# $p$-adic numerical methods in arithmetic geometry

Jan Tuitman

KU Leuven

February 20, 2018

# Algebraic curves

An *algebraic variety* is the zero locus of finite number of polynomial equations in finite number of variables.

Defined *over* a field $k$ if the polynomials have coefficients in that field.

A *curve* is an algebraic variety of dimension 1, always smooth and projective, e.g. $y^2 = x^3 + ax + b$ elliptic curve.

However, sometimes defined by *(singular) plane model* $f(x, y) = 0$.

$k$ will always be a finite field $\mathbb{F}_q$ or the field of rational numbers $\mathbb{Q}$.

Recall that $q = p^n$ and for all such $q$ there exists a unique finite field $\mathbb{F}_q$ with $q$ elements.

# Zeta function

Let $X$ be an algebraic curve over a finite field $\mathbb{F}_q$ with $q = p^n$.

**Definition**

$$Z(X, T) := \exp\left(\sum_{i=1}^{\infty} |X(\mathbb{F}_{q^i})| \frac{T^i}{i}\right)$$

**Example (Projective line)**

$$\begin{aligned}
Z(\mathbb{P}^1_{\mathbb{F}_q}, T) &= \exp\left(\sum_{i=1}^{\infty} (q^i + 1) \frac{T^i}{i}\right) \\
&= \exp\left(\sum_{i=1}^{\infty} \frac{T^i}{i}\right) \exp\left(\sum_{i=1}^{\infty} \frac{(qT)^i}{i}\right) \\
&= \frac{1}{(1-T)(1-qT)}
\end{aligned}$$

# Weil conjectures

**Theorem (Weil, 1948)**

*Let $X$ be a smooth projective curve of genus $g$ over $\mathbb{F}_q$. Then*

$$Z(X,T) = \frac{\chi(T)}{(1-T)(1-qT)}$$

*with $\chi(T) \in \mathbb{Z}[T]$ of degree $2g$. Moreover,*

$$\chi(T) = \prod_{i=1}^{2g} (1-\alpha_i T),$$

*where:*

- *the $\alpha_i$ are algebraic integers,*
- *of absolute value $\sqrt{q}$,*
- *permuted by $\alpha \mapsto q/\alpha$.*

# Computing zeta functions

Since the zeta function is given by a *finite* amount of data, one can hope to compute it.

**Problem**

*Compute $Z(X, T)$ efficiently.*

Bounds on the the degrees of the numerator and denominator of $Z(X, T)$ are known, so computing $Z(X, T)$ reduces to computing a finite number of $X(\mathbb{F}_{q^i})$.

For a curve of genus $g$, have to compute up to $X(\mathbb{F}_{q^g})$. Counting *naively* need at least $q^g$ operations. Too slow for all but the smallest values of $q$ and $g$.

Let us first give some applications.

# Cryptography

Can associate to curve $X/\mathbb{F}_q$ a finite Abelian group $J(\mathbb{F}_q)$ called its *Jacobian*. The order of this group is $\chi(1)$. The *Discrete Logarithm Problem* (DLP) on $J(\mathbb{F}_q)$ is:

**Problem**

*given $P, Q \in J(\mathbb{F}_q)$ find (the smallest) $n \in \mathbb{N}$ such that $nP = Q$.*

This problem is used in cryptography in *Diffie Helmann* key exchange. When the order of $J(\mathbb{F}_q)$ only has small prime factors the DLP is easy.

So we need to compute $\chi(1)$ and we can do this by computing $Z(X, T)$.

# Sato-Tate distributions

Let $X$ be a smooth projective curve of genus $g$ defined over $\mathbb{Q}$.

For every prime $p$ let $X_p/\mathbb{F}_p$ denote the reduction of $X$ modulo $p$. Again, for all but a finite number of $p$:

$$Z(X_p, T) = \frac{\chi_p(T)}{(1-T)(1-qT)}$$

for some polynomial $\chi_p(T) \in \mathbb{Z}[T]$ of degree $2g$.

**Problem**

*How is the polynomial $\chi_p(T/\sqrt{p})$ distributed when $p$ varies?*

*Conjectural answer:* as the (reverse) characteristic polynomial of a random conjugacy class of a certain compact group. So far only known for $g = 1$.

Andrew Sutherland (with coauthors) computed $\chi_p(T)$ for $X$ with $g = 2$ and found all predicted distributions!

# p-adic numbers

Let:

- $p$ a prime,
- $\text{ord}_p$ the $p$-adic valuation on $\mathbb{Z}$ (number of factors $p$),
- $\|\cdot\|_p = p^{-\text{ord}_p(\cdot)}$ associated metric on $\mathbb{Z}$.

**Definition ($p$-adic integers)**

*$\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ w.r.t. $\|\cdot\|_p$.*

Elements $a_0 + a_1 p + a_2 p^2 + \ldots$, with $a_i \in \{0, 1, \ldots, p-1\}$.

$\mathbb{Z}_p$ has a unique maximal ideal $(p)$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. The field of fractions $\mathbb{Q}_p$ has characteristic 0.

Similarly, can define $\mathbb{Z}_q$ such that $\mathbb{Z}_q/p\mathbb{Z}_q \cong \mathbb{F}_q$, field of fractions $\mathbb{Q}_q$.

# p-adic cohomology

Let $X/\mathbb{F}_q$ be a smooth projective curve.

Can define $p$-adic (rigid/Monsky Washnitzer) cohomology space $H^1_{\mathrm{rig}}(X)$:

- finite dimensional $\mathbb{Q}_q$ vector space,
- with action $\mathrm{F}_q^*$ of the $q$-th power map $\mathrm{F}_q$,

such that:

$$\chi(T) = \det(1 - \mathrm{F}_q^* \, T | H^1_{\mathrm{rig}}(X)).$$

**Idea:** first lift $X$ to characteristic 0, then take (overconvergent) de Rham cohomology.

# Smooth affine case

Let:

- $X = \mathrm{Spec}(\overline{A})$ with $\overline{A}$ a smooth $\mathbb{F}_q$ algebra of finite type.
- smooth lift $A = \mathbb{Z}_q[x_1, \ldots, x_l]/(f_1, \ldots, f_m)$ such that $A \otimes_{\mathbb{Z}_q} \mathbb{F}_q = \overline{A}$.
- weak completion $A^\dagger = \mathbb{Z}_q\langle x_1, \ldots, x_l\rangle^\dagger/(f_1, \ldots, f_m)$, where

$$\mathbb{Z}_q\langle x_1, \ldots, x_l\rangle^\dagger := \{\sum_I a_I x^I : a_I \in \mathbb{Z}_q, \exists \rho > 1 \text{ s.t. } \lim_{|I|\to\infty} |a_I|\rho^{|I|} = 0\}.$$

- 1-forms $\Omega^1_{A^\dagger} = (A^\dagger dx_1 \oplus \ldots \oplus A^\dagger dx_l)/(A^\dagger df_1 + \ldots + A^\dagger df_m)$.
- $d : A^\dagger \mapsto \Omega^1_{A^\dagger}$.

Then: $H^1_{\mathrm{rig}}(X) = \mathrm{coker}(d) \otimes \mathbb{Q}_q$.

# Hyperelliptic curves

Let:

- $\mathbb{F}_q$ a finite field of odd characteristic,
- $Q \in \mathbb{F}_q[x]$ monic of degree $2g + 1$ without repeated roots,
- $X$ the smooth projective curve defined by $y^2 = Q(x)$.

$X$ is a hyperelliptic curve of genus $g$ (with a rational Weierstrass point).

For characteristic 2 or curves without a rational Weierstrass point this has to be modified slightly.

Kedlaya (2001) proposed to compute $Z(X, T)$ using $p$-adic cohomology.

# Kedlaya's algorithm

Sketch:

- $X : y^2 = Q(x)$ hyperelliptic of genus $g$ over $\mathbb{F}_q$ with $q = p^n$ odd.
- $U$ open in $X$ defined by $y \notin \{0, \infty\}$.
- $\mathcal{Q} \in \mathbb{Z}_q[x]$ a monic lift of $Q$.
- $A^\dagger = \mathbb{Z}_q\langle x, y, 1/y\rangle^\dagger/(y^2 - \mathcal{Q})$.
- basis for $H^1_{rig}(X) \subset H^1_{rig}(U)$ given by $[\frac{dx}{y}, \ldots, x^{2g-1}\frac{dx}{y}]$.
- lift Frobenius to $A^\dagger$: $\mathrm{F}_p(x) := x^p$, find $\mathrm{F}_p(y) \equiv y^p \bmod p$ (Hensel).
- Apply $\mathrm{F}_p$ to basis for $H^1_{rig}(X)$ and reduce to find matrix $\mathrm{F}_p$.
- Compute $\chi(T) = \det(1 - T\mathrm{F}_p^n | H^1_{rig}(X))$.
- $Z(X, T) = \chi(T)/((1 - T)(1 - qT))$.

# Complexity

$X/\mathbb{F}_q$ hyperelliptic $q = p^n$ genus $g$.

**Theorem (Kedlaya, 2001)**

*$Z(X, T)$ can be computed in time $O((pg^4n^3)^{1+\epsilon})$.*

Input size about $\log(p)gn$, so (only) polynomial time for fixed $p$.

All $p$-adic algorithms suffer from this, but the dependence on $p$ can be improved to $O(p^{1/2+\epsilon})$ and *average polynomial time* (Harvey).

# General curves

Let $X/\mathbb{F}_q$ with $q = p^n$ be the smooth projective curve birational to a (singular) plane curve

$$f(x, y) = 0$$

with $f \in \mathbb{F}_q[x, y]$ irreducible and monic in $y$ of degree $d_x, d_y$ in $y, x$.

**Theorem (Tuitman, 2014)**

*Suppose that we know a 'good' lift $F \in \mathbb{Z}_q[x, y]$ of $f$ to characteristic zero (technical). Then the zeta function of $X$ can be computed in time:*

$$O((pd_y^6 d_x^4 n^3)^{1+\epsilon})$$

Input size about $\log(p) d_x d_y n$, so again (only) polynomial time for fixed $p$.

Good lift condition rather technical. However often known or easy to construct (e.g. when $g \leq 5$, joint work with Castryck).

# Some examples

## Example: the modular curve $X_1(17)$

```
> P<x>:=PolynomialRing(RationalField());
> R<y>:=PolynomialRing(P);
> f:=y^4 + (x^3 + x^2 - x + 2)*y^3 + (x^3 - 3*x + 1)*y^2 - (x^4 + 2*x)*y + x^3 + x^2;
> p:=101;
> ZetaFunction(f,p);
(10510100501*T^10 + 6035503258*T^9 + 1900905345*T^8 + 396288448*T^7 + 60231754*T^6 + 6865620*T^5 +
596354*T^4 + 38848*T^3 + 1845*T^2 + 58*T + 1)/(101*T^2 - 102*T + 1)
```

## Example: a generic genus 5 curve

```
> C:=RandomGenus5CurveNonTrigonal(FiniteField(37));
> C;
Curve over GF(37) defined by
19*$.1^2 + 18*$.1*$.2 + 31*$.2^2 + $.1*$.3 + 19*$.2*$.3 + 25*$.3^2 + 8*$.1*$.4 + 17*$.2*$.4 + 29*$.3*$.4 +
19*$.4^2 + 18*$.1*$.5 + 27*$.2*$.5 + 26*$.3*$.5 + 14*$.4*$.5 + 32*$.5^2,
12*$.1^2 + 31*$.1*$.2 + 18*$.2^2 + 11*$.1*$.3 + 24*$.2*$.3 + 21*$.3^2 + 12*$.1*$.4 + 4*$.2*$.4 + 21*$.3*$.4
+ 22*$.4^2 + 4*$.1*$.5 + 31*$.2*$.5 + 23*$.3*$.5 + 20*$.4*$.5 + 35*$.5^2,
21*$.1^2 + 35*$.1*$.2 + 17*$.2^2 + 8*$.1*$.3 + 12*$.2*$.3 + 32*$.3^2 + 34*$.1*$.4 + 22*$.2*$.4 + 24*$.3*$.4 +
18*$.4^2 + 19*$.1*$.5 + 10*$.2*$.5 + 19*$.3*$.5 + 10*$.4*$.5
> ZetaFunction(C);
(69343957*T^10 - 5622483*T^9 + 1418284*T^8 + 217671*T^7 - 2997*T^6 + 6604*T^5 - 81*T^4 + 159*T^3 + 28*T^2
- 3*T + 1)/(37*T^2 - 38*T + 1)
```

Fields very small in these examples, but same thing works over $GF(p)$ with $p \sim 2^{15}$ and $GF(q)$ with $q = p^n$ much larger still!

# Precision

Can only compute with $p$-adic numbers to finite precision $N$ (i.e. mod $p^N$).

Recall that

$$\chi(T) = \chi_{2g} T^{2g} + \ldots + \chi_1 T + 1 = \prod_{i=1}^{2g} (1 - \alpha_i T)$$

with $|\alpha_i| = \sqrt{q}$ and $\alpha \mapsto q/\alpha$ permuting the $\alpha_i$. So $|\chi_i| \leq \binom{2g}{g} q^{g/2}$ and $\chi_{2g-i} = q^{g-i}\chi_i$. Sufficient to compute $\chi$ to precision $N$ such that

$$p^N > 2\binom{2g}{g} q^{g/2}.$$

Have to keep track of $p$-adic precision throughout the algorithm. This involves very interesting (and rather technical) mathematics.

# Rational points

$X/\mathbb{Q}$ a smooth projective curve of genus $g > 1$.

Given by (singular) plane model $f(x, y) = 0$.

**Theorem (Faltings, 1983)**

*The set $X(\mathbb{Q})$ of rational points on $X$ is finite.*

Usually points are easily found by a search (if they exist).

**Example ($g = 4$)**

$$f(x, y) = y^3 - (x^5 - 2x^4 - 2x^3 - 2x^2 - 3x)$$
$$X(\mathbb{Q}) \supset \{(1, -2), (0, 0), (-1, 0), (3, 0), \infty\}$$

**Problem**

*How to prove that these are all points?*

# Chabauty's theorem

$J$ will denote the Jacobian variety of $X$, i.e. divisors of degree 0 modulo divisors of functions. Note that $J$ is naturally an abelian variety.

**Theorem (Mordell-Weil)**

*$J(\mathbb{Q})$ is a finitely generated abelian group.*

Given a point $b \in X(\mathbb{Q})$, we get an embedding $X(\mathbb{Q}) \to J(\mathbb{Q})$:

$$P \mapsto (P) - (b)$$

**Theorem (Chabauty, 1941)**

*Let $r$ be the rank of $J(\mathbb{Q})$. If $r < g$ then $X(\mathbb{Q})$ is finite.*

Coleman: can make this effective using $p$-adic line integrals.

# Coleman integrals

Let:

- $p$ a prime at which $X$ has good reduction,
- $P, Q \in X(\mathbb{Q}_p)$,
- $\omega$ a 1-form on $X_{\mathbb{Q}_p}$ (more generally on some wide open of a rigid analytic space).

In the 80's Coleman defined path independent line integrals

$$\int_P^Q \omega$$

which can be extended to integrate over $D \in J(\mathbb{Q}_p)$, where $J$ is the Jacobian of $X$ (above: $D = (Q) - (P)$).

# Properties

The Coleman integral has the following properties:

1. Linearity: $\int_P^Q (a\omega_1 + b\omega_2) = a\int_P^Q \omega_1 + b\int_P^Q \omega_2$.
2. Additivity in endpoints: $\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega$.
3. Change of variables: If $V' \subset X'$ is a wide open subspace of a rigid analytic space $X'$ and $\phi : V \to V'$ a rigid analytic map then $\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$.
4. Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$ for $f$ a rigid analytic function on $V$.

A residue disk on $X_{\mathbb{Q}_p}$ is the inverse image under reduction mod $p$ of a single point. Coleman integrals within a single residue disk are called tiny.

# Tiny integrals

Let: $P, Q \in X(\mathbb{Q}_p)$ points in the same residue disk, $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$.

Then $\int_P^Q \omega$ can be computed by expanding $\omega$ in a local coordinate $t$ on the disk:

$$\omega = \sum_{i \geq 0} c_i t^i dt$$

and integrating as usual

$$\int_{t(P)}^{t(Q)} \sum_{i \geq 0} c_i t^i dt = \sum_{i \geq 0} \frac{c_i}{i+1} (t(Q)^{i+1} - t(P)^{i+1}).$$

When $P$ and $Q$ not in the same residue disk, does not work: series do not converge.

Analytic continuation fails over $\mathbb{Q}_p$. Coleman: use Frobenius action on $p$-adic cohomology.

# $p$-adic cohomology

Let $U \subset X$ be an open such that $X - U$ is smooth over $\mathbb{Z}_p$ and $\omega_1, \ldots, \omega_{2g} \in \Omega^1(U_{\mathbb{Q}_p})$ a basis for $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})$.

Then there exist:

- a matrix $\Phi \in M_{2g \times 2g}(\mathbb{Q}_p)$,
- (overconvergent) functions $f_1, \ldots, f_{2g}$ on some open of $X_{\mathbb{Q}_p}$,

such that

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_{j=1}^{2g} \Phi_{ij}\omega_j \qquad \text{for } i = 1, \ldots, 2g.$$

We can take $\omega_1, \ldots, \omega_g$ to be a basis for $H^0(X_{\mathbb{Q}_p}, \Omega^1)$.

## General integrals

Recall that

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_{j=1}^{2g} \Phi_{ij}\omega_j \qquad \text{for } i = 1, \ldots, 2g.$$

Assume that $\mathrm{F}_p(P) = P$ and $\mathrm{F}_p(Q) = Q$ (Teichmüller points). No loss of generality, can correct with tiny integrals. Integrating, we find

$$\int_P^Q \omega_i = \int_{\mathrm{F}_p(P)}^{\mathrm{F}_p(Q)} \omega_i = \int_P^Q \mathrm{F}_p^*(\omega_i) = f_i(Q) - f_i(P) + \sum_j \Phi_{ij} \int_P^Q \omega_j.$$

So we can determine the $\int_P^Q \omega_i$ by solving the linear system

$$(\Phi - I) \int_P^Q \omega_i = f_i(P) - f_i(Q) \qquad \text{for } i = 1, \ldots, 2g.$$

# Chabauty-Coleman

Assume a point $b \in X(\mathbb{Q})$ is known and embed $X \hookrightarrow J$ into its Jacobian by $P \mapsto (P) - (b)$.

**Theorem (Chabauty-Coleman)**

*Let $r$ denote the Mordell-Weil rank of $J$ and suppose that $r < g$. Then there exists $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that $\int_b^P \omega = 0$ for all $P \in X(\mathbb{Q})$.*

**Sketch of proof.**

$$\begin{array}{ccccc}
X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & \xrightarrow{AJ_b} & \\
\downarrow & & \downarrow & & \searrow \\
J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{D \mapsto \int_D} & H^0(X_{\mathbb{Q}_p}, \Omega^1)^*
\end{array}$$

$X(\mathbb{Q})$ lands in a subspace of $H^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ of dimension at most $r$. □

# Implementation

Together with Balakrishnan we have developed and implemented algorithm for computing (single) Coleman integrals and carrying out effective Chabauty on *arbitrary curves*:

`www.github.com/jtuitman/Coleman`

Note that we need Mordell-Weil rank $r$ to be known and $r < g$.

When $r \geq g$ there is an extension of the effective Chabauty method by Kim (non-Abelian Chabauty), involving *iterated* Coleman integrals.

Together with Balakrishnan, Dogra, Müller and Vonk we have recently succeeded in applying Kim's method to the split Cartan modular curve of level 13 (also known as the *cursed curve*).

# Example

Let us return to the example $f(x,y) = y^3 - (x^5 - 2x^4 - 2x^3 - 2x^2 - 3x)$. The Magma function *RankBounds()* proves that the rank of $J$ is 1. This uses work of Poonen-Schaefer (1997). Now we use our code:

```
> load "coleman.m";
> Q:=y^3 - (x^5 - 2*x^4 - 2*x^3 - 2*x^2 - 3*x);
> p:=7;
> N:=15;
> data:=coleman_data(Q,p,N);
> Qpoints:=Q_points(data,1000); // PointSearch
> #vanishing_differentials(Qpoints,data:e:=50);
3
> #effective_chabauty(data,1000:e:=50),#Qpoints;
5 5
```

This proves that our list of rational points is complete.