<table>
<thead>
<tr>
<th>Title</th>
<th>On the Cyclicity of finite CM abelian varieties (Automorphic forms and automorphic L-functions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Virdol, Cristian</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2013), 1826: 163-167</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2013-03</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/194755">http://hdl.handle.net/2433/194755</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
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 $\text{End}_F A \otimes \mathbb{Q} = K$, 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 $\overline{A}$ 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 $\overline{A}(\mathbb{F}_\wp)$ has at most $2r-1$ cyclic components.

1 The Main result

Consider $A$ an abelian variety defined over a number field $F$, of conductor $N$, and of dimension $r$, where $r \geq 1$ is an integer. Let $\Sigma_F$ 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. $(N_{F/\mathbb{Q}} \wp, N_{F/\mathbb{Q}} N) = 1$). For $\wp \in \mathcal{P}_A$, we denote by $\overline{A}$ the reduction of $A$ at $\wp$.

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

$$\overline{A}(\mathbb{F}_\wp) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z},$$

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 $\overline{A}(\mathbb{F}_\wp)$. If $s < 2r$, we say that $\overline{A}(\mathbb{F}_\wp)$ has at most $(2r - 1)$ cyclic components (thus if $r = 1$ this means that $\overline{A}(\mathbb{F}_\wp)$ is cyclic). For $x \in \mathbb{R}$, define

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

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 $\text{End}_{\bar{F}} A \otimes \mathbb{Q} = K$, 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

$$f_{A,F}(x) = c_{A,F} li x + O_{A,F}(x^{\frac{5}{6}}(\log x)^{25}),$$

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 $G_{F} := \text{Gal}(\bar{F}/F)$. 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

$$\Phi_{m} : \text{Gal}(F(A[m])/F) \hookrightarrow \text{Aut}(A[m]) \simeq GL_{2r}(\mathbb{Z}/m\mathbb{Z}).$$

For $l$ a rational prime, define

$$T_{l}(A) = \lim_{\arrow} A[l^{n}].$$

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

$$\rho_{A,l} : G_{F} \to \text{Aut}(T_{l}(A)) \simeq GL_{2r}(\mathbb{Z}_{l}),$$

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 $P_{A,\wp}(X) = X^{2r} + a_{2r-1,A}(\wp)X^{2r-1} + \ldots + a_{1,A}(\wp)X + N_{F/\mathbb{Q}}\wp \in \mathbb{Z}[X]$ 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 $\text{End}_F(A) \otimes \mathbb{Q} = \mathcal{F}$, where $\mathcal{F}$ is a CM-field satisfying $[\mathcal{F} : \mathbb{Q}] = 2r$. 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 $\phi_1, \ldots, \phi_r, \overline{\phi}_1, \ldots, \overline{\phi}_r$, be the set of embeddings of $K$ into $\mathbb{C}$, where $\overline{\phi}_i$ is the complex conjugate of $\phi_i$. 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 $\pi_1(\wp), \ldots, \pi_r(\wp), \overline{\pi}_1(\wp), \ldots, \overline{\pi}_r(\wp)$, where $\overline{\pi}_i(\wp)$ is the complex conjugate of $\pi_i(\wp)$, and $\pi_i(\wp)\overline{\pi}_i(\wp) = N_{\mathcal{F}/\mathbb{Q}}(\wp)$, for all $i = 1, \ldots, r$. Moreover one can assume that $\pi_1(\wp) \in \text{End}_\mathcal{F}(A) \subseteq O_K$, 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 a rational prime. Then $A(\mathbb{F}_p)$ 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 $(N_{\mathcal{F}/\mathbb{Q}}(\wp), m) = 1$, splits completely in $F(A[m])$ iff $\pi_1(\wp) - 1 \in \text{End}_\mathcal{F}(A)$, 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 $A(\mathbb{F}_p)$ 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

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

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

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

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

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

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

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

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

$$= \text{main} + \text{error}. \quad (4.1)$$

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

$$\text{main} = \sum_{m \leq y} \frac{\mu(m)}{n(m)} \text{li} x + \sum_{m \leq y} O(x^{\frac{1}{2}} \log(mN_{F/\mathbb{Q}}N_{x}))$$
\[ = \sum_{m \leq y} \frac{\mu(m)}{n(m)} \text{li} x + O(yx^{\frac{1}{2}} \log(N_{F/\mathbb{Q}}N x)), \] (4.2)

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

\[
\text{error} \ll \sum_{y < m \leq 2x^{\frac{1}{2}}} \frac{x^{\frac{3}{2}}}{m^3} \ll \frac{x^{\frac{3}{2}}}{y^2}.
\]

For
\[
y := \frac{x^{\frac{1}{2}}}{(\log(N_{F/\mathbb{Q}}N x))^{\frac{1}{3}}},
\]
from \( \S 2 \) one gets (see \( \S 4 \) of [V])
\[
\sum_{m > y} \frac{\mu(m)}{n(m)} \text{li} x \ll \sum_{m \text{ square-free}} \frac{(\log \log m)^2}{m^2} \text{li} x \ll \frac{(\log \log y)^2}{y} \text{li} x \ll x^{\frac{5}{6}}.
\]

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

References


