

R. Gerkmann

Counting Points on Varieties using p -adic Cohomology

February 14th, winter term 2001/02, Essen

Notation:

- p a prime number (even or odd)
- q a power of p , $q = p^a$ with $a \in \mathbb{N}$
- variety = integral separated scheme over k algebraically closed
(in most cases affine or projective)
- variety over \mathbb{F}_q = variety of the form $V \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$
where V separated and of finite type over \mathbb{F}_q
- curve (over \mathbb{F}_q) = one-dimensional variety (over \mathbb{F}_q)
- $V(K)$ set of K -rational points on V , where
 $K \mid \mathbb{F}_q$ is a field extension (finite or infinite)

Point Counting and Cryptography

$(G, *)$ finite, abelian group

enumeration of G = injective map $\varphi : G \longrightarrow \mathbb{N}_0$

discrete logarithm problem (DLP) of (G, φ) :

given $a, b \in \varphi(G)$,

compute $p \in \mathbb{N}_0$ with $\alpha^p = \beta$, where $\varphi(\alpha) = a$, $\varphi(\beta) = b$ (if it exists)

- The complexity of $\text{DLP}(G, \varphi)$ depends on *both* G and φ .
- Given $a, b \in \varphi(G)$, computation of

$$a \oplus b \quad := \quad \varphi(\varphi^{-1}(a) * \varphi^{-1}(b))$$

should be easy.

E/\mathbb{F}_p elliptic curve, smooth and projective, $p \neq 2, 3$,

with equation $Y^2 = X^3 + aX + b$.

$$E(\mathbb{F}_p) \quad = \quad \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

define numeration von $E(\mathbb{F}_p)$:

- find an injective map $\psi : \mathbb{F}_p \times \mathbb{F}_p \longrightarrow \mathbb{N}$
- define $\varphi : E(K) \longrightarrow \mathbb{N}_0$, $(x, y) \mapsto \psi(x, y)$, $\infty \mapsto 0$

The problem $\text{DLP}(E(\mathbb{F}_p), \varphi)$ is hard only if

$\# E(\mathbb{F}_p)$ is divided by a large prime

\Rightarrow need to compute $\# E(\mathbb{F}_p)$ and its factorization

(or construct E so that $\# E(\mathbb{F}_p)$ is known)

counting on higher-dimensional varieties:

C/\mathbb{F}_q curve with genus $g > 1$

$\text{Pic}(C)$ divisor class group of C

$\text{Pic}^0(C)$ divisor classes of degree 0

$\text{Pic}(C)_{\mathbb{F}_q}$ divisor classes invariant under $\sigma \in \text{Gal}(\overline{\mathbb{F}_q} | \mathbb{F}_q)$

Theorem: There is an abelian variety $\text{Jac}(C)$ so that

$$\text{Jac}(C)(\overline{\mathbb{F}_q}) \cong \text{Pic}^0(C) \quad \text{and} \quad \text{Jac}(C)(\mathbb{F}_q) \cong \text{Pic}^0(C)_{\mathbb{F}_q}$$

as abelian groups.

Theory of point counting: The “Weil conjectures”

X/\mathbb{F}_q smooth projective variety, $\dim X = d$

zeta function of X

$$Z(X, T) = \exp\left(\sum_{m \geq 1} N_m \frac{T^m}{m}\right), \quad N_m = \# X(\mathbb{F}_{q^m})$$

Properties of the function $Z(X, T)$:

- *Rationality:*

$$Z(X, T) = \prod_{i=0}^{2d} P_i(T)^{(-1)^{i+1}}, \quad P_i(T) \in \mathbb{Z}(T)$$

where $P_0(T) = 1 - T$ and $P_{2d}(T) = 1 - q^d T$.

- *Functional equation:* $Z(X, q^{-1}T^{-1}) = \pm q^{d\chi/2} \cdot t^\chi \cdot Z(X, T)$, where χ is the Euler-Poincaré characteristic of X
- *Riemann hypothesis:* $P_i(T) = \prod_{j=1}^{\beta_i} (1 - \alpha_{i,j}T)$ where $\alpha_{i,j}$ are algebraic integers with $|\alpha_{i,j}| = q^{i/2}$ for all archimedean valuations

If the numbers $\alpha_{i,j}$ are known, one can easily compute $\# X(\mathbb{F}_{q^m})$

for all $m \in \mathbb{N}$!

The Riemann “hypothesis” gives an upper bound on $\# X(\mathbb{F}_{q^m})$ (the so-called Hasse-Weil bound).

Weil conjectures and sheaf cohomology

On every variety X , there is an endomorphism $\text{Frob} : X \longrightarrow X$.

Frobenius endomorphism on $X = \text{Spec } \mathbb{F}_q[X_1, \dots, X_n]/(f_1, \dots, f_r)$

$$(x_1, \dots, x_n) \mapsto (x_1^q, \dots, x_n^q), \quad X_i \mapsto X_i^q \quad 1 \leq i \leq n$$

(homeomorphism on the topological space, but *no automorphism* of X in general)

main idea on the proof of Weil conjectures:

The polynomials $P_i(T)$ are characteristic polynomials of “the Frobenius” on some vector spaces attached to X .

first idea: take cohomology of Zariski sheaf \mathcal{O}_X on X

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{F}_1 \longrightarrow \mathcal{F}_2 \longrightarrow \mathcal{F}_3 \longrightarrow \dots \quad (\text{injective resolution})$$

$$0 \longrightarrow \Gamma(X, \mathcal{O}_X) \xrightarrow{d_0} \Gamma(X, \mathcal{F}_1) \xrightarrow{d_1} \Gamma(X, \mathcal{F}_2) \xrightarrow{d_2} \Gamma(X, \mathcal{F}_3) \longrightarrow \dots$$

$$H_{zar}^i(X, \mathcal{O}_X) \quad := \quad \ker(d_i)/\text{im}(d_{i-1}) \quad \text{for all } i \in \mathbb{N}_0$$

problem: $H_{zar}^i(X, \mathcal{O}_X) = 0$ for $d < i \leq 2d$

$\Rightarrow H_{zar}^i$ does not give the “right” betti numbers $\beta_i = \dim H^i(X)$.

solution:

- search for another topology (Zariski topology is too “coarse”)
- generalize to Grothendieck topologies (“sites”)

A site \mathcal{S} consists of

- a category \mathcal{C}
- for each $U \in \mathcal{C}$, a set $\text{cov}(U)$ of families $\{U_i \longrightarrow U\}_{i \in I}$ of morphisms (“coverings”)

so that three conditions are satisfied:

- (a) $\{\text{id}_U\} \in \text{cov}(U)$
- (b) “transitivity” of cov
- (c) “compatibility” of cov with morphisms $U \longrightarrow V$

sheaf on \mathcal{S} = contravariant functor $\mathcal{F} : \mathcal{C} \longrightarrow \text{Ens}$ so that

$$\mathcal{F}(U) \longrightarrow \prod_{i \in I} \mathcal{F}(U_i) \rightrightarrows \prod_{(i,j) \in I \times I} \mathcal{F}(U_i \times_U U_j)$$

for all $\{U_i \longrightarrow U\}_{i \in I} \in \text{cov}(U)$

first example: Zariski topology $\text{Zar}(X/\mathbb{F}_q)$ on X/\mathbb{F}_q

- objects of \mathcal{C} = open subsets $U \subseteq X$
- morphisms = inclusions $U \hookrightarrow V$
- coverings of U = families $\{U_i \hookrightarrow U\}$ with $U = \bigcup_{i \in I} U_i$

second example: étale topology $\text{Et}(X/\mathbb{F}_q)$ on X/\mathbb{F}_q

U, V smooth varieties over \mathbb{F}_q

morphism $\varphi : U \longrightarrow V$ étale $:\Leftrightarrow$ induces isomorphisms

$$T_P(U) \cong T_{\varphi(P)}(V)$$

for all (closed) points $P \in U$

- objects of \mathcal{C} = étale morphisms $U \longrightarrow X$
- morphisms = commutative diagrams

$$\begin{array}{ccc} U & \longrightarrow & V \\ \downarrow & & \downarrow \\ X & = & X \end{array}$$

- coverings of U = families $\{\varphi_i : U_i \longrightarrow U\}_{i \in I}$ with $U = \bigcup_{i \in I} \varphi_i(U_i)$

Let $l \neq p$ be a prime.

definition of l -adic cohomology:

$$\mathbb{Z}/l^n\mathbb{Z} \quad := \quad \text{constant sheaf } \mathbb{Z}/l^n\mathbb{Z} \text{ on } \text{Et}(X/S)$$

$$H_{et}^i(X, \mathbb{Z}_l) \quad := \quad \lim_{n \in \mathbb{N}} H_{et}^i(X, \mathbb{Z}/l^n\mathbb{Z})$$

$$H_l^i(X/\mathbb{F}_q) \quad := \quad H_{et}^i(X, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

- Frobenius on X induces linear endomorphism F_i on the \mathbb{Q}_l -vector space $H_l^i(X/\mathbb{F}_q)$ for $0 \leq i \leq 2d$
- $P_i(T)$ (see above) appears as characteristic polynomial of F on $H_l^i(X/\mathbb{F}_q)$

$H_l^i(X/\mathbb{F}_q)$ hard to compute (no upper bounds of $\dim H_l^i(X/\mathbb{F}_q)$ known in general), but one knows

$$X \text{ abelian variety (e.g., an elliptic curve)} \quad \Rightarrow \quad H_l^1(X/\mathbb{F}_q) \cong T_l(X)$$

as \mathbb{Z}_l -modules, where

$$T_l(X) := \lim_{n \in \mathbb{N}} X[l^n] \quad l\text{-adic Tate module of } X$$

and $X[l^n] := l^n$ -torsion points of $X \Rightarrow$ Schoof algorithm (see below)

Let S be a PD-scheme (e.g., $S = \text{Spec } W(\mathbb{F}_q)$)

and U, T schemes over S

nilpotent immersion := closed S -immersion $U \hookrightarrow T$ given by a nilpotent ideal sheaf \mathcal{J} on T

third example: crystalline topology $\text{Cris}(X/S)$ on X/S

- objects = nilpotent immersions $U \hookrightarrow V$, where $U \subseteq X$ Zariski-open
- morphisms = commutative diagrams

$$\begin{array}{ccc} U & \hookrightarrow & T \\ \downarrow & & \downarrow \\ U' & \hookrightarrow & T' \end{array}$$

where $U \longrightarrow U'$ is an open immersion

(may identify a morphism with $T \longrightarrow T'$)

- coverings = families $\{\varphi_i : T_i \longrightarrow T\}_{i \in I}$ with $T = \bigcup_{i \in I} \varphi_i(T_i)$

problem in defining cohomology:

- $\text{Cris}(X/S)$ has no final object in general
- take final object of the topos $(X/S)_{\text{cris}}$ instead

definition of p -adic cohomology:

Every variety V over \mathbb{F}_q is a scheme over $W_n(\mathbb{F}_q)$ for all $n \geq 1$.

Every commutative diagram with $m \leq n$

$$\begin{array}{ccc} X & = & X \\ \downarrow & & \downarrow \\ S_m & \rightarrow & S_n \end{array}$$

where $S_n = \text{Spec } W_n(\mathbb{F}_q)$ induces a homomorphism

$$i_{mn} : H^i((X/S_n)_{\text{cris}}, \mathcal{O}_{X_{\text{cris}}}) \longrightarrow H^i((X/S_m)_{\text{cris}}, \mathcal{O}_{X_{\text{cris}}})$$

define $H_p^i(X/\mathbb{F}_q) = \lim_{n \in \mathbb{N}} H^i((X/S_n)_{\text{cris}}, \mathcal{O}_{X_{\text{cris}}})$

properties of $H_p^i(X/\mathbb{F}_q)$ (if X is smooth and projective)

- finitely generated $W(\mathbb{F}_q)$ -module
- polynomials $P_i(T)$ (see above) are given by the characteristic polynomial of the “Frobenius“ on $H_p^i(X/\mathbb{F}_q)$
- Y/S smooth lifting of X , where $S = \text{Spec } W(\mathbb{F}_q)$, then

$$H_p^i(X/\mathbb{F}_q) \cong H_{DR}^i(Y/S) := \mathbb{H}^i(Y, \Omega_{Y/S}^\bullet)$$

The last statement leads to an interpretation of $H_p^i(X/\mathbb{F}_q)$ in terms of *rigid analytic spaces* (see below).

F -crystal structure on $H_p^i(X/\mathbb{F}_q)/\text{tors}$

$W = W(\mathbb{F}_q)$, $K =$ quotient field of W

$\sigma : W \longrightarrow W$ (small) Frobenius endomorphism of W

F -crystal = pair (M, ϕ) consisting of

- (i) a free W -module M
- (ii) an injective, additive, σ -linear map
(means that $\phi(am) = \sigma(a)\phi(m)$ for all $a \in W$, $m \in M$)

Examples:

- $H_p^i(X/\mathbb{F}_q)/\text{tors}$ is an F -crystal for all X projective and smooth.
- Let $\alpha = r/s \in \mathbb{Q}_+$ with $r \in \mathbb{N}_0$, $s \in \mathbb{N}$. Set

$$M_\alpha := W_\alpha[T]/(T^s - p^r)$$

where $W_\alpha[T]$ is the ring of σ -commutative polynomials.

Define ϕ by $m \mapsto Tm$. Then (M_α, ϕ) is an F -crystal.

Theorem: Every F -crystal M is isogenous (isomorphic after tensorization with K) to a finite, direct sum of M_α .

$$M \sim \bigoplus_{\alpha \in \mathbb{Q}_+} M_\alpha^{n_\alpha}$$

- One can attach to each F -crystal M a piecewise linear function

$$\text{Nw}_M : [0, \text{rg}_W(M)] \longrightarrow \mathbb{R}$$

(called Newton polygon) where the α with $n_\alpha \neq 0$ appear as slopes.

- All possible Newton polygons of $H_p^i(X)$, X elliptic curve or abelian variety, are explicitly known.
- If the Newton-Polygon is known, one can use it together with the Hasse-Weil bound to reduce the computation of the $P_i(T)$ to the computation in a

free $W_n(\mathbb{F}_q)$ -module of finite rank

(the bigger the “slopes“, the smaller is n)

disadvantages of crystalline cohomology:

- restriction to smooth and projective curves
- definition yields no method of construction
- isomorphism $H_p^i(X/\mathbb{F}_q) \cong H_{DR}^i(X/S)$ does not help much, because
 - (i) module given in terms of hyper-cohomology (hard to compute)
 - (ii) Although smooth projective X/\mathbb{F}_q can be lifted to Y/S in many cases,

the Frobenius can *almost never* be lifted

Rigid cohomology

K non-archimedean valued, complete field, $\text{char}(K) = 0$

\mathcal{V} its ring of integers, \mathfrak{m} maximal ideal, $\mathcal{V}/\mathfrak{m} \cong \mathbb{F}_q$

A a separated and complete \mathcal{V} -algebra

formal spectrum of A := ringed space $(\text{Spf}(A), \mathcal{O}_P)$ where

- $\text{Spf}(A) = \text{topological space } \text{Spec}(A/p^n A)$ for *any* $n \in \mathbb{N}$
- $\mathcal{O}_P = \lim \mathcal{O}_{P_n}$ where $\mathcal{O}_{P_n} = \mathcal{O}_{\text{Spec}(A/p^n A)}$ for all $n \in \mathbb{N}$

\mathcal{V} -formal scheme := ringed space $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ that “locally“ looks like a formal spectrum

Tate algebra := homomorphic image of $K \langle X_1, \dots, X_n \rangle$ for some n , where

$$\begin{aligned} K \langle X_1, \dots, X_n \rangle &:= \text{ring of } \textit{convergent} \text{ power series} \\ &= \left\{ \sum_{\underline{u} \in \mathbb{N}^n} a_{\underline{u}} \underline{X}^{\underline{u}} \mid \lim_{|\underline{u}| \rightarrow \infty} |a_{\underline{u}}| = 0 \right\} \end{aligned}$$

rigid-analytic space := ringed space (X, \mathcal{O}_X) where

- X is “locally“ the *maximal spectrum* of a Tate algebra
- Every point has a basis $\{U_i\}_{i \in I}$ of neighbourhoods so that $\Gamma(U_i, \mathcal{O}_X)$ is a Tate algebra.

Facts:

- For every \mathcal{V} -formal scheme \mathfrak{X} there is a rigid analytic space \mathfrak{X}^\sim and a morphism of ringed spaces

$$\text{sp} : \mathfrak{X}^\sim \longrightarrow \mathfrak{X}$$

(If $\mathfrak{X} = \text{Spf}(A)$, simply take $\mathfrak{X}^\sim := \text{Spm}(A \otimes_{\mathcal{V}} K)$.)

- Every quasi-projective variety X/\mathbb{F}_q can be embedded in a \mathcal{V} -formal, affine scheme P .

$$\underline{\text{open tube of } X \text{ in } \tilde{P}} \quad := \quad]X[_P \quad := \quad \text{sp}^{-1}(X) \subseteq \tilde{P}$$

One has

$$]X[_P = \{x \in \tilde{P} \mid |f_i(x)| < 1, 1 \leq i \leq r\}$$

where $f_1, \dots, f_r \in \Gamma(P, \mathcal{O}_P)$ generate the ideal of X in P .

Theorem: If X is a smooth projektve variety over \mathbb{F}_q , then

$$H_p^i(X/\mathbb{F}_q) \cong \mathbb{H}^i(]X[_P, \Omega_{]X[_P}^\bullet) =: H_{rig}^i(X/\mathbb{F}_q)$$

Rigid cohomology for affine varieties

X/\mathbb{F}_q smooth, affine variety,

$Y :=$ projective closure of X , $Z := Y \setminus X$

embed Y into an affine, smooth \mathcal{V} -formal scheme P

\Rightarrow get subsets $]X[_P,]Y[_P,]Z[_P$ of \tilde{P}

$$]Z[_{P,\lambda} := \{x \in \tilde{P} \mid |g_i(x)| < \lambda\}$$

where $\lambda < 1$ and $g_1, \dots, g_r \in \Gamma(P, \mathcal{O}_P)$ generate the ideal of Z in P .

For any shear \mathcal{F} on $]Y[_P$, set

$$U_\lambda :=]Y[_P \setminus]Z[_{P,\lambda}, \quad j_\lambda : U_\lambda \hookrightarrow]Y[_P, \quad j^\dagger \mathcal{F} := \lim_{\lambda \rightarrow 1} j_{\lambda*} j_\lambda^* \mathcal{F}$$

Then define $H_{rig}^i(X) := \mathbb{H}^i(]Y[_P, j^\dagger \Omega_{]Y[_P}^\bullet) \cong H^i(\Gamma(]Y[_P, j^\dagger \Omega_{]Y[_P}^\bullet))$.

Theorem: $H_{rig}^i(X/\mathbb{F}_q)$ is a finite-dimensional K -vector space.

Remark: The canonical morphisms of sheaves

$$\Omega_{]Y[_P}^\bullet \longrightarrow j_{\lambda*} j_\lambda^* \Omega_{]Y[_P}^\bullet \longrightarrow j^\dagger \Omega_{]Y[_P}^\bullet$$

induce a canonical homomorphism $H_{rig}^i(Y/\mathbb{F}_q) \longrightarrow H_{rig}^i(X/\mathbb{F}_q)$ (that commutes with Frobenius).

advantages of rigid cohomology:

- It is more explicit than crystalline cohomology.
- It is defined for non-projective and singular varieties.
- We have a simple relation between cohomology of affine and projective varieties.
- One can apply the theory rigid analytic spaces: comparison theorem of Čech and sheaf cohomology, Serre duality etc.

algebraic description of rigid cohomology:

X affine variety over \mathbb{F}_q

\bar{A} coordinate ring $\mathbb{F}_q[X_1, \dots, X_n]/(f_1, \dots, f_r)$ of X

A lifting of \bar{A} to $W(\mathbb{F}_q)$

A^\dagger weak \mathfrak{p} -adic completion of $A =$ homomorphic image of

$$W(\mathbb{F}_q)[X_1, \dots, X_n]^\dagger = \left\{ \sum_{\underline{u}} a_{\underline{u}} X^{\underline{u}} \mid \exists C > 0, 0 < \rho < 1 : |a_{\underline{u}}| < C \rho^{|\underline{u}|} \right\}$$

Theorem: There is a canonical isomorphism

$$H_{rig}^i(X/\mathbb{F}_q) \cong H_{DR}^i(A^\dagger \otimes_{W(\mathbb{F}_q)} K) =: H_{MW}^i(\bar{A})$$

Algorithms (l -adic and p -adic)

(1) Schoof's algorithm (l -adic, rough idea)

- given an elliptic curve E/\mathbb{F}_q with $q = p^a$, $p \neq 2, 3$
- for several primes $l_1, l_2, \dots, l_r \neq p$
 - (a) compute action of Frobenius on $E[l_i]$
(using n -division polynomials)
 - (b) obtain trace of Frobenius on $T_{l_i}(E)$ “modulo l_i ”
 (“first order approximation of Frobenius on $H_{l_i}^1(E)$ ”)
- CRT yields trace of Frobenius on E “modulo $(\prod_{i=1}^r l_i)$ ”
- product $> 2\sqrt{q} \Rightarrow$ get exact Frobenius c on E from $|c| \leq \sqrt{q}$
- $\#E(\mathbb{F}_q) = q + 1 - c$

“small Frobenius“:

E/\mathbb{F}_q elliptic curve, $q = p^a$, $a \geq 2$

The mapping $(x, y) \mapsto (x^p, y^p)$ gives a morphism $E \longrightarrow E^{(p)}$.

If E is given by $f(x, y) = 0$, then $E^{(p)}$ is given by $f^\sigma(x, y) = 0$

(Frobenius applied to coefficients of f).

\Rightarrow cycle of curves

$$\dots \longrightarrow E \longrightarrow E^{(p)} \longrightarrow E^{(p^2)} \longrightarrow \dots \longrightarrow E^{(p^a)} = E \longrightarrow \dots$$

(2) Satoh’s algorithm (p -adic)

- given an elliptic curve E/\mathbb{F}_q
- compute the a -cycle of curves $E^{(p^i)}$ and their j -invariants j_i
- compute a p -adic approximation of all the j -invariants J_i of the canonical lifts of the a curves
(The J_i are given by a p -adic polynomial equation system;
use Newton iteration to approximate solution)
- compute the coefficients of the lifted curves from their j -invariants
- compute the p -torsion groups of the lifted curves
(given by a factor of the p -division polynomial)
- from that compute the traces of the small Frobenius

(3) Kedlaya's algorithm (p -adic, cohomological!)

- given a hyperelliptic curve $C : Y^2 = f(X)$ over \mathbb{F}_q
- $\bar{A} :=$ coordinate ring of $C \setminus \{\infty, \text{Weierstrass points}\}$
- rough idea: approximate computation of Frobenius on $H_{MW}^1(\bar{A})$
(required precision given by Hasse-Weil bound)
- decompose Frobenius into “small Frobenii“, obtain cycle

$$\dots \xleftarrow{\text{frob}} H_{MW}^1(\bar{A}) \xleftarrow{\text{frob}} H_{MW}^1(\bar{A}^{(p)}) \xleftarrow{\text{frob}} H_{MW}^1(\bar{A}^{(p^2)}) \xleftarrow{\text{frob}} \dots$$

- basis of $H_{MW}^1(\bar{A}^{(p^i)})$ given by

$$\mathcal{B}_i := \{X^k Y^{-1} dX, X^k Y^{-2} dX, 0 \leq k \leq 2g - 1\}$$

- first step: computation of lifting of small Frobenius

$$(A^\dagger)^{(p)} = W(\mathbb{F}_q)[X, Y]/(Y^2 - \tilde{f}^\sigma)^\dagger \longrightarrow A^\dagger = W(\mathbb{F}_q)[X, Y]/(Y^2 - \tilde{f})^\dagger$$

(a) send X to $X^{\text{frob}} := X^p$

(b) obtain Y^{frob} from (app.) solving $(Y^{\text{frob}})^2 = \tilde{f}^\sigma(X^{\text{frob}})$ in A^\dagger

- second step: compute small frobenius on differentials

$$(X^k Y^{-j} dX)^{\text{frob}} = p X^{pk+(p-1)} (Y^{\text{frob}})^{-j} dX$$

and reduce modulo “exact differentials“

$$(\text{image of } d : A^\dagger \otimes K \longrightarrow \Omega_{A \otimes K}^1)$$

- If the homomorphism

$$H_{MW}^1(\bar{A}^{(p)}) \longrightarrow H_{MW}^1(\bar{A})$$

relative to $\mathcal{B}_1, \mathcal{B}_0$ given by the matrix M , then

$$H_{MW}^1(\bar{A}^{(p^{i+1})}) \longrightarrow H_{MW}^1(\bar{A}^{(p^i)})$$

relative to $\mathcal{B}_{i+1}, \mathcal{B}_i$ is given by M^{σ^i} .

- third step: compute $N = M \cdot M^\sigma \cdot \dots \cdot M^{\sigma^{a-1}}$
- fourth step: compute the trace of N

Problems in extending Kedlaya's algorithm to general varieties:

- need a basis (or at least a generating system) of $H_{MW}^i(\bar{A})$
(use theory of rigid analytic spaces and relation between “projective“ and “affine“ rigid cohomology)
- computation of lifting of Frobenius on $(A^{(p)})^\dagger \longrightarrow A^\dagger$
existence of lifting is granted by theorems of Artin and Bosch
task: use proofs to formulate a general algorithm
- use information on “slopes of Frobenius“ for complexity estimates