

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) are less than p , $\sum_{k=0}^p \binom{p}{k} a^{p-k} b^k$ is divisible by p . This means that $\sum_{k=0}^p \binom{p}{k} a^{p-k} b^k \equiv 0 \pmod{p}$. Consequently,

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

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 nonzero element b of $\mathbb{Z}/m\mathbb{Z}$ (by definition of zero divisor). As such,

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

and

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

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

4. Let a be some nonzero element of $\mathbb{Z}/m\mathbb{Z}$. Either $(a, m) = 1$ or $(a, m) > 1$. First, let $(a, m) = 1$. If $(a, m) = 1$, then a is a unit and we are done. Next, let $(a, m) = c$ for some c such that $c > 1$. Let $a = p_0^{a_0} p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of a such that $a_i \geq 0$ for all i . Similarly, let $m = p_0^{m_0} p_1^{m_1} \dots p_k^{m_k}$ be the prime factorization of m such that $m_i \geq 0$ for all i . Since a and m are not relatively prime and a is a nonzero element, there exists some $d = p_0^{\max(a_0, m_0)} \dots p_k^{\max(a_k, m_k)}$, which is divisible by a and is a zero element of $\mathbb{Z}/m\mathbb{Z}$. Let $x = p_0^{x_0} \dots p_k^{x_k}$ such that $x_i \cdot a_i =$

$\max(a_i, m_i)$ for all i . Thus, $ax \equiv d \equiv 0 \pmod{m}$. We know that x is a nonzero element because x could only be a nonzero element if $x_i = 0$ for all i , implying that $\max(a_i, m_i) = 0$ for all i (which would only be true if $a = 1$ and $p = 1$). Therefore, if $(a, m) \neq 1$, then a is a zero divisor.