$ Let $f(x), g(x) \in R[x]$ be polynomials, where $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$ for prime p. Prove that $\deg(fg) = \deg(f) + \deg(g)$. However, show that this need not be true when $R = \mathbb{Z}/n\mathbb{Z}$ for composite n.

   (b) Come up with conditions on the polynomials $f(x), g(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ to guarantee that $\deg(fg) = \deg(f) + \deg(g)$.

5. $(*)$ Let p be a prime and let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a non-constant polynomial of degree d. Prove that $f([a]) = [0]$ if and only if $x - [a]$ is a factor of $f(x)$.

6. (a) For prime p, what are the roots of the polynomial $x^p - x \in (\mathbb{Z}/p\mathbb{Z})[x]$?

   (b) $x^3 - x$ vanishes at every element of $\mathbb{Z}/6\mathbb{Z}$. Is there a degree 2 polynomial with that property?

7. Find all solutions to $x^2 \equiv 2 \bmod 7$. How many are there? Use that information to find all solutions to $x^2 \equiv 2 \bmod 49$. How many are there? How about solutions mod 7^3 and 7^4? Any conjectures?