PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 139-140

Reductions of elliptic curves

Antonella Perucca

This is joint work with Davide Lombardo [3] and Peter Bruin [1]. The problem under consideration can be formulated for connected commutative algebraic groups, and our main results hold for all products of abelian varieties and tori. For simplicity, we focus here on the case of elliptic curves and present a selection of the results.

Let E be an elliptic curve defined over a number field K, and fix some prime number ℓ. Let $\alpha \in E(K)$ be a point of infinite order and consider the primes $\mathfrak{p}$ of K for which the reduction of α modulo $\mathfrak{p}$ is well-defined and has order coprime to ℓ. The aim of this paper is understanding the natural density $\mathrm{Dens}_\ell(\alpha)$ of this set (which is known to exist).

In [2], Jones and Rouse considered the Galois action on the tree of ℓ^∞ division points over α, which encodes the Kummer representation for α and the ℓ-adic representation attached to E. By refining their method, we are able to remove all assumptions and prove:

Theorem 1 *If $\mathcal{G}$ is the image of the ℓ-adic representation, we have*

$$\mathrm{Dens}_\ell(\alpha) = \mathrm{c}_{Kummer} \cdot \int_{\mathcal{G}} \ell^{-v_\ell(\det(x-I))} \cdot \mathrm{w}(x)\ d\mu_{\mathcal{G}}(x),$$

where $\mu_{\mathcal{G}}$ is the normalized Haar measure on $\mathcal{G}$, where the rational number c_{Kummer} measures the failure of maximality for the Kummer extensions of α, and where the function w *describes the Galois action* *on the tree of ℓ^∞ division points over α (its values can be either zero or a power of ℓ with exponent in $\mathbb{Z}_{\leq 0}$).*

With different techniques we prove a completely new result:

Theorem 2 *The density* $\mathrm{Dens}_\ell(\alpha)$ *is a rational number (strictly between* 0 *and* 1*), and there is a theoretical algorithm that computes it. The minimal denominator of* $\mathrm{Dens}_\ell(\alpha)$ *divides, up to a power of* ℓ*, the expression* $(\ell - 1)(\ell^2 - 1)^2(\ell^{12} - 1)$.

The power of ℓ in the minimal denominator of $\mathrm{Dens}_\ell(\alpha)$ cannot be uniformly bounded, therefore we give a bound depending on α.

We also generalize the above results by replacing ℓ with a (squarefree) integer m.

References

[1] P. Bruin and A. Perucca, *Reductions of points on algebraic groups II*, submitted for publication.

[2] R. Jones and J. Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 3, 763–794.

[3] D. Lombardo and A. Perucca, *Reductions of points on algebraic groups*, submitted for publication.

Antonella Perucca
Mathematics Research Unit
University of Luxembourg
6, av. de la Fonte
4364 Esch-sur-Alzette, Luxembourg.
email: antonella.perucca@uni.lu