give the following table for each case.

q	9	13	17	25	29	37	41	49
g	α	2	3	β	2	5	6	γ
x	α	4	6	1	4	2	3	2
y	α	1	2	β^2	4	2	3	$2\gamma^7$

where $\alpha = 1+\sqrt{-1}$ in $\mathbb{F}_9 = \mathbb{F}_3(\sqrt{-1})$, $\beta = 1+2\sqrt{2}$ in $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2})$ and $\gamma = 4+\sqrt{-1}$ in $\mathbb{F}_{49} = \mathbb{F}_7(\sqrt{-1})$.

This completes the verifications of all cases in which $N_g > 0$. Moreover, we've exhibited all solutions (x,y) such that $xy \neq 0$ and thus finish the proof. □

We would like to point out that it's possible to prove Corollary 2.3 by using the bound (6) without applying the Hasse-Weil bound.

In view of Conjecture C, we only need to find a generator g of $\mathbb{F}_q^\times$ such that $\mathscr{C}_g(\mathbb{F}_q)$ is non-empty. Instead of computing N_g, our goal is to show that the following sum

$$N(q,\ell) = \sum_{\mathbb{F}_q^\times = \langle g' \rangle} N_{g'} = \sum_{\substack{1 \le t \le q-1, \\ \gcd(t,q-1)=1}} N_{g^t}$$

is a positive integer under appropriate conditions.

3. Key Ingredients

In this section, we gather tools and results that are needed for the proof of Theorem A. To simplify the notation, we'll put $(a_1,a_2) = \gcd(a_1,a_2)$, the greatest common divisor of integers a_1 and a_2. The following lemma is an elementary fact in algebra which we will use repeatedly. As one can easily find a proof in any algebra text book, we skip the proof here.

Lemma 3.1. *Let $n \in \mathbb{N}$ and let d be a divisor of n. Then the canonical group homomorphism*

$$\pi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$$

induced by

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ k+n\mathbb{Z} & \mapsto & k+d\mathbb{Z} \end{array}$$

is surjective. Furthermore, this homomorphism splits. Namely, there exists a subgroup M of $(\mathbb{Z}/n\mathbb{Z})^\times$ which is isomorphic to $(\mathbb{Z}/d\mathbb{Z})^\times$ under π and $(\mathbb{Z}/n\mathbb{Z})^\times = M \cdot N$ where $N = \ker(\pi)$.

For $n \in \mathbb{N}$ and $m \in \mathbb{Z}$, the *Ramanujan's sum* $c_n(m)$ ([Ram18] or [HSW00, pp. 179–199]) is defined by

$$c_n(m) = \sum_{\substack{1 \le t < n, \\ (t,n)=1}} \zeta_n^{mt}$$