MA 541: Modern Algebra I / Fall 2019
Problems on the cyclicity of $\mathbb{Z}_N^\times$

The first problem below will appear on one of the homework sets this semester, and will be due whenever that set it due. The rest are optional challenge problems, due thenabouts, or any time before the end of the semester.

(1) **$\mathbb{Z}_p^\times$ is cyclic.**

(a) How many roots does the polynomial $X^2 + 13X + 12$ have in $\mathbb{Z}_{35}$?

(b) Suppose G is a finite abelian group. Let M be the maximum of the orders of any of the elements of G. Prove that $g^M = 1$ for any element $g \in G$. (*Hint:* Use problem 10 on HW #6.)

(c) Let p be a prime. Assume the following statement as a black box:

$$\boxed{\text{A polynomial of degree } n \text{ has no more than } n \text{ roots in } \mathbb{Z}_p.}$$

Use part (b) to show that the group $\mathbb{Z}_p^\times$ is cyclic.

(2) **Optional challenge problem: φ is multiplicative.**

(a) Let $n \geq 1$ and $m \geq 1$ be relatively prime. Show that $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times = \mathbb{Z}_{mn}^\times$. Problem 6 from HW #5 may be helpful.

(b) Compute $\varphi(p^k)$ for p prime and $k \geq 1$.

(c) Show that φ is a *multiplicative function*: if $m, n \in \mathbb{Z}^+$ are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

(d) Derive a formula for $\varphi(n)$.

(3) **Optional challenge problem: Cyclicity of units mod odd prime powers:** Now let p be an odd prime.

(a) Show that for every $n \geq 1$ the group $\mathbb{Z}_{p^n}^\times$ has an element of order $p-1$. (*Hint:* Start with an integer a that generates $\mathbb{Z}_p^\times$ (see problem 1), and show that the order of a in $\mathbb{Z}_{p^n}^\times$ must be *divisible* by $p-1$.)

(b) Show that $1+p$ has order p^{n-1} in $\mathbb{Z}_{p^n}^\times$.
(*Hint:* for $b \in p\mathbb{Z}$ and $k \geq 1$, show that $1+b \equiv 1$ modulo p^k if and only if $(1+b)^p \equiv 1$ modulo p^{k+1}.)

(c) Conclude that $\mathbb{Z}_{p^k}^\times$ is a cyclic group.

(4) **Optional challenge problem: Which $\mathbb{Z}_N^\times$ are cyclic?**

(a) Explain where your argument in 3 above fails for $p = 2$.

(b) Show that $\mathbb{Z}_{2^k}^\times$ is never cyclic if $k \geq 3$.

(c) Show that $\mathbb{Z}_N^\times$ is cyclic if and only if $N = 1, 2, 4$, an odd prime power, or twice an odd prime power.