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

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

e.g. $p = 7$ ⇒ 1, 2, 4 □

3, 5, 6 ⊠

To quantify question

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

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

Heuristic: $f(x)$ are random elts of $\mathbb{F}_p$

expect $a_p \approx 0$

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

Not always true:

- $f = ax + b \rightsquigarrow a_p = 0$
- $f = x^2 \rightsquigarrow a_p = 1 - p$

f defines a hyperelliptic curve

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

(actually take C smooth projective model)

Algebraic curve / $\mathbb{Q}$ genus $g = \left\lfloor \frac{d-1}{2} \right\rfloor$

$d = \deg(f)$

elliptic curve

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

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

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

Hasse-Weil: $|a_p| \leq 2g\sqrt{p}$ (if C has good reduction mod p e.g. if $p \nmid \mathrm{disc}(f)$)

Question: what can we say about a_p

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

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

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

Thm: $\exists$ [and 2) have positive answer for $g=1,2$

$g=1$ this a consequence of modularity thm of Wiles, Taylor-Wiles, BCDT

$g=2$ follows from work w/ F. Calegari T. Gee V. Pilloni on Potential modularity of genus 2 curves

$g>2$ 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 eigenvals of Frob_p on $H^1(C_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$

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

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

Conjecture (Hasse-Weil)

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

just knowing that $L(E,s)$ is holomorphic and nonvanishing for $\mathrm{Re}(s)=\frac{3}{2}$ implies "prime number theorem" for a_p

$$\sum_{p<X} \frac{a_p}{\sqrt{p}} = o\left(\frac{X}{\log X}\right)$$

(also need PNT for a_p^2)

One approach to Hasse-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 $z \in \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$

lots of functional equations

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

$\forall \; a,b,c,d \in \mathbb{Z}$ $ad-bc=1$, $c \neq 0$ (and k)

Langlands correspondence:

$$\left\{\begin{array}{c}\text{"Motives"} \\ x^2 = f(x)\end{array}\right\} \overset{???}{\longleftrightarrow} \left\{\begin{array}{c}\text{Automorphic} \\ \text{forms} \\ F\end{array}\right\}$$

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

Weil conjectures $\Longrightarrow$ Ramanujan conjecture

Hasse-Weil conjecture $\Longleftarrow$ good analytic properties of L-functions

(analytic continuation, f.e. eq, zero free region)

Genus 2 curves / abelian surfaces

C genus 2 curve

$\rightsquigarrow$ $Jac(C)$ abelian surface

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

$H^1(C) \cong H^1(Jac(C))$

Conjecture

$$\left\{ \begin{array}{l} \text{Ab surfaces } /\mathbb{Q} \\ \text{End}(A) = \mathbb{Z} \end{array} \right\} / \text{isogeny} \longleftrightarrow \left\{ \begin{array}{l} \text{certain Siegel} \\ \text{modular forms} \\ \text{of wt 2, genus 2} \end{array} \right\}$$

Very little known

results of BCDP

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 properties of L-functions)

Thm B If in addition A has real multiplication by $\mathcal{O}$ then A is modular

modular abelian surface $/\mathbb{Q}$ $\text{End}(A_{\bar{\mathbb{Q}}}) = \mathbb{Z}$