Lior Silberman's Math 312: ComPAIR Assignment 3

- This assignment is due Wednesday, 3/3/2021 at noon (Vancover time)
- Comparisons are due Sunday, 7/3/2021 at 11pm (Vancouver time).

1. (pth powers are funny mod p) Fix a prime number p.
   (a) ("Binominal formula") Prove by induction on $n \geq 0$ that $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. You may use the identity $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.
   (b) Let p be a prime number and let $0 < k < p$. Show that $p \mid \binom{p}{k}$.
   (c) Show that $(x+y)^p \equiv x^p + y^p \, (p)$.
   (d) (Fermat's Little Theorem) prove by induction on a that $a^p \equiv a \, (p)$.
   RMK In class we showed that $a^{p-1} \equiv a$ if a is invertible mod p, which can be deduced from part (d) by multiplying by $\bar{a}$.

2. Let $M = m_1 \cdots m_r$ where the m_i are pairwise relatively prime.
   (a) Suppose a is invertible mod M. Show that a is invertible mod each m_i (hint: you need an inverse ...).
   (b) Suppose a_i is invertible mod each m_i, and let a mod M be such that $a \equiv a_i \, (m_i)$ for all i as in the CRT. Show that a is invertible mod M.
   (c) Let $\phi(M)$ be the number of invertible residue classes mod M. Show that $\phi(M) = \prod_{i=1}^{r} \phi(m_i)$.