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 $\sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \equiv 0$ (mod p). Consequently,

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