The Trace-Zero Subgroup and the Relative Trace for BN254

Julius Zhang

January 6, 2026

We prove a result in [1] which seems to be assumed to be well-known in cryptography literature, but the proof does not appear to be explicitly written down and there is confusion in certain literature which uses weaker results.

Recall that BN254 is the elliptic curve $E : y^2 = x^3 + 3$ over $\mathbb{F}_q$ with embedding degree 12. We work with the standard definitions: $\mathbb{G}_1 = E[n] \cap \ker(\text{Frob} - [1])$ and $\mathbb{G}_2 = E[n] \cap \ker(\text{Frob} - [q])$, where Frob is the usual Frobenius map, following Costello [2] [pp. 53–55]. 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 $E[n]$; see Math StackExchange question 3731481 [1] for this argument. Here we prove the analogous characterization for the quadratic relative trace $\text{Tr}_{E(\mathbb{F}_{q^{12}})/E(\mathbb{F}_{q^6})}(P) = P + \text{Frob}^6(P)$[2], where Frob^6 is the Frobenius map applied 6 times, using the BN-specific divisibility $n \mid q^6 + 1$ from [1]. 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 BN254 curve defined over a prime field $\mathbb{F}_q$, with associated trace map $\text{tr}_{E(\mathbb{F}_{q^6})} : E(\mathbb{F}_{q^{12}}) \to E(\mathbb{F}_{q^6})$. Let $n = |E(\mathbb{F}_q)|$. 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. First notice that both $E[n] \cap \ker(tr_{E(\mathbb{F}_{q^6})})$ and $E[n] \cap \ker(\text{Frob} - [q])$ are indeed subgroups of $E[n]$ as they are intersections of two subgroups of rational points on the elliptic curve and are contained in $E[n]$. The map $tr_{E(\mathbb{F}_{q^6})}$ is given by

$$tr_{E(\mathbb{F}_{q^6})}(Q) = Q + \text{Frob}^6(Q). \tag{1}$$

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

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 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 since $|E(\mathbb{F}_q)| = n$

[1] https://math.stackexchange.com/questions/3731481/elliptic-curve-r-torsion-points-trace-and-antitrace

[2] This is built up as a Galois descent of the normal field trace map $tr_{\mathbb{F}_{q^{12}}/\mathbb{F}_{q^6}}$.

implies every point has order dividing n, hence 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 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 [3]). Therefore, for $y = \mathrm{Frob}(x) - x$ where $x \in E[n]$ we have

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

where the last step follows by substituting $\mathrm{Frob}(x)$ into the characteristic polynomial of the Frobenius, and $y \in E[n]$ since $[n]y = \mathrm{Frob}([n]x) - [n]x = O$. 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 Frobenius trace.

References

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

[2] Craig Costello. Pairings for beginners. Lecture notes, 2012.

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, 2nd edition, 2009.