Mathematics 361: Number Theory
Assignment #6

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

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

The multiplication-by-\(e\) map \(\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}\) given by \(x \mapsto ex\) has image \(\langle \gcd(e, n) + n\mathbb{Z} \rangle\) of order \(n/\gcd(e, n)\),
and it has kernel \(\langle n/\gcd(e, n) + n\mathbb{Z} \rangle\) of order \(\gcd(e, n)\).

Especially this applies to the map \(x \mapsto x^e\) on \((\mathbb{Z}/p\mathbb{Z})^\times\); here the abelian group is written multiplicatively, and \(n = p - 1\).

Problems:

Ireland and Rosen, Exercises 4.8, 4.13 as it should be phrased (do these first); 4.1, 4.17, 4.18; 4.2 (for \(p = 7, 11, 13\)), 4.19; 4.9; 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.)