Proof. Let $a,b \in \mathbb{Z}$ be two fixed integers and let

$$S(d,t) = \{(x,y) \in I \times I \mid ax+by \equiv td \pmod{n}\}.$$

Then the union of $S(d,t)$ for all such d and t is a subset of $I \times I$. This union indeed contains all elements of $I \times I$. To see this, let $(x,y) \in I \times I$ and let $d = (ax+by,n)$. Pick $1 \le t \le \frac{n}{d}$ such that $t \equiv \frac{ax+by}{d} \pmod{\frac{n}{d}}$. Then $(t,\frac{n}{d}) = 1$ and $ax+by \equiv td \pmod{n}$. Thus, $(x,y) \in S(d,t)$. Finally, if $S(d,t) \cap S(d',t') \neq \varnothing$, then choose one pair (x,y) in this intersection. We obtain $d = (ax+by,n) = d'$. Furthermore, $td \equiv t'd \pmod{n}$ implies that $t \equiv t' \pmod{\frac{n}{d}}$. Since $1 \le t,t' \le \frac{n}{d}$, we have $t = t'$. □

4. Proof of the Main Result

Recall that we aim at showing the following sum

$$N(q,\ell) = \sum_{\substack{1\le t\le q-1,\\ (t,q-1)=1}} N_{g^t}$$

is not equal to zero where g is a fixed generator of $\mathbb{F}_q^\times$. It's not hard to see that if $g^tL = g^sL$ then $N_{g^t} = N_{g^s}$. We have the following reduction for $N(q,\ell)$.

Proposition 4.1. *Let g be generator of $\mathbb{F}_q^\times$ and $\ell \mid q-1$. Then*

$$N(q,\ell) = \frac{\varphi(q-1)}{\varphi(\ell)} \sum_{\substack{1\le t\le \ell,\\ (t,\ell)=1}} N_{g^t}.$$

Proof. By the definition of $N(q,\ell)$, it is a sum indexed by all elements of $(\mathbb{Z}/(q-1)\mathbb{Z})^\times$. Recall that $(\mathbb{Z}/(q-1)\mathbb{Z})^\times = M \cdot N$ where M and N are given in Lemma 3.1 for $n = q-1$ and $d = \ell$. Note that if $t_1 \in N$, then $t_1 \equiv 1 \pmod{\ell}$ and $g^{t_1}L = gL$. It follows that $N_{g^{t_1 t_2}} = N_{g^{t_2}}$ for any integer t_2. Hence,

$$N(q,\ell) = \sum_{t\in(\mathbb{Z}/(q-1)\mathbb{Z})^\times} N_{g^t} = \sum_{t_1\in N}\sum_{t_2\in M} N_{g^{t_1t_2}} = |N| \sum_{t_2\in M} N_{g^{t_2}}.$$

The result follows since $|N| = \frac{\varphi(q-1)}{\varphi(\ell)}$ and $M \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$. □

Recall from (5) that

$$N_{g^t} = q + \sum_{1\le j,k\le \ell-1} \chi^j(-g^{-2t})\chi^k(-g^{-t})J(\chi^j,\chi^k)$$

where χ is a nontrivial character of $\mathbb{F}_q$ of order ℓ. We can rewrite N_{g^t} as follows.

Lemma 4.2. *For $1 \le t \le \ell$ and $(t,\ell) = 1$,*

$$N_{g^t} = q+1+ \sum_{\substack{1\le j,k\le \ell-1,\\ j+k\neq \ell}} \chi(-1)^{j+k}\chi(g^{-1})^{(2j+k)t}J(\chi^j,\chi^k).$$