Mathematics 361: Number Theory
Assignment D

Reading: Ireland and Rosen, Chapter 4 (including the exercises) and into Chapter 5

For this assignment it will be very helpful to bear in mind the following result:

> Given n and e, let $\tilde{e} = \gcd(e, n)$. The multiplication-by-e map $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ given by $x \mapsto ex$ has image $\langle \tilde{e} + n\mathbb{Z} \rangle$ of order $n/\tilde{e}$, and it has kernel $\langle n/\tilde{e} + n\mathbb{Z} \rangle$ of order $\tilde{e}$, so it is $\tilde{e}$-to-1. Especially the map is an isomorphism if $\gcd(e, n) = 1$.

This result transfers to the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ where p is prime, a cyclic group having a generator g, through the isomorphism $(\mathbb{Z}/(p-1)\mathbb{Z}, +) \longrightarrow (G, \cdot)$ given by $a \mapsto g^a$. The self-map of G corresponding to $x \mapsto ex$ on $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ is $y \mapsto y^e$. Thus the eth power map on $(\mathbb{Z}/p\mathbb{Z})^\times$ is is $\tilde{e}$-to-1 and it takes the $(p-1)/\tilde{e}$ values $\{1, h, h^2, \ldots, h^{(p-1)/\tilde{e}-1}\}$ where $h = g^{\tilde{e}}$.

Problems:

Ireland and Rosen, Exercises 4.8, 4.13 as it *should* be phrased (do these first and then use them freely in working the rest of the problems); 4.1, 4.17, 4.18; 4.2 (for $p = 7, 11, 13$), 4.19; 4.10 (let $f(d) = \sum_{u:\text{ order } d} u$ and let $g(d) = \sum_{u:u^d=1} u$, which can be evaluated as a geometric sum; g has an expression in terms of f and then Möbius inversion gives f in terms of g; the exercise is requesting $f(p-1)$); 4.20 excluding the $p = 19$ part. (The more you use algebra, the less tedious these will be.)