Random Dieudonné Modules and the Cohen-Lenstra Heuristics

David Zureick-Brown
Bryden Cais
Jordan Ellenberg

Emory University
Slides available at http://www.mathcs.emory.edu/~dzb/slides/

Arithmetic of abelian varieties in families
Lausanne, Switzerland
November 13, 2012

Basic Question

How often does p **divide** $h(-D)$?

Basic Question

What is

$$P(p \mid h(-D)) = \lim_{X \to \infty} \frac{\#\{0 \leq D \leq X \text{ s.t. } p \mid h(-D)\}}{\#\{0 \leq D \leq X\}}?$$

Guess: Random Integer?

$$P(p \mid h(-D)) = P(p \mid D) = \frac{\mathbf{1}}{\mathbf{p}} ???$$

Data (Buell '76)

$$P(p \mid h(-D)) \approx \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + \cdots \qquad (p \text{ odd })$$

$$= 1 - \prod_{i \geq 1}\left(1 - \frac{1}{p^i}\right)$$

$$= \mathbf{0.43} \ldots \neq \mathbf{1/3} \qquad (p = 3)$$

$$= \mathbf{0.23} \ldots \neq \mathbf{1/5} \qquad (p = 5)$$

$$P(\mathrm{Cl}(-D)_3 \cong \mathbb{Z}/9\mathbb{Z}) \approx \mathbf{0.070}$$

$$P(\mathrm{Cl}(-D)_3 \cong (\mathbb{Z}/3\mathbb{Z})^2) \approx \mathbf{0.0097}$$

Random finite abelian groups

Idea

$$P(p \mid h(-D)) = P(p \mid \#G) = \text{ ???}$$

Random finite abelian groups

Idea

$$P(p \mid h(-D)) = P(p \mid \#G) = \ ???$$

Let $\underline{G}_p$ be the set of isomorphism classes of **finite abelian groups of** p-**power order.**

Random finite abelian groups

Idea

$$P(p \mid h(-D)) = P(p \mid \#G) = \ ???$$

Let $\underline{G}_p$ be the set of isomorphism classes of **finite abelian groups of** p-**power order.**

Theorem (Cohen, Lenstra)

(i) $$\sum_{G \in \underline{G}_p} \frac{1}{\# \operatorname{Aut} G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1}$$

Random finite abelian groups

Idea

$$P(p \mid h(-D)) = P(p \mid \#G) = \ ???$$

Let $\underline{G}_p$ be the set of isomorphism classes of **finite abelian groups of** p-**power order.**

Theorem (Cohen, Lenstra)

(i) $$\sum_{G \in \underline{G}_p} \frac{1}{\# \operatorname{Aut} G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1}$$

(ii) $G \mapsto \dfrac{C_p}{\# \operatorname{Aut} G}$ *is a* **probability distribution** *on* $\underline{G}_p$

Random finite abelian groups

Idea

$$P(p \mid h(-D)) = P(p \mid \#G) = \ ???$$

Let $\underline{G}_p$ be the set of isomorphism classes of **finite abelian groups of p-power order.**

Theorem (Cohen, Lenstra)

(i) $$\sum_{G \in \underline{G}_p} \frac{1}{\#\,\mathrm{Aut}\, G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1}$$

(ii) $G \mapsto \dfrac{C_p}{\#\,\mathrm{Aut}\, G}$ *is a* **probability distribution** *on* $\underline{G}_p$

(iii) $\mathrm{Avg}\,(\#G[p]) = \mathrm{Avg}\left(p^{r_p(G)}\right) = 2$

Cohen and Lenstra's conjecture

Let $f \colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\# \operatorname{Aut} G} \cdot f(G)$$

Cohen and Lenstra's conjecture

Let $f \colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\# \operatorname{Aut} G} \cdot f(G)$$

$$\operatorname{Avg}_{\mathrm{Cl}} f = \frac{\sum_{0 \le D \le X} f(\mathrm{Cl}(-D)_p)}{\sum_{0 \le D \le X} 1}$$

Cohen and Lenstra's conjecture

Let $f\colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\# \operatorname{Aut} G} \cdot f(G)$$

$$\operatorname{Avg}_{\mathrm{Cl}} f = \frac{\sum_{0 \le D \le X} f(\mathrm{Cl}(-D)_p)}{\sum_{0 \le D \le X} 1}$$

Conjecture (Cohen, Lenstra)

(i) $\operatorname{Avg}_{\mathrm{Cl}} f = \operatorname{Avg} f$

Cohen and Lenstra's conjecture

Let $f \colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\# \operatorname{Aut} G} \cdot f(G)$$

$$\operatorname{Avg}_{\mathrm{Cl}} f = \frac{\sum_{0 \le D \le X} f(\mathrm{Cl}(-D)_p)}{\sum_{0 \le D \le X} 1}$$

Conjecture (Cohen, Lenstra)

(i) $\operatorname{Avg}_{\mathrm{Cl}} f = \operatorname{Avg} f$

(ii) $\operatorname{Avg} (\# \mathrm{Cl}(-D)[p]) \quad = 2$

Cohen and Lenstra's conjecture

Let $f\colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\#\operatorname{Aut} G} \cdot f(G)$$

$$\operatorname{Avg}_{\mathrm{Cl}} f = \frac{\sum_{0 \le D \le X} f(\mathrm{Cl}(-D)_p)}{\sum_{0 \le D \le X} 1}$$

Conjecture (Cohen, Lenstra)

(i) $\operatorname{Avg}_{\mathrm{Cl}} f = \operatorname{Avg} f$

(ii) $\operatorname{Avg}\left(\#\,\mathrm{Cl}(-D)[p]\right)^2 = 2 + p$

Cohen and Lenstra's conjecture

Let $f\colon \underline{G}_p \to \mathbb{Z}$ be a function.

Definition

$$\operatorname{Avg} f = \sum_{G \in \underline{G}_p} \frac{C_p}{\# \operatorname{Aut} G} \cdot f(G)$$

$$\operatorname{Avg}_{\mathrm{Cl}} f = \frac{\sum_{0 \le D \le X} f(\mathrm{Cl}(-D)_p)}{\sum_{0 \le D \le X} 1}$$

Conjecture (Cohen, Lenstra)

(i) $\operatorname{Avg}_{\mathrm{Cl}} f = \operatorname{Avg} f$

(ii) $\operatorname{Avg} (\# \mathrm{Cl}(-D)[p])^2 = 2 + p$

(iii) $P(\mathrm{Cl}(-D)_p \cong G) = \frac{C_p}{\# \operatorname{Aut} G}$.

Progress

Davenport-Heilbronn	–	$\text{Avg}\,\text{Cl}(-D)[3] = 2$
Bhargava	–	$\text{Avg}\,\text{Cl}(K)[2] = 3$ (K cubic)
Bhargava	–	counts quartic dihedral extensions
Kohnen-Ono	–	$N_{p \nmid h}(X) \gg \frac{x^{\frac{1}{2}}}{\log x}$
Heath-Brown	–	$N_{p \mid h}(X) \gg \frac{x^{\frac{9}{10}}}{\log x}$
Byeon	–	$N_{\text{Cl}_p \cong (\mathbb{Z}/g\mathbb{Z})^2}(X) \gg \frac{x^{\frac{1}{g}}}{\log x}$

Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

$$\mathrm{Cl}(-D) = \mathrm{Pic}(\operatorname{Spec} \mathcal{O}_K)$$

vs

$$\mathrm{Pic}(C)$$

Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

$$\mathrm{Cl}(-D) = \mathrm{Pic}(\operatorname{Spec} \mathcal{O}_K)$$

vs

$$\mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

$$\mathrm{Cl}(-D) = \mathrm{Pic}(\operatorname{Spec} \mathcal{O}_K)$$

VS

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Basic Question over $\mathbb{F}_q(t)$, $\ell \neq p$

Fix $G \in \underline{G}_\ell$.

What is

$$P(\mathrm{Pic}^0(C)_\ell \cong G)?$$

(Limit is taken as $\deg f \to \infty$, where $C\colon y^2 = f(x)$.)

Main Tool over $\mathbb{F}_q(t)$ – Tate Module

$$\operatorname{Aut} \mathrm{T}_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^{2g}$$

Main Tool over $\mathbb{F}_q(t)$ – Tate Module

$$\mathrm{Gal}_{\mathbb{F}_q} \to \mathrm{Aut}\, \mathrm{T}_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^{2g}$$

Main Tool over $\mathbb{F}_q(t)$ – Tate Module

$$\mathrm{Frob} \in \mathrm{Gal}_{\mathbb{F}_q} \to \mathrm{Aut}\, \mathrm{T}_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^{2g}$$

Main Tool over $\mathbb{F}_q(t)$ – Tate Module

- $\mathrm{Frob} \in \mathrm{Gal}_{\mathbb{F}_q} \to \mathrm{Aut}\, \mathrm{T}_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^{2g}$

- $\mathrm{coker}\,(\mathrm{Frob} - \mathrm{Id}) \cong \mathrm{Jac}_C(\mathbb{F}_q)_\ell = \mathrm{Pic}^0(C)$

Random Tate-modules

$F \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ (w/ Haar measure)

Random Tate-modules

$F \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ (w/ Haar measure)

Theorem (Friedman, Washington)

$$P(\operatorname{coker} F - I \cong L) = \frac{C_\ell}{\# \operatorname{Aut} L}$$

Random Tate-modules

$$F \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \text{ (w/ Haar measure)}$$

Theorem (Friedman, Washington)

$$P(\operatorname{coker} F - I \cong L) = \frac{C_\ell}{\# \operatorname{Aut} L}$$

Conjecture

$$P(\operatorname{Pic}^0(C) \cong L) = \frac{C_\ell}{\# \operatorname{Aut} L}$$

Progress

In the limit (w/ upper and lower densities):

Achter	–	conjectures are true for GSp_{2g} instead of GL_{2g}.
Ellenberg-Venkatesh	–	conjectures are true if $\ell \nmid q-1$.
Garton	–	explicit conjectures for $\mathrm{GSp}_{2g}, \ell \mid q-1$.

Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

Basic question – what is

$$P(p \mid \# \operatorname{Jac}_C(\mathbb{F}_p))?$$

Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

$$T_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^r,\ 0 \le r \le g$$

Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

$$T_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^r,\ 0 \leq r \leq g$$

Definition

The *p*-**rank** of Jac_C is the integer r.

Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

$$T_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^r,\ 0 \leq r \leq g$$

Definition

The p-**rank** of Jac_C is the integer r.

Complication

As C varies, r varies. Need to know the distribution of p-ranks, or find a better algebraic gadget than $\mathrm{T}_\ell(\mathrm{Jac}_C)$.

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^{\sigma} F, Vz = z^{\sigma^{-1}} V)$.

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

Jac_C

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^{\sigma} F, Vz = z^{\sigma^{-1}} V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

$$\begin{tikzcd}
 & M = H^1_{\mathrm{cris}}(\mathrm{Jac}_C, \mathbb{Z}_p) \\
\mathrm{Jac}_C \arrow[ur, dashed] &
\end{tikzcd}$$

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

$$\begin{tikzcd}
 & M = H^1_{\mathrm{cris}}(\mathrm{Jac}_C, \mathbb{Z}_p) \\
\mathrm{Jac}_C \arrow[ur, dashed] \arrow[dr, dashed] & \\
 & \{\mathrm{Jac}_C[p^n]\}_n \arrow[uu, dashed]
\end{tikzcd}$$

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

$$\begin{tikzcd}
 & M = H^1_{\mathrm{cris}}(\mathrm{Jac}_C, \mathbb{Z}_p) \arrow[dr] & \\
\mathrm{Jac}_C \arrow[ur, dashed] \arrow[dr, dashed] & & H^1_{\mathrm{dR}}(\mathrm{Jac}_C, \mathbb{F}_p) \\
 & \{\mathrm{Jac}_C[p^n]\}_n \arrow[uu, dashed] &
\end{tikzcd}$$

Dieudonné Modules

Definition

(i) $\mathbb{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^{\sigma}F, Vz = z^{\sigma^{-1}}V)$.

(ii) A **Dieudonné module** is a $\mathbb{D}$-module which is finite and free as a $\mathbb{Z}_q$ module.

$$\begin{tikzcd}
 & M = H^1_{\mathrm{cris}}(\mathrm{Jac}_C, \mathbb{Z}_p) \arrow[dr] & \\
\mathrm{Jac}_C \arrow[ur, dashed] \arrow[dr, dashed] & & H^1_{\mathrm{dR}}(\mathrm{Jac}_C, \mathbb{F}_p) \arrow[loop below] \\
 & \{\mathrm{Jac}_C[p^n]\}_n \arrow[uu, dashed] &
\end{tikzcd}$$

$$V^{-1} \colon df \mapsto \frac{\text{“}d(f^p)\text{”}}{p}$$

Invariants via Dieudonné Modules

Invariants

(i) p-rank$(\mathrm{Jac}_C) = \dim F^\infty(M \otimes \mathbb{F}_p)$.

(ii) $a(\mathrm{Jac}_C) = \dim \mathrm{Hom}(\alpha_p, \mathrm{Jac}_C[p]) = \dim\,(\ker V \cap \ker F)$.

(iii) $\mathrm{Jac}_C(\mathbb{F}_p)_p = \mathrm{coker}(F - \mathrm{Id})|_{F^\infty(M\otimes\mathbb{F}_p)}$.

Principally quasi polarized Dieudoneé modules

Definition

A **principally quasi polarized** Dieudoneé module a Dieudoneé module M together with a non-degenerate symplectic pairing $\langle\,,\,\rangle$ such that for all $x, y \in M$,

$$\langle Fx, y\rangle = \sigma\langle x, Vy\rangle.$$

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

(ii) $$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

(ii) $$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

(iii) $P(r(M) = g - s) =$ *complicated but explicit expression.*

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

(ii) $$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

(iii) $P(r(M) = g - s) =$ *complicated but explicit expression.*

(iii') $$P(r(M) = g - 2) = (p^{-2} + p^{-3}) \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

(ii) $$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

(iii) $P(r(M) = g - s) =$ *complicated but explicit expression.*

(iii') $$P(r(M) = g - 2) = (p^{-2} + p^{-3}) \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$

(iv) 1^{st} *moment is 2.*

Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) $\mathrm{Mod}^{pqp}\,\mathbb{D}$ *has a natural probability measure.*

(Push forward along $\mathrm{Sp}_{2g}(\mathbb{Z}_p)^2 \to \mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$*)*

(ii) $$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

(iii) $P(r(M) = g - s) =$ *complicated but explicit expression.*

(iii') $$P(r(M) = g - 2) = (p^{-2} + p^{-3}) \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$

(iv) 1^{st} *moment is 2.*

(v) $P\left(p \nmid \#\,\mathrm{coker}(F - \mathrm{Id})|_{F^\infty(M \otimes \mathbb{F}_p)}\right) = C_p.$

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\, \mathbb{D}$ has a natural probability measure.

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\,\mathbb{D}$ has a natural probability measure.

1. $(D, \langle\ ,\ \rangle, F, V)$ s.t., $FV = VF = p$ and $\langle F(-)\,, -\rangle = \sigma\langle -\,, V(-)\rangle$.

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\,\mathbb{D}$ has a natural probability measure.

1. $(D, \langle\ ,\ \rangle, F, V)$ s.t., $FV = VF = p$ and $\langle F(-)\,, -\rangle = \sigma\langle -\,, V(-)\rangle$.
2. $D = \mathbb{Z}_q^{2g}$, $\langle\ ,\ \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, $F_0 = \begin{bmatrix} pI & 0 \\ 0 & I \end{bmatrix}$, $V_0 = pF^{-1}$.

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\,\mathbb{D}$ has a natural probability measure.

1. $(D, \langle\,,\rangle, F, V)$ s.t., $FV = VF = p$ and $\langle F(-)\,,-\rangle = \sigma\langle -\,, V(-)\rangle$.
2. $D = \mathbb{Z}_q^{2g}$, $\langle\,,\rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, $F_0 = \begin{bmatrix} pI & 0 \\ 0 & I \end{bmatrix}$, $V_0 = pF^{-1}$.

Proposition

The double coset space $\mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$ contains **all** pqp Dieudoneé modules.

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\,\mathbb{D}$ has a natural probability measure.

1. $(D, \langle\,,\rangle, F, V)$ s.t., $FV = VF = p$ and $\langle F(-)\,,-\rangle = \sigma\langle -\,, V(-)\rangle$.
2. $D = \mathbb{Z}_q^{2g}$, $\langle\,,\rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, $F_0 = \begin{bmatrix} pI & 0 \\ 0 & I \end{bmatrix}$, $V_0 = pF^{-1}$.

Proposition

The double coset space $\mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$ contains **all** pqp Dieudoneé modules.

Proof: Witt's theorem – Sp_{2g} acts transitively on symplecto-bases.

Proofs

Part (i)

$\mathrm{Mod}^{\mathrm{pqp}}\,\mathbb{D}$ has a natural probability measure.

1. $(D, \langle\ ,\ \rangle, F, V)$ s.t., $FV = VF = p$ and $\langle F(-)\,, -\rangle = \sigma\langle -\,, V(-)\rangle$.
2. $D = \mathbb{Z}_q^{2g}$, $\langle\ ,\ \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, $F_0 = \begin{bmatrix} pI & 0 \\ 0 & I \end{bmatrix}$, $V_0 = pF^{-1}$.

Proposition

The double coset space $\mathrm{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \mathrm{Sp}_{2g}(\mathbb{Z}_p)$ contains **all** pqp Dieudoneé modules.

Proof: Witt's theorem – Sp_{2g} acts transitively on symplecto-bases.
Note: $F \notin \mathrm{Sp}_{2g}(\mathbb{Z}_p)$, but rather the subset of $\mathrm{GSp}_{2g}(\mathbb{Z}_p)$ of multiplier p^g matricies.

Proofs

Part (ii)

$$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

Proofs

Part (ii)

$$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

1. Duality implies that $W_1 := \ker(F \otimes \mathbb{F}_p)$ and $W_2 := \ker(V \otimes \mathbb{F}_p)$ are maximal isotropics.

Proofs

Part (ii)

$$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

1. Duality implies that $W_1 := \ker(F \otimes \mathbb{F}_p)$ and $W_2 := \ker(V \otimes \mathbb{F}_p)$ are maximal isotropics.
2. $a(M) = \dim\left(W_1 \cap W_2\right)$

Proofs

Part (ii)

$$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

1. Duality implies that $W_1 := \ker(F \otimes \mathbb{F}_p)$ and $W_2 := \ker(V \otimes \mathbb{F}_p)$ are maximal isotropics.
2. $a(M) = \dim\left(W_1 \cap W_2\right)$
3. Argue that W_1 and W_2 are randomly distributed.

Proofs

Part (ii)

$$P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s} \left(1 - p^{-i}\right)^{-1}.$$

1. Duality implies that $W_1 := \ker(F \otimes \mathbb{F}_p)$ and $W_2 := \ker(V \otimes \mathbb{F}_p)$ are maximal isotropics.
2. $a(M) = \dim(W_1 \cap W_2)$
3. Argue that W_1 and W_2 are randomly distributed.
4. This expression is the probability that two random maximal isotropics intersect with dimension s.

Proofs

Part (ii)

$$P(a(M)=s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty}\left(1+p^{-i}\right)^{-1} \cdot \prod_{i=1}^{s}\left(1-p^{-i}\right)^{-1}.$$

1. Duality implies that $W_1 := \ker(F \otimes \mathbb{F}_p)$ and $W_2 := \ker(V \otimes \mathbb{F}_p)$ are maximal isotropics.
2. $a(M) = \dim\left(W_1 \cap W_2\right)$
3. Argue that W_1 and W_2 are randomly distributed.
4. This expression is the probability that two random maximal isotropics intersect with dimension s.
5. Compute this with Witt's theorem (Sp_{2g} acts transitively on *pairs* of maximal isotropics whose intersection has dimension s), and compute explicitly the size of the stabilizers.

Proofs

Part (iii)

$P(r(M) = g - s) =$ complicated but explicit expression.

Proofs

Part (iii)

$$P(r(M) = g - s) = \text{complicated but explicit expression.}$$

1. Recall: $r(M) = \dim F^{\infty}(M) = \operatorname{rank}(F \otimes \mathbb{F}_p)^g$.

Proofs

Part (iii)

$$P(r(M) = g - s) = \text{complicated but explicit expression.}$$

1. Recall: $r(M) = \dim F^{\infty}(M) = \operatorname{rank}(F \otimes \mathbb{F}_p)^g$.
2. (Prüfer, Crabb, others) The number of nilpotent $N \in \mathrm{M}_n(\mathbb{F}_q)$ is $q^{n(n-1)}$. Able to modify Crabb's argument:

Proofs

Part (iii)

$$P(r(M) = g - s) = \text{complicated but explicit expression.}$$

1. Recall: $r(M) = \dim F^{\infty}(M) = \operatorname{rank}(F \otimes \mathbb{F}_p)^g$.
2. (Prüfer, Crabb, others) The number of nilpotent $N \in \mathrm{M}_n(\mathbb{F}_q)$ is $q^{n(n-1)}$. Able to modify Crabb's argument:
    1. Given N nilpotent, get a flag $V_i := N^i(V)$.

Proofs

Part (iii)

$P(r(M) = g - s) =$ complicated but explicit expression.

1. Recall: $r(M) = \dim F^\infty(M) = \mathrm{rank}(F \otimes \mathbb{F}_p)^g$.
2. (Prüfer, Crabb, others) The number of nilpotent $N \in \mathrm{M}_n(\mathbb{F}_q)$ is $q^{n(n-1)}$. Able to modify Crabb's argument:
   1. Given N nilpotent, get a flag $V_i := N^i(V)$.
   2. There is a unique basis $\{y_1, \ldots, y_g\}$ such that $N(y_g) = 0$ and $V_i = \langle N^i(y_{m_i+1}), \ldots, N(y_{g-1})\rangle$ (where $m_i = g - \dim V_{i-1}$)

Proofs

Part (iii)

$P(r(M) = g - s) =$ complicated but explicit expression.

1. Recall: $r(M) = \dim F^{\infty}(M) = \operatorname{rank}(F \otimes \mathbb{F}_p)^g$.
2. (Prüfer, Crabb, others) The number of nilpotent $N \in \mathrm{M}_n(\mathbb{F}_q)$ is $q^{n(n-1)}$. Able to modify Crabb's argument:
    1. Given N nilpotent, get a flag $V_i := N^i(V)$.
    2. There is a unique basis $\{y_1, \ldots, y_g\}$ such that $N(y_g) = 0$ and $V_i = \langle N^i(y_{m_i+1}), \ldots, N(y_{g-1})\rangle$ (where $m_i = g - \dim V_{i-1}$)
    3. The map $N \mapsto (N(y_1), \ldots, N(y_{g-1})) \in V^{n-1}$ is bijective.

Proofs

Part (iv)

1^{st} moment is 2: $\mathrm{Avg}\left(\#G(\mathbb{F}_p)[p]\right) = 2$

Proofs

Part (iv)

1^{st} moment is 2: $\operatorname{Avg}(\#G(\mathbb{F}_p)[p]) = 2$

1. First fix the p-corank.

Proofs

Part (iv)

1^{st} moment is 2: $\mathrm{Avg}\left(\#G(\mathbb{F}_p)[p]\right) = 2$

1. First fix the p-corank.
   1. Associated p-divisible group decomposes as

$$G = G^m \times G^{et} \times G^{ll}.$$

Proofs

Part (iv)

1^{st} moment is 2: $\operatorname{Avg}\left(\#G(\mathbb{F}_p)[p]\right) = 2$

1. First fix the p-corank.
   1. Associated p-divisible group decomposes as
   $$G = G^m \times G^{et} \times G^{ll}.$$
   2. Fixing the p-corank fixes the dimension of G^{ll}

Proofs

Part (iv)

1^{st} moment is 2: $\text{Avg}\,(\#G(\mathbb{F}_p)[p]) = 2$

1. First fix the p-corank.
   1. Associated p-divisible group decomposes as
   $$G = G^m \times G^{et} \times G^{ll}.$$
   2. Fixing the p-corank fixes the dimension of G^{ll}
2. (Show that G random $\Rightarrow G^{et}$ random.)

Proofs

Part (iv)

1^{st} moment is 2: $\mathrm{Avg}\left(\# G(\mathbb{F}_p)[p]\right) = 2$

1. First fix the p-corank.
    1. Associated p-divisible group decomposes as
    $$G = G^m \times G^{et} \times G^{ll}.$$
    2. Fixing the p-corank fixes the dimension of G^{ll}
2. (Show that G random $\Rightarrow G^{et}$ random.)
3. $G(\mathbb{F}_p) = G^{et}(\mathbb{F}_p) = \mathrm{coker}(F|_{M^{et}} - \mathrm{Id})$.

Proofs

Part (iv)

1[st] moment is 2: $\mathrm{Avg}\left(\#G(\mathbb{F}_p)[p]\right) = 2$

1. First fix the p-corank.
   1. Associated p-divisible group decomposes as
      $$G = G^m \times G^{et} \times G^{ll}.$$
   2. Fixing the p-corank fixes the dimension of G^{ll}
2. (Show that G random $\Rightarrow G^{et}$ random.)
3. $G(\mathbb{F}_p) = G^{et}(\mathbb{F}_p) = \mathrm{coker}(F|_{M^{et}} - \mathrm{Id})$.
4. $F|_{M^{et}}$ is random in $\mathrm{GL}_g(\mathbb{Z}_p)$.

Proofs

Part (v)

$$P\left(p \nmid \#\operatorname{coker}(F - \mathrm{Id})|_{F^\infty(M\otimes\mathbb{F}_p)}\right) = C_p.$$

Proofs

Part (v)

$$P\left(p \nmid \#\operatorname{coker}(F - \mathrm{Id})|_{F^\infty(M \otimes \mathbb{F}_p)}\right) = C_p.$$

Basically the same proof as the last part.

Data, Moduli Spaces and Wild Speculation

Question

Does $P(p \nmid \# \operatorname{Jac}_C(\mathbb{F}_p)) = C_p$?

Data, Moduli Spaces and Wild Speculation

Question

Does $P(p \nmid \# \mathrm{Jac}_C(\mathbb{F}_p)) = C_p$?

Data

- C hyperelliptic, $p \neq 2$ – **YES**!

Data, Moduli Spaces and Wild Speculation

Question

Does $P(p \nmid \# \mathrm{Jac}_C(\mathbb{F}_p)) = C_p$?

Data

- C hyperelliptic, $p \neq 2$ – **YES**!
- C plane curve, $p \neq 2$ – **YES**!

Data, Moduli Spaces and Wild Speculation

Question

Does $P(p \nmid \# \mathrm{Jac}_C(\mathbb{F}_p)) = C_p$?

Data

- C hyperelliptic, $p \neq 2$ – **YES**!
- C plane curve, $p \neq 2$ – **YES**!
- C plane curve, $p = 2$ –

Data, Moduli Spaces and Wild Speculation

Question

Does $P(p \nmid \# \operatorname{Jac}_C(\mathbb{F}_p)) = C_p$?

Data

- C hyperelliptic, $p \neq 2$ – **YES**!
- C plane curve, $p \neq 2$ – **YES**!
- C plane curve, $p = 2$ – **NO**!?!

C plane curve, $p = 2$

Theorem (Cais, Ellenberg, ZB)

$P(2 \nmid \# \operatorname{Jac}_C(\mathbb{F}_2)) = 0$ for plane curves of **odd** degree.

C plane curve, $p = 2$

Theorem (Cais, Ellenberg, ZB)

$P(2 \nmid \# \mathrm{Jac}_C(\mathbb{F}_2)) = 0$ for plane curves of **odd** degree.

Proof – theta characteristics.

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$
$$= \prod_{i=1}^{\infty} \left(1 - p^{-2i+1}\right)?$$

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$
$$= \prod_{i=1}^{\infty} \left(1 - p^{-2i+1}\right)?$$

Data

- C hyperelliptic, $p \neq 2$ –

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$
$$= \prod_{i=1}^{\infty} \left(1 - p^{-2i+1}\right)?$$

Data

- C hyperelliptic, $p \neq 2$ – **not quite**.

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$
$$= \prod_{i=1}^{\infty} \left(1 - p^{-2i+1}\right)?$$

Data

- C hyperelliptic, $p \neq 2$ – **not quite**.

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = 1 - 3^{-1} \qquad (p = 3)$$

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1}$$
$$= \prod_{i=1}^{\infty} \left(1 - p^{-2i+1}\right)?$$

Data

- C hyperelliptic, $p \neq 2$ – **not quite**.

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = 1 - 3^{-1} \qquad (p = 3)$$
$$= (1 - 5^{-1})(1 - 5^{-3}) \qquad (p = 5)$$

a-number data

Does

$$P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} \left(1 + p^{-i}\right)^{-1} = \prod_{i=1}^{\infty} (1 - p^{-2i+1})?$$

Data

- C hyperelliptic, $p \neq 2$ – **not quite**.

$$\begin{aligned} P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) &= 1 - 3^{-1} && (p = 3) \\ &= (1 - 5^{-1})(1 - 5^{-3}) && (p = 5) \\ &= (1 - 7^{-1})(1 - 7^{-3})(1 - 7^{-5}) && (p = 7) \end{aligned}$$

Rational points on Moduli Spaces

- $P(a(\mathrm{Jac}_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{H}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{H}_g(\mathbb{F}_p)}$.

Rational points on Moduli Spaces

- $P(a(\mathrm{Jac}_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{H}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{H}_g(\mathbb{F}_p)}$.
- One can access this through cohomology and the Weil conjectures.

Rational points on Moduli Spaces

- $P(a(\mathrm{Jac}_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{H}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{H}_g(\mathbb{F}_p)}$.
- One can access this through cohomology and the Weil conjectures.
- Our data suggests that $\mathcal{H}_g^{\mathrm{ord}}$ has cohomology that **does not arise by pulling back** from $\mathcal{H}_g$.

Rational points on Moduli Spaces

- $P(a(\mathrm{Jac}_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{H}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{H}_g(\mathbb{F}_p)}$.
- One can access this through cohomology and the Weil conjectures.
- Our data suggests that $\mathcal{H}_g^{\mathrm{ord}}$ has cohomology that **does not arise by pulling back** from $\mathcal{H}_g$.
- $P(a(\mathrm{Jac}_C(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{M}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{M}_g(\mathbb{F}_p)} = ???$

Rational points on Moduli Spaces

- $P(a(\mathrm{Jac}_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{H}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{H}_g(\mathbb{F}_p)}$.

- One can access this through cohomology and the Weil conjectures.

- Our data suggests that $\mathcal{H}_g^{\mathrm{ord}}$ has cohomology that **does not arise by pulling back** from $\mathcal{H}_g$.

- $P(a(\mathrm{Jac}_{C}(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{M}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{M}_g(\mathbb{F}_p)} = ???$

- $P(a(A(\mathbb{F}_p)) = 0) = \lim_{g\to\infty} \frac{\#\mathcal{A}_g^{\mathrm{ord}}(\mathbb{F}_p)}{\#\mathcal{A}_g(\mathbb{F}_p)} = ???$

Thank You!