Journal of Number Theory 159 (2016) 426–433

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Cyclic components of abelian varieties (mod $\wp$)

Cristian Virdol

Department of Mathematics, Yonsei University, Republic of Korea

ARTICLE INFO

Article history:
Received 17 May 2015
Received in revised form 26 August 2015
Accepted 26 August 2015
Available online 13 October 2015
Communicated by David Goss

MSC:
11G10
11G15

Keywords:
Abelian varieties
Cyclicity

ABSTRACT

Consider A an abelian variety of dimension r, defined over a number field F. For $\wp$ a finite prime of F, we denote by $\mathbb{F}_\wp$ the residue field at $\wp$. If A has good reduction at $\wp$, let $\bar{A}$ be the reduction of A at $\wp$. In this paper, under GRH, we obtain an asymptotic formula for the number of primes $\wp$ of F, with $N_{F/\mathbb{Q}}\wp \leq x$, for which $\bar{A}(\mathbb{F}_\wp)$ has at most $2r-1$ cyclic components.

1. Introduction

Let A be an abelian variety defined over a number field F, of conductor $\mathcal{N}$, and of dimension r, where $r \geq 1$ is an integer. Let Σ_F be the set of finite places of F, and for $\wp$ a prime of F, let $\mathbb{F}_\wp$ be the residue field at $\wp$. Let $\mathcal{P}_A$ be the set of primes $\wp \in \Sigma_F$ of good reduction for A (i.e. $(N_{F/\mathbb{Q}}\wp, N_{F/\mathbb{Q}}\mathcal{N}) = 1$). For $\wp \in \mathcal{P}_A$, we denote by $\bar{A}$ the reduction of A at $\wp$.

E-mail address: cristian.virdol@gmail.com.

http://dx.doi.org/10.1016/j.jnt.2015.08.015

We have that $\bar{A}(\mathbb{F}_\wp) \subseteq \bar{A}[m](\bar{\mathbb{F}}_\wp) \subseteq (\mathbb{Z}/m\mathbb{Z})^{2r}$ for any positive integer m satisfying $|\bar{A}(\mathbb{F}_\wp)||m$. Hence

$$\bar{A}(\mathbb{F}_\wp) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}, \tag{1.1}$$

where $s \leq 2r$, $m_i \in \mathbb{Z}_{\geq 2}$, and $m_i | m_{i+1}$ for $1 \leq i \leq s-1$. Each $\mathbb{Z}/m_i\mathbb{Z}$ is called a cyclic component of $\bar{A}(\mathbb{F}_\wp)$. If $s < 2r$, we say that $\bar{A}(\mathbb{F}_\wp)$ has at most $(2r-1)$ cyclic components (thus if $r = 1$ this means that $\bar{A}(\mathbb{F}_\wp)$ is cyclic). For $x \in \mathbb{R}$, define

$$f_{A,F}(x) = |\{\wp \in \mathcal{P}_A | N_{F/\mathbb{Q}}\wp \leq x,\ \bar{A}(\mathbb{F}_\wp) \text{ has at most } (2r-1) \text{ cyclic components}\}|.$$

Let $F(A[m])$ be the field obtained by adjoining to F the m-division points $A[m]$ of A.

In this paper we prove the following result (for the very particular case of abelian varieties over $\mathbb{Q}$ that contain elliptic curves defined also over $\mathbb{Q}$ see the main theorems of [AG], and for the case of elliptic curves see [S,MU,CM,KL]):

Theorem 1.1. *Let A be an abelian variety over a number field F of dimension $r \geq 1$. Assume that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta functions of the division fields for A. Then we have*

$$f_{A,F}(x) = c_{A,F}\,\mathrm{li}\ x + O(x^{5/6}(\log x)^{2/3}),$$

where li $x := \int_2^x \frac{1}{\log t} dt$, *and*

$$c_{A,F} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[F(A[m]) : F]},$$

where $\mu(\cdot)$ is the Mobius function.

2. General abelian varieties

For F a number field, we denote $G_F := \mathrm{Gal}(\bar{F}/F)$. Let A be an abelian variety over F of dimension $r \geq 1$, and of conductor $\mathcal{N}$. We denote by $\mathcal{P}_A$ the set of primes $\wp \in \Sigma_F$ of good reduction for A (i.e. $(N_{F/\mathbb{Q}}\wp, N_{F/\mathbb{Q}}\mathcal{N}) = 1$). For $m \geq 1$ an integer, let $A[m]$ be the m-division points of A in $\bar{F}$. Then

$$A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}.$$

If $F(A[m])$ is the field obtained by adjoining to F the elements of $A[m]$, then we have a natural injection

$$\Phi_m : \mathrm{Gal}(F(A[m])/F) \hookrightarrow \mathrm{Aut}(A[m]) \simeq \mathrm{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}).$$