Mathematics 3310.01
Homework 3
Due September 21, 2018

Please remember that if your submission is longer than one page, you must use a stapler or paper clip.

1. Let n be an integer that is 13 or larger. Prove using induction that $n^2 < 1.5^n$.

2. Let n be any integer. Show that $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer.

3. Find the remainder when 3^{255} is divided by 29.

4. Let n be any integer. Show that $n^{101} - n$ is always a multiple of 33.

5. Let $G = U_{19}$, the unit group in $\mathbf{Z}/19\mathbf{Z}$.
   (a) List all of the elements in the cyclic subgroup generated by 7.
   (b) List all of the elements in the cyclic subgroup generated by 12.
   (c) List all of the elements in the cyclic subgroup generated by 8.

6. Let $G = U_{16}$. Find a subgroup H containing 4 elements so that every element of H other than the identity has order 2. Is H a cyclic subgroup?

7. In an earlier problem set, we studied the set R, defined in this way:

> In $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$, the equation $x^2 + 1 \equiv 0$ has no solution. Just as we have done working with $\mathbf{R}$, we can invent a solution to this congruence. Let's call it α, so as not to confuse it with the imaginary number i, and we will use the rule that $\alpha^2 \equiv -1 \equiv 2$ when evaluating expressions. Let R be the ring
>
> $$\{a + b\alpha \mid a, b \in \mathbf{F}_3\}$$
>
> There are 9 elements in R, including 0, 1, and 2.

We showed that every non-zero element in R is a unit, and so R is a field with 9 elements. We will call it $\mathbf{F}_9$ from now on.
   (a) Show that the element $1 + \alpha$ has order 8. Use the entries in the multiplication table from that earlier assignment.
   (b) Find all elements of order 8 in $\mathbf{F}_9$.

8. Suppose that $(a, d) = 1$, and m is any integer. Show that we can always find k so that $(a + dk, m) = 1$. HINT: Let q be the product of all primes p so that $p|m$ and $(a, p) = 1$. Show that $(a + dq, m) = 1$.

9. Suppose that $d|m$ and $(a, d) = 1$. Show that we can find an integer b so that $a \equiv b \pmod{d}$ and $(b, m) = 1$. That suffices to show that the homomorphism $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$ from last week's homework maps U_m onto U_d.