Computing modular Galois representations - the modulo p approach (after Jinxiang Zeng)

Maarten Derickx [1]

Universiteit Leiden
and
Université Bordeaux 1

Sage Days 51
22-26 July 2013

[1] Original slides by Jinxiang Zeng, modified by D.

Computing Coefficients of modular forms

1. Introduction/Main Results
   - How fast can $\tau(p)$ be computed?
   - An algorithm work with finite fields
   - Complexity analysis
   - A lower bound on the number of generators of $\mathfrak{m} \subset \mathbb{T}$
2. A First Description of the Algorithm
   - Congruence of Modular Forms
   - Galois Representations and Modular Forms
   - Computing The Ramanujan subspace
3. Future work

The discriminant modular form

Discriminant Modular Form

Let $q := e^{2\pi iz}$, the discriminant modular form is defined by

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n \in \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$$

where $\tau : \mathbb{Z} \to \mathbb{Z}$ is called Ramanujan tau function.

$\Delta(q)$ plays a crucial role during the developments of theory of modular forms. In this lecture we focus on the computational aspects of $\Delta(q)$.

The discriminant modular form

Arithmetic of the Ramanujan tau function

- $\tau(mn) = \tau(m)\tau(n)$ for any integers satisfying $(m, n) = 1$.
- $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ for any prime $p, n \geq 1$.
- $|\tau(p)| \leq 2p^{11/2}$, Deligne's bound.
- $\tau(p) \equiv p(1 + p^9) \mod 25, \tau(p) \equiv p(1 + p^3)$ mod 7,$\tau(p) \equiv 1 + p^{11} \mod 691$

Lehmer's Conjecture

- $\tau(n) \neq 0$ for any $n \geq 1$.

Serre: if $\tau(p) = 0$ then $p = hM - 1$ with $M = 2^{14}3^7 5^3 691$, $\left(\frac{h+1}{23}\right) = 1$ and some $h \mod 49 \in \{0, 30, 48\}$.

How fast can $\tau(p)$ be computed?

A question that Schoof asked to Edixhoven in 1995

Can we compute $\tau(p)$ for prime p in time polynomial in $\log p$?

Theorem (Edixhoven, Couveignes, etc.)

For prime p, there exist algorithms to compute $\tau(p)$ in time polynomial in $\log p$.

- work with complex number field, using numerical approximation.
- work with finite fields, using CRT.

$|\tau(p)| \leq 2p^{11/2}$ so $\tau(p)$ can be computed by computing $\tau(p) \mod \ell$ for sufficiently many small primes ℓ (where small means $\mathrm{O}(\log p)$.)

How fast can $\tau(p)$ be computed?

Generalization and explicit calculation

- Bruin generalized the methods to modular forms for the groups of the form $\Gamma_1(n)$.
- Bosman implemented an algorithm using numerical approximation $\mathbb{C}$ and computed

$$\rho_l^{proj} : \mathrm{Gal}\bar{Q}/Q \to \mathrm{PGL}(V_l)$$

for $\ell \in \{13, 17, 19\}$. This allows one to calculate $\pm\tau(p) \mod l$ which he used to prove

$$\tau(n) \neq 0, \forall n < 2 \cdot 10^{19}.$$

A probabilistic algorithm

Algorithm(Zeng 2012)

Following Couveignes's idea, working with finite fields, we give a probabilistic algorithm, which is rather simple and well suited for implementation.

The following calculation was done using a personal computer.

level	time (projective representation)	time (entire representation)
ℓ=13	several minutes	one hour
ℓ=17	several hours	one day
ℓ=19	several days	less than four days
$\ell = 29$	waiting	waiting
$\ell = 31$	several days	several days

A probabilistic algorithm

Exact value of $\tau(p) \mod \ell$

Since we can compute the entire representation, the exact values of $\tau(p) \mod \ell$ for $\ell \in \{13, 17, 19\}$ can be computed.

Nonvanishing of tau function

Since we can compute the projective representation for $\ell = 31$, we can prove[a]

$$\tau(n) \neq 0, \text{for all } n < 982149821766199295999 \approx 9 \cdot 10^{20}$$

[a] Bosman proved the nonvanishing holds for $n < 22798241520242687999 \approx 2 \cdot 10^{19}$

Complexity of the algorithm

Theorem(Zeng 2012)

For prime p, $\tau(p)$ can be computed in time $\mathrm{O}(\log^{6+2\omega+\delta+\epsilon} p)$.

- ω is a constant in [2,4], refers to that addition in Jacobian can be done in time $\mathrm{O}(g^{\omega})$,
- δ is a constant, measuring the heights of the points of the Ramanujan subspace V_ℓ,
- ϵ is any real positive number.

ω depends on the complexity of calculations in $J_1(l)(\mathbb{F}_{p^e})$. Using Khuri-Makdisi's algorithm, the constant ω is 2.376. Our computation suggests $\delta \approx 3$, although this is based on a very small sample ($l = 13, 17, 19$)

On the generators of the maximal ideal

Theorem(Zeng 2012)

If $\ell \geq 13$ is prime and $\mathfrak{m} = (l, T_1 - \tau(1), T_2 - \tau(2), T_3 - \tau(3), \ldots) \subset \mathbb{T}$, then $\mathfrak{m}$ can be generated by ℓ and $T_n - \tau(n)$ with $n \leq \frac{2\ell+1}{12}$.

Remarks

- It makes the algorithm faster. The previous known upper-bound was $(\ell^2 - 1)/6$, making step 5 very slow.
- In practice the upper bound is even much better.
  - $\mathfrak{m} = (\ell, T_2 - \tau(2))$ for $\ell \in \{13, 17, 19, 29, 37, 41, 43\}$
  - $\mathfrak{m} = (\ell, T_3 - \tau(3))$ for $\ell = 31$

Congruence of Modular Forms

Theorem (Mazur, Ribet, Gross, Edixhoven etc.)

Let $n, k \in \mathbb{Z}_+$, $\mathbb{F}/\mathbb{F}_\ell$ finite extension, and $f : \mathbb{T}(n,k) \to \mathbb{F}$ a surjective ring morpism. Assume $2 < k \leq \ell + 1$ and the associated Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ is absolutely irreducible. Then there is a unique ring morphism $f_2 : \mathbb{T}(n\ell, 2) \to \mathbb{F}$ such that:

- f_2 is surjective, $f_2(T_i) = f(T_i), f_2(< a >) = f(< a >)a^{k-2}$ for all $i \geq 1$ and any a satisfying $(a, n\ell) = 1$.
- $V_f := J_1(n\ell)[\ker f_2]$ realizes ρ_f.

Remark

For the rest of this talk: $f = \Delta(q) \bmod \ell$, so $\mathbb{F} = \mathbb{F}_\ell$,
$\ker f_2 =< \ell, T_i - \tau(i) : i \geq 1 >$ and $V_\ell := V_{\Delta,\ell} = J_1(\ell)[\ker f_2]$.

Galois Representation

Galois representation associated to $\Delta(q)$

Let ρ_ℓ be the Galois representation associated to the newform $\Delta(q)$

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

then

- For prime $p \neq \ell$:
  $\mathrm{Tr}(\rho_\ell(\mathrm{Frob}_p)) \equiv \tau(p) \mod \ell$ and $\det(\rho_\ell(\mathrm{Frob}_p)) \equiv p^{11} \mod \ell$.
- The representation space (called Ramanujan subspace denoted by V_ℓ) is

$$V_\ell = \bigcap_{1 \leq k \leq \frac{\ell^2-1}{6}} \ker(T_k - \tau(k), J_1(\ell)[\ell])$$

Computing V_ℓ mod p: the strategy

1) Find an e s.t. $V_\ell(\bar{\mathbb{F}}_p) = V_\ell(\mathbb{F}_{p^e})$
2) Compute $n := \#J_1(\ell)(\mathbb{F}_{p^e})$
3) Pick $P \in J_1(\ell)(\mathbb{F}_{p^e})$ random.
4) Multiply P by $n\ell^{-v_\ell(n)}$, and then repeatedly by ℓ until $P \in J_1(\ell)[\ell]$
5) Compute $Q := f(P)$ for some surjection $J_1(\ell)[\ell] \to V_\ell$.
6) Repeat 3), 4) and 5) till you find linearly independent $Q_1, Q_2 \in V_\ell$.

Step 1: find e s.t.: $V_\ell(\bar{\mathbb{F}}_p) = V_\ell(\mathbb{F}_{p^e})$

The characteristic polynomial of Frob_p on V_ℓ is $X^2 - \tau(p)X + p^{11}$
We need $\mathrm{Frob}_p = \mathrm{Id}_{V_\ell}$ so we can take:

$$e := \min\{t \mid t \geq 1, X^t = 1 \in \mathbb{F}_\ell[X]/(X^2 - \tau(p)X + p^{11})\}$$

Remark

Step 4 is very expensive if e is big. So we only compute V_ℓ mod p for the p s.t. e is small.

Step 5: Computing the surjection $J_1(\ell)[\ell] \to V_\ell$

Let $\mathcal{S} \subset \mathbb{N}$ s.t. $\mathfrak{m}$ is generated by ℓ and $T_n - \tau(n)$ for $n \in \mathcal{S}$.
Let $A_n(X)$ be the characteristic polynomial of T_n on $S_2(\Gamma_1(\ell))$.
Write $A_n(X) \equiv B_n(X) \cdot (X - \tau(n))^{e_n} \mod \ell$, with $e_n \geq 1$ and $A_n(\tau(n)) \not\equiv 0 \mod \ell$.
Let $\pi_{\mathcal{S}} := \prod_{n \in \mathcal{S}} B_n(T_n)$, then for all $P \in J_1(\ell)[\ell]$ and all $n \in S$:

$$(T_n - \tau(n))^{e_n} \pi_{\mathcal{S}}(P) = 0.$$

If $\pi_{\mathcal{S}}(P) \neq 0$ then there are $d_n < e_n$ s.t.

$$Q := \left(\prod_{n \in \mathcal{S}} (T_n - \tau(n))^{d_n} \right) \pi_{\mathcal{S}}(P)$$

is a nonzero point in $V_\ell = J_1(\ell)[\ell] \cap \bigcap_{n \in \mathcal{S}} \ker T_n - \tau(n)$.

Speeding up step 4

In step 4 we have to multiply a $P \in J_1(\ell)(\mathbb{F}_{p^e})$ by a huge integer ($\approx p^{eg}$). But in fact $J_1(\ell)$ is isogenous to $\prod_f A_f$ where f runs through Galois conj. classes of newforms of $S_2(\Gamma_1(\ell))$ and $A_f \subset J_1(\ell)$ is the factor corresponding to f.
Instead of computing $(\ell^{-v_\ell N} N)P$ where $N := \#J_1(\ell)(\mathbb{F}_{p^e}))$ we can instead compute $(\ell^{-v_\ell N'} N')T(P)$ where $T \in \mathbb{T}$ s.t. $T(J_1(\ell)) \subset A_f$ and $N := \#A_f(\mathbb{F}_{p^e}))$. Advantage: $N' \approx p^{e \dim A_f}$

Comparing dimensions for $f \equiv \Delta \mod \ell$

Level ℓ	13	17	19	29	31	37	41	43	47	53	59
$\dim J_1(\ell)$	2	5	7	22	26	40	51	57	70	92	117
$\dim A_{f_\ell}$	2	4	6	12	4	18	6	36	66	48	112

Special case $\ell \equiv 1 \mod 10$

Let $f \equiv 1 \mod \ell$ be a newform and χ be the character associated to f then the characteristic polynomial of Frob_p on V_ℓ is $X^2 - \tau(p) + \chi(p)p = X^2 - \tau(p) + p^{11}$. In other words $\chi(p) \equiv p^10 \mod \ell$, in particular if $\ell \equiv 1 \mod 10$ then $\chi(\langle d^{(l-1)/10} \rangle) \equiv d^{(l-1)} = 1 \mod \ell$. This shows that $\langle d^{(l-1)/10} \rangle f = \chi(\langle d^{(l-1)/10} \rangle) \equiv d^{(l-1)} f = f$. So V_l can also be found in $J_H(\ell)$, the jacobian of $X_1(\ell)/\langle d^{(l-1)/10} \rangle$ with d a generator of $\mathbb{F}_\ell^*$.

Comparing dimensions for $f \equiv \Delta \mod \ell$

Level ℓ	13	17	19	29	31	37	41	43	47	53	59
dim $J_1(\ell)$	2	5	7	22	26	40	51	57	70	92	117
dim A_{f_ℓ}	2	4	6	12	4	18	6	36	66	48	112
dim $J_H(\ell)$					6		11				

How to compute in T_p in $J_1(\ell)(\mathbb{F}_q)$

Computations are $J_1(\ell)(\mathbb{F}_q)$ done using the identification:

$$J_1(\ell)(\mathbb{F}_q) = \mathrm{Cl}^0\mathbb{F}_q(X_1(\ell))$$

and using magma's function field+class group capabilities.
There exist explicit algebraic model's

$$\mathbb{F}_q(X_1(\ell)) \cong \mathbb{F}_q(x)[y]/(f_\ell(x, y))$$

that also allows you to go back and fort between zeros of $f_\ell(x, y)$ and pairs (E, P).
To compute $T_p(x)$ for $D \in \mathrm{Cl}^0\mathbb{F}_q(X_1(\ell))$, we write $D = \sum n_i Q_i$ with Q_i places of $F_q(X_1(\ell))$, find the pair (E_i, P_i) corresponding to each Q_i) and compute $T_p(E_i, P_i) = \sum_G (E_i/G, P_i \mod G)$

T. and V. Dokchitser's method for finding frobenius

Let $P(t) \in \mathbb{Z}[t]$ be a polynomial with splitting field L, denote it's roots by $a_1, \dots, a_n$. For $C \subset \mathrm{Gal}(L/\mathbb{Q})$ a conjugacy class and $h \in \mathbb{Q}[X]$ define

$$\Gamma_C^h(t) := \prod_{\sigma \in C} (t - \sum_i h(a_i)\sigma(a_i)) \in \mathbb{Q}[X]$$

Theorem

- The set of h with $\deg h \leq n-1$ s.t. for all C, C' : $\mathrm{Res}(\Gamma_C^h, \Gamma_{C'}^h) \neq 0$ is open and Zarisky dense in the polynomials of $\deg \leq n-1$.
- For p not deviding any of the resultants $\mathrm{Res}(\Gamma_C^h, \Gamma_{C'}^h)$ and also not dividing the leading coefficient of $P(t)$ one has:

$$\mathrm{Frob}_p \in C \Leftrightarrow \Gamma_C(\mathrm{Tr}_{\mathbb{F}_p[t]/(P(t))} h(t) t^p) \equiv 0 \mod p$$

Equation

An equation[2] for the projective representation of Δ mod 31 :

$$x^{32}-4x^{31}-155x^{28}+713x^{27}-2480x^{26}+9300x^{25}-5921x^{24}+24707x^{23}+127410x^{22}-646195x^{21}+747906x^{20}-7527575x^{19}+4369791x^{18}-28954961x^{17}-40645681x^{16}+66421685x^{15}-448568729x^{14}+751001257x^{13}-1820871490x^{12}+2531110165x^{11}-4120267319x^{10}+4554764528x^{9}-5462615927x^{8}+4607500922x^{7}-4062352344x^{6}+2380573824x^{5}-1492309000x^{4}+521018178x^{3}-201167463x^{2}+20505628x-1261963$$

[2] Thanks to Mark van Hoeij for finding this smaller equation, the equation produced by the algorithm had coefficients of 700 digits!

Future work

- Operation in $J_1(\ell)(\mathbb{F}_q)$ is very slow (uing Heß's algorithm which is in magma), it would be interesting to know whether using Khuri-Makdisi's algorithm will be faster.
- Computing the points in V_ℓ modulo a single prime p is possible if e is very small using the current implementation for $\ell = 29$ and $\ell = 41$. But this takes 6 hours for $\ell = 41$ so probably something smarter is needed to reconstruct the entire polynomial. Maybe p-adically lifting these points will be faster then trying a lot of different primes.

Future work

How to reduce $P(t)$?

The polynomial $P(t)$ has degree $\ell^2 - 1$ and huge coefficients as well. The calculation of $\Gamma_C(t)$ for all the conjugacy classes $C \subset \mathrm{GL}_2(\mathbb{F}_\ell)$, not only took a lot of time but also a lot of memory! Actually the coefficients of $\Gamma_C(t)$ are much bigger then those of $P(t)$. It becomes a bottleneck when dealing with higher levels. So a good algorithm for reducing the size of $P(t)$ (after we have computed it) will be usefull.

The Magma code of our implementation can be downloaded from:

http://faculty.math.tsinghua.edu.cn/~lsyin/publication.htm

The end!

$$\tau(10^{1000} + 1357) = \pm 18 \mod 31$$

Thank you very much!