Finite Fields and Their Applications 32 (2015) 207–232

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Counting curves over finite fields

Gerard van der Geer

Korteweg–de Vries Instituut, Universiteit van Amsterdam, Postbus 94248, 1090 GE Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 25 August 2014
Received in revised form 10 September 2014
Accepted 18 September 2014
Available online 4 November 2014
Communicated by H. Stichtenoth

MSC:
11G20
10D20
14G15
14H10

Keywords:
Curve
Finite field
Modular form
Moduli of curves
Cohomology

ABSTRACT

This is a survey on recent results on counting of curves over finite fields. It reviews various results on the maximum number of points on a curve of genus g over a finite field of cardinality q, but the main emphasis is on results on the Euler characteristic of the cohomology of local systems on moduli spaces of curves of low genus and its implications for modular forms.

1. Introduction

Reduction modulo a prime became a standard method for studying equations in integers after Gauss published his Disquisitiones Arithmeticae in 1801. In §358 of the Disquisitiones Gauss counts the number of solutions of the cubic Fermat equation

E-mail address: G.B.M.vanderGeer@uva.nl.

http://dx.doi.org/10.1016/j.ffa.2014.09.008
1071-5797/

$x^3 + y^3 + z^3 = 0$ modulo a prime p and finds for a prime $p \not\equiv 1 \pmod 3$ always $p + 1$ points on the projective curve, while for a prime $p \equiv 1 \pmod 3$ the number of points equals $p + 1 + a$, if one writes $4p = a^2 + 27b^2$ with $a \equiv 1 \pmod 3$ and he notes that $|a| \leq 2\sqrt{p}$. But although Galois introduced finite fields in 1830 and algebraic curves were one of the main notions in 19th century mathematics, one had to wait till the beginning of the 20th century before algebraic curves over finite fields became an important topic for mathematical investigation. Artin considered in his 1924 thesis (already submitted to Mathematische Zeitschrift in 1921) the function fields of hyperelliptic curves defined over a finite field and considered for such fields a zeta function $Z(s)$ that is an analogue of the Riemann zeta function and of the Dedekind zeta function for number fields. He derived a functional equation for them and formulated an analogue of the Riemann hypothesis that says that the zeros of the function of t obtained by substituting $t = q^{-s}$ in $Z(s)$ have absolute value $q^{-1/2}$. In 1931 Friedrich Karl Schmidt brought a more geometric approach by writing the zeta function for a smooth absolutely irreducible projective curve C over a finite field $\mathbb{F}_q$ as the generating function for the number of rational points $c(n) = \#C(\mathbb{F}_{q^n})$ over extension fields as

$$Z(t) = \exp\left(\sum_{n=1}^{\infty} c(n)\frac{t^n}{n}\right),$$

which turns out to be a rational function of t of the form

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)}$$

for some polynomial $P \in \mathbb{Z}[t]$ of degree $2g$ with g the genus of the curve. He observed that the functional equation $Z(1/qt) = q^{1-g}t^{2-2g}Z(t)$ is a consequence of the theorem of Riemann–Roch. A couple of years later (1934) Hasse proved the Riemann hypothesis for elliptic curves over finite fields using correspondences. The proof appeared in 1936, see [29]. Deuring observed then that to extend this result to curves of higher genus one needed a theory of algebraic correspondences over fields of arbitrary characteristic. This was at the time that the need was felt to build algebraic geometry on a more solid base that would allow one to do algebraic geometry over arbitrary fields. Weil was one of those who actively pursued this goal. Besides doing foundational work, he also exploited the analogy between geometry in characteristic zero and positive characteristic by extending an inequality on correspondences of Castelnuovo and Severi to positive characteristic and deduced around 1940 the celebrated Hasse–Weil inequality

$$\left|\#C(\mathbb{F}_q) - (q+1)\right| \leq 2g\sqrt{q}$$

for the number of rational points on a smooth absolutely irreducible projective curve C of genus g over a finite field $\mathbb{F}_q$ [51].

Geometry entered the topic more definitely when Weil applied the analogy with the Lefschetz fixed point theorem, which expresses the number of fixed points of a map on a compact manifold in terms of the trace of the induced map on (co-)homology, to the case of the Frobenius morphism on a projective variety over a finite field and formulated in 1949 the famous 'Weil Conjectures' on zeta functions of varieties over finite fields. Dwork set the first step by proving the rationality of the zeta function in 1960.

Grothendieck's revolution in algebraic geometry in the late 1950s started a new era in which it was possible to do algebraic geometry on varieties over finite fields. It also led to the construction of étale cohomology, which made it possible to carry out the analogy envisioned by Weil. The first milestone in this new era was Deligne's completion of the proof of the Weil conjectures in 1974.

Among all these developments the theme of curves over finite fields was pushed to the background, though there was progress. In 1969 Stepanov showed a new approach in [48] to deriving the Hasse–Weil bound for hyperelliptic curves by just using Riemann–Roch; Stark used it to get a somewhat stronger bound than Hasse–Weil for hyperelliptic curves over a prime field $\mathbb{F}_p$, see [47]. Stepanov's method was elegantly extended by Bombieri in [7] to prove the Hasse–Weil bound in the general case.

The return of curves over finite fields to the foreground around 1980 was triggered by an outside impulse, namely from coding theory. Goppa observed that one could construct good codes by evaluating meromorphic functions on a subset of the points of the projective line, where "good" meant that they reached the so-called Gilbert–Varshamov bound. He then realized that this could be generalized by evaluating meromorphic functions on a subset of the rational points of a higher genus curve, that is, by associating a code to a linear system on a curve over a finite field, cf. [27]. The quality of the code depended on the number of rational points of the curve. In this way it drew attention to the question how many rational points a curve of given genus g over a finite field $\mathbb{F}_q$ of given cardinality q could have. The 1981 paper by Manin [36] explicitly asks in the title for the maximum number of points on a curve over $\mathbb{F}_2$. Thus the question emerged how good the Hasse–Weil bound was.

2. The maximum number of points on a curve over a finite field

In [33] Ihara employed a simple idea to obtain a better estimate than the Hasse–Weil bound for the number of rational points on a curve over a finite field $\mathbb{F}_q$. The idea is to write

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n,$$

with α_i the eigenvalues of Frobenius on $H^1_{\text{et}}(C, \mathbb{Q}_\ell)$ for ℓ different from the characteristic, and to note that $\#C(\mathbb{F}_q) \leq \#C(\mathbb{F}_{q^2})$. By using the Cauchy–Schwartz inequality for the

α_i he found the improvement

$$\#C(\mathbb{F}_q) \leq q + 1 + \left[\left(\sqrt{(8q+1)g^2 + 4\left(q^2 - q\right)g} - g\right)/2\right].$$

For $g > (q - \sqrt{q})/2$ this is better than the Hasse–Weil bound. Instead of just playing off $\#C(\mathbb{F}_q)$ against $\#C(\mathbb{F}_{q^2})$, one can use the extensions of $\mathbb{F}_q$ of all degrees, and a systematic analysis (in [12]) due to Drinfel'd and Vlăduţ led to an asymptotic upper bound for the quantity

$$A(q) := \lim\sup_{g\to\infty} N_q(g)/g,$$

which was introduced by Ihara, with $N_q(g)$ as usual defined as

$$N_q(g) := \max\left\{\#C(\mathbb{F}_q) : g(C) = g\right\},$$

the maximum number of rational points on a smooth absolutely irreducible projective curve of genus g over $\mathbb{F}_q$. The resulting asymptotic bound is

$$A(q) \leq \sqrt{q} - 1.$$

As we shall see below, this is sharp for q a square.

The systematic study of $N_q(g)$ was started by Serre in the 1980s. He showed in [42] that by using some arithmetic the Hasse–Weil bound can be improved slightly to give

$$\left|\#C(\mathbb{F}_q) - (q+1)\right| \leq g\lfloor 2\sqrt{q}\rfloor,$$

as opposed to just $\leq \lfloor 2g\sqrt{q}\rfloor$. Serre applied the method of 'formules explicites' from number theory to the zeta functions of curves over finite fields to get better upper bounds. An even trigonometric polynomial

$$f(\theta) = 1 + 2\sum_{n\geq 1} u_n \cos n\theta$$

with real coefficients $u_n \geq 0$ such that $f(\theta) \geq 0$ for all real θ gives an estimate for $\#C(\mathbb{F}_q)$ of the form

$$\#C(\mathbb{F}_q) \leq a_f g + b_f,$$

with g the genus of C and a_f and b_f defined by setting $\psi = \sum_{n\geq 1} u_n t^n$ and

$$a_f = \frac{1}{\psi(1/\sqrt{q})} \quad \text{and} \quad b_f = 1 + \frac{\psi(\sqrt{q})}{\psi(1/\sqrt{q})}.$$

Oesterlé found the solution to the problem of finding the optimal choices for the functions f, see [41]. For $g > (q - \sqrt{q})/2$ these bounds are better than the Hasse–Weil bound.

Curves that reach the Hasse–Weil upper bound are called *maximal curves*. In such a case q is a square and $g \leq (q - \sqrt{q})/2$. Stichtenoth and Xing conjectured that for maximal curves over $\mathbb{F}_q$ one either has that $g = (q - \sqrt{q})/2$ or $g \leq (\sqrt{q} - 1)^2/4$, and after they made considerable progress towards it, see [49], the conjecture was proved by Fuhrmann and Torres, cf. [16]. In this direction it is worth mentioning a recent result of Elkies, Howe and Ritzenthaler [14] that gives a bound on the genus of curves whose Jacobian has Frobenius eigenvalues in a given finite set.

Stichtenoth conjectured that all maximal curves over $\mathbb{F}_{q^2}$ are dominated by a 'hermitian' curve defined by an equation

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

This curve is of genus $q(q-1)/2$ and has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$. This conjecture was disproved by Giulietti and Korchmáros, who exhibited a counterexample over $\mathbb{F}_{q^6}$, see [26]. In [40] Rück and Stichtenoth proved that maximal curves with $g = (q - \sqrt{q})/2$ are isomorphic to the hermitian curve.

For a curve C over a finite field $\mathbb{F}_q$ the quantity

$$\delta := \left(q + 1 + g[2\sqrt{q}]\right) - \#C(\mathbb{F}_q)$$

is called the *defect*. The result of Fuhrmann and Torres proves the non-existence of curves with a small defect. Many more results excluding curves with small defects have been obtained by various arithmetic and geometric methods, see especially work of Howe and Lauter; we refer to the papers [30–32,34,35,45].

However, testing how good the resulting upper bounds on $N_q(g)$ are, can only be done by providing a curve with a number of points that reaches or comes close to this upper bound; that is, by constructing a curve with many points.

In [42–44] Serre listed the value of $N_q(g)$ for small values of q and g or a small interval in which $N_q(g)$ lies when the value of $N_q(g)$ was not known. Wirtz extended in [54] these tables for small q that are powers of 2 and 3 by carrying out a computer search in certain families. (His table is reproduced in [22, p. 185].) In the 1990s the challenge to find curves over finite fields with many points, that is, close to the best upper bound for $N_q(g)$, attracted a lot of interest. In 1996 van der Geer and van der Vlugt published 'Tables for the function $N_q(g)$' that listed intervals for the function $N_q(g)$ for $1 \leq g \leq 50$ and q a small power of 2 or 3. These tables were regularly updated and published on a website. In 1998 the tables were replaced by a new series of tables ('Tables of Curves with Many Points'), one of the first of which was published in Mathematics of Computation [23], and it was regularly updated on a website. In a series of papers (see [37] and the references there) Niederreiter and Xing efficiently applied methods from class field theory to construct curves with many points, resulting in many good entries in the tables. Other methods, like the ones used in [22,20], employed fiber products of Artin–Schreier curves or were based on coding theory, see [23] and the references given there. The resulting tables were the joint effort of many people. The last update was dated October 2009; after that the tables were replaced by a new website, www.manypoints.org, an initiative of van der Geer, Howe, Lauter and Ritzenthaler, where new records can be registered. At the end of this review we include a copy of a recent version of the tables for small powers of 2 and 3 and $1 \leq g \leq 50$. As the reader will see, the intervals for $N_q(g)$ are still quite large for many pairs (g, q).

As mentioned above, the result of Drinfel'd and Vlăduţ led to the asymptotic bound $A(q) \leq \sqrt{q} - 1$. For q a square, Ihara and independently Tsfasman, Vlăduţ and Zink showed in [50,33] that modular curves have many rational points and that one can use this to prove

$$A(q) \geq \sqrt{q} - 1,$$

so that $A(q) = \sqrt{q} - 1$ for q a square. It came as a surprise in 1995 when Garcia and Stichtenoth came forward (see [17]) with a tower over $\mathbb{F}_{q^2}$ (q an arbitrary prime power)

$$\ldots C_i \to C_{i-1} \to \cdots \to C_2 \to C_1$$

of Artin–Schreier curves defined over $\mathbb{F}_{q^2}$ by a simple recursion with

$$\lim_{i \to \infty} g(C_i) = \infty \quad \text{and} \quad \lim_{i \to \infty} \frac{\#C_i(\mathbb{F}_{q^2})}{g(C_i)} = q - 1.$$

The simple recursion starts with $\mathbb{P}^1$ over $\mathbb{F}_{q^2}$ with function field $F_1 = \mathbb{F}_{q^2}(x_1)$ and defines Artin–Schreier extensions F_n by with $F_{n+1} = F_n(y_{n+1})$ given by $y_{n+1}^q + y_{n+1} = x_n^{q+1}$ with $x_{n+1} := y_{n+1}/x_n$ for $n \geq 1$. This has stimulated much research. Elkies has shown in [13] that this tower is in fact a tower of modular curves. Over fields the cardinality of which is not a square it is more difficult to find good towers. There are towers resulting from class field theory, see for example [37]. In a paper from 1985, [55], Zink used certain degenerate Shimura surfaces to construct a tower over $\mathbb{F}_{p^3}$ for p prime with limit $\#(C_i(\mathbb{F}_{p^3}))/g(C_i) \geq 2(p^2 - 1)/(p + 2)$. The first good explicit wild tower in the non-square case was a tower of Artin–Schreier covers over $\mathbb{F}_8$ with limit $3/2$, see [24]. This has been generalized by Bezerra, Garcia and Stichtenoth to towers over $\mathbb{F}_q$ with q a cube. If $q = \ell^3$ with ℓ prime power they deduce that

$$A(\ell^3) \geq \frac{2(\ell^2 - 1)}{\ell + 2},$$

and this was extended again in [2] to all nonprime finite fields $\mathbb{F}_q$. For a detailed review of the progress on towers we refer to the paper by Garcia and Stichtenoth [18].

The question of the maximum number of points on a curve of given genus g over a finite field $\mathbb{F}_q$ is just one small part of the question which values the number of points on a curve of genus g over $\mathbb{F}_q$ can have. The answer can take various forms. One answer is in [1], where it is shown that for sufficiently large genus, every value in a small interval $[0, c]$ is assumed. But, more precisely, one may ask which values are assumed and how often if the curve varies through the moduli space of curves of genus g defined over $\mathbb{F}_q$. The answer could be presented as a list of all possible Weil polynomials with the frequencies with which they occur. The question arises how to process all the information contained in such a list. For example, take the case of elliptic curves over a finite prime field $\mathbb{F}_p$. Each isomorphism class $[E]$ of elliptic curves defined over $\mathbb{F}_p$ defines a pair $\{\alpha_E, \bar{\alpha}_E\}$ of algebraic integers with $\#E(\mathbb{F}_p) = p+1-\alpha_E-\bar{\alpha}_E$. We can study the weighted 'moments'

$$\sigma_k(p) := -\sum \frac{\alpha_E^k + \alpha_E^{k-1}\bar{\alpha}_E + \cdots + \bar{\alpha}_E^k}{\#\mathrm{Aut}_{\mathbb{F}_p}(E)},$$

where the sum is over a complete set of representatives E of all the isomorphism classes of elliptic curves over $\mathbb{F}_p$. For odd k the answer is 0 due to the fact that the contribution of an elliptic curve and its -1-twist cancel. For $k = 0$ we find $-q$, while for even k with $2 \leq k \leq 8$ we find 1. But for $k = 10$ we find for $p = 2, 3, 5, 7, 11$ the following values

p	2	3	5	7	11
σ_{10}	-23	253	4831	$-16\,743$	534 613

Many readers will not fail to notice that the numbers appearing here equal $\tau(p) + 1$ with $\tau(p)$ the pth Fourier coefficient of the celebrated modular form $\Delta = \sum \tau(n)q^n$ of weight 12 on $\mathrm{SL}(2, \mathbb{Z})$ with Fourier development

$$\Delta = q - 24\,q^2 + 252\,q^3 - 1472\,q^4 + 4830\,q^5 - 6048\,q^6 - 16\,744\,q^7 + \cdots$$

where the reader will hopefully forgive us for having used the customary $q = e^{2\pi i\tau}$. This hints at treasures hidden in such frequency lists of Weil polynomials and the rest of this survey paper is dedicated to this phenomenon. (For a different view on such statistics we refer to [8].)

3. Varieties over the integers

A customary approach for studying algebraic varieties begins by trying to calculate their cohomology. For a variety defined over a finite field $\mathbb{F}_q$ we can extract a lot of information on the cohomology by counting rational points of the variety over the extension fields $\mathbb{F}_{q^r}$. The connection is through the Lefschetz trace formula which says that the number of points equals the trace of the Frobenius morphism on the rational Euler characteristic of the variety. And for a variety defined over the integers we can look at its reduction modulo a prime and then count rational points over extension fields $\mathbb{F}_{p^r}$. This characteristic p information can then be pieced together to find cohomological information about the variety in characteristic zero, more precisely, about the cohomology as a representation of the absolute Galois group of the rational numbers.

Let us look at proper varieties defined over the integers with good reduction everywhere. The first examples are given by projective space and Grassmann varieties. For projective space we have $\#\mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + \cdots + 1$ and for the Grassmann variety $G(d,n)$ of d-dimensional projective linear subspaces of $\mathbb{P}^n$ we have

$$\#G(d,n) = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q := \frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^d)}{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}.$$

In fact, for these varieties we have a cell decomposition and we know the class in the Grothendieck group of varieties. Recall that if k is a perfect field k and Var_k is the category of algebraic varieties over k, then the Grothendieck group $K_0(\mathrm{Var}_k)$ of varieties over k is, by definition, the free abelian group generated by the symbols $[X]$ with X an object of Var_k modulo the two relations (i) $[X] = [Y]$ whenever $X \cong Y$; (ii) for every closed subvariety Z of X we have $[X] = [Z] + [X \backslash Z]$. The class of the affine line $\mathbb{A}^1$ is denoted by $\mathbf{L}$ and called the Lefschetz class. For example, for the projective space $\mathbb{P}^n$ and the Grassmann variety $G(d,n)$ we find

$$[\mathbb{P}^n] = \mathbf{L}^n + \mathbf{L}^{n-1} + \cdots + 1 \quad \text{and} \quad [G(d,n)] = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_{\mathbf{L}}.$$

For varieties X like projective spaces and Grassmannian varieties, where we know a cell decomposition, we find that there exists a polynomial $P \in \mathbb{Z}[x]$ such that $\#X(\mathbb{F}_q) = P(q)$ for every finite field $\mathbb{F}_q$. Conversely, one can ask how much we can learn about a proper smooth variety defined over the integers by counting the number of $\mathbb{F}_q$-rational points for many fields $\mathbb{F}_q$.

For example, if we find that there exists such a polynomial P with $\#X(\mathbb{F}_q) = P(q)$, what do we know? There is a theorem by van den Bogaart and Edixhoven [6] which says that for a proper variety we then know the ℓ-adic étale cohomology for all ℓ of $X_{\overline{\mathbb{Q}}}$ as a representation of the absolute Galois group of the rational numbers: the cohomology is a direct sum of copies of the cyclotomic representation $\mathbb{Q}_\ell(-i)$ in degree $2i$ and zero in odd degrees; moreover the number of copies of $\mathbb{Q}_\ell(-i)$ is given by the ith coefficient of P. (For non-proper spaces then the result holds for the Euler characteristic in a suitable Grothendieck group.) Note that the realization of the motive $\mathbf{L}^i$ as a Galois representation equals $\mathbb{Q}_\ell(-i)$.

The spaces $\mathbb{P}^n$ and the Grassmann varieties are moduli spaces as they parametrize linear subspaces of projective space. The first further examples of varieties defined over the integers with everywhere good reduction are also moduli spaces, the moduli spaces $\mathcal{M}_g$ of curves of genus g and the moduli spaces $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g. More generally, there are the moduli spaces $\mathcal{M}_{g,n}$ of n-pointed curves of genus g and their Deligne–Mumford compactifications $\overline{\mathcal{M}}_{g,n}$ of stable n-pointed curves. All these spaces, $\mathcal{A}_g$, $\mathcal{M}_g$, $\mathcal{M}_{g,n}$ and $\overline{\mathcal{M}}_{g,n}$, are Deligne–Mumford stacks defined over the integers and smooth over $\mathbb{Z}$. The spaces $\overline{\mathcal{M}}_{g,n}$ are also proper over $\mathbb{Z}$. These spaces constitute the most intriguing series of varieties (or rather Deligne–Mumford stacks) over the integers with everywhere good reduction. In the last two decades our knowledge about them has increased dramatically, but clearly so much remains to be discovered.

While the cohomology of projective space and the Grassmann varieties is a polynomial in $\mathbf{L}$ (or $\mathbb{Q}(-1)$), it is unreasonable to expect the same for the moduli space $\mathcal{A}_g$ and $\mathcal{M}_{g,n}$. In fact, we know that over the complex numbers $\mathcal{A}_g$ can be described as a quotient $\mathrm{Sp}(2g,\mathbb{Z})\backslash\mathfrak{H}_g$, with $\mathfrak{H}_g$ the Siegel upper half-space (see below), and that modular forms are supposed to contribute to its cohomology. In fact, the compactly supported cohomology possesses a mixed Hodge structure and cusp forms of weight $g+1$ (see next section) contribute to the first step in the Hodge filtration on middle-dimensional cohomology. Since we know that for large g there exist non-trivial cusp forms of this weight (e.g. $g = 11$) this shows that the cohomology is not so simple. In fact, we know that the cohomology can be described in terms of automorphic forms on the symplectic group $\mathrm{Sp}(2g)$. Despite this, for low values of g and n the cohomology of $\mathcal{M}_{g,n}$ can be a polynomial in $\mathbf{L}$. For example, for $g = 1$ and $n \leq 9$, for $g = 2$ with $n \leq 7$ and $g = 3$ for $n \leq 7$ we have explicit polynomial formulas for the number of points over finite fields, and hence for the Euler characteristic of the moduli space $\mathcal{M}_{g,n} \otimes \mathbb{F}_q$ as a polynomial in $\mathbf{L}$, see Getzler [25] and Bergström [3].

If one does not find an explicit polynomial in q that gives the number of $\mathbb{F}_q$-rational points on our moduli space over $\mathbb{F}_q$, one nevertheless might try to count the number of $\mathbb{F}_q$-rational points of $\mathcal{A}_g \otimes \mathbb{F}_p$ to get information on the Euler characteristic of the cohomology. Since $\mathcal{A}_g \otimes \mathbb{F}_p$ (or $\mathcal{M}_g \otimes \mathbb{F}_p$) is a moduli space its points are represented by objects (abelian varieties or curves) and the first question then is how to represent the objects parametrized by $\mathcal{A}_g$ (or $\mathcal{M}_g$). For $g = 1$ this is clear. If we make a list of all elliptic curves defined over $\mathbb{F}_q$ up to isomorphism over $\mathbb{F}_q$ and calculate for each such elliptic curve the number of $\mathbb{F}_q$-rational points we should be able to calculate $\#\mathcal{M}_{1,n}(\mathbb{F}_q)$ for all $n \geq 1$. (This has to be taken with a grain of salt as $\mathcal{M}_{1,n}$ is a stack and not a variety; this aspect is taken care of by taking into account the automorphism groups of the objects.) This is the approach we shall take in the next section.

4. Counting points on elliptic curves

Hasse proved in 1934 that the number of rational points on an elliptic curve E defined over a finite field $\mathbb{F}_q$ can be given as

$$\#E(\mathbb{F}_q) = q + 1 - \alpha - \bar{\alpha}$$

with $\alpha = \alpha_E$ an algebraic integer with $\alpha\bar{\alpha} = q$. Isomorphism classes of elliptic curves over the algebraic closure $\overline{\mathbb{F}}_q$ are given by their j-invariant $j(E)$; over the field $\mathbb{F}_q$ this is no longer true due to automorphisms of the curve. But for any given value of $j \in \mathbb{F}_q$ there is an elliptic curve E_j defined over $\mathbb{F}_q$ and the $\mathbb{F}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with this j-invariant correspond 1–1 with the elements of the pointed set $H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}, \mathrm{Isom}(E_j))$ with Isom the group of $\mathbb{F}_q$-automorphisms of the genus 1 curve underlying E. For each E_j this set contains at least two elements. Nevertheless, a given value of $j \in \mathbb{F}_q$ contributes just

$$\sum_{E/\mathbb{F}_q/\cong_{\mathbb{F}_q},\, j(E)=j} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)} = 1$$

to the number of elliptic curves defined over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism, if we count them in the right way, that is, with weight $1/\#\mathrm{Aut}_{\mathbb{F}_q}(E)$, see [21] for a proof.

We are interested in how the α vary over the whole j-line. To this end one considers the moments of the α_E

$$\sigma_a(q) := -\sum_{E/\mathbb{F}_q/\cong_{\mathbb{F}_q}} \frac{\alpha_E^a + \alpha_E^{a-1}\bar{\alpha}_E + \cdots + \bar{\alpha}_E^a}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)}, \tag{1}$$

where the sum is over all elliptic curves defined over $\mathbb{F}_q$ up to isomorphism over $\mathbb{F}_q$ and a is a non-negative integer. For odd a one finds zero, due to the fact that the contributions of a curve and its -1-twist cancel. But for even $a > 0$ one finds something surprising and very interesting at which we hinted at the end of Section 2: for a prime p we have

$$\sigma_a(p) = 1 + \text{Trace of } T(p) \text{ on } S_{a+2}\big(\mathrm{SL}(2,\mathbb{Z})\big) \tag{2}$$

with $S_k(\mathrm{SL}(2,\mathbb{Z}))$ the space of cusp forms of weight k on $\mathrm{SL}(2,\mathbb{Z})$ and $T(p)$ the Hecke operator associated to p on this space. Recall that a modular form of weight k on $\mathrm{SL}(2,\mathbb{Z})$ is a holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ on the upper half-plane $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ of $\mathbb{C}$ that satisfies

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \text{for all } \tau \in \mathfrak{H} \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),$$

in particular, it satisfies $f(\tau + 1) = f(\tau)$ and thus admits a Fourier development

$$f = \sum_n a(n) e^{2\pi i n \tau},$$

and we require that f be holomorphic at infinity, i.e. $a(n) = 0$ for $n < 0$. A *cusp form* is a modular form with vanishing constant term $a(0) = 0$. The modular forms of given weight k form a vector space $M_k(\mathrm{SL}(2,\mathbb{Z}))$ of finite dimension; this dimension is zero for

k negative or odd and equals $[k/12] + 1$ for even $k \not\equiv 2 \pmod{12}$ and $[k/12]$ for even $k \equiv 2 \pmod{12}$. The subspace $S_k(\mathrm{SL}(2,\mathbb{Z}))$ of cusp forms of weight k is of codimension 1 in $M_k(\mathrm{SL}(2,\mathbb{Z}))$ if the latter is nonzero. One has an algebra of Hecke operators $T(n)$ with $n \in \mathbb{Z}_{\geq 1}$ operating on $M_k(\mathrm{SL}(2,\mathbb{Z}))$ and $S_k(\mathrm{SL}(2,\mathbb{Z}))$ and there is a basis of common eigenvectors, called eigenforms, for all $T(n)$ with the property that $T(n)f = a(n)f$ for such an eigenform f if one normalizes these such that $a(1) = 1$. Modular forms belong to the most important objects in arithmetic algebraic geometry and number theory. It may come as a surprise that we can obtain information about modular forms, that are holomorphic functions on $\mathfrak{H}$, by counting points on elliptic curves over finite fields.

On the other hand, our knowledge of modular forms on $\mathrm{SL}(2,\mathbb{Z})$ is extensive. Since a product of modular forms of weights k_1 and k_2 is a modular form of weight $k_1 + k_2$ one obtains a graded algebra $\bigoplus_k M_k(\mathrm{SL}(2,\mathbb{Z}))$ of modular forms on $\mathrm{SL}(2,\mathbb{Z})$ and it is the polynomial algebra generated by the Eisenstein series E_4 and E_6, explicit modular forms of weights 4 and 6. This does not tell us much about the action of the Hecke operators, but the fact is that one has a closed formula for the trace of the Hecke operator $T(n)$ on the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$ for even $k > 0$:

$$\mathrm{Trace}\big(T(n)\big) = -\frac{1}{2}\sum_{t=-\infty}^{\infty} P_k(t,n)H\big(4n - t^2\big) - \frac{1}{2}\sum_{dd'=n} \min\big(d,d'\big)^{k-1},$$

where $P_k(t,n)$ is the coefficient of x^{k-2} in the Taylor series of $(1 - tx + nx^2)^{-1}$ and $H(n)$ is a class number defined as follows. For $n < 0$ we put $H(n) = 0$; furthermore $H(0) = -1/12$, while for $n > 0$ we let $H(n)$ be the number of $\mathrm{SL}(2,\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = -n$ with the forms equivalent to $x^2 + y^2$ (resp. to $x^2 + xy + y^2$) counted with weight 1/2 (resp. 1/3). So in view of all we know, we do not gain new information from our counts of points over finite fields.

The fact that we can obtain information on modular forms by counting points over finite fields illustrates two ideas: the idea of Weil that counting points on varieties over finite fields gives the trace of Frobenius on the cohomology and the idea that the cohomology of the variety obtained by reducing a variety defined over the integers modulo p reflects aspects of the cohomology of the variety over the integers. Moreover, it shows that modular forms are cohomological invariants.

Note that the expression $\sigma_a(p)$ in (1) is the sum over all elliptic curves defined over $\mathbb{F}_p$ up to isomorphism of the negative of the trace of Frobenius on the ath symmetric power of the cohomology $H^1_{\mathrm{et}}(E \otimes \overline{\mathbb{F}}_p, \mathbb{Q}_\ell)$ with ℓ a prime different from p.

One thus is led to look at the local system $\mathbb{V} := R^1\pi_*\mathbb{Q}_\ell$ on the moduli space $\mathcal{A}_1$ of elliptic curves with $\pi : \mathcal{X}_1 \to \mathcal{A}_1$ the universal family of elliptic curves. This is a local system of vector spaces with fiber over $[E]$ equal to $H^1(E, \mathbb{Q}_\ell)$. Note that $\pi : \mathcal{X}_1 \to \mathcal{A}_1$ is defined over $\mathbb{Z}$.

For even $a > 0$ we look at the local system $\mathbb{V}_a = \mathrm{Sym}^a(\mathbb{V})$; this is a local system of rank $a + 1$ on $\mathcal{A}_1$ with fiber $\mathrm{Sym}^a(H^1(E, \mathbb{Q}_\ell))$ over a point $[E]$ of the base $\mathcal{A}_1$. It is in the cohomology of $\mathbb{V}_a \otimes \mathbb{C}$ over $\mathcal{A}_1 \otimes \mathbb{C}$ that we find the modular forms. In fact, a famous theorem of Eichler and Shimura says that

$$H^1(\mathcal{A}_1 \otimes \mathbb{C}, \mathbb{V}_a \otimes \mathbb{C}) \cong S_{a+2}\big(\mathrm{SL}(2,\mathbb{Z})\big) \oplus \overline{S}_{a+2}\big(\mathrm{SL}(2,\mathbb{Z})\big) \oplus \mathbb{C}. \tag{3}$$

So the space $S_{a+2}(\mathrm{SL}(2,\mathbb{Z}))$ of cusp forms of weight $a+2$ and its complex conjugate constitute this cohomology, except for the summand $\mathbb{C}$. This latter summand is a (partial) contribution of the Eisenstein series E_{a+2} of weight $a+2$. We refer to the paper by Deligne [11].

The relation just given is just one aspect of a deeper motivic relation; this aspect deals with the complex moduli space $\mathcal{A}_1 \otimes \mathbb{C}$; if we look at $\mathcal{A}_1 \otimes \mathbb{F}_p$ we see another aspect. For $\ell \neq p$ we have an isomorphism

$$H^i_c(\mathcal{A}_1 \otimes \overline{\mathbb{F}}_p, \mathbb{V}_a) \xrightarrow{\cong} H^i_c(\mathcal{A}_1 \otimes \overline{\mathbb{Q}}_p, \mathbb{V}_a)$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-representations, which bridges the gap between characteristic 0 and characteristic p. We can use this to see that for compactly supported étale ℓ-adic cohomology with ℓ different from p, the trace of Frobenius on $H^1_c(\mathcal{A}_1 \otimes \overline{\mathbb{F}}_p, \mathbb{V}_a)$ equals 1 plus the trace of the Hecke operator $T(p)$ on $S_{a+2}(\mathrm{SL}(2,\mathbb{Z}))$, and this explains the identity (2). A more sophisticated version is that

$$\big[H^1_c(\mathcal{A}_1 \otimes \mathbb{Q}, \mathbb{V}_a)\big] = S[a+2] + 1, \tag{4}$$

where the left hand side is viewed as a Chow motive with rational coefficients and $S[k]$ denotes the motive associated by Scholl to the space of cusp forms of even weight $k > 2$ on $\mathrm{SL}(2,\mathbb{Z})$. This incorporates both the Hodge theoretic and the Galois theoretic version.

But for elliptic curves and modular forms on $\mathrm{SL}(2,\mathbb{Z})$ we have explicit knowledge and this way of mining information about modular forms by counting over finite fields might seem superfluous. Nevertheless, it is a practical method. Once one has a list of all elliptic curves defined over $\mathbb{F}_q$ up to isomorphism over $\mathbb{F}_q$, together with their number of points over $\mathbb{F}_q$ and the order of their automorphism groups, then one can easily calculate the trace of the Hecke operator $T(q)$ on the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$ for *all* even weights $k > 2$.

The situation changes drastically if one considers curves of higher genus or abelian varieties of higher dimension and modular forms of higher degree. There our knowledge of modular forms is rather restricted and counting curves over finite fields provides us with a lot of useful information that is difficult to access otherwise.

We end this section with giving the relation between the cohomology of the local systems $\mathbb{V}_a$ on $\mathcal{A}_1$ and the cohomology of $\mathcal{M}_{1,n}$. The following beautiful formula due to Getzler [25] expresses the Euler characteristic $e_c(\mathcal{M}_{1,n+1})$ in terms of the Euler characteristics of the local systems $\mathbb{V}_a$ in a concise way as a residue for $x = 0$ in a formal expansion as follows:

$$\frac{e_c(\mathcal{M}_{1,n+1})}{n!} = \mathrm{res}_0 \left[\binom{L - x - L/x}{n} \sum_{k=1}^{\infty} \left(\frac{S[2k+2]+1}{L^{2k+1}} x^{2k} - 1 \right) \cdot (x - L/x) dx \right]$$

5. Counting curves of genus two

The notion of elliptic curve allows two obvious generalizations: one is that of an abelian variety of dimension $g > 1$ and the other one is that of a curve of genus $g > 1$. For $g = 2$ these two generalizations are rather close. The moduli space $\mathcal{M}_2$ of curves of genus 2 admits an embedding in the moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces by the Torelli map, which associates to a curve of genus 2 its Jacobian. The image is an open part, the complement of the locus $\mathcal{A}_{1,1}$ of products of elliptic curves. The moduli spaces $\mathcal{M}_2$ and $\mathcal{A}_2$ are defined over $\mathbb{Z}$.

The Hasse–Weil theorem tells us that for a curve C of genus 2 defined over a finite field $\mathbb{F}_q$ the action of Frobenius on $H^1_{\mathrm{et}}(C \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$, with ℓ a prime different from the characteristic, is semi-simple and the eigenvalues α satisfy $\alpha\bar{\alpha} = q$.

The analogues of the notions that appeared in the preceding section are available. We have the universal curve of genus 2 over $\mathcal{M}_2$, denoted by $\gamma : \mathcal{C}_2 \to \mathcal{M}_2$, and the universal principally abelian surface $\pi : \mathcal{X}_2 \to \mathcal{A}_2$. This gives rise to a local system $\mathbb{V} := R^1\pi_*\mathbb{Q}_\ell$ on $\mathcal{A}_2$. This is a local system of rank 4 and the pull back of this system under the Torelli morphism coincides with $R^1\gamma_*\mathbb{Q}_\ell$. The fiber of this local system $\mathbb{V}$ over a point $[X]$ with X a principally polarized abelian variety, is $H^1(X, \mathbb{Q}_\ell)$ and this is a $\mathbb{Q}_\ell$-vector space of dimension 4 and $\mathbb{V}$ is provided with a non-degenerate symplectic pairing $\mathbb{V} \times \mathbb{V} \to \mathbb{Q}_\ell(-1)$ that comes from the Weil pairing.

Instead of just considering the symmetric powers $\mathrm{Sym}^a\mathbb{V}$ of $\mathbb{V}$, as we did for $g = 1$, we can make more local systems now. To every irreducible finite-dimensional representation of $\mathrm{Sp}(4, \mathbb{Q})$, say of highest weight $\lambda = (a, b)$ with $a \geq b$, we can associate a local system $\mathbb{V}_\lambda$ by applying a Schur functor to $\mathbb{V}$. For $\lambda = (a, 0)$ we recover $\mathrm{Sym}^a(\mathbb{V})$, and for example, $\mathbb{V}_{(1,1)}$ is a 5-dimensional local system occurring in $\bigwedge^2 \mathbb{V}$. A weight $\lambda = (a, b)$ is called *regular* if $a > b > 0$.

We then look at the Euler characteristic

$$\sum_{i=0}^{6} (-1)^i \left[H^i_c(\mathcal{A}_2 \otimes \overline{\mathbb{Q}}, \mathbb{V}_\lambda) \right],$$

where we consider the cohomology groups either as Hodge structures over the complex numbers if we deal with complex cohomology over $\mathcal{A}_2 \otimes \mathbb{C}$, or as ℓ-adic Galois representations when we consider ℓ-adic étale cohomology over $\mathcal{A}_2 \otimes \overline{\mathbb{Q}}$, and the brackets indicate that the sum is taken in a Grothendieck group of the appropriate category

(Hodge structures or Galois representations). The information on the cohomology over $\mathbb{F}_p$ for all p together gives the whole information over $\mathbb{Q}$.

On the other hand the notion of modular form also generalizes. The moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized complex abelian varieties can be represented by a quotient

$$\mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}_2$$

with $\mathfrak{H}_2 = \{\tau \in \mathrm{Mat}(2\times 2,\mathbb{C}) : \tau^t = \tau,\ \mathrm{Im}(\tau) > 0\}$, the Siegel upper half-space of degree 2. The symplectic group $\mathrm{Sp}(4,\mathbb{Z})$ acts on $\mathfrak{H}_2$ in the usual way by

$$\tau \mapsto (a\tau+b)(c\tau+d)^{-1} \quad \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z}).$$

A holomorphic function $f : \mathfrak{H}_2 \to W$ with W a finite-dimensional complex vector space that underlies a representation ρ of $\mathrm{GL}(2,\mathbb{C})$, is called a Siegel modular form of weight ρ if f satisfies

$$f\big((a\tau+b)(c\tau+d)^{-1}\big) = \rho(c\tau+d)f(\tau) \quad \text{for all } \tau \in \mathfrak{H}_2 \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z}).$$

If ρ is the 1-dimensional representation $\det^k$, then f is a scalar-valued function and is called a classical Siegel modular form of weight k. The Siegel modular forms of a given weight ρ form a finite-dimensional vector space $M_\rho(\mathrm{Sp}(4,\mathbb{Z}))$. It contains a subspace $S_\rho(\mathrm{Sp}(4,\mathbb{Z}))$ of cusp forms characterized by a growth condition.

Without loss of generality we may consider only irreducible representations ρ of $\mathrm{GL}(2)$. Such a representation is of the form $\mathrm{Sym}^j(W) \otimes \det(W)^k$ with W the standard representation. Therefore we shall use the notation $S_{j,k}(\mathrm{Sp}(4,\mathbb{Z}))$ instead of $S_\rho(\mathrm{Sp}(4,\mathbb{Z}))$, and similarly $M_{j,k}(\mathrm{Sp}(4,\mathbb{Z}))$ for $M_\rho(\mathrm{Sp}(4,\mathbb{Z}))$. We know that $M_{j,k}(\mathrm{Sp}(4,\mathbb{Z}))$ vanishes if j is odd or negative and also if k is negative. For the graded algebra of classical Siegel modular forms

$$M = \bigoplus_k M_{0,k}\big(\mathrm{Sp}(4,\mathbb{Z})\big)$$

generators are known by work of Igusa. For a few cases of low values of j we know generators for the M-module $\bigoplus_k M_{j,k}(\mathrm{Sp}(4,\mathbb{Z}))$.

One also has a commutative algebra of Hecke operators acting on the spaces $M_\rho(\mathrm{Sp}(4,\mathbb{Z}))$ and $S_\rho(\mathrm{Sp}(4,\mathbb{Z}))$. But in general we know much less than for genus 1.

In order to get information about Siegel modular forms by counting curves of genus 2 over finite fields one needs an analogue of the formula (2) (or (4)).

For genus 1 we considered only the cohomology group H^1. It is known by work of Faltings that for a local system $\mathbb{V}_\lambda$ with regular weight the cohomology groups $H^i_c(\mathcal{A}_2 \otimes \mathbb{Q}, \mathbb{V}_\lambda)$ vanish unless $i = 3 = \dim \mathcal{A}_2$. If W_λ is an irreducible representation of $\mathrm{Sp}(4,\mathbb{Q})$

of highest weight λ, then the Weyl character formula expresses the trace of an element of $\mathrm{Sp}(4,\mathbb{Q})$ as a symmetric function σ_λ of the roots of its characteristic polynomial.

Since we can describe curves of genus 2 very explicitly, we therefore consider for a curve C of genus 2 over $\mathbb{F}_q$ with eigenvalues α_1, $\bar{\alpha}_1$, α_2, $\bar{\alpha}_2$ of Frobenius, i.e. such that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \bar{\alpha}_1^n - \alpha_2^n - \bar{\alpha}_2^n,$$

the expression

$$\frac{\sigma_\lambda(\alpha_1, \bar{\alpha}_1, \alpha_2, \bar{\alpha}_2)}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)}$$

and sum this over all isomorphism classes of genus 2 curves defined over $\mathbb{F}_q$. Here we are using the fact that each $\mathbb{F}_q$-isomorphism class of genus 2 curves defined over $\mathbb{F}_q$ contains a curve defined over $\mathbb{F}_q$. In this way we find the analogue of the sum $\sigma_a(q)$ defined in the preceding section. This gives us a way to calculate the trace of Frobenius on the Euler characteristic of the cohomology of the local system $\mathbb{V}_{a,b}$ on $\mathcal{M}_2 \otimes \overline{\mathbb{F}}_p$. Define the (motivic) Euler characteristic

$$e_c(\mathcal{M}_2 \otimes \mathbb{Q}, \mathbb{V}_{a,b}) := \sum_{i=0}^{6} (-1)^i \bigl[H^i(\mathcal{M}_2 \otimes \mathbb{Q}, \mathbb{V}_{a,b})\bigr]$$

and similarly $e_c(\mathcal{A}_2 \otimes \mathbb{Q}, \mathbb{V}_{a,b})$, where the interpretation (Hodge structures or Galois modules) depends on whether one takes complex cohomology or ℓ-adic étale cohomology. We can then calculate the trace of Frobenius on $e_c(\mathcal{M}_2 \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{a,b})$ and $e_c(\mathcal{A}_2 \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{a,b})$ by counting curves of genus 2 over $\mathbb{F}_p$. The difference between the two

$$e_c(\mathcal{A}_2 \otimes \mathbb{Q}, \mathbb{V}_{a,b}) - e_c(\mathcal{M}_2 \otimes \mathbb{Q}, \mathbb{V}_{a,b}) = e_c(\mathcal{A}_{1,1} \otimes \mathbb{Q}, \mathbb{V}_{a,b})$$

is the contribution from abelian surfaces that are products of two elliptic curves. Or phrased differently, from stable curves of genus 2 that consists of two elliptic curves meeting in one point.

How does this relate to the trace of Hecke operators on a space $S_\rho(\mathrm{Sp}(4,\mathbb{Z}))$? There is an analogue of the relation (2), but the analogue of the term 1 there is more complicated. Based on extensive calculations, in joint work with Carel Faber [15] we formulated a conjecture that is a precise analogue of (2). We gave a formula for the Euler characteristic of the local system $\mathbb{V}_{a,b}$ in the Grothendieck group of ℓ-adic Galois representations.

The formula says that

$$\begin{aligned}&\mathrm{Trace}\bigl(T(p), S_{a-b,b+3}\bigl(\mathrm{Sp}(4,\mathbb{Z})\bigr)\bigr)\\ &\quad = -\mathrm{Trace}\bigl(F_p, e_c(\mathcal{A}_2 \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{a,b})\bigr) + \mathrm{Trace}\bigl(F_p, e_{2,\mathrm{extra}}(a,b)\bigr)\end{aligned}$$

with $e_{2,\mathrm{extra}}(a,b)$ a correction term given by

$$s_{a-b+2} + s_{a_b+4}\big(S[a-b+2]+1\big)\mathbf{L}^{b+1} + \begin{cases} S[b+2]+1 & a \text{ even} \\ -S[a+3] & a \text{ odd.} \end{cases}$$

Here $s_k = \dim S_k(\mathrm{SL}(2,\mathbb{Z}))$ and $\mathbf{L} = h^2(\mathbb{P}^1)$ is the Lefschetz motive. The trace of Frobenius on $\mathbf{L}^k$ is p^k.

The conjecture has been proved by work of Weissauer for the regular case and was completed by Petersen, see [52,53,38]. One consequence is that the cohomology of the moduli spaces $\overline{\mathcal{M}}_{2,n}$ of stable n-pointed curves of genus 2 is now completely known. It has also led to progress on the tautological rings of the moduli spaces $\mathcal{M}_{2,n}$ by Petersen and Tommasi [39].

This result allows us to calculate the traces of the Hecke operators on spaces of classical and vector-valued Siegel modular forms. The strategy to do this is by making a list of all Weil polynomials, that is, characteristic polynomials of Frobenius together with the frequency with which they occur if we go through all isomorphism classes, that is, if we run over $\mathcal{A}_2$. Once one has this list for a field $\mathbb{F}_q$, one can compute the trace of the Hecke operator on the space of cusp forms $S_{j,k}(\mathrm{Sp}(4,\mathbb{Z}))$ for *all* pairs (j,k) with $k \geq 3$. We illustrate this with a few examples.

Example 5.1. The space $S_{0,35}(\mathrm{Sp}(4,\mathbb{Z}))$ has dimension 1 and is generated by the scalar-valued form χ_{35}. It corresponds to the case $(a,b) = (32,32)$. The eigenvalues of the Hecke operators for $q \leq 37$ (and $q \neq 8, 16, 27, 32$) are given below. Note that for q a square the value differs from the usual one, see Definition 10.1 in [4]. (The values for $q = p^r$ with $r \geq 3$ follow from those for $q = p$ and $q = p^2$.)

q	Eigenvalue
2	−25 073 418 240
3	−11 824 551 571 578 840
4	−203 922 016 925 674 110 976
5	9 470 081 642 319 930 937 500
7	−10 370 198 954 152 041 951 342 796 400
9	−270 550 647 008 022 226 363 694 871 019 974
11	−8 015 071 689 632 034 858 364 818 146 947 656
13	−20 232 136 256 107 650 938 383 898 249 808 243 380
17	118 646 313 906 984 767 985 086 867 381 297 558 266 980
19	2 995 917 272 706 383 250 746 754 589 685 425 572 441 160
23	−1 911 372 622 140 780 013 372 223 127 008 015 060 349 898 320
25	−86 593 979 298 858 393 096 680 290 648 986 986 047 363 281 250
29	−2 129 327 273 873 011 547 769 345 916 418 120 573 221 438 085 460
31	−157 348 598 498 218 445 521 620 827 876 569 519 644 874 180 822 976
37	−47 788 585 641 545 948 035 267 859 493 926 208 327 050 656 971 703 460

Example 5.2. Since explicitly known eigenvalues of Hecke operators on Siegel modular forms are rather scarce, even for scalar-valued forms of degree 2, we give another example that shows how effective curve counting is. The space $S_{0,43}(\mathrm{Sp}(4,\mathbb{Z}))$ is of dimension 1 and generated by a form $\chi_{43} = E_4^2\chi_{35}$. We list the Hecke eigenvalues (with the same conventions for prime powers as in the preceding one).

q	Eigenvalue
2	−4 069 732 515 840
3	−65 782 425 978 552 959 640
4	−20 941 743 921 027 137 625 128 960
5	−44 890 110 453 445 302 863 489 062 500
7	−19 869 584 791 339 339 681 013 202 023 932 400
9	−7 541 528 134 863 704 740 446 843 276 725 979 791 820
11	4 257 219 659 352 273 691 494 938 669 974 303 429 235 064
13	1 189 605 571 437 888 391 664 528 208 235 356 059 600 166 220
17	−1 392 996 132 438 667 398 495 024 262 137 449 361 275 278 473 925 020
19	−155 890 765 104 968 381 621 459 579 332 178 224 814 423 111 191 589 240
23	−128 837 520 803 382 146 891 405 898 440 571 781 609 554 910 722 934 311 120
25	7 099 903 749 386 561 314 439 988 230 597 055 761 986 231 311 645 507 812 500
29	4 716 850 092 556 381 736 632 805 755 807 948 058 560 176 106 387 507 397 101 740
31	3 518 591 320 768 311 083 473 550 005 851 115 474 157 237 215 091 087 497 259 584
37	−80 912 457 441 638 062 043 356 244 171 113 052 936 003 605 371 913 289 553 380 964 260

Example 5.3. The first cases where one finds a vector-valued cusp form that is not a lift from elliptic modular forms are the cases $(j,k) = (6,8)$ and $(4,10)$. We give the eigenvalues. We also give the eigenvalues for $(j,k) = (34,4)$. In all these cases the space of cusp forms is 1-dimensional.

q	$(6,8)$	$(4,10)$	$(34,4)$
2	0	−1680	−633 600
3	−27 000	55 080	91 211 400
4	409 600	−700 160	271 415 050 240
5	2 843 100	−7 338 900	11 926 488 728 700
7	−107 822 000	609 422 800	6 019 524 504 994 000
9	333 371 700	1 854 007 380	−1 653 726 849 656 615 820
11	3 760 397 784	25 358 200 824	−121 499 350 185 684 258 216
13	9 952 079 500	−263 384 451 140	655 037 831 218 999 528 300
17	243 132 070 500	−2 146 704 955 740	714 735 598 649 071 209 833 700
19	595 569 231 400	43 021 727 413 960	−3 644 388 446 450 362 098 497 240
23	−6 848 349 930 000	−233 610 984 201 360	179 014 316 167 538 651 075 065 200
25	−15 923 680 827 500	−904 546 757 727 500	−1 338 584 707 016 863 344 819 747 500
29	53 451 678 149 100	−545 371 828 324 260	52 292 335 454 052 856 173 814 993 740
31	234 734 887 975 744	830 680 103 136 064	−256 361 532 431 714 633 455 270 321 856
37	448 712 646 713 500	11 555 498 201 265 580	−826 211 657 019 923 608 686 387 368 900

The fact that one can calculate these eigenvalues has motivated Harder to make an idea about congruences between elliptic modular forms and Siegel modular forms of degree 2 concrete and formulate a conjecture about such congruences. Already many years ago, Harder had the idea that there should be congruences between the Hecke eigenvalues of elliptic modular forms and Siegel modular forms of genus 2 modulo a prime that divides a critical value of the L-function of the elliptic modular form, but the fact that the genus 2 eigenvalues could be calculated spurred him to make his ideas more concrete. He formulated his conjecture in [28].

If $f = \sum a(n)q^n \in S_k(\mathrm{SL}(2,\mathbb{Z}))$ is a normalized ($a(1) = 1$) elliptic modular cusp form with L-function $\sum a(n)n^{-s}$ and $\Lambda(f,s) = (\Gamma(s)/(2\pi)^s)L(f,s)$ that satisfies the functional equation $\Lambda(f,s) = (-1)^{k/2}\Lambda(f,k-s)$, then the values $\Lambda(f,r)$ with $k/2 \leq r \leq k-1$ are called the *critical values*. According to Manin and Vishik there are real numbers $\omega_\pm(f)$ with the property that all values $\Lambda'(f,r) := \Lambda(f,r)/\omega_+(f)$ for r even (resp. $\Lambda'(f,r) := \Lambda(f,r)/\omega_-(f)$ for r odd) lie in $\mathbb{Q}_f = \mathbb{Q}(a(n) : n \in \mathbb{Z}_{\geq 1})$, the field of eigenvalues $\lambda_p(f) = a(p)$ of the Hecke operators. If ℓ is a prime in $\mathbb{Q}_f$ lying above p it is called ordinary if $a(p) \not\equiv 0 \pmod{\ell}$.

Harder's conjecture says the following.

Conjecture 5.4. *(See Harder [28].) Let $a > b$ be natural numbers and $f \in S_{a+b+4}(\mathrm{SL}(2,\mathbb{Z}))$ be an eigenform. If ℓ is an ordinary prime in the field $\mathbb{Q}_f$ of Hecke eigenvalues $\lambda_p(f)$ of f and ℓ^s with $s \geq 1$ divides the critical value $\Lambda'(f, a+3)$, then there exists an eigenform $F \in S_{a-b,b+3}(\mathrm{Sp}(4,\mathbb{Z}))$ with Hecke eigenvalues $\lambda_p(F)$ satisfying*

$$\lambda_p(F) \equiv p^{a+2} + \lambda_p(f) + p^{b+1} \pmod{\ell^s}$$

in the ring of integers of the compositum of the fields $\mathbb{Q}_f$ and $\mathbb{Q}_F$ of Hecke eigenvalues of f and F for all primes p.

The counting of curves over finite fields provided a lot of evidence for his conjecture. We give one example.

Let $(a, b) = (20, 4)$ and let $f \in S_{28}(\mathrm{SL}(2,\mathbb{Z}))$ be the normalized eigenform. This form has eigenvalues in the field $\mathbb{Q}(\sqrt{d})$ with $d = 18\,209$. We have $f = \sum_{n\geq 1} a(n)q^n$ with

$$f = q + (-4140 - 108\sqrt{d})q^2 + (-643\,140 - 20\,737\sqrt{d})q^3 + \cdots$$

with

$$a(37) = \lambda_{37}(f) = 933\,848\,602\,341\,412\,283\,390 + 4\,195\,594\,851\,869\,555\,712\sqrt{d}.$$

The critical value of $\Lambda(f, 22)$ is divisible by the ordinary prime 367. Harder's conjecture claims that there should be a congruence. Indeed, the space $S_{16,7}(\mathrm{Sp}(4,\mathbb{Z}))$ has dimension 1 and is thus generated by a Hecke eigenform F and our results give the eigenvalue

$$\lambda_{37}(F) = -1\,845\,192\,652\,253\,792\,587\,940.$$

The prime 367 splits in $\mathbb{Q}(\sqrt{18\,209})$ as $367 = \pi \cdot \pi'$ with $\pi = (367, 260 + 44\sqrt{d})$. The reader may check that indeed we have the congruence

$$\lambda_{37}(F) \equiv 37^{22} + a(37) + 37^5 \pmod{\pi}.$$

Thus the counting of curves provides evidence for these conjectures. For more details see [19,28,4].

6. Counting curves of genus three

Like for genus 2, the moduli spaces $\mathcal{M}_3$ of curves of genus 3 and $\mathcal{A}_3$ of principally polarized abelian varieties of dimension 3 are rather close; in this case the Torelli map is a morphism $t : \mathcal{M}_3 \to \mathcal{A}_3$ of Deligne–Mumford stacks of degree 2. This is due to the fact that every abelian variety X has an automorphism of order 2 given by -1_X, while the generic curve of genus 3 has no non-trivial automorphisms. The universal families $\pi : \mathcal{X}_3 \to \mathcal{A}_3$ and $\gamma : \mathcal{C}_3 \to \mathcal{M}_3$ define local systems $\mathbb{V} := R^1\pi_*\mathbb{Q}_\ell$ and $R^1\gamma_*\mathbb{Q}_\ell$ with the pull back $t^*\mathbb{V} = R^1\gamma_*\mathbb{Q}_\ell$. The local system $\mathbb{V}$ carries a non-degenerate symplectic pairing $\mathbb{V} \times \mathbb{V} \to \mathbb{Q}_\ell(-1)$ and again we find for each irreducible representation of $\mathrm{Sp}(6, \mathbb{Q})$ of highest weight $\lambda = (a, b, c)$ with $a \geq b \geq c \geq 0$ a local system $\mathbb{V}_\lambda$. We are interested in

$$e_c(\mathcal{A}_3, \mathbb{V}_\lambda) = \sum_{i=0}^{12} (-1)^i \left[H_c^i(\mathcal{A}_3, \mathbb{V}_\lambda)\right],$$

again viewed in a Grothendieck group of Hodge structures or Galois representations.

What does the trace of Frobenius on this Euler characteristic tell us about traces of Hecke operators on Siegel modular forms? Here a Siegel modular form is a holomorphic function $f : \mathfrak{H}_3 \to W$ with W a finite-dimensional complex representation ρ of $\mathrm{GL}(3, \mathbb{C})$ satisfying

$$f\big((a\tau + b)(c\tau + d)^{-1}\big) = \rho(c\tau + d) f(\tau) \quad \text{for all } \tau \in \mathfrak{H}_3 \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(6, \mathbb{Z}).$$

If ρ is an irreducible representation of $\mathrm{GL}(3)$ of highest weight (α, β, γ) with $\alpha \geq \beta \geq \gamma$, then the corresponding space of modular forms (resp. cusp forms) is denoted by $M_{i,j,k}(\mathrm{Sp}(6, \mathbb{Z}))$ (resp. by $S_{i,j,k}(\mathrm{Sp}(6, \mathbb{Z}))$) and their weight (in the sense of modular forms) is denoted with $(i, j, k) = (\alpha - \beta, \beta - \gamma, \gamma)$.

In joint work with Bergström and Faber [4] we formulated a conjecture relating the trace of the Hecke operator on a space of vector-valued Siegel modular forms with the counts of curves. It was based on extensive calculations using counting of curves. It says:

Conjecture 6.1. *For $\lambda = (a, b, c)$ the trace of the Hecke operator $T(p)$ on the space of cusp forms $S_{a-b,b-c,c+4}(\mathrm{Sp}(6, \mathbb{Z}))$ is given by the trace of Frobenius on $e_c(\mathcal{A}_3, \mathbb{V}_\lambda)$ minus a correction term $e_{3,\mathrm{extra}}(a, b, c)$ given by*

$$\begin{aligned} e_{3,\mathrm{extra}} = & -e_c(\mathcal{A}_2, \mathbb{V}_{a+1,b+1}) + e_c(\mathcal{A}_2, \mathbb{V}_{a+1,c}) - e_c(\mathcal{A}_2, \mathbb{V}_{b,c}) \\ & - e_{2,\mathrm{extra}}(a+1, b+1) \otimes S[c+2] + e_{2,\mathrm{extra}}(a+1, c) \otimes S[b+3] \\ & - e_{2,\mathrm{extra}}(b, c) \otimes S[a+4]. \end{aligned}$$

The evidence for this conjecture is overwhelming. It fits with all we know about classical Siegel modular forms. The dimensions fit with the numerical Euler characteristics (replacing $[H_c^i(\mathcal{A}_3, \mathbb{V}_\lambda)]$ by its dimension). Moreover, the answers that we find by counting turn out to be integers, which is already quite a check, as we are summing rational numbers due to the factors $1/\#\mathrm{Aut}_{\mathbb{F}_q}(C)$. These results also fit with very recent (conjectural) results concerning Siegel modular forms obtained by the Arthur trace formula, see [9].

In order to show that it leads to very concrete results we give an illustration.

Example 6.2. The lowest weight examples of cusp forms that are not lifts occur in weights $(3,3,7)$, $(4,2,8)$ and $(2,6,6)$. In these cases the spaces $S_{i,j,k}(\mathrm{Sp}(6,\mathbb{Z}))$ are 1-dimensional. We give the (conjectured) Hecke eigenvalues.

$p\backslash(i,j,k)$	$(3,3,7)$	$(4,2,8)$	$(2,6,6)$
2	1080	9504	5184
3	181 440	970 272	−127 008
4	15 272 000	89 719 808	62 394 368
5	368 512 200	−106 051 896	2 126 653 704
7	13 934 816 000	112 911 962 240	86 958 865 280
8	−15 914 672 640	1 156 260 593 664	32 296 402 944
9	483 972 165 000	5 756 589 166 536	1 143 334 399 176
11	424 185 778 368	44 411 629 220 640	64 557 538 863 840
13	26 955 386 811 080	209 295 820 896 008	−34 612 287 925 432
16	1 224 750 814 466 048	−369 164 249 202 688	12 679 392 014 630 912
17	282 230 918 895 240	1 230 942 201 878 664	7 135 071 722 206 344
19	5 454 874 779 704 000	51 084 504 993 278 240	46 798 706 961 571 040

Example 6.3. As stated, our data allow the calculation for the trace of the Hecke operator $T(q)$ for $q \leq 19$ for all weights if Conjecture 6.1 is granted. Here we present the case of weight $(60,0,4)$. The space $S_{60,0,4}(\mathrm{Sp}(6,\mathbb{Z}))$ is of dimension 1 and a generator is not a lift. We give the Hecke eigenvalues, where for prime powers we use the convention of 10.1 in [4].

p	Eigenvalue
2	1 478 987 712
3	−2 901 104 577 414 432
4	−81 213 310 977 988 096 000
5	17 865 070 879 279 088 017 800
7	−6 212 801 311 610 929 434 173 542 528
8	−1 127 655 095 344 679 889 821 203 955 712
9	5 614 158 763 137 782 860 896 126 573 000
11	−1 849 697 485 178 583 502 997 203 666 501 152
13	2 477 960 171 489 248 682 447 718 208 861 099 208
16	−8 941 917 317 486 628 689 603 624 398 015 726 354 432
17	−73 908 079 488 243 072 323 266 509 093 278 640 761 208
19	592 331 726 239 601 530 766 675 208 936 630 486 956 000

As for genus 2, the heuristics of counting has led to new conjectured liftings to modular forms of genus 3, to new Harder type congruences and other results. We refer to [4].

7. Other cases

For genus $g \geq 4$ the dimension of the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g is larger than the dimension of the moduli space $\mathcal{M}_g$ of curves of genus g. This means that one cannot use the Torelli map $t : \mathcal{M}_g \otimes \mathbb{F}_q \to \mathcal{A}_g \otimes \mathbb{F}_q$, which associates to a curve its Jacobian variety, to enumerate all principally polarized abelian varieties of dimension g over $\mathbb{F}_q$. For genus $g = 4$ or 5 one might consider instead the Prym varieties of double étale covers of curves of genus $g+1$, but enumerating these double covers is already considerably more difficult. And for $g \geq 7$ the moduli spaces $\mathcal{A}_g$ are of general type, hence not unirational and therefore cannot be parametrized by open parts of affine or projective spaces. Nevertheless, there are other families of curves and abelian varieties to which the method of counting over finite fields can be applied.

In [46] Shimura describes a number of moduli spaces that over the complex numbers have a complex ball as universal cover and are rational varieties (birationally equivalent to projective space). In all these cases these are moduli spaces of curves that are described as covers of the projective line. One such case concerns triple Galois covers of genus 3 of the projective line. If the characteristic of the field is not 3, then such a curve can be given as $y^3 = f(x)$ with $f \in k[x]$ a degree 4 polynomial with distinct zeros. The Jacobians of such curves are abelian threefolds with multiplication by $F = \mathbb{Q}(\sqrt{-3}\,)$ induced by the action of the Galois automorphism α of the curve of order 3. The moduli of such abelian threefolds over $\mathbb{C}$ are described by an arithmetic quotient of the complex 2-ball by a discrete subgroup of the algebraic group of similitudes $G = \{g \in \mathrm{GL}(3, F) : h(gz, gz) = \eta(g)h(z, z)\}$ of a non-degenerate hermitian form $h = z_1\bar{z}_2 + z_2\bar{z}_1 + z_3\bar{z}_3$ on F^3, where the bar refers to the Galois automorphism of F. In fact, the discrete subgroup is the group $\Gamma[\sqrt{-3}\,]$

$$\left\{g \in \mathrm{GL}(3, O_F) : h(gz, gz) = h(z, z),\ g \equiv 1 \pmod{\sqrt{-3}\,}\right\}.$$

On our moduli space $\mathcal{M}$ defined over the ring of integers $O_F[1/3]$ of F with 3 inverted we have a universal family $\pi : \mathcal{C} \to \mathcal{M}$ and hence we get again a local system $\mathbb{V} = R^1\pi_*\mathbb{Q}$ or $R^1\pi_*\mathbb{Q}_\ell$. This is a local system of rank 6 provided with a non-degenerate alternating pairing $\mathbb{V} \times \mathbb{V} \to \mathbb{Q}(-1)$. The action of α on the cohomology gives rise to a splitting of $\mathbb{V}$ as a direct sum of two local systems of rank 3 over F: $\mathbb{V} \otimes F = \mathbb{W} \oplus \mathbb{W}'$. The non-degenerate pairing implies that $\mathbb{W}' \cong \mathbb{W}^\vee \otimes F(-1)$, where we denote by $\mathbb{W}^\vee$ the F-linear dual. From these basic local systems $\mathbb{W}$, $\mathbb{W}'$ we can obtain for each irreducible representation ρ of $\mathrm{GL}(3)$ local systems that appear as the analogues of the local systems $\mathbb{V}_a$ for $g = 1$ and $\mathbb{V}_\lambda$ for $g = 2$ and 3.

The role of the Siegel modular forms is now taken by so-called Picard modular forms. In fact, identifying $G(\mathbb{Q})$ with the matrix subgroup of $\mathrm{GL}(3, F)$ this group acts on the domain $B = \{(u,v) \in \mathbb{C}^2 : 2\mathrm{Re}(v) + |u|^2 < 0\}$ (isomorphic to a complex ball) by

$$(u,v) \mapsto \left(\frac{g_{31}v + g_{32} + g_{33}u}{g_{21}v + g_{22} + g_{23}u}, \frac{g_{11}v + g_{12} + g_{13}u}{g_{21}v + g_{22} + g_{23}u}\right).$$

For $g = (g_{ij}) \in G$ we let

$$j_1(g,u,v) = g_{21}v + g_{22} + g_{23}u$$

and

$$j_2\big(g,u,v^{-1}\big) = \det(g)^{-1}\begin{pmatrix} G_{32}u + G_{33} & G_{12}u + G_{13} \\ G_{12}u + G_{13} & G_{12}v + G_{11} \end{pmatrix}$$

with G_{ij} the minor of g_{ij}. Then a (vector-valued) Picard modular form of weight (j,k) on our discrete subgroup $\Gamma[\sqrt{-3}\,]$ is a holomorphic map $f : B \to \mathrm{Sym}^j(\mathbb{C}^2)$ satisfying

$$f\big(g \cdot (u,v)\big) = j_1(g,u,v)^k \mathrm{Sym}^j\big(j_2(g,u,v)\big) f(u,v)$$

for all $g \in \Gamma[\sqrt{-3}\,]$.

In joint work with Bergström we analyzed the Euler characteristic of compactly supported cohomology of local systems in this case by extensive counting over finite fields and came forward with conjectures that describe the Euler characteristics of these local systems and the traces of Hecke operators on the corresponding spaces of Picard modular forms, see [5]. These conjectures guided work of Cléry and van der Geer to construct the vector-valued modular forms and to find generators for modules of such vector-valued Picard modular forms. We refer to [10].

One of the charms of the subject of curves over finite fields is, that it is relatively easily accessible without requiring sophisticated techniques and amenable to direct calculations. Although it arose late, it is intimately connected to very diverse array of subdisciplines of mathematics. I hope to have convinced the reader that it is also a wonderful playground to find heuristically new phenomena and patterns that can help other areas of mathematics.

8. Tables

The following two tables (Tables 1 and 2) summarize the status quo as contained in the tables of the website www.manypoints.org for the function $N_q(g)$ for $1 \le g \le 50$ and q equal to a small power of 2 or 3. It gives either one value for $N_q(g)$, or an interval $[a,b]$ (denoted as a–b in the tables) in which $N_q(g)$ is supposed to lie, or an entry –b if b is the best upper bound known for $N_q(g)$ and no curve with at least $[b/\sqrt{2}\,]$ rational points is known, see [23].

Table 1
$p = 2$.

$g\backslash q$	2	4	8	16	32	64	128
1	5	9	14	25	44	81	150
2	6	10	18	33	53	97	172
3	7	14	24	38	64	113	192
4	8	15	25	45	71–72	129	215
5	9	17	29	49–53	83–85	140–145	227–234
6	10	20	33–34	65	86–96	161	243–256
7	10	21	34–38	63–69	98–107	177	262–283
8	11	21–24	35–42	63–75	97–118	169–193	276–302
9	12	26	45	72–81	108–128	209	288–322
10	13	27	42–49	81–86	113–139	225	296–345
11	14	26–29	48–53	80–91	120–150	201–235	294–365
12	14–15	29–31	49–57	88–97	129–160	257	321–388
13	15	33	56–61	97–102	129–171	225–267	–408
14	16	32–35	65	97–107	146–182	257–283	353–437
15	17	35–37	57–67	98–112	158–193	258–299	386–454
16	17–18	36–38	56–70	95–118	147–204	267–315	–476
17	18	40	63–73	112–123	154–211	–331	–499
18	18–19	41–42	65–77	113–128	161–219	281–347	–519
19	20	37–43	60–80	129–133	172–227	315–363	–542
20	19–21	40–45	76–83	127–139	177–235	342–379	–562
21	21	44–47	72–86	129–144	185–243	281–395	–591
22	21–22	42–48	74–89	129–149	–251	321–411	–608
23	22–23	45–50	68–92	126–155	–259	–427	–630
24	23	49–52	81–95	129–161	225–266	337–443	513–653
25	24	51–53	86–97	144–165	–274	408–459	–673
26	24–25	55	82–100	150–170	–282	425–475	–696
27	24–25	52–56	96–103	156–176	213–290	416–491	–716
28	25–26	54–58	97–106	145–181	257–297	513	577–745
29	26–27	52–60	97–109	161–186	227–305	–523	–761
30	25–27	53–61	96–112	162–191	273–313	464–535	609–784
31	27–28	60–63	89–115	168–196	–321	450–547	578–807
32	27–29	57–65	90–118	–201	–328	–558	–827
33	28–29	65–66	97–121	193–207	–336	480–570	–850
34	27–30	65–68	98–124	183–212	–344	462–581	–870
35	29–31	64–69	112–127	187–217	253–351	510–593	–899
36	30–31	64–71	112–130	185–222	–359	490–604	705–914
37	30–32	66–72	121–132	208–227	–367	540–615	–938
38	30–33	64–74	129–135	193–233	291–375	518–627	–961
39	33	65–75	120–138	194–238	–382	494–638	–981
40	32–34	75–77	103–141	225–243	293–390	546–649	–1004
41	34–35	72–78	118–144	220–248	308–397	560–661	–1024
42	33–35	75–80	129–147	209–253	307–405	574–672	–1053
43	34–36	72–81	116–150	226–259	306–412	546–683	–1068
44	33–37	68–83	130–153	226–264	325–420	516–695	–1092
45	36–37	80–84	144–156	242–268	313–427	572–706	–1115
46	36–38	81–86	129–158	243–273	–435	585–717	–1135
47	36–38	73–87	126–161	–277	–443	598–728	–1158
48	35–39	80–89	128–164	243–282	–450	564–739	–1178
49	36–40	81–90	130–167	240–286	–458	624–751	913–1207
50	40	91–92	130–170	255–291	–465	588–762	–1222

Acknowledgments

The author thanks Jonas Bergström, Fabien Cléry and the referees for some helpful remarks.

Table 2
$p = 3$.

$g\backslash q$	3	9	27	81
1	7	16	38	100
2	8	20	48	118
3	10	28	56	136
4	12	30	64	154
5	13	32–35	72–75	167–172
6	14	35–38	76–84	190
7	16	40–43	82–95	180–208
8	17–18	42–46	92–105	226
9	19	48–50	99–113	244
10	20–21	54	94–123	226–262
11	21–22	55–58	100–133	220–280
12	22–23	56–61	109–143	298
13	24–25	64–65	136–153	298–312
14	24–26	56–69	–163	278–330
15	28	64–73	136–170	292–348
16	27–29	74–76	144–178	370
17	28–30	74–80	128–184	288–384
18	28–31	68–84	148–192	306–400
19	32	84–88	145–199	–418
20	30–34	70–91	–206	–436
21	32–35	88–95	163–213	352–454
22	33–36	78–98	–220	370–472
23	33–37	92–101	–227	–490
24	31–38	91–104	208–234	370–508
25	36–40	96–108	196–241	392–526
26	36–41	110–111	200–248	500–544
27	39–42	104–114	208–255	–562
28	37–43	105–117	–262	–580
29	42–44	104–120	196–269	–598
30	38–46	91–123	196–276	551–616
31	40–47	120–127	–283	460–634
32	40–48	93–130	–290	–652
33	48–49	128–133	220–297	576–670
34	46–50	111–136	–304	594–688
35	47–51	119–139	–311	612–706
36	48–52	118–142	244–318	730
37	52–54	126–145	236–325	648–742
38	–55	111–149	–332	629–755
39	48–56	140–152	271–340	730–768
40	56–57	118–155	273–346	663–781
41	50–58	140–158	–353	680–794
42	52–59	122–161	280–360	697–807
43	56–60	147–164	–367	672–821
44	47–61	119–167	278–374	–834
45	54–62	136–170	–380	704–847
46	60–63	162–173	–387	720–859
47	54–65	154–177	299–394	690–872
48	55–66	163–180	325–401	752–885
49	64–67	168–183	316–408	768–898
50	63–68	182–186	312–415	784–911

References

[1] N. Anbar, H. Stichtenoth, Curves of every genus with a prescribed number of rational points, Bull. Braz. Math. Soc. (N.S.) 44 (2) (2013) 173–193.

[2] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of function fields over non-prime finite fields, arXiv:1202.5922.

[3] J. Bergström, Cohomology of moduli spaces of genus three curves via point counts, J. Reine Angew. Math. 622 (2008) 155–187.

[4] J. Bergström, C. Faber, G. van der Geer, Siegel modular forms of degree three and the cohomology of local systems, Sel. Math. New Ser. 20 (1) (2014) 83–124.

[5] J. Bergström, G. van der Geer, Curves of genus three and modular forms on a Picard modular group, in preparation.

[6] T. van den Bogaart, B. Edixhoven, Algebraic stacks whose number of points over finite fields is polynomial, in: Number Fields and Function Fields – Two Parallel Worlds, in: Prog. Math., vol. 239, Birkhäuser Verlag, 2005, pp. 39–50.

[7] E. Bombieri, Counting points on curves over finite fields, in: Séminaire N. Bourbaki 1972–1973, in: Lect. Notes Math., vol. 383, Springer, Berlin, 1974, pp. 234–241, exp. no. 430.

[8] B. Brock, A. Granville, More points than expected on curves over finite field extensions, Finite Fields Appl. 7 (1) (2001) 70–91.

[9] G. Chenevier, D. Renard, Level one algebraic cusp forms of classical groups of small ranks, arXiv:1207.0724.

[10] F. Cléry, G. van der Geer, Generators for modules of vector-valued Picard modular forms, Nagoya Math. J. 212 (2014) 19–57.

[11] P. Deligne, Formes modulaires et représentations ℓ-adiques, in: Séminaire Bourbaki 1968–1969, in: Lect. Notes Math., vol. 179, Springer-Verlag, Berlin, 1971, pp. 139–172, exp. no. 355.

[12] S.G. Vlăduţ, V.G. Drinfel'd, The number of points of an algebraic curve, Funkc. Anal. Prilozh. 17 (1) (1983) 68–69 (in Russian).

[13] N. Elkies, Explicit towers of Drinfeld modular curves, in: European Congress of Mathematics, vol. II, Barcelona, 2000, in: Prog. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 189–198.

[14] N. Elkies, E. Howe, C. Ritzenthaler, Genus bounds for curves with fixed Frobenius eigenvalues, Proc. Am. Math. Soc. 142 (2014) 71–84.

[15] C. Faber, G. van der Geer, Sur la cohomologie des systèmes locaux sur les espaces des modules des courbes de genre 2 et des surfaces abéliennes, I, II, C. R. Acad. Sci. Paris, Sér. I 338 (2004) 381–384, 467–470.

[16] R. Fuhrmann, F. Torres, The genus of curves over finite fields with many rational points, Manuscr. Math. 89 (1996) 103–106.

[17] A. Garcia, H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, Invent. Math. 121 (1995) 211–222.

[18] A. Garcia, H. Stichtenoth, Explicit towers of function fields over finite fields, in: Topics in Geometry, Coding Theory and Cryptography. Algebra and Applications, Springer-Verlag, Dordrecht, 2007, pp. 1–58.

[19] G. van der Geer, Siegel modular forms and their applications, in: J. Bruinier, G. van der Geer, G. Harder, D. Zagier (Eds.), The 1-2-3 of Modular Forms, Springer-Verlag, 2008.

[20] G. van der Geer, Hunting for curves with many points, in: Coding and Cryptology, in: Lect. Notes Comput. Sci., vol. 5557, Springer, Berlin, 2009, pp. 82–96.

[21] G. van der Geer, M. van der Vlugt, Supersingular curves of genus 2 over finite fields of characteristic 2, Math. Nachr. 159 (1992) 73–81.

[22] G. van der Geer, M. van der Vlugt, How to construct curves over finite fields with many points, in: F. Catanese (Ed.), Arithmetic Geometry, Cortona, 1994, in: Symp. Math., vol. 37, Cambridge University Press, Cambridge, 1997, pp. 169–189.

[23] G. van der Geer, M. van der Vlugt, Tables of curves with many points, Math. Comput. 69 (230) (2000) 797–810.

[24] G. van der Geer, M. van der Vlugt, An asymptotically good tower of curves over the field with eight elements, Bull. Lond. Math. Soc. 34 (2002) 291–300.

[25] E. Getzler, Resolving mixed Hodge modules on configuration spaces, Duke Math. J. 96 (1999) 175–203.

[26] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. 343 (1) (2009) 229–245.

[27] V.D. Goppa, Codes on algebraic curves, Sov. Math. Dokl. 24 (1981) 170–172.

[28] G. Harder, A congruence between a Siegel and an elliptic modular form, in: J. Bruinier, G. van der Geer, G. Harder, D. Zagier (Eds.), The 1-2-3 of Modular Forms, Springer-Verlag, 2008.

[29] H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper. I. Die Struktur der Gruppe der Divisisorenklassen endlicher Ordnung. II. Automorphismen und Meromorphismen. Das Additionstheorem. III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung, J. Reine Angew. Math. 175 (1936) 55–62, 69–88, 193–207.
[30] E. Howe, K. Lauter, Improved upper bounds for the number of points on curves over finite fields, Ann. Inst. Fourier 53 (2003) 1677–1737.
[31] E. Howe, K. Lauter, Corrigendum to: Improved upper bounds for the number of points on curves over finite fields, Ann. Inst. Fourier (Grenoble) 57 (3) (2007) 1019–1021.
[32] E. Howe, K. Lauter, New methods for bounding the number of points on curves over finite fields, in: C. Faber, G. Farkas, R. de Jong (Eds.), Geometry and Arithmetic, in: Ser. Congr. Rep., EMS, 2012, pp. 173–212.
[33] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci., Univ. Tokyo, Sect. 1A, Math. 28 (3) (1981) 721–724 (1982).
[34] K. Lauter, Improved upper bounds for the number of rational points on algebraic curves over finite fields, C. R. Acad. Sci. Paris, Sér. I 328 (1999) 1181–1185.
[35] K. Lauter, Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points, Proc. Am. Math. Soc. 128 (2000) 369–374.
[36] Yu.I. Manin, What is the maximum number of points on a curve over $\mathbb{F}_2$?, J. Fac. Sci., Tokyo 28 (1981) 715–720.
[37] H. Niederreiter, C.-P. Xing, Rational Points of Curves over Finite Fields, Cambridge University Press, Cambridge, 2001.
[38] D. Petersen, Cohomology of local systems on the moduli of principally polarized abelian surfaces, arXiv:1310.2508v4.
[39] D. Petersen, O. Tommasi, The Gorenstein conjecture fails for the tautological ring of $\overline{\mathcal{M}}_{2,n}$, Invent. Math. 196 (1) (2014) 139–161.
[40] H.-G. Rück, H. Stichtenoth, A characterization of Hermitian function fields over finite fields, J. Reine Angew. Math. 457 (1994) 185–188.
[41] R. Schoof, Algebraic curves and coding theory, Università di Trento, 1990, Preprint 336, 38 pp.
[42] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris 296 (1983) 397–402.
[43] J.-P. Serre, Nombre de points des courbes algébriques sur $\mathbb{F}_q$, in: Sém. de Théorie des Nombres de Bordeaux, 1982/1983, exp. no. 22 (= Oeuvres III, No. 129, pp. 664–668).
[44] J.-P. Serre, Quel est le nombre maximum de points rationnels que peut avoir une courbe algébrique de genre g sur un corps fini $\mathbb{F}_q$?, in: Résumé des Cours de 1983–1984 (= Oeuvres III, No. 132, Springer-Verlag, Berlin, 1986, pp. 701–705).
[45] J.-P. Serre, Rational Points on Curves over Finite Fields, Notes of lectures at Harvard University, 1985.
[46] G. Shimura, On purely transcendental fields of automorphic functions of several variables, Osaka Math. J. 1 (1964) 1–14.
[47] H. Stark, On the Riemann hypothesis in hyperelliptic function fields, in: Analytic Number Theory, St. Louis Univ., St. Louis, MO, 1972, in: Proc. Symp. Pure Math., vol. XXIV, Amer. Math. Soc., Providence, RI, 1973, pp. 285–302.
[48] S.A. Stepanov, On the number of points on a hyperelliptic curve over a finite prime field, Izv. Akad. Nauk SSSR, Ser. Mat. 33 (1969) 1103–1114.
[49] H. Stichtenoth, C.P. Xing, The genus of maximal function fields, Manuscr. Math. 86 (1995) 217–224.
[50] M.A. Tsfasman, S.G. Vladut, T. Zink, Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound, Math. Nachr. 109 (1982) 21–28.
[51] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.
[52] R. Weissauer, Endoscopy for GSp(4) and the Cohomology of Siegel Modular Threefolds, Lect. Notes Math., vol. 1968, Springer-Verlag, Berlin, 2009.
[53] R. Weissauer, The trace of Hecke operators on the space of classical holomorphic Siegel modular forms of genus two, arXiv:0909.1744.
[54] M. Wirtz, Konstruktion und Tabellen linearer Codes, Westfälische Wilhelms–Universität Münster, 1991.
[55] Th. Zink, Degeneration of Shimura surfaces and a problem in coding theory, in: Fundamentals of Computation Theory, Cottbus, 1985, in: Lect. Notes Comput. Sci., vol. 199, Springer, Berlin, 1985, pp. 503–511.