REDUCTIONS OF ONE-DIMENSIONAL TORI II

ANTONELLA PERUCCA

ABSTRACT. Consider a one-dimensional torus defined over a number field, and fix a finitely generated group of rational points. How often is the size of the reduction of this group coprime to some given (square-free) integer? In this short note we prove a formula that allows us to reduce to the case of a prime number.

Consider a one-dimensional torus defined over a number field K, and fix a finitely generated subgroup G of K-rational points (which we assume w.l.o.g. to be torsion-free and non-trivial). Up to excluding finitely many primes $\mathfrak{p}$ of K, we suppose that the reduction of G modulo $\mathfrak{p}$ is well-defined. Since the group $(G \bmod \mathfrak{p})$ is finite, we can ask whether its size is coprime to some given square-free integer m. We thus aim at understanding the natural density

$$D_m(K) := \operatorname{dens}\{\mathfrak{p} : \#(G \bmod \mathfrak{p}) \text{ is coprime to } m\}\,.$$

The case in which m is a prime number was treated in [3], and the same problem for split tori had been solved in [2] with a different approach. The result contained in this short note presents a very general closed formula. The existence of such an elegant formula, which combines the densities with respect to the different prime divisors of m, was quite surprising because the corresponding number fields are intertwined. Moreover, the splitting field of the torus can be contained in the involved torsion and Kummer extensions, but apparently no case distinction was needed.

Theorem. *If $m = \ell_1 \cdots \ell_f$ is the product of distinct prime numbers, we have*

$$D_m(K) = \sum_{\substack{A,B\subseteq\{1,\cdots,f\}\\ A\cap B=\emptyset}} (-1)^{\#B}\cdot [K_{A\cup B} : K]^{-1}\cdot \prod_{a\in A} D_{\ell_a}(K_{A\cup B})$$

where $K_{A\cup B}$ is the $(\prod_{i\in A\cup B}\ell_i)$-th torsion field of the torus.

By the results of [3] we may then compute $D_m(K)$ for all one-dimensional tori.

If $n \geqslant 1$, we write K_n for the n-th torsion field of the torus, which is the smallest extension of K over which all points of the torus having order n are defined. We also write $K(n^{-1}G)$ for the n-th division field of G, which is the smallest extension of K over which all n-th division points of G are defined, namely all points of the torus whose n-multiple lies in G. We write $N = (n_1, \ldots, n_f)$ for an f-tuple of non-negative integers, and we set $m^N := \ell_1^{n_1}\cdots\ell_f^{n_f}$. If $A \subseteq \{1, \ldots, f\}$, we write $m_A := \prod_{a\in A}\ell_a$ and $K_A := K_{m_A}$.

Lemma. *Consider the set $\Gamma_{K,m} := \{\mathfrak{p} : \#(G \bmod \mathfrak{p})$ is coprime to $m\}$.*

2010 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11R20, 11Y40.

Key words and phrases. Number field, reduction, order, density, one-dimensional torus.

(1) *The natural density $D_m(K)$ of $\Gamma_{K,m}$ is well-defined.*

(2) *The set $S_{m,N}$ consisting of the primes of K that split completely in $K(m^{-N}G)$ and that for each prime divisor ℓ of m do not split completely in $K_{\ell m^N}$ has a natural density. We have $\Gamma_{K,m} = \cup_N S_{m,N}$ and $D_m(K) = \sum_N \operatorname{dens}(S_{m,N})$.*

(3) *Let $P_{K,A}$ be the set of primes of K that split completely in K_A and that for each prime divisor ℓ of $\frac{m}{m_A}$ do not split completely in K_ℓ. Then $\Gamma_{K,m} \cap P_{K,A}$ has a natural density and we have $D_m(K) = \sum_A \operatorname{dens}(\Gamma_{K,m} \cap P_{K,A})$.*

(4) *If $K = K_m$, then considering all prime divisors ℓ of m we have $D_m(K) = \prod_\ell D_\ell(K)$.*

(5) *If ℓ is a prime factor of m, we have*
$$D_{\frac{m}{\ell}}(K) - D_m(K) = [K_\ell : K]^{-1} \cdot \left(D_{\frac{m}{\ell}}(K_\ell) - D_m(K_\ell)\right).$$

Proof. The first three assertions can be proven as for split tori, see [2, Theorem 9]. We obtain (4) by applying (2) to m and to each of its prime divisors:
$$D_m(K) = \sum_N \operatorname{dens}(S_{m,N}) = \sum_N \prod_i \operatorname{dens}(S_{\ell_i,n_i}) = \prod_i \sum_{n_i \geqslant 0} \operatorname{dens}(S_{\ell_i,n_i}) = \prod_i D_{\ell_i}(K).$$
Note, the second equality holds because $S_{m,N}$ consists of the primes that for every i split completely in $K(\ell_i^{-n_i}G)$ but not in $K_{\ell_i^{n_i+1}}$ (by [3, Section 2] the degree of these fields is a power of ℓ_i).

In (5) we count the primes of K for which the reduction of G has order coprime to $\frac{m}{\ell}$ and divisible by ℓ: these primes split completely in K_ℓ, and we may apply [2, Proposition 1]. □

Proof of the Theorem. By (4) we have $\prod_{a\in A} D_{\ell_a}(K_{A\cup B}) = D_{m_A}(K_{A\cup B})$ so by (3) it suffices to prove
$$\operatorname{dens}(\Gamma_{K,m} \cap P_{K,A}) = \sum_{B \subseteq \{1,\cdots,f\}\setminus A} (-1)^{\#B} \cdot [K_{A\cup B} : K]^{-1} \cdot D_{m_A}(K_{A\cup B}).$$
We clearly have $\Gamma_{K,m} \cap P_{K,A} = \Gamma_{K,m_A} \cap P_{K,A}$. These primes split completely in $F := K_A$ so by [2, Proposition 1] we are left to prove:
$$\operatorname{dens}(\Gamma_{F,m_A} \cap P_{F,A}) = \sum_{B \subseteq \{1,\cdots,f\}\setminus A} (-1)^{\#B} \cdot [F_B : F]^{-1} \cdot D_{m_A}(F_B).$$
The primes of F that split completely in F_B contribute to $D_{m_A}(F)$ with density
$$[F_B : F]^{-1} D_{m_A}(F_B)$$
by [2, Proposition 1]. The above formula can then be obtained with the inclusion-exclusion principle with respect to the finitely many conditions defining $P_{F,A}$: we are restricting to the primes of F which for every prime divisor ℓ of $\frac{m}{m_A}$ do not split completely in F_ℓ. □

The formula of the Theorem can also be obtained by repeatedly applying (5).

Corollary. *If F is a Galois extension of K which is linearly disjoint from the division field $K(m^{-\infty}G)$, then we have $D_m(F) = D_m(K)$.*

Proof. We may reduce to the case where m is prime and hence apply [1, Proposition 14]. □

REFERENCES

[1] D. Lombardo and A. Perucca, *Reductions of points on algebraic groups*, arXiv:1612.02847.

[2] A. Perucca, *Reductions of algebraic integers II*, to appear in the Proceedings of WINE2 (2017).

[3] A. Perucca, *Reductions of one-dimensional tori*, Int. J. Number Theory, **13** (2017), no. 6, 1473–1489.

UNIVERSITÄT REGENSBURG, UNIVERSITÄTSSTRASSE 31, 93053 REGENSBURG, GERMANY

E-mail address: antonella.perucca@mathematik.uni-regensburg.de