数理解析研究所講究録
第 1826 巻 2013 年 163-167

On the Cyclicity of finite CM abelian varieties

Cristian Virdol
Graduate School of Mathematics
Kyushu University
virdol@imi.kyushu-u.ac.jp

July 17, 2012

Abstract

Let A be an abelian variety over a number field F of dimension r, where $r \geq 1$ is an integer. Assume that $\mathrm{End}_{\bar{F}} A \otimes \mathbb{Q} = K$, where K is a CM-field such that $[K : \mathbb{Q}] = 2r$. 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 $\wp$. Under GRH, we obtain ([V]) 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 The Main result

Consider A 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 $\wp$.

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.

We obtain (this is the main result of [V]; when $F = \mathbb{Q}$ and $r = 1$, i.e. when A is a CM elliptic curve over $\mathbb{Q}$, Theorem 1.1 is similar to Theorem 1.2 of [CM]):

Theorem 1.1. *Let A be an abelian variety over a number field F of dimension $r \geq 1$, of conductor $\mathcal{N}$, such that $End_{\bar{F}} A \otimes \mathbb{Q} = K$, where K is a CM-field satisfying $[K : \mathbb{Q}] = 2r$. Assume that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta functions of the division fields for A. Then we have*

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

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

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

Here $\mu(\cdot)$ is the Mobius function, and the implicit $O_{A,F}$-constant depends on A and F.

2 Odds and ends

If F is 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 $\mathcal{P}_A$ 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 $m \geq 1$ 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

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

For l a rational prime, define

$$T_l(A) = \lim_{\longleftarrow} A[l^n].$$

The Galois group G_F acts on

$$T_l(A) \simeq \mathbb{Z}_l^{2r},$$

where $\mathbb{Z}_l$ is the l-adic completion of $\mathbb{Z}$ at l, and we obtain a representation

$$\rho_{A,l} : G_F \to \mathrm{Aut}(T_l(A)) \simeq \mathrm{GL}_{2r}(\mathbb{Z}_l),$$

which is unramified outside $lN_{F/\mathbb{Q}}\mathcal{N}$. If $\wp \in \mathcal{P}_A$, let $\sigma_\wp$ be the Artin symbol of $\wp$ in G_F, and let l be a rational prime satisfying $(l, N_{F/\mathbb{Q}}\wp) = 1$. We denote by $P_{A,\wp}(X) = X^{2r} + a_{2r-1,A}(\wp)X^{2r-1} + \ldots + a_{1,A}(\wp)X + N_{F/\mathbb{Q}}\wp^r \in \mathbb{Z}[X]$ the characteristic polynomial of $\sigma_\wp$ on $T_l(A)$. Then $P_{A,\wp}(X)$ is independent of l. One can identify $T_l(A)$ with $T_l(\bar{A})$, where $\bar{A}$ is the reduction of A at $\wp$, and the action of $\sigma_\wp$ on $T_l(A)$ is the same as the action of the Frobenius $\pi_\wp$ of $\bar{A}$ on $T_l(\bar{A})$.

We say that an abelian variety A defined over a number field F of dimension r is CM (or has many complex multiplications) if $\mathrm{End}_{\bar{F}}(A) \otimes \mathbb{Q} = K$, where K is a CM-field satisfying $[K:\mathbb{Q}] = 2r$. We denote by $\mathcal{F}$ the maximal totally real number field contained in K, and let $O_{\mathcal{F}}$ be the ring of integers of $\mathcal{F}$ and let O_K be the ring of integers of K. Let $\phi_1, \ldots, \phi_r, \bar{\phi}_1, \ldots, \bar{\phi}_r$, be the set of embeddings of K into $\mathbb{C}$, where $\bar{\phi}_i$ is the complex conjugate of ϕ_i. Then we have $[K:\mathcal{F}] = 2$, and $K = \mathcal{F}(\sqrt{-D})$ for some totally positive $D \in O_{\mathcal{F}}$.

Lemma 2.1. *(Ribet [R]) Let A be a CM abelian variety defined over a number field F, of dimension r, of conductor $\mathcal{N}$, and let m be a positive integer. Then*
1.
$$\phi(m)^2 \ll [F(A[m]):F],$$
where $\phi(m)$ is the Euler function,
2. the extension $F(A[m])/F$ is ramified only at places dividing $m\mathcal{N}$.

Lemma 2.2. *(Shimura [SH]) Let A be a CM abelian variety defined over a number field F, of dimension r, and of conductor $\mathcal{N}$. Then for all $\wp \in \mathcal{P}_A$, the characteristic polynomial $P_{A,\wp}(X)$ has roots $\pi_1(\wp), \ldots, \pi_r(\wp), \bar{\pi}_1(\wp), \ldots, \bar{\pi}_r(\wp)$, where $\bar{\pi}_i(\wp)$ is the complex conjugate of $\pi_i(\wp)$, and $\pi_i(\wp)\bar{\pi}_i(\wp) = N_{F/\mathbb{Q}}\wp$, for all $i = 1, \ldots, r$. Moreover one can assume that $\pi_1(\wp) \in \mathrm{End}_{\bar{F}}(A) \subseteq O_K$, and that for any $i = 1, \ldots, r$, we have $\pi_i(\wp) = \phi_i(\pi_1(\wp))$.*

On can prove the following results (see [V]):

Lemma 2.3. *Let A be an abelian variety over a number field F, of conductor $\mathcal{N}$. Let $\wp \in \mathcal{P}_A$, and let p be the rational prime below $\wp$. Let $q \neq p$ be a rational prime. Then $\bar{A}(\mathbb{F}_\wp)$ contains a $(q, \ldots, q)$-type subgroup (q appears $2r$-times), i.e. a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \ldots \times \mathbb{Z}/q\mathbb{Z}$, iff $\wp$ splits completely in $F(A[q])$.*

Lemma 2.4. *Let A be a CM abelian variety defined over a number field F, of dimension r, and of conductor $\mathcal{N}$. Let m be a positive integer. Then $\wp \in \mathcal{P}_A$, with $(N_{F/\mathbb{Q}}\wp, m) = 1$, splits completely in $F(A[m])$ iff $\frac{\pi_1(\wp)-1}{m} \in \mathrm{End}_{\bar{F}}(A)$, where $\pi_1(\wp)$ appears in Lemma 2.2.*

Lemma 2.5. *Let A be an abelian variety over a number field F, of conductor $\mathcal{N}$. Let $\wp \in \mathcal{P}_A$, and let p be the rational prime below $\wp$. Then $\bar{A}(\mathbb{F}_\wp)$ contains at most $(2r-1)$-cyclic components iff $\wp$ does not split completely in $F(A[q])$ for any rational prime $q \neq p$.*

Lemma 2.6. *With the same notations as above, for any $m \in \mathbb{N}^*$ and any $x \in \mathbb{R}$, we have that*

$$S_m := |\{\wp \in \Sigma_F |\ N_{F/\mathbb{Q}}\wp \le x,\ N_{F/\mathbb{Q}}\wp = (\alpha m + 1)^2 + D\beta^2 m^2,$$
$$for\ some\ \alpha + \sqrt{-D}\beta \in O_K,\ where\ \alpha, \beta \in \mathcal{F}\}|$$
$$\ll \frac{x^{\frac{3}{2}}}{m^3} + 1.$$

3 Chebotarev

Consider L/F a Galois extension of number fields, with Galois group G. We denote by n_L and d_L the degree and the discriminant of $L/\mathbb{Q}$, and by d_F the discriminant of $F/\mathbb{Q}$. Let $\mathcal{P}(L/F)$ be the set of rational primes p which lie below places of F which ramify in L/F.

Lemma 3.1. *(Serre [SE]) If L/F is Galois extension of number fields, then*

$$\log d_L \leq |G|\log d_F + n_L(1-\frac{1}{|G|})\sum_{p\in\mathcal{P}(L/F)}\log p + n_L\log|G|.$$

Let C be a conjugacy class in G. For a positive real number x, let

$$\pi_C(x,L/F) := |\{\wp\in\Sigma_F | N_{F/\mathbb{Q}}\wp \leq x,\ \wp \text{ unramified in } L/F,\ \sigma_\wp\in C\}|,$$

where $\sigma_\wp$ is a Frobenius element at $\wp$. The Chebotarev density theorem says that

$$\pi_C(x,L/F)\sim\frac{|C|}{|G|}\mathrm{li}\ x\sim\frac{|C|}{|G|}\frac{x}{\log x},$$

and moreover:

Lemma 3.2. *(Serre [SE]) Let L/F be a Galois extension of number fields. If the Dedekind zeta function of L satisfies the GRH, then*

$$|\pi_C(x,L/F)-\frac{|C|}{|G|}li\ x| \ll |C|x^{\frac{1}{2}}(\log x+\frac{\log|d_L|}{|G|}),$$

where the implied O-constant depends only on F.

4 Sketch of the proof of Theorem 1.1

Using §2 one obtains (see §4 of [V]), for $y=y(x)$ any real number with $y\leq 2x^{\frac{1}{2}}$, that

$$f_{A,F}(x) = \sum_{m\leq 2x^{\frac{1}{2}}}\mu(m)\pi_1(x,F(A[m])/F)$$

$$= \sum_{m\leq y}\mu(m)\pi_1(x,F(A[m])/F) + \sum_{y<m\leq 2x^{\frac{1}{2}}}\mu(m)\pi_1(x,F(A[m])/F)$$

$$= \text{main} + \text{error}. \tag{4.1}$$

Using §2 and Chebotarev, under GRH, one obtains (see §4 of [V])

$$\text{main} = \sum_{m\leq y}\frac{\mu(m)}{n(m)}\mathrm{li}\ x + \sum_{m\leq y}O(x^{\frac{1}{2}}\log(mN_{F/\mathbb{Q}}\mathcal{N}x))$$

$$= \sum_{m \le y} \frac{\mu(m)}{n(m)} \mathrm{li}\, x + O(yx^{\frac{1}{2}} \log(N_{F/\mathbb{Q}}\mathcal{N}x)), \qquad (4.2)$$

where $n(m) := [F(A[m]) : F]$, and

$$\text{error} \ll \sum_{\substack{y<m\le 2x^{\frac{1}{2}} \\ m \text{ square-free}}} \frac{x^{\frac{3}{2}}}{m^3} \ll \frac{x^{\frac{3}{2}}}{y^2}.$$

For

$$y := \frac{x^{\frac{1}{3}}}{(\log(N_{F/\mathbb{Q}}\mathcal{N}x))^{\frac{1}{3}}},$$

from §2 one gets (see §4 of [V])

$$\sum_{m>y} \frac{\mu(m)}{n(m)} \mathrm{li}\, x \ll \sum_{\substack{m>y \\ m \text{ square-free}}} \frac{(\log\log m)^2}{m^2} \mathrm{li}\, x \ll \frac{(\log\log y)^2}{y} \mathrm{li}\, x \ll x^{\frac{5}{6}}.$$

Hence

$$f_{A,F}(x) = \sum_{m=1}^{\infty} \frac{\mu(m)}{n(m)} \mathrm{li}\, x + O(x^{\frac{5}{6}} (\log(N_{F/\mathbb{Q}}\mathcal{N}x))^{\frac{2}{3}}).$$

■

References

[CM] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linniks problem*, Math. Ann. 330 (2004) 601-625.

[M] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, by Oxford University Press.

[R] K. A. Ribet, *Division points of abelian varieties with complex multiplication*, Mem. Soc. Math. de France 2e serie 2 (1980), 75-94.

[SE] J. -P. Serre, *Quelques applications du theoreme de densite de Chebotarev*, Inst. Hautes Etudes Sci. Publ. Math., no. 54, 1981, pp. 123-201.

[SH] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[SI] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151. Springer, New York (1994).

[V] C. Virdol, *Cyclicity of finite CM abelian varieties*, submitted.