How hard is it to be ordinary?

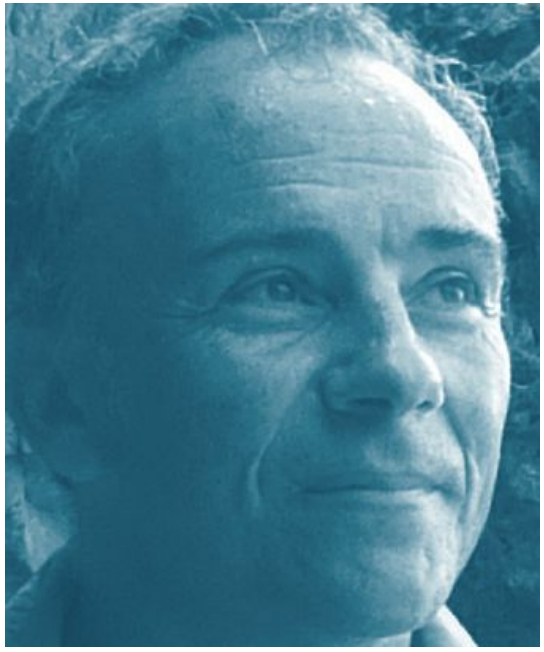
Nicholas M. Katz

Princeton University

Banyuls-sur-Mer, May 29, 2018

It is a great pleasure to be here to honor Francois Loeser.

Here he is.



You are all familiar with the concept of a zero-knowledge proof.

This will be a zero-theorem talk, with emphasis on our zero knowledge about some aspects of curves over finite fields.

Starting with Emil Artin's thesis (1920, published 1923), pursuit of

(function fields of) curves over $\mathbb{F}_q$ as analogues of number fields.

Artin defines Zeta for curves,

$$\mathrm{Zeta}_{C/\mathbb{F}_q}(T) := \prod_{\text{closed points } \mathcal{P}} 1/(1 - T^{degree(\mathcal{P})})$$

$$= \exp(\sum_{n \geq 1} \#C(\mathbb{F}_{q^n}) T^n/n),$$

formulates RH, checks some examples. Nearly 100 years later, still much we don't know.

1931: F.K. Schmidt; correct shape for Zeta of curves over $\mathbb{F}_q$. Denominator is

$$(1 - T)(1 - qT)$$

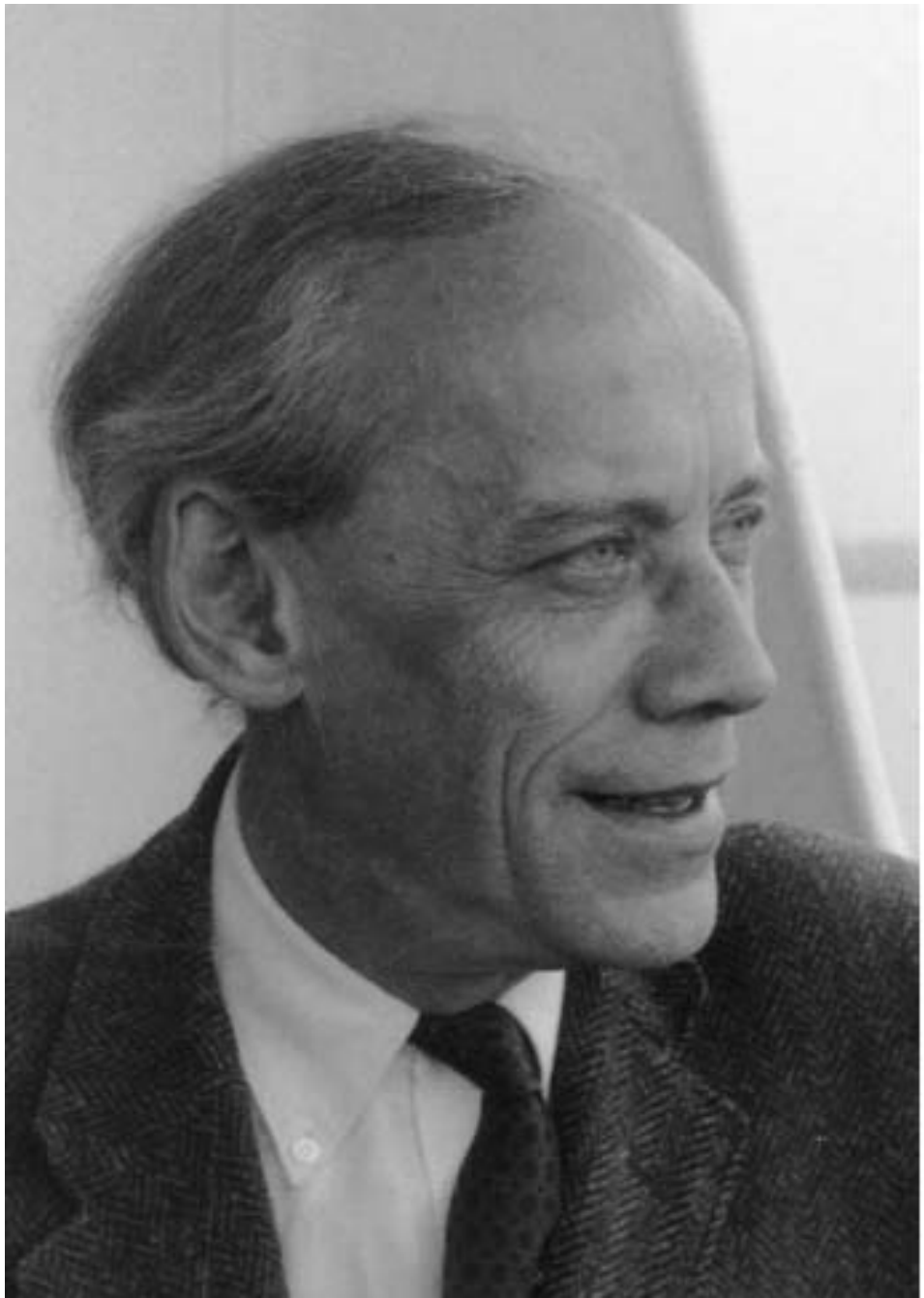
Numerator is 1 for genus 0. For genus $g \geq 1$, numerator is

$$1 - a_1 T + a_2 T^2 + \ldots + q^g T^{2g}$$

with functional equation

$$a_{g+i} = q^i a_{g-i}$$

Artin



F.K. Schmidt

1933,1936; Hasse; proves RH in genus one.

His first proof studies the endomorphism ring of the elliptic curve. When over $\mathbb{F}_q$, an extension of $\mathbb{F}_p$, the numerator of Zeta is

$$1 - aT + qT^2$$

Hasse discovers that whether or not $p|a$ is important, invents “the Hasse invariant" to give a formula for a mod p.

Hasse find that a is prime to p precisely when, over $\overline{\mathbb{F}_q}$, the group of points of order dividing p

has order p (the “ordinary" case). When $p|a$, this group has order 1 (the “supersingular" case).

In odd characteristic, the curve has equation $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ a cubic with nonzero discriminant, and a mod p is

the norm from $\mathbb{F}_q$ to $\mathbb{F}_p$ of the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$.

This last expression is the “Hasse invariant".

Hasse (standing) with Artin

In genus g, where the numerator of Zeta is

$$1 - a_1 T + a_2 T^2 + ... q^g T^{2g}$$

with functional equation

$$a_{g+i} = q^i a_{g-i},$$

it is whether or not $p|a_g$ which is important for us. If a is prime to p, the curve is called “ordinary". If $p|a$, the curve is called “non-ordinary".

The curve is ordinary is if and only if, over $\overline{\mathbb{F}_q}$, the group of points of order dividing p on the Jacobian has order p^g. Otherwise this group has strictly lower order.

Here are the two key formulas for the **reduction mod** p of the numerator $P_{2g}(T)$ of Zeta of $C/\mathbb{F}_q$.

$$= \det(1 - TFrob_{q,arith} | H^1(C, \mathcal{O}_C))$$

This formula, in coherent cohomology, shows that being ordinary is an open condition in the moduli space.

$$= \det(1 - TFrob_{q,geom} | H^1_{et}(C \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{F}_p)).$$

This fomula show that over the open set $\mathcal{M}_g^{\text{ordinary}}/\mathbb{F}_p$, we have a representation of the π_1 of each connected component (**if there any any**) toward $GL(g, \mathbb{F}_p)$.

For example, if we look at a hyperelliptic curve of genus $g \geq 1$ in odd characteristic, of equation

$$y^2 = f(x),$$

$f \in \mathbb{F}_q[x]$ of degree $2g+1$ or $2g+2$ with nonzero discriminant, then we are ordinary if and only if the $g \times g$ matrix whose (i,j) entry is

the coefficient of x^{pi-j} in $f^{(p-1)/2}$

has a **nonzero** determinant.

Not obvious from this that there are any.

In fact, it is known that in each of the cases

$$\mathcal{A}_g/\mathbb{F}_p,\ \mathcal{M}_g/\mathbb{F}_p,\ \mathcal{H}_g/\mathbb{F}_p$$

of the moduli of principally polarized abelian varieties of dimension g, or of genus g curves, or of genus g hyperelliptic curves, (in each case with a suitable rigidification, e.g. a basis of H^1_{DR} if p is odd), the ordinary locus is open, dense, and geometrically irreducible, and the corresponding homomorphism

$$\pi_1 \to GL(g, \mathbb{F}_p)$$

is surjective.

These results are due to Faltings-Chai, Ekedahl, and Achter-Pries respectively.

Where is ℓ-adic monodromy in our story, for ℓ a prime, $\ell \neq p$?

In all three cases considered above, we know that if we look at the H^1 along the fibres with $\mathbb{Q}_\ell$ coefficients (and half a Tate twist, say using an ℓ mod which p is a square), we have a representation

$$\pi_1 \to Sp(2g, \mathbb{Q}_\ell)$$

whose image is Zariski dense.

Moreover, there are lots of one-parameter families of hyperelliptic curves of any genus $g \geq 1$ whose monodromy representations have Zariski dense image in $Sp(2g, \mathbb{Q}_\ell)$.

For example, in odd characteristic p,

take $n = 2g + 1$ or $n = 2g + 2$,

$$y^2 = x^n - nx - t$$

over (an open dense set of) the t-line, in any characteristic p not dividing $n(n-1)$.
or take

$$y^2 = f(x)(x - t)$$

with f any polynomial of degree $n = 2g$ or $n = 2g + 1$ and nonvanishing discriminant, again over (an open dense set of) t-line

One might hope that in any one-parameter family of genus g curves over a (geometrically connected, smooth open) base curve $S/\mathbb{F}_q$,

$$\mathcal{C} \to S/\mathbb{F}_q,$$

if the ℓ-adic monodromy has image which is Zariski dense in $Sp(2g)$, then we have both

(1) the ordinary locus S^{ordinary} is nonempty, AND

(2) $\pi_1(S^{\text{ordinary}})$ maps onto $GL(g, \mathbb{F}_p)$

SADLY, BOTH CAN FAIL

Computer experiments suggest that for the

$$y^2 = f(x)(x - t)$$

families, (1) will be okay in characteristic $p \geq 2g + 2$, but that it will fail in some lower characteristics.

On the other hand, for the

$$y^2 = x^n - nx - t$$

families, (1) can fail unless $p \geq n^2 \approx 4g^2$.

For $n = 21$, (1) fails for $p = 359$.
For $n = 31$, (1) fails for $p = 839$.
For $n = 41$, (1) fails for $p = 1439$.
For $n = 51$, (1) fails for $p = 2399$.

Computer experiments indicate that

for $n = 65$, (1) seems to fail for $p = 3967$.
for $n = 81$, (1) seems to fail for $p = 6079$.
for $n = 105$, (1) seems to fail for $p = 10607$.
for $n = 125$, (1) seems to fail for $p = 14879$.

WHY? What (if any) is the “meaning" of $p \geq n^2$?

Let me end with two conjectures.

Conjecture 1

Start with a one parameter family "over $\mathbb{Z}$" of genus g curves $\mathcal{C} \to S/\mathbb{Z}[/N]$, whose topological monodromy over $S(\mathbb{C})^{an}$ is a subgroup of $Sp(2g, \mathbb{Z})$ of finite index (e.g. any of the families we wrote down). Then in characteristic p sufficiently large, both hopes (generically ordinary, and onto $GL(g, \mathbb{F}_p)$) hold.

This is okay and easy for $g = 1$. For $g = 2$, the generically ordinary is okay, by an argument of Will Sawin. For $g \geq 3$, it is completely open (though it can be checked in examples for p up to 1000 and $g = 3$).

Conjecture 2

Suppose we start with a single curve $C/\mathbb{Z}[1/N]$ whose ℓ-adic representation (for one, or equivalently for every ℓ) has open image in $GSp(2g, \mathbb{Q}_\ell)$. Then $C \otimes \mathbb{F}_p$ is ordinary for a set of primes of density one, AND, if $g \geq 2$, we have an estimate

$$\#\{\text{non} - \text{ordinary } p \leq X\} = O(\log\log(X))$$

Thanks to Zarhin, we know that for C a hyperelliptic curve $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ of degree $n = 2g + 1 \text{or } 2g + 2$ and having galois group over $\mathbb{Q}$ either S_n or A_n, its ℓ-adic representation does indeed have open image in $GSp(2g, \mathbb{Q}_\ell)$.

One knows (Schur) that the truncated exponential polynomials

$$f_n(x) := \sum_{j=0}^{n} x^j/j!$$

have galois group S_n unless $4|n$, in which case the galois group is A_n. One also knows (Osada) that Selmer's polynomial

$$x^n - x - 1$$

has galois group S_n. So there are plenty of explicit curves to try.

The first part of this conjecture, ordinary in density one, was proved by Sawin for $g = 2$, but is completely open for $g \geq 3$.

The loglog part of the conjecture is based on the idea that in each characterstic p, the middle coefficient a_g is sufficiently "random" that the chance of its being divisible by p is $1/p$.

MUCH REMAINS TO BE DONE.