Computation of Gal. repns ass. to modular forms: numerical part using finite fields, after J-M. Couveignes.

Reference: Linearizing torsion classes in the Picard group of algebraic curves over finite fields; arxiv.

Thm 2. $\exists$ probabilistic (Las Vegas) algorithm that on input l and $p \geq 7$, $p \neq l$, computes $V_l := \bigcap_{n \geq 1} \ker(T_n - \tau(n), J_1(l)(\overline{\mathbb{F}}_p)[l])$ (2 dim. $\mathbb{F}_l$-vect-space).

The answer is given as a list of l^2 degree g_l effective divisors on $X_1(5l)_{\overline{\mathbb{F}}_p}$. The expected running time is polynomial in p and l.

Remark. 1. Essential for the result (Edixh, Couveignes, R. de Jong, F. Merkl) (on arxiv) on computation of $\overline{\rho}_{\Delta, l}$ in time pol. in l.

2. Same works for all modular forms of level 1.

(I simplify it a little bit)

Thm 1. $\exists$ probabilistic Monte-Carlo algorithm that on input

1. a plane curve $C \subset \mathbb{P}^2_{\mathbb{F}_q}$, abs. irr. and reduced, of degree d,
2. the smooth model $\mathcal{X}$ of C, of genus g,
3. a rational point $O \in \mathcal{X}(\mathbb{F}_q)$,
4. a prime $l \neq p | q$ and $n = l^k$,
5. the zeta function of $\mathcal{X}$ (i.e. the char. pol. of Frob_q of $J := \mathrm{jac}(\mathcal{X})$),

computes a set $g_1, \ldots, g_w$ in $J(\mathbb{F}_q)$ s.t. $J(\mathbb{F}_q)[l^k] = \langle g_1 \rangle \oplus \ldots \oplus \langle g_w \rangle$.

Each g_i is given as $[G_i - g.O]$ with G_i an effective divisor on $\mathcal{X}$.

The algorithm runs in prob. pol. time in d, g, $\log q$, l^k. Its output is correct with probability $\geq 1/2$. Otherwise, it may return nothing or a strict subgroup of $J(\mathbb{F}_q)[l^k]$.

For D of degree 0 on $\mathcal{X}$ with $[D] \in J(\mathbb{F}_q)[l^k]$ one can compute $a_i \in \mathbb{Z}$ s.t. $[D] = \sum_i a_i g_i$ in time polynomial in d, $\log q$, l^k and $\deg(D^+)$ (where $D = D^+ - D^-$ with D^+, D^- effective).

More information about the statement of the theorem.

1. $C = V(F)$, $F \in \mathbb{F}_q[X,Y,Z]_d$, F abs. irreducible.
2. Let $\mathcal{X} \xrightarrow{\pi} C$ be the normalisation map, it is an isomorphism outside C^{sing}.
   $\forall c \in C^{sing}$ (closed point), one is given $\pi^{-1}\{c\}$ as a labeled set, and, $\forall x \in \pi^{-1}\{c\}$, a uniformiser t_x in $\mathcal{O}_{\mathcal{X},x}$, and algorithms to compute the images of X/Z and Y/Z (or of the coordinates of another affine chart) in $\mathcal{O}_{\mathcal{X},x}/(t_x)^m = \mathbb{F}_{q^{d_x}}[T]/(T^m)$ in time polynomial in $\log q$, d, m. (note: $d_x \leq \frac{(d-1)(d-2)}{2}$)
3. $\mathcal{O}_C \rightarrowtail \pi_*\mathcal{O}_{\mathcal{X}} \twoheadrightarrow Q$ $\quad Q \rightarrowtail H^1(C, \mathcal{O}_C) \twoheadrightarrow H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$, $g + \underbrace{\dim_{\mathbb{F}_q} Q}_{\delta} = \frac{1}{2}(d-1)(d-2)$
   $\mathcal{O}_{\mathcal{X}}(-\underline{c}) :=$ largest $\mathcal{O}_{\mathcal{X}}$-submod. of $\mathcal{O}_C$, then $\deg(\underline{c}) = 2\delta$, (plane sing's are Gorenstein).
4. Let $\chi \in \mathbb{Z}[T]$ be the char. pol. of Frob_q on J.
   Note that χ determines $\# J(\mathbb{F}_q)$, but not necessarily $\# J(\mathbb{F}_q)[\ell^k]$.
   This explains that the algorithm is not better than Monte-Carlo; the algorithm in Thm 2 is Las Vegas because we know that there we are dealing with ℓ^2 elements.

The case of $X_1(\ell)$ and $X_1(5\ell)$.

For ℓ given, one can provide input for Thm 1 in time polynomial in ℓ, $\log q$ and p. Need p for χ (use modular symbols for T_p). We have $d = \ell^2 - 1$, $g = (\ell-2)^2$. See §9–10.

Thm 1 $\Rightarrow$ Thm 2. Thm 1 gives an $\mathbb{F}_\ell$-basis of $J(\mathbb{F}_q)[\ell]$ (take $q = p^r$ s.t. $V_\ell \subset J(\mathbb{F}_q)[\ell]$, e.g. $r = \# GL_2(\mathbb{F}_\ell) = (\ell^2-1)(\ell^2-\ell)$ suffices). Then compute the T_n, $1 \leq n < \ell^2$ on $J(\mathbb{F}_q)[\ell]$ and compute $\bigcap_{n<\ell^2} \ker(T_n - \tau(n))$.
Here we use that the basic operations in $J(\mathbb{F}_q)$ (+, correspondences..) can be done in time polynomial in d and $\log q$. See §3.

+: $[A - g\cdot 0] + [B - g\cdot 0]$: $\quad H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(A+B-\underline{c})) \subset \text{image}\left(\mathbb{F}_q[X,Y,Z]_{2d} \longrightarrow H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(2d))\right)$

(Brill-Noether?) $\quad 0 \neq f_1 \quad 0 \neq f_2 \in H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(2d - \underline{c} - R - g\cdot 0))$ $\quad [B - g\cdot 0]$

$(f_1) = A + B + \underline{c} + R \qquad (f_2) = \underline{c} + R + g\cdot 0 + D. \quad [D - g\cdot 0] = [A - g\cdot 0] +$

Now on the proof of Thm 1.

§4, lemma 8. $\exists$ a Monte-Carlo algorithm that on input $C/\mathbb{F}_q$, $\mathcal{X} \to C$ and $O \in \mathcal{X}(\mathbb{F}_q)$ gives, ~~ouse~~ with probability $\geq 1/2$, a sequence (α_i) in $J(\mathbb{F}_q)$ s.t. $\# J(\mathbb{F}_q)/\langle\langle \alpha_i \rangle\rangle \leq \max(48g, 24d, 720) =: \iota$ (iota) in time polynomial in d & $\log q$.

Remark: one may assume $q \geq 4g^2$ (if not, use that $\{D \mid D \geq 0, \deg D \leq 2\log_q(4g-2)\}$ generates $\mathrm{Pic}(\mathcal{X})$, or use that for proving theorem 1 one can replace q by a suitable power).

$r :=$ smallest prime $> 30, 2g-2, d$. $\quad \mathcal{P}(r,q) := \{$degree r points on $\mathcal{X}\}$

$\mathcal{X} \to \mathbb{P}^1_{\mathbb{F}_q}$ lin. projection. $\quad$ fibers of card. in $[0,d]$ $\downarrow$

$\mathcal{U}(r,q) := \{$degree r points on $\mathbb{A}^1_{\mathbb{F}_q}\}$ $= \{f \in \mathbb{F}_q[T] \mid f$ monic, irred. $\deg r\}$

In $\mathcal{U}(r,q)$ we can take random uniformly distributed points.

In $\mathcal{P}(r,q)$: take random element in fiber over random elmt. of $\mathcal{U}(r,q)$.

Gives a measure μ on $\mathcal{P}(r,q)$ s.t. $\frac{1}{d}\cdot$ unif. m. $\leq \mu \leq d\cdot$ unif. m.

$\mathcal{D}(r,q) := \{D$ on $\mathcal{X} \mid D \geq 0, \deg D = r\}$. $\quad \mathcal{P}(r,q) \subset \mathcal{D}(r,q) \xrightarrow{\text{fibers are } \mathbb{P}^{r-g}(\mathbb{F}_q)\text{'s}} J(\mathbb{F}_q)$

$\# \mathcal{P}(r,q) \approx q^r/r$, $\quad \# \mathcal{D}(r,q) \lessapprox q^{r-g}\cdot(\sqrt{q}+1)^{2g} = q^r\cdot\left(1+\frac{1}{\sqrt{q}}\right)^{2g} \underset{\text{bec. } q \geq 4g^2}{\leq} e\cdot q^r$

So: $\frac{1}{re}\cdot \#\mathcal{D}(r,q) \lessapprox \#\mathcal{P}(r,q) \leq \#\mathcal{D}(r,q)$

Consider some $J(\mathbb{F}_q) \xrightarrow{\varphi} G$ $\quad \#(\varphi\circ\zeta)^{-1}(0) = \frac{\#\mathcal{D}(r,q)}{\#G} \leq \frac{e\cdot q^r}{\#G}$

$\mathcal{P}(r,q) \underset{i}{\hookrightarrow} \mathcal{D}(r,q) \xrightarrow{\zeta} J(\mathbb{F}_q)$

hence: $\#\left((\varphi\circ\zeta\circ i)^{-1}(G - \{0\})\right) \gtrapprox \frac{q^r}{r} - \frac{e q^r}{\#G} = q^r\cdot\left(\frac{1}{r} - \frac{e}{\#G}\right)$

View $J(\overline{\mathbb{F}}_q)[\ell^{\cancel{k}\,\infty}]$ as $\mathbb{Z}[X]$-module, X acts as Frob_q.

Then $J(\overline{\mathbb{F}}_q)[\ell^{\cancel{k}\,\infty}] = \underbrace{J(\overline{\mathbb{F}}_q)[\ell^{\infty}][(X-1)^{\infty}]}_{=:\, G_1(\overline{\mathbb{F}}_q)[\ell^{\infty}]} \oplus \mathrm{rest}_1$

$= \underbrace{J(\overline{\mathbb{F}}_q)[\ell^{\infty}][(X-q)^{\infty}]}_{=:\, G_q(\overline{\mathbb{F}}_q)[\ell^{\infty}]} \oplus \mathrm{rest}_q$

$Q_k := q^{(\ell-1)\cdot \ell^{\gamma}\cdot \ell^{k-1}}$ where $\ell^{\gamma} \geq 2g$, γ minimal.

Then $G_1(\overline{\mathbb{F}}_q)[\ell^k] = G_1(\mathbb{F}_{Q_k})[\ell^k]$, and same for G_q.

One has
$$J(\mathbb{F}_{Q_k}) \twoheadrightarrow J(\mathbb{F}_{Q_k})[\ell^{\infty}] \twoheadrightarrow G_1(\mathbb{F}_{Q_k}) \twoheadrightarrow G_1(\mathbb{F}_{Q_k})[\ell^k]$$

index ≤ 2 · integer

suitable elmt. of $\mathbb{Z}[X]$ (Bezout-identity)

"Kummer map", given by suitable element in $\mathbb{Z}[X]$.

$\langle \gamma_1, \dots, \gamma_I \rangle \to \langle \alpha_1, \dots, \alpha_I \rangle$ index ≤ 2.

+ same for $G_q(\mathbb{F}_{Q_k})[\ell^k]$.
$\langle \beta_1, \dots, \beta_I \rangle$

Weil pairing: $G_1(\mathbb{F}_{Q_k})[\ell^k] \times G_q(\mathbb{F}_{Q_k})[\ell^k] \xrightarrow{\text{perfect}} \mu_{\ell^k}(\mathbb{F}_{Q_k}) \xrightarrow{\sim} \mathbb{Z}/\ell^k\mathbb{Z}$.

<u>Note</u>: $\langle \alpha_1, \dots, \alpha_I \rangle \supset G_1(\mathbb{F}_{Q_k})[\ell^{k-\delta}]$, $\ell^{\delta} \geq 2$, δ minimal.

$\langle \beta_1, \dots, \beta_I \rangle \supset G_q(\mathbb{F}_{Q_k})[\ell^{k-\delta}]$.

$$\begin{tikzcd} R' \arrow[dr] & & \\ R \arrow[u, hook] \arrow[r, hook] \arrow[u, bend left, "\text{index} \leq 2"'] & \mathbb{Z}^I \arrow[r, "\alpha"] \arrow[dr] & G_1(\mathbb{F}_{Q_k})[\ell^k] \arrow[d, "\beta"] \\ & & (\mathbb{Z}/\ell^k\mathbb{Z})^I \end{tikzcd}$$

R' computed from the $\beta_i(\alpha_j)$,
R from R' by "black box groups".

~~[illegible]~~ This gives $\langle \alpha_1, \dots, \alpha_I \rangle \xleftarrow{\sim} \bigoplus_i \mathbb{Z}/\ell^{e_i}\mathbb{Z}$,
then get $G_1(\mathbb{F}_{Q_k})[\ell^{k-\delta}]$, $J(\mathbb{F}_q)[\ell^{k-\delta}]$. $\boxtimes$