ON THE REDUCTION OF POINTS ON ABELIAN VARIETIES AND TORI

ANTONELLA PERUCCA

Abstract. Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R_1, \ldots, R_n$ be points in $G(K)$. Let $\ell$ be a rational prime and let $a_1, \ldots, a_n$ be non-negative integers. Consider the set of primes $p$ of $K$ satisfying the following condition: the $\ell$-adic valuation of the order of $(R_i \mod p)$ equals $a_i$ for every $i = 1, \ldots, n$. We show that this set has a natural density and we characterize the $n$-tuples $a_1, \ldots, a_n$ for which the density is positive. More generally, we study the $\ell$-part of the reduction of the points.

1. Introduction

Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $\mathcal{O}$ be the ring of integers of $K$. We reduce $G$ modulo $p$, where $p$ is a prime of $K$ (a non-zero prime ideal of $\mathcal{O}$). By fixing a model of $G$ over an open subscheme of $\text{Spec} \mathcal{O}$, one can define the reduction $G_p$ of $G$ for all but finitely many primes $p$ of $K$. We fix a point $R$ in $G(K)$ and consider its reduction $(R \mod p)$, which is well-defined for all but finitely many primes $p$ of $K$ (the set of excluded primes depends on the point, unless the toric part of $G$ is trivial). We are interested in the set of values taken by the order of $(R \mod p)$, by varying $p$.

If $R$ is a torsion point of order $n$ then the order of $(R \mod p)$ equals $n$ for all but finitely many primes $p$ of $K$: the excluded primes are either of bad reduction or divide $n$ (bad reduction here means that the reduction is not defined on $R$ or that $G_p$ is not the product of an abelian variety and a torus).

Now assume that $R$ has infinite order. Call $n_R$ the number of connected components of the smallest $K$-algebraic subgroup of $G$ containing $R$. In [12, Main Theorem] we proved that $n_R$ is the greatest positive integer dividing the order of $(R \mod p)$ for all but finitely many primes $p$ of $K$.

Let $\ell$ be a rational prime. We study the $\ell$-adic valuation of the order of $(R \mod p)$. We write $\text{ord}_\ell$ to indicate the $\ell$-adic valuation of the order. Let $a$ be a non-negative integer and consider the following set:

$$\Gamma = \{ p : \text{ord}_\ell(R \mod p) = a \}$$

We prove that $\Gamma$ is finite if $a < \nu_\ell(n_R)$ and it has a positive natural density if $a \geq \nu_\ell(n_R)$. See Corollary [19]

For several points we have the following result:
Theorem 1. Let $K$ be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let $G_i$ be the product of an abelian variety and a torus defined over $K$ and let $R_i$ be a point in $G_i(K)$. Let $\ell$ be a rational prime. For every $i \in I$, let $a_i$ be a non-negative integer. Consider the following set of primes of $K$:
\[
\Gamma = \{p : \forall i \in I \text{ ord}_\ell(R_i \mod p) = a_i\}
\]

The set $\Gamma$ is either finite or it has a positive natural density.

Write $G = \prod_{i=1}^{n} G_i$ and $R = (R_1, \ldots, R_n)$. Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$ and call $G_R^1$ the connected component of $G_R$ containing $R$.

The set $\Gamma$ is infinite if and only if the following condition is satisfied: there exists a torsion point $T = (T_1, \ldots, T_n)$ in $G_R^1(K)$ such that $\text{ord}_\ell T_i = a_i$ for every $i \in I$.

Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R$ be a point in $G(K)$. Let $\ell$ be a rational prime and let $p$ be a prime of $K$ of good reduction, not over $\ell$. Call $a = \text{ord}_\ell(R \mod p)$. Let $L$ be a finite Galois extension of $K$ where the points in $G[\ell^a]$ are defined. Then for every prime $q$ of $L$ over $p$ there exists a unique $T$ in $G[\ell^a]$ such that $\text{ord}_\ell(R - T \mod q) = 0$. We define the $\ell$-part of $(R \mod p)$ as the $\text{Gal}(\bar{K}/K)$-class of $T$, which is independent of the choice of $q$ and of $L$.

Theorem 2. Let $G$ be the product of an abelian variety and a torus defined over $K$. Let $R$ be a point in $G(K)$. Let $\ell$ be a rational prime. Let $L$ be a finite Galois extension of $K$. Let $\mathcal{T}$ be a $\text{Gal}(\bar{K}/K)$-stable subset of $G[\ell^\infty](L)$. Then the following set of primes of $K$ is either finite or it has a positive natural density:
\[
\Gamma = \{p : \forall \text{ prime } q \text{ of } L \text{ over } p \text{ ord}_\ell(R - Y \mod q) = 0 \text{ for some } Y \text{ in } \mathcal{T}\}
\]

Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$. Call $n_{R,\ell}$ the greatest power of $\ell$ dividing the number of connected components of $G_R$. Call $G_R^j$ the connected component of $G_R$ containing the point $jR$. The set $\Gamma$ is infinite if and only if $\mathcal{T}$ contains a point in
\[
\bigcup_{j=1 \text{ (mod } n_{R,\ell})} G_R^j[\ell^\infty](L)
\]

Notice that throughout the paper we replace $\ell$ by a finite set $S$ of rational primes.

To prove the existence of the densities, we apply a method by Jones and Rouse ([9, Theorem 7]). An alternative method is due to Pink and Rütsche, see [15, Chapter 4].

To determine the conditions under which the densities are positive, we refine results of [12] which were based on a method by Khare and Prasad ([10, Lemma 5]). An alternative method is due to Pink, see [14, Theorem 4.1]. Notice that the same method by Khare and Prasad has been applied in the following papers by Banaszak, Gajda, Krasoń, Barańczuk and Górnisiewicz: [1, 3, 7, 2].

Some explicit calculations for the density have been made by Jones and Rouse in [9]. About the order of the reductions of points on the multiplicative group and elliptic curves, see [16] and [15] respectively.

A reason to study the order of the reduction of points is the following. Fix a number field $K$. Let $A$ be a simple abelian variety defined over $K$ and let $R$ be a point in $A(K)$ of
infinite order. Consider the sequence \( \{ \text{ord}(R \mod p) \} \) indexed by the primes \( p \) of \( K \) (put 1 if the expression is not well-defined). This sequence determines the isomorphism class of \( A \) and determines \( R \) up to isomorphism. This is a corollary of the results on the support problem ([13, Corollary 8 and Proposition 9]).

2. Preliminaries

Let \( G \) be the product of an abelian variety and a torus defined over a number field \( K \). Let \( R \) be a point in \( G(K) \). Call \( G_R \) the smallest \( K \)-algebraic subgroup of \( G \) containing \( R \), which is the Zariski closure of \( \mathbb{Z}R \). The connected component of the identity of \( G_R \) is the product of an abelian variety and a torus defined over \( K \) (see [12, Proposition 5]). Call it \( G_R^0 \). Let \( n_R \) be the number of connected components of \( G_R \).

For every finite extension \( L \) of \( K \), the smallest \( L \)-algebraic subgroup of \( G \) containing \( R \) is the base change \( G_R \times_K \text{Spec} L \). Notice that \( n_R \) does not depend on the field \( L \) because \( G_R^0 \) is geometrically connected (since it has a rational point).

The point \( n_R R \) is the smallest positive multiple of \( R \) which belongs to \( G_R^0 \). There exists a torsion point \( X \) in \( G_R(K) \) of order \( n_R \) such that \( R - X \) belongs to \( G_R^0 \) (see [12, Lemma 1]). In particular, the point \( n_R X \) is the smallest positive multiple of \( X \) which belongs to \( G_R^0 \).

The group of connected components of \( G_R \) is cyclic of order \( n_R \). The connected components of \( G_R \) are \( G_R^0, \ldots, G_R^{n_R-1} \), where \( G_R^i \) is the connected component of \( G_R \) containing \( iR \) (or equivalently containing \( iX \)).

**Lemma 3.** For all but finitely many primes \( p \) of \( K \), the connected components of \( (G_R \mod p) \) are \( (G_R^i \mod p) \) for \( i = 0, \ldots, n_R - 1 \). In particular, the group of connected components of \( (G_R \mod p) \) is cyclic of order \( n_R \). If \( L \) is a finite Galois extension of \( K \), the analogue properties hold for every prime \( q \) of \( L \) lying outside a finite set of primes of \( K \) not depending on \( L \).

**Proof.** Let \( F \) be a finite Galois extension of \( K \) where the points in \( G[n_R] \) are defined. Apply [11] Lemma 4.4 to \( G[n_R] \) and to \( G_R^0[n_R] \). We deduce that for all but finitely many primes \( w \) of \( F \) the following holds: \( (n_R X \mod w) \) is the smallest positive multiple of \( (X \mod w) \) which belongs to \( (G_R^0 \mod w) \). Thus for all but finitely many primes \( p \) of \( K \) the point \( (n_R R \mod p) \) is the smallest positive multiple of \( (R \mod p) \) which belongs to \( (G_R^0 \mod p) \). The first assertion follows.

Let \( q \) be a prime of \( L \) lying over a prime \( p \) of \( K \). The group of connected components of \( (G_R \mod q) \) is cyclic of order dividing \( n_R \). Then the second assertion holds since \( (G_R \mod q) \) is a base change of \( (G_R \mod p) \), up to discarding a set of primes \( p \) of \( K \) not depending on \( L \). \( \square \)

**Lemma 4** (see also [11] Lemma 4.4). Let \( L \) be a finite Galois extension of \( K \). Let \( n \) be a positive integer such that \( G[n] \subseteq G(L) \). For every prime \( q \) of \( L \) coprime to \( n \) and not lying over a finite set of primes of \( K \) (not depending on \( n \) nor on \( L \)), the reduction modulo \( q \) gives an isomorphism from \( G_R^i[n] \) to \( (G_R \mod q)[n] \) for every \( i = 0, \ldots, n_R - 1 \).

**Proof.** By [11] Lemma 4.4, the property in the statement holds for \( G_R^0[n] \) and for \( G[n] \). By Lemma 3 up to excluding a finite set of primes \( q \) (lying over a finite set of primes of \( K \) not
depending on $n$ nor on $L$), we may assume that the connected components of $(G_R \mod q)$ are $(G'_R \mod q)$ for $i = 0, \ldots, n_R - 1$. We conclude because the reduction modulo $q$ maps $G'_R[n]$ to $(G'_R \mod q)[n]$.

\textbf{Lemma 5} (see also [8] Proposition C.1.5). Let $m$ be a positive integer. For every $n > 0$ call $K_n$ the smallest extension of $K$ over which the $m^n$-th roots of $R$ are defined. Then the primes of $K$ which ramify in $\bigcup_{n>0} K_n$ are contained in a finite set.

\textbf{Proof.} First step. For every common multiple. Since $G$ every finite and in particular it has density zero. Now assume that $m^n$th roots of $R$ is trivial. Let $\sigma$ be in the inertia group of $q$ over $p$. Then $\sigma$ induces the identity automorphism on the reduction modulo $q$ of the $m^n$-th roots of $R$. Because of the injectivity of the reduction modulo $q$ on $G[m^n]$, $\sigma$ induces the identity automorphism on the $m^n$-th roots of $R$ hence it is the identity of $\text{Gal}(K_n/K)$.

\section{On the existence of the density}

In this section we generalize a result by Jones and Rouse ([9] Theorem 7). We apply the same method to prove the existence of the natural density.

The results by Pink and Rütsche in [15] Chapter 4 concern the existence of the Dirichlet density. Their method has the advantage (say with respect to Corollary 9) to allow the set $T$ to be infinite.

\textbf{Theorem 6.} Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R$ be a point in $G(K)$. Let $S$ be a finite set of rational primes and let $m$ be the product of the elements of $S$. Let $T$ be a point in $G[m^\infty](L)$, where $L$ is a finite Galois extension of $K$. Call $T$ the $\text{Gal}(K/K)$-conjugacy class of $T$. Then the following set of primes of $K$ has a natural density:

$$\Gamma = \{p : \forall \ell \in S \ \text{ord}_\ell(R - T \mod q) = 0 \ \text{for some prime } q \ \text{of } L \ \text{over } p\}$$

$$= \{p : \forall \ell \in S \ \forall \text{ prime } q \ \text{of } L \ \text{over } p \ \text{ord}_\ell(R - Y \mod q) = 0 \ \text{for some } Y \ \text{in } T\}$$

\textbf{Proof.} First step. For every $Y \in T$, we have $G_{R-Y} = G_R$ because $R$ and $R - Y$ have a common multiple. Since $G'_R$ and $R$ are defined over $K$, it follows that $n_{R-Y} = n_{R-T}$ for every $Y \in T$. If $m$ and $n_{R-T}$ are not coprime then by [12] Proposition 2 the set $\Gamma$ is finite and in particular it has density zero. Now assume that $m$ and $n_{R-T}$ are coprime. By replacing $R$ and $T$ by $n_{R-T}R$ and $n_{R-T}T$ respectively, we may assume that for every $Y \in T$ the algebraic group $G_{R-Y}$ is connected hence equal to $G'_R$. Call $G' = G'_R$, which is the product of an abelian variety and a torus defined over $K$.

Second step. Let $a$ be such that $m^a(R - Y) = m^a R$ for every $Y \in T$. In particular, $m^a R$ belongs to $G'$. Call $K_n$ the smallest extension of $K$ over which the $m^{n+a}$-th roots of $m^a R$ are defined. By Lemma 5, we may consider only the primes $p$ of $K$ which do not ramify in $\bigcup_{n>0} K_n$. We also avoid the primes of bad reduction. By Lemma 4, we may
also assume the following: for every $n$ and for every prime $\wp$ of $K_n$ over $\wp$ the reduction modulo $\wp$ is injective on $G'[m^{n+q}]$. Call $k_{\wp}$ the residue field. Then, for every $Y \in T$, the reduction modulo $\wp$ induces a bijection from the $m^n$-th roots of $R - Y$ in $G'$ to the $m^n$-th roots of $(R - Y \mod \wp)$ in $G'(k_{\wp})$.

By excluding finitely many primes $\wp$ of $K$, we may also assume that $G_{\wp}$ (respectively $G_{\wp}'$) is the base change of $G_{\wp}$ (respectively $G_{\wp}'$). In particular, we identify $G_{\wp}(k_{\wp})$ (respectively $G_{\wp}'(k_{\wp})$) with $G_{\wp}(k_{\wp})$ (respectively $G_{\wp}'(k_{\wp})$).

Third step. Call $H_n$ the subset of $\text{Gal}(K_n/K)$ consisting of the automorphisms which fix some $m^n$-th root of $R - Y$ in $G'$ for some $Y \in T$. We write $\text{Fr}_\wp$ for the Frobenius at $\wp$ without specifying the prime of $K_n$ lying over $\wp$.

Since $H_n$ is closed by conjugation, the following set of primes of $K$ is well-defined:

$$B_n = \{ \wp : \text{Fr}_\wp \in H_n \}$$

The set $B_n$ has a natural density because of the Cebotarev Density Theorem.

Now we prove that $B_n \supseteq \Gamma$ for every $n$. Take $\wp$ in $\Gamma$ and let $q$ be a prime of $L$ over $\wp$. Let $Y \in T$ be such that the order of $(R - Y \mod q)$ is coprime to $m$ or equivalently such that the orbit of $(R - Y \mod q)$ via the iterates of $[m]$ is periodic. Since $(R \mod q)$ belongs to $G_{\wp}(k_{\wp})$ and $(Y \mod q)$ is a multiple of $(R \mod q)$, the point $(R - Y \mod q)$ belongs to $G_{\wp}(k_{\wp}) \cap (G' \mod q)$. Then $(R - Y \mod q)$ has $m^n$-th roots in that set for every $n$. Fix $n$ and let $\wp$ be a prime of $K_n$ over $q$. We deduce that there exists $Z$ in $G'(K_n)$ such that $m^nZ = R - Y$ and $(Z \mod \wp)$ is in $G_{\wp}(k_{\wp})$. In particular, $Z$ is fixed by $\text{Fr}_\wp$.

Now we suppose that $\wp$ belongs to $B_n$ for infinitely many $n$ and show that $\wp$ belongs to $\Gamma$. We have to prove that for every prime $q$ of $L$ over $\wp$ there exists $Y \in T$ such that the orbit of $(R - Y \mod q)$ via the iterates of $[m]$ is periodic. Since $T$ and $G_q(k_q)$ are finite sets, it suffices to show that for infinitely many $n$ the point $(R - Y \mod q)$ has $m^n$-th roots in $G_q(k_q)$ for some $Y \in T$.

Let $n$ be such that $\wp$ belongs to $B_n$ and fix a prime $\wp'$ of $K_n$ over $q$. Let $Y \in T$ be such that there exists $Z$ in $G'(K_n)$ satisfying the following properties: $m^nZ = R - Y$ and $Z$ is fixed by $\text{Fr}_\wp$. Then $(Z \mod \wp')$ is in $G_{\wp}(k_{\wp})$ and $m^n(Z \mod \wp') = (R - Y \mod \wp')$. It follows that $(R - Y \mod q)$ has $m^n$-th roots in $G_q(k_q)$.

Fourth step. For every $\sigma$ in $\text{Gal}(K_n/K)$, call $\sigma_n$ (respectively $\sigma_{n,\ell}$) the image of $\sigma$ in the group of automorphisms of $G'[m^{n+q}]$ (respectively $G'[\ell^{n+q}]$). Notice that the determinant of $\sigma_{n,\ell}$ is an element of $\mathbb{Z}/\ell^{n+1}\mathbb{Z}$ and the fact that the determinant is zero is invariant by conjugation. Then the following set of primes of $K$ is well-defined and it has a natural density because of the Cebotarev Density Theorem:

$$A_n = \{ \wp \in B_n : \det(\text{Fr}_{\wp,n,\ell} - \text{id}) \neq 0 \ \forall \ell \in S \}$$

We now prove that $A_n \subseteq \Gamma$ for every $n$. It suffices to show that for every $n$ it is $A_n \subseteq A_{n+1}$ since then $A_n$ is contained in $B_n$ for infinitely many $n$.

Fix $\wp$ in $A_n$. Since $\det(\text{Fr}_{\wp,n,\ell} - \text{id}) \neq 0$ it follows that $\det(\text{Fr}_{\wp,n+1,\ell} - \text{id}) \neq 0$. Furthermore, the image of $(\text{Fr}_{\wp,n,\ell} - \text{id})$ in $G'[\ell^{n+q}]$ has the same index as the image of $(\text{Fr}_{\wp,n+1,\ell} - \text{id})$ in $G'[\ell^{n+1+q}]$. Thus the $m$-th roots of the image of $(\text{Fr}_{\wp,n} - \text{id})$ belong to the image of $(\text{Fr}_{\wp,n+1} - \text{id})$. 


For every $Y \in T$, let $P_Y$ be a $m^{n+1}$-th root of $R - Y$ in $G'$. Notice that any other $m^{n+1}$-th root of $R - Y$ in $G'$ differs from $P_Y$ by an element of $G'[m^{n+1}]$. Then $F_{p}$ is in $H_{n+1}$ if and only if for some $Y \in T$ the point $F_{p}(P_Y) - P_Y$ is of the form $F_{p, n+1}(X) - X$ for some $X$ in $G'[m^{n+1}]$. Similarly, because $p$ is in $H_n$, we know that for some $Y$ the point $F_{p}(mP_Y) - mP_Y$ is of the form $F_{p, n}(X) - X$ for some $X$ in $G'[m^n]$. For such $Y$, the $m$-th root $F_{p}(P_Y) - P_Y$ is of the form $F_{p, n+1}(X) - X$ for some $X$ in $G'[m^{n+1}]$. Thus $F_{p}$ belongs to $H_{n+1}$. We conclude that $p$ belongs to $A_{n+1}$.

**Fifth step.** To conclude the proof, we show that the natural density of $B_n \setminus A_n$ goes to zero for $n$ going to infinity. We have:

$$B_n \setminus A_n \subseteq \bigcup_{\ell \in S} \{ p : F_{p} \in H_n ; \det(F_{p, n, \ell} - \text{id}) = 0 \}$$

Without loss of generality, we fix $\ell$ in $S$ and show that the following set (which is well-defined and whose natural density exists by the Cebotarev Density Theorem) has density going to zero for $n$ going to infinity:

$$E_n = \{ p : F_{p} \in H_n ; \det(F_{p, n, \ell} - \text{id}) = 0 \}$$

Because of the Cebotarev Density Theorem, the density of $E_n$ is at most the maximum of

$$\frac{\# \{ \sigma \in \text{Gal}(K_n/K) : \sigma_{n, \ell} = g ; \sigma \in H_n ; \det(g - \text{id}) = 0 \}}{\# \{ \sigma \in \text{Gal}(K_n/K) : \sigma_{n, \ell} = g \}}$$

where $g$ varies in the group of the automorphisms of $G'[\ell^{n+a}]$ induced by $\text{Gal}(K_n/K)$.

To estimate the above ratio, we may replace $H_n$ with the subset of $\text{Gal}(K_n/K)$ fixing some $\ell^{n+a}$-th root of $m^a R$ in $G'$. Then we may replace $K_n$ by the smallest extension of $K$ where the $\ell^{n+a}$-th roots of $m^a R$ in $G'$ are defined (since the properties of $\sigma$ are determined by its restriction to this subfield).

By [4, Theorem 2] (applied to the point $m^a R$ in $G'$) there exists a positive integer $c$, not depending on $n$ nor on $g$, such that the denominator is at least $\frac{1}{c} \#(G'[\ell^{n+a}])$.

Now we estimate the numerator. Let $Z$ be an $\ell^{n+a}$-th root of $m^a R$ in $G'$. Any $\sigma$ such that $\sigma_{n, \ell} = g$ is determined by $\sigma(Z) - Z$. Since $\sigma \in H_n$, $\sigma(Z) - Z$ is in the image of $g - \text{id}$. By the assumptions on $g$, the cardinality of the image of $g - \text{id}$ is at most $\frac{1}{\ell^{n+a}} \#(G'[\ell^{n+a}])$. We deduce that the density of $E_n$ is bounded by $\frac{1}{c}$.

Notice that if $R$ is a torsion point then $\Gamma$ or its complement is a finite set.

**Remark 7.** In Theorem 2 it is not necessary to require that the point $T$ has order dividing a power of $m$.

**Proof.** Write $T = T' + T''$ where the order of $T'$ divides a power of $m$ and the order of $T''$ is coprime to $m$. Then $T''$ does not influence the condition defining $\Gamma$. \qed

**Remark 8.** In the theorem, if $T = 0$ we have

$$\Gamma = \{ p : \forall \ell \in S \ \text{ord}_\ell(R \mod p) = 0 \}$$
Call $K_n$ the smallest extension of $K$ where the $m^n$-th roots of $R$ are defined. If $G_R = G$, the density of $\Gamma$ is

$$\lim_{n \to \infty} \frac{\#\{\sigma \in \text{Gal}(K_n/K) : \sigma \text{ fixes some } m^n\text{-th root of } R\}}{\# \text{Gal}(K_n/K)}$$

Proof. In the proof of the Theorem 6 (in which $a = 0$, $G' = G$), notice that the density of $\Gamma$ is the limit of the density of $B_n$. 

Corollary 9. Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R$ be a point in $G(K)$. Let $S$ be a finite set of rational primes. Let $T$ be a finite $\text{Gal}(\bar{K}/K)$-stable subset of $G(K)_{\text{tors}}$. Let $L$ be a finite Galois extension of $K$ over which the points in $T$ are defined. Then the following set of primes of $K$ has a natural density:

$$\Gamma = \{p : \forall \ell \in S \ \forall \text{ prime } q \text{ of } L \text{ over } p \ \text{ord}_\ell(R - Y \mod q) = 0 \text{ for some } Y \in T\}$$

Proof. The set $T$ is the disjoint union of the $\text{Gal}(\bar{K}/K)$-orbits of its element. To each orbit we can apply Theorem 6 in view of Remark 7. Then $\Gamma$ is the disjoint union of finitely many sets admitting a natural density. 

Corollary 10. Let $K$ be a number field and let $I = \{1, \ldots, n\}$. For every $i \in I$ let $G_i$ be the product of an abelian variety and a torus defined over $K$ and let $R_i$ be a point in $G_i(K)$. Let $S$ be a finite set of rational primes. For every $i \in I$, let $T_i$ be a finite $\text{Gal}(\bar{K}/K)$-stable subset of $G_i(\bar{K})_{\text{tors}}$. Let $L$ be a finite Galois extension of $K$ where the points of $T_i$ are defined for every $i$. Then the following set of primes of $K$ has a natural density:

$$\Gamma = \{p : \forall \ell \forall i \ \forall \text{ prime } q \text{ of } L \text{ over } p \ \text{ord}_\ell(R_i - Y_i \mod q) = 0 \text{ for some } Y_i \in T_i\}$$

Proof. Write $G = \prod G_i$ and $R = (R_1, \ldots, R_n)$. Call $T$ the set of points $T = (T_1, \ldots, T_n)$ such that $T_i \in T_i$ for every $i \in I$. Then it suffices to apply Corollary 9 to $R$ and $T$. 

Corollary 11. Let $K$ be a number field and let $I = \{1, \ldots, n\}$. For every $i \in I$ let $G_i$ be the product of an abelian variety and a torus defined over $K$ and let $R_i$ be a point in $G_i(K)$. Let $S$ be a finite set of rational primes. For every $i \in I$ and for every $\ell \in S$, let $a_{\ell i}$ be a non-negative integer. Consider the following set of primes of $K$:

$$\Gamma = \{p : \forall \ell \in S \ \forall i \in I \ \text{ord}_\ell(R_i \mod p) = a_{\ell i}\}$$

The set $\Gamma$ has a natural density.

Proof. Call $m$ the product of the elements of $S$. For every $i$, let $T_i$ be the set consisting of the points $Y_i$ in $G_i[m\infty](\bar{K})$ satisfying $\text{ord}_\ell(Y_i) = a_{\ell i}$ for every $\ell \in S$. Let $L$ be a finite Galois extension of $K$ where the points of $T_i$ are defined for every $i$. It suffices to apply Corollary 10 since by Lemma 3 up to excluding finitely many primes $p$, we have

$$\Gamma = \{p : \forall \ell \forall i \ \forall \text{ prime } q \text{ of } L \text{ over } p \ \text{ord}_\ell(R_i - Y_i \mod q) = 0 \text{ for some } Y_i \in T_i\}$$

\[\square\]
4. ON THE POSITIVITY OF THE DENSITY

Theorems [1] and [2] are proven respectively in Theorems [14] and [12].

**Theorem 12.** Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R$ be a point in $G(K)$. Let $S$ be a finite set of rational primes. Call $m$ the product of the elements of $S$. Let $L$ be a finite Galois extension of $K$. Let $T$ be a $\text{Gal}(\overline{K}/K)$-stable subset of $G[m^\infty](L)$. Then the following set of primes of $K$ is either finite or it has a positive natural density:

$$
\Gamma = \{ p : \forall \ell \in S \ \forall \text{ prime } q \ of \ L \ over \ p \ \text{ ord}_\ell(R - Y \ mod \ q) = 0 \text{ for some } Y \ in \ T \}
$$

Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$. For every $\ell$, call $n_{R,\ell}$ the greatest power of $\ell$ dividing the number of connected components of $G_R$. Call $G_R^{j}$ the connected component of $G_R$ containing $jR$. The set $\Gamma$ is infinite if and only if the set $T$ contains a point which can be written as the sum for $\ell \in S$ of elements in

$$
\bigcup_{j \equiv 1 \ (mod \ n_{R,\ell})} G_R^{j}[\ell^\infty](L)
$$

**Proof.** The existence of the density was proven in Corollary [3]. Since the set $\Gamma$ increases by enlarging $T$, we may reduce to the case where $T$ is the $\text{Gal}(\overline{K}/K)$-orbit of a point $T$. By [12, Main Theorem] applied to the point $R - T$, the set $\Gamma$ is infinite if and only if $n_{R-T}$ is coprime to $m$.

Suppose that $\Gamma$ is infinite. By [12, Theorem 7] applied to the point $n_{R-T}(R - T)$, there exists a positive density of primes $p$ of $K$ such that for some prime $q$ of $L$ over $p$ it is $\text{ord}_\ell(R - T \ mod \ q) = \text{ord}_\ell(n_{R-T}(R - T) \ mod \ q) = 0$ for every $\ell \in S$. Hence $\Gamma$ has a positive density.

Write $T = \sum T_\ell$ where $T_\ell$ is in $G[\ell^\infty](L)$. Notice that $T_\ell$ is a multiple of $T$ for every $\ell \in S$. If $\Gamma$ is infinite, there exist infinitely many primes $q$ of $L$ such that $\text{ord}_\ell(R - T \ mod \ q) = 0$. For every $\ell \in S$ the point $(T_\ell \ mod \ q)$ is a multiple of $(R \ mod \ q)$ hence it belongs to $(G_R \ mod \ q)$. By applying Lemma [4] to $G$ and $G_R$, we deduce that $T_\ell$ belongs to $G_R$ for every $\ell \in S$. Then to prove the criterion in the statement we may assume that the point $T$ is such that $T_\ell$ belongs to $G_R$ for every $\ell \in S$.

Notice that $n_{R-T}$ is coprime to $\ell$ if and only if $n_{R-T_\ell}$ is coprime to $\ell$. To conclude, we show that $n_{R-T_\ell}$ is coprime to $\ell$ if and only if the point $T_\ell$ belongs to $G_R^{j}[\ell^\infty](L)$ for some $j \equiv 1 \ (mod \ n_{R,\ell})$. The last condition is equivalent to saying that $R - T_\ell$ belongs to $G_R^{j}[\ell^\infty](L)$ for some $j \equiv 0 \ (mod \ n_{R,\ell})$.

Let $R - T_\ell$ belong to $G_R^{j}$ and let $X$ be as in Section [2]. Then $G_R^{j} = G_R^{0} + jX$ and the smallest multiple of $jX$ lying in $G_R^{0}$ is $[n_R/(n_R, j)]jX$. Since $G_{R-T_\ell}^{0} = G_R^{0}$, we deduce that $n_{R-T_\ell}$ is coprime to $\ell$ if and only if $n_R/(n_R, j)$ is coprime to $\ell$. This is equivalent to saying that $j \equiv 0 \ (mod \ n_{R,\ell})$. \[ \square \]

**Corollary 13.** Let $K$ be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let $G_i$ be the product of an abelian variety and a torus defined over $K$ and let $R_i$ be a point in $G_i(K)$. Let $S$ be a finite set of rational primes. Call $m$ the product of the elements of $S$. Let $L$ be a
finite Galois extension of $K$. For every $i$, let $T_i$ be a $\text{Gal}(\bar{K}/K)$-stable subset of $G_i[m^\infty](L)$. Then the following set of primes of $K$ is either finite or it has a positive natural density:

$$\Gamma = \{ p : \forall \ell \forall \text{ prime } q \text{ of } L \text{ over } p \text{ } \text{ord}_\ell(R_i - Y_i \mod q) = 0 \text{ for some } Y_i \text{ in } T_i \}$$

Write $G = \prod_{i=1}^n G_i$ and $R = (R_1, \ldots, R_n)$. Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$. For every $\ell$, call $n_{R,\ell}$ the greatest power of $\ell$ dividing the number of connected components of $G_R$. Call $G_R^j$ the connected component of $G_R$ containing $jR$. Let $T$ be the product of the $T_i$ for $i \in I$. The set $\Gamma$ is infinite if and only if the set $T$ contains a point which can be written as the sum for $\ell \in S$ of elements in

$$\bigcup_{j=1 \ (\text{mod } n_{R,\ell})} G_R^j[\ell^\infty](L)$$

Proof. Notice that

$$\Gamma = \{ p : \forall \ell \in S \forall \text{ prime } q \text{ of } L \text{ over } p \text{ } \text{ord}_\ell(R - Y \mod q) = 0 \text{ for some } Y \text{ in } T \}$$

Then it suffices to apply Theorem 12.

**Theorem 14.** Let $K$ be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let $G_i$ be the product of an abelian variety and a torus defined over $K$ and let $R_i$ be a point in $G_i(K)$. Let $S$ be a finite set of rational primes. For every $i \in I$ and for every $\ell \in S$, let $a_{\ell i}$ be a non-negative integer. Consider the following set of primes of $K$:

$$\Gamma = \{ p : \forall \ell \in S \forall i \in I \text{ } \text{ord}_\ell(R_i \mod p) = a_{\ell i} \}$$

The set $\Gamma$ is either finite or it has a positive natural density.

Write $G = \prod_{i=1}^n G_i$ and $R = (R_1, \ldots, R_n)$. Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$. For every $\ell$, call $n_{R,\ell}$ the greatest power of $\ell$ dividing the number of connected components of $G_R$. Call $G_R^j$ the connected component of $G_R$ containing $jR$.

The set $\Gamma$ is infinite if and only if one of the following equivalent conditions is satisfied:

(i): for every $\ell \in S$ there exists a torsion point $T_\ell = (T_{\ell 1}, \ldots, T_{\ell n})$ such that $\text{ord}_\ell(T_{\ell i}) = a_{\ell i}$ for every $i \in I$ and $T_\ell$ belongs to

$$\bigcup_{j=1 \ (\text{mod } n_{R,\ell})} G_R^j[\ell^\infty]$$

(ii): for every $\ell \in S$ there exists a torsion point $T_\ell = (T_{\ell 1}, \ldots, T_{\ell n})$ in $G_R^1(\bar{K})$ such that $\text{ord}_\ell(T_{\ell i}) = a_{\ell i}$ for every $i \in I$.

**Lemma 15.** In Theorem 14, suppose that condition (ii) is satisfied. Then there exists a torsion point $T = (T_1, \ldots, T_n)$ in $G_R^1(\bar{K})$ such that $\text{ord}_\ell(T_i) = a_{\ell i}$ for every $i \in I$ and for every $\ell \in S$.

Proof. For every $\ell \in S$, the torsion point $T_\ell - X$ belongs to $G_R^0(\bar{K})$. Then we can write $T_\ell - X = Z_\ell + Z'_\ell$, where $Z_\ell$ is a point in $G_R^0[\ell^\infty]$ and $Z'_\ell$ is a torsion point in $G_R^0(\bar{K})$ of
order coprime to ℓ. Define \( T = \sum \zeta_\ell + X \). The point \( T \) is a torsion point in \( G_R^1(\bar{K}) \). For every \( \ell \in S \) and for every \( i \in I \) we have:

\[
\text{ord}_\ell(T_i) = \text{ord}_\ell(\sum \zeta_\ell + X_i) = \text{ord}_\ell(\zeta_\ell + X_i) = \text{ord}_\ell(\zeta_\ell + Z_\ell + X_i) = \text{ord}_\ell(T_\ell) = a_{\ell i}
\]

\[ \square \]

**Proof of Theorem 14.** The existence of the density for \( \Gamma \) was proven in Corollary 11.

Call \( m \) the product of the elements of \( S \). Let \( L \) be a finite Galois extension of \( K \) where the points in \( G_i[\ell^{\alpha_i}] \) are defined for every \( \ell \in S \) and for every \( i \in I \). We may assume (see Lemma 3) that for every prime \( q \) of \( L \) the reduction modulo \( q \) gives a bijection from \( G_i[\ell^{\alpha_i}] \) to \( (G_i[\ell^{\alpha_i}] \mod q) \), for every \( \ell \in S \) and for every \( i \in I \).

Let \( T \) be the set consisting of the points \( Y = (Y_1, \ldots, Y_n) \) in \( G[m^\infty] \) such that \( \text{ord}_\ell(Y_i) = a_{\ell i} \) for every \( \ell \in S \) and for every \( i \in I \). Notice that \( T \) is contained in \( G[m^\infty](L) \) and it is \( \text{Gal}(\bar{K}/K) \)-stable. A prime \( p \) of \( K \) belongs to \( \Gamma \) if and only if for every prime \( q \) of \( L \) over \( p \) the following holds: for some \( Y \in T \) \( \text{ord}_q(R - Y \mod q) = 0 \) for every \( \ell \in S \). Apply Theorem 12 to \( R \) and \( T \). We deduce that the set \( \Gamma \) is infinite if and only if it has a positive density. We also deduce that \( \Gamma \) is infinite if and only if \( T \) contains a point \( T = (T_1, \ldots, T_n) \) with the following property: we can write \( T = \sum \zeta_\ell T_\ell \) where for every \( \ell \in S \) the point \( T_\ell \) is in \( G_R^1[\ell^\infty](L) \) for some \( j \equiv 1 \pmod {n_{R,\ell}} \). Notice that \( T \) contains such an element if and only if condition (i) is satisfied.

Suppose again that \( \Gamma \) is infinite. We show that condition (ii) is satisfied. Without loss of generality, fix \( \ell \in S \). Because of condition (i) there exists \( T_\ell = (T_{\ell 1}, \ldots, T_{\ell n}) \) such that \( \text{ord}_\ell(T_{\ell i}) = a_{\ell i} \) for every \( i \in I \) in \( G_R^1[\ell^\infty](L) \) for some \( j \equiv 1 \pmod {n_{R,\ell}} \). Let \( X \) be as in section 2 and notice that the order of \( (j - 1)X \) is coprime to \( \ell \). Since \( G_R^1(\bar{K}) = G_R^1(\bar{K}) + (j - 1)X \) we deduce that \( T_\ell - (j - 1)X \) is in \( G_R^1(\bar{K}) \) and satisfies the properties of condition (ii).

Vice versa, suppose that condition (ii) is satisfied. By Lemma 15 there exists a torsion point \( T = (T_1, \ldots, T_n) \) in \( G_R^1(\bar{K}) \) such that \( \text{ord}_\ell(T_i) = a_{\ell i} \) for every \( i \in I \) and for every \( \ell \in S \). In particular, the point \( R - T \) belongs to \( G_0^0(\bar{K}) \). Furthermore, \( G_{R - T}^0 = G_R^0 \) since \( R \) and \( R - T \) have a common multiple. We deduce that \( G_{R - T} \) is connected.

Let \( F \) be a finite Galois extension of \( K \) where \( T \) is defined. By applying Theorem 7 to the point \( R - T \), we find infinitely many primes \( p \) of \( K \) such that for some prime \( \wp \) of \( F \) over \( p \) it is \( \text{ord}_\ell(R - T \mod \wp) = 0 \) for every \( \ell \in S \).

Up to excluding finitely many primes \( p \), we may assume that the order of \( (T_i \mod \wp) \) equals the order of \( T_i \) for every \( i \in I \).

Then such primes \( p \) belong to \( \Gamma \) since for every \( \ell \in S \) and for every \( i \in I \) it is

\[
\text{ord}_\ell(R_i \mod p) = \text{ord}_\ell(R_i \mod \wp) = \text{ord}_\ell(T_i \mod \wp) = \text{ord}_\ell T_i = a_{\ell i}
\]

Suppose that in Theorem 14 every \( G_i \) and every \( R_i \) is non-zero. Then the condition \( G_R = G \) implies that for every choice of the parameters \( a_{\ell i} \) the set \( \Gamma \) is infinite. The condition \( G_R = G \) is equivalent to saying that \( R \) generates a free \( \text{End}_K G \)-submodule of
$G(K)$, see \cite[Remark 6]{12}. The following example shows that the set $\Gamma$ may be infinite for every choice of the parameters even if $G_R \neq G$.

**Example 16.** Let $E$ be an elliptic curve over $\mathbb{Q}$ without complex multiplication and such that $E(\mathbb{Q})$ contains three points $P_1, P_2$ and $P_3$ which are $\mathbb{Z}$-linearly independent. For example consider the curve $[0,0,1,-7,6]$ of \cite{13}. Let $I = \{1, 2\}$ and let $S = \{\ell\}$. Let $G_1 = G_2 = E^2$. Consider the points $R_1 = (P_1, P_3)$ and $R_2 = (P_2, P_3)$. Let $a_1$ and $a_2$ be non-negative integers. There exist infinitely many primes $p$ such that $\text{ord}_\ell(R_i \mod p) = a_i$ for $i = 1, 2$. Indeed, the point $(P_1, P_2, P_3)$ is independent in $E^3$ so we can apply \cite[Proposition 12]{12}. Thus we find infinitely many $p$ such that $\text{ord}_\ell(P_i \mod p) = a_i$ for $i = 1, 2$ and $\text{ord}_\ell(P_3 \mod p) = 0$.

**Remark 17.** Suppose that the number of connected components of $G_R$ is coprime to $\ell$. Then in condition (ii) of Theorem \cite{14} it suffices to require that $T_\ell$ is in $G_R$ and not necessarily in $G^1_R$. In general, it suffices to require that $T_\ell$ is in $G^b_R$ for some $b$ coprime to $\ell$.

**Proof.** Let $X$ be as in section \cite{2}. If the number of connected components of $G_R$ is coprime to $\ell$ then the order of $X$ is coprime to $\ell$. Then by summing to $T_\ell$ a multiple of $X$ we may assume that $T_\ell$ is in $G^1_R$. For the second assertion, notice that $G^b_R = G^1_{bR}$. So by applying Theorem \cite{14} to the point $bR$ we find infinitely many primes $p$ of $K$ such that for every $i \in I$ and for every $\ell \in S$ it is

$$\text{ord}_\ell(R_i \mod p) = \text{ord}_\ell(bR_i \mod p) = a_{\ell i}$$

We deduce that the set $\Gamma$ is infinite. \hfill $\square$

**Remark 18.** With the notations of Theorem \cite{14} for every $\ell \in S$ define the following set:

$$\Gamma_\ell = \{p \in K : \forall i \in I \text{ \hspace{1em} } \text{ord}_\ell(R_i \mod p) = a_{\ell i}\}$$

We have $\Gamma = \bigcap_\ell \Gamma_\ell$ and $\Gamma$ is an infinite set if and only if $\Gamma_\ell$ is an infinite set for every $\ell \in S$.

**Proof.** In Theorem \cite{14} condition (ii) is a collection of conditions for every $\ell \in S$. \hfill $\square$

For one point of infinite order we have:

**Corollary 19.** Let $G$ be the product of an abelian variety and a torus defined over a number field $K$. Let $R$ be a point in $G(K)$ of infinite order. Let $S$ be a finite set of rational primes. For every $\ell \in S$ let $a_\ell$ be a non-negative integer. Consider the following set of primes of $K$:

$$\Gamma = \{p : \forall \ell \in S \text{ \hspace{1em} } \text{ord}_\ell(R \mod p) = a_\ell\}$$

The set $\Gamma$ is either finite or it has a positive natural density. Let $G_R$ be the smallest $K$-algebraic subgroup of $G$ containing $R$ and call $n_R$ the number of connected components of $G_R$. Then $\Gamma$ is infinite if and only if for every $\ell$ in $S$ it is $a_\ell \geq v_\ell(n_R)$. Furthermore, $n_R$ is the greatest positive integer dividing the order of $(R \mod p)$ for all but finitely many primes $p$ of $K$. 


Proof. The assertions are consequences of [12, Main Theorem] and Corollary [11].

Notice that $G^1_R(\bar{K})$ contains a torsion point of order $n$ if and only if $n$ is a multiple of $n_R$. This follows from the fact that $G^1_R(\bar{K}) = X + G^0_R(\bar{K})$, where $X$ is as in Section [2].

Acknowledgements

I thank Rafe Jones and Jeremy Rouse for helpful discussions. I thank Peter Jossen, Emmanuel Kowalski and Dino Lorenzini for useful comments.

References

[1] G. Banaszak, W. Gajda, and P. Krasoński, Detecting linear dependence by reduction maps, J. Number Theory 115 (2005), no. 2, 322–342.
[2] G. Banaszak and P. Krasoński, On arithmetic in Mordell-Weil groups, arXiv:0904.2848.
[3] S. Barańskiuk, On reduction maps and support problem in K-theory and abelian varieties, J. Number Theory 119 (2006), no. 1, 1–17.
[4] D. Bertrand, Galois Representations and Transcendental Numbers, New Advances in Trascendence Theory (Durham, 1986), 37–55, Cambridge Univ. Press, Cambridge, 1988.
[5] J. Cheon and S. Hahn, The Orders of the Reductions of a Point in the Mordell-Weil Group of an Elliptic Curve, Acta Arith. 88 (1999), no. 3, 219–222.
[6] J. Cremona, Elliptic Curve Data, http://www.warwick.ac.uk/staff/J.E.Cremona/.
[7] W. Gajda and K. Górniakiewicz, Linear dependence in Mordell-Weil groups, J. Reine Angew. Math. 630 (2009), 219–233.
[8] M. Hindry and J. H. Silverman, Diophantine Geometry. An Introduction, Graduate Texts in Mathematics 201, Springer Verlag, New York, 2000.
[9] R. Jones and J. Rouse, Iterated Endomorphisms of Abelian Algebraic Groups, arXiv:0706.2384.
[10] C. Khare and D. Prasad, Reduction of homomorphisms mod $p$ and algebraicity, J. Number Theory, 105 (2004), no. 2, 322–332.
[11] E. Kowalski, Some local-global applications of Kummer theory, Manuscripta Math. 111 (2003), no. 1, 105–139.
[12] A. Perucca, Prescribing valuations of the order of a point in the reductions of abelian varieties and tori, J. Number Theory 129 (2009), no. 2, 469–476.
[13] A. Perucca, Two variants of the support problem for products of abelian varieties and tori, J. Number Theory 129 (2009), no. 8, 1883–1892.
[14] R. Pink, On the order of the reduction of a point on an abelian variety, Math. Ann. 330 (2004), no. 2, 275–291.
[15] E. Rütsche, Über das Reduktionsverhalten von Punkten auf abelschen Varietäten, Master thesis at ETH Zürich, March 2004, http://www.math.ethz.ch/~pink/Theses/Master.html.
[16] A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, J. Reine Angew. Math. 268/269 (1974), 27–33.

Antonella Perucca
EPFL Station 8, CH-1015, Lausanne, Switzerland
antonella.perucca@epfl.ch