The Relative Trace-Zero Subgroup of the Barreto-Naehrig Curves

Julius Zhang[1,2]

[1]Courant Institute of Mathematical Sciences, New York University
[2]LayerZero Labs

June 23, 2026

We prove a result in [BN05] which is assumed to be well-known in cryptography literature, but the proof does not appear to be explicitly written down. Certain literature uses weaker results.

Recall that the Barreto-Naehrig (BN) family curve is parameterized by the equation $E : y^2 = x^3 + b$ over $\mathbb{F}_q$ with embedding degree 12, where b varies with the curve. The order of the group of $\mathbb{F}_q$-rational points on the curve is $n = |E(\mathbb{F}_q)|$, which is an odd prime number not equal to q in the BN parameterization, where the BN curve is instantiated over a prime base field $\mathbb{F}_q$.

We work with the standard definitions of the input pairing subgroups following [Cos12]:

$$\mathbb{G}_1 = E[n] \cap \ker(\text{Frob} - [1]), \tag{1}$$
$$\mathbb{G}_2 = E[n] \cap \ker(\text{Frob} - [q]), \tag{2}$$

where Frob is the usual Frobenius map, and $[k]$ denotes the standard multiplication by k map on the elliptic curve. That $\mathbb{G}_2$ coincides with the kernel of the full trace $\text{Tr}_{E(\mathbb{F}_{q^k})/E(\mathbb{F}_q)}$ follows from the Frobenius characteristic polynomial $T^2 - tT + q$ restricted to $E[n]$. We prove the analogous characterization for the quadratic relative trace

$$\text{Tr}_{E(\mathbb{F}_{q^{12}})/E(\mathbb{F}_{q^6})}(P) = P + \text{Frob}^6(P),$$

where Frob^6 is the Frobenius map applied 6 times, using the BN-specific divisibility condition $n \mid q^6 + 1$ from [BN05]. We shall use the shorthand $tr_{E(\mathbb{F}_{q^6})}$ to denote the relative trace $\text{Tr}_{E(\mathbb{F}_{q^{12}})/E(\mathbb{F}_{q^6})}$.

Theorem 1. *Let E be a BN curve defined over a prime field $\mathbb{F}_q$, with an associated relative trace map $\text{tr}_{E(\mathbb{F}_{q^6})} : E(\mathbb{F}_{q^{12}}) \to E(\mathbb{F}_{q^6})$. Then $E[n] \cap \ker(\text{tr}_{E(\mathbb{F}_{q^6})})$ and $E[n] \cap \ker(\text{Frob} - [q])$ coincide as subsets of $E[n]$.*

Proof. The map $tr_{E(\mathbb{F}_{q^6})}$ is given by

$$tr_{E(\mathbb{F}_{q^6})}(Q) = Q + \mathrm{Frob}^6(Q). \tag{3}$$

Hence, if $\mathrm{Frob}(Q) = [q]Q$, then $tr_{E(\mathbb{F}_{q^6})}(Q) = Q + [q^6]Q = [1+q^6]Q = O$, where recall from [BN05] that n divides $1+q^6$. This proves $E[n] \cap \ker(\mathrm{Frob} - [q]) \subset E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$.

Since the order of $E[n]$ is n^2, the square of a prime number, by Lagrange's theorem, the order of either subgroup can only be 1, n or n^2. By a cardinality argument, it suffices to prove that both groups have order n.

First, observe that the order of $E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$ cannot be n^2, which would imply $tr_{E(\mathbb{F}_{q^6})}$ vanishes on $E[n]$, but we have $E(\mathbb{F}_q) \subset E[n]$ since $E(\mathbb{F}_q)$ has order n, so in particular each element $Q \in E(\mathbb{F}_q)$ is n-torsion. Each element $Q \in E(\mathbb{F}_q)$ is mapped to $[2]Q$ under $tr_{E(\mathbb{F}_{q^6})}$ which is non-zero if $Q \neq O$. Hence $E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$ must have order n or 1.

Then, notice that the group $E[n] \cap \ker(\mathrm{Frob} - [q])$ is not trivial. This is because the Frobenius has the characteristic polynomial $X^2 - tX + q$, where the Frobenius trace t satisfies the equation $t = 1 + q - n$ by Hasse's proof of the Weil bound for elliptic curves (for standard references, see [Sil09]). Therefore, for $y = \mathrm{Frob}(x) - x$ where $x \in E[n]$ we have

$$(\mathrm{Frob} - [q])(y) = (\mathrm{Frob} - [q])(\mathrm{Frob}(x) - x) = \mathrm{Frob}^2(x) - [q+1]\mathrm{Frob}(x) + [q]x = 0, \tag{4}$$

where the last equality follows from substituting $\mathrm{Frob}(x)$ into the characteristic polynomial of the Frobenius and the fact that multiplication by n kills n-torsion points. Since $y \neq O$ for $x \notin E(\mathbb{F}_q)$, we have that the group $E[n] \cap \ker(\mathrm{Frob} - [q])$ is not trivial, so it has order n or n^2.

Since $E[n] \cap \ker(\mathrm{Frob} - [q]) \subset E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$, the fact that $E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$ has order at most n and that $E[n] \cap \ker(\mathrm{Frob} - [q])$ has order at least n implies that they both have order n and therefore are equal as sets. □

Acknowledgements

The author thanks Brian Conrad for helpful discussion about the trace homomorphism of elliptic curves.

References

[BN05] Paulo S. L. M. Barreto and Michael Naehrig, *Pairing-friendly elliptic curves of prime order*, Cryptology ePrint Archive, Paper 2005/133, 2005.

[Cos12] Craig Costello, *Pairings for beginners*, 2012, Introductory notes on pairing-based cryptography.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, New York, 2009.