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?

\[ P(p \mid h(-D)) = P(p \mid D) = \frac{1}{p} \]
\begin{equation}
P(p \mid h(-D)) \approx \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + \cdots \quad (p \text{ odd})
\end{equation}

\begin{align*}
&= 1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^i}\right) \\
&= 0.43 \ldots \neq 1/3 \quad (p = 3) \\
&= 0.23 \ldots \neq 1/5 \quad (p = 5)
\end{align*}

\begin{align*}
P(\text{Cl}(-D)_3 \cong \mathbb{Z}/9\mathbb{Z}) &\approx 0.070 \\
P(\text{Cl}(-D)_3 \cong (\mathbb{Z}/3\mathbb{Z})^2) &\approx 0.0097
\end{align*}
Random finite abelian groups

Idea

\[ P(p \mid h(-D)) = P(p \mid \#G) = ??? \]
Let $G_p$ 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 \( G_p \) be the set of isomorphism classes of **finite abelian groups of \( p \)-power order**.

Theorem (Cohen, Lenstra)

(i) \[ \sum_{G \in G_p} \frac{1}{\# \text{Aut } G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1} \]
Random finite abelian groups

Idea

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

Let \( G_p \) be the set of isomorphism classes of finite abelian groups of \( p \)-power order.

Theorem (Cohen, Lenstra)

(i) \[ \sum_{G \in G_p} \frac{1}{\# \text{Aut } G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1} \]

(ii) \( G \mapsto \frac{C_p}{\# \text{Aut } G} \) is a probability distribution on \( G_p \)
Random finite abelian groups

**Idea**

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

Let \( G_p \) be the set of isomorphism classes of **finite abelian groups of \( p \)-power order.**

**Theorem (Cohen, Lenstra)**

(i) \[ \sum_{G \in G_p} \frac{1}{\# \text{Aut } G} = \prod_i \left(1 - \frac{1}{p^i}\right)^{-1} = C_p^{-1} \]

(ii) \( G \mapsto \frac{C_p}{\# \text{Aut } G} \) is a **probability distribution** on \( G_p \)

(iii) \[ \text{Avg } (\#G[p]) = \text{Avg } (p^{r_{p}(G)}) = 2 \]
Cohen and Lenstra’s conjecture

Let \( f : G_p \rightarrow \mathbb{Z} \) be a function.

**Definition**

\[
\text{Avg } f = \sum_{G \in G_p} \frac{C_p}{\# \text{Aut } G} \cdot f(G)
\]
Cohen and Lenstra’s conjecture

Let $f: G_p \rightarrow \mathbb{Z}$ be a function.

**Definition**

$$\text{Avg } f = \sum_{G \in G_p} \frac{C_p}{\# \text{Aut } G} \cdot f(G)$$

$$\text{Avg}_{\text{Cl}} f = \frac{\sum_{0 \leq D \leq X} f(\text{Cl}(-D)_p)}{\sum_{0 \leq D \leq X} 1}$$
Cohen and Lenstra’s conjecture

Let \( f : G_p \to \mathbb{Z} \) be a function.

**Definition**

\[
\text{Avg } f = \sum_{G \in G_p} \frac{C_p}{\# \text{Aut } G} \cdot f(G)
\]

\[
\text{Avg}_{\text{Cl}} f = \frac{\sum_{0 \leq D \leq X} f(\text{Cl}(-D)_p)}{\sum_{0 \leq D \leq X} 1}
\]

**Conjecture (Cohen, Lenstra)**

(i) \( \text{Avg}_{\text{Cl}} f = \text{Avg } f \)
Cohen and Lenstra’s conjecture

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

**Definition**

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

$$\text{Avg}_\text{Cl } f = \sum_{0 \leq D \leq X} f(\text{Cl}(-D)[p]) \frac{1}{\sum_{0 \leq D \leq X} 1}$$

**Conjecture (Cohen, Lenstra)**

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

(ii) $\text{Avg } (\# \text{Cl}(-D)[p]) = 2$
Cohen and Lenstra’s conjecture

Let $f : G_p \rightarrow \mathbb{Z}$ be a function.

**Definition**

$$\text{Avg } f = \sum_{G \in G_p} \frac{C_p}{\# \text{Aut } G} \cdot f(G)$$

$$\text{Avg}_{\text{Cl}} f = \frac{\sum_{0 \leq D \leq X} f(\text{Cl}(-D)_p)}{\sum_{0 \leq D \leq X} 1}$$

**Conjecture (Cohen, Lenstra)**

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

(ii) $\text{Avg } (\# \text{Cl}(-D)[p])^2 = 2 + p$
Cohen and Lenstra’s conjecture

Let $f : \mathbb{G}_p \rightarrow \mathbb{Z}$ be a function.

**Definition**

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

$$\text{Avg}_{\text{Cl } f} = \frac{\sum_{0 \leq D \leq X} f(\text{Cl}(-D)_p)}{\sum_{0 \leq D \leq X} 1}$$

**Conjecture (Cohen, Lenstra)**

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

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

(iii) $P(\text{Cl}(-D)_p \cong G) = \frac{C_p}{\# \text{ Aut } G}$. 
<table>
<thead>
<tr>
<th>Researcher</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Davenport-Heilbronn</td>
<td>$\text{Avg Cl}(–D)[3] = 2$</td>
</tr>
<tr>
<td>Bhargava</td>
<td>$\text{Avg Cl}(K)[2] = 3$ ($K$ cubic)</td>
</tr>
<tr>
<td>Bhargava</td>
<td>counts quartic dihedral extensions</td>
</tr>
<tr>
<td>Kohnen-Ono</td>
<td>$N_{p</td>
</tr>
<tr>
<td>Heath-Brown</td>
<td>$N_{p</td>
</tr>
<tr>
<td>Byeon</td>
<td>$N_{\text{Cl}_p \cong (\mathbb{Z}/g\mathbb{Z})^2}(X) \gg \frac{x^{\frac{1}{g}}}{\log x}$</td>
</tr>
</tbody>
</table>
Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

\[
\text{Cl}(-D) = \text{Pic}(\text{Spec } \mathcal{O}_K)
\]

VS

\[
\text{Pic}(C)
\]
Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

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

VS

$$\text{Pic}(C) \xrightarrow{\text{deg}} \mathbb{Z} \to 0$$
Cohen-Lenstra over $\mathbb{F}_q(t)$, $\ell \neq p$

\[
\text{Cl}(-D) = \text{Pic}(\text{Spec } \mathcal{O}_K)
\]

\[
\text{VS}
\]

\[
0 \rightarrow \text{Pic}^0(C) \rightarrow \text{Pic}(C) \xrightarrow{\text{deg}} \mathbb{Z} \rightarrow 0
\]
Basic Question over $\mathbb{F}_q(t)$, $\ell \neq p$

Fix $G \in G_{\ell}$.

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

(Limit is taken as $\deg f \to \infty$, where $C : y^2 = f(x)$.)
\[ \text{Aut } T_\ell (\text{Jac}_C) \cong \mathbb{Z}_\ell^{2g} \]
\[ \text{Gal}_{\mathbb{F}_q} \to \text{Aut} \, T_\ell(Jac_C) \cong \mathbb{Z}_\ell^{2g} \]
Frob ∈ Gal_{F_q} → Aut T_ℓ(Jac_C) ≅ \mathbb{Z}_ℓ^{2g}
Main Tool over $\mathbb{F}_q(t)$ – Tate Module

- $\text{Frob} \in \text{Gal}_{\mathbb{F}_q} \to \text{Aut } T_\ell(Jac_C) \cong \mathbb{Z}_\ell^{2g}$

- $\text{coker } (\text{Frob} - \text{Id}) \cong Jac_C(\mathbb{F}_q)_\ell = \text{Pic}^0(C)$
Random Tate-modules

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

**Theorem (Friedman, Washington)**

$$P(\text{coker } F - I \cong L) = \frac{C_\ell}{\# \text{Aut } L}$$
\[ F \in \text{GL}_{2g}(\mathbb{Z}_\ell) \text{ (w/ Haar measure)} \]

**Theorem (Friedman, Washington)**

\[ P(\text{coker } F - I \cong L) = \frac{C_\ell}{\# \text{ Aut } L} \]

**Conjecture**

\[ P(\text{Pic}^0(C) \cong L) = \frac{C_\ell}{\# \text{ Aut } L} \]
In the limit (w/ upper and lower densities):

Achter – conjectures are true for $\text{GSp}_{2g}$ instead of $\text{GL}_{2g}$.

Ellenberg-Venkatesh – conjectures are true if $\ell \nmid q - 1$.

Garton – explicit conjectures for $\text{GSp}_{2g}, \ell \mid q - 1$. 
Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

Basic question – what is $P(p \mid \# \text{Jac}_C(\mathbb{F}_p))$?
Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

\[ T_\ell(\text{Jac}_C) \cong \mathbb{Z}_\ell^r, \quad 0 \leq r \leq g \]
Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

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

**Definition**

The $p$-**rank** of $\text{Jac}_C$ is the integer $r$. 
Cohen-Lenstra over $\mathbb{F}_p(t)$, $\ell = p$

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

**Definition**

The \textbf{$p$-rank} of $\text{Jac}_C$ 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 $T_\ell(\text{Jac}_C)$. 
(i) $\mathcal{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V)$. 

Definition
Dieudonné Modules

Definition

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

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

Definition

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

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

\[ \text{Jac}_C \]
Dieudonné Modules

Definition

1. \( \mathcal{D} = \mathbb{Z}_q[F, V]/(FV = VF = p, Fz = z^\sigma F, Vz = z^{\sigma^{-1}} V) \).
2. A **Dieudonné module** is a \( \mathcal{D} \)-module which is finite and free as a \( \mathbb{Z}_q \) module.

\[
M = H^1_{\text{cris}}(\text{Jac} C, \mathbb{Z}_p)
\]

\( \text{Jac} C \)
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.

\[
M = H^1_{\text{cris}}(\text{Jac}_C, \mathbb{Z}_p)
\]
Dieudonné Modules

**Definition**

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

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

\[
M = H^1_{\text{cris}}(\text{Jac}_C, \mathbb{Z}_p)
\]

\[
\{ \text{Jac}_C[p^n] \}_n
\]

\[
H^1_{\text{dR}}(\text{Jac}_C, \mathbb{F}_p)
\]
Dieudonné Modules

**Definition**

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

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

\[
M = H^1_{\text{cris}}(\text{Jac}_C, \mathbb{Z}_p)
\]

\[
\{ \text{Jac}_C[p^n] \}_n
\]

\[
H^1_{\text{dR}}(\text{Jac}_C, \mathbb{F}_p)
\]

\[
V^{-1}: df \mapsto \frac{"d(f^p)"}{p}
\]
Invariants via Dieudonné Modules

Invariants

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

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

(iii) \( \text{Jac}_C(\mathbb{F}_p)_p = \text{coker}(F - \text{Id})|_{F^\infty(M \otimes \mathbb{F}_p)}. \)
A **principally quasi polarized** Dieudonné module is a Dieudonné module $M$ together with a non-degenerate symplectic pairing $\langle \cdot, \cdot \rangle$ such that for all $x, y \in M$,

$$\langle Fx, y \rangle = \sigma \langle x, V y \rangle.$$
Main Theorem

Theorem (Cais, Ellenberg, ZB)

(i) Mod\(^{pqp}\) \(D\) has a natural probability measure.
Main Theorem

**Theorem (Cais, Ellenberg, ZB)**

(i) $\text{Mod}^{p_{qp}} \mathbb{D}$ has a natural probability measure.

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

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

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

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

(iv) 1st moment is 2.

(v) $P(p \nmid \# \text{coker}(F - \text{Id}) | F_\infty (M \otimes F_p)) = C_p.$
Main Theorem

**Theorem (Cais, Ellenberg, ZB)**

(i) $\text{Mod}^{pqp} \mathcal{D}$ has a natural probability measure.

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

(ii) $P(a(M) = s) = p^{-(s+1)/2} \cdot \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} \cdot \prod_{i=1}^{s} (1 - p^{-i})^{-1}.$
Main Theorem

Theorem (Cais, Ellenberg, ZB)

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

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

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

(iii) $P(r(M) = g - s) = \text{complicated but explicit expression}$.
Theorem (Cais, Ellenberg, ZB)

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

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

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

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

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

Theorem (Cais, Ellenberg, ZB)

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

\[(\text{Push forward along } \text{Sp}_{2g}(\mathbb{Z}_p)^2 \to \text{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \text{Sp}_{2g}(\mathbb{Z}_p))\]

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

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

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

(iv) $1^{st}$ moment is 2.
Main Theorem

**Theorem (Cais, Ellenberg, ZB)**

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

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

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

(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) $P \left( p \nmid \# \text{coker}(F - \text{Id}) \mid F_{\infty} (M \otimes_{F_p}) \right) = C_p$. 

David Zureick-Brown  (Emory University)  Random Dieudonné Modules  November 13, 2012  19 / 29
Proofs

Part (i)

Mod^{qp} D has a natural probability measure.
Part (i)

\[\text{Mod}^{\text{pp}} \mathbb{D} \text{ has a natural probability measure.}\]

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

Part (i)

\( \text{Mod}^{\text{pqp}} \mathbb{D} \) has a natural probability measure.

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

2. \(D = \mathbb{Z}_q^{2g}, \langle \cdot, \cdot \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, F_0 = \begin{bmatrix} pl & 0 \\ 0 & I \end{bmatrix}, V_0 = pF^{-1}\).
Proofs

Part (i)

\( \text{Mod}^{pqp} \mathbb{D} \) 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. \( D = \mathbb{Z}_q^{2g}, \langle , \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, F_0 = \begin{bmatrix} pl & 0 \\ 0 & I \end{bmatrix}, V_0 = pF^{-1}. \)

Proposition

The double coset space \( \text{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \text{Sp}_{2g}(\mathbb{Z}_p) \) contains all \( pqp \) Dieudonné modules.
Proofs

Part (i)

\[ \text{Mod}_{pq}^D \text{ has a natural probability measure.} \]

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

2. \(D = \mathbb{Z}_{q^2}, \langle , \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, F_0 = \begin{bmatrix} pl & 0 \\ 0 & I \end{bmatrix}, V_0 = pF^{-1}.\)

Proposition

The double coset space \(\text{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \text{Sp}_{2g}(\mathbb{Z}_p)\) contains all \(pq\) Dieudonné modules.

Proof: Witt’s theorem – \(\text{Sp}_{2g}\) acts transitively on symplecto-bases.
Proofs

Part (i)

\( \text{Mod}^{pqp} \mathbb{D} \) has a natural probability measure.

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

2. \(D = \mathbb{Z}_q^{2g}, \langle \cdot, \cdot \rangle = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, F_0 = \begin{bmatrix} pl & 0 \\ 0 & I \end{bmatrix}, V_0 = pF^{-1}\).

Proposition

The double coset space \(\text{Sp}_{2g}(\mathbb{Z}_p) \cdot F_0 \cdot \text{Sp}_{2g}(\mathbb{Z}_p)\) contains all \(pqp\) Dieudonné modules.

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

Part (ii)

\[ P(a(M) = s) = p^{-\binom{s+1}{2}} \cdot \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} \cdot \prod_{i=1}^{s} (1 - p^{-i})^{-1}. \]
Part (ii)

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

**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)

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

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. \( a(M) = \dim(W_1 \cap W_2) \)
Part (ii)

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

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.
Part (ii)

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

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 \( s \).
Part (ii)

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

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 \( s \).

5. Compute this with Witt’s theorem (\( \text{Sp}_{2g} \) acts transitively on pairs of maximal isotropics whose intersection has dimension \( s \)), and compute explicitly the size of the stabilizers.
Part (iii)

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

Part (iii)

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

1. Recall: \( r(M) = \dim F^\infty(M) = \text{rank}(F \otimes F_p)^g \).
Proofs

Part (iii)

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

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

2. (Prüfer, Crabb, others) The number of nilpotent \( N \in M_n(\mathbb{F}_q) \) 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: \( r(M) = \dim F^\infty(M) = \text{rank}(F \otimes \mathbb{F}_p)^g. \)

2. (Prüfer, Crabb, others) The number of nilpotent \( N \in M_n(\mathbb{F}_q) \) is \( q^{n(n-1)}. \) Able to modify Crabb’s argument:
   
   1. Given \( N \) nilpotent, get a flag \( V_i := N^i(V). \)
Part (iii)

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

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

2. (Prüfer, Crabb, others) The number of nilpotent \( N \in M_n(\mathbb{F}_q) \) 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)

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

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

2. (Prüfer, Crabb, others) The number of nilpotent \( N \in M_n(\mathbb{F}_q) \) 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.
Part (iv)

$1^{st}$ moment is 2: $\text{Avg}(\#G(F_p)[p]) = 2$
### Part (iv)

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

1. First fix the \( p \)-corank.
Proofs

Part (iv)

1st moment is 2: \( \text{Avg} \left( \# G(F_p)[p] \right) = 2 \)

1. First fix the \( p \)-corank.
   - Associated \( p \)-divisible group decomposes as
     \[
     G = G^m \times G^{\text{et}} \times G^{ll}.
     \]
Proofs

Part (iv)

1\textsuperscript{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 \( G^{ll} \)
Part (iv)

1\textsuperscript{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
      \[
      G = G^m \times G^{et} \times G^\flat.
      \]

2. Fixing the \( p \)-corank fixes the dimension of \( G^\flat \)

2. (Show that \( G \) random \( \Rightarrow \) \( G^{et} \) random.)
Part (iv)

1\textsuperscript{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.)

3 \( G(\mathbb{F}_p) = G^{et}(\mathbb{F}_p) = \text{coker}(F|_{\mathcal{M}^{et}} - \text{Id}). \)
Part (iv)

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

1. First fix the \( p \)-corank.
   
   Associated \( p \)-divisible group decomposes as
   
   \[ G = G^m \times G^{et} \times G'^{ll}. \]

2. Fixing the \( p \)-corank fixes the dimension of \( G'^{ll} \)

   (Show that \( G \) random \( \Rightarrow G^{et} \) random.)

3. \( G(\mathbb{F}_p) = G^{et}(\mathbb{F}_p) = \text{coker}(F|_{\text{Met}} - \text{Id}). \)

4. \( F|_{\text{Met}} \) is random in \( \text{GL}_g(\mathbb{Z}_p) \).
Part (v)

\[ P \left( p \nmid \# \text{coker}(F - \text{Id}) \mid_{F^\infty(M \otimes \mathbb{F}_p)} \right) = C_p. \]
Part (v)

\[ P \left( p \mid \# \text{coker}(F - \text{Id}) \mid F^\infty(M \otimes \mathbb{F}_p) \right) = C_p. \]

Basically the same proof as the last part.
Question

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

Data
- \( C \) hyperelliptic, \( p \neq 2 \) – **YES**!
Question

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

Data

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

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

Data

- \( C \) hyperelliptic, \( p \neq 2 \) – **YES**!
- \( C \) plane curve, \( p \neq 2 \) – **YES**!
- \( C \) plane curve, \( p = 2 \) –
Question

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

Data

- \( C \) hyperelliptic, \( p \neq 2 \) – YES!
- \( C \) plane curve, \( p \neq 2 \) – YES!
- \( C \) plane curve, \( p = 2 \) – NO!?!
Theorem (Cais, Ellenberg, ZB)

\[ P(2 \nmid \# \text{Jac}_C(\mathbb{F}_2)) = 0 \] for plane curves of \textbf{odd} degree.
Theorem (Cais, Ellenberg, ZB)

\[ P(2 \nmid \# \text{Jac}_C(F_2)) = 0 \] for plane curves of odd degree.

Proof – theta characteristics.
\[ P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} \]

\[ = \prod_{i=1}^{\infty} (1 - p^{-2i+1})? \]
$a$-number data

**Does**

\[
P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} = \prod_{i=1}^{\infty} (1 - p^{-2i+1})?
\]

**Data**

- $C$ hyperelliptic, $p \neq 2$ -
$a$-number data

**Does**

$$P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1}$$

$$= \prod_{i=1}^{\infty} (1 - p^{-2i+1})?$$

**Data**

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

\[ P(\text{a}(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} \]

\[ = \prod_{i=1}^{\infty} (1 - p^{-2i+1})? \]

Data

- \( C \) hyperelliptic, \( p \neq 2 \) – not quite.

\[ P(\text{a}(\text{Jac}_C(\mathbb{F}_p)) = 0) = 1 - 3^{-1} \]

\((p = 3)\)
Does

$$P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1}$$

$$= \prod_{i=1}^{\infty} (1 - p^{-2i+1})?$$

Data

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

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

$$= (1 - 5^{-1})(1 - 5^{-3}) \quad (p = 3)$$

$$= (1 - 7^{-1})(1 - 7^{-3})(1 - 7^{-5}) \quad (p = 5)$$
a-number data

\[ P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \prod_{i=1}^{\infty} (1 + p^{-i})^{-1} \]

\[ = \prod_{i=1}^{\infty} (1 - p^{-2i+1})? \]

Data

- C hyperelliptic, \( p \neq 2 \) – not quite.

\[ P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = 1 - 3^{-1} \quad (p = 3) \]
\[ = (1 - 5^{-1})(1 - 5^{-3}) \quad (p = 5) \]
\[ = (1 - 7^{-1})(1 - 7^{-3})(1 - 7^{-5}) \quad (p = 7) \]
Rational points on Moduli Spaces

\[ P(a(\text{Jac}_{C_f}(\mathbb{F}_p))) = 0) = \lim_{g \to \infty} \frac{\#H^\text{ord}_g(\mathbb{F}_p)}{\#H_g(\mathbb{F}_p)}. \]
- \( P(a(Jac_{C_f}(\mathbb{F}_p)) = 0) = \lim_{g \to \infty} \frac{\#H^\text{ord}_g(\mathbb{F}_p)}{\#H_g(\mathbb{F}_p)}. \)

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

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

- Our data suggests that $\mathcal{H}_g^{\text{ord}}$ has cohomology that does not arise by pulling back from $\mathcal{H}_g$. 
Rational points on Moduli Spaces

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

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

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

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

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

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

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

- $P(a(\text{Jac}_C(\mathbb{F}_p)) = 0) = \lim_{g \to \infty} \frac{\#M^\text{ord}_g(\mathbb{F}_p)}{\#M_g(\mathbb{F}_p)} = ???$

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

Thank You!