SOME OPEN QUESTIONS ABOUT CURVES AND ABELIAN VARIETIES OVER FINITE FIELDS

NICHOLAS M. KATZ

Dedicated to Pham Huu Tiep with the greatest admiration

Introduction

This is an entirely expository paper. We explain some open questions about curves and abelian varieties over finite fields, and about possible interrelations, or nonexistence thereof, among them.

1. the background

Fix an integer $g \geq 2$, a prime p, and a finite extension $\mathbb{F}_q/\mathbb{F}_p$. We denote by $\mathcal{M}_g(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-isomorphism classes of projective, smooth, geometrically connected curves of genus g over $\mathbb{F}_q$, and by $\mathcal{A}_g(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-isomorphism classes of principally polarized abelian varieties of dimension g over $\mathbb{F}_q$. We denote by $\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ the set of symplectic q-Weil polynomials, i.e., the set of integer polynomials

$$P(T) = \sum_{i=0}^{2g}(-1)^i a_i T^i, \quad a_i \in \mathbb{Z}, a_0 = 1, a_{g+i} = q^i a_{g-i} \text{ for } i = 0, ..., g,$$

for which

$$P(T) = \prod_{i=1}^{2g}(1 - \alpha_i T) \text{ with } |\alpha_i| = \sqrt{q} \text{ for all } i.$$

We have natural maps of sets

$$\mathcal{M}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q), \quad \mathcal{A}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q).$$

These maps attach to a curve $C/\mathbb{F}_q$ or to an abelian variety $A/\mathbb{F}_q$ the reversed characteristic polynomial of Frobenius on its ℓ-adic H^1 for any $\ell \nmid q$:

$$C/\mathbb{F}_q \mapsto P_{C/\mathbb{F}_q} := \det(1 - T\mathrm{Frob}_q | H^1(C \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)),$$

respectively

$$A/\mathbb{F}_q \mapsto P_{A/\mathbb{F}_q} := \det(1 - T\mathrm{Frob}_q | H^1(A \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)).$$

Recall the explicit relation between these polynomials and the point counts on the varieties that gave rise to them. For $A/\mathbb{F}_q$ with

$$P_{A/\mathbb{F}_q}(T) = \prod_{i=1}^{2g}(1 - \alpha_i T),$$

we have, for each $n \geq 1$,

$$\#A(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1 - \alpha_i^n).$$

For $P_{C/\mathbb{F}_q}(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, we have, for each $n \geq 1$,

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

This second relation is more succinctly formulated as the statement that $P_{C/\mathbb{F}_q}(T)$ is the numerator of the zeta function of $C/\mathbb{F}_q$.

One knows that $\mathrm{Jac}(C/\mathbb{F}_q)$, the Jacobian of $C/\mathbb{F}_q$, has the same characteristic polynomial over $\mathbb{F}_q$ as does $C/\mathbb{F}_q$.

$$P_{C/\mathbb{F}_q}(T) = P_{\mathrm{Jac}(C/\mathbb{F}_q)}(T).$$

2. Questions about "square root cancellation"

For $P(T) \in \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$, we have the estimates for the coefficients

$$|a_i| \leq \binom{2g}{i}\sqrt{q}^i \text{ for } i = 1, ..., g,$$

so we get the bound

$$\#\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q) \leq (\prod_{i=1}^{g}(1 + 2\binom{2g}{i}))\sqrt{q}^{1+2+...+g}.$$

See

So for fixed g and variable q, we have

$$\#\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q) = O_g(q^{g(g+1)/4}).$$

[In fact, by [DiPippo-Howe, Theorem 1.1], this is the correct order of magnitude.] On the other hand,

$$\#\mathcal{A}_g(\mathbb{F}_q) = q^{g(g+1)/2}(2 + O_g(1/\sqrt{q})).$$

The perhaps unexpected factor $2 + O_g(1/\sqrt{q})$ instead of $1 + O_g(1/\sqrt{q})$ in the above estimate comes from the fact that any abelian variety has automorphism group containing ± 1, and generally no more, cf. [Ka-Sar, Lemmas 11.2.5 and 11.2.6, and &11.3.3].

Thus there is at least "**square root cancellation**" in passing from abelian varieties over $\mathbb{F}_q$ to their characteristic polynomials over $\mathbb{F}_q$. We say "at least" because not every element of $\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ is a $P_{A/\mathbb{F}_q}$, cf. [Howe, sections 12 and 13], so the size of the image may be even smaller than $O_g(q^{g(g+1)/4})$. Additionally, one knows that the p-adic Newton polygon of any $P_{A/\mathbb{F}_q}$, when computed with respect to

$$\mathrm{ord}_q := (1/\mathrm{ord}_p(q))\mathrm{ord}_p,$$

has integer break-points.

By Tate [Tate66, section 3, Theorem 1 (c)], the characteristic polynomial of $A/\mathbb{F}_q$ determines the isogeny class of $A/\mathbb{F}_q$. Thus over a given $\mathbb{F}_q$, we have square root cancellation in passing from abelian varieties to their isogeny classes.

When we look instead at curves, we have

$$\#\mathcal{M}_g(\mathbb{F}_q) = q^{3g-3}(1 + O_g(1/\sqrt{q})),$$

cf. [Ka-Sar, Lemmas 10.6.8 and 10.6.13, and Theorem 10.6.14].

Let us denote by

$$\mathrm{CurvesSp}\mathcal{W}_g(\mathbb{F}_q) \subset \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$$

the set of $P_{C/\mathbb{F}_q}$ as $C/\mathbb{F}_q$ runs over $\mathcal{M}_g(\mathbb{F}_q)$.

A natural question is to wonder if, in passing from genus g curves over $\mathbb{F}_q$ to their zeta functions, or equivalently to their characteristic polynomials, there is a similar phenomenon of square root cancellation.

Challenge 2.1. Fix $g \geq 2$. Prove or disprove that, as q grows, $\#\mathrm{CurvesSp}\mathcal{W}_g(\mathbb{F}_q) = O_g(q^{(3g-3)/2})$.

This is trivially true for $g = 2, 3$, as these are the genera for which

$$3g - 3 = g(g+1)/2,$$

but already for $g \geq 4$ it seems completely open.

Let us take the opposite point of view. For $g \geq 10$, we have

$$3g - 3 < g(g+1)/4.$$

So there would seem to be room for the map $\mathcal{M}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ to be injective. However, as a careful referee pointed out, when $\mathbb{F}_q$ is no longer the prime field, then curves over $\mathbb{F}_q$ which are $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$-conjugate have the same zeta function, so the map $\mathcal{M}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ cannot be injective in general.

Challenge 2.2. Fix $g \geq 10$. Prove or disprove the existence of a constant D_g such that the map $\mathcal{M}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ is at most $(\#\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p))D_g$ to one.

There are obvious variants of the two challenges, where we replace $\mathcal{M}_g(\mathbb{F}_q)$ by "natural" subsets. For example, one might take

(1) $\mathcal{H}_g(\mathbb{F}_q)$, the the set of $\mathbb{F}_q$-isomorphism classes of hyperelliptic curves of genus g over $\mathbb{F}_q$. Here there are $O_g(q^{2g-1})$ points, so there is room for the existence of a constant $D_{\mathrm{hyp},g}$ such that the map $\mathcal{H}_g(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ is at most $(\#\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p))D_{\mathrm{hyp},g}$ to one, if $g \geq 7$. Or do we have square root cancellation?

(2) $\mathrm{Plane}_d(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-isomorphism classes of smooth plane curves of degree d over $\mathbb{F}_q$. Here there are on the order of $q^{\frac{(d+1)(d+2)}{2}-9}$ points, the genus is $(d-1)(d-2)/2$, so there is room for the existence of a constant $D_{\mathrm{plane},g}$ such that the map $\mathrm{Plane}_d(\mathbb{F}_q) \to \mathrm{Sp}\mathcal{W}_g(\mathbb{F}_q)$ is at most $(\#\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p))D_{\mathrm{plane},g}$ to one, if $d \geq 6$. Or do we have square root cancellation?

3. The situation over $\mathbb{F} := \overline{\mathbb{F}_q}$

Given an integer polynomial of degree $d \geq 1$ with constant term 1,

$$P(T) = 1 + \sum_{i=1}^{d} a_i T^i = \prod_{i=1}^{d} (1 - \alpha_i T),$$

for each integer $n \geq 1$ we denote by $P^{(n)}(T)$ the polynomial

$$P^{(n)}(T) = \prod_{i=1}^{d} (1 - \alpha_i^n T).$$

This polynomial also lies in $1 + t\mathbb{Z}[t]$, and its coefficients $a_i^{(n)}$ are universal $\mathbb{Z}$-polynomials in the coefficients a_i of $P(t)$.

Notice that the Newton polygon of $P(T)$, computed using $(1/\mathrm{ord}_p(q))\mathrm{ord}_p$, is equal to the Newton polygon of $P^{(n)}(T)$, computed using $(1/\mathrm{ord}_p(q^n))\mathrm{ord}_p$.

If we start with $A/\mathbb{F}_q$, we can extend scalars to obtain $(A\otimes\mathbb{F}_{q^n})/\mathbb{F}_{q^n}$. The reversed characteristic polynomials of these abelian varietes are related by

$$P_{(A\otimes\mathbb{F}_{q^n})/\mathbb{F}_{q^n}}(T) = P^{(n)}_{A/\mathbb{F}_q}(T).$$

Similarly, if we start with $C/\mathbb{F}_q$, we can extend scalars to obtain $(C\otimes\mathbb{F}_{q^n})/\mathbb{F}_{q^n}$. The reversed characteristic polynomials of these curves are related by

$$P_{(C\otimes\mathbb{F}_{q^n})/\mathbb{F}_{q^n}}(T) = P^{(n)}_{C/\mathbb{F}_q}(T).$$

We follow Deligne's convention and denote by $\mathbb{F}$ a chosen algebraic closure of $\mathbb{F}_q$. Suppose now we are given a point in $\mathcal{A}_g(\mathbb{F})$, i.e., an $A/\mathbb{F}$. Then for some integer $n\geq 1$, there exists a descent: an $A_n/\mathbb{F}_{q^n}$ which, after extension of scalars from $\mathbb{F}_{q^n}$ to $\mathbb{F}$, gives back $A/\mathbb{F}$. But there is no uniqueness in either n or the choice of $A_n/\mathbb{F}_{q^n}$. All that we can say is this. If we are also given $m\geq 1$ and a descent $A_m/\mathbb{F}_{q^m}$ of $A/\mathbb{F}$, then for some integer multiple d of lcm(n, m), $A_n\otimes_{\mathbb{F}_{q^n}}\mathbb{F}_{q^d}$ and $A_m\otimes_{\mathbb{F}_{q^m}}\mathbb{F}_{q^d}$ become isomorphic over $\mathbb{F}_{q^d}$.

We repeat the above paragraph verbatim with $\mathcal{A}_g$ replaced by $\mathcal{M}_g$ and with A replaced by C.

With this in mind, we consider the set

$$\bigcup_{n\geq 1}\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_{q^n})$$

of all degree $2g$ polynomials which are symplectic q^n-Weil polynomials for some power q^n of q. [We can read the n from the coefficient q^{ng} of T^{2g}.]

We define an equivalence relation on this set as follows: given $P_n(T)\in\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_{q^n})$ and $P_m(T)\in\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_{q^m})$, we say that $P_n\equiv P_m$ if, for some integer $d\geq 1$, we have

$$P_n^{(md)} = P_m^{(nd)}.$$

Notice that "the Newton polygon" makes sense for an equivalence class.

We then define $\mathrm{Sp}\mathcal{W}_g(\mathbb{F})$ to be the set of equivalence classes:

$$Sp\mathcal{W}_g(\mathbb{F}) := (\bigcup_{n\geq 1}\mathrm{Sp}\mathcal{W}_g(\mathbb{F}_{q^n}))/\equiv .$$

In view of the behavior of reversed characteristic polynomials under extension of scalars, we get well defined maps

$$\mathcal{A}_g(\mathbb{F})\to Sp\mathcal{W}_g(\mathbb{F}),\quad \mathcal{M}_g(\mathbb{F})\to Sp\mathcal{W}_g(\mathbb{F}),$$

by taking an $A/\mathbb{F}$, (respectively a $C/\mathbb{F}$), descending it to an $A_n\mathbb{F}_{q^n}$, (respectively to a $C_n/\mathbb{F}_{q^n}$), and attaching to it the equivalence class of $P_{A_n/\mathbb{F}_{q^n}}$ (respectively of $P_{C_n/\mathbb{F}_{q^n}}$) in $\mathrm{Sp}\mathcal{W}_g(\mathbb{F})$.

Thus two points $A/\mathbb{F}$ and $B/\mathbb{F}$ in $\mathcal{A}_g(\mathbb{F})$ are isogenous over $\mathbb{F}$ if and only if they have the same image in $Sp\mathcal{W}_g(\mathbb{F})$.

4. The isogeny question

In 1996, Oort and I stumbled upon the following question, which remains open.

Question 4.1. Do the two maps

$$\mathcal{A}_g(\mathbb{F})\to Sp\mathcal{W}_g(\mathbb{F}),\quad \mathcal{M}_g(\mathbb{F})\to Sp\mathcal{W}_g(\mathbb{F}),$$

have the same image? In other words, is every $A/\mathbb{F}\in\mathcal{A}_g(\mathbb{F})$ isogenous over $\mathbb{F}$ to the Jacobian of some curve $C/\mathbb{F}\in\mathcal{M}_g(\mathbb{F})$?

5. Evidence and heuristics

For each $g \geq 10$, and large q, there are more $\mathbb{F}_q$ isogeny classes of g dimensional abelian varieties over $\mathbb{F}_q$ than there are isomorphism classes of genus g curves over $\mathbb{F}_q$: this is the inequality $3g-3 < g(g+1)/4$ for $g \geq 10$.

This inequality suggests, but sadly does not prove, that for $g \geq 10$, there "should" be abelian varieties over $\mathbb{F}$ of dimension g which are not isogenous to Jacobians. See also [Shan-Tsim, Conjecture 2.1] for a heuristic discussion of this question, where $\mathcal{M}_g$ is replaced by any irreducible $V \subset \mathcal{A}_g$ of dimension $< g(g+1)/4$.

Over $\mathbb{C}$, a Baire category argument, cf. [Chai-Oort, 3.11], shows that for any $g \geq 4$ there are abelian varieties which are not isogenous to Jacobians.

Of course no such argument exists if we replace $\mathbb{C}$ by a countable, but algebraically closed, field. For the ground field $\overline{\mathbb{Q}}$, Chai and Oort [Chai-Oort] showed that for any $g \geq 4$ there are abelian varieties which are not isogenous to Jacobians, conditional on the André Oort conjecture for $\mathcal{A}_g$. Tsimerman gave an unconditional proof, see [Tsim1]. Masser and Zannier [Mas-Zan] gave another proof. [Tsimerman later proved the André Oort conjecture for $\mathcal{A}_g$, see [Tsim2].]

In the case of $\mathbb{F}$, the question remains open. One approach, suggested by Oort, is through Newton polygons. Can we exhibit Newton polygons which do not occur for curves? For example, fix a genus $g \geq 3$, and consider the polynomial

$$1 - pT + p^g T^2.$$

The slopes are $1/g$ and $(g-1)/g$, and both reciprocal roots have absolute value $\sqrt{p^g}$. The g'th power

$$(1 - pT + p^g T^2)^g$$

is the least power whose Newton polygon has integer break points. By [Honda] and [Tate68], $(1 - pT + p^g T^2)^g$ is the reversed characteristic polynomial of an $A/\mathbb{F}_{p^g}$, which is simple (because its slopes have exact denominator g, and so $(1 - pT + p^g T^2)^g$ cannot be the product of two integer polynomials, each of strictly positive degree, each of whose Newton polygons has integer break points and slopes invariant by $\lambda \mapsto 1 - \lambda$.). If g is odd, then by Howe [Howe-Ker, Theorem1.2], the isogeny class of this $A/\mathbb{F}_{p^g}$ admits a principal polarization, and so gives an element of $\mathcal{A}_g(\mathbb{F}_{p^g})$. If g is even, the same is true over $\mathbb{F}$, so we get an element of $\mathcal{A}_g(\mathbb{F})$ with these slopes as well.

Challenge 5.1. Prove or disprove that for every $g \geq 4$, there exists no $C/\mathbb{F}$ of genus g whose Newton polygon has slopes

$$\{1/g \text{ repeated } g \text{ times}, (g-1)/g \text{ repeated } g \text{ times}\}.$$

Perhaps easier(?) is

Challenge 5.2. Prove or disprove that for every odd **prime** $p \geq 691$, there exists no $C/\mathbb{F}$ of genus p whose Newton polygon has slopes

$$\{1/p \text{ repeated } p \text{ times}, (p-1)/p \text{ repeated } p \text{ times}\}.$$

Here 691 is Ramanujan's prime, it could be replaced in the challenge by any any prime large enough to eliminate "low genus accidents", if in fact there are any.

Much remains to be done.

References

[Chai-Oort] Chai,C.-L., and F. Oort, F., Abelian varieties isogenous to a Jacobian, Ann. of Math. (2) 176(1) (2012), 589-635.

[DiPippo-Howe] DiPippo,S. and Howe,E., Real polynomials with all roots on the unit circle and abelian varieties over finite fields, J. Number Theory 73(2) (1998), 426-450, and Corrigendum, J. Number Theory 83 (2000), no. 1, 182.

[G-K] Giulietti, M., Korchmáros, G., Algebraic curves with a large non-tame automorphism group fixing no point. Trans. Amer. Math. Soc. 362 (2010), no. 11, 5983-6001.

[H-K-T] Hirschfeld, J.W.P., Korchmáros, G., Torres, F., Algebraic Curves over a finite Field, Princeton Series in Applied Mathematics, Princeton Univ. Press, Princeton, NJ, 2008,. xx+696 pp.

[Honda] Honda, T., Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan 20 (1968), 83-95.

[Howe] E. Howe, Principally polarized ordinary abelian varieties over finite fields, Trans. Amer. Math. Soc. 347(7) (1995), 2361-2401.

[Howe-Ker] Howe, E., Kernels of polarizations of abelian varieties over finite fields. J. Algebraic Geom. 5 (1996), no. 3, 583-608. [

[Ka-Sar] Katz, N., and Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, **45**. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[Mas-Zan] Masser, D., and Zannier, U., Abelian varieties isogenous to no Jacobian, Ann. of Math. (2) 191(2)(2020), 635-674.

[Shan-Tsim] Shankar, A. N., and Tsimerman j., Unlikely intersections in finite characteristic, Forum Math. Sigma 6 (2018), e13, 17. https://doi.org/10.1017/fms.2018.15.

[Tate66] Tate, J., Endomorphisms of abelian varieties over finite fields. Invent. Math. 2 (1966), 134-144.

[Tate68] Tate, J., Classes d'isogénie des variétés abéliennes sur un corps fini (d'aprés T. Honda). (French) [Isogeny classes of abelian varieties over finite fields (after T. Honda)] Séminaire Bourbaki. Vol. 1968/69: Exposés 347-363, Exp. No. 352, 95-110, Lecture Notes in Math., 175, Springer, Berlin, 1971.

[Tsim1] Tsimerman, J., The existence of an abelian varietiy over $\mathbb{Q}$ isogenous to no Jacobian, Ann. of Math. (2) 176(1) (2012), 637-650.

[Tsim2] Tsimerman, J., The André-Oort conjecture for $\mathcal{A}_g$. Ann. of Math. (2) 187 (2018), no. 2, 379-390

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: nmk@math.princeton.edu