# On the Second Condition of Theorem 5.2 ($\ell = 2$)

Sebastiano Tronto

October 17, 2018

**Question:** is Lemma 1 of Lang's *Elliptic Curves Diophantine Analysis*, Chapter 5 Section 5, page 117 (References/Kummer theory/LANG-book-EC.pdf) consistent with Jones-Rouse's Theorem 5.2, i.e. can we deduce that $F(\beta_1)$ is partially contained in $F(A[2])$ already?

I believe the answer is no. Lang is working over a base field that contains all the $\ell^\infty$ torsion of $A$, so it doesn't apply in our case (J&R assume surjectivity of the torsion part).

A counterexample is actually given by J&R right after the proof of the theorem ("Remark"). They don't say explicitly that $\mathbb{Q}(\beta_1) \cap \mathbb{Q}(A[2]) = \mathbb{Q}$ in this case, but I have tested this with sage (see the file `2-division-counterex.sage`): $\mathbb{Q}(\beta_1)$ has degree 24 over $\mathbb{Q}$ and $\mathbb{Q}(A[2])$ has degree 2, which together imply that $[\mathbb{Q}(A[2], \beta_1) : \mathbb{Q}(A[2])] \geq 4$, so it is maximal.

The file `2-division.sage` contains some code that looks for other counterexamples (varying the parameters of a short Weierstrass equation), but it is quite slow (about 3 minutes on my pc for each elliptic curve of which it computes the 4-torsion field).