Panoramas & Synthèses
60, 2023, p. 113–144

CURVES OVER FINITE FIELDS AND MODULI SPACES

by

Gerard van der Geer

Abstract. **–** This survey deals with moduli aspects of curves over finite fields. We discuss counting points on moduli spaces of curves over finite fields. Formulas for the number of points on such moduli spaces lead to modular forms. In this way counting curves and their points over finite fields offers a way to obtain information on the traces of Hecke operators on modular forms. We also discuss stratifications on moduli spaces of curves and their relevance for curves over finite fields.

Résumé **(Courbes sur les corps finis et espaces de modules).** **–** Cet article traite de certains aspects des espaces de modules de courbes algébriques sur un corps fini. Nous y discutons le comptage de points sur de tels espaces. Les formules pour le nombre de points sur ces espaces de modules nous conduisent vers des formes modulaires. De cette façon, le comptage des courbes et de leurs points sur les corps finis offre une manière d'obtenir des informations sur les traces des opérateurs de Hecke sur certains espaces de formes modulaires. Nous discutons également certaines stratifications des espaces de modules des courbes et de leur pertinence pour les courbes sur les corps finis.

1. Introduction

This survey deals with moduli aspects of curves over finite fields. A large part of the research on curves in the last century has been on the moduli of curves. The foundational results on moduli spaces in the 1960s by Grothendieck and Mumford cleared the way for a study of their properties. Before this it was difficult to study these moduli spaces in positive characteristic.

An attractive aspect of studying curves over a finite field is that one can obtain a lot of information about them by just counting their rational points over the given finite field and its extension fields. Another nice aspect of studying curves over a given finite field is that if you fix the genus there are only finitely many of them up

2010 Mathematics Subject Classification. **–** 11G20, 14H10, 14G35, 11F03, 14H45, 14J15.
Key words and phrases. **–** Algebraic curves over finite fields, modular forms, moduli spaces of curves.

to isomorphism over the given finite field. This suggests that we count these. The counting can be done in various ways; for example, one can also count curves defined over a finite field $\mathbb{F}_q$ of cardinality q together with an n-tuple of $\mathbb{F}_q$-rational points.

Doing the counting for the case of curves of genus one leads very quickly to the topic of modular forms and their Hecke eigenvalues. The reason is that counting points of a variety over a finite field yields information on the cohomology of that variety. In the case at hand the variety is a moduli space and modular forms enter naturally in the description of the cohomology of moduli spaces. Thus we can use the counting of points on curves over finite fields of cardinality a power of a prime p to study the cohomology of moduli spaces, and to study the traces of Hecke operators T_{p^n} on spaces of modular forms, and also Hecke eigenvalues of modular forms. In this way counting points on curves over finite fields becomes a heuristic tool in the exploration of uncharted terrain.

The interesting thing is that this connection can also be used in both directions. Knowing traces of Hecke operators provides us with formulas for the number of rational points on moduli spaces over finite fields.

Moduli of curves admit several stratifications. Examples of these are the stratification by automorphism group or by gonality. Apart from these that apply to all characteristics, the moduli of curves in positive characteristic possess stratifications that are special for given positive characteristic. These stratifications can be quite relevant for curves over finite fields. There has been a flurry of activity on these stratifications. We discuss just a few aspects of these stratifications and point to several open questions.

Acknowledgement

This survey covers mainly developments where I participated or contributed. I owe a lot to my collaborators in our joint projects through these years and enjoyed enormously the pleasant and fruitful cooperation. Thanks are due to Marcel van der Vlugt, Torsten Ekedahl, Carel Faber and Jonas Bergström.

2. Moduli Spaces

To begin at the beginning, assume that we fix non-negative integers g and n with $2g-2+n \geq 1$. A smooth projective geometrically irreducible curve C of genus g together with n distinct labeled points $P_1, \ldots, P_n$ is called an n-pointed curve of genus g. It is called stable if the group of automorphisms of C fixing $P_1, \ldots, P_n$ is finite. Here a morphism of $(C, P_1, \ldots, P_n)$ to $(D, Q_1, \ldots, Q_n)$ is a morphism $\varphi : C \to D$ with $\varphi(P_i) = Q_i$ for $i = 1, \ldots, n$. The most basic fact here, due to Mumford, is the existence for $2g-2+n \geq 1$ of a moduli space $\mathcal{M}_{g,n}$ of stable n-pointed curves of genus g, [**51**]. It is an irreducible Deligne-Mumford stack of dimension $3g-3+n$ defined over $\mathbb{Z}$. That we have to deal with stacks and not just with varieties, is due to the fact that curves can have non-trivial automorphism groups.

The moduli spaces $\mathcal{M}_{g,n}$ are in general not complete since curves can degenerate. To compactify these one introduces the notion of a nodal n-pointed curve of genus g; it is a reduced connected proper curve C with finitely many singular points which are ordinary double points such that C has arithmetic genus g and non-singular points $P_1, \ldots, P_n$. Again we call such a curve stable if the automorphism group of C fixing $P_1, \ldots, P_n$ is finite. The basic existence result on moduli spaces just mentioned can be strengthened to the fact that there exists a moduli space $\overline{\mathcal{M}}_{g,n}$, defined over $\mathbb{Z}$, of stable nodal n-pointed curves of genus g. It is again a Deligne-Mumford stack defined over $\mathbb{Z}$. The moduli of non-singular stable n-pointed curves of genus g form an open dense part $\mathcal{M}_{g,n}$ of $\overline{\mathcal{M}}_{g,n}$. This cornerstone theorem is due to Deligne and Mumford ([**20**]) and was established in 1969.

For $g = 1$ we need $n \geq 1$ and for $n = 1$ we find the moduli space $\mathcal{M}_{1,1}$ of elliptic curves. For $g \geq 2$ we can have $n = 0$ and we then just write $\mathcal{M}_g$ and $\overline{\mathcal{M}}_g$ for $\mathcal{M}_{g,0}$ and $\overline{\mathcal{M}}_{g,0}$.

Since the moduli space $\mathcal{M}_{g,n}$ is defined over $\mathbb{Z}$ we can consider its fiber $\mathcal{M}_{g,n} \otimes \mathbb{F}_p$ in characteristic p. These are the moduli spaces that here we are interested in. We also have their compactifications $\overline{\mathcal{M}}_{g,n} \otimes \mathbb{F}_p$.

If $(C, P_1, \ldots, P_n)$ is a (smooth) projective curve defined over a finite field $\mathbb{F}_q$, that is, $P_i \in C(\mathbb{F}_q)$ for $i = 1, \ldots, n$, then it defines a $\mathbb{F}_q$-valued point $[C, P_1, \ldots, P_n]$ of $\mathcal{M}_{g,n}$. But the point of the moduli space may a priori be defined over a smaller field. In general if $(C, P_1, \ldots, P_n)$ is defined over a field L that is a Galois extension of the field K with Galois group $G_{L/K}$, then we can view $(C, P_1, \ldots, P_n)$ as a scheme over K and we have an exact sequence

$$1 \to \mathrm{Aut}_L((C, P_1, \ldots, P_n)) \to \mathrm{Aut}_K((C, P_1, \ldots, P_n)) \xrightarrow{\alpha} G_{L/K}.$$

Then we have:

Lemma 2.1. – *The moduli point $[C, P_1, \ldots, P_n]$ can be defined over K if and only if α is surjective; the stable n-pointed curve $(C, P_1, \ldots, P_n)$ can be defined over K if and only if α admits a lift.*

The second statement is (a variation of) a well-known theorem of Weil [**73**, Thm 1]. In particular, since in our case of finite fields we may restrict to the case where $G_{L/K}$ is a cyclic group, we see that a $\mathbb{F}_q$-valued point of $\mathcal{M}_{g,n} \otimes \mathbb{F}_p$ can be represented by a n-pointed curve defined over $\mathbb{F}_q$.

Thus we can count the number of $\mathbb{F}_q$-valued points of $\mathcal{M}_{g,n}$. But here the stacky character of the moduli space comes into play. This stacky aspect means that when we count we have to take into account the automorphisms of our objects. For example, when dealing with $\mathcal{M}_{1,1}$, the moduli of elliptic curves, we have

$$\#\,\mathcal{M}_{1,1}(\mathbb{F}_q) = \sum_E \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)},$$

where the sum is over all elliptic curves $E = (C, P_1)$ defined over $\mathbb{F}_q$ up to isomorphism over $\mathbb{F}_q$.

In the case at hand we find $\#\mathcal{M}_{1,1}(\mathbb{F}_q) = q$. Indeed, there are q possibilities for the j-invariant of an elliptic curve over $\mathbb{F}_q$. The justification for this is that there is another type of moduli space, the coarse moduli space $M_{1,1}$, which is a scheme with the property that its k-valued points for an algebraically closed field k correspond bijectively to the k-isomorphism classes of elliptic curves; this is the j-line, where j refers to the famous j-invariant of elliptic curves. For each value of $j \in \mathbb{F}_q$ we might have several $\mathbb{F}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$, but they contribute in total 1 in the sum. In fact, there is the following lemma, see [**34**, Prop. 5.1] for a proof.

Lemma 2.2. – *Let C be a stable curve defined over $\mathbb{F}_q$. Then we have*

$$\sum_{C'} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(C')} = 1,$$

where the sum is over representatives C' of the $\mathbb{F}_q$-isomorphism classes contained in the $\overline{\mathbb{F}}_q$-isomorphism class of C.

We thus can ask for $\#\mathcal{M}_g(\mathbb{F}_q)$ for $g \geq 2$. To find this number we can make a list of all isomorphism classes of curves of the given genus g and determine for each curve in the list the order of the automorphism group.

This leads immediately to the question how to find all isomorphism classes and how to calculate the automorphism groups. Is the answer always a polynomial in q ? We will deal with these questions in the next sections.

Determining the automorphism group of a curve can be difficult. One remark is that one can avoid calculating the order of the automorphism groups by considering a family of curves in normal form whose generic member has no non-trivial automorphisms such that this family is a finite cover of the moduli space. Then we count in this family and divide by the degree of the cover.

Other moduli spaces that enter here are the moduli spaces of principally polarized abelian varieties of a given dimension g. These appear if we study curves via their Jacobians. Let $\mathcal{A}_g$ be the moduli space of principally polarized abelian varieties of dimension g. This is again an irreducible Deligne-Mumford stack defined over $\mathbb{Z}$. By associating to a curve its Jacobian we obtain a map of stacks for $g \geq 2$, the Torelli map,

$$t = t_g : \mathcal{M}_g \to \mathcal{A}_g, \quad [C] \mapsto [\mathrm{Jac}(C)]$$

and $t_1 : \mathcal{M}_{1,1} \xrightarrow{\sim} \mathcal{A}_1$. Note that the relative dimension of $\mathcal{A}_g$ over $\mathbb{Z}$ is $g(g+1)/2$ and that of $\mathcal{M}_g$ is $3g-3$ and the codimension of the image is $(g-2)(g-3)/2$ for $g \geq 2$. For $g = 2$ the map t_2 is an embedding of $\mathcal{M}_2$ as an open part of $\mathcal{A}_2$. But for $g \geq 3$ the map t_g is of stacky degree 2 onto its image, due to the fact that every abelian variety has an automorphism of order 2, while the generic curve has no non-trivial automorphism.

3. Counting points of $\mathcal{M}_{g,n}$ over finite fields

The first case deals with the moduli spaces $\mathcal{M}_{0,n}$ of stable n-pointed smooth curves of genus 0. This implies $n \geq 3$. The coarse moduli space $M_{0,3}$ equals one point and the coarse moduli space $M_{0,4}$ equals $\mathbb{P}^1 - \{0, 1, \infty\}$. For $n \geq 3$ we have the formula

$$\#\mathcal{M}_{0,n}(\mathbb{F}_q) = \prod_{i=2}^{n-2}(q-i),$$

settling the case $g = 0$.

For $g = 1$ we have $\mathcal{M}_{1,1} = \mathcal{A}_1$ and we find $\#\mathcal{M}_{1,1}(\mathbb{F}_q) = q$ as observed above. Since we know normal forms for elliptic curves we can write down a list of all isomorphism classes over $\mathbb{F}_q$. For example, if the characteristic is not 2, we can write every elliptic curve defined over $\mathbb{F}_q$ as $y^2 = f$ with $f \in \mathbb{F}_q[x]$ of degree 3 with non-vanishing discriminant. We find for $q = 3$ the following list of isomorphism classes of elliptic curves over $\mathbb{F}_3$. The first column gives the polynomial f defining the curve $y^2 = f$. The last column, that gives the j-invariants, illustrates Lemma 2.2.

f	$\#C(\mathbb{F}_3)$	$1/\#\mathrm{Aut}_{\mathbb{F}_3}(C)$	j
x^3+x^2+1	6	1/2	−1
x^3-x^2-1	2	1/2	−1
x^3+x^2-1	3	1/2	1
x^3-x^2+1	5	1/2	1
x^3+x	4	1/2	0
x^3-x	4	1/6	0
x^3-x+1	7	1/6	0
x^3-x-1	1	1/6	0

We deduce from this table the frequency list

m	1	2	3	4	5	6	7
freq	1/6	1/2	1/2	2/3	1/2	1/2	1/6

where the frequency for given $\#C(k) = m$ is obtained by adding the contributions $1/\#\mathrm{Aut}_k(C)$.

Given this frequency list we know $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ for this value of q and all n. Indeed, using the map $\mathcal{M}_{1,n} \to \mathcal{M}_{1,1}$ we have

$$\#\mathcal{M}_{1,n}(\mathbb{F}_q) = \sum_m \mathrm{freq}(m)\binom{m-1}{n-1}(n-1)!$$

Interpolating the answers for various q one finds experimentally for low values

n	$\#\mathcal{M}_{1,n}(\mathbb{F}_q)$
1	q
2	q^2
3	q^3-1
4	$q^4-q^2-3\,q+3$
5	$q^5-5\,q^3-q^2+15\,q-12$
6	$q^6-15\,q^4+25\,q^3+19\,q^2-80\,q+60$
7	$q^7-35\,q^5+125\,q^4-126\,q^3-155\,q^2+490\,q-360$

Notice that the degree in q is in accordance with the fact that $\dim \mathcal{M}_{1,n} = n$. One may continue and find

$$\#\mathcal{M}_{1,10}(\mathbb{F}_q) = q^{10} - 210\,q^8 + 2274\,q^7 - 11655\,q^6 + 34944\,q^5 - 62140\,q^4 + 42126\,q^3 + 89124\,q^2 - 245664\,q + 181440,$$

where one may check that $\#\mathcal{M}_{1,10}(\mathbb{F}_q)$ vanishes for $q = 2$ and $q = 3$. This answer looks already a bit complicated and raises the question:

Question 3.1. – Is $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ always a polynomial in q? More generally, is $\#\mathcal{M}_{g,n}(\mathbb{F}_q)$ or $\#\overline{\mathcal{M}}_{g,n}(\mathbb{F}_q)$ polynomial?

Later we shall see that these experimentally obtained values given above in the tabel are correct for all prime powers q.

Since Weil and Deligne we know that counting points over finite fields of a variety defined over a finite field gives information on the cohomology and vice-versa knowledge of the cohomology tells us about the number of rational points.

The Lefschetz fixed point theorem connects the number of rational points on a separated scheme of finite type over $\overline{\mathbb{F}}_q$, that is, the number of fixed points of Frobenius, to the trace of Frobenius acting on étale compactly supported cohomology, see [**19**, Théorème 3.2]. By work of Behrend [**3**] this result extends to the setting of Deligne-Mumford stacks.

Question 3.1 leads to the following question.

Question 3.2. – What does it mean for the cohomology that we find polynomials in q?

The answer is given by a theorem by van den Bogaart and Edixhoven [**11**].

Theorem 3.3. – *Let $\mathcal{X}$ be a Deligne-Mumford stack that is proper smooth and of pure dimension d over $\mathbb{Z}$. Suppose that for all primes p in a set S of Dirichlet density* 1 *there exists a polynomial $P = \sum_{i\geq 0} P_i x^i \in \mathbb{Q}[x]$ such that*

$$\#\mathcal{X}(\mathbb{F}_{p^n}) = P(p^n) + o(p^{nd/2}) \quad (n \to \infty).$$

Then $P \in \mathbb{Z}[x]$ has degree d and satisfies $P(x) = x^d P(1/x)$ and we have $\#\mathcal{X}(\mathbb{F}_{p^n}) = P(p^n)$ for all primes p and all $n \geq 1$.

The statement says that if there exists a polynomial P with rational coefficients such that $\lim_{n\to\infty} |\#\mathcal{X}(\mathbb{F}_{p^n}) - P(p^n)|p^{-nd/2} = 0$ for enough primes p, then $\#\mathcal{X}(\mathbb{F}_{p^n})$ is an integral polynomial and of degree d.

Another way of expressing it is by saying that the cohomology of $\mathcal{X}$ is a polynomial $P(\mathbb{L})$ in the Lefschetz motive $\mathbb{L}$. Or, equivalently, that $H^i_{\text{ét}}(\mathcal{X}_{\mathbb{Q}}, \mathbb{Q}_\ell)$ with $\ell \neq p$ vanishes for i odd and equals $\mathbb{Q}_\ell(-i/2)^{P_{i/2}}$ for i even. Or, one could say that geometric Frobenius in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $H^i_{\text{ét}}(\mathcal{X}\otimes\overline{\mathbb{F}}_p, \overline{\mathbb{Q}}_\ell)$ for $\ell \neq p$ and even i with eigenvalues $q^{i/2}$.

But we should bear in mind that, as remarked above, $\mathcal{M}_{g,n}$ is in general not complete. In order to apply the theorem just given we need to consider the compactification $\overline{\mathcal{M}}_{g,n}$.

The complement $\partial\mathcal{M}_{g,n}$ of $\mathcal{M}_{g,n}$ in $\overline{\mathcal{M}}_{g,n}$ is a union of divisors. This complement is stratified and the strata are quotients by finite groups of products of $\mathcal{M}_{g',n'}$ for $g' \leq g$ and $n' \leq n+g-g'$. In particular, one sees that even if one is interested in $\mathcal{M}_g$ only, the spaces $\mathcal{M}_{g,n}$ naturally appear.

There is an action of the symmetric group $\mathfrak{S}_n$ on $\mathcal{M}_{g,n}$ and $\overline{\mathcal{M}}_{g,n}$. We can then count equivariantly. That is, instead of counting fixed points of Frobenius F on $\mathcal{M}_{g,n}(\overline{\mathbb{F}}_p)$, we count the fixed points of $F\circ\sigma$ for $\sigma \in \mathfrak{S}_n$. This depends only on the cycle type of σ. So we count the number of $\overline{\mathbb{F}}_q$-isomorphism classes of curves together with an n-tuple of points $(P_1,\dots,P_n)$ on the curve such that it is fixed by $F\circ\sigma$. For example, one can use Lemma 2.1 to see that the number of fixed points of $F\circ\sigma$ with $\sigma = (1\,2) \in \mathfrak{S}_2$ for $\mathcal{M}_{g,2}(\overline{\mathbb{F}}_q)$ equals

$$\sum_C \frac{\#C(\mathbb{F}_{q^2}) - \#C(\mathbb{F}_q)}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)},$$

where the sum is over all curves C of genus g over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism.

There is a formula of Getzler-Kapranov (see [**37**], also [**9**]) that expresses $\#\overline{\mathcal{M}}_{g,n}(\mathbb{F}_q)$ in terms in terms of the $\mathfrak{S}_{n'}$-equivariant counts of $\mathcal{M}_{g',n'}(\mathbb{F}_q)$ for $g' \leq g$ and $n' \leq n+g-g'$.

This shows that we can use induction to apply the theorem above not only to $\overline{\mathcal{M}}_{g,n}$, but also to $\mathcal{M}_{g,n}$. But this shows also that one needs the equivariant formulas in order to calculate the contributions of the boundary strata.

The paper by Getzler and Kapranov deals with the cohomology, but we have translated it here in terms of number of rational points. See also the paper [**21**] by Diaconu, who gives (following Getzler-Kapranov) effective formulas expressing the $\mathfrak{S}_n$-equivariant Euler characteristics of $\overline{\mathcal{M}}_{g,n}$ in terms of the Euler characteristics of $\mathcal{M}_{g',n'}$ with the indices g', n' restricted by $\max\{0, 3-2g'\} \leq n' \leq 2(g-g')+n$.

4. Polynomial formulas

The first equivariant counting for $\mathcal{M}_{g,n}$ was done by Kisin-Lehrer in [**45**] for $g = 0$ and they applied it to conclude facts about the cohomology of $\mathcal{M}_{0,n}$. They found polynomial functions in q for these equivariant counts of $\#\mathcal{M}_{0,n}(\mathbb{F}_q)$. They showed for example that the alternating representation of $\mathfrak{S}_n$ does not show up in the cohomology of $\mathcal{M}_{0,n}$.

Getzler did equivariant counting for $g = 1$ in [**36**]. In the preceding section we gave a sample of the formulas for $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ and we add here a sample of those for $\#\overline{\mathcal{M}}_{1,n}(\mathbb{F}_q)$.

n	$\#\overline{\mathcal{M}}_{1,n}(\mathbb{F}_q)$
1	$q+1$
2	q^2+2q+1
3	q^3+5q^2+5q+1
4	$q^4+12q^3+23q^2+12q+1$
5	$q^5+27q^4+102q^3+102q^2+27q+1$
6	$q^6+58q^5+421q^4+756q^3+421q^2+58q+1$

Note the symmetry in the formulas for $\overline{\mathcal{M}}_{1,n}$ displaying Poincaré duality. We will come back to the case $\mathcal{M}_{1,n}$ and $\overline{\mathcal{M}}_{1,n}$ in the next section.

Polynomial formulas for higher genus were first obtained by Getzler for $g = 2$ and $n \leq 3$ in [**35**] and then by Bergström for $g = 2$ and $g = 3$ for some n in [**4, 5**]. Since these tell us about the cohomology, which is a representation space of $\mathfrak{S}_n$, the answer is phrased in terms of Schur functions $\mathbf{s}_\lambda$, where λ runs through the partitions of n and these λ correspond to the irreducible representations of $\mathfrak{S}_n$. Recall that the Schur functions form a basis for the symmetric functions, like the elementary or complete symmetric functions. We refer for the representation theory to [**29**]. We write the answer as

$$\sum_{\lambda\vdash n} P_\lambda(q)\,\mathbf{s}_\lambda \quad \text{with} \quad P_\lambda(q) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \chi_\lambda(\sigma)\,|\,\mathcal{M}_{g,n}^{F\cdot\sigma}\,|,$$

with χ_λ the character of the irreducible irreducible representation determined by λ and $|\,\mathcal{M}_{g,n}^{F\cdot\sigma}\,|$ the number of fixed points of $F\cdot\sigma$. To give an idea, here is the equivariant answer for $\#\overline{\mathcal{M}}_{2,4}(\mathbb{F}_q)$:

$$\begin{aligned}&(q^7+8q^6+33q^5+67q^4+67q^3+33q^2+8q+1)\,\mathbf{s}_4\\ &\quad+(4q^6+26q^5+60q^4+60q^3+26q^2+4q)\,\mathbf{s}_{31}\\ &\quad+(2q^6+12q^5+28q^4+28q^3+12q^2+2q)\,\mathbf{s}_{22}\\ &\quad+(3q^5+10q^4+10q^3+3q^2)\,\mathbf{s}_{211}.\end{aligned}$$

As one may surmise and we will see, we cannot expect that $\#\mathcal{M}_{g,n}(\mathbb{F}_q)$ is always a polynomial in q. But it happens to be so for small g and n. Below we summarize

a number of cases where it turns out to be the case. In each of the cases one can normalize an equation for the curve and then count.

For $g = 1$ the $\mathfrak{S}_n$-equivariant version of $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ is polynomial for $1 \leq n \leq 10$. Similarly, $\mathfrak{S}_n$-equivariant version of $\#\overline{\mathcal{M}}_{1,n}(\mathbb{F}_q)$ is polynomial for $1 \leq n \leq 10$. This is due to Getzler, see [**36**]; we will come back to this in the next section.

For $g = 2$ the $\mathfrak{S}_n$-equivariant version of $\#\mathcal{M}_{2,n}(\mathbb{F}_q)$ is polynomial for $0 \leq n \leq 9$. The formulas are due to Bergström, [**5**] for $n \leq 7$, but using the results of Petersen [**58**] it extends to $n = 9$. Similarly, this holds also $\mathfrak{S}_n$-equivariantly for $\#\overline{\mathcal{M}}_{2,n}(\mathbb{F}_q)$.

For $g = 3$ the $\mathfrak{S}_n$-equivariant version of $\#\mathcal{M}_{3,n}(\mathbb{F}_q)$ is polynomial for $0 \leq n \leq 7$. The $\mathfrak{S}_n$-equivariant version of $\#\overline{\mathcal{M}}_{3,n}(\mathbb{F}_q)$ is polynomial for $0 \leq n \leq 9$, see [**4**].

For $g = 4$ not much is known. It is expected that $\#\mathcal{M}_{4,n}(\mathbb{F}_q)$ is polynomial for $n \leq 3$. The cohomology of $\mathcal{M}_{4,0}$ with its Hodge structure was computed by Tommasi [**71**]. These results suggest for $\mathcal{M}_4$ and $\overline{\mathcal{M}}_4$ the expected formulas

$$\#\mathcal{M}_4(\mathbb{F}_q) = q^9 + q^8 + q^7 - q^6,$$

$$\#\overline{\mathcal{M}}_4(\mathbb{F}_q) = q^9 + 4\,q^8 + 13\,q^7 + 32\,q^6 + 50\,q^5 + 50\,q^4 + 32\,q^3 + 13\,q^2 + 4\,q + 1.$$

For $q = 2$ this can be confirmed using counts of Xarles [**75**].

5. Modular Forms Appear

As noted above, we cannot expect that $\#\mathcal{M}_{g,n}(\mathbb{F}_q)$ is always polynomial in q for $g \geq 1$. This can be illustrated for the case $g = 1$, as we will do now. But instead of considering $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$, to simplify things we look at it from a different perspective.

For each elliptic curve $E = (C, P_1)$ defined over $\mathbb{F}_q$ we have by Hasse $\#E(\mathbb{F}_q) = q+1-\alpha-\bar{\alpha}$ with $\alpha = \alpha(E)$ an algebraic integer with $|\alpha| = \sqrt{q}$. Thus we can consider for a non-negative integer n

$$\sigma_n(q) := -\sum_E \frac{\alpha^n + \alpha^{n-1}\bar{\alpha} + \cdots + \bar{\alpha}^n}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)},$$

where we sum over all elliptic curves E defined over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism and the α depend on E.

For example, above we gave a frequency list for $p = 3$ which immediately provides the values of $\sigma_n(3)$. It is easy to see that $\sigma_n(q) = 0$ for n odd, since if $\alpha, \bar{\alpha}$ occurs, then $-\alpha, -\bar{\alpha}$ occurs for a twist with the same factor $1/\#\mathrm{Aut}_{\mathbb{F}_q}$. Working out the frequency lists for $q = 2, 3, 5, 7$ produces the following table.

n	0	2	4	6	8	10	12	14	16
$\sigma_n(2)$	-2	1	1	1	1	-23	1	217	-527
$\sigma_n(3)$	-3	1	1	1	1	253	1	-3347	-4283
$\sigma_n(5)$	-5	1	1	1	1	4831	1	52111	-1025849
$\sigma_n(7)$	-7	1	1	1	1	-16743	1	2822457	3225993

If we subtract the ubiquitous 1 we recognize that for $p = 2, 3, 5, 7$

$$\sigma_{10}(p) = 1 + \tau(p),$$

where

$$\Delta = \sum_{n\geq 1} \tau(n) q^n = q - 24\, q^2 + 252\, q^3 + \cdots = q \prod_{m\geq 1} (1 - q^m)^{24} \tag{0}$$

is the well-known normalized cusp form of weight 12 on $\mathrm{SL}(2, \mathbb{Z})$. And similarly, we recognize $\sigma_{14}(p)$ (resp. $\sigma_{16}(p)$) as $1 + a(p)$ with $a(p)$ the pth Fourier coefficient of the normalized cusp form $q + \sum_{n\geq 2} a(n) q^n$ that generates the space S_{16} of cusp forms of weight 16 (resp. S_{18} of weight 18) on $\mathrm{SL}(2, \mathbb{Z})$. Such counts were done by Birch [**10**] in the 1960s. He gave the formulas equivalent to those of σ_k for $2 \leq k \leq 10$.

In general we have for even $k > 0$

$$\sigma_k(p) = \mathrm{Tr}(T_p, S_{k+2}) + 1$$

with $S_k = S_k(\mathrm{SL}(2, \mathbb{Z}))$ the space of cusp forms of weight k on $\mathrm{SL}(2, \mathbb{Z})$ and T_p the Hecke operator at p. This is an aspect of the Eichler-Shimura-Deligne relation to which we now turn.

The expression $\sigma_k(p)$ calculates cohomological information. The moduli space $\mathscr{A}_1 = \mathscr{M}_{1,1}$ carries a local system $\mathbb{V} = R^1\pi_*(\mathbb{Q}_\ell)$ of rank 2 with $\pi : \mathscr{X} \to \mathscr{A}_1$ the universal elliptic curve. The fiber of this local system over $[E]$ is the cohomology $H^1_{\mathrm{et}}(E, \mathbb{Q}_\ell)$.

This local system gives rise for each $k > 0$ to a local system $\mathbb{V}_k = \mathrm{Sym}^k(\mathbb{V})$. As it turns out, for a prime power q the expression $\sigma_k(q)$ equals the trace of Frobenius F_q on the compactly supported cohomology of $\mathbb{V}_k$. The contribution of an elliptic curve $E/\mathbb{F}_q$ to $\sigma_k(q)$ is minus the trace of Frobenius F_q on $\mathrm{Sym}^k(H^1_{\mathrm{et}}(E \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))$.

A classical result of Eichler-Shimura ([**68**]) says that for even $k > 0$

$$H^1_c(\mathscr{A}_1(\mathbb{C}), \mathbb{V}_k \otimes \mathbb{C}) \cong S_{k+2} \oplus \overline{S}_{k+2} \oplus \mathbb{C}, \tag{1}$$

and this displays the mixed Hodge structure on $H^1_c(\mathscr{A}_1(\mathbb{C}), \mathbb{V}_k)$. Deligne showed in 1968 in [**17**] that this result has an analogue for étale ℓ-adic cohomology. Moreover, one can relate Frobenius there to the Hecke operator. The result may be summarized as follows.

Theorem 5.1. – *Let k be an even positive integer and p a prime. Then $\sigma_k(p)$ can be expressed in terms of the trace of the Hecke operator T_p on the space of cusp forms S_{k+2} of weight $k + 2$ on* $\mathrm{SL}(2, \mathbb{Z})$ *as*

$$\sigma_k(p) = \mathrm{Tr}(T_p, S_{k+2}) + 1.$$

This explains the experimental observation given above.

Thus we know $\sigma_k(p)$ if we know the trace of the Hecke operator T_p. And similarly, for prime powers q, but the formula is slightly different as F_q does not correspond exactly to T_q. But we can turn this around and use counting of elliptic curves over finite fields to calculate traces of Hecke operators. That one does not encounter this, is because we have a closed formula, the Eichler-Selberg formula, for the traces of the Hecke operators on the spaces of cusp forms on $\mathrm{SL}(2, \mathbb{Z})$.

In order to go back to the (cohomology of the) spaces $\mathcal{M}_{1,n}$ that we started with, one may use a relation between $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ and the numbers $\sigma_k(q)$ for $k < n$. This relation can be beautifully expressed by using a formula of Getzler (see [**36**, p. 200])

Proposition 5.2. – *(Getzler's formula)*

$$\frac{\#\mathcal{M}_{1,n}(\mathbb{F}_q)}{n!} = \text{residue at 0 of the formal expression}$$
$$\binom{q-t-q/t}{n} \sum_{k=1}^{\infty} \left(\frac{\sigma_k(q)}{q^{2k+1}t^{2k}-1} \right) (t - \frac{q}{t})\, dt.$$

We thus see that $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ in general is not a polynomial in q for $n \geq 11$. And indeed, the modular form Δ shows up in the formulas for $n = 11$;

$$\begin{aligned}\#\mathcal{M}_{1,11}(\mathbb{F}_p) =& p^{11} - 330\,p^9 + 4575\,p^8 - 30657\,p^7 + 124992\,p^6 - 336820\,p^5 + 584550\,p^4 \\ & - 406769\,p^3 - 865316\,p^2 + 2437776\,p - 1814400 - \tau(p), \\ \#\overline{\mathcal{M}}_{1,11}(\mathbb{F}_p) =& p^{11} + 2037\,p^{10} + 213677\,p^9 + 4577630\,p^8 + 30215924\,p^7 + 74269967\,p^6 + \\ & 30215924\,p^5 + \cdots + 2037\,p + 1 - \tau(p).\end{aligned}$$

Note that because of Poincaré duality the expression $\#\overline{\mathcal{M}}_{1,11}(\mathbb{F}_p)$ possesses a symmetry. The complicated formulas for $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ also explain why we preferred to deal with the function $\sigma_k(q)$ instead of those for $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$.

The formulas for $\sigma_k(q)$ and $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ are displaying one aspect of the cohomology of the local systems $\mathbb{V}_k$ on $\mathcal{A}_1$. There is a motivic form of this that incorporates more aspects. Scholl showed in [**65**] the existence of a motive $S[k+2]$ associated to the space S_{k+2} of cusp forms on $\mathrm{SL}(2,\mathbb{Z})$. Then the Eichler-Shimura-Deligne relation takes the form for $k > 0$

$$H^1_c(\mathcal{A}_1, \mathbb{V}_k) = S[k+2] + 1$$

and this incorporates both (1) and Deligne's generalization for ℓ-adic étale cohomology. The relation between the Hecke operator T_p and geometric Frobenius F_p then implies

$$1 + \mathrm{Tr}(F_p, S[k+2]) = \sigma_k(p).$$

6. Genus Two

For genus 2 the Torelli map $t_2 : \mathcal{M}_2 \to \mathcal{A}_2$ is an embedding with image the open subset whose complement is $\mathcal{A}_{1,1}$, the locus of principally polarized abelian surfaces that are products of elliptic curves with the product polarization. It is natural to look for an analogue of the $g = 1$ formula

$$\mathrm{Tr}(T_p, S_{k+2}) = -1 + \sigma_k(p).$$

As we saw in the preceding section, the contribution of an elliptic curve $E/\mathbb{F}_q$ to $\sigma_k(q)$ is minus the trace of Frobenius F_q on $\mathrm{Sym}^k(H^1_{\mathrm{et}}(E \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))$. For an abelian

surface X over a finite field the 4-dimensional vector space $H^1_{\text{et}}(X, \mathbb{Q}_\ell)$ (with ℓ prime to the characteristic) is provided with a non-degenerate symplectic pairing

$$H^1_{\text{et}}(X, \mathbb{Q}_\ell) \times H^1_{\text{et}}(X, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-1),$$

which corresponds to the Weil pairing if one identifies $H^1_{\text{et}}(X, \mathbb{Q}_\ell)$ with the dual of the ℓ-adic Tate module of X. Thus the natural analogue of Sym^k is an irreducible representation $R_{a,b}$ of $\text{Sp}(4, \mathbb{Q})$ with highest weight $a \geq b \geq 0$.

We recall that the irreducible representations of $\text{Sp}(4, \mathbb{Q})$ are parametrized by the pairs (a, b) of integers with $a \geq b \geq 0$, and $R_{a,b}$ occurs in $\text{Sym}^{a-b}(V) \otimes \text{Sym}^b(\wedge^2 V)$ with $V = R_{1,0}$ the standard representation of $\text{Sp}(4, \mathbb{Q})$. We refer to [**29**] for the representation theory.

For a smooth projective curve C of genus 2 over $\mathbb{F}_q$ there exist by Weil algebraic integers α_1 and α_2 of absolute value $\sqrt{q}$ such that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \overline{\alpha}_1^n - \alpha_2^n - \overline{\alpha}_2^n \qquad \text{for all } n \in \mathbb{Z}_{\geq 1}.$$

The trace of Frobenius on $R_{a,b}(H^1_{\text{et}}(X \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))$, with X the Jacobian of C, can be expressed by certain symmetric expressions (Schur functions) in these α_i and $\overline{\alpha}_i$.

Summing this over all principally polarized abelian surfaces X over $\mathbb{F}_q$ up to isomorphism over $\mathbb{F}_q$, including the abelian surfaces that are products of elliptic curves, yields a number $\sigma_{a,b}(q)$ that generalizes the $\sigma_k(q)$ of $g = 1$.

Around 2002 Carel Faber and I embarked on a program to find the analogue of Theorem 5.1 for $g = 2$. What we did ([**25**]) was counting curves of genus 2 over finite fields; for given field $\mathbb{F}_q$ with $q \leq 37$ (later $q < 200$) we compiled a frequency list of possible Weil polynomials as the curve ran through all curves of genus 2 up to isomorphism over $\mathbb{F}_q$ (with factor $1/\#\text{Aut}_{\mathbb{F}_q}(C)$) and added the contribution from the degenerate curves (corresponding to products of elliptic curves). Thus we calculated $\sigma_{a,b}(q)$ and then interpolated the outcome by polynomials in q and known motives, like that of Δ. When this no longer worked we encountered new modular forms.

The modular forms that are expected to appear here are Siegel modular forms of degree 2. To explain this notion we introduce the Siegel upper half space of degree g by

$$\mathfrak{H}_g = \{\tau \in \text{Mat}(g \times g, \mathbb{C}) : \tau = \tau^t, \text{Im}(\tau) > 0\}.$$

The symplectic group $\Gamma_g = \text{Sp}(2g, \mathbb{Z})$ is the automorphism group of the $\mathbb{Z}$-module of rank $2g$ generated by a basis $e_1, \ldots, e_g$ and $f_1, \ldots, f_g$ and symplectic form $\langle , \rangle$ with $\langle e_i, e_j \rangle = 0 = \langle f_i, f_j \rangle$ and $\langle e_i, f_j \rangle = \delta_{ij}$, the Kronecker δ_{ij}. Using this basis an element $\gamma \in \text{Sp}(2g, \mathbb{Z})$ can be written as a 2×2 matrix of $g \times g$ matrices of integers. An element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts on $\mathfrak{H}_g$ by $\tau \mapsto (a\tau + b)(c\tau + d)^{-1}$.

We now fix a finite-dimensional irreducible complex representation

$$\rho : \text{GL}(g) \to W.$$

A Siegel modular form of weight ρ and degree $g > 1$ is a holomorphic map $f : \mathfrak{H}_g \to W$ with

$$f((a\tau + b)(c\tau + d)^{-1}) = \rho(c\tau + d)f(\tau) \qquad \text{for all} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z}).$$

For $g = 2$ we take as representation the irreducible $\mathrm{GL}(2)$-representation

$$W = \mathrm{Sym}^j(\mathrm{St}) \otimes \det(\mathrm{St})^{\otimes k}$$

with St the standard representation and j and k integers with $j \geq 0$. We call the weight (j, k). We have the notion of cusp forms and $S_{j,k} = S_{j,k}(\Gamma_2)$ denotes the vector space of cusp forms of weight (j, k). For $j = 0$ we are dealing with scalar-valued Siegel modular forms. We also have an algebra of operators, the Hecke algebra with operators T_p for every prime p; see for example [**13**] and the references there. Scalar-valued Siegel modular forms of degree 2 were studied by Igusa in the 1960s [**41, 42**]. Igusa determined the ring of scalar-valued modular forms of degree 2. Satoh was one of the first to study vector-valued ones [**64**].

Let us note that one may also express Siegel modular forms of degree 2 as sections of a bundle. If $\mathbb{E}$ is the Hodge bundle on $\mathcal{A}_2$ whose fiber over $[X]$ is the 2-dimensional space $H^0(X, \Omega^1_X)$, then a Siegel modular form of weight (j, k) can be viewed as a section of $\mathrm{Sym}^j(\mathbb{E}) \otimes \det(\mathbb{E})^{\otimes k}$.

In 2002 using the frequency counts of Weil polynomials of genus 2 curves over finite fields Carel Faber and I found experimentally for $(a, b) \neq (0, 0)$ and $a + b$ even, a formula that expresses the trace of the Hecke operator T_p on the space $S_{a-b,b+3}$ of cusp forms of weight $(a - b, b + 3)$ in terms of the expressions $\sigma_{a,b}(p)$ obtained by counting. The formula has the following form, see [**25**].

Formula 6.1. – *Let a, b be non-negative integers with $a+b$ even and positive. The trace of the Hecke operator T_p on the space $S_{a-b,b+3}$ of degree 2 Siegel modular cusp forms of weight $(a - b, b + 3)$ can be expressed in the counting function $\sigma_{a,b}(p)$ by*

$$\mathrm{Tr}(T_p, S_{a-b,b+3}) = \sigma_{a,b}(p) + c_{a,b}(p),$$

where the 'correction term' $c_{a,b}(p)$ equals

$$s_{a-b+2} - s_{a+b+4}\,\sigma_{a-b+2}(p)\,p^{b+1} + \begin{cases} \sigma_{b+2}(p) \\ 1 - \sigma_{a+3}(p) \end{cases}$$

with $s_k = \dim S_k(\mathrm{SL}(2, \mathbb{Z}))$.

This term $c_{a,b}(p)$ (and more generally a term $c_{a,b}(q)$) is the analogue of the term 1 for $g = 1$. Note that the correction involves only $g = 1$ data.

This conjectured Formula 6.1 for $c_{a,b}(q)$ was later proved by Weissauer (2009) [**74**]. For this one needs the Eisenstein cohomology; we refer to [**32**] and to Harder [**38**] and Petersen [**58**] for the local systems of irregular highest weight.

Counting points over finite fields thus provides a very efficient way to calculate traces of Hecke operators on cusp forms of degree 2. If you have counted for one prime p you know $\mathrm{Tr}(T_p, S_{j,k})$ *for all* j, k with $k \geq 3$. Similarly for prime powers q.

We illustrate this with two examples where $\dim S_{j,k} = 1$; then the trace of T_p equals the eigenvalue. Eigenvalues for T_p are denoted by $\lambda(p)$. One can calculate eigenvalues of a modular form which is an eigenform under the Hecke algebra if one knows the Fourier expansion. In general it is difficult to give such Fourier expansions and also very laborious to calculate the eigenvalues. Except for very few cases, such eigenvalues were not known for vector-valued forms or for scalar-valued forms of larger weight.

The two examples are illustrated by tables of Hecke eigenvalues. The first table gives eigenvalues $\lambda(p)$ of T_p on a generator of $S_{8,8}$.

p	$\lambda(p)$ on $S_{8,8}$
2	$2^6 \cdot 3 \cdot 7$
3	$-2^3 \cdot 3^2 \cdot 89$
5	$-2^2 \cdot 3 \cdot 5^2 \cdot 13^2 \cdot 607$
7	$2^4 \cdot 7 \cdot 109 \cdot 36973$
11	$2^3 \cdot 3 \cdot 4759 \cdot 114089$
13	$-2^2 \cdot 13 \cdot 17 \cdot 109 \cdot 3404113$
17	$2^2 \cdot 3 \cdot 17 \cdot 41 \cdot 1307 \cdot 168331$
19	$-2^3 \cdot 5 \cdot 74707 \cdot 9443867$

The next table deals with the first non-zero scalar modular form of odd weight 35. This form $\chi_{35} \in S_{0,35}$ is one of the generators of the ring of scalar-valued Siegel modular forms of degree 2 as described by Igusa [**41**].

p	$\lambda(p)$ on $S_{0,35}$
2	-25073418240
3	-11824551571578840
5	$947008164231993093750 0$
7	$-10370198954152041951342796400$
11	$-80150716896320348583648181469476 56$
13	$-20232136256107650938383898249808243380$
17	$11864631390698476798508686738129755826 6980$
19	$29959172727063832507467545896685425572441160$
23	$-19113726221407800133722231270080150603498983 20$
29	$-21293272738730115477693459164181205732214380854 60$
31	$-15734859849821844552162082787656951964487418082297 6$
37	$-47788585641545948035267859493926208327050656971703460$

Note that the parabolic shape of the figures in this diagram nicely reflects Deligne's result on the absolute values of the eigenvalues of Frobenius [**17, 18**].

For $g = 1$ knowing the Hecke eigenvalues of a normalized eigenform means knowing the Fourier expansion of the form. That is no longer the case for $g > 1$.

These results on the Hecke eigenvalues of genus 2 forms stimulated Harder to formulate a precise conjecture on congruences between elliptic modular forms and Siegel modular forms, see [**13**]. For a long time he had suspected that there should be such conguences. Our work provided strong evidence for this conjecture. For me such results beautifully show the use of counting points over finite fields.

With Bergström and Faber we extended this in [**6**] to $g = 2$ and level 2 (and $p \neq 2$) by taking into account ramification points of the genus 2 curve $y^2 = f$ for f of degree 6. The symmetric group $\mathfrak{S}_6$ acts and we can count equivariantly. The equivariant formulas are somewhat complicated. These were later proved to be correct by Rösner [**63**] using the theory of automorphic representations.

Results on traces of Hecke operators obtained by counting points of curves over finite fields can be found on the website `smf.compositio.nl`.

As a final remark, we point out that as soon as cusp forms appear we will not have polynomial formulas for $\#\mathcal{M}_{2,n}(\mathbb{F}_q)$. In particular, for $n = 10$ and $\mathfrak{S}_n$-representation $\lambda = [1^{10}]$ we see modular forms appear. The dimension of $S_{j,k}$ grows fast, for fixed j cubically in k.

7. Genus Three

When one goes from genus 2 to 3 the complexity increases. One aspect of this is that for genus 3 the Torelli map $t : \mathcal{M}_3 \to \mathcal{A}_3$ is a morphism of stacks of degree 2. Indeed, every principally polarized abelian variety X of dimension 3 has an automorphism -1_X of order 2 which acts by sending an element to its inverse in the group, but the generic curve of genus 3 does not have such an automorphism. A hyperelliptic curve has such an involution and it induces the automorphism -1_X on its Jacobian. We thus can interpret $\mathcal{M}_3 \to \mathcal{A}_3$ as a double cover ramified along the (closure of) the hyperelliptic locus.

Igusa showed in [**42**] that the closure of the locus of hyperelliptic Jacobians in $\mathcal{A}_3$ is the zero divisor of a Siegel modular cusp form χ_{18} of degree 3 and weight 18. One can view χ_{18} as a section of the line bundle $\det(\mathbb{E})^{\otimes 18}$ with $\mathbb{E}$ the rank 3 Hodge bundle on $\overline{\mathcal{M}}_3$. It allows us to view $\mathcal{M}_3$ as a double cover of $\mathcal{A}_3$ obtained by taking a square root χ_9 of χ_{18}. Ichikawa showed in 1995 that χ_9 is a Teichmüller modular form of weight 9, that is, a section of $\det(\mathbb{E})^{\otimes 9}$ on $\overline{\mathcal{M}}_3$, [**40**]. An algebraic way to construct it is by observing that there is a natural morphism of locally free sheaves of rank 6

$$\mathrm{Sym}^2(\mathbb{E}) \longrightarrow \pi_*(\omega^{\otimes 2}_{\mathcal{C}/\mathcal{M}_3})$$

with $\pi : \mathcal{C} \to \mathcal{M}_3$ the universal curve, obtained by multiplying differential forms. This morphism is an isomorphism outside the hyperelliptic locus; taking the determinant

gives a map $\det(\mathbb{E})^{\otimes 4} \to \det(\mathbb{E})^{\otimes 13}$, hence a section of $\det(\mathbb{E})^{\otimes 9}$ that vanishes on the hyperelliptic locus.

When suitably normalized this form gives the obstruction of an indecomposable principally polarized abelian threefold X for being a Jacobian of a curve; it is expressed by saying that χ_{18} assumes a square value at $[X]$. We refer to the paper by Ritzenthaler [**66**] in the Serre book [**67**].

Since there are no scalar-valued Siegel modular forms (on the full group $\mathrm{Sp}(6,\mathbb{Z})$) of odd weight, the existence of the Teichmüller form χ_9 shows that $\mathcal{M}_3$ carries more cohomology than $\mathcal{A}_3$.

In joint work with Bergström and Faber [**7**] we found the generalization to $g = 3$ of the formulas for $g = 1$ and $g = 2$. For X a principally polarized abelian threefold over a finite field $\mathbb{F}_q$ we consider $H^1(X, \mathbb{Q}_\ell)$ with ℓ prime to q. For varying X it defines a local system $\mathbb{V}$ of rank 6 on $\mathcal{A}_3$. The space $H^1(X, \mathbb{Q}_\ell)$ carries a non-degenerate symplectic pairing

$$H^1(X, \mathbb{Q}_\ell) \times H^1(X, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-1).$$

For each irreducible representation $R_{a,b,c}$ of $\mathrm{Sp}(6,\mathbb{Q})$ of highest weight (a, b, c) with $a \geq b \geq c$ we can form a local system $\mathbb{V}_{a,b,c}$ with fiber $R_{a,b,c}(H^1_{\mathrm{et}}(X, \mathbb{Q}_\ell))$.

The trace of Frobenius on the cohomology

$$R_{a,b,c}(H^1_{\mathrm{et}}(X \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))$$

for $\ell \neq p$ is a symmetric expression (Schur polynomial) in the roots of the Weil polynomial of X. Summing this over all X up to isomorphism over $\mathbb{F}_q$ gives a number $\sigma_{a,b,c}(q)$. This number generalizes $\sigma_a(q)$ for $g = 1$ and $\sigma_{a,b}(q)$ for $g = 2$.

For $g = 1$ and $g = 2$ we saw the formulas

$$\mathrm{Tr}(T_p, S_{a+2}(\Gamma_1)) = \sigma_a(p) - 1, \quad \mathrm{Tr}(T_p, S_{a,b}(\Gamma_2)) = \sigma_{a,b}(p) + c_{a,b}(p),$$

with the sigmas obtained by counting and -1 and $c_{a,b}(p)$ a correction term. Now we deal with Siegel modular forms of degree 3. We found experimentally a formula for the trace of the Hecke operator T_p on the space of cusp forms $S_{i,j,k} = S_{i,j,k}(\Gamma_3)$. Note that the weight of a modular form on $\Gamma_3 = \mathrm{Sp}(6,\mathbb{Z})$ is now given by a triple (i, j, k). Scalar-valued modular forms correspond to $i = j = 0$.

The formula of [**7**] takes the form

$$\mathrm{Tr}(T_p, S_{a-b,b-c,c+4}) = \sigma_{a,b,c}(p) + c_{a,b,c}(p),$$

where $\sigma_{a,b,c}(p)$ is the trace of Frobenius on the compactly supported cohomology of the local system $\mathbb{V}_{a,b,c}$ over $\mathcal{A}_3 \otimes \mathbb{F}_p$ and the correction term $c_{a,b,c}(p)$ is given by

$$\begin{aligned} &-\sigma_{a+1,b+1}(p) + \sigma_{a+1,c}(p) - \sigma_{b,c}(p) - c_{a+1,b+1}(p)\sigma_{c+2}(p) \\ &\qquad + c_{a+1,c}(p)\sigma_{b+3}(p) - c_{b,c}(p)\sigma_{a+4}(p) + c_{a+1,b+1}(p) - c_{a+1,c}(p) + c_{b,c}(p). \end{aligned}$$

The correction term is expressed in genus 2 and 1 terms and its form was suggested by formulas in [**32**].

So far, the formula has not yet been proved. But it works perfectly. That is, there is overwhelming evidence that it produces indeed the right values of the traces of

the Hecke operators on the spaces of cusp forms. Not only that, it also allows us to see the contributions of 'lifts', modular forms of degree 1 and 2. After identifying these, one is left with the genuine Siegel modular forms of degree 3 that correspond to 8-dimensional Galois representations in the cohomology of a local system on $\mathcal{A}_3$. Genuine means that these modular forms do not belong to $g = 1$ and $g = 2$. Details can be found in [**7**].

We refer to the website `smf.compositio.nl` where results on the traces of Siegel modular forms of degree 3 thus obtained can be found. So counting points on curves over finite fields tells us about Siegel modular forms. Here are two examples. The spaces $S_{6,3,6}$ and $S_{2,4,8}$ are 1-dimensional and the next tables give the eigenvalues $\lambda(p)$ of the Hecke operators T_p on these spaces.

p	$\lambda(p)$ on $S_{6,3,6}$	$\lambda(p)$ on $S_{4,2,8}$
2	0	9504
3	−453600	970272
4	10649600	89719808
5	−119410200	−106051896
7	12572892800	112911962240
8	0	1156260593664
9	−29108532600	5756589166536
11	−57063064032	44411629220640
13	−25198577349400	209295820896008
16	341411782197248	−369164249202688
17	−107529004510200	1230942201878664
19	1091588958605600	51084504993278240

If we go to $\mathcal{M}_3$ instead there is more cohomology. It is known that the cohomology of local systems on $\mathcal{A}_3$ can be described in terms of Siegel modular forms (of degree ≤ 3). But for $\mathcal{M}_3$ it is not known what automorphic forms show up in the cohomology of local systems on $\mathcal{M}_3$. It is a mystery which modular forms or motives we will encounter. But we can use counting points over finite fields to try to explore the first cases. For the cohomology of $\mathcal{M}_3$ we know that we are dealing with motives or modular forms 'of level one', or in other words, with everywhere good reduction.

An example is provided by the local system $\mathbb{V}_{11,3,3}$ whose fiber for a curve C is the irreducible representation of highest weight $(11, 3, 3)$ on $H^1_{\text{et}}(C, \mathbb{Q}_\ell)$, see [**16**, p. 34]. We see a 6-dimensional motive of weight 23 appearing in the cohomology with Hodge degrees $0, 5, 9, 14, 18, 23$. It cannot come from a Siegel modular form of degree 3. It should correspond to a Teichmüller modular form of weight $(8, 0, 7)$, that is, a section of $\text{Sym}^8(\mathbb{E}) \otimes \det(\mathbb{E})^{\otimes 7}$ on $\overline{\mathcal{M}}_3$. We can construct such a Teichmüller modular form. It is fascinating to be able to explore this cohomology and these motives simply by counting points on curves over finite fields.

8. Other Cases

The fact that a moduli space of curves like $\mathcal{M}_g$ for $g = 1, 2, 3$ maps generically finitely to a Shimura variety helps a lot for understanding the cohomology of local systems, and hence understanding the behavior of quantities like $\#\mathcal{M}_{g,n}(\mathbb{F}_q)$. Things become much harder if one does not know a priori which modular forms or motives may show up. The case of $\mathcal{M}_4$ and $\mathcal{M}_{4,n}$ illustrates this. We do not know what motives or modular forms we can expect. Again, for the cohomology of $\mathcal{M}_{g,n}$ we know that we are dealing with motives or modular forms 'of level one', or in other words, with everywhere good reduction. As far as I know, nobody has an idea of the nature of the zeta function of $\mathcal{M}_g$ for general g. Results of Chenevier, Lannes and Renard on motives of level 1 and small rank [**14, 15**] can help in identifying the results for low values of g and n.

Given the absence of knowledge what answer to expect in general, it is natural to first look at cases where moduli spaces of curves are closely related to arithmetic quotients. In 1964 Shimura gave a list in [**69**] of arithmetic quotients of the ball that appear as moduli spaces of curves. Rohde extended this list in [**62**] and Moonen proved his list is complete [**50**]. In these cases one can count and hope to be able to interpret the result in terms of modular forms for the arithmetic group in question.

One case of Shimura's list deals with the family of Picard curves. These are curves of genus 3 that are cyclic Galois covers of degree 3 of the projective line; these can be given by an equation $y^3 = f$ with f a polynomial of degree 4 with non-zero discriminant. Picard studied these curves in the late 19th century. The Jacobians of these curves have multiplication by the ring of integers O_F of $F = \mathbb{Q}(\sqrt{-3})$ and the moduli space is a so-called Picard modular surface. In this case this modular surface is a ball quotient associated to a discrete subgroup of the group of unitary similitudes $\mathrm{U}(2, 1, \mathbb{Q}(\sqrt{-3}))$.

In a long term project with Bergström ([**8**]) we have counted points on such curves over finite fields and using this we arrived heuristically at a complete formula for the traces of Hecke operators on the corresponding modular forms in terms of these counts over finite fields.

The formula expresses the trace of a Hecke operator T_ν for ν a prime of O_F of norm congruent to 1 modulo 3 on a space of cusp forms in terms of counts on curves over finite fields; more precisely, it expresses it in terms of an analogue of the functions σ_k and $\sigma_{a,b}$ obtained by counting that we saw above, and a correction term.

But the results provided further insights. A careful analysis of the results allowed us to distill from this the traces of the Hecke operators on the spaces of genuine Picard modular forms, that is, the modular forms that correspond to Galois representations of degree 3.

The results of [**8**] are conjectural, but as in the case $g = 3$, it works perfectly. Here the weight of a modular form is a pair (j, k) of non-negative integers, the case $j = 0$ corresponding to scalar-valued modular forms.

We counted for primes $p \equiv 1 (\mathrm{mod}\ 3)$ with $p \leq 43$. For these primes we can predict the trace of the Hecke operator T_ν, for ν a prime of O_F with norm p, on the space of cusp forms of given weight (j,k) and also on the space of genuine cusp forms of given weight (j,k) *for any weight* (j,k) with $k \geq 3$.

We illustrate this by one example, but must refer to [**8**] for details. It concerns a 1-dimensional space of cusp forms of weight $(0,33)$ with a character of order 2. The Hecke eigenvalues of a generator of this space, that we found, agree with a congruence modulo 17093 of the type of congruences predicted by Harder (see Harder's contribution to [**13**]).

If p is a prime with $p \equiv 1 \bmod 3$ then p splits in O_F as $p = \nu_p \bar{\nu}_p$ with $\nu_p \equiv \bar{\nu}_p \equiv 1 (\mathrm{mod} 3)$. The Hecke eigenvalues λ_{ν_p} that we found are given in the next table. There ρ denotes a third root of 1.

p	λ_{ν_p}
7	$-50515470688848 + 19722585570921\rho$
13	$-641186317588670376 - 28497381958498509\rho$
19	$-207202261228535219325 - 223900464575892946149\rho$
31	$-72536002932093668516175 - 511708107362090202586656\rho$
37	$-15066567237821284922757576 - 12800018433999723562677897\rho$
43	$22639232969349660757698 69 - 61311985796827137336770952\rho$

These eigenvalues λ_{ν_p} satisfy the congruence

$$\lambda_{\nu_p} \equiv \bar{\nu_p}^{32} + (p^{31} + 1)\nu_p \,(\mathrm{mod}\ 17093),$$

as the reader may verify. We refer to [**8**, Section 14].

Besides this case we intend to treat other cases of Shimura's list. But one may decide to go further into unknown territory and count for other families of curves not closely related to Shimura varieties. One obvious case are the families $\mathscr{H}_g$ of hyperelliptic curves of given g and their variants $\mathscr{H}_{g,n}$. Here the case of characteristic 2 plays a special role. Bergström gives in [**4**] recursive formulas in the genus for the equivariant number of points of $\mathscr{H}_{g,n}$ over a fixed finite field. This reduces the problem for fixed n to the cases of low genera. We refer to [**4**] for more details.

9. Stratifications

The moduli spaces $\mathscr{M}_g$ and $\mathscr{A}_g$ admit stratifications. Some of these stratifications work in all characteristics, other ones are special to positive characteristic.

Maybe the best known stratification is by automorphism group. Here we see considerable differences between characteristic zero and positive characteristic. The well-known Hurwitz bound on the order of the automorphism group of a curve in characteristic 0 is no longer true in positive characteristic.

For some low genera we know explicit stratifications of $\mathcal{M}_g(\mathbb{C})$ by automorphism group. It would be nice to have such explicit stratifications also for $\mathcal{M}_g(\overline{\mathbb{F}}_p)$ and for $\mathcal{M}_g(\mathbb{F}_q)$.

Another example of a stratification of $\mathcal{M}_g$ is given by gonality. Here gonality of a curve C over a field k is the smallest degree of a morphism $C \to \mathbb{P}^1$ over k.

The gonality of a curve C defined over $\mathbb{F}_q$ puts clear restrictions on the number of $\mathbb{F}_q$-rational points of C. Thus gonality may be relevant for the study of the invariant $N_q(g)$, the maximum number of rational points on a smooth projective curve of genus g over $\mathbb{F}_q$, that plays such an important role in Serre's lectures notes [**67**].

In [**31**] I asked the question: *what is the maximum number of rational points on a curve of genus g and gonality γ defined over $\mathbb{F}_q$?* It suggests to study a variant of $N_q(g)$; namely the invariant $N_q(g,\gamma)$: the maximum number of $\mathbb{F}_q$-rational points on a (smooth projective) curve over $\mathbb{F}_q$ of genus g and gonality γ.

Recently, this question was taken up by X. Faber and Grantham for small q and g in [**26, 27**]. It is well-known that the gonality over a finite field is at most $g+1$, a result due to F.K. Schmidt. Moreover, if $\#C(\mathbb{F}_q) > 0$ then $\gamma(C) \leq g$. Indeed, for $g \geq 2$ if $P \in C(\mathbb{F}_q)$ then $h^0(K-(g-2)P) \geq 2$ by Riemann-Roch, providing a linear system of degree g.

But if $\#C(\mathbb{F}_q) = \emptyset$, then the gonality can be $g+1$. For example, the curve C of genus 3 defined over $\mathbb{F}_2$ given by

$$x^4+y^4+z^4+x^2y^2+x^2z^2+y^2z^2+x^2yz+xy^2z+xyz^2=0$$

in $\mathbb{P}^2$ has no rational points and it is not difficult to show that it has gonality 4. Here is a table with some of their results (taken from [**27**]). The cross $\times$ indicates the absence of curves over $\mathbb{F}_q$ with given (g,γ).

g	γ	$N_2(g,\gamma)$	$N_3(g,\gamma)$	$N_4(g,\gamma)$
3	2	6	8	10
3	3	7	10	14
3	4	0	0	0
4	2	6	8	10
4	3	8	12	15
4	4	5	10	13
4	5	0	0	$\times$
5	2	6	8	10
5	3	8	12	15
5	4	9	13	17

5	5	3	4	5
5	6	×	×	×

Faber-Grantham conjecture in [27] that an optimal curve has gonality at most $\lfloor \frac{g+3}{2} \rfloor$ and that for fixed $\gamma \geq 2$ and fixed q and for g large one has $N_q(g,\gamma) = \gamma(q+1)$. Together with Howe they show for $g \geq 5$ in [28] that over a finite field gonality is at most g.

In a recent paper [72] Floris Vermeulen shows by a construction of curves in a toric variety the following result.

Theorem 9.1. – *For fixed q and γ with $\gamma \leq q+1$ we have* $\lim_{g\to\infty} N_q(g,\gamma) = \gamma\,(q+1)$.

10. Characteristic p stratifications

There are stratifications on the moduli of curves and abelian varieties that are special to positive characteristic. The first well-known case where this phenomenon appears is the case of elliptic curves. Elliptic curves in characteristic $p > 0$ come into two sorts: ordinary or supersingular. A formula of Deuring gives the number of supersingular curves. The number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ equals

$$h_p = \frac{p-1}{12} + \left(1 - (\frac{-3}{p})\right)\frac{1}{3} + \left(1 - (\frac{-4}{p})\right)\frac{1}{4}.$$

But a stacky interpretation gives the more elegant formula

$$\sum \frac{1}{\#\mathrm{Aut}(E)} = \frac{p-1}{24},$$

where the summation is over all isomorphism classes of supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$. This stratification on $\mathscr{A}_1 \otimes \mathbb{F}_p$ generalizes for higher g to a stratification on $\mathscr{A}_g \otimes \mathbb{F}_p$ in two ways:

1. The Newton Polygon stratification (NP).
2. The Ekedahl-Oort stratification (E–O).

The simplest examples of strata in both stratifications are the p-rank strata. If X/k is an abelian variety over a field k of characteristic $p > 0$ and $X[p]$ denotes the kernel of multiplication by p on X with $\#X[p](\overline{k}) = p^f$ then the p-rank of X is f. The (closed) p-rank strata are

$$V_f = \{[X] \in \mathscr{A}_g(\overline{k}) : f(X) \leq f\}.$$

Koblitz showed already in 1975 in [46, Thm. 7] that this gives a stratification with $\mathrm{codim}(V_f) = g - f$ in $\mathscr{A}_g \otimes \mathbb{F}_p$.

The study of these stratifications was pursued by Oort and has become a very active area of research. I summarize a few salient features before discussing their relevance for curves over finite fields.

The first one, the Newton Polygon stratification, extends the p-rank stratification and was introduced by Grothendieck and Katz. They showed that Newton polygons can be used to define a stratification. This stratification on $\mathscr{A}_g \otimes \mathbb{F}_p$ was much studied by Oort, who determined basic properties, see [**55**].

In order to define the Newton Polygon stratification, one takes for a principally polarized abelian variety X defined over $\overline{\mathbb{F}}_q$ the Newton polygon of the action of geometric Frobenius F_q on the cohomology group $H^1_{\text{et}}(X \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$, or more generally the Newton polygon of the p-divisible group of X. The Newton polygon is a symmetric polygon starting at $(0,0)$ and ending at $(2g, g)$, lying below the line with slope $1/2$ and with integral vertices (break points). Here symmetric means that if slope s occurs, then $1 - s$ occurs with the same multiplicity.

For principally polarized abelian varieties all such symmetric polygons appear and thus there are $g(g-1)/2 + 2$ strata in the NP stratification on $\mathscr{A}_g \otimes \mathbb{F}_p$. The codimensions of the strata are known by Oort [**55**]. The NP stratification depends only on the isogeny class of the abelian variety.

The most degenerate NP stratum is the supersingular stratum corresponding to slope $1/2$. For $g = 1$ and $g = 2$ the p-rank zero stratum V_0 coincides with the supersingular stratum, but not for $g \geq 3$.

The second stratification is due to Ekedahl and Oort, see [**54, 56**]. For the Ekedahl-Oort stratification one looks at the isomorphism type of the group scheme $X[p]$ together with Frobenius F and Verschiebung V. Alternatively, one can look at the de Rham cohomology $H^1_{\text{dR}}(X)$ and at the relative position of the kernels $\ker(F)$ and $\ker(V)$, as done in [**30**]. These are totally isotropic subspaces in the space $H^1_{\text{dR}}(X)$, which is a non-degenerate symplectic space by the Weil pairing. This stratification possesses 2^g strata. I showed in 1994 that the strata Y_μ are indexed by Young diagrams, or equivalently, by tuples $\mu = [\mu_1, \ldots, \mu_r]$ with $0 \leq r \leq g$ and $\mu_i > \mu_{i+1}$. In fact, they can be interpreted as the degeneration loci of maps between vector bundles, see [**30**].

The largest open stratum is the locus of ordinary abelian varieties. The codimension of Y_μ is $\sum_i \mu_i$. The stratification can be extended to good toroidal compactifications of Faltings-Chai type.

The Ekedahl-Oort and the Newton Polygon stratification share a number of strata: the p-rank strata. The E-O strata are in general not preserved by isogenies and deal with more subtle properties. The dimensions of the E-O strata are known. There has been a lot of research on this stratification, with a finer structure provided by a foliation, for example see [**57**].

11. Cycle Classes

The most degenerate E-O stratum is the superspecial locus. An abelian variety is superspecial if it isomorphic to a product of supersingular elliptic curves (as an unpolarized abelian variety). This superspecial locus has dimension 0. All its points are rational over $\mathbb{F}_{p^2}$. The stacky interpretation of Deuring's formula allows a generalization. It was given by Ekedahl ([**22**]).

Theorem 11.1. – *The number of superspecial abelian varieties is given by*

$$\sum_X \frac{1}{\#\mathrm{Aut}(X)} = (p-1)(p^2-1)\cdots(p^g+(-1)^g)\,p(g),$$

where the sum is over the isomorphism classes of principally polarized superspecial abelian varieties X over $\overline{\mathbb{F}}_p$ and $p(g)$ is the constant

$$p(g) = (-1)^{g(g+1)/2}2^{-g}\,\zeta(-1)\zeta(-3)\cdots\zeta(1-2g),$$

where ζ denotes the Riemann zeta function.

This constant $p(g)$ is a proportionality constant related to the volume of $\mathrm{Sp}(2g,\mathbb{Z})\backslash\mathfrak{H}_g$. Here is a little table.

g	1	2	3	4
$p(g)$	1/24	1/5760	1/2903040	1/1393459200

The formula of Ekedahl can be interpreted as a formula for the degree of the class of the 0-dimensional superspecial stratum. As such it allows a far reaching generalization: the cycle classes of the E-O strata are known. The interpretation of these strata as degeneracy classes of maps between vector bundles allows their calculation. We refer to [**30, 23**].

For example, for the p-rank stratum V_f on $\mathscr{A}_g\otimes\mathbb{F}_p$ the cycle class is

$$[V_f] = (p-1)(p^2-1)\cdots(p^{g-f}-1)\,\lambda_{g-f},$$

where λ_i is the ith Chern class of the Hodge bundle $\mathbb{E}$. This formula holds on $\mathscr{A}_g\otimes\mathbb{F}_p$ but can be extended to good toroidal compactifications $\tilde{\mathscr{A}}_g\otimes\mathbb{F}_p$. Such formulas can be seen as a generalization of Deuring's formula. Indeed, for $g=1$ the locus V_0 is the locus of supersingular elliptic curves and it has class $(p-1)\lambda_1$. To connect it with Deuring's formula, observe that the modular form Δ, given in (0) in Section 3, represents a section of $\det(\mathbb{E})^{12}$ and its zero divisor, which represents $12\,\lambda_1$, is the cusp of $\tilde{\mathscr{A}}_1$, which represents a physical point with multiplicity $1/2$ (since the degenerate elliptic curve it represents has $\#\mathrm{Aut}=2$). Thus we find $\deg(V_0)=(p-1)/24$.

An intuitive explanation of the formula for the cycle class of the p-rank locus V_f may be given as follows. If an abelian variety X of dimension g has p-rank g, then its p-kernel $X[p]$ contains the infinitesimal group scheme μ_p^g. Choosing a basis gives us g tangent vectors at the origin of X. The (open) p-rank locus $V_f - V_{f-1}$ is the locus

where f sections survive. Chern classes measure the independence of sections. So it is natural that the $(g-f)$th Chern class of the Hodge bundle appears.

For the NP stratification the cycle classes of the strata are in general not known for strata that do not occur as E-O strata. But the class of the supersingular locus S_3 for $g=3$, which is not an E-O stratum, is known; its class is

$$[S_3] = (p-1)^2(p^3-1)(p^4-1)\lambda_1\lambda_3,$$

see [**30**, Thm 11.3]. We intend to come back to the calculation of such cycle classes in the near future.

12. Strata on $\mathcal{M}_g \otimes \mathbb{F}_p$

Via the Torelli morphism these two stratifications on $\mathcal{A}_g \otimes \mathbb{F}_p$ induce stratifications on $\mathcal{M}_g \otimes \mathbb{F}_p$. But here questions abound. First: what are the dimensions of the strata? In particular: which strata are non-empty?

A first example is $g=2$. Here $\mathcal{M}_2$ is an open subset of $\mathcal{A}_2$. The cycle classes give information. To avoid the stacky aspect we may look at the moduli space $\mathcal{A}_2[n]$ of level n. This space is for $n \geq 3$ a variety and we can consider for p not dividing n the cover

$$\mathcal{A}_2[n] \otimes \mathbb{F}_p \longrightarrow \mathcal{A}_2 \otimes \mathbb{F}_p.$$

It is a Galois cover of degree $r(n) = \#\mathrm{Sp}(4, \mathbb{Z}/n\mathbb{Z})$.

The supersingular locus consists of a number of projective lines, so-called Moret-Bailly lines. Indeed, every supersingular principally polarized abelian surface can be obtained as a quotient $E^2/j(\alpha_p)$, where E is a fixed supersingular elliptic curve over $\mathbb{F}_p$, the product E^2 is provided with the polarization Frobenius F, and where $j : \alpha_p \hookrightarrow \alpha_p^2 \cong E^2[F]$ is an embedding of the group scheme α_p into the kernel $E^2[F]$ of F. These embeddings are parametrized by a $\mathbb{P}^1$ and it is easy to see that the determinant of the Hodge bundle of the resulting family over $\mathbb{P}^1$ has degree $p-1$. We know the class of the supersingular locus $[V_0] = (p-1)(p^2-1)\lambda_2$ and since the degree of λ_1 on each line is $p-1$ and $\deg(\lambda_1\lambda_2) = 1/5760$, we find $(p^2-1)r(n)/5760$ projective lines.

We also know that the degree of the superspecial locus is $(p-1)(p^2+1)r(n)/5760$. This fits, since on each line we have p^2+1 points that are rational over $\mathbb{F}_{p^2}$ and so we see that through each superspecial point $p+1$ lines pass.

So the supersingular locus consists of $(p^2-1)r(n)/5760$ projective lines meeting in $(p-1)(p^2+1)r(n)/5760$ superspecial points. But only

$$(p-1)(p-2)(p-3)\frac{r(n)}{5760}$$

of these lie in $\mathcal{M}_2[n] \otimes \mathbb{F}_p$, as one sees by subtracting those that lie in the complement $\mathcal{A}_{1,1}[n] \otimes \mathbb{F}_p$. This simple example shows the use of the cycle classes and agrees with results in [**44**].

In particular, we see that there are no such superspecial points on $\mathcal{M}_2 \otimes \mathbb{F}_p$ for $p = 2$ and $p = 3$. Of course, this is related to the well-known fact that there are no maximal curves of genus 2 over $\mathbb{F}_4$ and $\mathbb{F}_9$.

The formula just given illustrates that strata can be empty on $\mathcal{M}_g \otimes \mathbb{F}_p$. But the p-rank strata on $\mathcal{M}_g \otimes \mathbb{F}_p$ have the expected dimension as Faber and I showed.

Theorem 12.1 **([24])**. – *For every p the locus in $\mathcal{M}_g \otimes \mathbb{F}_p$ of curves with p-rank $\leq f$ is pure of dimension $g - f$.*

The same idea can be applied to other cases, see **[2]**. Recently, there has been a lot of activity trying to investigate the dimensions of NP and E-O strata on $\mathcal{M}_g \otimes \mathbb{F}_p$ for low values of g by constructions of explicit curves or families of curves over finite fields, see for example papers by Rachel Pries and others, **[1, 59, 49, 48]**. But our knowledge is still very limited.

13. Supersingular curves

Starting at the other end of the NP stratification on $\mathcal{M}_g \otimes \mathbb{F}_p$ we may ask: Is there a supersingular curve of genus g in characteristic p? Maximal curves over a finite field are supersingular, so if available provide an answer. For example, Ibukiyama showed the existence for $g = 3$ and $p > 2$.

Theorem 13.1 **([39])**. – *For odd p there exists a curve of genus 3 over $\mathbb{F}_p$ whose Jacobian is superspecial over $\mathbb{F}_{p^2}$.*

It follows from Ekedahl's formula that there is no superspecial curve of genus 3 for $p = 2$.

For $g = 4$ we have a positive answer by Kudo, Harashita and Senda.

Theorem 13.2 **([47])**. – *There exists a supersingular curve of genus 4 in every characteristic.*

But one can also fix p and vary g. Coding theory led van der Vlugt and me to consider curves related to Reed-Muller codes in **[33]**. For q a power of 2 these curves over $\mathbb{F}_q$ are given by an equation

$$y^2 + y = xR(x)$$

with $R = \sum_{i=0}^{h} a_i x^{2^i} \in \mathbb{F}_q[x]$ a so-called 2-linearized polynomial. These curves are supersingular of genus 2^{h-1} for R of degree 2^h. They possess large extra-special groups of automorphisms. Using such curves as building blocks and using fiber products one can construct supersingular curves of arbitrary genus in characteristic 2, even over $\mathbb{F}_2$.

Theorem 13.3. – (**[33]**) *For every g there exists a supersingular curve of genus g defined over $\mathbb{F}_2$.*

To give one example, for $g = 2021$ we have the supersingular curve over $\mathbb{F}_2$

$$y^{256} + y^{64} + y^4 + y = x^{68} + x^{20} + x^{17} + x^{12} + x^{10}.$$

The same method can be applied to the case $p > 2$ with as building blocks Artin-Schreier curves $y^p - y = xR(x)$ with $R = \sum_{i=0}^{h} a_i x^{p^i}$ a p-linearized polynomial of degree p^h of genus $p^h(p-1)/2$, as studied in [**33**, Section 13], but here these do not cover all genera.

Proposition 13.4. – *For odd p there exists a supersingular curve over $\mathbb{F}_p$ for every genus g with only* 0 *and* $(p-1)/2$ *in its p-adic expansion.*

As an example, for $g = 999$ one finds over $\mathbb{F}_3$ the supersingular curve

$$y^{27} + y^9 + y^3 + y = x^{246} + x^{84} + x^{82}.$$

Unfortunately, this proposition covers only a very thin set of genera for $p > 2$. But one can do variations. One can take quotients of these curves, or of other supersingular curves. For example, if d is a divisor of $p^h + 1$ then the curve $y^{p^m} - y = x^d$ for $m \geq 1$ and $h \geq 0$ is supersingular because it can be obtained as a quotient of a curve $y^{p^m} - y = x^{p^h+1}$.

For $3 \leq p \leq 23$ Riccardo Re constructed a supersingular curve in characteristic p for almost all $g \leq 100$ with very few undecided exceptions, see [**61**]. He used a variety of methods, for examples taking quotients of Fermat type curves. For a related reference see [**12**].

14. Bounds on the a-number

Besides the p-rank of an abelian variety there is another invariant closely related to the E-O stratification, the a-number, introduced by Oort. It measures the dimension of the intersection of $\ker(F)$ and $\ker(V)$ in $X[p]$ (or in $H^1_{\mathrm{dR}}(X)$) and may be defined by

$$a(X) = \dim_k \left(\ker F^* : H^1(X, O_X) \to H^1(X, O_X)\right).$$

We have $0 \leq a(X) \leq g$. For a curve C we put $a(C) = a(\mathrm{Jac}(C))$ and have

$$a(C) = g - \mathrm{rank}(V),$$

with $V : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$ the Cartier operator. The loci T_a of abelian varieties with a-number $\geq a$ are (closed) strata of the E-O stratification on $\mathscr{A}_g \otimes \mathbb{F}_p$ and have codimension $a(a+1)/2$.

The most special case of the E-O stratification is the case of superspecial abelian varieties. Oort showed in 1975 [**53**]: an abelian variety X is superspecial if and only if $a(X) = g$.

For superspecial Jacobians of curves there is a theorem of Ekedahl that limits the genus of a curve with a superspecial Jacobian.

Theorem 14.1 **([22])**. – *If C is a superspecial curve of genus g in characteristic p then $g \leq p(p-1)/2$.*

We thus see that for large g the superspecial stratum is empty on $\mathcal{M}_g \otimes \mathbb{F}_p$. We can interpret Ekedahl's result, Theorem 14.1 as: $a = g$ implies $g \leq p(p-1)/2$. Zijian Zhou, improving work of Riccardo Re ([**60**]), showed an upper bound on the genus for the case that $a = g - 1$.

Theorem 14.2 **([76])**. – *If C is a curve in characteristic p with $a(C) = g - 1$, then $g \leq p + p(p-1)/2$.*

One may ask for a generalization. Here is my conjecture for the optimal result.

Conjecture 14.3. – *For a curve C of genus g in characteristic $p > 0$ we have*

$$a(C) \leq \frac{p-1}{p} g + \frac{p-1}{2},$$

equivalently, with $a(C) = g - r$ with r the rank of the Cartier operator, we have

$$g \leq p\, r + \frac{p(p-1)}{2}.$$

Note that this is in accordance with the results of Ekedahl and Zhou. Moreover, for $p = 2$ this gives $a \leq (g+1)/2$, a result of Stöhr-Voloch, [**70**]. They show that this inequality is strict if $g \geq 3$ and C non-hyperelliptic.

The conjecture predicts empty strata of the E-O stratification on $\mathcal{M}_g \otimes \mathbb{F}_p$.

15. Counting points on strata

An interesting question is: which strata on $\mathcal{M}_g \otimes \mathbb{F}_p$ have dimension 0? For these strata one should determine their number of rational points. It could provide interesting curves over finite fields.

One can try to count number of points over finite fields on strata. Here the foliations introduced by Oort should play a role. This could lead to congruences for modular forms. In general not much is known.

A simple example are the E-O strata on $\mathcal{M}_2 \otimes \mathbb{F}_2$. The number of points $\#S(\mathbb{F}_q)$ on a (closed) stratum S for $q = 2^m$ were given in [**34**] and are shown in the following table. We index the strata by the 2-rank f or by the a-number.

stratum	$f \leq 2$	$f \leq 1$	$f = 0$	$a = 2$
$\#S(\mathbb{F}_q)$	q^3	q^2	q	0

One may interpret some of the results of [**43**] on the supersingular locus for $g = 3$ as a result in this vein.

Nart and Ritzenthaler (see [**52**]) gave the cardinalities of $\mathbb{F}_q$-rational points for $q = 2^m$ for the NP strata on $\mathscr{M}_3 \otimes \mathbb{F}_2$. We give a table with their results, where the strata S are indicated by the p-rank f or the slope $s = 1/2$. Also the cardinalities of the intersection with the hyperelliptic locus $\mathscr{H}_3$ are given.

stratum	$f \leq 3$	$f \leq 2$	$f \leq 1$	$f = 0$	$s = 1/2$
$\#S(\mathbb{F}_q)$	$q^6 + q^5 + 1$	$q^5 + q^4$	$q^4 + 2q^3 - q^2$	$q^3 + q^2$	q^2
$\#(S \cap \mathscr{H}_3)(\mathbb{F}_q)$	q^5	q^4	$2q^3 - q^2$	q^2	0

The author hopes that this text will entice some readers to engage in the many possibilities for fruitful and pleasant experimentation in this fascinating corner of mathematics.

References

[1] J. D. Achter & R. Pries – "Monodromy of the p-rank strata of the moduli space of curves", *Int. Math. Res. Not.* **2008** (2008), Art. ID rnn053.

[2] ———, "The p-rank strata of the moduli space of hyperelliptic curves", *Adv. Math.* **227** (2011), p. 1846–1872.

[3] K. A. Behrend – "The Lefschetz trace formula for algebraic stacks", *Invent. math.* **112** (1993), p. 127–149.

[4] J. Bergström – "Cohomology of moduli spaces of curves of genus three via point counts", *J. reine angew. Math.* **622** (2008), p. 155–187.

[5] ———, "Equivariant counts of points of the moduli spaces of pointed hyperelliptic curves", *Doc. Math.* **14** (2009), p. 259–296.

[6] J. Bergström, C. Faber & G. van der Geer – "Siegel modular forms of genus 2 and level 2: cohomological computations and conjectures", *Int. Math. Res. Not.* **2008** (2008), Art. ID rnn 100.

[7] ———, "Siegel modular forms of degree three and the cohomology of local systems", *Selecta Math. (N.S.)* **20** (2014), p. 83–124.

[8] J. Bergström & G. van der Geer – "Picard modular forms and the cohomology of local systems on a Picard modular surface", *Comment. Math. Helv.* **97** (2022), p. 305–381.

[9] J. Bergström & O. Tommasi – "The rational cohomology of $\overline{\mathscr{M}}_4$", *Math. Ann.* **338** (2007), p. 207–239.

[10] B. J. Birch – "How the number of points of an elliptic curve over a fixed prime field varies", *J. London Math. Soc.* **43** (1968), p. 57–60.

[11] T. van den Bogaart & B. Edixhoven – "Algebraic stacks whose number of points over finite fields is a polynomial", in *Number fields and function fields—two parallel worlds*, Progr. Math., vol. 239, Birkhäuser, 2005, p. 39–49.

[12] I. Bouw, W. Ho, B. Malmskog, R. Scheidler, P. Srinivasan & C. Vincent – "Zeta functions of a class of Artin-Schreier curves with many automorphisms", in *Directions in number theory*, Assoc. Women Math. Ser., vol. 3, Springer,, 2016, p. 87–124.

[13] J. H. Bruinier, G. van der Geer, G. Harder & D. Zagier – *The 1-2-3 of modular forms*, Universitext, Springer, 2008.

[14] G. Chenevier & J. Lannes – *Automorphic forms and even unimodular lattices*, Ergebn. Math. Grenzg., vol. 69, Springer, 2019.

[15] G. Chenevier & D. Renard – "Level one algebraic cusp forms of classical groups of small rank", *Mem. Amer. Math. Soc.* **237** (2015), p. 122.

[16] F. Cléry, C. Faber & G. van der Geer – "Concomitants of ternary quartics and vector-valued Siegel and Teichmüller modular forms of genus three", *Selecta Math. (N.S.)* **26** (2020), Paper No. 55.

[17] P. Deligne – "Formes modulaires et représentations l-adiques", Séminaire Bourbaki, vol. 1968/1969, exposé n° 355, Lecture Notes in Math., vol. 175, Springer, 1971, p. 139–172.

[18] ———, "Théorie de Hodge. III", *Inst. Hautes Études Sci. Publ. Math.* **44** (1974), p. 5–77.

[19] ———, *Cohomologie étale*, Lecture Notes in Math., vol. 569, Springer, 1977, Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[20] P. Deligne & D. Mumford – "The irreducibility of the space of curves of given genus", *Inst. Hautes Études Sci. Publ. Math.* **36** (1969), p. 75–109.

[21] A. Diaconu – "Equivariant Euler characteristics of $\overline{M}_{g,n}$", *Algebr. Geom.* **7** (2020), p. 523–543.

[22] T. Ekedahl – "On supersingular curves and abelian varieties", *Math. Scand.* **60** (1987), p. 151–178.

[23] T. Ekedahl & G. van der Geer – "Cycle classes of the E-O stratification on the moduli of abelian varieties", in *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I*, Progr. Math., vol. 269, Birkhäuser, 2009, p. 567–636.

[24] C. Faber & G. van der Geer – "Complete subvarieties of moduli spaces and the Prym map", *J. reine angew. Math.* **573** (2004), p. 117–137.

[25] ———, "Sur la cohomologie des systèmes locaux sur les espaces de modules des courbes de genre 2 et des surfaces abéliennes. II", *C. R. Math. Acad. Sci. Paris* **338** (2004), p. 467–470.

[26] X. Faber & J. Grantham – "Binary curves of small fixed genus and gonality with many rational points", *J. Algebra* **597** (2022), p. 24–46.

[27] ———, "Ternary and quaternary curves of small fixed genus and gonality with many rational points", *Exp. Math.* **32** (2023), p. 337–349.

[28] X. Faber, J. Grantham & E. W. Howe – "On the Maximum Gonality of a Curve over a Finite Field", preprint arXiv:2207.14307.

[29] W. Fulton & J. Harris – *Representation theory*, Graduate Texts in Math., vol. 129, Springer, 1991.

[30] G. van der Geer – "Cycles on the moduli space of abelian varieties", in *Moduli of curves and abelian varieties*, Aspects Math., E33, Friedr. Vieweg, Braunschweig, 1999, p. 65–89.

[31] ———, "Curves over finite fields and codes", in *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, Progr. Math., vol. 202, Birkhäuser, 2001, p. 225–238.

[32] ———, "Rank one Eisenstein cohomology of local systems on the moduli space of abelian varieties", *Sci. China Math.* **54** (2011), p. 1621–1634.

[33] G. van der Geer & M. van der Vlugt – "Reed-Muller codes and supersingular curves. I", *Compos. math.* **84** (1992), p. 333–367.

[34] ———, "Supersingular curves of genus 2 over finite fields of characteristic 2", *Math. Nachr.* **159** (1992), p. 73–81.

[35] E. Getzler – "Topological recursion relations in genus 2", in *Integrable systems and algebraic geometry (Kobe/Kyoto, 1997)*, World Sci. Publ., River Edge, NJ, 1998, p. 73–106.

[36] ———, "Resolving mixed Hodge modules on configuration spaces", *Duke Math. J.* **96** (1999), p. 175–203.

[37] E. Getzler & M. M. Kapranov – "Modular operads", *Compos. math.* **110** (1998), p. 65–126.

[38] G. Harder – "The Eisenstein motive for the cohomology of $\mathrm{GSp}_2(\mathbb{Z})$", in *Geometry and arithmetic*, EMS Ser. Congr. Rep., Eur. Math. Soc., 2012, p. 143–164.

[39] T. Ibukiyama – "On rational points of curves of genus 3 over finite fields", *Tohoku Math. J.* **45** (1993), p. 311–329.

[40] T. Ichikawa – "Teichmüller modular forms of degree 3", *Amer. J. Math.* **117** (1995), p. 1057–1061.

[41] J.-i. Igusa – "On Siegel modular forms of genus two", *Amer. J. Math.* **84** (1962), p. 175–200.

[42] ———, "Modular forms and projective invariants", *Amer. J. Math.* **89** (1967), p. 817–855.

[43] V. Karemaker, F. Yobuko & C.-F. Yu – "Mass formula and Oort's conjecture for supersingular abelian threefolds", *Adv. Math.* **386** (2021), Paper No. 107812.

[44] T. Katsura & F. Oort – "Families of supersingular abelian surfaces", *Compos. math.* **62** (1987), p. 107–167.

[45] M. Kisin & G. I. Lehrer – "Equivariant Poincaré polynomials and counting points over finite fields", *J. Algebra* **247** (2002), p. 435–451.

[46] N. Koblitz – "p-adic variation of the zeta-function over families of varieties defined over finite fields", *Compos. math.* **31** (1975), p. 119–218.

[47] M. Kudo, S. Harashita & H. Senda – "The existence of supersingular curves of genus 4 in arbitrary characteristic", *Res. Number Theory* **6** (2020), Paper No. 44.

[48] W. Li, E. Mantovan, R. Pries & Y. Tang – "Newton polygons arising from special families of cyclic covers of the projective line", *Res. Number Theory* **5** (2019), Paper No. 12.

[49] ———, "Newton polygon stratification of the Torelli locus in unitary Shimura varieties", *Int. Math. Res. Not.* **2022** (2022), p. 6464–6511.

[50] B. Moonen – "Special subvarieties arising from families of cyclic covers of the projective line", *Doc. Math.* **15** (2010), p. 793–819.

[51] D. Mumford – *Geometric invariant theory*, Ergebn. Math. Grenzg., vol. 34, Springer, 1965.

[52] E. Nart & C. Ritzenthaler – "Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2", *Finite Fields Appl.* **14** (2008), p. 676–702.

[53] F. Oort – "Which abelian surfaces are products of elliptic curves?", *Math. Ann.* **214** (1975), p. 35–47.

[54] ———, "A stratification of a moduli space of polarized abelian varieties in positive characteristic", in *Moduli of curves and abelian varieties. The Dutch Intercity Seminar* (C. Faber & E. Looijenga, eds.), Aspects of Mathematics, vol. 33, Vieweg, 1999, p. 47–60.

[55] ———, "Newton polygons and formal groups: conjectures by Manin and Grothendieck", *Ann. of Math.* **152** (2000), p. 183–206.

[56] ———, "A stratification of a moduli space of abelian varieties", in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., vol. 195, Birkhäuser, 2001, p. 345–416.

[57] ———, "Foliations in moduli spaces of abelian varieties", *J. Amer. Math. Soc.* **17** (2004), p. 267–296.

[58] D. Petersen – "Cohomology of local systems on the moduli of principally polarized abelian surfaces", *Pacific J. Math.* **275** (2015), p. 39–61.

[59] R. Pries – "Current results on Newton polygons of curves", in *Open problems in arithmetic algebraic geometry*, Adv. Lect. Math. (ALM), vol. 46, Int. Press, 2019, p. 179–207.

[60] R. Re – "The rank of the Cartier operator and linear systems on curves", *J. Algebra* **236** (2001), p. 80–92.

[61] ———, "Invariants of curves and Jacobians in positive characteristic", Ph.D. Thesis, University of Amsterdam, 2004.

[62] J. C. Rohde – *Cyclic coverings, Calabi-Yau manifolds and complex multiplication*, Lecture Notes in Math., vol. 1975, Springer, 2009.

[63] M. Rösner – "Parahoric restriction for GSp(4)", *Algebr. Represent. Theory* **21** (2018), p. 145–161.

[64] T. Satoh – "On certain vector valued Siegel modular forms of degree two", *Math. Ann.* **274** (1986), p. 335–352.

[65] A. J. Scholl – "Motives for modular forms", *Invent. math.* **100** (1990), p. 419–430.

[66] J-P. Serre – *Rational points on curves over finite fields*, Documents Mathématiques, vol. 18, Société Mathématique de France, 2020.

[67] ———, *Rational points on curves over finite fields*, Documents Mathématiques, vol. 18, Société Mathématique de France, 2020.

[68] G. Shimura – "Sur les intégrales attachées aux formes automorphes", *J. Math. Soc. Japan* **11** (1959), p. 291–311.

[69] ———, "On purely transcendental fields automorphic functions of several variable", *Osaka Math. J.* **1** (1964), p. 1–14.

[70] K.-O. Stöhr & J. F. Voloch – "A formula for the Cartier operator on plane algebraic curves", *J. reine angew. Math.* **377** (1987), p. 49–64.

[71] O. Tommasi – "Rational cohomology of the moduli space of genus 4 curves", *Compos. Math.* **141** (2005), p. 359–384.

[72] F. Vermeulen – "Curves of fixed gonality with many rational points", preprint arXiv:2102.00900.

[73] A. Weil – "The field of definition of a variety", *Amer. J. Math.* **78** (1956), p. 509–524.

[74] R. Weissauer – "The trace of Hecke operators on the space of classical holomorphic Siegel modular forms of genus two", preprint arXiv:0909.1744.

[75] X. Xarles – "A census of all genus 4 curves over the field with 2 elements", preprint arXiv:2007.07822v1.

[76] Z. Zhou – "The a-number and the Ekedahl-Oort types of Jacobians of curves", Ph.D. Thesis, University of Amsterdam, 2019.

Gerard van der Geer, Korteweg-de Vries Instituut, Universiteit van Amsterdam, Postbus 94248, 1090 GE Amsterdam, The Netherlands • *E-mail :* g.b.m.vandergeer@uva.nl