

With this lower bound, one can easily verify the truth of Conjecture [C](#) (and Conjecture [B](#)) for small values of ℓ . The following results are direct consequences of Theorem [1](#). For the reader's convenience, we give a proof.

Corollary 2.3. *For $1 \leq \ell \leq 4$, we have $N_g > 0$ for every generator g of \mathbb{F}_q^\times . Moreover, there exists a point $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ such that $xy \neq 0$ and hence Conjecture [C](#) holds for the case where $\ell_0 = [\mathbb{F}_p^\times : H] \leq 4$.*

Proof. As it's easy to deduce the conclusion if $\ell = 1$, we leave the verification of this case to the reader. Let's first consider the case where $\ell = 2$. Notice that in this case $p > 2$ and $g_\ell = 0$. Therefore, $\widetilde{N}_g = q + 1$ by Theorem [1](#). It's not hard to verify that

$$N_g = \begin{cases} \widetilde{N}_g & \text{if } q \equiv 1 \pmod{4} \\ \widetilde{N}_g - 2 & \text{if } q \equiv 3 \pmod{4} \end{cases}.$$

Therefore, $N_g = q + 1$ if $q \equiv 1 \pmod{4}$ and $N_g = q - 1$ if $q \equiv 3 \pmod{4}$. In either case, we clearly have $N_g > 0$. It remains to show that there exists a point $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ such that $xy \neq 0$. Observe that there are at most four points in $\mathcal{C}_g(\mathbb{F}_q)$ with either $x = 0$ or $y = 0$. In the case where $q \equiv 1 \pmod{4}$ we have $N_g = q + 1 \geq 6$. It remains to look at the case where $q \equiv 3 \pmod{4}$. Since $\ell = 2$ is a proper divisor of $q - 1$ by assumption, we see that $q \geq 7$ and we also have $N_g = q - 1 \geq 6$. Now, it's clear that there's a point $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ such that $xy \neq 0$ since $N_g > 4$ in both cases.

Next, we consider the cases where $\ell = 3$ and 4. Since $\ell > 2$, we have that $N_g = \widetilde{N}_g$ by Lemma [2.1](#). Suppose that $\ell = 3$. In this case $\widetilde{\mathcal{C}}_g$ is of genus one. Then the Hasse-Weil bound gives that

$$N_g \geq (q + 1) - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0.$$

Therefore, $N_g > 0$ for any generator g of \mathbb{F}_q^\times in this case. Suppose that there exists a solution (x, y) to Equation [\(3\)](#) such that either $x = 0$ or $y = 0$ for $\ell = 3$. Then we get that either g or g^2 is a cube in \mathbb{F}_q^\times . This implies that the order of gL in the group \mathbb{F}_q^\times/L divides 2 which is absurd since $|\mathbb{F}_q^\times/L| = 3$. Therefore, any $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ must satisfy $xy \neq 0$ as desired.

Assume that $\ell = 4$. A direct computation shows that for $q > 49$, we have that $N_g > 8$. Since there are at most eight solutions to Equation [\(3\)](#) such that either $x = 0$ or $y = 0$ for $\ell = 4$, we see that for $q > 49$ there exists $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ such that $xy \neq 0$ as asserted. It remains to check prime power numbers q satisfying $q \leq 49$ such that 4 is a proper divisor of $q - 1$. Hence, we are left with eight cases where $q = 9, 13, 17, 25, 29, 37, 41, 49$ to verify. Note that if $(x, y) \in \mathcal{C}_g(\mathbb{F}_q)$ with $xy \neq 0$ then $(x^{-1}, x^{-1}y) \in \mathcal{C}_{g^{-1}}(\mathbb{F}_q)$. It follows that $\mathcal{C}_g(\mathbb{F}_q)$ contains a point whose coordinates are nonzero if and only if $\mathcal{C}_{g^{-1}}(\mathbb{F}_q)$ has this property as well. Also, for any generator g' of \mathbb{F}_q^\times we have $g'L \in \{gL, g^{-1}L\}$ in the case where $|\mathbb{F}_q^\times/L| = 4$. It follows that $\mathcal{C}_g(\mathbb{F}_q)$ contains a point whose coordinates are nonzero if and only if $\mathcal{C}_{g'}(\mathbb{F}_q)$ has this property as well. Hence, it suffices to show that $\mathcal{C}_g(\mathbb{F}_q)$ containing a point with nonzero coordinates for just one generator g of \mathbb{F}_q^\times . We