Homework 2

Madilyn Simons

1. By definition, $\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{k!(p-k)!}$. Since $k < p$ and $p - k < p$, neither $k!$ nor $(p-k)!$ have any prime factors that divide p, and $\frac{p!}{k!(p-k)!}$ is an integer, $\frac{(p-1)!}{k!(p-k)!}$ must also be an integer. This implies that $p|\binom{p}{k}$.

2. By definition of binomial coefficients,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k = (a^p + b^p) + \sum_{k=1}^{p-1}(\binom{p}{k} a^{p-k}b^k).$$

   Since $p|\binom{p}{k}$ for all $k < p$ and all numbers between 1 and p-1 (inclusive) as less than p, $\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k$ is divisible by p. This means that $\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k \equiv 0 \pmod{\text{p}}$. Consequently,

$$(a^p + b^p) + \sum_{k=1}^{p-1}(\binom{p}{k} a^{p-k}b^k) \equiv (a^p + b^p) + 0 \equiv a^p + b^p (\text{mod } p).$$

3. Let a be some element of $\mathbb{Z}/m\mathbb{Z}$. Assume a is a unit and let a^{-1} be its inverse. Also assume a is a zero divisor and let $ab \equiv 0 \pmod{m}$ for some non-zero element b of $\mathbb{Z}/m\mathbb{Z}$ (by definition of zero divisor). As such,

$$a^{-1}ab \equiv (a^{-1}a)b \equiv 1b \equiv b (\text{mod } m)$$

   and

$$a^{-1}ab \equiv a^{-1}(ab) \equiv a^{-1}(0) \equiv 0 (\text{mod } m)$$

   Thus, $b \equiv 0 \pmod{m}$. This is a contradiction. Therefore, a cannot be a zero divisor and a unit.