Number Theory and Cryptography
Homework 2 (due 1/31)

1. Prove the "extended Euclid lemma": Given a prime p and nonzero integers $a_1, \ldots, a_k \in \mathbf{Z}$, then $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_k)$ implies that $p|a_i$ for some $1 \leq i \leq k$.

2. Prove that for any $n \in \mathbf{N}$, any prime p such that $p|(n! + 1)$ satisfies $p > n$. Deduce from this another proof of the infinitude of primes.

3. Given nonzero integers $a, b \in \mathbf{Z}$, prove that a given $c \in \mathbf{Z}$ can be written in the form $c = ma + nb$ for some $m, n \in \mathbf{Z}$ if and only if $(a, b)|c$.

4. Given nonzero integers $a, b \in \mathbf{Z}$, the *least common multiple of a and b* is the smallest positive integer n such that $a|n$ and $b|n$. Write $\mathrm{lcm}(a, b)$ for this integer.

i) Prove that $\mathrm{lcm}(a, b)$ is well-defined. (Hint: Use the least element principle.)

ii) Prove that $\mathrm{lcm}(a, b) = \frac{ab}{(a,b)}$.

5. In the decimal expansion of 99!, how many zeros does it end with?

6. Figure out which of the following elements exist in $\mathbf{Z}_{13}$: $1/4$, $\sqrt{-1}$, $\sqrt{3}$, $5^{1/3}$, $7^{1/5}$.