

George Boxer g.Boxer@imperial

Question: Given a polynomial

$f \in \mathbb{Z}[X]$  does  $f$  take more square  
or non-square values mod  $p$ ?

$p$  prime

Recall: in  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  there is 0,

$\frac{p-1}{2}$  nonzero squares

$\frac{p-1}{2}$  nonsquares

e.g.  $p=7 \Rightarrow 1, 2, 4 \quad \square$

$3, 5, 6 \quad \not\square$

To quantify question

$a_p := \#\{x \in \mathbb{F}_p \mid f(x) \text{ is } \not\square\}$

$- \#\{x \in \mathbb{F}_p \mid f(x) \text{ is } \square\}$

Heuristic:  $f(x)$  can random elems of  $\mathbb{F}_p$

expect  $a_p \approx 0$

$|a_p| \leq \sqrt{p}$

Not always true:

-  $f = ax + b \rightarrow a_p = 0$

-  $f = x^2 \rightarrow a_p = 1 - p$

$f \in \mathbb{A}^1$  defines a hyperelliptic curve

$$C: y^2 = f(x)$$

(actually take a smooth projective model)

$$\text{Algebraic curve / genus } g = \lfloor \frac{d-1}{2} \rfloor$$
$$d = \deg(f)$$

elliptic curve

$$d = 3, 4 \rightarrow g = 1$$

$$d = 5, 6 \rightarrow g = 2$$

$$\#C(\mathbb{F}_p) \leq 1 + p - a_p$$

Hasse bound:  $|a_p| < 2\sqrt{p}$  (if  $C$  has good reduction mod  $p$ )  
e.g. if  $\text{disc}(f) \not\equiv 0 \pmod{p}$

Question: what can we say about  $a_p$

e.g. 1. is  $\limsup_p \frac{a_p}{\sqrt{p}} = 2g$  (conjecture) yes

2. is  $\limsup_p \frac{a_p}{\sqrt{p}} > 0$

3. are there infinitely many  $p$  w/  $a_p > 0$   
 $(a_p < 0)$

Thm:  $\zeta_2$  (and 2) have positive abscissa  
for  $s=1, 2$

$s=1$  this a consequence of modularity thru  
of Wiles, Taylor-Wiles, BCDT

$s=2$  follows from work of F. Calegari  
T. Gee V. Pilloni on potential  
modularity of genus 2 curves

$s > 2$  wide open in general.

Generating function:

$$L(C, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \prod_{i=1}^{2g} (1 - \alpha_{p,i} p^{-s})^{-1}$$

$\alpha_{p,i}$  are eigenvalues of  $\text{Frob}_p$  on  
 $H^1(C_{\overline{\mathbb{F}}_p}, \overline{\mathbb{Q}}_l)$

$$\#(C(\mathbb{F}_p)) = 1 + p^n - \sum \alpha_{p,i}^n$$

$L(C, s)$  converges absolutely for  $\text{Re}(s) > \frac{3}{2}$

Conjecture (Hösser - Weil)

$L(G, S)$  has a holomorphic continuation to  $\mathbb{C}$  and satisfies functional eq

just knowing that  $L(G, S)$  is holomorphic and nonvanishing for ~~at~~  $\Re(s) = \frac{3}{2}$  implies "prime number theorem" for  $g_p$

$$\sum_{p \leq X} \frac{g_p}{p} = o\left(\frac{X}{\log X}\right)$$

(also need PNT for  $g_r^2$ )

one approach to Hösser-Weil conjecture:  
modularity

EX:  $y^2 + y = x^3 - x^2$

There is an associated modular form

$$F = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \sum a_n q^n$$

if  $q = e^{2\pi i z}$  then this converges

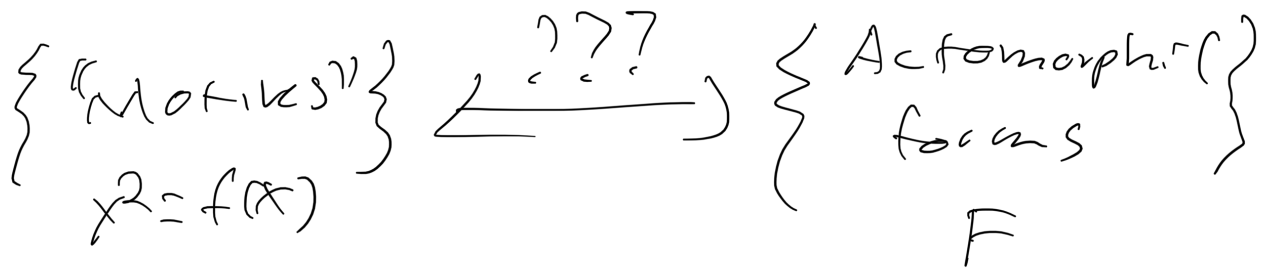
for  $z \in \mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$

lots of functional equations

$$F\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k} F(z)$$

$a, b, c, d \in \mathbb{C}$  and  $ad - bc \neq 0$ ,  $k \in \mathbb{Z}$  (and 11)

Landsberg's correspondence:



$$L(M, S) \longleftrightarrow L(F, S)$$

Weil conjectures  $\implies$

Ramanujan conjecture

Hasse-Weil conjecture  $\longleftarrow$

good analytic properties of L-functions

(analytic continuation)  
field eq, zero free regions

genus 2 curves / abelian surfaces

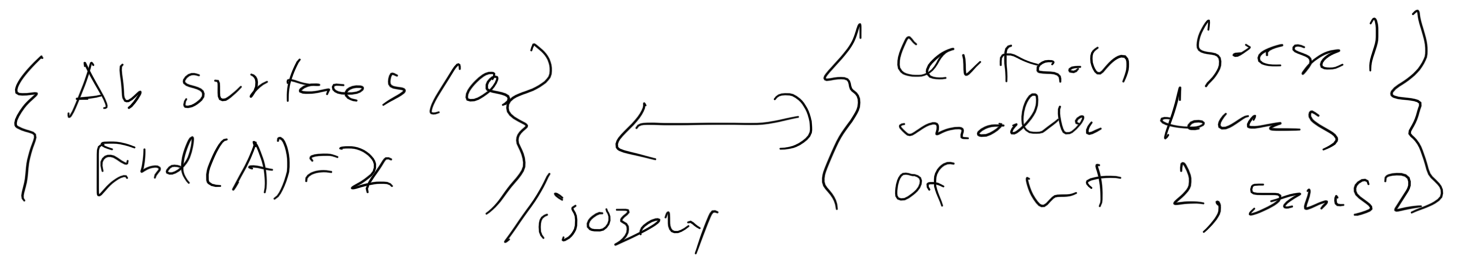
$\mathbb{C}$  genus 2 curves

$\rightarrow$  Jac(C) abelian surface

Modularity of C  $\iff$  Modularity of Jac(C)

$$H^1(C) \cong H^1(\text{Jac}(C))$$

# Conjecture



Very little known is

results of BCP

Thm A Abelian surfaces  $A/\mathbb{Q}$  are potentially modular.

(there is a  $F/\mathbb{Q}$  s.t.  $A_F$  is modular)  
 $\Rightarrow$  good arithmetic newforms of  $L$ -functions)

Thm B  $\exists$  infinitely many simple modular abelian surfaces  $(A) \text{ End}(A) \neq \mathbb{Z}$