HOMEWORK 2

There will be an in-class quiz on the material in this homework Thursday October 17th.
(1) Let $p, q$ be distinct prime numbers. Show the following are equivalent:
  \begin{itemize}
  \item $p$ is a quadratic residue mod $q$;
  \item $q$ is a quadratic residue mod $p$.
  \end{itemize}

(2) For each integer $N$ let $\Phi_N(x) = x^{N-1} + x^{N-2} + \cdots + x + 1$ be the $N$th cyclotomic polynomials. Classify the prime numbers $p$ for which $\Phi_N(x)$ is irreducible over $\mathbb{F}_p$.

(3) For which integers $n$ is the polynomial $x^3 + nx + 2$ irreducible in $\mathbb{Z}[x]$?

(4) Let $p$ be a prime number and $f(x) \in \mathbb{F}_p[x]$. Given a polynomial $h(x)$ let $R(h(x))$ denote the remainder of $h(x)$ when divide by $f(x)$, so
  \[ h(x) = q(x)f(x) + R(x) \] and $0 \leq \deg(R(x)) < \deg(f(x))$.
  Suppose that $h(x)$ is a polynomial such that $R(h(x^p)) = h(x)$. Show that $f(x)$ divides the following polynomial:
  \[ h(x)(h(x) - 1)(h(x) - 2) \cdots (h(x) - (p - 1)) \]

(5) Understand the proof of Theorem 2.2.5 from Prasolov’s Polynomials.