EVERY CONIC HAS A POINT OVER $\mathbb{F}_p$ (EXERCISE 14)

RANKEYA DATTA

The title is self explanatory and we will just start with the proof. So, let $F \in \mathbb{F}_p[X_0, X_1, X_2]$ be a conic. It suffices to prove that F has a point other than $(0,0,0)$ in ${\mathbb{F}_p}^3$. Let $V(F)$ denote the set of zeroes of F in ${\mathbb{F}_p}^3$. Consider the polynomial F^{p-1}. For all $x \in V(F)$, $F^{p-1}(x) = F(x)^{p-1} = 0$, and for all $x \in {\mathbb{F}_p}^3 - V(F)$, $F^{p-1}(x) = F(x)^{p-1} = 1$.

Let $G = F^{p-1}$. Then $|{\mathbb{F}_p}^3 - V(F)| \equiv \sum_{x \in {\mathbb{F}_p}^3} G(x) \pmod p$.

I claim that $\sum_{x \in {\mathbb{F}_p}^3} G(x) \equiv 0 \pmod p$. Since $p \| {\mathbb{F}_p}^3|$, it will follow that $p \| V(F)|$. But, F is homogeneous, so we already know that $(0,0,0) \in V(F)$. As $p > 1$, it follows that $|V(F)| > 1$, proving the result.

Now, G is the sum of monomials $M_a = bX_0{}^{a_0}X_1{}^{a_1}X_2{}^{a_2}$, where $a_0 + a_1 + a_2 = 2(p-1)$, and $b \neq 0$. Hence, to find $\sum_{x \in {\mathbb{F}_p}^3} G(x)$, it suffices to determine $\sum_{x \in {\mathbb{F}_p}^3} M_a(x) = \sum_{x \in {\mathbb{F}_p}^3} bx_0{}^{a_0}x_1{}^{a_1}x_2{}^{a_2} = b(\sum_{x_0 \in \mathbb{F}_p} x_0{}^{a_0})(\sum_{x_1 \in \mathbb{F}_p} x_1{}^{a_1})(\sum_{x_2 \in \mathbb{F}_p} x_2{}^{a_2})$. So, the problem reduces to calculating sums of the form $\sum_{z \in \mathbb{F}_p} z^\beta$, where $\beta \in \mathbb{N} \cup \{0\}$.

(1)If $\beta = 0$, then $\sum_{z \in \mathbb{F}_p} z^\beta = 0$, with the convention that $0^0 = 1$.

(2)If $\beta > 0$, then $0^\beta = 0$. So, $\sum_{z \in \mathbb{F}_p} z^\beta = \sum_{z \in \mathbb{F}_p^*} z^\beta$. Now, $\mathbb{F}_p^*$ is cyclic of order $p-1$. Let ω generate $\mathbb{F}_p^*$. Then, $\sum_{z \in \mathbb{F}_p^*} z^\beta = \sum_{0 \leq j \leq p-2} \omega^{j\beta}$, which is a geometric progression. Thus:

(a) If $\omega^\beta \neq 1$, i.e., β is not a multiple of $p-1$, then $\sum_{0 \leq j \leq p-2} \omega^{j\beta} = \frac{\omega^{\beta(p-1)}-1}{\omega^\beta - 1} = 0$ (since $\omega^{p-1} = 1$).

(a′) If $\omega^\beta = 1$, i.e., β is a multiple of $p-1$, then $\sum_{0 \leq j \leq p-2} \omega^{j\beta} = p-1$.

It follows from (1), (a) and (a′) that $\sum_{x \in {\mathbb{F}_p}^3} bx_0{}^{a_0}x_1{}^{a_1}x_2{}^{a_2}$ vanishes unless a_0, a_1, a_2 are all non-zero and multiples of $p-1$. In this case $a_0 + a_1 + a_2$ is at least $3(p-1)$, contradicting that $a_0 + a_1 + a_2 = 2(p-1)$. So, the latter case can never happen, and so $\sum_{x \in {\mathbb{F}_p}^3} M_a(x) = \sum_{x \in {\mathbb{F}_p}^3} bx_0{}^{a_0}x_1{}^{a_1}x_2{}^{a_2} = 0$. This proves that $\sum_{x \in {\mathbb{F}_p}^3} G(x) = 0$, since G is the sum of the monomials M_a. This completes the proof.

Remark: This result is due to Chevalley, and can be easily generalized to finite fields of any order, as long as the degree of the homogeneous polynomial is less that the number of variables.