Cubic twin prime polynomials are counted by a modular form

LIOR BARY-SOROKER AND JAKOB STIX

Abstract — We present the geometry lying behind counting twin prime polynomials in $\mathbb{F}_q[T]$ in general. We compute cohomology and explicitly count points by means of a twisted Lefschetz trace formula applied to these parametrizing varieties for *cubic* twin prime polynomials. The elliptic curve $X^3 = Y(Y-1)$ occurs in the geometry, and thus counting cubic twin prime polynomials involves the associated modular form. In theory, this approach can be extended to higher degree twin primes, but the computations becomes harder.

The formula we get in degree 3 is compatible with the Hardy-Littlewood heuristic on average, agrees with the prediction for $q \equiv 2 \pmod 3$ but shows anomalies for $q \equiv 1 \pmod 3$.

1. Introduction

One of the most exciting open problems in number theory is the *twin prime conjecture*, predicting infinitely many twin primes, i.e., pairs $(n, n+2)$ with both n, $n+2$ being primes. There is nothing special about the difference being 2 or about pairs, and indeed, one may easily state a general conjecture for k-tuples of the form $n+h_i$ for a fixed set of shifts $h_1 < h_2 < \ldots < h_k$. Applications often necessitate a quantitative version of the twin prime conjecture. Hardy and Littlewood made a precise quantitative conjecture in [HL23, §5 Theorem XI[1]], which essentially means that the events that 'n is prime' and '$n+2$ is prime' are independent up to a precise correlation factor $\mathfrak{S}(0,2) \approx 1.32032363169\ldots$.

Conjecture 1.1 (The Hardy-Littlewood Prime Tuple Conjecture)**.** *Let $h = (h_1, \ldots, h_k) \in \mathbb{Z}^k$ be a k-tuple of pairwise distinct integers. Then in the limit $x \to \infty$,*

$$\frac{1}{x}\#\{x \le n < 2x \ : \ n+h_1, \ldots, n+h_k \text{ are prime}\} = \mathfrak{S}(h)\frac{1}{(\log x)^k}(1+o(1)), \tag{1.1}$$

where, with $\nu_p(h)$ denoting the number of residues covered by $h_1, \ldots, h_k$ modulo p, we have

$$\mathfrak{S}(h) = \prod_{p \ prime} \frac{1-\nu_p(h)p^{-1}}{(1-p^{-1})^k}. \tag{1.2}$$

Note that a *local obstruction* occurs, if there is a prime p with $\nu_p(h) = p$. Then the conjecture trivially holds, because both sides of (1.1) are zero. If there are no local obstructions, the singular series $\mathfrak{S}(h)$ may be shown to converge to a positive constant.

In the course of history there were many attempts to solve this conjecture that, in spite of failing, produced exciting results. In his seminal work, Brun [Bru19] was the first to apply sieve methods to the twin prime problem and showed that the sum of reciprocals of twin primes converges. Brun also showed that there are infinitely many pairs $(n, n+2)$ with at most 16 prime factors. Chen [Che66] gave the state-of-the-art result in this direction proving that there exist infinitely many primes p such that $p+2$ is a product of at most 2 primes. In their famous theorem about arithmetic progression of primes, Green and Tao [GrT08] and Green, Tao, and Ziegler [GTZ12] tackle the easier problem when one more degree of freedom is added. More recently, Zhang [Zha14] made a breakthrough, by showing that there exist infinitely many prime pairs with bounded distance. The bound was improved by Polymath8 [Pol14] and later Maynard [May15] generalized Zhang's result to k-tuples, for any fixed $k > 0$. See the survey paper [Gra15] for more details.

The objective of this paper is to give more evidence to the Hardy-Littlewood prime tuple conjecture by studying its function field analog. For a finite field $\mathbb{F}_q$ we take the set

$$M_{d,q} = \{f(T) \in \mathbb{F}_q[T] \ ; \ \text{ monic of } \deg(f) = d\}$$

Date: November 15, 2017.

The authors acknowledge support provided by DAAD-Programm 57271540 Strategische Partnerschaften (supported by BMBF). The first author was partially supported by a grant of the Israel Science Foundation.

[1]Actually not a Theorem but a consequences of Hypothesis X of loc. cit.

as the analog of the interval $[x, 2x)$ with $q^d = \#M_{d,q}$ playing the role of $x \sim \#\{x \le n < 2x\}$. The goal is now to give for a k-tuple of pairwise distinct polynomials $h = (h_1, \dots, h_k) \in \mathbb{F}_q[T]$ with $\deg h_i < d$, precise asymptotics in the limit $q^d \to \infty$ for

$$\pi(d, q; h) = \#\{f \in M_{d,q} \ ; \ f + h_1, \dots f + h_k \text{ are irreducible}\}.$$

If we fix h, this only makes sense with fixed q and $d \to \infty$, and this case should be considered an analog of Conjecture 1.1 for the field $\mathbb{F}_q(T)$. If $h = (0, 1)$, or if we expect some uniformity in h, then we can also ask for the asymptotics for d fixed and $q \to \infty$.

Hall [Hal06] proved that for any fixed $q > 3$ there exist infinitely many d's and $f \in M_{d,q}$ such that f and $f+1$ are prime. This proof is elementary, and extends to k-tuples with scalar shifts if q is sufficiently large with respect to k and using the Riemann hypothesis for curves. The sequence of d's in Hall's proof grows exponentially fast and hence is very sparse. Adapting Maynard's result to function fields, Castillo et al [Cas15] extend Hall's result for sufficiently large fixed q, to any d in an explicit arithmetic progression and give a lower bound on the number of pairs of the right order of magnitude. However these method seems to fail when the shift is not a monomial.

Another approach taken in recent studies is to let $q \to \infty$ and control $\pi(d, q; h)$ as an application of the Lang-Weil bounds. This direction proved successful as the analogue of the Hardy-Littlewood prime tuple conjecture was completely resolved: Bender and Pollack [BeP09] for pairs in odd characteristic, the first author [Bar12] for general tuples in odd characteristic, and Carmon [Car15] applies the method of the first author in even characteristic, and establishes the following in all cases in the limit $q \to \infty$:

$$\pi(d, q; h) = \frac{q^d}{d^k} \mathfrak{S}_q(h)(1 + E(d, q; h)), \qquad \text{with error term} \quad E(d, q; h) \ll_{d,k} q^{-1/2}. \tag{1.3}$$

Note that the size of the error term depends on the tuple h only through its degree bound d. We discuss the function field analog $\mathfrak{S}_q(h)$ of the Hardy-Littlewood singular series in Section §2.

One may naively expect a square root cancelation, namely a bound for the error term of the form

$$E(d, q; h) \ll q^{-d/2+\epsilon}.$$

Some results give better error terms than (1.3) on average [KRG16] and for special h [GS18] based on variance computations [KeR14] and equidistribution results by Katz [Kat12a, Kat12b]. We also remark that (1.3) has inspired more work, see [ABR15, BaB15, BSF18, Ent14]. The downside of (1.3), is that the error term is not small enough for us to see the 'arithmetic' due to the dependence on h. Pollack [Pol08, Appendix] computed that

$$\mathfrak{S}_q(h) = 1 + O(q^{-1}),$$

so in the limit $q \to \infty$ the events that the $f + h_i$ are irreducible are indeed independent.

In this paper we give an exact formula for $\pi(d, q; h)$ when $d \le 3$ and $h = (0, 1)$. The case of $d = 1$ is trivial and left to the reader. The case $d = 2$ is straight forward using Weil's bounds on exponential sums. We use the technique of the present paper to deduce the $d = 2$ case in Example 3.2 as (3.5):

$$\pi(2, q; (0, 1)) = \frac{1}{4} q^2 \cdot \begin{cases} 1 - (2 - (-1)^{(q-1)/2}) \cdot q^{-1} & \text{if } q \text{ is odd,} \\ 1 - 2q^{-1} & \text{if } q \text{ is even.} \end{cases}$$

For $d = 3$, the formula depends on whether or not the characteristic is 3. If $3 \mid q$ we get a polynomial formula, while if $3 \nmid q$, our formula involves the number of rational points in the reduction of the elliptic curve $\mathscr{E}$ with Weierstraß-equation

$$X^3 = Y(Y - 1).$$

Recall that if $3 \nmid q$, the curve $\mathscr{E}$ has good reduction and by the Hasse bound

$$|q + 1 - \#\mathscr{E}(\mathbb{F}_q)| \le 2\sqrt{q}. \tag{1.4}$$

Theorem 1.2. *Let q be a prime power. Then, we have*

$$\pi(3, q; (0, 1)) = \frac{1}{9} q^3 \cdot \begin{cases} 1 - q^{-1} - 3q^{-2} & \text{if } q \equiv 0 \pmod 3, \\ 1 + \left(c_q^2 - 3\right) \cdot q^{-1} - 2q^{-2} & \text{if } q \equiv 1 \pmod 3, \\ 1 - q^{-1} - 2q^{-2} & \text{if } q \equiv 2 \pmod 3, \end{cases} \tag{1.5}$$

where $c_q := \frac{1+q-\#\mathscr{E}(\mathbb{F}_q))}{\sqrt{q}}$, so that $0 \le c_q^2 \le 4$ by (1.4).

We will discuss the comparison with the prediction by the analog of the Hardy-Littlewood conjecture in Section §2.

Remark 1.3. Since all elliptic curves over $\mathbb{Q}$ are modular, there is a newform $f_{\mathscr{E}}(q)$ associated to the elliptic curve $\mathscr{E}$ with Weierstraß-equation $X^3 = Y(Y-1)$. The newform can easily be determined being the only newform of weight 2 and level 27, see the database [LMFDB, Elliptic Curve 27.a4],

$$f_{\mathscr{E}}(q) = \sum_{n\geq 1} a_n q^n = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} + O(q^{20}).$$

This means that for all prime numbers p not divisible by 3 we have by the Eichler-Shimura congruence relation

$$a_p = 1 + p - \#\mathscr{E}(\mathbb{F}_p) = \alpha_p + \beta_p,$$

where α_p, β_p are the eigenvalues of Frobenius, i.e., the roots of

$$T^2 - a_p T + p = 0.$$

For both $\lambda = \alpha_p$ or β_p, the sequence $(\lambda^m)_m$ belongs to the 2-dimensional vector space V of all sequences $(b_m)_m$ satisfying

$$b_{m+1} = a_p b_m - p b_{m-1}.$$

Moreover, for $3 \nmid p$, the coefficients of $f_{\mathscr{E}}(q)$ satisfy the recursion $a_{p^{m+1}} = a_p a_{p^m} - p a_{p^{m-1}}$ for all $m \geq 1$ due to the relations among the various Hecke operators, see for example [Ser73, §VII.5.4]. Hence $(a_{p^m})_m$ and $(a_{p^{m-1}})_m$ (the latter suitably interpreted as 0 for $m = 0$) also belong to V. It follows easily that for $q = p^m$ and all $m \geq 1$

$$1 + q - \#\mathscr{E}(\mathbb{F}_q) = (\alpha_p)^m + (\beta_p)^m = 2a_{p^m} - a_p a_{p^{m-1}} = 2a_q - a_p a_{q/p}.$$

In conclusion the term c_q^2 in Theorem 1.2 can be computed as

$$c_q^2 = \frac{1}{q} \cdot (2a_q - a_p a_{q/p})^2$$

as a combination of q-expansion coefficients of the newform $f_{\mathscr{E}}(q)$.

The geometric description of the parametrizing variety and thus also the computation of its cohomology can be adapted easily to the case of general scalar shifts $h \in \mathbb{F}_q^\times$. The resulting fomula involves the cubic twist $\mathscr{E}_h/\mathbb{F}_q$ of the elliptic curve $\mathscr{E} \otimes_{\mathbb{Z}[1/3]} \mathbb{F}_q$ over $\mathbb{F}_q$ given by

$$hX^3 = Y(Y-1).$$

We set $c_{q,h} := \frac{1+q-\#\mathscr{E}_h(\mathbb{F}_q)}{\sqrt{q}}$, so that $0 \leq c_{q,h}^2 \leq 4$ by (1.4). Note also that $c_{q,h}$ only depends on h modulo cubes: the class of h in $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$.

Theorem 1.4. *Let q be a prime power. For all $h \in \mathbb{F}_q$, $h \neq 0$, we have*

$$\pi(3, q; (0,h)) = \frac{1}{9}q^3 \cdot \begin{cases} 1 - q^{-1} - 3q^{-2} & \text{if } q \equiv 0 \pmod 3, \\ 1 + (c_q^2 - 3) \cdot q^{-1} - 2q^{-2} & \text{if } q \equiv 1 \pmod 3 \text{ and } h \text{ is a cube in } \mathbb{F}_q, \\ 1 + c_q \cdot c_{q,h} \cdot q^{-1} - 8q^{-2} & \text{if } q \equiv 1 \pmod 3 \text{ and } h \text{ is not a cube in } \mathbb{F}_q, \\ 1 - q^{-1} - 2q^{-2} & \text{if } q \equiv 2 \pmod 3. \end{cases} \tag{1.6}$$

On avarage over all $h \in \mathbb{F}_q^\times$ we obtain the predicted asymptotic up to $\mathrm{O}(q^{-2})$ in the error term:

$$\frac{1}{q-1} \sum_{h \in \mathbb{F}_q^\times} \pi(3, q; (0,h)) = \frac{1}{9}q^3 \cdot \begin{cases} 1 - q^{-1} - 3q^{-2}, & \text{if } q \equiv 0 \pmod 3, \\ 1 - q^{-1} - 6q^{-2}, & \text{if } q \equiv 1 \pmod 3, \\ 1 - q^{-1} - 2q^{-2}, & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

Method. The proof of Theorem 1.2 will be given at the end of Section §5.3 when enough of the geometry and cohomology of the problem has been explained. It then follows by combining the twisted Lefschetz trace formula of Proposition 3.1, which reduces the counting to the problem of determining the effect of Frobenius and the twisting 3-cycle on cohomology, with the explicit computation of the respective traces that is completed in Proposition 5.10.

We will study the $\mathbb{F}_q$-variety parametrizing pairs of algebraic elements over $\mathbb{F}_q$ of general degree d such that the respective minimal polynomials differ by 1 . We count these pairs by means of the Lefschetz trace formula in étale cohomology. This strategy is applicable in principle for all d, but we succeed to pursue it only for $d \leq 3$ because here we manage to compute the respective cohomology as a representation. To summarize, the geometry for $d = 3$ is as follows.

Theorem 1.5. *Let q be a prime power and $3 \nmid q$. Roots of Cubic twin prime polynomial pairs in $\mathbb{F}_q[T]$ are parametrized by a variety that is an $\mathbb{F}_q$-form of a variety which is an $\mathbb{A}^1$-bundle over the complement of an explicit divisor on an explicit hyperelliptic surface.*

Proof. This is the geometric content of Section §4. The hyperelliptic surface is covered by $E \times E$ for the elliptic curve $E : X^3 = Y(Y-1)$, and the divisor to be removed is $T + H$ in the notation of loc. cit. □

Outline. In Section §3 we recall how to count rational $\mathbb{F}_q$-points of a Galois-twisted variety and describe the variety U_τ over $\mathbb{F}_q$ that enumerates twin prime polynomial pairs of any degree d over $\mathbb{F}_q$. In Section §4 we analyse its geometry in the case $d = 3$ with special emphasis on the action of a 3-cycle τ. Section §5 is devoted to the computation of (total) étale cohomology with compact support as a virtual representation in a Grothendieck-group of Galois representations together with an action by τ. In the penultimate Section §5.3 we then evaluate the trace of the twisted Frobenius and derive the formula of Theorem 1.2.

2. The singular series for function fields

Since we are interested in studying the number of prime polynomials of fixed degree d as a function of the number of elements in the field q, we denote by $\pi_d(q) = \pi(d, q; (0))$ the number of primes of $\mathbb{F}_q[T]$ of degree d. We would like to express the Hardy-Littlewood singular series for the function field $\mathbb{F}_q(T)$

$$\mathfrak{S}_q((0,1)) = \prod_{\mathfrak{p} \text{ prime of } \mathbb{F}_q[T]} \left(\frac{1 - 2N(\mathfrak{p})^{-1}}{(1 - N(\mathfrak{p})^{-1})^2} \right) = \prod_{d \geq 1} \left(\frac{1 - 2q^{-d}}{(1 - q^{-d})^2} \right)^{\pi_d(q)}$$

as the value of a convergent power series $S(u) \in \mathbb{Q}[[u]]$ in $u = q^{-1}$. Here $S(u)$ shall be independent of q and thus is uniquely determined if it exists. This can be done as follows. First, for $q = 2$ we have a local obstruction at places of degree 1, hence $\mathfrak{S}_2((0,1)) = 0$. Therefore we assume from now on that $q \geq 3$.

Lemma 2.1. *For all $d \geq 1$ there is a polynomial $P_d(u) \in \mathbb{Q}[u]$ such that for all prime powers q*

$$P_d(q^{-1}) = \pi_d(q) \cdot q^{-d}.$$

Moreover, we have $|P_d(t)| \leq 1$ for all complex $|t| \leq 1$.

Proof. This follows from Gauß's formula $\pi_d(q) = \frac{1}{d} \sum_{k|d} \mu(k) q^{d/k}$. Concretely, we have

$$P_d(u) = \frac{1}{d} \sum_{k|d} \mu(k) u^{d - d/k}.$$

The estimate is trivial because there are at most d summands. □

Lemma 2.2. *The following power series is convergent for $|u| < 1/2$:*

$$\lambda(u) := \sum_{k \geq 2} \frac{2 - 2^k}{k} u^{k-1} \in u \cdot \mathbb{Q}[[u]].$$

For all $0 < t_0 < 1/2$ there is a constant $c = c(t_0)$ such that $|\lambda(t)| \leq c \cdot |t|$ for all complex $|t| \leq t_0$.

Proof. The power series is an expansion of $\frac{\log(1-2u) - 2\log(1-u)}{u}$ which is holomorphic in $|u| < 1/2$, hence its radius of convergence is $1/2$.

The existence of a constant $c(t_0)$ and the estimate follows because $\lambda(u)/u$ is continuous and thus bounded on the compact ball of radius t_0. □

Since $\lambda(u^d)$ is divisible by u^d, the following sum formally converges

$$S(u) := \exp\left(\sum_{d \geq 1} P_d(u) \cdot \lambda(u^d) \right) \in \mathbb{Q}[[u]].$$

Proposition 2.3. *The power series $S(u)$ converges for $|u| < 1/2$. For all prime powers $q \geq 3$ we have*

$$S(q^{-1}) = \mathfrak{S}_q((0,1)).$$

In particular, the product defining the function field singular series converges absolutely.

Proof. It suffices to show that the sum of holomorphic functions $\sum_{d\geq 1} P_d(u)\cdot\lambda(u^d)$ converges uniformly on any ball of radius $t_0 < 1/2$. This follows at once from the estimates in Lemma 2.1 and Lemma 2.2.

In order to compute the value $S(q^{-1})$ we rather compute its logarithm as follows:

$$\begin{aligned}\log S(q^{-1}) &= \sum_{d\geq 1} P_d(q^{-1})\cdot\lambda(q^{-d}) = \sum_{d\geq 1}\pi_d(q)q^{-d}\cdot\frac{\log(1-2q^{-d})-2\log(1-q^{-d})}{q^{-d}}\\ &= \sum_{d\geq 1}\pi_d(q)\cdot\log\left(\frac{1-2q^{-d}}{(1-q^{-d})^2}\right) = \log\prod_{d\geq 1}\left(\frac{1-2q^{-d}}{(1-q^{-d})^2}\right)^{\pi_d(q)} = \log\mathfrak{S}_q((0,1)).\end{aligned}$$

□

Remark 2.4. In order to analyse $S(u)$ at $u = 1/2$, we use $P_1(u) = 1$ and split the factor corresponding to $d = 1$ by writing

$$S(u) = (1-2u)^2\cdot\exp\Big(\sum_{k\geq 1}\big(2^{k+1}(\frac{1}{k}-\frac{1}{k+1})+\frac{2}{k+1}\big)u^k\Big)\cdot\exp\left(\sum_{d\geq 2}P_d(u)\cdot\lambda(u^d)\right).$$

The factor $\exp\left(\sum_{d\geq 2}P_d(u)\cdot\lambda(u^d)\right)$ converges for $u < 1/\sqrt{2}$, and the middle factor can be dealt with at $u = 1/2$ by Abel's theorem of converging power series on their radius of convergence. Hence the series $S(u)$ converges at $u = 1/2$ and takes the value $S(1/2) = 0$ there. This agrees with $\mathfrak{S}_2((0,1)) = 0$.

Remark 2.5. It is not difficult to calculate the low degree terms of the power series $S(u)$. For all $m \geq 1$, we have in $\mathbb{Q}[[u]]$, by truncating all of the power series in the definition, that

$$S(u) = \sum_{\nu=0}^{m}\frac{1}{\nu!}\left(\sum_{d=1}^{m}P_d(u)\sum_{k=2}^{\lfloor 1+\frac{m}{d}\rfloor}\frac{2-2^k}{k}u^{d(k-1)}\right)^{\nu} + \mathrm{O}(u^{m+1}).$$

Concretely, we obtain using SageMath:

$$S(u) = 1 - u - 2u^2 - u^3 - 2u^4 + 2u^5 + 6u^7 + 7u^8 + 13u^9 + 20u^{10} + 32u^{11} + 41u^{12} + O(u^{13}).$$

Remark 2.6. When analysing the asymptotic $q\to\infty$ for fixed d, then of course the primes of degree $> d$ do not pose any constraints in the heuristic. Consequently, the correlation factor $\mathfrak{S}_q((0,1))$ should skip these primes. If we use the truncated power series

$$S(u) = S_d(u) + \mathrm{O}(u^{d+1}),$$

with a polynomial $S_d(u)$ of degree $\leq d$, then it is easy to see that primes of degree $> d$ do not influence $S_d(u)$. Moreover, in order to take into acount the translation invariance for $h = (0,1)$, we should rather truncate modulo u^d. Hence we propose to compare the actual count with the truncated series $\frac{q^d}{d^2}\cdot S_{d-1}(q^{-1})$:

$$\pi(d,q;(0,1)) = \frac{q^d}{d^2}\cdot S_{d-1}(q^{-1})\cdot\big(1+E(d,q;(0,1))\big).$$

Here are the predictions and error terms accordingly:

d	prediction	q	$\pi(d,q;(0,1))$	$E(d,q;(0,1))$
1	q		q	0
2	$\frac{q^2}{4}(1-q^{-1})$	$\equiv 0\ (2)$	$\frac{q^2}{4}(1-2q^{-1})$	$q^{-1}+\mathrm{O}(q^{-2})$
		$\equiv 1\ (4)$	$\frac{q^2}{4}(1-q^{-1})$	0
		$\equiv 3\ (4)$	$\frac{q^2}{4}(1-3q^{-1})$	$2q^{-1}+\mathrm{O}(q^{-2})$
3	$\frac{q^3}{9}(1-q^{-1}-2q^{-2})$	$\equiv 0\ (3)$	$\frac{q^3}{9}(1-q^{-1}-3q^{-2})$	$q^{-2}+O(q^{-3})$
		$\equiv 1\ (3)$	$\frac{q^3}{9}(1-(c_q^2-3)q^{-1}-2q^{-2})$	$(2-c_q^2)q^{-1}+\mathrm{O}(q^{-2})$
		$\equiv 2\ (3)$	$\frac{q^3}{9}(1-q^{-1}-2q^{-2})$	0

Thus, if $d = 3$ and $q \not\equiv 1 \pmod 3$, then (1.5) is consistent with square root cancelation in (1.3). When $q \equiv 1 \pmod 3$, the coefficient of q^{-1} varies with q. We will now argue that at least on avarage among those q this coefficient is again -1. There are unique angles $\vartheta_q \in [0, \pi]$ such that $c_q = 2\cos(\vartheta_q)$. Since $\mathscr{E}$ is a CM-curve, its L-function can be expressed in terms of a Hecke character following Deuring [Deu53]. In this case already Hecke [Hec18] showed that for primes split in the field of multiplication, here $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, the distribution of angles is uniform with respect to the measure $\frac{1}{\pi} d\vartheta$, see Section §2.4 of the survey by Sutherland [Su17] for more details and references. Hence, the value of c_q^2 on average is

$$\frac{1}{\pi} \int_0^\pi 4\cos^2(\vartheta) d\vartheta = 2,$$

and the average value of the coefficient of q^{-1} becomes again -1.

3. Parametrizing irreducible polynomials

In this section we describe the geometry of the parametrizing varieties of twin primes.

3.1. **Rational points of twists.** Let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Let $X_0/\mathbb{F}_q$ be a variety and denote by $X = X_0 \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ or by the usual notation $X_{0,\bar{\mathbb{F}}_q}$ the base change to $\bar{\mathbb{F}}_q$. The $\bar{\mathbb{F}}_q$-linear geometric q-Frobenius map

$$F : X \to X$$

raises coordinates (defined over $\mathbb{F}_q$, i.e., coordinates of X_0) to q-th powers. Hence the set of $\mathbb{F}_q$-rational points of X_0 is the set of Frobenius fixed points of X

$$X_0(\mathbb{F}_q) = \{x \in X(\bar{\mathbb{F}}_q) \ ; \ F(x) = x\}, \tag{3.1}$$

and counted by the Lefschetz trace formula in étale cohomology with compact support for $\ell \neq p$ as

$$\#X_0(\mathbb{F}_q) = \operatorname{tr}\big(F | \operatorname{H}^*_{\mathrm{c}}(X, \mathbb{Q}_\ell)\big) := \sum_{i=0}^{2\dim X} (-1)^i \operatorname{tr}\big(F | \operatorname{H}^i_{\mathrm{c}}(X, \mathbb{Q}_\ell)\big). \tag{3.2}$$

For background on étale cohomology and a proof of the Lefschetz trace formula we refer to [FK88].

Forms of X_0 over $\mathbb{F}_q$ are obtained by Galois descent via a twisted Galois action on X by means of a continuous 1-cocycle $\sigma \mapsto a_\sigma$

$$a : \operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \operatorname{Aut}(X/\bar{\mathbb{F}}_q)$$

with values in the $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-module $\operatorname{Aut}(X/\bar{\mathbb{F}}_q)$, see for example [Sk01, §2]. Being a cocycle means for all $\sigma, \pi \in \operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ that $a_{\sigma\pi} = a_\sigma \circ \sigma(a_\pi)$. Equivalently, the map

$$\sigma \mapsto a_\sigma \sigma \in \operatorname{Aut}(X/\mathbb{F}_q)$$

defines another Galois action on X. The a-twist of $X_0/\mathbb{F}_q$ is defined as the quotient of X by the twisted Galois action and is here denoted by

$$X_a/\mathbb{F}_q.$$

Let $\varphi \in \operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be the arithmetic q-Frobenius map $\varphi(z) = z^q$. The 1-cocycle a is uniquely determined by its value $\alpha = a(\varphi)$. The Frobenius of X arising from the new $\mathbb{F}_q$-structure X_a is nothing but

$$F_a = \alpha F.$$

It follows that $\mathbb{F}_q$-rational points of the twist are described by

$$X_a(\mathbb{F}_q) = \{x \in X(\bar{\mathbb{F}}_q) \ ; \ F_a(x) = x\} = \{x \in X(\bar{\mathbb{F}}_q) \ ; \ F(x) = \alpha^{-1}(x)\} \tag{3.3}$$

and counted as

$$\#X_a(\mathbb{F}_q) = \operatorname{tr}\big(\alpha F | \operatorname{H}^*_{\mathrm{c}}(X, \mathbb{Q}_\ell)\big). \tag{3.4}$$

3.2. **Twisting varieties of polynomials.** Monic polynomials of degree d

$$f(T) = T^d + a_1 T^{d-1} + \ldots + a_{d-1}T + a_d$$

with coefficients $a_i \in \mathbb{F}_q$ are parametrized by d-dimensional affine space as

$$f = (a_1, \ldots, a_d) \in \mathbb{A}^d(\mathbb{F}_q).$$

We have a finite branched S_d-cover $s : \mathbb{A}^d \to \mathbb{A}^d$

$$s(x_1, \ldots, x_d) = (-\sigma_1(\underline{x}), \ldots, (-1)^d \sigma_d(\underline{x})) = \prod_{i=1}^{d}(T - x_i)$$

whose coordinates are given by the elementary symmetric polynomials in $\underline{x} = (x_1, \ldots, x_d)$

$$\sigma_r(\underline{x}) = \sum_{1 \le i_1 < \ldots < i_r \le n} x_{i_1} \cdot \ldots \cdot x_{i_r}.$$

The ramification locus of s is given by the vanishing locus of the discriminant

$$\Delta_x := \prod_{i \neq j}(x_i - x_j) \in \mathbb{Z}[a_1, \ldots, a_d] \subseteq \mathbb{Z}[x_1, \ldots, x_d],$$

that is the locus of polynomials with multiple roots.

We consider the twist[2] of $\mathbb{A}^d$ by the 1-cocycle τ determined by its value on Frobenius being the d-cycle

$$\tau(\varphi) = (123 \ldots d) \in S_d$$

with respect to the permutation representation

$$S_d \to \mathrm{GL}_d(\mathbb{F}_q) \to \mathrm{Aut}(\mathbb{A}^d).$$

As described in (3.3), rational points of the twist are those points $\underline{x} = (x_1, \ldots, x_d) \in \mathbb{A}^d(\bar{\mathbb{F}}_q)$ invariant under the twisted Frobenius (with indices considered modulo d):

$$(\mathbb{A}^d)_\tau(\mathbb{F}_q) = \{\underline{x} \in \mathbb{A}^d(\bar{\mathbb{F}}_q) \ ; \ x_i^q = x_{i+1} \ \text{ for all } i = 1, \ldots, d\}.$$

Being S_d-invariant, the cover s becomes a cover

$$s_\tau : (\mathbb{A}^d)_\tau \to \mathbb{A}^d.$$

Rational points of the twist outside of the discriminant locus map under s to polynomials whose roots are all distinct and cyclically permuted by q-Frobenius, hence exactly to irreducible polynomials. Every unramified point $f \in \mathbb{A}^d(\mathbb{F}_q)$ in the image of the map

$$s_\tau : (\mathbb{A}^d)_\tau(\mathbb{F}_q) \to \mathbb{A}^d(\mathbb{F}_q)$$

has d preimages, because each preimage in $(\mathbb{A}^d)_\tau(\mathbb{F}_q)$ is determined by its $x_1 \in \bar{\mathbb{F}}_q$ which can be any of the d distinct roots of the irreducible polynomial f.

3.3. **Parametrizing twin prime polynomials.** Let M be the $\mathbb{F}_q$-vector space with generators

$$x_1, \ldots, x_d, y_1, \ldots, y_d, z$$

and the only relation $\sigma_1(\underline{x}) = \sigma_1(\underline{y})$. The corresponding projective space

$$\mathbb{P}(M) = \mathrm{Proj}(\mathrm{Sym}^\bullet M)$$

is the hyperplane $V\big(\sigma_1(\underline{x}) = \sigma_1(\underline{y})\big)$ in $\mathbb{P}^{2d}$, the projective space with homogeneous coordinates

$$[x_1 : \ldots : x_d : y_1 : \ldots : y_d : z].$$

In $\mathbb{P}(M)$ we consider the subvariety

$$X = V\big(\sigma_2(\underline{x}) - \sigma_2(\underline{y}), \ \ldots, \sigma_{d-1}(\underline{x}) - \sigma_{d-1}(\underline{y}), \ \sigma_d(\underline{x}) - \sigma_d(\underline{y}) + (-z)^d\big) \subseteq \mathbb{P}(M).$$

On the distinguished open $z \neq 0$ we map a point $[\underline{x} : \underline{y} : 1]$ to the pair of polynomials

$$f(T) = \prod_{i=1}^{d}(T - x_i), \qquad g(T) = \prod_{j=1}^{d}(T - y_j)$$

[2]Because of the general theorem Hilbert 90, $\mathrm{H}^1(\mathbb{F}_q, \mathrm{GL}_d) = 1$, the twisted $\mathbb{A}^d$ is isomorphic to $\mathbb{A}^d$. This fact leads to good asymptotic formulae for the number of irreducible polynomials in $\mathbb{F}_q[X]$ of degree d.

by means of which the defining equations for X take the simple form

$$g(T) = f(T) + 1.$$

Let Δ_x (resp. Δ_y) denote the discriminant in terms of the tuple of variables $\underline{x}$ (resp. $\underline{y}$). Let $U \subseteq X$ be the open

$$U = X \cap \{\Delta_x \cdot \Delta_y \cdot z \neq 0\},$$

i.e., the locus where the description is by separable polynomials.

We let S_d act diagonally on M by permuting blockwise both tuples of variables $\underline{x}$ and $\underline{y}$, keeping z fixed. This induces actions on $\mathbb{P}(M)$, X and U respectively. It follows from Section 3.2 and the notation introduced there that rational points of the twist U_τ are

$$U_\tau(\mathbb{F}_q) = \{(x_1, \dots, y_d) \in \bar{\mathbb{F}}_q^{2d} \ ; \ f \text{ and } g \text{ are monic, irreducible and } g(T) = f(T) + 1\}.$$

Therefore we have proved the following proposition as a consequence of (3.2). Recall that we denote by $U_{\bar{\mathbb{F}}_q}$ the base change $U \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$.

Proposition 3.1. *The number of twin prime polynomial pairs in $\mathbb{F}_q[T]$ of degree d is*

$$\pi(d, q; (0,1)) = \frac{1}{d^2} \cdot \#U_\tau(\mathbb{F}_q) = \frac{1}{d^2} \mathrm{tr}\big(\tau F \,|\, \mathrm{H}_{\mathrm{c}}^*(U_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)\big).$$

We are left with the task to understand $\mathrm{H}_{\mathrm{c}}^*(U_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ as $S_d \times \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-module. Since we are only interested in a certain trace, it suffices to determine cohomology in a Grothendieck group of virtual representations.

Example 3.2. We compute the case $d = 2$ using the above notation along the strategy for the $d = 3$ case to be treated in the following section §4. The variety X is given in $\mathbb{P}^4$ by the equations

$$\begin{aligned} x_1 + x_2 &= y_1 + y_2, \\ x_1 x_2 &= y_1 y_2 - z^2. \end{aligned}$$

Using $a = x_1 - y_2$, $b = x_2 - y_2$, $c = y_1 - y_2$, and z we may express these as

$$\begin{aligned} a + b &= c, \\ ab &= -z^2, \end{aligned}$$

so that the complement of $\star_M := [1:1:1:1:0]$ in X forms an $\mathbb{A}^1$-bundle over the smooth conic

$$\mathbb{P}^1 \simeq Y = V(z^2 + ab) \subseteq \mathbb{P}^2.$$

The open $U = X \cap \{(x_1 - x_2)(y_1 - y_2)z \neq 0\}$ is the preimage in this $\mathbb{A}^1$-bundle of

$$V = Y \cap \{(a - b)(a + b)z \neq 0\}.$$

In coordinates $[a : b : z]$, this removes the following set of points D from Y:

- If the characteristic is 2, the points $D = \{P_1, P_2, P_3\}$ with
$$P_1 = [0:1:0], \ P_2 = [1:0:0], \text{ and } P_3 = [1:1:1].$$
- If the characteristic is not 2, the points $D = \{P_1, P_2, Q_+, Q_-, R_+, R_-\}$ with
$$\begin{aligned} P_1 &= [0:1:0], \ P_2 = [1:0:0], \\ Q_+ &= [1:1:i], \ Q_- = [-1:-1:i], \\ R_+ &= [1:-1:1], \ R_- = [-1:1:1]. \end{aligned}$$
Here i denotes a square root of -1, possibly in a quadratic extension of $\mathbb{F}_q$.

The involution τ defined by $x_1 \leftrightarrow x_2$, $y_1 \leftrightarrow y_2$ acts via $a \mapsto -a$ and $b \mapsto -b$, hence the points P_k, for $k = 1, \dots, 3$, are fixed while the points with index $\pm$ are swapped. The action of Frobenius on these points is only nontrivial for $Q_\pm$, swapping these points, if -1 is not a square in $\mathbb{F}_q$, i.e., if the Jacobi-symbol $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ equals -1 (here q is odd).

In summary, we may evaluate the trace formula of Proposition 3.1 as

$$\begin{aligned}\pi(2,q;(0,1)) &= \frac{1}{4}\mathrm{tr}\big(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(U_{\bar{\mathbb{F}}_q},\mathbb{Q}_\ell)\big) = \frac{1}{4}q\cdot\mathrm{tr}\big(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(V_{\bar{\mathbb{F}}_q},\mathbb{Q}_\ell)\big)\\ &= \frac{1}{4}q\cdot\Big(\mathrm{tr}\big(\tau F|\,\mathrm{H}^*(\mathbb{P}^1_{\bar{\mathbb{F}}_q},\mathbb{Q}_\ell)\big)-\mathrm{tr}\big(\tau F|\,\mathrm{H}^*(D_{\bar{\mathbb{F}}_q},\mathbb{Q}_\ell)\big)\Big)\\ &= \frac{1}{4}q\cdot\Big(1+q-\#D_\tau(\mathbb{F}_q)\Big)\\ &= \frac{1}{4}q^2\cdot\begin{cases}1-(2-\left(\frac{-1}{q}\right))q^{-1} & q\text{ is odd},\\ 1-2q^{-1} & q\text{ is even}.\end{cases}\end{aligned} \tag{3.5}$$

4. Geometry

We keep the notation of Section 3.3 but specialize to $d=3$. Moreover, we consider variables

$$\underline{x}=(x_0,x_1,x_\infty)\quad\text{and}\quad\underline{y}=(y_0,y_1,y_\infty)$$

in order to simplify notation when dealing with symmetries. The reader is advised to consult with Figure 4.7 which provides a visualizations of the construction.

4.1. **Linear projection.** Recall that M is the $\mathbb{F}_q$-vector space spanned by $x_0,x_1,x_\infty,y_0,y_1,y_\infty,z$ subject to the relation $\sigma_1(\underline{x})=\sigma_1(\underline{y})$. We introduce the following subspaces

$$M\supseteq N\supseteq L$$

with L generated by the images of x_i-y_j for all $i,j\in\{0,1,\infty\}$ and N generated by L and the image of z. The space L has a basis a,b,c,d given by the matrix entries of

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}y_\infty-x_1 & x_\infty-y_1\\ x_0-y_1 & y_0-x_1\end{pmatrix}.$$

Lemma 4.1. *We will need the following descriptions with respect to the basis a,b,c,d:*

$$\begin{array}{lcl|lcl|lcl}
x_\infty-y_\infty &=& d-c & x_\infty-y_0 &=& a-c & x_\infty-y_1 &=& b\\
x_0-y_\infty &=& d-b & x_0-y_0 &=& a-b & x_0-y_1 &=& c\\
x_1-y_\infty &=& -a & x_1-y_0 &=& -d & x_1-y_1 &=& b+c-a-d\\
\hline
 & & & y_\infty-y_1 &=& b+c-d & y_\infty-y_0 &=& a-d\\
x_\infty-x_1 &=& a+d-c & & & & y_0-y_1 &=& b+c-a\\
x_\infty-x_0 &=& b-c & x_0-x_1 &=& a+d-b & & &
\end{array}$$

Proof. This is elementary, for example, recall that $\sigma_1(\underline{x})=\sigma_1(\underline{y})$, hence

$$x_\infty-y_\infty=y_0+y_1-x_0-x_1=d-c.$$

Moreover, the symmetry $x_i\longleftrightarrow y_i$ for $i=0,1,\infty$ translates to the involution

$$a\longleftrightarrow b\quad\text{and}\quad c\longleftrightarrow d.$$

This helps deducing other linear combinations from known ones. □

In each step of $M\supseteq N\supseteq L$ the dimension drops by 1 and the induced rational maps

$$\mathbb{P}(M)\dashrightarrow\mathbb{P}(N)\dashrightarrow\mathbb{P}(L)$$

are each defined outside one point. More precisely, let

$$\star_M=[1:1:\ldots:1:0]$$

be the point in $\mathbb{P}(M)\subseteq\mathbb{P}^6$ where all linear coordinates in N vanish, then linear projection is a geometric line bundle (Zariski-locally isomorphic to $\mathbb{P}(N)\times\mathbb{A}^1$)

$$\mathbb{P}(M)\setminus\star_M\to\mathbb{P}(N).$$

The equations for $X \subseteq \mathbb{P}(M)$ allow the following manipulations: under the assumption $\sigma_i(\underline{x}) = \sigma_i(\underline{y})$ for $i = 1, 2$ a quick calculation shows that we have

$$\begin{aligned}\sigma_3(\underline{x}) = \sigma_3(\underline{y}) + z^3 &\iff (T-y_0)(T-y_1)(T-y_\infty) = z^3 + (T-x_0)(T-x_1)(T-x_\infty)\\ &\iff (x_\infty - y_0)(x_\infty - y_1)(x_\infty - y_\infty) = z^3\\ &\iff (a-c)b(d-c) = z^3. \end{aligned} \tag{4.1}$$

Moreover we find

$$\begin{aligned}\det\begin{pmatrix} a & b\\ c & d\end{pmatrix} &= (y_\infty - x_1)(y_0 - x_1) - (x_\infty - y_1)(x_0 - y_1)\\ &= y_\infty y_0 - x_1(y_\infty + y_0) + x_1^2 - y_1^2 - x_\infty x_0 + y_1(x_\infty + x_0)\\ &= \sigma_2(\underline{y}) - \sigma_2(\underline{x}) + (x_1 + y_1)(\sigma_1(\underline{x}) - \sigma_1(\underline{y}))\\ &= \sigma_2(\underline{y}) - \sigma_2(\underline{x}).\end{aligned} \tag{4.2}$$

Hence, we define $Y \subseteq \mathbb{P}(N)$ by the equations

$$Y := V((a-c)b(d-c) = z^3,\ ad - bc = 0) \subseteq \mathbb{P}(N).$$

Proposition 4.2. *The restriction of the linear projection $\mathbb{P}(M) \dashrightarrow \mathbb{P}(N)$ to Y is a geometric line bundle*

$$\mathrm{pr}_N : X \setminus \star_M \to Y.$$

Proof. Immediately from the computations (4.1) and (4.2). □

4.2. **A torsor.** We now analyse the second linear projection $\mathrm{pr}_L : \mathbb{P}(N) \dashrightarrow \mathbb{P}(L)$, which in coordinates $[a : b : c : d : z]$ is defined outside of the point

$$\star_N = [0 : \ldots : 0 : 1].$$

Because $\star_N \notin Y$ (the cubic equation fails) the second linear projection restricts to a finite map

$$j = \mathrm{pr}_L\,|_Y : Y \to Z := V(ad - bc = 0) \subseteq \mathbb{P}(L).$$

The quadric Z is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ by the following isomorphism

$$\begin{aligned}\mathbb{P}^1 \times \mathbb{P}^1 &\xrightarrow{\sim} Z\\ ([u : v], [r : s]) &\mapsto \begin{pmatrix} a & b\\ c & d\end{pmatrix} = \begin{pmatrix} u\\ v\end{pmatrix} \cdot (r, s).\end{aligned}$$

For later use we also record the inverse map as

$$[u : v] = [a : c] = [b : d], \qquad [r : s] = [a : b] = [c : d]. \tag{4.3}$$

The map $j : Y \to Z$ has the structure of a ramified μ_3-torsor on Z defined by the equation

$$z^3 = (a-c)b(d-c).$$

The μ_3-action is given by $z \mapsto \zeta \cdot z$ for $\zeta \in \mu_3$. In the bihomogeneous coordinates $[u : v], [r : s]$ the equation for the torsor becomes

$$z^3 = (ur - vr)us(vs - vr) = uv(u - v) \cdot rs(s - r).$$

This allows to read off the branch locus as

$$S = \{0, 1, \infty\} \times \mathbb{P}^1 \cup \mathbb{P}^1 \times \{0, 1, \infty\} \subseteq \mathbb{P}^1 \times \mathbb{P}^1,$$

and that j induces an isomorphsm

$$j|_T :\ T := j^{-1}(S)_{\mathrm{red}} \xrightarrow{\sim} S. \tag{4.4}$$

of S with the reduced preimage in Y of the branch locus.

4.3. **Symmetries and automorphisms of the projective line.** We consider the symmetric group S_3 as the group of permutations of the set $\{0,1,\infty\}$. It acts naturally on variables $\underline{x}$ (homogeneous linear coordinate functions) by the right action

$$\sigma^*(x_i) = x_{\sigma^{-1}(i)} \tag{4.5}$$

and similarly for $\underline{y}$. Since we let z be fixed by S_3, we obtain induced S_3-actions on $L \subseteq N \subseteq M$ and furthermore on

$$X \setminus \star_M \to Y \to Z.$$

There is also a natural S_3-action on $\mathbb{P}^1$ by projective linear transformations permuting the subset $\{0,1,\infty\} \subseteq \mathbb{P}^1(\mathbb{F}_q)$ accordingly. For example, the 3-cycle

$$\tau = (01\infty)$$

acts on a parameter λ for $\mathbb{P}^1$ as

$$\tau^*(\lambda) = \frac{1}{1-\lambda}. \tag{4.6}$$

Since counting cubic twin prime polynomials requires control of the effect on cohomology of the 3-cycle τ, we compute its effect on geometry more explicitly in coordinates:

Lemma 4.3. *The 3-cycle $\tau = (01\infty)$ acts on X, Y and $Z = \mathbb{P}^1 \times \mathbb{P}^1$ respectively as*

$$\tau([x_0 : x_1 : x_\infty : y_0 : y_1 : y_\infty : z]) = [x_\infty : x_0 : x_1 : y_\infty : y_0 : y_1 : z], \tag{4.7}$$

$$\tau([a : b : c : d : z]) = [-c : -d : a-c : b-d : z], \tag{4.8}$$

$$\tau([u : v], [r : s]) = ([-v : u-v], [r : s]). \tag{4.9}$$

In particular τ acts on Z by $\tau \times \mathrm{id}$ for the natural action of τ on $\mathbb{P}^1$.

Proof. This follows from (4.5) and Lemma 4.1:

$$\begin{aligned}
\tau^*(a) &= \tau^*(y_\infty - x_1) = y_1 - x_0 = -c,\\
\tau^*(b) &= \tau^*(x_\infty - y_1) = x_1 - y_0 = -d,\\
\tau^*(c) &= \tau^*(x_0 - y_1) = x_\infty - y_0 = a - c,\\
\tau^*(d) &= \tau^*(y_0 - x_1) = y_\infty - x_0 = b - d.
\end{aligned}$$

For $Z \simeq \mathbb{P}^1 \times \mathbb{P}^1$ we use rational parameters, see (4.3),

$$\lambda = \frac{u}{v} = \frac{a}{c} = \frac{b}{d}, \qquad \mu = \frac{r}{s} = \frac{a}{b} = \frac{c}{d} \tag{4.10}$$

for the two factors $\mathbb{P}^1$.

$$\begin{aligned}
\lambda \mapsto \ & \frac{\tau^*(a)}{\tau^*(c)} = \frac{-c}{a-c} = \frac{-v}{u-v} = \frac{1}{1-\lambda} = \tau^*(\lambda),\\
\mu \mapsto \ & \frac{\tau^*(a)}{\tau^*(b)} = \frac{-c}{-d} = \mu.
\end{aligned}$$

□

4.4. **Enters the elliptic curve.** The cubic curve E given by the cubic equation

$$E = \{w^3 = uv(u-v)\}$$

is a branched μ_3-torsor (with $\zeta \in \mu_3$ acting by $w \mapsto \zeta w$)

$$\pi : E \to \mathbb{P}^1, \qquad \pi([u : v : w]) = [u : v].$$

The curve E is an elliptic curve unless $p = 3$ when it is rational. In any case, there are unique $\mathbb{F}_q$-rational points $P_0, P_1, P_\infty \in E(\mathbb{F}_q)$ with $\pi(P_i) = i$ for all $i \in \{0,1,\infty\}$. These points all lie on the line $w = 0$:

$$P_0 = [0 : 1 : 0], \quad P_1 = [1 : 1 : 0], \quad P_\infty = [1 : 0 : 0].$$

Proposition 4.4. *Let $p \neq 3$, and consider E as an elliptic curve with P_0 as the 0 for the group law.*

1. *P_1 and P_∞ are 3-torsion elements with $P_\infty = 2P_1$.*
2. *Translation by P_1 defines an isomorphism $\tau_E : E \to E$ of order 3*

$$\tau_E([u : v : w]) = [-v : u - v : w].$$

lifting $\tau : \mathbb{P}^1 \to \mathbb{P}^1$, the action by the 3-cycle $\tau = (01\infty)$ defined by (4.6).

(3) *The μ_3-torsor $E \to \mathbb{P}^1$ ramifies exactly in $\{P_0, P_1, P_\infty\}$, i.e., we have a finite étale covering*

$$\pi : E \setminus \{P_0, P_1, P_\infty\} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}.$$

Proof. (1) The line $w = 0$ intersects E in the divisor $P_0 + P_1 + P_\infty$, thus $P_\infty = -P_1$ with respect to the group law with $P_0 = 0$. The map $\pi : E \to \mathbb{P}^1$ is totally ramified in $0, 1, \infty$. Hence, for all $i, j \in \{0, 1, \infty\}$, the divisor $3(P_i - P_j)$ is a difference of fibres and thus linearly equivalent to 0. It follows that with respect to the group structure on E we have $3P_1 = 3P_\infty = 0$ and $P_\infty = 2P_1$.

(2) The points P_0, P_1, P_∞ are μ_3-invariant. Therefore μ_3 acts via automorphisms of E as a group and translation by P_1 commutes with the action by μ_3. Hence there is a unique commutative square

$$\begin{array}{ccc} E & \xrightarrow{\tau_E} & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow{\tilde{\tau}} & \mathbb{P}^1 \end{array}$$

Since τ_E permutes $P_0 \rightsquigarrow P_1 \rightsquigarrow P_\infty \rightsquigarrow P_0$, the induced map $\tilde{\tau}$ does likewise with $0 \rightsquigarrow 1 \rightsquigarrow \infty \rightsquigarrow 0$ and thus agrees with τ acting by (4.6) on $\mathbb{P}^1$.

We now determine the formula for τ_E. The Weierstraß-equation of the elliptic curve E has the form

$$y^2 - y = x^3$$

with $x = -w/u$ and $y = v/u$. In these coordinates $P_0 = [0 : 1 : 0]$ becomes the point at infinity. Addition with $P_1 = (0, 1)$ in xy-coordinates takes the form, see [Sil09] group law algorithm 2.3 for formulas,

$$\tau_E([u : v : w]) = \tau_E(x, y) = (-\frac{x}{y}, 1 - \frac{1}{y}) = (\frac{-w}{-v}, \frac{u - v}{-v}) = [-v : u - v : w].$$

(3) This is clear: by the Riemann-Hurwitz formula there is no ramification left. □

We now consider a second copy of E with coordinates $[r : s : t]$ and equation

$$t^3 = rs(r - s)$$

The μ_3-torsor $j : Y \to Z$ is dominated by the (branched) $\mu_3 \times \mu_3$-torsor

$$\pi \times \pi : \ Y' := E \times E \to \mathbb{P}^1 \times \mathbb{P}^1 \simeq Z$$

by means of the map $j' : Y' \to Y$ in $[a : b : c : d : z]$-coordinates

$$j'([u : v : w], [r : s : t]) = [ur : us : vr : vs : -wt]. \tag{4.11}$$

This identifies Y with the quotient by the antidiagonal μ_3-action on $Y' = E \times E$, i.e., with respect to $\zeta \in \mu_3$ acting by

$$([u : v : w], [r : s : t]) \mapsto ([u : v : \zeta w], [r : s : \zeta^{-1} t]).$$

We let τ act on $E \times E$ by

$$\tau := \tau_E \times \mathrm{id} = \Big(([u : v : w], [r : s : t]) \mapsto ([-v : u - v : w], [r : s : t])\Big).$$

Corollary 4.5. *Let $p \neq 3$. The map $j' : Y' \to Y$ is τ-equivariant.*

Proof. This follows from (4.8), (4.11) and Proposition 4.4(2). □

The reduced preimage in $Y' = E \times E$ of the branch locus is

$$T' = j'^{-1}(T)_{\mathrm{red}} = (\pi \times \pi)^{-1}(S)_{\mathrm{red}} = \{P_0, P_1, P_\infty\} \times E \cup E \times \{P_0, P_1, P_\infty\} \subseteq E \times E.$$

4.5. **The open part.** We are ultimately interested in twists of

$$U = X \setminus \{\Delta_x \cdot \Delta_y \cdot z = 0\}.$$

Because of Lemma 4.1 we set

$$V := Y \setminus V((b-c)(a+d-c)(a+d-b)(a-d)(b+c-d)(b+c-a)z = 0),$$

and immediately obtain the following corollary from Proposition 4.2.

Corollary 4.6. *The linear projection $\mathbb{P}(M) \dashrightarrow \mathbb{P}(N)$ restricts to a geometric line bundle*

$$\mathrm{pr}_N : U \to V.$$

The image of $V \subseteq Y$ in $Z \simeq \mathbb{P}^1 \times \mathbb{P}^1$ can best be described in terms of rational parameters λ and μ, see (4.10). The locus $z = 0$ is the preimage of S. The locus $\Delta_x = 0$ is given by the equation

$$0 = \Delta_x = (b-c)(a+d-c)(a+d-b) = (us-vr)(ur+vs-vr)(ur+vs-us)$$

which adds outside of S the following divisors

$$\{\mu = \lambda\}, \qquad \{\mu = \frac{1}{1-\lambda}\}, \qquad \{\mu = 1 - \frac{1}{\lambda}\}.$$

For $\Delta_y = 0$ we obtain in addition

$$\{\mu = \frac{1}{\lambda}\}, \qquad \{\mu = 1-\lambda\}, \qquad \{\mu = \frac{\lambda}{\lambda-1}\}.$$

These are the graphs

$$\Gamma_\sigma \subseteq \mathbb{P}^1 \times \mathbb{P}^1 \simeq Z$$

of all the automorphisms $\sigma : \mathbb{P}^1 \to \mathbb{P}^1$ for all $\sigma \in S_3$ with respect to the action recalled in Section 4.3. We set

$$\Gamma = \bigcup_{\sigma \in S_3} \Gamma_\sigma.$$

Now V is the preimage under $j : Y \to Z$ of the open

$$W := Z \setminus (S \cup \Gamma).$$

We furthermore set

$$H = \bigcup_{\sigma \in S_3} H_\sigma, \qquad \text{with } H_\sigma := j^{-1}(\Gamma_\sigma)_{\mathrm{red}},$$

and similarly H' and H'_σ as reduced preimages of H and H_σ under $j' : E \times E \to Y$.

Lemma 4.7. *For all $\sigma \in S_3$ we have*

$$\tau(H_\sigma) = H_{\sigma\tau^{-1}}, \quad \text{and} \quad \tau(\Gamma_\sigma) = \Gamma_{\sigma\tau^{-1}}.$$

Proof. This is a consequence of abstract nonsense on graphs. □

4.6. **Intersections of components.** For the curves $C = S, \Gamma, T, H, T'$ and H' we denote by C_0 the subvariety of points that lie in at least two components. For a point $P \in \Gamma_0 \setminus S$ we set

$$n_P := \#\{\sigma \ ; \ P \in \Gamma_\sigma\}.$$

Moreover, we set as reduced subvarieties

$$\Gamma_n = \bigcup_{P \in \Gamma_0 \setminus S,\ n_P = n} P.$$

Although the individual P might not be defined over $\mathbb{F}_q$, their union with a fixed number n_P is.

Lemma 4.8. *In rational parameters λ, μ of $Z = \mathbb{P}^1 \times \mathbb{P}^1$ we have the following description of $\bar{\mathbb{F}}_q$-rational points:*

$$\Gamma_2(\bar{\mathbb{F}}_q) = \begin{cases} \{-1, \frac{1}{2}, 2\} \times \{-1, \frac{1}{2}, 2\} & p \neq 2, 3, \\ \emptyset & p = 2, 3, \end{cases}$$

$$\Gamma_3(\bar{\mathbb{F}}_q) = \begin{cases} \{-\zeta_3, -\zeta_3^2\} \times \{-\zeta_3, -\zeta_3^2\} & p \neq 3, \\ \emptyset & p = 3, \end{cases}$$

$$\Gamma_6(\bar{\mathbb{F}}_q) = \begin{cases} \emptyset & p \neq 3, \\ \{(-1, -1)\} & p = 3. \end{cases}$$

and $\Gamma_n(\bar{\mathbb{F}}_q) = \emptyset$ for $n = 4$, 5 and $n \geq 7$.

Proof. If $P = (\lambda_0, \mu_0) \in \Gamma_\sigma \cap \Gamma_{\sigma'}$ with $\sigma \neq \sigma'$, then $\sigma'(\lambda_0) = \mu_0 = \sigma(\lambda_0)$. Hence λ_0 and therefore μ_0 are fixed points for non-trivial elements of the natural S_3 action on $\mathbb{P}^1$. The fixed points are easily listed and catalogued according to the size of the stabilizer as given in the lemma. □

In the same way we define for a point $P \in H_0 \setminus T$

$$n_P := |\{\sigma \ ; \ P \in H_\sigma\}|,$$

and set as reduced subvarieties

$$H_n = \bigcup_{P \in H_0 \setminus T, \ n_P = n} P.$$

Since $H_\sigma = j^{-1}(\Gamma_\sigma)$ we find $n_P = n_{j(P)}$ for all $P \in H_0 \setminus T$, in particular

$$H_n = j^{-1}(\Gamma_n).$$

Lemma 4.9. *Let $p \neq 3$. Then, in terms of coordinates $\xi = z/(vs), \lambda = u/v, \mu = r/s$,*

$$H_3(\bar{\mathbb{F}}_q) \simeq \{-1, -\zeta_3, -\zeta_3^2\} \times \{-\zeta_3, -\zeta_3^2\} \times \{-\zeta_3, -\zeta_3^2\}.$$

The induced action of τF on $H_3(\bar{\mathbb{F}}_q)$ has no fixed points.

Proof. The fibres above (λ, μ) with $\lambda, \mu \neq \infty$ are roots of

$$\xi^3 = \lambda(\lambda - 1) \cdot \mu(1 - \mu).$$

Evaluating for $(\lambda, \mu) \in \{-\zeta_3, -\zeta_3^2\} \times \{-\zeta_3, -\zeta_3^2\}$ results in each case in the equation

$$\xi^3 = -1,$$

hence the description of H_3 as given in the lemma.

The points $\lambda = -\zeta_3, -\zeta_3^2$ are the fixed points for τ acting on $\mathbb{P}^1$. The action on ξ is as follows:

$$\tau^*(\xi) = \frac{\tau^*(z)}{\tau^*(vs)} = \frac{z}{(u - v)s} = \xi \frac{v}{u - v} = \xi \frac{1}{\lambda - 1}.$$

For $\lambda = -\zeta_3, -\zeta_3^2$ the factor $1/(\lambda - 1)$ equals $-\lambda \in \mu_3$. If (ξ, λ, μ) is a fixed point under τF, then

$$(\xi, \lambda, \mu) = \tau F(\xi, \lambda, \mu) = \tau(\xi^q, \lambda^q, \mu^q) = (-\lambda^q \xi^q, \lambda^q, \mu^q).$$

Hence $\lambda^q = \lambda$, i.e., $\zeta_3 \in \mathbb{F}_q^\times$, hence also $\xi^q = \xi$, and therefore equating the first coordinate yields $\lambda = -1$, a contradiction. □

4.7. **Summary.** Here is a diagram summarizing the varieties and maps considered above:

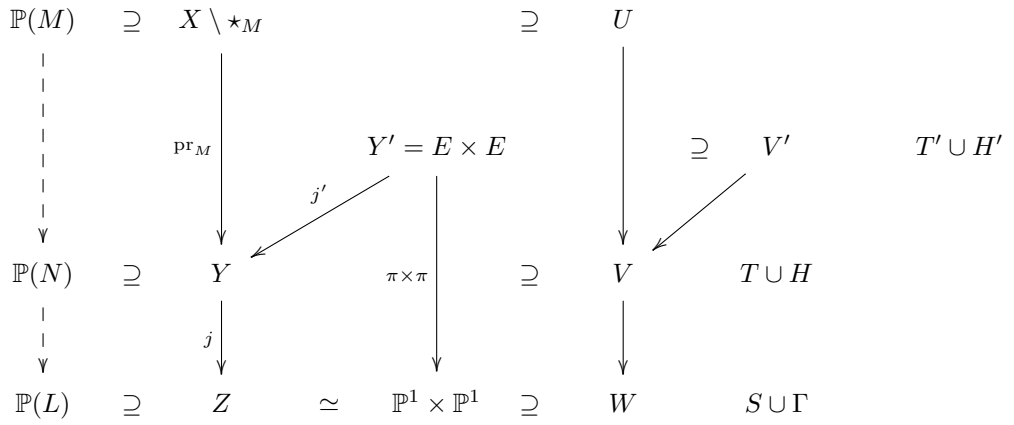

FIGURE 1. Diagram of varieties used to describe U

Note that the 3-cycle $\tau = (01\infty)$ acts in a compatible way on the diagram, including compatibility with the torsor structures.

5. COHOMOLOGY

5.1. **Cohomology with values in a Grothendieck group.** The 3-cycle $\tau = (01\infty)$ generates the alternating group $A_3 \subseteq S_3$. We consider cohomology by formally taking the alternating sum as an object in the Grothendieck group of $A_3 \times \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-representations with $\overline{\mathbb{Q}}_\ell$-coefficients: for any variety over $\mathbb{F}_q$ with A_3-action we set

$$\mathrm{H}^*_{\mathrm{c}}(-) := \sum_i (-1)^i \left[\mathrm{H}^i_{\mathrm{c}}(-_{\bar{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)\right]$$

as a virtual $A_3 \times \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-representation. Here we denote by $[-]$ the class of a representation in the Grothendieck group. Recall that the cohomology of $\mathbb{A}^1$ agrees with the inverse of the Tate twist

$$\mathrm{H}^*_{\mathrm{c}}(\mathbb{A}^1) = \left[\mathrm{H}^2_{\mathrm{c}}(\mathbb{A}^1_{\bar{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)\right] = \left[\overline{\mathbb{Q}}_\ell(-1)\right],$$

and, since the generator in degree 2 is the fundamental class, moreover has trivial τ-action.

Lemma 5.1. $\mathrm{H}^*_{\mathrm{c}}(U) = \left[\overline{\mathbb{Q}}_\ell(-1)\right] \cdot \left(\mathrm{H}^*_{\mathrm{c}}(Y) - \mathrm{H}^*_{\mathrm{c}}(S) - \mathrm{H}^*_{c}(H \setminus T)\right)$.

Proof. The constructible decomposition $V \cup (H \setminus T) \cup T = Y$ shows

$$\mathrm{H}^*_{\mathrm{c}}(V) = \mathrm{H}^*_{\mathrm{c}}(Y) - \mathrm{H}^*_{\mathrm{c}}(T) - \mathrm{H}^*_{c}(H \setminus T).$$

Since $T \simeq S$ by (4.4), we are left to prove

$$\mathrm{H}^*_{\mathrm{c}}(U) = \left[\overline{\mathbb{Q}}_\ell(-1)\right] \cdot \mathrm{H}^*_{\mathrm{c}}(V).$$

This holds more generally for any geometric line bundle and the argument is recalled for the convenience of the reader. The assertion is local with respect to a constructible decomposition of the base V. We may therefore assume that the bundle is trivial. Then the Künneth-formula yields

$$\mathrm{H}^*_{\mathrm{c}}(U) = \mathrm{H}^*_{\mathrm{c}}(\mathbb{A}^1 \times V) = \mathrm{H}^*_{\mathrm{c}}(\mathbb{A}^1) \cdot \mathrm{H}^*_{\mathrm{c}}(V) = \left[\overline{\mathbb{Q}}_\ell(-1)\right] \cdot \mathrm{H}^*_{\mathrm{c}}(V). \qquad \square$$

We denote the μ_3-invariants on cohomology for the antidiagonal μ_3-action on $E \times E$ by

$$\mathrm{H}^*_{\mathrm{c}}(E \times E)^{\mu_3} = \sum_{i=0}^{4} (-1)^i \left[\mathrm{H}^i_{\mathrm{c}}((E \times E)_{\bar{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)^{\mu_3}\right],$$

and similarly for μ_3-stable and τ-stable locally closed subvarieties defined over $\mathbb{F}_q$. Since the torsor action commutes (resp. is Galois conjugated) with the action by A_3 (resp. Galois action by $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$), we obtain a well defined object in the Grothendieck group.

Lemma 5.2. *We have the following identities:*

(1) *If $p \neq 3$, then*
$$\mathrm{H}^*_{\mathrm{c}}(Y) = \mathrm{H}^*_{\mathrm{c}}(E \times E)^{\mu_3}.$$
(2) *If $p = 3$, then*
$$\mathrm{H}^*_{\mathrm{c}}(Y) = \mathrm{H}^*_{\mathrm{c}}(\mathbb{P}^1 \times \mathbb{P}^1).$$

Proof. (1) Let $p \neq 3$. The μ_3-torsor $Y' = E \times E \to Y$ is finite étale outside the set of fixed points T_0'. (Note that having ramification only in codimension 2 is no contradiction since Y is not regular in the branch points of $j' : Y' \to Y$.) Thus pull back identifies
$$\mathrm{H}^*_{\mathrm{c}}(Y \setminus T_0) = \mathrm{H}^*_{\mathrm{c}}(E \times E \setminus T_0')^{\mu_3}.$$
We therefore have
$$\begin{aligned}\mathrm{H}^*_{\mathrm{c}}(Y) &= \mathrm{H}^*_{\mathrm{c}}(Y \setminus T_0) + \mathrm{H}^*_{\mathrm{c}}(T_0) = \mathrm{H}^*_{\mathrm{c}}(E \times E \setminus T_0')^{\mu_3} + \mathrm{H}^*_{\mathrm{c}}(T_0)\\ &= \mathrm{H}^*_{\mathrm{c}}(E \times E)^{\mu_3} - \mathrm{H}^*_{\mathrm{c}}(T_0')^{\mu_3} + \mathrm{H}^*_{\mathrm{c}}(T_0) = \mathrm{H}^*_{\mathrm{c}}(E \times E)^{\mu_3}.\end{aligned}$$
(2) Let now $p = 3$. The μ_3-torsor $Y \to Z$ is now purely inseparable and the claim follows from topological invariance of étale cohomology. □

Let us abbreviate for all $\sigma \in S_3$ the smooth part of the divisor H_σ as part of the divisor $H \cup T$ (this is actually an irreducible component, but we don't need that) by
$$H^0_\sigma := H_\sigma \setminus (T \cup H_0).$$
Similarly Γ^0_σ denotes the smooth part $\Gamma_\sigma \setminus (S \cup \Gamma_0)$ of Γ_σ as a component of $S \cup \Gamma$.

Lemma 5.3. *We have the following identities:*

(1) *If $p \neq 3$, then*
$$\mathrm{H}^*_{\mathrm{c}}(H \setminus T) = \sum_{\sigma \in S_3} \mathrm{H}^*_{\mathrm{c}}(H^0_\sigma) + \sum_{n \geq 2} \mathrm{H}^*_{\mathrm{c}}(H_n).$$
(2) *If $p = 3$, then*
$$\mathrm{H}^*_{\mathrm{c}}(H \setminus T) = \sum_{\sigma \in S_3} \mathrm{H}^*_{\mathrm{c}}(\Gamma^0_\sigma) + \sum_{n \geq 2} \mathrm{H}^*_{\mathrm{c}}(\Gamma_n).$$

Proof. (1) This is obvious from the constructible decomposition
$$H \setminus T = \bigcup_{\sigma \in S_3} H^0_\sigma \cup \bigcup_{n \geq 2} H_n.$$
Assertion (2) follows by the same argument applied to $\Gamma \setminus S$ using that $\mathrm{H}^*_{\mathrm{c}}(H \setminus T) = \mathrm{H}^*_{\mathrm{c}}(\Gamma \setminus S)$ by topological invariance of étale cohomology. □

5.2. **Cohomology of the elliptic curve.** Let $p \neq 3$. The elliptic curve $E/\mathbb{F}_q$ is the base change $E = \mathscr{E} \otimes_{\mathbb{Z}[1/3]} \mathbb{F}_q$ of the smooth integral model over $\operatorname{Spec}(\mathbb{Z}[1/3])$
$$\mathscr{E} = \{Y(Y - Z)Z = X^3\} \subseteq \mathbb{P}^2_{\mathbb{Z}[1/3]}.$$
The generic fibre $\mathscr{E}_{\mathbb{Q}}$ is an elliptic curve over $\mathbb{Q}$ with CM by $\mathbb{Z}[\zeta_3]$. First, we consider cohomology of the geometric generic fibre as $\mu_3 \subseteq \operatorname{Aut}(\mathscr{E})$-module and as $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. For this purpose we recall some CM-theory for the convenience of the reader. Complex uniformisation yields
$$\mathscr{E}(\mathbb{C}) \simeq \mathbb{C}/\mathbb{Z}[\zeta_3],$$
which follows from CM by $\mathbb{Z}[\zeta_3]$ since $\mathbb{Q}(\zeta_3)$ has class number 1, and hence all lattices with an action by $\mathbb{Z}[\zeta_3]$ are isomorphic to $\mathbb{Z}[\zeta_3]$. This computes
$$\mathbb{Z}[\zeta_3] \otimes \overline{\mathbb{Q}}_\ell \simeq \mathrm{H}^1(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$$
as μ_3-module. It follows that after fixing a faithful character $\psi : \mu_3 \hookrightarrow \overline{\mathbb{Q}}_\ell^\times$ we have 1-dimensional eigenspaces for $r = 1, 2$
$$\mathrm{H}(\psi^r) \subset \mathrm{H}^1(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$$
on which μ_3 acts by character ψ^r, and
$$\mathrm{H}^1(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) = \mathrm{H}(\psi) \oplus \mathrm{H}(\psi^2)$$

Now $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ either fixes the eigenspaces $\mathrm{H}(\psi^r)$ if $\sigma(\zeta_3) = \zeta_3$ or interchanges the summands if $\sigma(\zeta_3) = \zeta_3^{-1}$. This means that there are characters (these are the Hecke characters of Remark 2.6)

$$\alpha, \beta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3)) \to \overline{\mathbb{Q}}_\ell^\times$$

such that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3))$ acts by α on $\mathrm{H}(\psi)$ and by β on $\mathrm{H}(\psi^2)$. We rename the eigenspaces as

$$\mathrm{H}_\alpha = \mathrm{H}(\psi), \quad \text{and} \quad \overline{\mathrm{H}}_\beta = \mathrm{H}(\psi^2),$$

with the bar indicating that on this summand μ_3 acts via $\bar{\psi} = \psi^2$.

Note that if we take the inverse μ_3-action, i.e., by precomposing with $\zeta \mapsto \zeta^{-1}$, then we have

$$\mathrm{H}^1(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) = \overline{\mathrm{H}}_\alpha \oplus \mathrm{H}_\beta,$$

according to the bar-convention for indicating the character by which μ_3 acts.

Lemma 5.4. *Let μ_3 act antidiagonally on $\mathscr{E} \times \mathscr{E}$. Then*

$$\mathrm{H}^i(\mathscr{E}_{\overline{\mathbb{Q}}} \times \mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)^{\mu_3} = \begin{cases} \overline{\mathbb{Q}}_\ell & i = 0, \\ 0 & i = 1, 3, \text{ and } i \geq 5, \\ \overline{\mathbb{Q}}_\ell(-1) \oplus (H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta) \oplus \overline{\mathbb{Q}}_\ell(-1) & i = 2, \\ \overline{\mathbb{Q}}_\ell(-2) & i = 4, \end{cases}$$

as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3))$-representation.

Proof. This follows from the Künneth-formula together with the discussion above for H^1 and the well known and μ_3-invariant $\mathrm{H}^0(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell$ and $\mathrm{H}^2(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell(-1)$. □

For $p \neq 3, \ell$, the Galois representation of the geometric generic fibre

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(\mathrm{H}^1(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell))$$

is unramified in p, hence there is a well defined action of Frobenius $\rho(\mathrm{Frob}_p)$. Cospecialisation induces an isomorphism for all i

$$\mathrm{H}^i(\mathscr{E}_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) \simeq \mathrm{H}^i(E_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$$

compatible with action of Frobenius by $\rho(\mathrm{Frob}_p)^e$ and F where $q = p^e$.

Proposition 5.5. *Let $p \neq 3$, and let α, β be the eigenvalues of Frobenius $\rho(\mathrm{Frob}_p)$ on $\mathrm{H}^1(E_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$. Then we have for $q = p^e$*

$$\mathrm{tr}\big(\tau F | \, \mathrm{H}_{\mathrm{c}}^*(E \times E)^{\mu_3}\big) = (1+q)^2 + (\alpha^e + \beta^e)^2 - q(1 + \left(\frac{-3}{q}\right)).$$

Moreover, for q with $\left(\frac{-3}{q}\right) = -1$ we have $\alpha^e + \beta^e = 0$.

Proof. First, since τ acts on the abelian surface $E \times E$ by translation with $(P_1, 0)$, it is part of a connected group of endomorphisms and, by homotopy invariance, it acts as identity on cohomology. We may therefore ignore τ.

If $\left(\frac{-3}{q}\right) = -1$, then F interchanges H_α and $\overline{\mathrm{H}}_\beta$, and consequently

$$\mathrm{tr}\big(F | (H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta)\big) = 0.$$

With F also $\rho(\mathrm{Frob}_p)$ interchanges H_α and $\overline{\mathrm{H}}_\beta$, hence its trace on $\mathrm{H}^1(E_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$ vanishes and $\alpha = -\beta$. Moreover e must be odd, so that in this case

$$\alpha^e + \beta^e = 0.$$

The trace of F on the remaining cohomology, see Lemma 5.4, is easily computed as $(1+q)^2$ from which the claim follows.

If $\left(\frac{-3}{q}\right) = 1$, then F preserves the two eigenspaces and acts by a matrix

$$F \sim \begin{pmatrix} \alpha^e & \\ & \beta^e \end{pmatrix}$$

on $\mathrm{H}^1(E_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$ with wlog eigenvalue α^e on H_α and eigenvalue β on $\overline{\mathrm{H}}_\beta$. It follows that

$$\operatorname{tr}\big(F|(H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta)\big) = \alpha^{2e} + \beta^{2e}.$$

Since $\alpha\beta = p$ we find using Lemma 5.4

$$\operatorname{tr}\big(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(E \times E)^{\mu_3}\big) = (1+q)^2 + \alpha^{2e} + \beta^{2e} = (1+q)^2 + (\alpha^e + \beta^e)^2 - q(1 + \left(\frac{-3}{q}\right)). \qquad \square$$

Corollary 5.6. *Let $p \neq 3$, and let $q = p^e$. With c_q as in Theorem 1.2 we have*

$$\operatorname{tr}\big(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(E \times E)^{\mu_3}\big) = (1+q)^2 + q \cdot (c_q^2 - 1 - \left(\frac{-3}{q}\right)).$$

Moreover, for q with $\left(\frac{-3}{q}\right) = -1$ we have $c_q = 0$.

Proof. This follows immediately from Proposition 5.5 and the definition of $c_q = (\alpha^e + \beta^e)/\sqrt{q}$. $\square$

5.3. **Traces of Frobenius.** If τ permutes varieties defined over $\mathbb{F}_q$, then cohomology becomes an induced module with respect to at least the τ-action. But then τF has trace 0 on these parts. We will make use of this observation repeatedly in what follows.

Lemma 5.7. $\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(S)) = 3(1+q)$.

Proof. We compute

$$\begin{aligned}\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(S)) &= \operatorname{tr}\Big(\tau F|\sum_{i\in\{0,1,\infty\}} \mathrm{H}_{\mathrm{c}}^*(\mathbb{P}^1 \times \{i\}) + \mathrm{H}_{\mathrm{c}}^*(\{i\} \times \mathbb{P}^1)\Big) - \operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(S_0)) \\ &= 3 \cdot \operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(\mathbb{P}^1)) + \operatorname{tr}(\tau F|\, \operatorname{ind}_1^{A_3} \mathrm{H}_{\mathrm{c}}^*(\mathbb{P}^1)) - \operatorname{tr}(\tau F|\, \operatorname{ind}_1^{A_3} \mathrm{H}_{\mathrm{c}}^*(\{0,1,\infty\})) \\ &= 3 \cdot \operatorname{tr}(F|\, \mathrm{H}_{\mathrm{c}}^*(\mathbb{P}^1)) = 3(1+q),\end{aligned}$$

because τ acts trivially on cohomology of $\mathbb{P}^1$. $\square$

Lemma 5.8. *We have the following traces of Frobenius:*

(1) *If $p \neq 3$ and $n \geq 2$, then*

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H_n)) = 0.$$

(2) *If $p = 3$, then*

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(\Gamma_n)) = \begin{cases} 0 & n \neq 6, \\ 1 & n = 6. \end{cases}$$

Proof. (1) By Lemma 4.8 we have only to consider $n = 2$ and $n = 3$. By the Lefschetz trace formula, these traces of Frobenius are the τF-fixed points of $H_n(\overline{\mathbb{F}}_q)$. For $n = 3$, Lemma 4.9 shows that there are no fixed points. For $n = 2$ this is obvious because any fixed point of $H_n(\overline{\mathbb{F}}_q)$ lies over a fixed point of $\Gamma_n(\overline{\mathbb{F}}_q)$. The description of $\Gamma_2(\overline{\mathbb{F}}_q)$ shows that there are none since τ acts on Z as $\tau \times \mathrm{id}$ and thus permutes the entries $\{1/2, 2, -1\}$ in the first coordinate cyclically, see Lemma 4.3.

(2) By Lemma 4.8 we have only to consider $n = 6$. Here there is a single point which is clearly τF-invariant. $\square$

Lemma 5.9. *We have the following traces of Frobenius:*

(1) *If $p \neq 3$ and $n \geq 2$, then*

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H \setminus T)) = 0.$$

(2) *If $p = 3$, then*

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H \setminus T)) = 1.$$

Proof. The sum of cohomologies of H_σ^0 (resp. of Γ_σ^0) yields induced modules with respect to the τ action compatible with Frobenius, because τ permutes the components without fixed points, see Lemma 4.7.

(1) We can compute by Lemma 5.3(1) and Lemma 5.8(1)

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H \setminus T)) = \operatorname{tr}(\tau F|\sum_\sigma \mathrm{H}_{\mathrm{c}}^*(H_\sigma^0)) + \sum_{n\geq 2} \operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H_n)) = 0.$$

(2) Analogously, we can compute by Lemma 5.3(2) and Lemma 5.8(2)

$$\operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(H \setminus T)) = \operatorname{tr}(\tau F|\sum_\sigma \mathrm{H}_{\mathrm{c}}^*(\Gamma_\sigma^0)) + \sum_{n\geq 2} \operatorname{tr}(\tau F|\, \mathrm{H}_{\mathrm{c}}^*(\Gamma_n)) = 1. \qquad \square$$

Proposition 5.10. *We have the following traces of Frobenius:*

(1) *If $p \neq 3$, then*

$$\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(U)) = q\big(q^2 + q(c_q^2 - 2 - \left(\frac{-3}{q}\right)) - 2\big).$$

(2) *If $p = 3$, then*

$$\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(U)) = q(q^2 - q + 3).$$

Proof. By Lemma 5.1 we have in both cases

$$\begin{aligned}\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(U)) &= \operatorname{tr}(\tau F|\,\mathrm{H}_c^*(\mathbb{A}^1)) \cdot \Big(\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(Y)) - \operatorname{tr}(\tau F|\,\mathrm{H}_c^*(H \setminus T)) - \operatorname{tr}(\tau F|\,\mathrm{H}_c^*(S))\Big)\\ &= q \cdot \Big(\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(Y)) - 3(1+q) - \left\{\begin{array}{ll} 0 & p \neq 3 \\ 1 & p = 3 \end{array}\right.\Big).\end{aligned}$$

Here we also used Lemma 5.7 and Lemma 5.9.

(1) We compute further by Lemma 5.2(1) and Corollary 5.6 that

$$\begin{aligned}\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(U)) &= q\big(\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(E \times E)^{\mu_3}) - 3(1+q)\big)\\ &= q\big((1+q)^2 + q(c_q^2 - 1 - \left(\frac{-3}{q}\right)) - 3(1+q)\big)\\ &= q\big(q^2 + q(c_q^2 - 2 - \left(\frac{-3}{q}\right)) - 2\big).\end{aligned}$$

(2) We compute further by Lemma 5.2(2), that

$$\operatorname{tr}(\tau F|\,\mathrm{H}_c^*(U)) = q\big((1+q)^2 - 3(1+q) - 1\big) = q(q^2 - q - 3).$$ □

Proof of Theorem 1.2. The formula for cubic twin prime polynomial pairs now follows immediately by combining Proposition 3.1 with Proposition 5.10, and by noting

$$\left(\frac{-3}{q}\right) = \left(\frac{q}{3}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 3 \\ -1 & \text{if } q \equiv 2 \pmod 3, \end{cases}$$

by quadratic reciprocity, and $c_q = 0$ if $q \equiv 2 \pmod 3$ as in Corollary 5.6. □

5.4. **General scalar shift.** We now count prime polynomial pairs with difference $h \in \mathbb{F}_q^\times$ beyond the case $h = 1$. The corresponding parametrizing variety is the open $U_h = X_h \cap \{\Delta_x \cdot \Delta_y \cdot z \neq 0\}$ in the cubic twist

$$X_h = V\big(\sigma_2(\underline{x}) - \sigma_2(\underline{y}),\ \sigma_3(\underline{x}) - \sigma_3(\underline{y}) - hz)^3\big) \subseteq \mathbb{P}(M).$$

of the variety $X = X_1$ parametrizing prime polynomial pairs of degree 3 and shift 1. In the following, we will decorate the notation with an index h for the corresponding twisted geometric object.

The geometric description of U_h is analogous to that for U. We have a geometric line bundle $U_h \to V_h$, due to translation invariance. There is a compactification $V_h \subseteq Y_h$ and a μ_3-torsor $j_h : Y_h \to Z_h$ given in bihomogeneous coordinates $[u : v], [r : s]$ for $Z_h = Z = \mathbb{P}^1 \times \mathbb{P}^1$ by the equation

$$hz^3 = uv(u - v) \cdot rs(s - r).$$

The branch locus of the torsor j_h is still $S_h = S$.

Let $E/\mathbb{F}_q$ be the elliptic curve $\{w^3 = uv(u - v)\}$ as before, and let $ht^3 = rs(r - s)$ be the equation of its cubic twist $E_h/\mathbb{F}_q$. The arithmetic of the μ_3-cover $j' : E \times E \to Y$ necessary to compute cohomology (as virtual $A_3 \times \mathrm{Gal}_{\mathbb{F}_q}$-representation) is twisted to the torsor $j'_h : Y'_h = E \times E_h \to Y_h$ given by

$$j'_h([u : v : w], [r : s : t]) = [ur : us : vr : vs : -wt].$$

Let α, β be the eigenvalues of p-Frobenius on $\mathrm{H}^1(E_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$, and let $q = p^e$ as usual. Then there is a cube root of unity ζ, with $\zeta = 1$ if and only if h is a cube in $\mathbb{F}_q^\times$, such that

$$\zeta\alpha^e,\ q \cdot (\zeta\alpha^e)^{-1} = \zeta^2\beta^e$$

are the eigenvalues of q-Frobenius on $\mathrm{H}^1(E_{h,\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. The Lefschetz trace formula shows

$$\zeta\alpha^e + \zeta^2\beta^e = 1 + q - \#E_h(\mathbb{F}_q) =: \sqrt{q} \cdot c_{q,h},$$

with $c_q = c_{q,h}$ if h is a cube in $\mathbb{F}_q^\times$. We get that

$$\frac{\zeta\alpha^{2e} + \zeta^2\beta^{2e}}{q} = c_{q,h}\cdot c_q - (\zeta + \zeta^2) = \begin{cases} c_q^2 - 2 & \text{if } h \text{ is a cube, hence } \zeta = 1, \\ c_{q,h}\cdot c_q + 1 & \text{if } h \text{ is not a cube, hence } \zeta \neq 1. \end{cases} \tag{5.1}$$

For $q = p^e$ not divisible by 3, we will need the trace $\operatorname{tr}(\tau F | \operatorname{H}_{\mathrm{c}}^*(E \times E_h)^{\mu_3})$ which we compute as in Proposition 5.5. If $\left(\frac{-3}{q}\right) = -1$ and with the notation of loc. cit. used analogously, we have

$$\operatorname{tr}\big(F | (H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta)\big) = 0.$$

If $\left(\frac{-3}{q}\right) = 1$, we have to take into account that the second factor of $E \times E_h$ is twisted, hence the eigenvalues of Frobenius are multiplied by cubic roots of unity as explained above. We obtain

$$\operatorname{tr}\big(F | (H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta)\big) = \zeta\alpha^{2e} + \zeta^2\beta^{2e}.$$

Consequently, the analogue of Corollary 5.6 based on (5.1) is

$$\begin{aligned} \operatorname{tr}\big(\tau F | \operatorname{H}_{\mathrm{c}}^*(E_h \times E)^{\mu_3}\big) &= (1+q)^2 + \operatorname{tr}\big(F | (H_\alpha \otimes \overline{\mathrm{H}}_\alpha) \oplus (\overline{\mathrm{H}}_\beta \otimes \mathrm{H}_\beta)\big) \\ &= \begin{cases} (1+q)^2 & \text{if } \left(\frac{-3}{q}\right) = -1, \\ (1+q)^2 + q\cdot(c_q^2 - 2) & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is a cube}, \\ (1+q)^2 + q\cdot(c_{q,h}\cdot c_q + 1) & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is not a cube}. \end{cases} \end{aligned} \tag{5.2}$$

For the point counting we also need $\operatorname{tr}\big(\tau F | \operatorname{H}_{\mathrm{c}}^*(H_{3,h})\big)$ which is best computed, as in Lemma 4.9, by counting the τF-fixed points of

$$H_{3,h}(\bar{\mathbb{F}}_q) \simeq \{\xi \,;\, h\xi^3 = -1\} \times \{-\zeta_3, -\zeta_3^2\} \times \{-\zeta_3, -\zeta_3^2\}.$$

Here F acts as q-Frobenius, and τ fixes the second and third component, while in the first component we have (for $\lambda = -\zeta_3, -\zeta_3^2$ the factor $1/(\lambda - 1)$ equals $-\lambda \in \mu_3$)

$$\tau^*(\xi) = \xi\frac{1}{\lambda - 1} = -\lambda\xi.$$

Therefore $(\xi, \lambda, \mu) \in H_{3,h}(\bar{\mathbb{F}}_q)$ is fixed by τF if and only if

$$(\xi, \lambda, \mu) = \tau F(\xi, \lambda, \mu) = \tau(\xi^q, \lambda^q, \mu^q) = (-\lambda^q\xi^q, \lambda^q, \mu^q).$$

If τF-fixed points in $H_{3,h}(\bar{\mathbb{F}}_q)$ exist, we must have $\lambda^q = \lambda$, i.e., ζ_3 is fixed under q-Frobenius. That means $\zeta_3 \in \mathbb{F}_q^\times$ and furthermore $1 = \left(\frac{-3}{q}\right)$. In this case, the tuple (ξ, λ, μ) is a fixed point if and only if

$$\xi/F(\xi) = -\lambda.$$

Since $h\xi^3 = -1$, this happens if and only if h is not a cube in $\mathbb{F}_q^\times$. In that case we have three values of ξ, each determines a unique suitable value for λ, and μ can be arbitrary in $\{-\zeta_3, -\zeta_3^2\}$. This shows:

$$\operatorname{tr}\big(\tau F | \operatorname{H}_{\mathrm{c}}^*(H_{3,h})\big) = \begin{cases} 0 & \text{if } \left(\frac{-3}{q}\right) = -1, \\ 0 & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is a cube}, \\ 6 & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is not a cube}. \end{cases} \tag{5.3}$$

Proof of Theorem 1.4. For $3 \mid q$, twisting U to U_h has no effect on the point count because the relevant μ_3-torsor is purely inseparable. So in this case the formula follows from Theorem 1.2.

For $3 \nmid q$, we compute as in the proof of Theorem 1.2 and of Proposition 5.10 based on (5.2) and (5.3)

$$\begin{aligned}\pi(3,q;(0,h)) &= \frac{1}{9}\mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(U_h)) = \frac{q}{9}\cdot\Big(\mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(Y_h)) - \mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(H_h\setminus T_h)) - \mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(S))\Big)\\ &= \frac{q}{9}\cdot\Big(\mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(E_h\times E)^{\mu_3}) - \mathrm{tr}(\tau F|\,\mathrm{H}_{\mathrm{c}}^*(H_{3,h})) - 3(1+q)\Big)\\ &= \frac{q}{9}\cdot\begin{cases} q^2-q-2 & \text{if } \left(\frac{-3}{q}\right) = -1,\\ q^2+q\cdot(c_q^2-3)-2 & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is a cube},\\ q^2+q\cdot c_{q,h}\cdot c_q - 8 & \text{if } \left(\frac{-3}{q}\right) = 1 \text{ and } h \text{ is not a cube}.\end{cases}\end{aligned}$$

□

References

[ABR15] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, *Shifted convolution and the Titchmarsh divisor problem over $F_q[t]$*, Philos. Trans. A 373 (2015), no. 2040, 20140308, 18 pp.

[BaB15] E. Bank and L. Bary-Soroker, *Prime polynomial values of linear functions in short intervals*, J. Number Theory **151** (2015), 263-275.

[Bar12] L. Bary-Soroker, *Hardy-Littlewood tuple conjecture over large finite fields*, Int. Math. Res. Not. (2014), no. 2, 568–575.

[BSF18] L. Bary-Soroker and A. Fehm, *Correlations of sums of two squares and other arithmetic functions in function fields*, preprint 2017, arXiv:1701.04092, to appear.

[BeP09] A. O. Bender, P. Pollack, *On quantitative analogues of the Goldbach and twin prime conjectures over $F_q[t]$*, preprint 2009, arXiv:0912.1702.

[Bru19] V. Brun, *La série $1/5+1/7+1/11+1/13+1/17+1/19+1/29+1/31+1/41+1/43+1/59+1/61+\cdots$, où les dénominateurs sont nombres premiers jumeaux est convergente ou finie*, Bulletin des Sciences Mathematiques. 43: 100–104, 124–128, (1919).

[Car15] D. Carmon, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic 2*, Phil. Trans. R. Soc. A (2015) 373 20140315.

[Cas15] A. Castillo, Ch. Hall, R. J. Lemke Oliver, P. Pollack, and L. Thompson, *Bounded gaps between primes in number fields and function fields*, Proceedings of the AMS 143 (2015), no. 7, 2841–2856.

[Che66] J. R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Kexue Tongbao **11** (1966), no. 9, 385–386.

[Deu53] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins I-III*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. **1953** (1953), 85–94, **1955** (1955), 13–42, **1956** (1956), 37–76.

[Ent14] A. Entin, *On the Bateman-Horn conjecture for polynomials over large finite fields*, Compositio Mathematica **152** (2016), no. 12, 2525–2544.

[FK88] E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjecture*, Springer 1988, xviii+320 pp.

[GS18] O. Gorodetsky and W. Sawin, work in progress.

[Gra15] A. Granville, *Primes in intervals of bounded length*, Bulletin of the AMS **52** (2015), 171–222.

[GrT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), no. 2, 481–547.

[GTZ12] B. Green, T. Tao, and T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Annals of Mathematics **176** (2012), no. 2, 1231–1372.

[Hal06] Ch. Hall, *L-functions of twisted Legendre curves*, Journal of Number Theory **119** (2006), no. 1, 128–147.

[HL23] G. H. Hardy, J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.

[Hec18] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. **1** (1918), no. 4, 357–376; *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. **6** (1920), no. 1-2, 11–51.

[Kat12a] N. M. Katz, *On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor*, Int. Math. Res. Not. (2013), no. 14, 3221–3249.

[Kat12b] N. M. Katz, *Witt vectors and a question of Keating and Rudnick*, Int. Math. Res. Not. (2013), no. 16, 3613–3638.

[KeR14] J. P. Keating and Z. Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes*, Int. Math. Res. Not. (2014), no. 1, 259–288.

[KRG16] J. P. Keating, and E. Roditty-Gershon, *Arithmetic Correlations Over Large Finite Fields*, Int. Math. Res. Not. (2016), 860–874.

[LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2017, [Online; accessed 28 September 2017].

[May15] J. Maynard, *Small Gaps Between Primes*, Annals of Mathematics (2), **181** (2015), 383–413.

[Pol08] P. Pollack, *An explicit approach to Hypothesis H for polynomials over finite fields*, in: Anatomy of integers. Proceedings of a conference on the anatomy of integers, Montreal, March 13th-17th, 2006, J.-M. De Koninck, A. Granville, F. Luca, eds., CRM Proceedings and Lecture Notes, vol. 46, 2008, pp. 47–64.

[Pol14] D. H. J. Polymath, *New equidistribution estimates of Zhang type*, Algebra & Number Theory, **8** (2014), no. 9, 2067–2199.

[Ser73] J.-P. Serre, *A Course in Arithmetic*, Springer GTM **7**, Springer 1973, viii+115 pp.

[Sil09] J. H. Silverman, The arithmetic of ellitpic curves, Springer GTM **106**, 2nd edition, Springer 2009, xx+513 pp.
[Sk01] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press 2001, viii+187 pp.
[Su17] A. V. Sutherland, *Sato-Tate distributions*, preprint 2017, arXiv:1604.01256v4, 45 pp.
[Zha14] Y. Zhang, *Bounded gaps between primes*, Annals of Mathematics **179** (2014), no. 3, 1121–1174.

Lior Bary-Soroker, School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 6997801, Israel
E-mail address: barylior@post.tau.ac.il

Jakob Stix, Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Strasse 6–8, 60325 Frankfurt am Main, Germany
E-mail address: stix@math.uni-frankfurt.de