In Section 358 of *Disquisitiones Mathematicae* (1801), Gauss computed

$$\#\{(x, y) \in [0, p-1]^2,\ ax^3 - by^3 \equiv 1 \pmod{p}\}.$$

Nowadays

$$C/\mathbb{F}_p : ax^3 - by^3 - 1 = 0 \subset \mathbb{A}^2 \text{ (better: } ax^3 - by^3 - z^3 = 0 \subset \mathbb{P}^2\text{)}$$

and ask for $\#C(\mathbb{F}_p)$.

Applications: cryptography, error-correcting codes, information on moduli spaces,. . .

Let $k = \mathbb{F}_q$ and C/k be a projective smooth absolutely irreducible curve of genus g over k.

Zeta function:

$$Z(C/k; T) = exp\left(\sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) \cdot \frac{T^n}{n}\right).$$

Weil conjectures (1949): $Z(C/k; T) = \frac{\chi(T)}{(1-T)(1-qT)}$ where

$$\chi(T) = \prod_{i=1}^{g}(1-\alpha_i T)(1-\bar{\alpha}_i T) \in \mathbb{Z}[T]$$

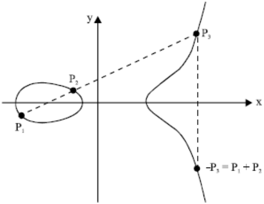
with $|\alpha_i| = \sqrt{q}$.

Ex. : $C/\mathbb{F}_{13} : x^3 - y^3 - z^3 = 0$, $\chi(T) = 13x^2 - 5x + 1$

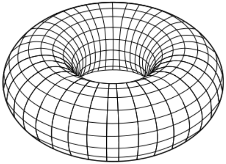
$$\#C(\mathbb{F}_{13}) = 9,\ \#C(\mathbb{F}_{13^2}) = 171, \ldots,$$

$$\#C(\mathbb{F}_{13^{20}}) = 19004963775136363496979$$

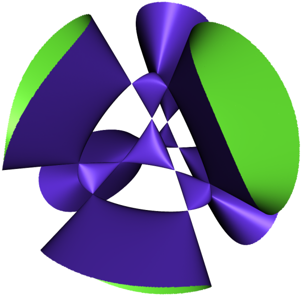
Jac C: an abelian variety A of dimension g over k.



elliptic curve



$\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$



$A/\{\pm 1\}$

Action of the Frobenius on $T_\ell(A) \otimes \mathbb{Q}$: $h_A(T) = T^{2g}\chi(1/T)$.

Existence of a (canonical) principal polarization: an isomorphism $\lambda : A \to A^\vee$ such that $\lambda(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ for an ample line bundle $\mathcal{L}$ on A.

Two ways to understand the concept:

- Over $\mathbb{C}$: $A = V/\Lambda$ then $A^\vee = V^\vee/\Lambda^\vee$ where
  - $V^\vee = \mathrm{Hom}_{\bar{\mathbb{C}}}(V, \mathbb{C})$;
  - $\Lambda^\vee = \{\ell \in V^\vee, \mathrm{Im}\ell(v) \in \mathbb{Z}\ \forall v \in \Lambda\}$.

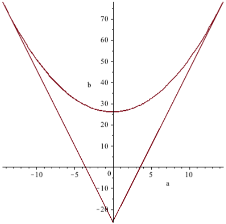
  A p.p is a positive definite hermitian form $H : V \times V \to \mathbb{C}$ (to be continued)
- The case of $A = E^g$ when $\mathrm{End}(E) \simeq \mathbb{Z}$:

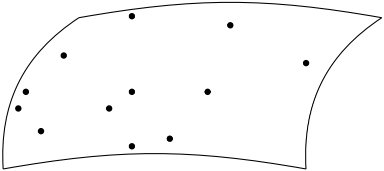
$$\{\text{principal polarizations}\} \longleftrightarrow \{\text{symmetric matrices} > 0 \in \mathrm{GL}_g(\mathbb{Z})\}$$

Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$



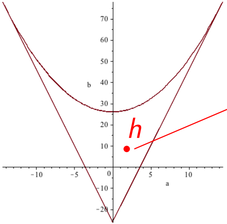


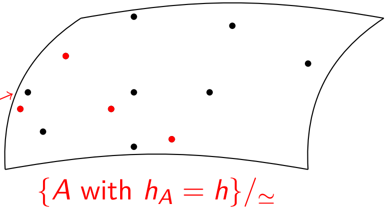
$\{$abelian surfaces A over $\mathbb{F}_q\}/_{\simeq}$

Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$

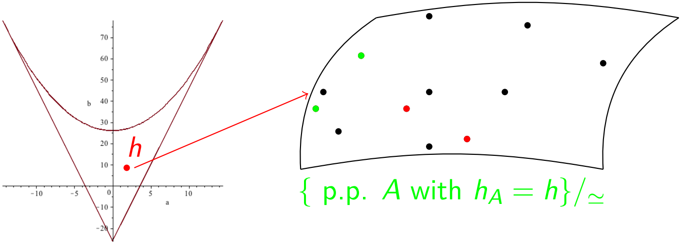




Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$

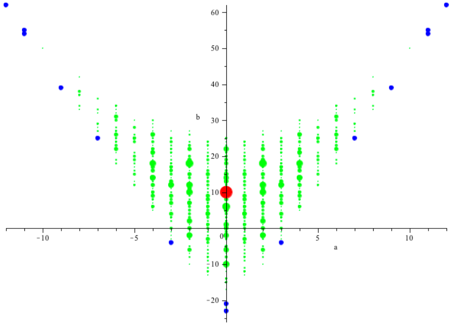


$\{\text{ p.p. } A \text{ with } h_A = h\}/_{\simeq}$

Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

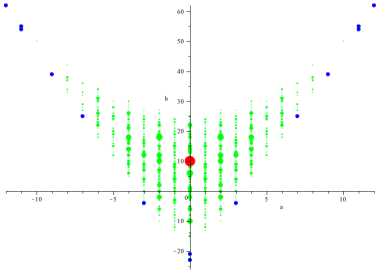
Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$

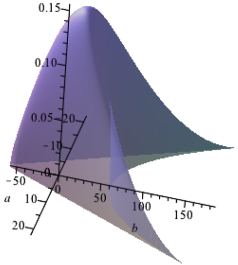


Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$





Honda-Tate (1966-1968):

- gives a complete description of the possible h_A;
- $h_A = h_B$ if and only if $\dim A = \dim B$ and there exists $f : A \to B$ surjective.

Ex. for $g = 2$ over $\mathbb{F}_{13}$: $h_A = T^4 + aT^3 + bT^2 + aqT + q^2$

Definition

An a.v. A over $\mathbb{F}_{p^n}$ of dimension g is ordinary if $h_A \pmod{p}$ is not divisible by p^{g+1}.

Deligne equivalence for ordinary abelian varieties (1969)

- Serre-Tate (1964) prove that A can be lifted over $\mathbb{C}$ to an abelian variety $\widetilde{A}$ *with* $\mathrm{End}(A)$;
- Let $F : \widetilde{A} \to \widetilde{A}$ be the lift of the Frobenius $f : A \to A$;
- $\widetilde{A} = \mathbb{C}^g/\Lambda$ and let $T(A) = \Lambda$.

Theorem

The functor $A \mapsto (T(A), F)$ is an equivalence of categories between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the categories of free $\mathbb{Z}$-modules T of rank $2g$ with an endomorphism F such that

1. *F is semi-simple and its eingenvalues have absolute value $p^{n/2}$;*
2. *half of these roots are p-adic units;*
3. *there exists an endomorphism V of T such that $FV = q$.*

Howe's work on polarizations (1995)

Let $R = \mathbb{Z}[F, V]$ and $K = R \otimes \mathbb{Q}$. Let

$$\Phi = \{\phi : K \to \mathbb{C},\ v_p(\phi(F)) > 0\}.$$

Duality: $(T(A^\vee), F^\vee) = (\mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Z}), \psi \mapsto \psi \circ V)$.

Theorem

A morphism $\lambda : (T, F) \to (T^\vee, F^\vee)$ is a polarization if and only if

- $\lambda \otimes \mathbb{Q}$ *is invertible (i.e. an isogeny);*
- $\lambda = \mathrm{tr}_{K/\mathbb{Q}} \circ S$ *where S is a R-skew-hermitian form, i.e.* $S(t_1, t_2) = -\overline{S(t_2, t_1)}$;
- $\mathrm{Im}(\phi(S(t, t))) \leq 0$ *for all $\phi \in \Phi$ and $t \in T \otimes \mathbb{Q}$.*