Homework on §20
Due: Thursday, April 11

A. Silverman 20.3.

B. Suppose that p is a prime with $p \equiv 1 \pmod 3$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

   (a) Show that if a is a cubic residue, then $a^{(p-1)/3} \equiv 1 \pmod p$.

   (b) ~~Show the converse.~~

C. Write a program that implements the CRT for an arbitrary list of moduli. The input should be a list of ordered pairs $[(a_1, m_1), (a_2, m_2), \ldots, (a_n, m_n)]$ where the m_i are pairwise relatively prime, and the output should be a such that $a \equiv a_i \pmod{m_i}$ for all i. Remember to prove your algorithm works!

D. Let $f(x)$ be a polynomial, and suppose $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Show that $f(x) \equiv 0 \pmod{mn}$ has a solution if and only if $f(x) \equiv 0 \pmod m$ and $f(x) \equiv 0 \pmod n$ both have solutions.

E. (a) Find all solutions to $x^2 \equiv 1 \pmod{143}$ using the Chinese Remainder Theorem.

   (b) Let p, q be distinct primes. How may solutions does $x^2 \equiv 1 \pmod{pq}$ have?

   (c) Let $p_1, p_2, \ldots, p_r$ be distinct primes. How many solutions does $x^2 \equiv 1 \pmod{p_1 p_2 \cdots p_r}$ have?