Some remarks fields and polynomials

- Examples of infinite fields: \(\mathbb{Q}, \mathbb{R}, \mathbb{C}\).
- Finite field of size \(p^k\) exists for every prime \(p\) and \(k \geq 1\) and is unique.
- The characteristic of a field is the number of times a nonzero element is added to obtain 0. Infinite fields have characteristic 0 and finite field of size \(p^k\) has characteristic \(p\).
- **Important!** A finite field of size \(q\) is NOT isomorphic to \(\mathbb{Z}/q\mathbb{Z}\) unless \(q\) is a prime.
- For a field \(F\), \(F[x]\) denotes the set of polynomials with coefficients from \(F\). You may apply the Euclidean algorithm to do operations modulo some polynomial \(f\). This means that for any \(f, g \in F[x]\), there exists some unique \(h, r \in F[x]\) with \(\deg(r) < \deg(g)\) (or \(r = 0\)) such that
  \[
  f(x) = g(x)h(x) + r(x)
  \]

**Fermats Little Theorem**

Consider a finite field \(F\) of size \(q = p^k\). Denote the nonzero elements of \(F\) as \(F^*\). Show that any \(x \in F^*\) satisfies \(x^{q-1} = 1\).

**Bonus problem:** Show that \(F^*\) is cyclic in the sense that there is some \(x \in F^*\) such that \(\{1, x, x^2, ..., x^{q-1}\} = F^*\).

**Containment**

Let \(p\) be a prime, \(1 \leq k_1 \leq k_2\). Let \(q_1 = p^{k_1}, q_2 = p^{k_2}\), \(F_1 = F_{q_1}\) and \(F_2 = F_{q_2}\). Show that if \(k_1\) divides \(k_2\) then \(F_2\) contains a copy of \(F_1\).

**Bonus problem:** Show the converse.

**Irreducibility**

Let \(n \geq 1\) and define \(P(x) = -1 + (x-1)(x-2)...(x-n)\). Show that \(P\) is irreducible over \(\mathbb{Z}[x]\).

**Lagrange Interpolation on \(\mathbb{Z}\)**

Suppose that \(n_1, ..., n_k\) are pairwise coprime integers and let \(N = n_1 \cdot n_2 \cdot ... \cdot n_k\). Then the system of equations

\[
X \equiv b_1 \mod n_1, X \equiv b_2 \mod n_2, ..., X \equiv b_k \mod n_k
\]

has a unique solution mod \(N\). This is commonly known as the Chinese Remainder Theorem.

**Dont be lazy**

Suppose that an attacker knows that some message \(m\) is being broadcasted from a server, but each message is encrypted using RSA with different parameters. Suppose that the attacker surveys the public
keys and finds $k$ many pairs of the form $(n_1, e), \ldots, (n_k, e)$ where the encryption key $e$ is the same for all $i$ and the $n_i$s are pairwise coprime. Show that if $k \geq e$, then the attacker can decipher the message $m$. 