Estimates for the number of rational points on simple abelian varieties over finite fields

As Published: https://doi.org/10.1007/s00209-020-02520-w

Publisher: Springer Berlin Heidelberg

Persistent URL: https://hdl.handle.net/1721.1/131955

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Estimates for the number of rational points on simple abelian varieties over finite fields

Cite this article as: Borys Kadets, Estimates for the number of rational points on simple abelian varieties over finite fields, Mathematische Zeitschrift https://doi.org/10.1007/s00209-020-02520-w

ESTIMATES FOR THE NUMBER OF RATIONAL POINTS ON SIMPLE ABELIAN VARIETIES OVER FINITE FIELDS

BORYS KADETS

Abstract. Let A be a simple abelian variety of dimension g over the field $\mathbb{F}_q$. The paper provides improvements on the Weil estimates for the size of $A(\mathbb{F}_q)$. For an arbitrary value of q we prove $(\lfloor(\sqrt{q}-1)^2\rfloor+1)^g \leqslant \#A(\mathbb{F}_q) \leqslant (\lceil(\sqrt{q}+1)^2\rceil-1)^g$ holds with finitely many exceptions. We compute improved bounds for various small values of q. For instance, the Weil bounds for $q=3,4$ give a trivial estimate $\#A(\mathbb{F}_q) \geqslant 1$; we prove $\#A(\mathbb{F}_3) \geqslant 1.359^g$ and $\#A(\mathbb{F}_4) \geqslant 2.275^g$ hold with finitely many exceptions. We use these results to give some estimates for the size of the rational 2-torsion subgroup $A(\mathbb{F}_q)[2]$ for small q. We also describe all abelian varieties over finite fields that have no new points in some finite field extension.

1. Introduction

Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$. The following classical theorem of Weil gives an estimate for the size of the group $A(\mathbb{F}_q)$.

Theorem 1.1 (Weil [Wei48]). *Suppose $A/\mathbb{F}_q$ is an abelian variety of dimension g. Then*

$$(\sqrt{q}-1)^{2g} \leqslant \#A(\mathbb{F}_q) \leqslant (\sqrt{q}+1)^{2g}.$$

Our goal is to improve on the estimates of Theorem 1.1. For example, note that the lower bound is vacuous for $q=2,3,4$; our results imply an exponential lower bound in the cases $q=3,4$, while for $q=2$ there are infinitely many abelian varieties with one point as proved in [MS77].

It is natural to consider only simple abelian varieties. Let $\mathcal{A}_q(g)$ denote the (finite) set of isogeny classes of simple abelian varieties of dimension g over $\mathbb{F}_q$. Let $\mathcal{A}_q$ denote the union $\mathcal{A}_q := \bigcup_g \mathcal{A}_q(g)$. Define the quantities $a(q), A(q)$ by the formulas

$$a(q) := \liminf_{A\in\mathcal{A}_q} \#A(\mathbb{F}_q)^{1/g}, \quad A(q) := \limsup_{A\in\mathcal{A}_q} \#A(\mathbb{F}_q)^{1/g}.$$

Serre (see [Ser11] Section 4.6) noticed that for general varieties the estimates coming from the Weil conjectures can be improved using some metric properties of totally positive algebraic integers. In the case of abelian varieties, Aubry, Haloui and Lachaud [AHL13] observed that the asymptotic behavior of $A(q)$ is related to the Schur-Siegel-Smyth trace problem. Let us briefly recall its statement.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: bkadets@math.mit.edu.

This research was supported in part by Simons Foundation grant #550033.

Definition 1.2. Suppose α is an algebraic integer. Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ denote the Galois orbit of α. The *normalized trace* of α is the average value of its Galois conjugates: $\operatorname{tr}(\alpha) := 1/n(\alpha_1 + \cdots + \alpha_n)$.

Definition 1.3. Let $\mathrm{TP} \subset \overline{\mathbb{Q}}$ denote the set of all totally positive algebraic integers. The *Schur-Siegel-Smyth* constant ρ is defined by

$$\rho := \liminf_{\alpha \in \mathrm{TP}} \operatorname{tr}(\alpha).$$

The following conjecture is known as the Schur-Siegel-Smyth trace problem; see [Bor02, Chapter 10].

Conjecture 1.4. With notation as above $\rho = 2$.

Modified Chebyshev polynomials give an infinite family of totally positive algebraic integers with normalized trace 2, so $\rho \leqslant 2$. The current best lower bound for ρ is 1.79193, see [LW11].

The following proposition is implicit in [AHL13].

Proposition 1.5. *We have*

$$\lim_{q \to \infty} (q+1)^2 - A(q^2) \geqslant \rho.$$

For every q we have $(q+1)^2 \leqslant A(q^2) + 2 + q^{-2}$.

Assuming Conjecture 1.4, from Proposition 1.5 we get $A(q^2) = (q+1)^2 - 2 + o(1)$. Even though the exact values of $a(q), A(q)$ seem hard to determine, it is easy to see that they are not far from their trivial approximations, as the following proposition shows.

Proposition 1.6. *For every prime power q the following inequalities hold*

$$(\sqrt{q}-1)^2 \leqslant a(q) \leqslant \lceil (\sqrt{q}-1)^2 \rceil + 2,$$
$$\lfloor (\sqrt{q}+1)^2 \rfloor - 2 - q^{-1} \leqslant A(q) \leqslant (\sqrt{q}+1)^2.$$

Therefore the Weil bounds cannot be significantly improved for large values of q. Nevertheless, it is still interesting to get some improvements on the Weil estimates. The following theorem of Aubry, Haloui and Lachaud gives one such improvement.

Theorem 1.7. [AHL13, Corollaries 2.2 and 2.14] *For any prime power q the following inequalities hold*

$$a(q) \geqslant \lceil (\sqrt{q}-1)^2 \rceil, \quad A(q) \leqslant \lfloor (\sqrt{q}+1)^2 \rfloor.$$

We will derive improved estimates for $a(q)$ and $A(q)$ without using metric properties of traces and focusing on the case of small values of q. As a demonstration of the method for arbitrary q we give a simple proof of a stronger version of Theorem 1.7.

Theorem 1.8. *For any prime power q the following inequalities hold*

$$a(q) \geqslant \lfloor (\sqrt{q}-1)^2 \rfloor + 1, \quad A(q) \leqslant \lceil (\sqrt{q}+1)^2 \rceil - 1.$$

Theorem 1.8 is equivalent to Theorem 1.7 when q is not a square. For small values of q we obtain the following result.

Theorem 1.9. *For $q = 2, 3, 4, 5, 7, 8, 9$ the upper and lower bounds on $a(q)$ and $A(q)$ are given in Table 1.*

q	$a(q)$	$A(q)$
2	*1*	*4.035*
3	*1.359*	*5.634*
4	*2.275*	*7.382*
5	*2.7*	*8.835*
7	*3.978*	*11.734*
8	*4.635*	*13.05*
9	*5.47*	*14.303*

Table 1. Lower and upper bounds on $a(q)$ and $A(q)$, respectively.

Madan and Sät [MS77] give an explicit list of all isogeny classes of simple abelian varieties over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = 1$. We do not know if there are infinitely many simple abelian varieties with $\#A(\mathbb{F}_2) = 2$.

2. Abelian varieties over large fields

We use an explicit description of the set $\mathcal{A}_q$ of isogeny classes of simple abelian varieties provided by the Honda-Tate correspondence (see, for example [Wat69]). Recall that by Honda-Tate the elements of $\mathcal{A}_q$ are in one-to-one correspondence with the q-Weil numbers. For our purposes it is more convenient to use an equivalent description of the set $\mathcal{A}_q$ in terms of certain totally real algebraic integers.

Proposition 2.1. *Let $\mathcal{A}'_q$ denote the set of all totally real algebraic integers α, such that α and all of its Galois conjugates lie on the segment $\left[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2\right]$. Then there is a bijection $A : \mathcal{A}'_q \to \mathcal{A}_q$ such that for every $\alpha \in \mathcal{A}'_q$ the following equality holds*

$$(\operatorname{Norm}\alpha)^{1/\deg\alpha} = \Big(\#A(\alpha)(\mathbb{F}_q)\Big)^{1/\dim A(\alpha)}$$

Proof. Given a q-Weil number γ, define the algebraic integer α by $\alpha := (1-\gamma)(1-\overline{\gamma}) = 1 + q - \gamma - q/\gamma$. The integer α is totally positive. If A is an abelian variety corresponding to γ, then $\#A(\mathbb{F}_q)^{1/2g} = (\operatorname{Norm}(1-\gamma))^{1/\deg\gamma} = (\operatorname{Norm}\alpha)^{1/2\deg\alpha}$. Since the absolute value of γ is $\sqrt{q}$ and $\alpha = 1 + q + \operatorname{Re}(\gamma)$, we conclude that α and all of its conjugates belong to the segment $\left[1+q-2\sqrt{q}, 1+q+2\sqrt{q}\right]$.

Let $\phi\colon \mathcal{A}_q \to \mathcal{A}'_q$ be the map $\gamma \mapsto (1-\gamma)(1-\overline{\gamma})$. We claim that ϕ is a bijection. Given $\alpha \in \mathcal{A}'_q$, a root of $x + q/x = 1 + q - \alpha$ is a q-Weil number (the discriminant of this quadratic equation is $(\alpha - 1 - q)^2 - 4q \leqslant 0$, and the product of its roots is q). This defines a map $A : \mathcal{A}'_q \to \mathcal{A}_q$ which is inverse to ϕ. □

Proposition 2.1 shows that we need to understand the possibilities for the norm of a totally real algebraic integer whose conjugates lie in a given segment $[A, B]$. The trivial inequalities $A^{\deg\alpha} \leqslant \operatorname{Norm}(\alpha) \leqslant B^{\deg\alpha}$ are equivalent to the Weil estimates under the correspondence of Proposition 2.1. We produce totally real integers with almost extremal norms in Proposition 2.3 by utilizing shifted Chebyshev polynomials of Lemma 2.2; Proposition 2.3 combined with Theorem 1.1 gives Proposition 1.6.

Lemma 2.2. *Let T_n denote the Chebyshev polynomial of degree n, and let P_n be the integer monic polynomial defined by $P_n := T_n(x/2-1)$. Then for a fixed positive $N \in \mathbb{R}$ the following inequalities hold:*

$$N+2-1/N \leqslant \lim_{n\to\infty} |P_n(-N)|^{1/n} \leqslant N+2.$$

Proof. We use the formula

$$T_n(x) = \frac{1}{2}\left(\left(x+\sqrt{x^2-1}\right)^n + \left(x-\sqrt{x^2-1}\right)^n\right),$$

see [MH02, Equation 1.49]. By calculus, $\lim |T_n(-M)|^{1/n} = M+\sqrt{M^2-1}$, and the conclusion follows. □

Proposition 2.3. *The numbers $a(q)$, $A(q)$ satisfy*

$$a(q) \leqslant \lceil(\sqrt{q}-1)^2\rceil + 2, \quad A(q) \geqslant \lfloor(\sqrt{q}+1)^2\rfloor - 2 - q^{-1}.$$

Proof. To demonstrate either of the inequalities it suffices to construct infinitely many algebraic integers $\alpha \in \mathcal{A}'_q$ with geometric mean of the conjugates of α close to an end of the interval $\left[(1-\sqrt{q})^2, (1+\sqrt{q})^2\right]$. Let N be a positive integer and consider the interval $[N, N+4]$. Choose a prime number q and let P_q be the polynomial of Lemma 2.2. Recall that the roots of Chebyshev polynomials belong to the segment $[-1,1]$, so the roots of P_q belong to $[0,4]$. The monic integer polynomial P_q factors as $P_q = (x-2)\overline{P_q}$, where $\overline{P_q}$ is irreducible. Let α_q denote a root of $\overline{P_q(x-N)}$, then α_q and all of its conjugates belong to the interval $[N, N+4]$. The norm of α_q satisfies

$$\lim_{q\to\infty} \operatorname{Norm}(\alpha_q)^{1/\deg \alpha_q} = \lim_{q\to\infty} |\overline{P_q}(-N)|^{1/(q-1)} = \lim_{q\to\infty} |P_q(-N)|^{1/q}.$$

The right hand side is close to $N+2$ by Lemma 2.2. Taking $N = \lceil(1-\sqrt{q})^2\rceil$ produces infinitely many algebraic integers on $\left[(1-\sqrt{q})^2, (1+\sqrt{q})^2\right]$ with geometric mean of the conjugates asymptotically less than $\lceil(1-\sqrt{q})^2\rceil + 2$. Therefore $a(q) \leqslant \lceil(\sqrt{q}-1)^2\rceil + 2$. Similarly, taking $N = \lfloor(\sqrt{q}-1)^2\rfloor - 4$, gives the estimate on $A(q)$. □

Proposition 2.3 shows that the bounds of Theorem 1.1 are almost tight. We now give a simple proof of a more precise version of Proposition 1.5 (the original claim is recovered by taking limits as $q\to\infty$).

Proposition 2.4. *Let ρ be as in Definition 1.3. Then the following inequalities hold*

$$A(q^2) \geqslant (q+1)^2 - 2 - q^{-2}$$

$$A(q^2) \leqslant (q+1)^2 - \rho + O(q^{-1}).$$

Proof. The first inequality follows from Proposition 2.3. For the second inequality, fix a prime power q and an element $\alpha \in \mathcal{A}'_q$. For $x \in [(q-1)^2, (q+1)^2]$ we have

$$\log x = \log(q+1)^2 + \log\frac{x}{(q+1)^2} = 2\log(q+1) + \frac{x-(q+1)^2}{(q+1)^2} - \frac{1}{2}\left(\frac{x-(q+1)^2}{(q+1)^2}\right)^2 + O(q^{-3})$$
$$\leqslant 2\log(q+1) + \frac{x-(q+1)^2}{(q+1)^2} + O(q^{-3})$$

Averaging over the conjugates of α gives the following inequality, where tr denotes the normalized trace (trace divided by the degree) and the implied constants do not depend on α or q:

$$\log(\mathrm{Norm}(\alpha)^{1/g}) \leqslant 2\log(q+1) + \frac{\mathrm{tr}\,(\alpha-(q+1)^2)}{(q+1)^2} + O(q^{-3}).$$

Therefore

$$\begin{aligned} A(q^2) = \limsup_{\alpha\in\mathcal{A}'_q} \mathrm{Norm}(\alpha)^{1/\deg\alpha} &\leqslant \limsup_{\alpha\in\mathcal{A}'_q} (q+1)^2 e^{\mathrm{tr}(\alpha-(q+1)^2)/(q+1)^2} + O(q^{-1}) \\ &\leqslant (q+1)^2 + \inf_{\alpha\in\mathcal{A}'_q} \mathrm{tr}(\alpha-(q+1)^2) + O(q^{-1}). \end{aligned}$$

Since $(q+1)^2-\alpha$ is a totally positive algebraic integer, we have $A(q^2) \leqslant (q+1)^2 - \rho + O(q^{-1})$. □

The following theorem combined with Proposition 2.3 show that $a(q), A(q)$ can be determined up to an error of $1+q^{-1}$.

Theorem 2.5. *For all abelian varieties $A\in\mathcal{A}_q$ one of the following holds*

(1) *The element of $\mathcal{A}'_q$ corresponding to A is $\lfloor(\sqrt{q}-1)^2\rfloor$ or $\lceil(\sqrt{q}+1)^2\rceil$,*
(2) $\lfloor(\sqrt{q}-1)^2\rfloor + 1 \leqslant \#A(\mathbb{F}_q)^{1/g} \leqslant \lceil(\sqrt{q}+1)^2\rceil - 1.$

Proof. We want to estimate the norm of an algebraic integer $\alpha\in\mathcal{A}'_q$. First we derive the lower bound. It is straightforward to verify that for every integer $n>0$ the function

$$x \mapsto \frac{x}{(x-n)^{1/(n+1)}}$$

on the segment $[n,+\infty)$ has minimum $n+1$ at the point $x=n+1$. Let $n := \lfloor(\sqrt{q}-1)^2\rfloor$ and let $\alpha=\alpha_1\neq n$ be an element of $\mathcal{A}'_q$. Let $\alpha_2,\ldots,\alpha_d$ denote the conjugates of α_1. We have

$$\frac{\mathrm{Norm}\,\alpha}{\prod_i(\alpha_i-n)^{1/(n+1)}} = \prod_i \frac{\alpha_i}{(\alpha_i-n)^{1/(n+1)}} \geqslant (n+1)^d.$$

Since α is an algebraic integer, the product $\prod_i(\alpha_i-n)$ is a rational integer and therefore $|\prod_i(\alpha_i-n)| \geqslant 1$. Hence if $A\in\mathcal{A}_q$ is an abelian variety corresponding to α, then $\#A(\mathbb{F}_q)^{1/\dim A} = (\mathrm{Norm}\,\alpha)^{1/d} \geqslant (n+1)$. To get an upper bound, let $N=\lceil(\sqrt{q}+1)^2\rceil$. The function $x(N-x)^{1/(N-1)}$ has a maximum of $N-1$ at $x=N-1$. Similar argument as above shows that for every $\alpha\in\mathcal{A}'_q$, $\alpha\neq N$ we have $\mathrm{Norm}\,\alpha \leqslant (N-1)^d$. □

Theorem 2.5 improves on Theorem 1.7 when q is a square. In particular, it is possible to determine $a(q^2), A(q^2)$ up to an error of $1/2+q^{-2}$. It may be possible to improve Theorem 2.5 by replacing the function $x/(x-n)^{1/(n+1)}$ by a different auxiliary function. We don't know if this can be done for large q. However in the next section we find better auxiliary functions for small q and use them to improve the Weil estimates.

3. Abelian varieties over small fields

The following lemma gives a general form of the auxilary function method used in the proof of Theorem 2.5.

Lemma 3.1. *Suppose that for some positive $A, B, m, M \in \mathbb{R}$, some monic integer polynomials $P_1, ..., P_n$, $Q_1, ..., Q_m \in \mathbb{Z}[x]$, and for some positive $\gamma_1, ..., \gamma_n, \beta_1, ..., \beta_m \in \mathbb{R}$ the following inequalities hold for all $x \in [A, B]$:*

$$\frac{x}{\prod_i |P_i(x)|^{\gamma_i}} \geqslant m$$

$$x \prod_j |Q_j(x)|^{\beta_j} \leqslant M.$$

Suppose that α is an algebraic integer whose conjugates lie in $[A, B]$ and such that $P_i(\alpha), Q_j(\alpha) \neq 0$ for all i, j. Then

$$m \leqslant \mathrm{Norm}(\alpha)^{1/\deg \alpha} \leqslant M.$$

Proof. We will prove the lower bound, the upper bound can be derived similarly. Let $\{\alpha_1, ..., \alpha_d\}$ be the Galois orbit of $\alpha = \alpha_1$. Since P_i is a monic integer polynomial, the value of the product $\Pi_j |P_i(\alpha_j)|$ is a nonzero integer for every i. Therefore

$$\mathrm{Norm}\,\alpha \geqslant \frac{\mathrm{Norm}\,\alpha}{\prod_i \prod_j |P_i(\alpha_j)|^{\gamma_i}} = \prod_j \left(\frac{\alpha_j}{\prod_i P_i(\alpha_j)^{\gamma_i}} \right) \geqslant m^d.$$

□

We apply Lemma 3.1 to give bounds for $a(q)$ and $A(q)$ for small values of q.

Theorem 3.2. *For all but finitely many simple abelian varieties of dimension g over $\mathbb{F}_q$ the inequalities $b(q) \leqslant \#A(\mathbb{F}_q)^{1/g} \leqslant B(q)$ hold, where the values of $b(q), B(q)$ are given in Table 2. The elements of $P_i, Q_j \in \mathcal{A}'_q$ that do not satisfy the lower and the upper bound, respectively, are listed in Table 3.*

q	$b(q)$	$B(q)$
2	1	4.035
3	1.359	5.634
4	2.275	7.382
5	2.7	8.835
7	3.978	11.734
8	4.635	13.05
9	5.47	14.303

Table 2. Lower and upper bounds on $\#A(\mathbb{F}_q)^{1/g}$

Proof. For every q we obtain the bounds by applying Lemma 3.1 to the segment $[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$ and using the auxilary polynomials P_i, Q_j listed in Table 3; the corresponding parameters γ_i, β_j are in Table 4. The auxilary functions were found by searching for algebraic integers in $\mathcal{A}'_q$ with small degree and extremal norm and taking P_i, Q_j to be equal to the corresponding minimal polynomials. The parameters were then chosen by solving a linear programming problem of optimizing the extrema of the auxilary function of Lemma 3.1 on a fine mesh. Finally, the values of β_i or γ_j were used to create an auxilary function and find its extremal values. □

q	$P_i \in \mathcal{A}'_q$	$Q_j \in \mathcal{A}'_q$
2	n/a	$x-5$, $x^2-9x+19$, $x^3-13x^2+54x-71$
3	$x-1$, x^2-4x+2, $x^3-7x^2+12x-5$	$x-7$, $x-6$, $x^2-12x+34$
4	$x-1$, $x-3$, x^2-5x+5, $x^3-8x^2+19x-13$	$x-9$, $x-8$, $x^2-15x+55$, $x^3-22x^2+159x-377$
5	$x-2$, x^2-6x+7, $x^3-10x^2+28x-23$, $x^3-10x^2+30x-26$	$x-10$, $x-9$, $x^2-18x+79$, $x^2-17x+71$, $x^2-17x+69$
7	$x-3$, $x^2-10x+23$, $x^3-13x^2+54x-71$, $x^3-14x^2+61x-83$	$x-13$, $x-12$, $x^2-23x+131$, $x^2-22x+119$, $x^3-35x^2+406x-1561$, $x^3-34x^2+381x-1405$, $x^3-34x^2+379x-1379$
8	$x-3$, $x-4$, $x^2-9x+19$, $x^2-10x+23$ $x^3-15x^2+68x-97$, $x^3-15x^2+71x-107$	$x-14$, $x^2-27x+181$
9	$x-4$, $x-5$, $x-6$, $x^2-11x+29$, $x^2-12x+33$, $x^2-12x+34$	$x-16$, $x-15$, $x^2-129x+209$, $x^3-43x^2+614x-2911$

Table 3. Auxiliary polynomials for Theorem 3.2.

q	γ_i	β_j
2	n/a	0.141, 0.23, 0.09
3	0.306, 0.199, 0.019, 0.05, 0.108	0.1445, 0.155, 0.099
4	0.37, 0.12, 0.065, 0.01	0.054, 0.112, 0.02, 0.08
5	0.323, 0.063, 0.062, 0.007	0.11, 0.08, 0.066, 0.001, 0.003
7	0.289, 0.0048, 0.0457, 0.0178	0.055, 0.033, 0.026, 0.003, 0.035, 0.009, 0.006
8	0.044, 0.13, 0.09, 0.01, 0.02	0.08, 0.04
9	0.15, 0.08, 0.02, 0.03, 0.002, 0.003	0.033, 0.037, 0.033, 0.02

Table 4. Auxiliary parameters for Theorem 3.2

We apply the results of Theorem 3.2 to estimate the number of rational 2-torsion points on a simple abelian variety; a similar result for Jacobians is [BST+17, Theorem 7.1].

Corollary 3.3. *Suppose $q = 2$ or $q = 3$. Then for all but finitely many simple abelian varieties A over $\mathbb{F}_q$ the size of the set of rational 2-torsion points $A(\mathbb{F}_q)[2]$ is bounded from above by 2.717^g if $q = 2$ and by 3.782^g if $q = 3$.*

Proof. A rational 2-torsion point is in the kernel of both Frob $+1$ and Frob -1. Therefore $\#A(\mathbb{F}_q)[2] \leqslant \sqrt{\deg(\mathrm{Frob}-1)\deg(\mathrm{Frob}+1)} = \deg(\mathrm{Frob}^2-1)^{1/2} = \#A(\mathbb{F}_{q^2})^{1/2}$. Applying Theorem 3.2 to the right hand side proves the claimed inequalities. □

Recall that given a field extension L/K and a scheme X over K, a point $x \in X(L)$ is called *new* if $x \notin X(F)$ for all intermediate field extensions $L/F/K, F \neq L$.

Corollary 3.4. *Let $A/\mathbb{F}_q$ be a simple abelian variety. Suppose that A has no new points over $\mathbb{F}_{q^r}$. Then one of the following holds:*

(1) *$r = 2$, $q = 2, 3$ or 4, and A is the quadratic twist of an abelian variety $\hat{A}$ with $\hat{A}(\mathbb{F}_q) = 0$ (these are described in Theorem 3.2 for $q = 3, 4$, and in* [MS77] *for $q = 2$),*
(2) *$r = 3$, $q = 2$, and the element of $\mathcal{A}'_q$ corresponding to A is 4 or 5.*

Proof. Suppose $r = 2$. The equality $A(\mathbb{F}_{q^2}) = A(\mathbb{F}_q)$ is equivalent to the assertion that the quadratic twist A' of A has a unique rational point over $\mathbb{F}_q$. From now on suppose $r > 2$.

The Weil conjectures imply that A has a new point when q and r are sufficiently large, as we will now show. Suppose that for some abelian variety $A/\mathbb{F}_q$ of dimension g the set $A(\mathbb{F}_{q^r})$ has no new points. Then the following inequalities hold

$$\left(q^{r/2} - 1\right)^{2g} \leqslant \#A(\mathbb{F}_{q^r}) \leqslant \sum_{d|r,\, d<r} \#A(\mathbb{F}_{q^d}) \leqslant \sum_{d|r,\, d<r} \left(q^{d/2} + 1\right)^{2g} \leqslant 2\sqrt{r}\left(q^{r/4} + 1\right)^{2g}.$$

So $(q^{r/2} - 1)^{2g} \leqslant 2\sqrt{r}(q^{r/4} + 1)^{2g}$, which implies $(q^{r/4} - 1)^{2g} \leqslant 2\sqrt{r}$. The last inequality together with the condition $r > 2$ imply that the pair (q, r) is equal to one of the following $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 6)$, $(3, 3)$, $(3, 4)$, or $(4, 3)$. Out of these only the pairs $(2, 3)$, $(2, 4)$ satisfy the inequality $(q^{r/2} - 1)^{2g} \leqslant \sum_{d|r,d<r}(q^{d/2} + 1)^{2g}$ for some $g \geqslant 1$. Suppose $q = 2, r = 3$, then $A(\mathbb{F}_8) = A(\mathbb{F}_2)$. Since A is simple, $A_{\mathbb{F}_8}$ is isotypic: $A_{\mathbb{F}_8} \sim B^e$ with $e \leqslant 3$. Therefore, by Theorem 3.2 the following inequality holds with finitely many exceptions $\#A(\mathbb{F}_2)^{1/g} \leqslant 4.04 < 4.635 \leqslant \#A(\mathbb{F}_8)^{1/g}$. In each of the exceptional cases we test if $A(\mathbb{F}_2) = A(\mathbb{F}_8)$ by a direct computation; the resulting exceptions are listed in the statement of Case (2). Suppose that $q = 2$ and $r = 4$, which means $A(\mathbb{F}_{16}) = A(\mathbb{F}_2)$. Then $A(\mathbb{F}_4) = A(\mathbb{F}_{16})$, and so $A_{\mathbb{F}_4}$ is the quadratic twist of an abelian variety $\hat{A}$ with $\hat{A}(\mathbb{F}_4) = 0$. Theorem 3.2 implies that the element of $\mathcal{A}'_4$ corresponding to $\hat{A}$ is 1. A direct computation shows that the element of $\mathcal{A}'_2$ corresponding to A is 3 and that for this abelian variety $A(\mathbb{F}_2) \neq A(\mathbb{F}_{16})$. □

Acknowledgements

I thank my advisor Bjorn Poonen for many helpful suggestions. I thank Dinesh Thakur for suggesting the reference [MS77]. Finally I thank Padma Srinivasan, Nicholas Triantafillou, and Dmitri Kubrak for useful comments and discussions.

References

[AHL13] Yves Aubry, Safia Haloui, and Gilles Lachaud, *On the number of points on abelian and Jacobian varieties over finite fields*, Acta Arithmetica **160** (2013), no. 3, 201-241. MR3106095 ↑1, 1, 1.7

[BST+17] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, 2017. Preprint, `arXiv:1701.02458`. ↑3

[Bor02] Peter Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, vol. 10, Springer-Verlag, New York, 2002. MR1912495 (2003m:11045) ↑1

[LW11] Yanhua Liang and Qiang Wu, *The trace problem for totally positive algebraic integers*, J. Aust. Math Soc. **90** (2011), no. 3, 341–354. MR2833305 (2012h:11149) ↑1

[MS77] Manohar L. Madan and Pal Sät, *Abelian varieties and a conjecture of R.M. Robinson*, J. Reine Angew. Math. **291** (1977), 78–91. MR0439848 (55 #12730) ↑1, 1, (1), 3

[MH02] John C. Mason and David C. Handscomb, *Chebyshev polynomials*, Chapman and Hall/CRC, 2002. MR1937591 (2004h:33001) ↑2

[Ser11] Jean-Pierre Serre, *Lectures on Nx(p)*, 1st ed., Research Notes in Mathematics, vol. 11, CRC press, Boca Raton, 2011. MR2920749 ↑1

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369 (42 #279) ↑2

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann & Cie., Paris, 1948 (French). MR0027151 (10,262c) ↑1.1

URL: `http://math.mit.edu/~bkadets/`