Suppose that $S \subset \mathbb{F}_p^2$ (the vector space of dimension 2 over the finite field $\mathbb{F}_p$) with $|S| = p$. Show that S can contain at most $O(p^{3/2})$ pairs of vectors (remember, S is a collection of vectors with two coordinates) $(x_1, y_1), (x_2, y_2)$ such that

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 \ = \ 1. \tag{1}$$

A key fact that you will need is that a pair of circles in $\mathbb{F}_p$ can meet in at most 2 points (unless they are the same circle), just like in the usual two-dimensional plane $\mathbb{R}^2$.

Hint: Suppose that, on the contrary, there are more than, say, $cp^{3/2}$ (for some $c \geq 1$) pairs of points in S satisfying (1). Let $(u_1, v_1) \in S$ be any point having the most number of points $(u_2, v_2) \in S$ that are a distance 1 away from it – i.e. (u_1, v_1) has the most associated points $(u_2, v_2) \in S$ satisfying

$$(u_1 - u_2)^2 + (v_1 - v_2)^2 \ = \ 1.$$

Let A_1 denote the set of all such pairs (u_2, v_2) given that point (u_1, v_1). Then let $(u_1', v_1') \in S$ denote the point with the second-largest number (there could be a tie here – the largest and second-largest numbers could equal) of points $(u_2', v_2') \in S$ that are a distance 1 away, and let A_2 denote the set of those points (u_2', v_2'). Continue producing the sets $A_3, A_4, ...$ like this. Explain why $|A_1| \geq p^{1/2}$, and obtain similar lower bounds for $|A_2|, |A_3|, ...$ Now use problem 1.1.3 from the Tao-Vu book to obtain a contradiction.