Lemma. *Let S be a linearly independent subset of a vector space V over $\mathbb{F}$, and let x be an element of V that is not in S. Then $S \cup \{x\}$ is linearly dependent if and only if $x \in \operatorname{span} S$.*

Proof. By definition of linear dependence, if $S \cup \{x\}$ is linearly dependent, then

$$\exists(x_1, x_2, \ldots, x_n \in (S \cup \{x\}),\ a_1, a_2, \ldots, a_n \in \mathbb{F}, \prod_{i=1}^{n} a_1 a_2 \cdot \ldots \cdot a_n \neq 0) : \sum_{i=1}^{n} a_i x_i = 0.$$

Since S is linearly independent, one of x_i is equal to x. Without loss of generality assume that $x_1 = x$. Thus, $x = a_1^{-1}(-a_2 x_2 - \cdots - a_n x_n)$. Hence, x is a linear combination of vectors in S and thus $x \in \operatorname{span}(S)$.

Conversely, suppose that $x \in \operatorname{span}(S)$. Then, by the definition of span, $\exists(x_1, x_2, \ldots, x_n \in S,\ a_1, a_2, \ldots, a_n \in \mathbb{F}) : x = \sum_{i=1}^{n} a_i x_i$. Thus, $-x + \sum_{i=1}^{n} a_i x_i = 0$. Since all x_i and x are distinct, $\{x_1, \ldots, x_n, x\} = S \cup \{x\}$ is linearly dependent.

□

Theorem. *Let V be a vector space with a finite number of elements q, defined over $\mathbb{Z}_p$, where p is prime $(p \in \mathbb{P})$. Then $\exists(m \in \mathbb{Z}^+) : q = p^m$.*

Proof. If $V = 0$, then 0 is a basis for V. Since $q = 1$ and $\forall(p \in \mathbb{P}) : p^0 = 1 = q$, then the statement holds in case $V = 0$.

Otherwise, there exists a non-zero element x_1. Note that $\{x_1\}$ is a linearly independent subset of V, since x_1 is non-zero and $a x_1 = 0\ \exists(a \in \mathbb{Z}_p)$ if and only if $a = 0$.

If there are any other elements in V, continue picking elements $x_2, \ldots, x_k \in V$ such that $S := \{x_1, x_2, \ldots, x_k\}$ is linearly independent.

Since V has a finite number of elements, this procedure eventually terminates.

Take $x \in V$. If $x \in S$, then $x \in \operatorname{span}(S)$. If $x \notin S$, then by construction of S, $S \cup \{x\}$ is linearly dependent. But then by the Lemma, $x \in \operatorname{span}(S)$. Thus, all the elements of V are in S.

On the other hand, since V is closed under addition and scalar multiplication, $\operatorname{span}(S) \subseteq V$.

Hence, S is a basis of V and is finite.

Suppose that $\#(S) = m \in \mathbb{Z}^+$. Proceed to count the number of all the possible linear combinations of elements in S.

Since there are p possible values for each scalar, these scalars can be combined in p^m ways. But the set of all the linear combinations is span by definition, and since $V = \operatorname{span}(S) = q$, then $q = p^m$.

□