Wat gebeurt er als het aantal punten polynomiaal is in q?

Theo van den Bogaart*

June 21, 2004

Dit is ‘work in progress’ en er zitten nog wat ‘open problemen’ in. Bas heeft de stelling en het idee van het bewijs bedacht en nu proberen we samen het af te maken.

Laten we om te beginnen de vraag even vaag formuleren en tevens aangeven hoe het met het seminarium samenhangt.

Zij $X/\mathbb{Z}$ een meetkundig object. We kunnen punten tellen over eindige lichamen. We nemen aan dat er een polynoom bestaat $P(X) = \sum P_i x^i \in \mathbb{Q}[x]$ waarvoor $\#X(\mathbb{F}_q) = P(q)$ voor alle priemmachten (geen vaste p en ook voor $l \mid q$). Door cohomologie kunnen we een l-adische Galoisrepresentatie erbij maken; welke is dit?

Hier zijn enkele voorbeelden:

(i) $\mathbb{P}^n$: Het aantal punten over $\mathbb{F}_q$ is $q^n + q^{n-1} + \cdots + 1$. Men heeft ook

$$H^{2i}(\mathbb{P}^n_{\overline{\mathbb{Q}}}, \mathbb{Q}_l) \cong \mathbb{Q}_l(-i)$$

voor $0 \le i \le n$ en

$$H^{\text{anders}}(\mathbb{P}^n_{\overline{\mathbb{Q}}}, \mathbb{Q}_l) = 0.$$

(Cohomologie is hier altijd étale cohomologie.)

(ii) Moduli ruimte van gladde geslacht g krommen met daarop n geordende punten: $\mathcal{M}_{g,n}$. Men kijkt naar de compactificatie $\overline{\mathcal{M}_{g,n}}$ (zie Knudsen). Het is de moduli ruimte van *stabiele* geslacht g krommen met n geordende punten.

Dit zijn geen schema’s, maar stacks. Het Nederlands voor stack is *schelf* (terminologie van v/d Kallen).

*Notes typed by Gabor Wiese

(a) Subvoorbeeld: $\mathcal{M}_{1,1}(\mathbb{F}_q)$ categorie met objecten elliptische krommen over $\mathbb{F}_q$ en morfismen de isomorfismen over $\mathbb{F}_q$ van deze elliptische krommen.

Wat is het aantal punten op een schelf?

$$\#\mathcal{M}_{1,1}(\mathbb{F}_q) := \sum_{c \in [\mathcal{M}_{1,1}(\mathbb{F}_q)/\cong]} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(c)}$$

en dit is in dit geval gelijk aan q, want:

Opgave: Geef $A = \mathrm{Aut}_{\overline{\mathbb{F}_q}}(c)$ een A-actie zodat de banen de $\mathbb{F}_q$-isomorfieklassen zijn met dezelfde j-invariant als c en de stabilisator van c' gelijk is aan $\mathrm{Aut}_{\mathbb{F}_q}(c')$. Gebruik nu de banenformule

$$\#A = \sum_{\text{banen}} \frac{\#A}{\#\mathrm{Stab}}.$$

(Dit bewijs maakt (bijna) geen gebruik van dat we elliptische krommen hebben: alles kan veel algemener.)

Vraag in het algemeen.

$$\overline{\mathcal{M}_{g,n}} \to \overline{M_{g,n}},$$

waar de rechterkant de grove moduliruimte is. Men vindt dat het aantal punten over $\mathbb{F}_q$ hetzelfde is aan beide kanten.

Dit geeft ook $\#\overline{\mathcal{M}_{1,1}} = q + 1$.

Ook geldt

$$H^*(\overline{\mathcal{M}_{g,n}}, \mathbb{Q}_l) \cong H^*(\overline{M_{g,n}}, \mathbb{Q}_l).$$

Dit kan men uit de Leray spectraalrij halen.

Nu weten we dus ook

$$H^*(\overline{\mathcal{M}_{1,1}}, \mathbb{Q}_l) = H^*(\mathbb{P}^1, \mathbb{Q}_l).$$

Omdat de grove moduliruimten er vaak niet zo mooi uitzien, kijken we vanaf nu alleen nog maar naar de fijne modulischelven.

Onze motivatie is een vraag van Carel Faber. Hij heeft voorbeelden van $(g, n), g \geq 2$ (e.g. $(3, 5)$) zodat het aantal punten van $\overline{\mathcal{M}_{g,n}}$ polynomiaal is in q. Wat kan men zeggen over de cohomologie in deze gevallen?

Algemene voorwaarden vanaf nu: $X/\mathbb{Z}$ propere gladde DM schelf. Helaas blijkt er ook nog een extra voorwaarde nodig; zie beneden.

Nu een vergelijk. Aan de ene kant hebben we gladde propere schema's over $\mathbb{Z}$. In dat geval zijn bekend:

- l-adische representaties zijn onvertakt buiten l en cristalijn in l.
- Analogon van de Riemann hypothese (Deligne).
- Sporenformule. (Details beneden.)
- Poincare dualiteit.
- Propere basiswissel.
- Gladde basiswissel.
- De Rham en cristalijne 'vermoedens' (bewezen door Faltings).

Aan de andere kant bekijken we gladde propere schelven over $\mathbb{Z}$.

- We weten niet of l-adische representaties onvertakt buiten l en crystalline in l zijn..
- Het analogon van de Riemann hypothese lijkt niet bekend te zijn.
- Sporenformule bewezen door Behrend.
- Poincare dualiteit bewezen door Lafforgue.
- Propere basiswissel is bekend.
- Is gladde basiswissel bekend?
- De Rham en crystalline vermoedens zijn blijkbaar niet bekend; we kunnen zonder, maar er zijn dan geen conclusies over Hodge-structuren te trekken.

Om de eerste twee items te ondervangen, volgt hier een extra eis: Voor elk priemgetal p bestaat er een generiek eindige overdekking van $X_{\mathbb{Q}_p}$ door een glad en proper schema die lift naar een glad proper schema over $\mathbb{Z}_p$.

We hebben $Y_{\mathbb{Q}_p} \twoheadrightarrow X_{\mathbb{Q}_p}$. Wegens Poincare dualiteit krijgen we

$$(*) \qquad H^*(X_{\mathbb{Q}_p}) \hookrightarrow H^*(Y_{\mathbb{Q}_p}).$$

Zo krijgen we ook voor ons schelf dat zijn l-adische cohomologie onvertakt is buiten l en cristal-ijn in l.

Deze extra eis is waar voor $\mathcal{M}_{g,n}$ (Pikaart en Boggi).

Sporenformule van Behrend als $l \nmid q$:

$$\#X(\mathbb{F}_q) = \sum_i (-1)^i \operatorname{Tr}(F_q | H^i(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)).$$

Wij willen $X_{\overline{\mathbb{F}_q}}$ vervangen door $X_{\overline{\mathbb{Q}_p}}$. Dat is gladde basiswissel en we nemen aan dat dit gewoon werkt.

Zijn $\alpha_{i,1}, \ldots, \alpha_{i,d}$ de wortels van de karakteristieke polynoom van F_q op H^i. We hebben:

(i) Voor alle $r \geq 1$ geldt:

$$\sum P_i p^{ri} = \sum_i (-1)^i \sum_{1 \leq j \leq d_i} \alpha_{i,j}^r.$$

$(q = p^r)$

(ii) $|\alpha_{i,j}| = p^{i/2}$. Dit volgt ook uit $(*)$.

Lemma 1 *Stel dat (i) en (ii) gelden, dan kunnen we concluderen:*

(a) $d_{\text{oneven}} = 0$,

(b) $d_{2i} = P_i$ *en*

(c) $\alpha_{2i,j} = p^i$.

Het bewijs is analytisch en niet moeilijk; het werkt bovendien voor ieder willekeurig reëel getal $p > 1$.

Een opmerking. De eis aan de polynomialiteit kan worden verzwakt door:

> Zij S een verzameling priemgetallen van Dirichlet dichtheid 1, en voor elk $p \in S$ zij een positief getal n_p gegeven. Dan is het voldoende dat geldt $\#X(\mathbb{F}_q) = P(q)$ voor q alle machten van p_p^n voor $p \in S$.

Met Chebotarev krijgen we dan $\#X(\mathbb{F}_q) = P(q)$ voor alle q en:

"Stelling" 1 *We hebben*

$$H^{\text{oneven}} = 0,$$

de P_i zijn gehele niet-negatieve getallen,

$$(H^{2i})^{ss} \cong \mathbb{Q}_l(-i)^{P_i}$$

en de H^{2i} zijn onvertakt buiten l en crystalline in l.

We gaan nog een stap verder:

"Stelling" 2 *Er geldt zelfs dat* $H^{2i} \cong \mathbb{Q}_l(i)^{P_i}$.

We mogen aannemen na twisten dat $[H^{2i}]^{\mathrm{ss}} \cong \mathbb{Q}_l^{P_i}$. We zullen zien dat deze representatie overal onvertakt is en omdat we over $\mathbb{Q}$ werken volgt dan de stelling.

Men heeft de Fontaine functor D_{crys} van crystalline representaties van $G_{\mathbb{Q}_l}$ naar gefilterde zwak toelaatbare ϕ-modulen. Deze geeft een equivalentie van abelse categoriën.

We geven het idee voor $P_i = 2$. Wij hebben de exacte rij van gefilterde ϕ-modulen:

$$\mathbb{Q}_l \hookrightarrow D_{\mathrm{crys}}(H^{2i}) =: E \twoheadrightarrow \mathbb{Q}_l.$$

Dus

$$\mathrm{Fil}^i \, \mathbb{Q}_l \hookrightarrow \mathrm{Fil}^i \, E \twoheadrightarrow \mathrm{Fil}^i \, \mathbb{Q}_l.$$

En de term aan de linkerkant is $\mathbb{Q}_l$ als $i \leq 0$ en 0 als $i > 0$. De term in het midden is gelijk aan E als $i \leq 0$ en ook 0 als $i > 0$. Zo'n moduul hoort bij een onvertakte $G_{\mathbb{Q}_l}$-representatie.