Frobenius distributions of abelian varieties over finite fields[1]

Joint with Deewang Bhamidipati and Soumya Sankar

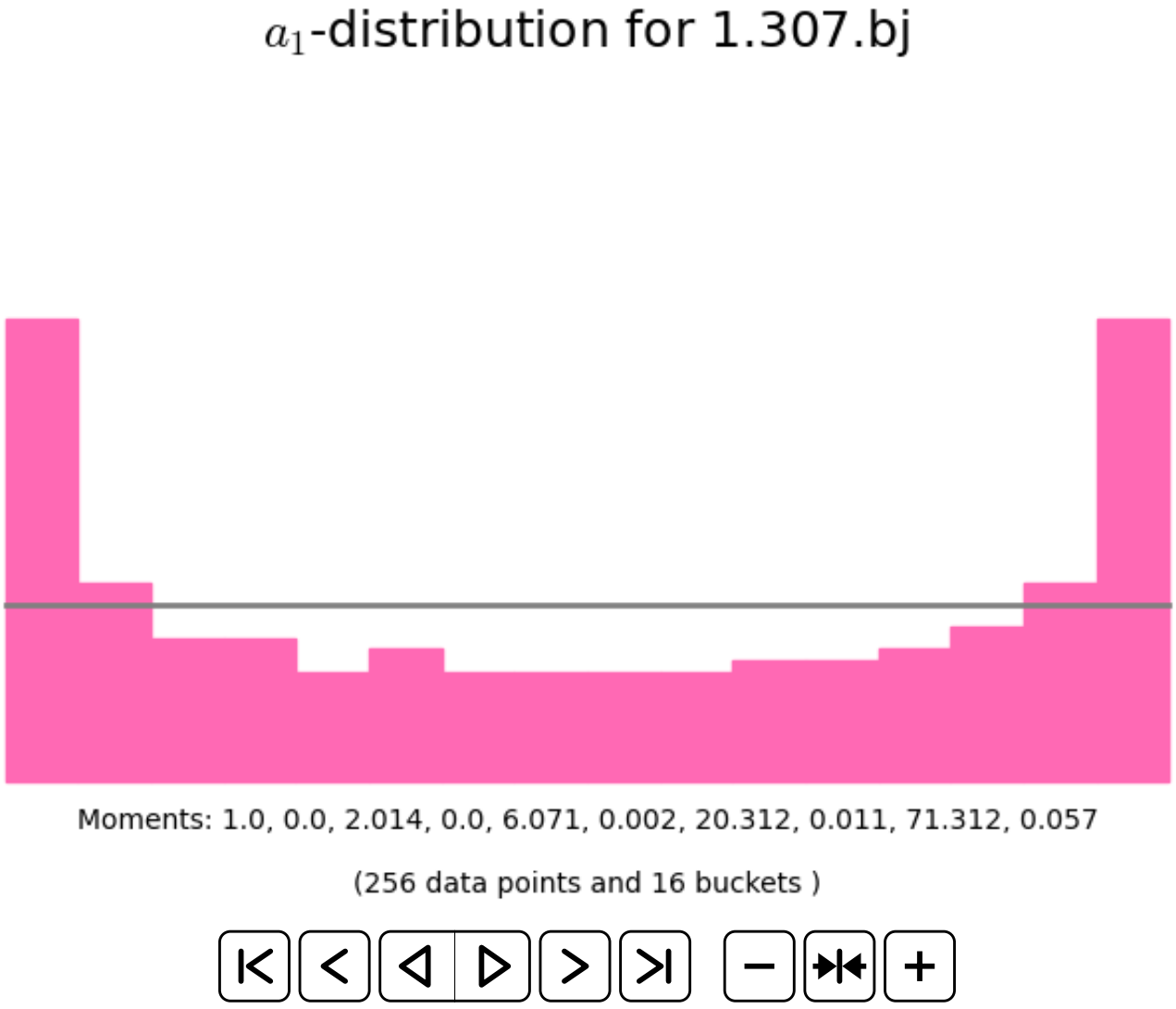
Santiago Arango-Piñeros

Emory University

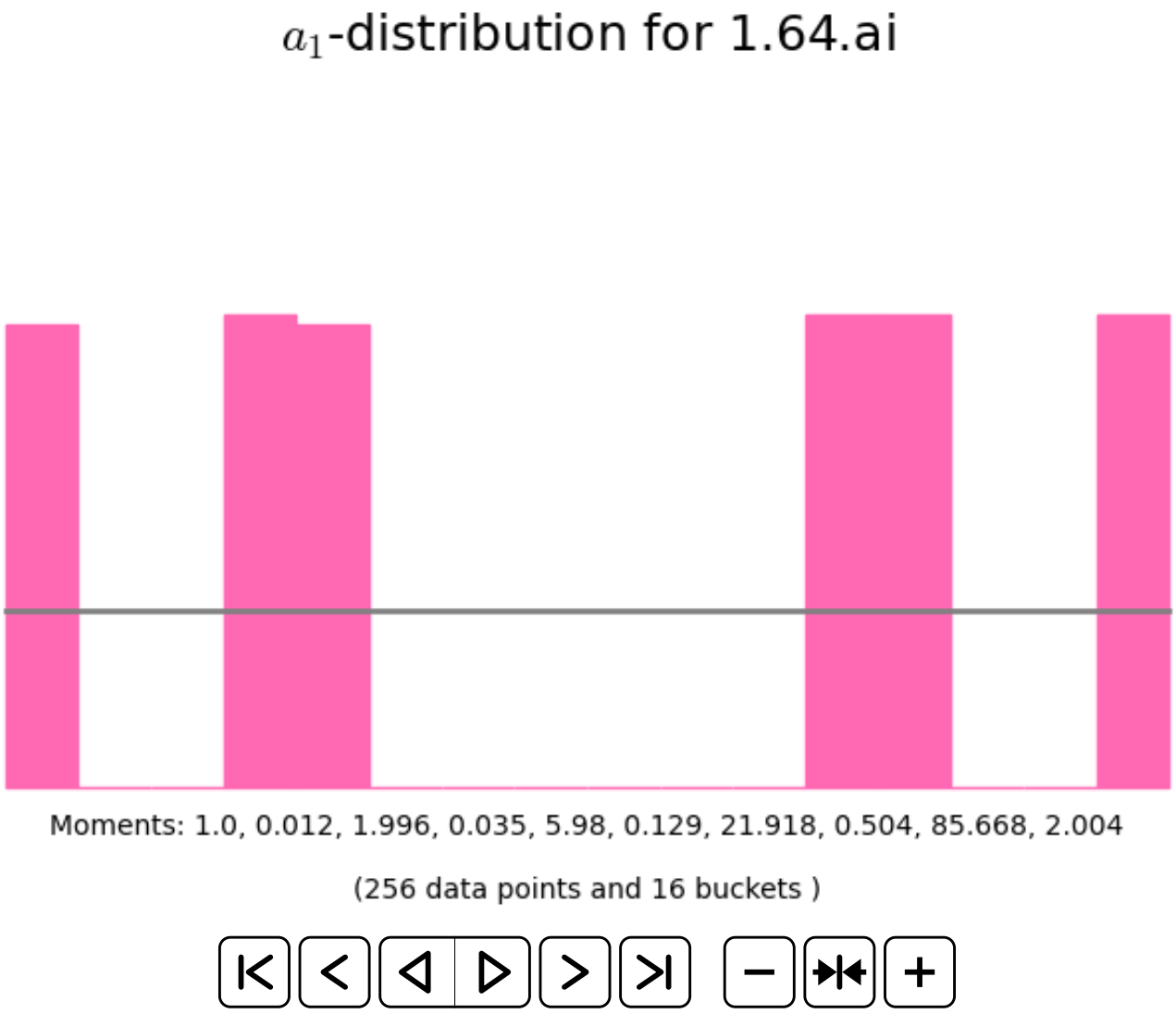
Conférence Statistiques Arithmétiques
CIRM
May 15, 2023

[1] Requires Acrobat Reader to play the animations.

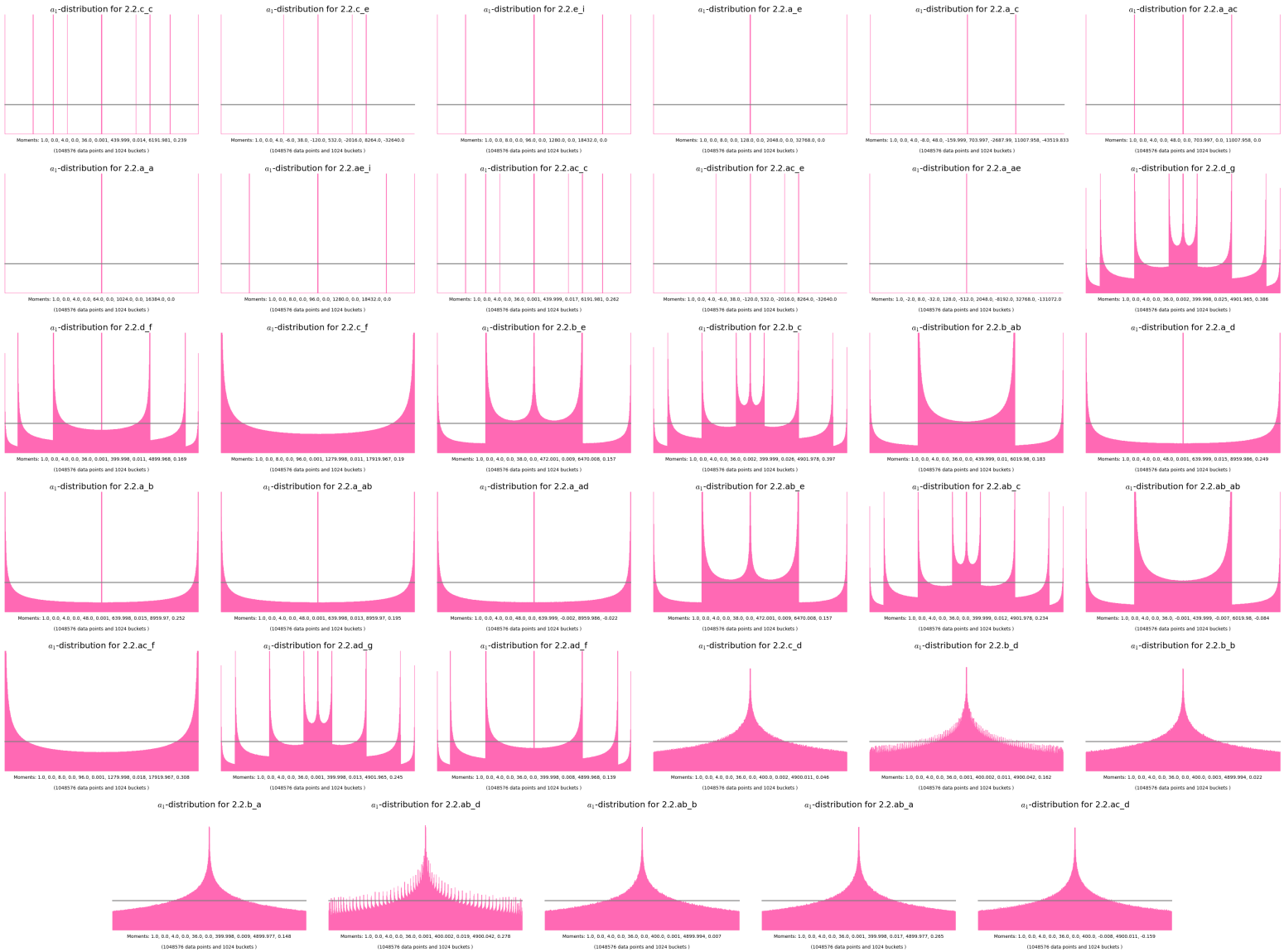
Ordinary elliptic curve 1.307.bj



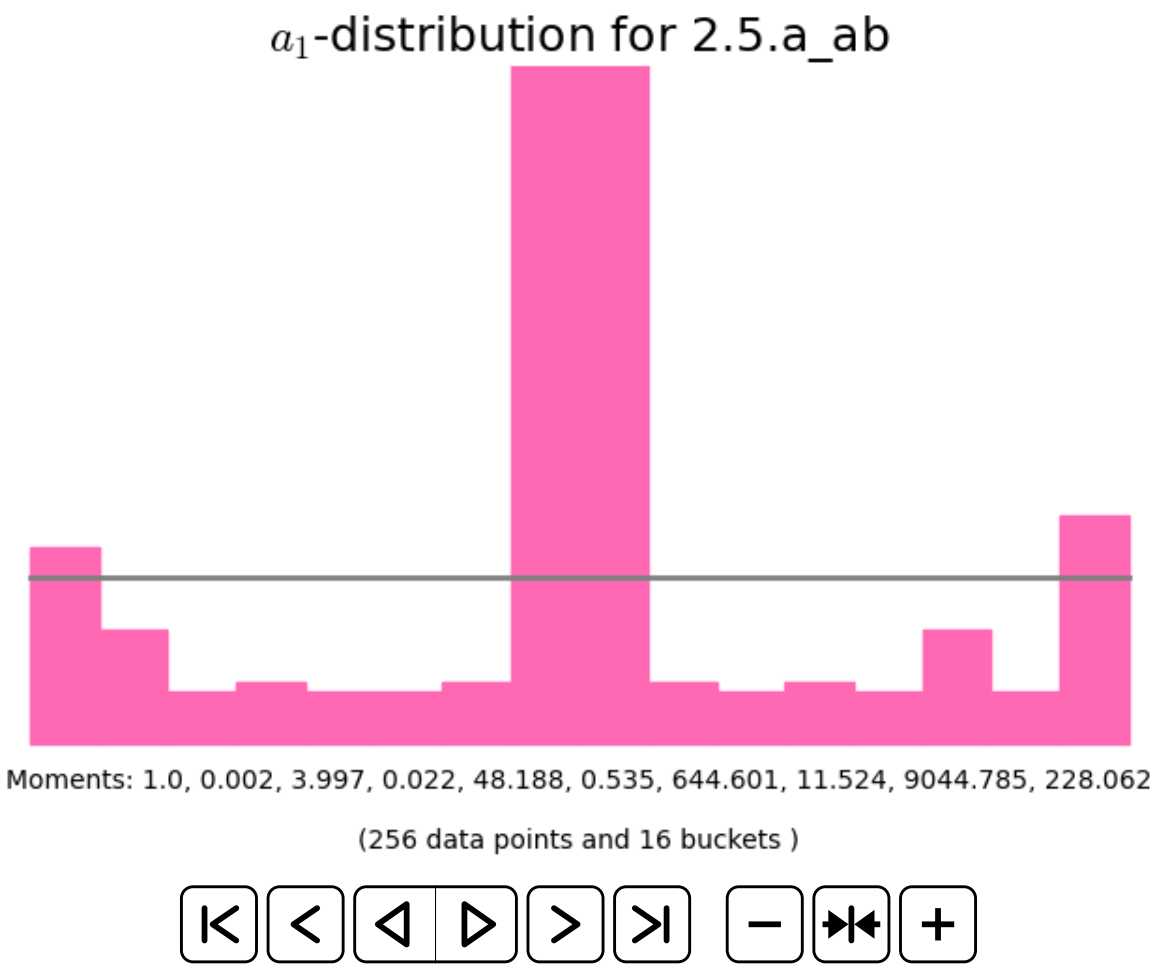
Supersingular elliptic curve 1.64.ai



The 35 isogeny classes of abelian surfaces over $\mathbf{F}_2$

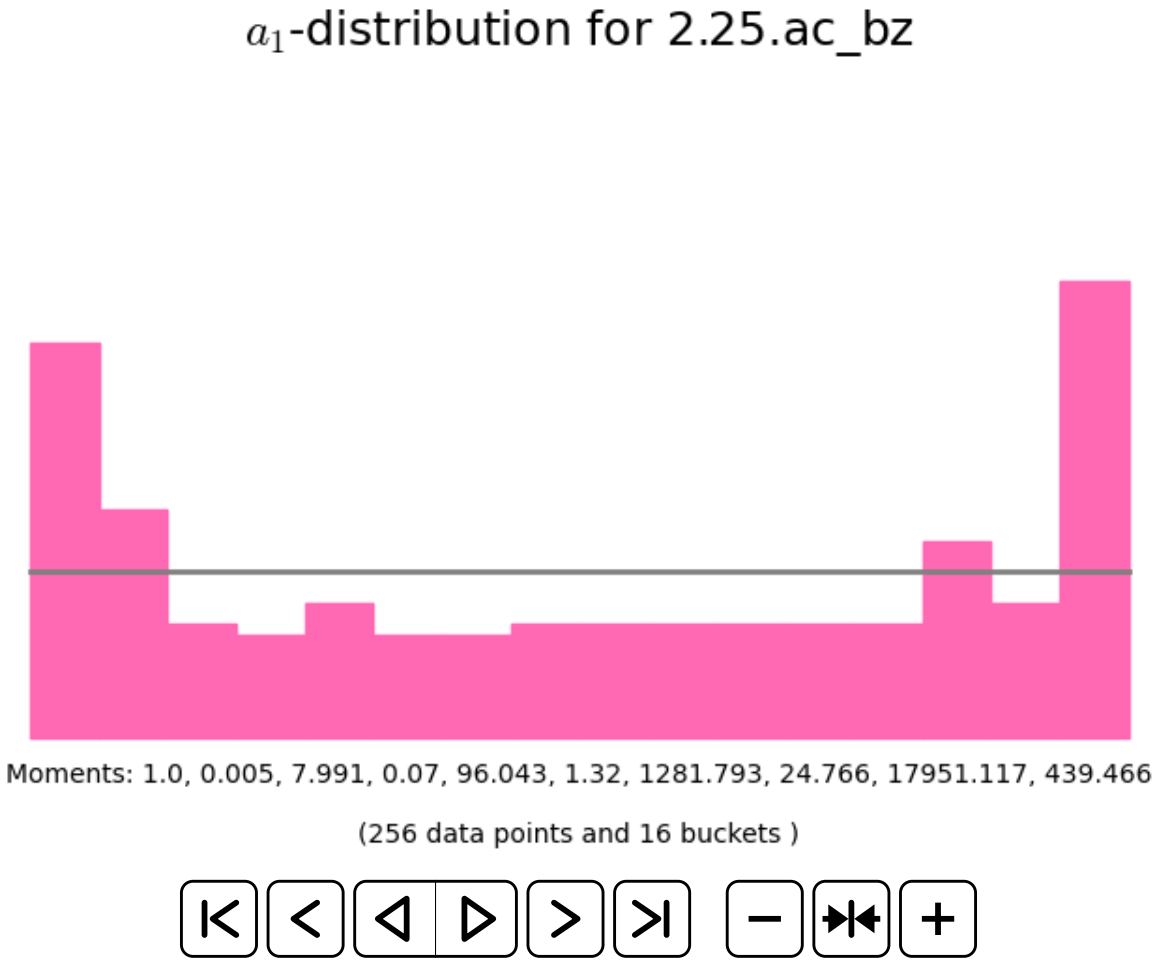


Simple ordinary surface 2.5.a_ab.



Let $A/\mathbf{F}_5$ be a simple ordinary abelian variety in this isogeny class.

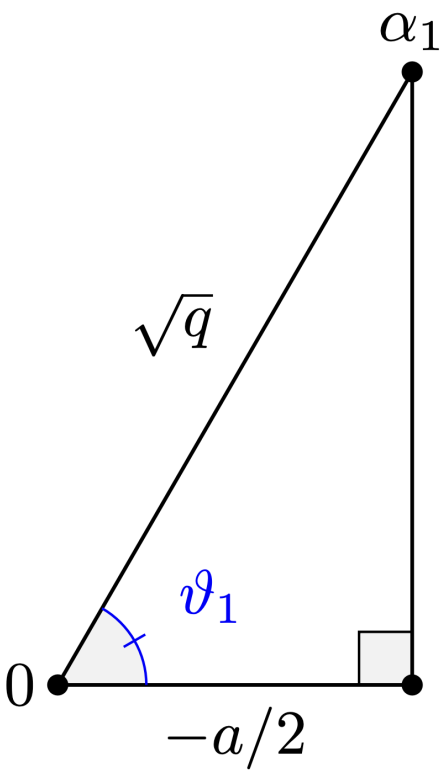
Ordinary surface 2.25.ac_bz $= 1.25.\mathrm{ab}^2$.



Let $A_{(2)}/\mathbf{F}_{25}$ the quadratic base extension of A. $A_{(2)} \sim E^2$.

Classification for $g = 1$

Waterhouse [Wat69], building on work of Deuring [Deu41], classified the possible Frobenius polynomials of elliptic curves.



Theorem (Elliptic curves)

Let E be an elliptic curve defined over $\mathbf{F}_q$. Then

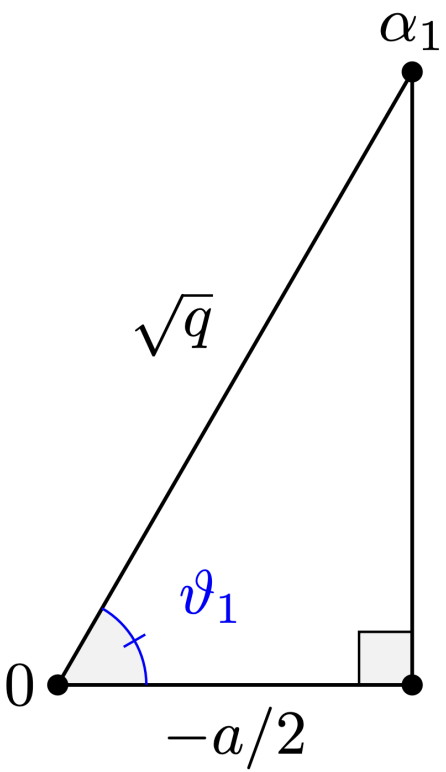
(1) *E is ordinary if and only if $\mathrm{SF}(E) = \mathrm{U}(1)$.*

(2) *E is supersingular if and only if $\mathrm{SF}(E) \in \{C_1, C_3, C_4, C_6, C_8, C_{12}\}$.*

Moreover, each one of these groups is realized for some prime power q.

Classification for $g = 1$

Waterhouse [Wat69], building on work of Deuring [Deu41], classified the possible Frobenius polynomials of elliptic curves.



Theorem (Elliptic curves)

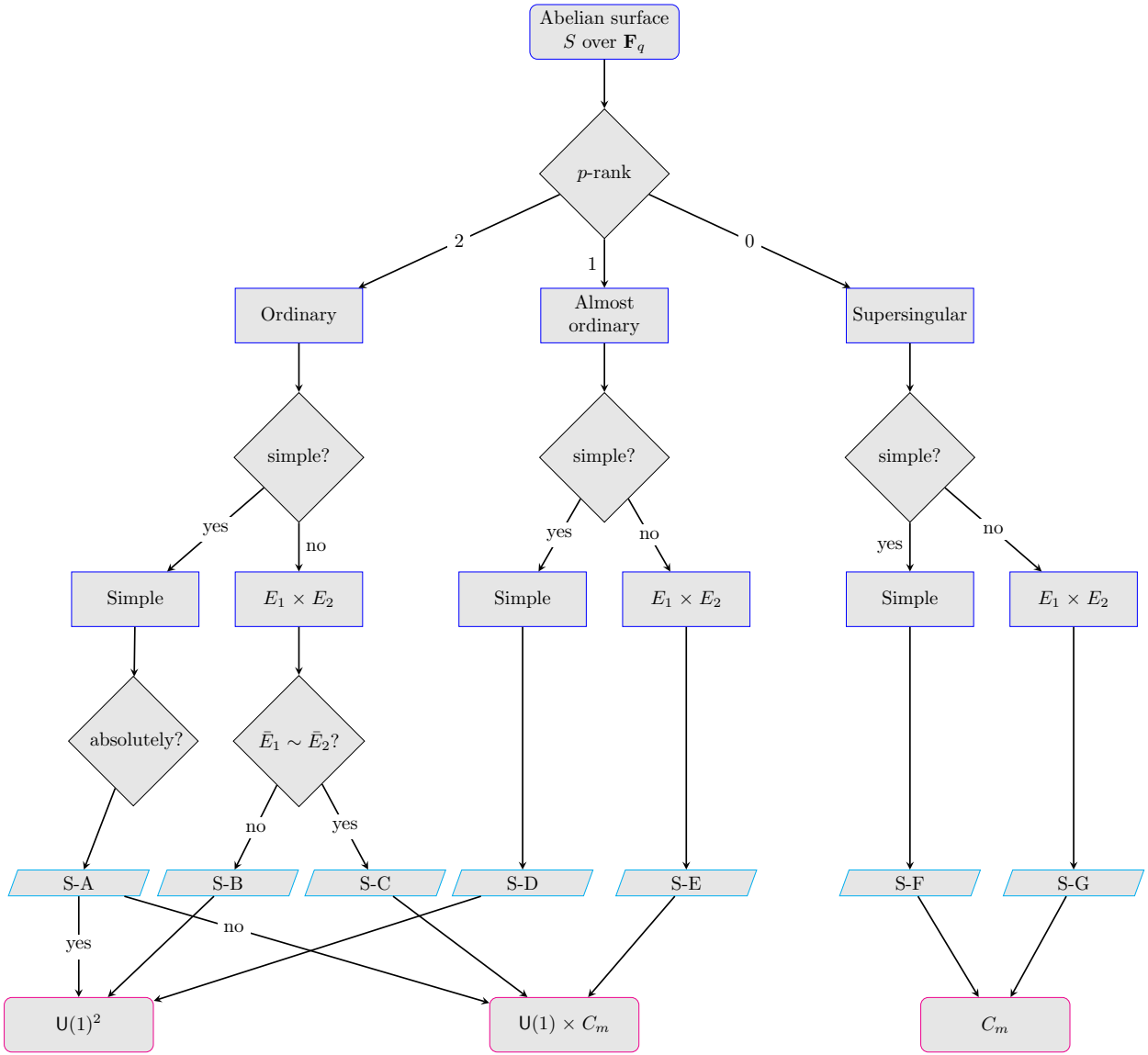
Let E be an elliptic curve defined over $\mathbf{F}_q$. Then

(1) *E is ordinary if and only if $\mathrm{SF}(E) = \mathrm{U}(1)$.*

(2) *E is supersingular if and only if $\mathrm{SF}(E) \in \{C_1, C_3, C_4, C_6, C_8, C_{12}\}$.*

Moreover, each one of these groups is realized for some prime power q.

Classification for $g = 2$



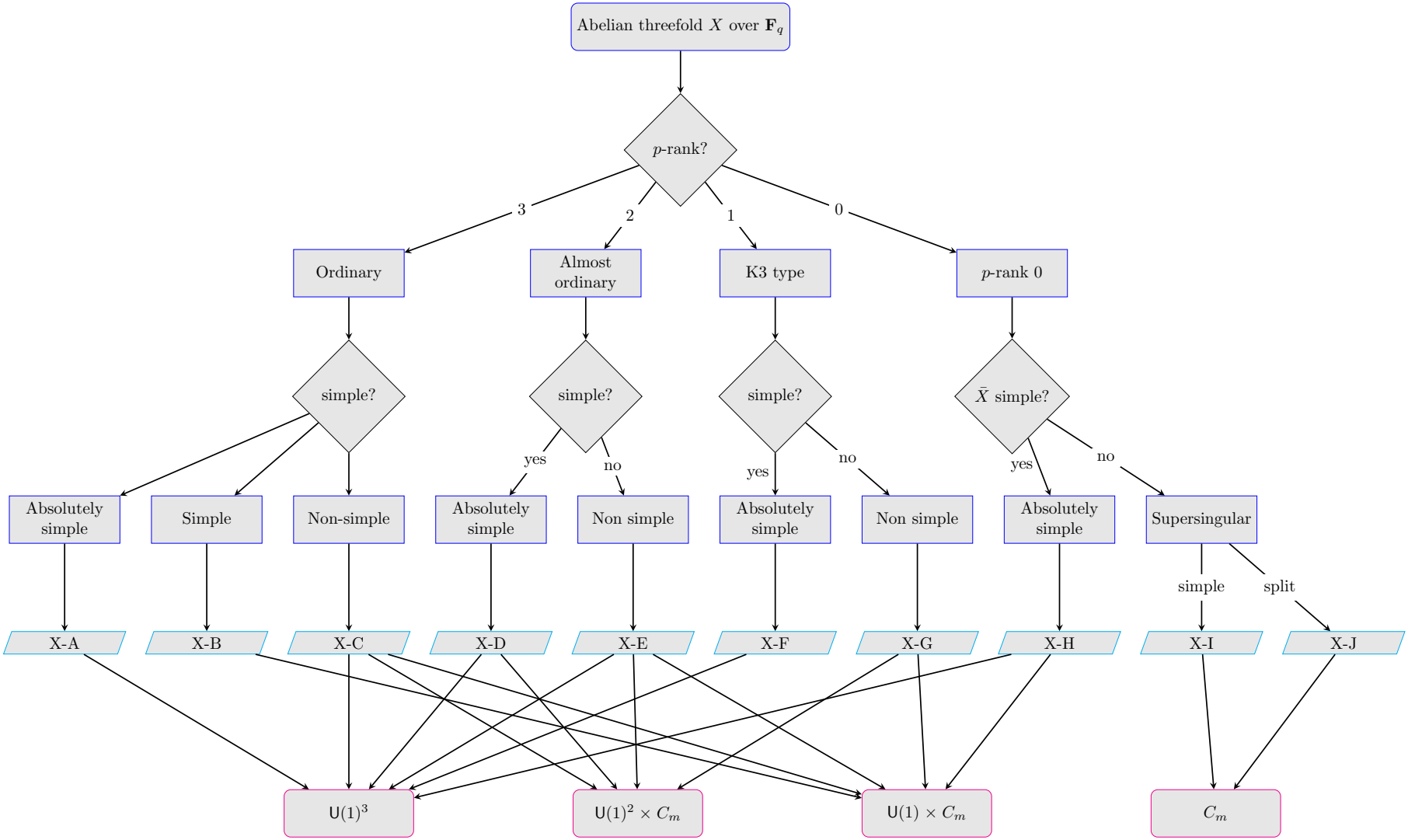
Classification for $g = 2$

Theorem (A-P, Bhamidipati, Sankar)

Let S be an abelian surface over $\mathbf{F}_q$. Then, S has Serre–Frobenius group according to the following table. Further, each one of these groups is realized for some prime power q.

$\mathsf{SF}(S)^\circ$	$\#\mathsf{SF}(S)/\mathsf{SF}(S)^\circ$
1	1,2,3,4,5,6,8,10,12,24
$\mathsf{U}(1)$	1,2,3,4,6,8,12
$\mathsf{U}(1)^2$	1

Classification for $g = 3$



Classification for $g = 3$

Theorem (A-P, Bhamidipati, Sankar)

Let X be an abelian threefold over $\mathbf{F}_q$. Then, X has Serre–Frobenius group according to the following table. Further, each one of these groups is realized for some prime power q.

$\mathsf{SF}(X)^\circ$	$\#\mathsf{SF}(X)/\mathsf{SF}(X)^\circ$
1	1,2,3,4,5,6,7,8,9,10,12,14,15,18,20,24,28,30,36
$\mathsf{U}(1)$	1,2,3,4,5,6,7,8,10,12,24
$\mathsf{U}(1)^2$	1,2,3,4,6,8,12,24
$\mathsf{U}(1)^3$	1

Previous work

We use previous work on the classification of Frobenius polynomials and the multiplicative relations between their roots. Most notably:

- Zarhin [Zar93; Zar91; Zar92; Zar15].
- Lenstra and Zarhin [LZ93].
- Zhu [Zhu01].
- Howe and Zhu [HZ02].
- Rück [Rüc90].
- Maisner and Nart [MN02].
- Nart and Ritzenthaler [NR08].
- Xing [Xin94; Xin96].
- Haloui [Hal10].
- Singh, McGuire, and Zaytsev [SMZ14].
- Dupuy, Kedlaya, Roe, Vincent [Dup+21].
- Dupuy, Kedlaya, Zureick-Brown [DKZ21].

Previous work

We use previous work on the classification of Frobenius polynomials and the multiplicative relations between their roots. Most notably:

- Zarhin [Zar93; Zar91; Zar92; Zar15].
- Lenstra and Zarhin [LZ93].
- Zhu [Zhu01].
- Howe and Zhu [HZ02].
- Rück [Rüc90].
- Maisner and Nart [MN02].
- Nart and Ritzenthaler [NR08].
- Xing [Xin94; Xin96].
- Haloui [Hal10].
- Singh, McGuire, and Zaytsev [SMZ14].
- Dupuy, Kedlaya, Roe, Vincent [Dup+21].
- Dupuy, Kedlaya, Zureick-Brown [DKZ21].

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Sophie Germain primes

Theorem (A-P, Bhamidipati, Sankar)

Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.

(1) *A is absolutely simple.*

(2) *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.*

(3) *$2g+1$ is prime and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$.*

This extends a result of Howe and Zhu [HZ02, Theorem 6] for $g = 2$.

Thank you!

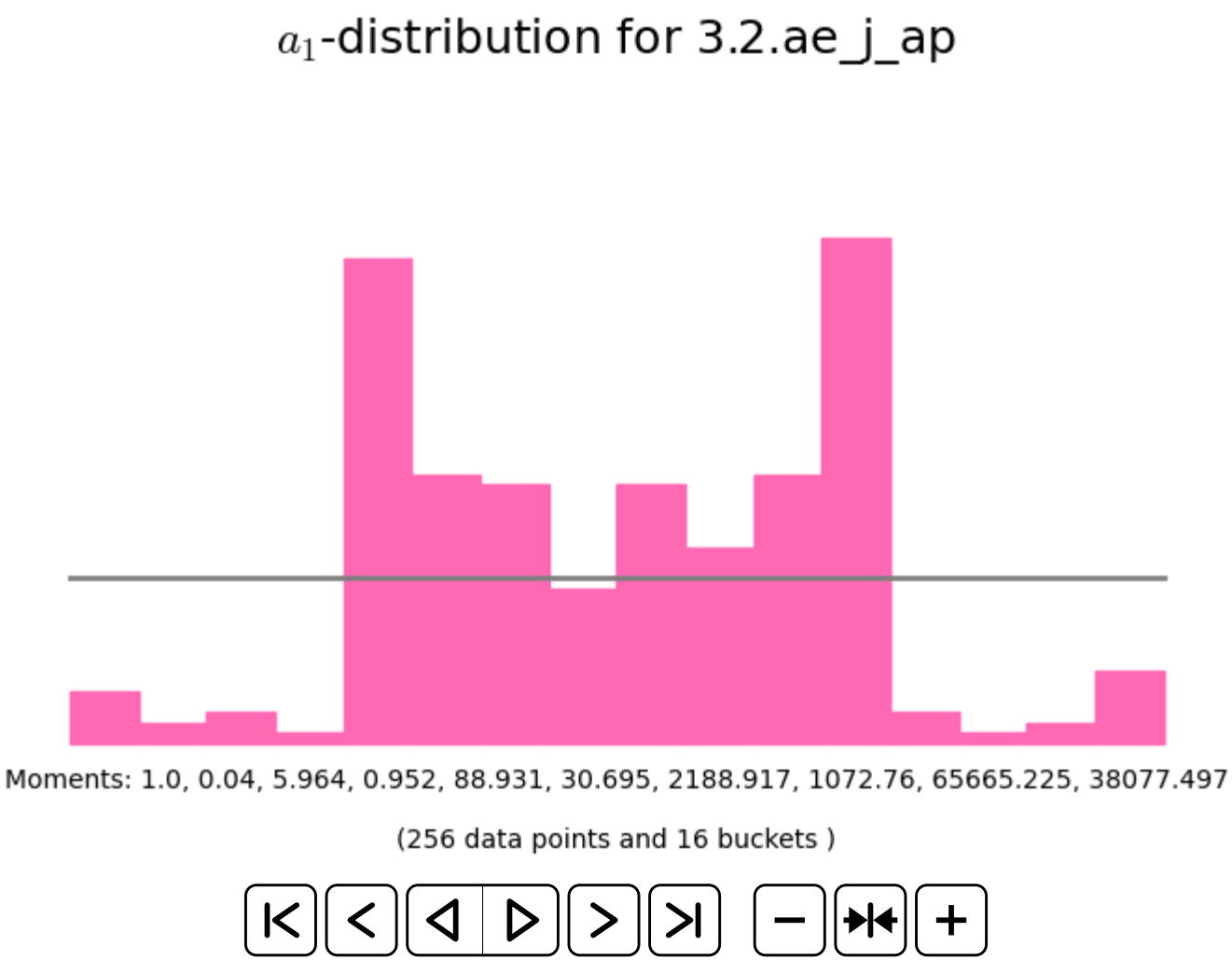


Figure: Isogeny class 3.2.ae_j_ap.

Bibliography I

[Deu41] Max Deuring. "Die typen der multiplikatorenringe elliptischer funktionenkörper". In: *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*. Vol. 14. 1. Springer. 1941, pp. 197–272.

[Wat69] William C. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École normale supérieure*. Vol. 2. 4. 1969, pp. 521–560.

[Rüc90] Hans-Georg Rück. "Abelian surfaces and Jacobian varieties over finite fields". In: *Compositio Math.* 76.3 (1990), pp. 351–366. ISSN: 0010-437X. URL: http://www.numdam.org/item?id=CM_1990__76_3_351_0.

Bibliography II

[Zar91] Yuri G. Zarhin. "Abelian Varieties of K3 Type and ℓ-Adic Representations". In: *ICM-90 Satellite Conference Proceedings*. Ed. by Akira Fujiki et al. Tokyo: Springer Japan, 1991, pp. 231–255.

[Zar92] Yuri G. Zarhin. "Abelian varieties having a reduction of K3 type". English (US). In: *Duke Mathematical Journal* 65.3 (Mar. 1992). Copyright: Copyright 2016 Elsevier B.V., All rights reserved., pp. 511–527. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-92-06520-3.

Bibliography III

[LZ93] Hendrik W. Lenstra Jr. and Yuri G. Zarhin. "The Tate conjecture for almost ordinary abelian varieties over finite fields". In: *Advances in number theory (Kingston, ON, 1991)*. Oxford Sci. Publ. Oxford Univ. Press, New York, 1993, pp. 179–194.

[Zar93] Yuri G. Zarhin. "Abelian varieties of $K3$ type". In: *Séminaire de Théorie des Nombres, Paris, 1990–91*. Vol. 108. Progr. Math. Birkhäuser Boston, Boston, MA, 1993, pp. 263–279.

[Xin94] Chaoping Xing. "The characteristic polynomials of abelian varieties of dimensions three and four over finite fields". In: *Sci. China Ser. A* 37.2 (1994), pp. 147–150. ISSN: 1001-6511.

Bibliography IV

[Xin96] Chaoping Xing. "On supersingular abelian varieties of dimension two over finite fields". In: *Finite Fields Appl.* 2.4 (1996), pp. 407–421. ISSN: 1071-5797. DOI: 10.1006/ffta.1996.0024. URL: https://doi.org/10.1006/ffta.1996.0024.

[Zhu01] Hui June Zhu. "Supersingular abelian varieties over finite fields". In: *Journal of Number Theory* 86.1 (2001), pp. 61–77.

[HZ02] Everett W. Howe and Hui June Zhu. "On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field". In: *Journal of Number Theory* 92.1 (2002), pp. 139–163.

Bibliography V

[MN02] Daniel Maisner and Enric Nart. "Abelian surfaces over finite fields as Jacobians". In: *Experiment. Math.* 11.3 (2002). With an appendix by Everett W. Howe, pp. 321–337. ISSN: 1058-6458. URL: http://projecteuclid.org/euclid.em/1057777425.

[NR08] Enric Nart and Christophe Ritzenthaler. "Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2". In: *Finite Fields Appl.* 14.3 (2008), pp. 676–702. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2007.09.006. URL: https://doi.org/10.1016/j.ffa.2007.09.006.

Bibliography VI

[Hal10] Safia Haloui. "The characteristic polynomials of abelian varieties of dimensions 3 over finite fields". In: *J. Number Theory* 130.12 (2010), pp. 2745–2752. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2010.06.008. URL: https://doi.org/10.1016/j.jnt.2010.06.008.

[SMZ14] Vijaykumar Singh, Gary McGuire, and Alexey Zaytsev. "Classification of characteristic polynomials of simple supersingular abelian varieties over finite fields". In: *Funct. Approx. Comment. Math.* 51.2 (2014), pp. 415–436. ISSN: 0208-6573. DOI: 10.7169/facm/2014.51.2.11. URL: https://doi.org/10.7169/facm/2014.51.2.11.

Bibliography VII

[Zar15] Yuri G. Zarhin. "Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension". In: *Journal of Pure and Applied Algebra* 219.6 (2015), pp. 2076–2098. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2014.07.024. URL: https://www.sciencedirect.com/science/article/pii/S0022404914002199.

[DKZ21] Taylor Dupuy, Kiran S. Kedlaya, and David Zureick-Brown. "Angle ranks of abelian varieties". In: *arXiv preprint arXiv:2112.02455* (2021), pp. 1–15.

Bibliography VIII

[Dup+21] Taylor Dupuy et al. “Isogeny Classes of Abelian Varieties over Finite Fields in the LMFDB”. In: *Arithmetic Geometry, Number Theory, and Computation*. Ed. by Jennifer S. Balakrishnan et al. Cham: Springer International Publishing, 2021, pp. 375–448. ISBN: 978-3-030-80914-0.