definition $\binom{n}{k} = \begin{cases} n \geq k & \frac{n!}{k!(n-k)!} \\ n < k & 0 \end{cases}$

Lemma 1 Given a prime p and a natural number k such that $0 < k < p$ then $p \mid \binom{p}{k}$.
Proof: Note that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Since p is prime, and $k < p$ and $p - k < p$, then there is no number which divides p in that range, therefore p cannot be divided out of the numerator.

Coro Given a prime p, then $(1+x)^p \equiv 1 + x^p \mod p$.
Proof: By the binomial theorem $(1+x)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = \binom{p}{0} + \binom{p}{p} x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k \equiv 1 + x^p + 0 \mod p = 1 + x^p$

Coro 2 Given a prime p, for all $i \in \mathbb{N} \cup \{0\}$, $(1+x)^{p^i} \equiv 1 + x^{p^i}$.
We have already shown the base case in the form of coro 1. By the principle of mathematical induction for all $j \in \mathbb{N}$ if $j < i$ then $(1+x)^{p^j} \equiv 1 + x^{p^j} \mod p$. Since $i - 1 < i$, then by the induction hypothesis $(1+x)^{p^{i-1}} \equiv 1 + x^{p^{i-1}} \mod p$. Therefore $(1+x)^{p^i} = (1+x)^{p^{i-1}p} = ((1+x)^{p^{i-1}})^p \equiv (1+x^{p^{i-1}})^p \mod p = \sum_{k=0}^{p} \binom{p}{k} x^{p^{i-1}k} \equiv 1 + x^{p^i}$
.

Lemma 2 Given any natural number n and d, there exists a unique $q, r \in \mathbb{Z}_{\geq 0}$ such that $0 \leq r < d$ where $n = dq + r$.
Proof: We have two cases: if $d \mid n$ and $d \nmid n$. If $d \mid n$, then by definition of divisibility there exists $k \in \mathbb{N}$ such that $n = kd$, which gives us our unique q and $r = 0$. Suppose $d \nmid n$. Then we can define the set S where $S = \{m \in \mathbb{Z}_+ : d \mid n - m\}$. Note that this set is non-empty as $n \in S$ since d divides 0. Therefore by the well ordering principle S contains a smallest element. Let's call the smallest element g. This element provides the existance for the element q as $n - g = dq$. We must check if g checks our requirements. Since g is a positive integer then $g \geq 0$ by definition. Therefore we must check $g < d$. Suppose for contradiction that $g \geq d$. This provides 2 cases for g, if $g = d$ and $g > d$. Suppose $g = d$. Then we have $dq + g = d(q+1)$, contradicting the fact that $d \nmid n$. Suppose $g > d$. Then we have that $g - d > 0$. Let $g - d = g_1$. Therefore $n - g_1 = n - g + d = dq + g - g + d = d(q+1)$, thus $g_1 \in S$. However this contradicts the fact that g is the smallest element in S as $g_1 < g$. Therefore $0 \leq g < d$, thus setting $g = r$ and $q = \frac{n-g}{d}$ satisifes the requirements.

Uniqueness: Suppose $n = db_1 + b_2 = dc_1 + c_2, 0 \leq b_2, c_2 < d$. Then $-d < b_2 - c_2 < d$. Since $b_2 - c_2 = d(c_1 - b_1)$ then $-1 < c_1 - b_1 < 1$. Therefore $c_1 - b_1 = 0$, thus $c_1 = b_1$. Thus $c_2 = b_2$.

Lemma 3 Given any natural number d and non-negative integer n then there exist $r_0, \ldots, r_m \in \mathbb{Z}_{\geq 0}, 0 \leq r_i < d$ for all i such that $n = d^m r_m + \ldots dr_1 + r_0$.

By PMI for all $k \in \mathbb{N}$ if $k < n$ then there exists $s_0, \ldots s_l \in \mathbb{Z}_{\geq 0}, 0 \geq s_i <$ such that $k = d^l s_l + \ldots + ds_1 + s_0$. By lemma 2

Lucas' Theorem Given any $m, n \in \mathbb{N} \cup \{0\}$, $\binom{m}{n} = \prod_{i=0}^{k} \binom{m_i}{n_i}$, where $m = m_k p^k + \ldots + m_1 p + m_0, n = n_k p^k + \ldots + n_1 p + n_0$