

Cohomology and the number of points

(joint work with Bas Edixhoven)

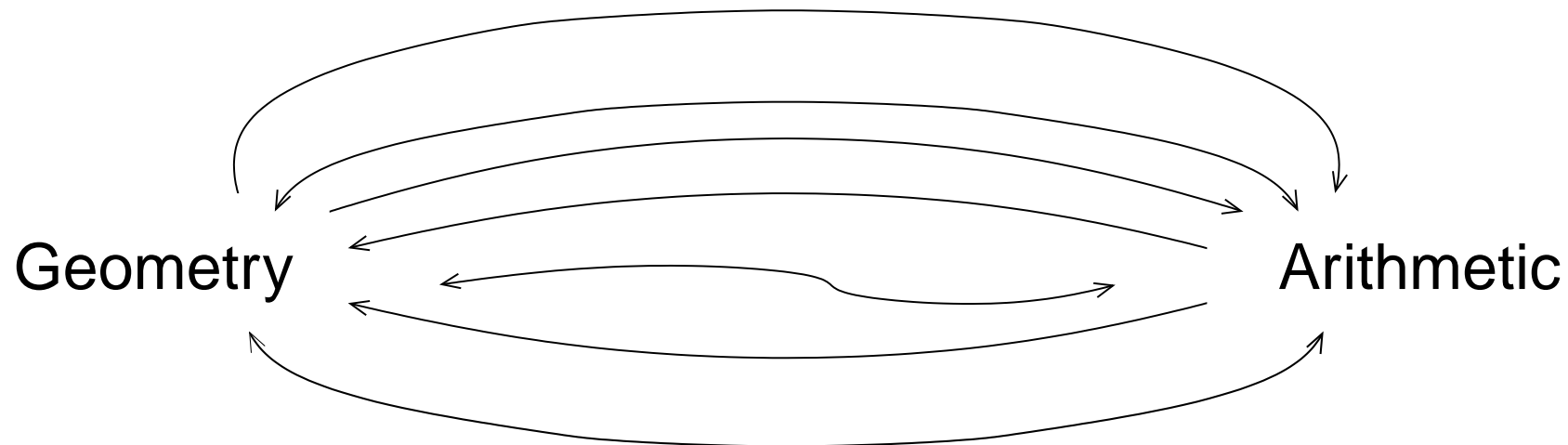
Theo van den Bogaart

bogaart@math.leidenuniv.nl



Leiden University

Introduction



Introduction

Geometry

Arithmetic



Introduction

Geometry

Arithmetic

Cohomology



How to use cohomology? (1/3)

X algebraic curve of genus g defined over \mathbf{F}_p

How to use cohomology? (1/3)

X algebraic curve of genus g defined over \mathbf{F}_p
for example:

$$X = \{(x, y) \in (\overline{\mathbf{F}}_p)^2 \mid y^2 = f(x)\} \cup \{\infty\}$$

where $f(x)$ is a polynomial with \mathbf{F}_p coefficients
(there are conditions on $f(x)$...)

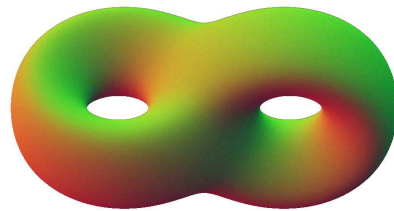
How to use cohomology? (1/3)

X algebraic curve of genus g defined over \mathbf{F}_p
for example:

$$X = \{(x, y) \in (\overline{\mathbf{F}}_p)^2 \mid y^2 = f(x)\} \cup \{\infty\}$$

where $f(x)$ is a polynomial with \mathbf{F}_p coefficients
(there are conditions on $f(x)\dots$)

Topologically:



genus = number of holes

How to use cohomology? (1/3)

X algebraic curve of genus g defined over \mathbf{F}_p
for example:

$$X = \{(x, y) \in (\overline{\mathbf{F}}_p)^2 \mid y^2 = f(x)\} \cup \{\infty\}$$

where $f(x)$ is a polynomial with \mathbf{F}_p coefficients
(there are conditions on $f(x)\dots$)

How to use cohomology? (2/3)

X algebraic curve of genus g defined over \mathbf{F}_p

Theorem (Hasse, Weil): There exist $\lambda_1, \dots, \lambda_{2g} \in \mathbf{C}$ such that for all $n \geq 1$:

$$\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \dots + \lambda_{2g}^n) + p^n$$

How to use cohomology? (2/3)

X algebraic curve of genus g defined over \mathbf{F}_p

Theorem (Hasse, Weil): There exist $\lambda_1, \dots, \lambda_{2g} \in \mathbf{C}$ such that for all $n \geq 1$:

$$\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \dots + \lambda_{2g}^n) + p^n$$

PROOF: Nice things about characteristic p :

- (i) raising to the p -th power defines an automorphism of X , this is called the **Frobenius** map F ;
- (ii) $X(\mathbf{F}_{p^n})$ is the set of fixed points of F^n .

How to use cohomology? (2/3)

X algebraic curve of genus g defined over \mathbf{F}_p

Theorem (Hasse, Weil): There exist $\lambda_1, \dots, \lambda_{2g} \in \mathbf{C}$ such that for all $n \geq 1$:

$$\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \dots + \lambda_{2g}^n) + p^n$$

PROOF: Nice things about characteristic p :

- (i) raising to the p -th power defines an automorphism of X , this is called the **Frobenius** map F ;
- (ii) $X(\mathbf{F}_{p^n})$ is the set of fixed points of F^n .

Now we need **cohomology**

Cohomology

Cohomology gives us for each integer i a complex vector space $H^i(X)$.

Useful properties:

- functoriality:
the frobenius morphism induces a linear map

$$\text{Frob}: H^i(X) \longrightarrow H^i(X)$$

- $H^i(X) = 0$ for i outside $[0, 2 \dim(X)]$
- etc.

How to use cohomology? (3/3)

Claim: $\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + p^n$

PROOF (cont.): Use the **fixed point formula**: $\#X(\mathbf{F}_{p^n}) =$

$$\mathrm{Tr}(\mathrm{Frob}^n | H^0(X)) - \mathrm{Tr}(\mathrm{Frob}^n | H^1(X)) + \mathrm{Tr}(\mathrm{Frob}^n | H^2(X))$$

How to use cohomology? (3/3)

Claim: $\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + p^n$

PROOF (cont.): Use the **fixed point formula**: $\#X(\mathbf{F}_{p^n}) =$

$$\mathrm{Tr}(\mathrm{Frob}^n | H^0(X)) - \mathrm{Tr}(\mathrm{Frob}^n | H^1(X)) + \mathrm{Tr}(\mathrm{Frob}^n | H^2(X))$$

- H^0 and H^2 are one-dimensional
(one = number of connected components of X)
- $\mathrm{Tr}(\mathrm{Frob}^n | H^0(X)) = 1$
- $\mathrm{Tr}(\mathrm{Frob}^n | H^2(X)) = p^n$
- H^1 has dimension $2g$

How to use cohomology? (3/3)

Claim: $\#X(\mathbf{F}_{p^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + p^n$

PROOF (cont.): Use the **fixed point formula**: $\#X(\mathbf{F}_{p^n}) =$

$$\mathrm{Tr}(\mathrm{Frob}^n | H^0(X)) - \mathrm{Tr}(\mathrm{Frob}^n | H^1(X)) + \mathrm{Tr}(\mathrm{Frob}^n | H^2(X))$$

- H^0 and H^2 are one-dimensional
(one = number of connected components of X)

- $\mathrm{Tr}(\mathrm{Frob}^n | H^0(X)) = 1$

- $\mathrm{Tr}(\mathrm{Frob}^n | H^2(X)) = p^n$

- H^1 has dimension $2g$

Now write $\mathrm{Frob} | H^1(X) = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_{2g} \end{pmatrix}$.

□

Frobenius

The $\lambda_1, \dots, \lambda_{2g}$ appearing in the theorem are the zeroes of the characteristic polynomial of Frobenius.

Frobenius

The $\lambda_1, \dots, \lambda_{2g}$ appearing in the theorem are the zeroes of the characteristic polynomial of Frobenius.

Task:

Given a prime p and a hyperelliptic curve of genus g over \mathbb{F}_p , determine the characteristic polynomial of Frobenius.

There is no algorithm known which does this in time polynomial in $\log p$ and g .

Frobenius

The $\lambda_1, \dots, \lambda_{2g}$ appearing in the theorem are the zeroes of the characteristic polynomial of Frobenius.

Task:

Given a prime p and a hyperelliptic curve of genus g over \mathbb{F}_p , determine the characteristic polynomial of Frobenius.

There is no algorithm known which does this in time polynomial in $\log p$ and g .

Is it possible to determine these eigenvalues from certain ‘arithmetic information’?

The Texel problem

Situation:

X a nice (=proper and smooth) variety defined over \mathbf{Z}

There exists a polynomial P with \mathbf{Q} coefficients, such that for all primes p and all $n \geq 1$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n).$$

Question:

What can we say about the cohomology of X ?

The Texel problem

Situation:

X a nice (=proper and smooth) variety defined over \mathbf{Z}

There exists a polynomial P with \mathbf{Q} coefficients, such that for all primes p and all $n \geq 1$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n).$$

Question:

What can we say about the cohomology of X ?

Well, start with the fixed point formula:

$$P(p^n) = \#X(\mathbf{F}_{p^n}) = \sum_i (-1)^i \operatorname{Tr}(\operatorname{Frob}_p^n | H^i(X)) \quad \dots$$

Theorem

X a proper, smooth variety defined over \mathbf{Z}

$P(t) = d_0 + d_1t + \cdots + d_rt^r$ a polynomial with \mathbf{Q} coefficients

Assume that for almost all primes p and all $n \gg 0$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n)$$

Then

Theorem

X a proper, smooth variety defined over \mathbf{Z}

$P(t) = d_0 + d_1t + \cdots + d_r t^r$ a polynomial with \mathbf{Q} coefficients

Assume that for almost all primes p and all $n \gg 0$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n)$$

Then

- $H^i(X) = 0$ if i is odd or outside $[0, 2 \dim X]$
- in the remaining cases $H^i(X)$ has dimension $d_{i/2}$ and $\text{Frob}_p = p^{i/2} \cdot \text{id}$
- to be precise: $H^i(X(\mathbf{C}), \mathbf{Q}) = \mathbf{Q}(-i/2)^{d_{i/2}}$ and the analogous result holds for the étale cohomology of $X_{\overline{\mathbf{Q}}}$

Theorem

X a proper, smooth variety defined over \mathbf{Z}

$P(t) = d_0 + d_1t + \cdots + d_r t^r$ a polynomial with \mathbf{Q} coefficients

Assume that for almost all primes p and all $n \gg 0$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n)$$

Then

- every closed C^∞ -differential s -forms on X is exact if s is odd
- the geometric genus of X is 0
- there are no global holomorphic s -forms on X for $s \geq 1$

Theorem

X a proper, smooth variety defined over \mathbf{Z}

$P(t) = d_0 + d_1t + \cdots + d_rt^r$ a polynomial with \mathbf{Q} coefficients

Assume that for almost all primes p and all $n \gg 0$:

$$\#X(\mathbf{F}_{p^n}) = P(p^n)$$

Then

- the degree n of $P(t)$ is equal to the dimension of X
- $P(t)$ is monic
- the coefficients of $P(t)$ are symmetric, i.e. $d_i = d_{r-i}$
- $\#X(\mathbf{F}_{p^n}) = P(p^n)$ for **all** p and **all** $n \geq 1$

Examples

Projective space,

Examples

Projective space, Grassmanians,

Examples

Projective space, Grassmanians, **flag varieties**

Examples

Projective space, Grassmanians, **flag varieties**

$B_n \subset GL_n$ Borel subgroup ('upper triangular matrices')

$$\begin{aligned} \#(GL_n/B_n)(\mathbf{F}_q) &= \frac{\#GL_n(\mathbf{F}_q)}{\#B_n(\mathbf{F}_q)} && \text{(Lang)} \\ &= \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{(q-1)^n q^{n(n-1)/2}} \end{aligned}$$

is polynomial in q

So we obtain information about the cohomology and geometry of the flag variety $Fl(n, \mathbf{C}) = (GL_n/B)(\mathbf{C})$.

Back to Texel

$\mathcal{M}_{g,n}$ the compactified moduli space of curves of genus g with n marked points

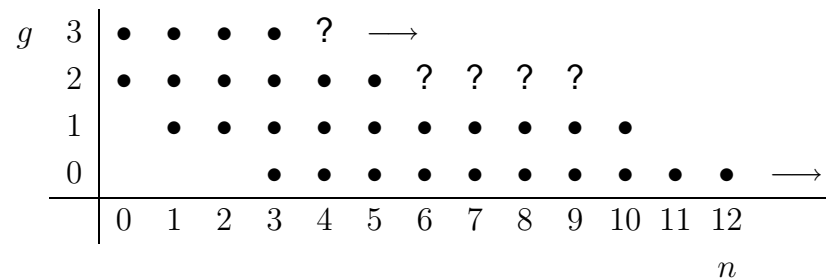
Studied by *Jonas Bergström* and *Orsola Tommasi*

Back to Texel

$\mathcal{M}_{g,n}$ the compactified moduli space of curves of genus g with n marked points

Studied by *Jonas Bergström* and *Orsola Tommasi*

$\#(\mathcal{M}_{g,n})(\mathbf{F}_q)$ is a polynomial in q if (g, n) is one of the following points:



One problem:

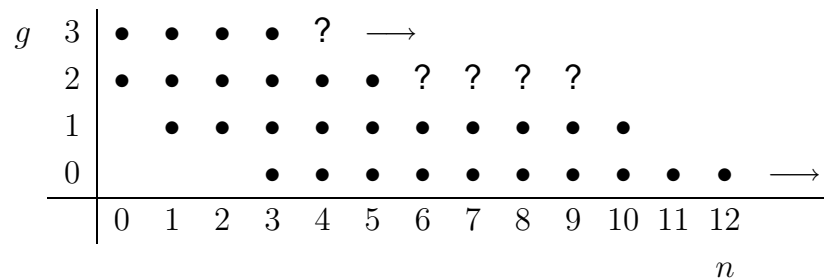
$\mathcal{M}_{g,n}$ is not a smooth variety...

Back to Texel

$\mathcal{M}_{g,n}$ the compactified moduli space of curves of genus g with n marked points

Studied by *Jonas Bergström* and *Orsola Tommasi*

$\#(\mathcal{M}_{g,n})(\mathbf{F}_q)$ is a polynomial in q if (g, n) is one of the following points:



One problem:

$\mathcal{M}_{g,n}$ is not a smooth variety... But it is a smooth **stack**.

Related stuff

- *Mark Kisin* and *Gus Lehrer* (2005) study the non-compact case. This gives application to reductive groups.
- Applications in mathematical physics to mirror symmetry. See for example work of *Tetsushi Ito* (2003).

The End

Thank you