Riddle from Assaf

November-28-13 4:49 AM

In a finite field there is always a solution to

$$x^2+y^2+1=0$$

Pf. Enough to work in $\mathbb{Z}/p$. If $p=2$, take $x=0$, $y=1$. If $p>2$,

$$|\{x^2 : x\in\mathbb{Z}/p\}| = \frac{p+1}{2} > p/2$$

and

$$|\{-1-y^2 : y\in\mathbb{Z}/p\}| = \frac{p+1}{2} > p/2$$

So by pigeonhole, these subsets of $\mathbb{Z}/p$ must intersect. □