Question 1.

(a) Prove that if $n > k$ and $\gcd(n, k) = 1$, then $n \mid \binom{n}{k}$.

Recall that the chairperson identity: for integers $n > k$,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

By definition, $k \mid n\binom{n-1}{k-1}$, but since n and k are coprime, it must be true that $k \mid \binom{n-1}{k-1}$. Thus $\frac{1}{k}\binom{n-1}{k-1} \in \mathbb{N}$ and

$$\binom{n}{k} = n \cdot \frac{1}{k}\binom{n-1}{k-1},$$

so $n \mid \binom{n}{k}$.

(b) Then, show that $(a+b)^n \equiv a^n + b^n \pmod{n}$ when n is prime.

Using the binomial theorem,

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

But notice that for all k with $0 < k < n$, we have that $\gcd(n, k) = 1$, so by the previous part, $n \mid \binom{n}{k}$ and

$$\binom{n}{k} a^k b^{n-k} \equiv 0 \pmod{n}.$$

Thus

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

as needed.

(c) Find two examples (that have different a, b, n) that show that if n is composite, then the statement in part (b) may or may not hold.

For the first example, let $n = 4, a = b = 1$. We have that

$$(1+1)^4 = 16 \equiv 0 \pmod{4}$$

but

$$1^4 + 1^4 \equiv 2 \pmod{4}$$

which shows that the statement does not hold.

Next, let $n = 6, a = 0, b = 2$. It is easy to see that

$$(a+b)^n = 2^6 = b^n$$

so the statement will hold, even though n is not prime.