Canad. J. Math. Vol. 71 (6), 2019 pp. 1323–1350
http://dx.doi.org/10.4153/CJM-2018-018-9
©Canadian Mathematical Society 2018

Cubic Twin Prime Polynomials are Counted by a Modular Form

Lior Bary-Soroker and Jakob Stix

Abstract. We present the geometry 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 become 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 can easily state a general conjecture for k-tuples of the form $n + h_i$ for a fixed set of shifts $h_1 < h_2 < \cdots < h_k$. Applications often necessitate a quantitative version of the twin prime conjecture. Hardy and Littlewood made a precise quantitative conjecture in [HL23, §5 Theorem X_1][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 (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

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

Received by the editors November 22, 2017.
Published electronically December 3, 2018.
The authors acknowledge support provided by DAAD-Programm 57271540 Strategische Partnerschaften (supported by BMBF). The first author was partially supported by a grant from the Israel Science Foundation.
AMS subject classification: 11T55, 11G25.
Keywords: twin primes, finite field, polynomial.

[1] This is actually not a theorem but a consequence of Hypothesis X of [HL23].

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 $\mathfrak{S}(h)$ can be shown to converge to a positive constant.

There have been 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] tackled 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 Polymath [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 for the Hardy–Littlewood prime tuple conjecture by studying its function field analog. For a finite field $\mathbb{F}_q$ we take the set $M_{d,q} = \{f(T) \in \mathbb{F}_q[T]\ ;\ \text{monic of } \deg(f) = d\}$ 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] extended Hall's result, for sufficiently large fixed q, to any d in an explicit arithmetic progression and gave a lower bound on the number of pairs of the right order of magnitude. However, this 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; see Bender and Pollack [BeP09] for pairs in odd characteristic, the first author [Bar12] for general tuples in odd characteristic. Carmon [Car15] applied the method of the first author in even characteristic and established the following for all cases in the limit $q \to \infty$, with error term $E(d, q; h) \ll_{d,k} q^{-1/2}$:

$$\pi(d, q; h) = \tfrac{q^d}{d^k} \mathfrak{S}_q(h)(1 + E(d, q; h)). \tag{1.2}$$

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 cancellation, 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 (1.2) on average [KRG16], based on variance computations [KeR14] and equidistribution results by Katz [Kat12a, Kat12b]. See [HM17] for a geometric interpretation of [KeR14]. The asymptotic formula (1.2) has inspired more work; see [ABR15, BaB15, BSF18, Ent14]. The downside of (1.2), 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 straightforward, 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 (3.3):

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

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 $\mathcal{E}$ with Weierstraß-equation

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

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

$$|q + 1 - \#\mathcal{E}(\mathbb{F}_q)| \le 2\sqrt{q}. \tag{1.3}$$

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

$$\pi(3,q;(0,1)) = \frac{1}{9}q^3 \cdot \begin{cases} 1 - q^{-1} - 3q^{-2} & \textit{if } q \equiv 0 \pmod 3, \\ 1 + (c_q^2 - 3) \cdot q^{-1} - 2q^{-2} & \textit{if } q \equiv 1 \pmod 3, \\ 1 - q^{-1} - 2q^{-2} & \textit{if } q \equiv 2 \pmod 3, \end{cases} \tag{1.4}$$

where $c_q := \frac{1+q-\#\mathcal{E}(\mathbb{F}_q))}{\sqrt{q}}$, so that $0 \le c_q^2 \le 4$ by (1.3).

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

Remark 1.3 Since every elliptic curve over $\mathbb{Q}$ is modular, there is a newform $f_{\mathcal{E}}(q)$ associated with the elliptic curve $\mathcal{E}$ with Weierstraß-equation $X^3 = Y(Y-1)$. The

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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, due to the relations among the various Hecke operators, 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 $m \geq 1$; 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 (1.3). 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*

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

On average 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 have 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 in pursuing 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 Section 4. ■

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 where $d = 3$ 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.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 $\mathbb{F}_q(T)$,

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

as the value of a convergent power series $S(u) \in \mathbb{Q}[[u]]$ in $u = q^{-1}$. Here $S(u)$ will 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 follow, 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:

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

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.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 Lemmas 2.1 and 2.2.

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

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

■

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

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

The factor $\exp(\sum_{d\geq 2}P_d(u)\cdot\lambda(u^d))$ converges for $u < 1/\sqrt{2}$, and the middle factor can be dealt with at $u = 1/2$ by Abel's theorem on 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

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

Concretely, using SageMath, we obtain

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

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 greater than d do not influence $S_d(u)$. Moreover, in order to take into account 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 $(q^d/d^2)\cdot S_{d-1}(q^{-1})$:

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 (1.4) is consistent with square root cancellation in (1.2). When $q\equiv 1 \pmod 3$, the coefficient of q^{-1} varies with q. We will now argue that at least on average 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, Hecke [Hec18] already 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 $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Let $X_0/\mathbb{F}_q$ be a variety and denote by $X = X_0\times_{\mathbb{F}_q}\overline{\mathbb{F}}_q$, or by the usual notation, $X_{0,\overline{\mathbb{F}}_q}$, the base change to $\overline{\mathbb{F}}_q$. The $\overline{\mathbb{F}}_q$-linear geometric q-Frobenius map $F\colon X\to X$ 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,

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

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

$$\text{(3.1)}\qquad \#X_0(\mathbb{F}_q) = \mathrm{tr}\big(F|\,\mathrm{H}_c^*(X,\mathbb{Q}_\ell)\big) := \sum_{i=0}^{2\dim X}(-1)^i\mathrm{tr}\big(F|\,\mathrm{H}_c^i(X,\mathbb{Q}_\ell)\big).$$

For background on étale cohomology and a proof of the Lefschetz trace formula, we refer the reader 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 $\sigma \mapsto a_\sigma$

$$a\colon \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow \operatorname{Aut}(X/\overline{\mathbb{F}}_q)$$

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

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

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 $\varphi \in \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ 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

$$X_a(\mathbb{F}_q) = \bigl\{x \in X(\overline{\mathbb{F}}_q)\,;\, F_a(x) = x\bigr\} = \bigl\{x \in X(\overline{\mathbb{F}}_q)\,;\, F(x) = \alpha^{-1}(x)\bigr\} \tag{3.2}$$

and counted as

$$\# X_a(\mathbb{F}_q) = \operatorname{tr}\bigl(\alpha F | \operatorname{H}^*_c(X, \mathbb{Q}_\ell)\bigr).$$

3.2 Twisting Varieties of Polynomials

Monic polynomials of degree d:

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

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 $s\colon \mathbb{A}^d \to \mathbb{A}^d$,

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

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

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

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

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

that is the locus of polynomials with multiple roots.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

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

As described in (3.2), rational points of the twist are those points $\underline{x} = (x_1, \ldots, x_d)$ in $\mathbb{A}^d(\overline{\mathbb{F}}_q)$ invariant under the twisted Frobenius (with indices considered modulo d):

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

Being S_d-invariant, the cover s becomes a cover $s_\tau \colon (\mathbb{A}^d)_\tau \to \mathbb{A}^d$. 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

$$s_\tau \colon (\mathbb{A}^d)_\tau(\mathbb{F}_q) \longrightarrow \mathbb{A}^d(\mathbb{F}_q)$$

has d preimages, because each preimage in $(\mathbb{A}^d)_\tau(\mathbb{F}_q)$ is determined by its $x_1 \in \overline{\mathbb{F}}_q$, 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 $V(\sigma_1(\underline{x}) = \sigma_1(\underline{y}))$ in $\mathbb{P}^{2d}$, the projective space with homogeneous coordinates

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

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 $[\underline{x} \colon \underline{y} \colon 1]$ to the pair of polynomials

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

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

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

[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.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

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

Therefore, we have proved the following proposition as a consequence of (3.1). Recall that we denote by $U_{\overline{\mathbb{F}}_q}$ the base change $U \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$.

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

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

We are left with the task of understanding $\mathrm{H}^*_c(U_{\overline{\mathbb{F}}_q},\mathbb{Q}_\ell)$ as an $S_d \times \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-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 Section 4. The variety X is given in $\mathbb{P}^4$ by the equations

$$\begin{aligned} x_1 + x_2 &= y_1 + y_2,\\ x_1x_2 &= y_1y_2 - z^2. \end{aligned}$$

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

$$a + b = c \quad\text{and}\quad ab = -z^2,$$

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

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

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
$$P_1 = [0{:}1{:}0], \quad P_2 = [1{:}0{:}0], \qquad P_3 = [1{:}1{:}1].$$
- 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 $\mathbb{F}_q$.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 ± 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 can evaluate the trace formula of Proposition 3.1 as

$$\begin{aligned}(3.3)\quad \pi(2,q;(0,1)) &= \frac{1}{4}\operatorname{tr}\big(\tau F|\mathrm{H}^*_{\mathrm{c}}(U_{\overline{\mathbb{F}}_q},\mathbb{Q}_\ell)\big) = \frac{1}{4}q\cdot\operatorname{tr}\big(\tau F|\mathrm{H}^*_{\mathrm{c}}(V_{\overline{\mathbb{F}}_q},\mathbb{Q}_\ell)\big)\\ &= \frac{1}{4}q\cdot\Big(\operatorname{tr}\big(\tau F|\mathrm{H}^*(\mathbb{P}^1_{\overline{\mathbb{F}}_q},\mathbb{Q}_\ell)\big) - \operatorname{tr}\big(\tau F|\mathrm{H}^*(D_{\overline{\mathbb{F}}_q},\mathbb{Q}_\ell)\big)\Big)\\ &= \frac{1}{4}q\cdot\Big(1+q-\#D_\tau(\mathbb{F}_q)\Big)\\ &= \frac{1}{4}q^2\cdot\begin{cases}1-(2-\left(\frac{-1}{q}\right))q^{-1} & \text{if } q \text{ is odd,}\\ 1-2q^{-1} & \text{if } q \text{ is even.}\end{cases}\end{aligned}$$

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 Figure 4.7, which provides a visualization 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 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:*

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

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

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

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

Moreover, the symmetry $x_i \leftrightarrow y_i$ 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

$$\star_M = [1{:}1{:}\cdots{:}1{:}0]$$

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 $\mathbb{P}(N) \times \mathbb{A}^1$),

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

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

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

Moreover, we find

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

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

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

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

$$\mathrm{pr}_N \colon X \smallsetminus \star_M \longrightarrow Y.$$

Proof This is immediate from computations (4.1) and (4.2). ■

4.2 A Torsor

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

$$\star_N = [0{:}\cdots{:}0{:}1].$$

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 isomorphism

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

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 us 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 isomorphism

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

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

$$X \smallsetminus \star_M \longrightarrow Y \longrightarrow Z.$$

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.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

$$\begin{aligned} \tau\big([x_0:x_1:x_\infty:y_0:y_1:y_\infty:z]\big) &= [x_\infty:x_0:x_1:y_\infty:y_0:y_1:z], \\ \tau\big([a:b:c:d:z]\big) &= [-c:-d:a-c:b-d:z], \\ \tau\big([u:v],[r:s]\big) &= \big([-v:u-v],[r:s]\big). \end{aligned} \tag{4.7}$$

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)),

$$\lambda = \frac{u}{v} = \frac{a}{c} = \frac{b}{d}, \qquad \mu = \frac{r}{s} = \frac{a}{b} = \frac{c}{d} \tag{4.8}$$

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

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

■

4.4 Enter 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 $w \mapsto \zeta w$)

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

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.*

(i) P_1 *and* P_∞ *are* 3*-torsion elements with* $P_\infty = 2P_1$.

(ii) *Translation by* P_1 *defines an isomorphism* $\tau_E\colon E \to E$ *of order* 3*:*

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

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

(iii) *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*

$$\pi\colon E \smallsetminus \{P_0, P_1, P_\infty\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,\infty\}.$$

Proof (i) 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 $\pi\colon E \to \mathbb{P}^1$ 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 $P_\infty = 2P_1$.

(ii) 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

$$\begin{tikzcd}
E \arrow[r, "\tau_E"] \arrow[d, "\pi"] & E \arrow[d, "\pi"] \\
\mathbb{P}^1 \arrow[r, dotted, "\tilde{\tau}"] & \mathbb{P}^1
\end{tikzcd}$$

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)

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

(iii) 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 $j\colon Y \to Z$ is dominated by the (branched) $\mu_3 \times \mu_3$-torsor

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

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

$$j'([u{:}v{:}w],[r{:}s{:}t]) = [ur{:}us{:}vr{:}vs{:}-wt]. \tag{4.9}$$

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

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

We let τ act on $E \times E$ by

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

Proof This follows from (4.7), (4.9), and Proposition 4.4((ii)). ∎

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

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

Because of Lemma 4.1, we set

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

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 $\mathrm{pr}_N \colon U \to V$.*

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 (4.8). 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 the following divisors outside of S:

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

In addition, for $\Delta_y = 0$ we obtain

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

These are the graphs $\Gamma_\sigma \subseteq \mathbb{P}^1 \times \mathbb{P}^1 \simeq Z$ of all the automorphisms $\sigma \colon \mathbb{P}^1 \to \mathbb{P}^1$ 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 $j \colon Y \to Z$ of the open $W := Z \smallsetminus (S \cup \Gamma)$. 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 $j' \colon E \times E \to Y$.

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

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

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 $P \in \Gamma_0 \smallsetminus S$, we set

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

Moreover, we set as reduced subvarieties

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

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 $\overline{\mathbb{F}}_q$-rational points:*

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

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

$$\Gamma_6(\overline{\mathbb{F}}_q) = \begin{cases} \varnothing & \textit{for } p \neq 3, \\ \{(-1, -1)\} & \textit{for } p = 3, \end{cases}$$

and $\Gamma_n(\overline{\mathbb{F}}_q) = \varnothing$ 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 $n_P := |\{\sigma\ ;\ P \in H_\sigma\}|$ for a point $P \in H_0 \smallsetminus T$ and set as reduced subvarieties

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

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

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

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

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

The induced action of τF on $H_3(\overline{\mathbb{F}}_q)$ 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.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

$$\begin{tikzcd}
\mathbb{P}(M) \arrow[dd, dashed] & \supseteq & X \smallsetminus \star_M \arrow[dd, "\mathrm{pr}_M"'] & & & \supseteq & U \arrow[dd] & & & \\
& & & & Y' = E \times E \arrow[dll, "j'"'] \arrow[dd, "\pi\times\pi"'] & & & \supseteq & V' \arrow[dll] & T' \cup H' \\
\mathbb{P}(N) \arrow[d, dashed] & \supseteq & Y \arrow[d, "j"'] & & & \supseteq & V \arrow[d] & & T \cup H & \\
\mathbb{P}(L) & \supseteq & Z & \simeq & \mathbb{P}^1 \times \mathbb{P}^1 & \supseteq & W & & S \cup \Gamma &
\end{tikzcd}$$

Figure 1: Diagram of varieties used to describe U.

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 $A_3 \times \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-representations with $\overline{\mathbb{Q}}_\ell$-coefficients: for any variety over $\mathbb{F}_q$ with A_3-action, we set

$$\mathrm{H}_c^*(-) := \sum_i (-1)^i \big[\, \mathrm{H}_c^i(-_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)\big]$$

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

with the inverse of the Tate twist

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

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

Lemma 5.1 $\mathrm{H}_c^*(U) = \big[\overline{\mathbb{Q}}_\ell(-1)\big] \cdot \big(\,\mathrm{H}_c^*(Y) - \mathrm{H}_c^*(S) - \mathrm{H}_c^*(H \smallsetminus T)\big).$

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

$$\mathrm{H}_c^*(V) = \mathrm{H}_c^*(Y) - \mathrm{H}_c^*(T) - \mathrm{H}_c^*(H \smallsetminus T).$$

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

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

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 can therefore assume that the bundle is trivial. Then the Künneth formula yields

$$\mathrm{H}_c^*(U) = \mathrm{H}_c^*(\mathbb{A}^1 \times V) = \mathrm{H}_c^*(\mathbb{A}^1) \cdot \mathrm{H}_c^*(V) = \big[\overline{\mathbb{Q}}_\ell(-1)\big] \cdot \mathrm{H}_c^*(V). \qquad \blacksquare$$

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

$$\mathrm{H}_c^*(E \times E)^{\mu_3} = \sum_{i=0}^{4} (-1)^i \Big[\,\mathrm{H}_c^i\big((E \times E)_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell\big)^{\mu_3}\Big],$$

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 $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$), we obtain a well defined object in the Grothendieck group.

Lemma 5.2 *We have the following identities:*

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

Proof (i) 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 $j' \colon Y' \to Y$.) Thus, pullback identifies $\mathrm{H}_c^*(Y \smallsetminus T_0)$ and $\mathrm{H}_c^*(E \times E \smallsetminus T_0')^{\mu_3}$. We therefore have

$$\begin{aligned}\mathrm{H}_c^*(Y) &= \mathrm{H}_c^*(Y \smallsetminus T_0) + \mathrm{H}_c^*(T_0) = \mathrm{H}_c^*(E \times E \smallsetminus T_0')^{\mu_3} + \mathrm{H}_c^*(T_0)\\ &= \mathrm{H}_c^*(E \times E)^{\mu_3} - \mathrm{H}_c^*(T_0')^{\mu_3} + \mathrm{H}_c^*(T_0) = \mathrm{H}_c^*(E \times E)^{\mu_3}.\end{aligned}$$

(ii) Let $p = 3$. The μ_3-torsor $Y \to Z$ is now purely inseparable, and the claim follows from topological invariance of étale cohomology. $\blacksquare$

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

$$H_\sigma^0 := H_\sigma \smallsetminus (T \cup H_0).$$

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

Similarly, Γ_σ^0 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:*

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

$$\mathrm{H}_c^*(H \setminus T) = \sum_{\sigma \in S_3} \mathrm{H}_c^*(H_\sigma^0) + \sum_{n \geq 2} \mathrm{H}_c^*(H_n).$$

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

$$\mathrm{H}_c^*(H \setminus T) = \sum_{\sigma \in S_3} \mathrm{H}_c^*(\Gamma_\sigma^0) + \sum_{n \geq 2} \mathrm{H}_c^*(\Gamma_n).$$

Proof (i) This is obvious from the constructible decomposition

$$H \setminus T = \bigcup_{\sigma \in S_3} H_\sigma^0 \cup \bigcup_{n \geq 2} H_n.$$

Assertion (ii) follows by the same argument applied to $\Gamma \setminus S$ using that $\mathrm{H}_c^*(H \setminus T) = \mathrm{H}_c^*(\Gamma \setminus S)$ 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 $E = \mathscr{E} \otimes_{\mathbb{Z}[1/3]} \otimes \mathbb{F}_q$ 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 $\psi\colon \mu_3 \hookrightarrow \overline{\mathbb{Q}}_\ell^\times$, 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 $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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)

$$\alpha, \beta\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3)) \longrightarrow \overline{\mathbb{Q}}_\ell^\times$$

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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 $\overline{\psi} = \psi^2$.

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*

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

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

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

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 $q = p^e$,*

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

Moreover, for q with $\Big(\frac{-3}{q}\Big) = -1$, 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 $\Big(\frac{-3}{q}\Big) = -1$, then F interchanges H_α and $\overline{\mathrm{H}}_\beta$, and consequently

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

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 $\mathrm{H}^1(E_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$ that ,without loss of generality, has eigenvalue α^e on H_α and eigenvalue β^e on $\overline{\mathrm{H}}_\beta$. It follows that

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

Since $\alpha\beta = p$, we find the following using Lemma 5.4:

$$\mathrm{tr}\Big(\tau F|\, \mathrm{H}_c^*(E\times E)^{\mu_3}\Big) = (1+q)^2 + \alpha^{2e} + \beta^{2e} = (1+q)^2 + (\alpha^e + \beta^e)^2 - q\Big(1 + \left(\tfrac{-3}{q}\right)\Big). \blacksquare$$

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

$$\mathrm{tr}\Big(\tau F|\, \mathrm{H}_c^*(E\times E)^{\mu_3}\Big) = (1+q)^2 + q\cdot\Big(c_q^2 - 1 - \left(\tfrac{-3}{q}\right)\Big).$$

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 $c_q = (\alpha^e + \beta^e)/\sqrt{q}$. ■

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 $\mathrm{tr}(\tau F|\, \mathrm{H}_c^*(S)) = 3(1+q)$.

Proof We compute

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

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

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

(i) *If $p \neq 3$ and $n \geq 2$, then* $\mathrm{tr}(\tau F|\, \mathrm{H}_c^*(H_n)) = 0$.

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

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

Proof (i) 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.

(ii) By Lemma 4.8 we have only to consider $n = 6$. Here there is a single point that is clearly τF-invariant. ∎

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

(i) *If* $p \neq 3$ *and* $n \geq 2$, *then* $\operatorname{tr}(\tau F|\,\mathrm{H}^*_c(H \smallsetminus T)) = 0$.
(ii) *If* $p = 3$, *then* $\operatorname{tr}(\tau F|\,\mathrm{H}^*_c(H \smallsetminus T)) = 1$.

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

(i) We can compute by Lemma 5.3((i)) and Lemma 5.8((i)):

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

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

$$\operatorname{tr}\big(\tau F|\,\mathrm{H}^*_c(H \smallsetminus T)\big) = \operatorname{tr}\Big(\tau F|\sum_\sigma \mathrm{H}^*_c(\Gamma^0_\sigma)\Big) + \sum_{n\geq 2} \operatorname{tr}\big(\tau F|\,\mathrm{H}^*_c(\Gamma_n)\big) = 1. \quad ∎$$

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

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

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

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

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

Proof By Lemma 5.1 we have in both cases

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

Here we also used Lemmas 5.7 and 5.9.

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

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

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

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

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

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

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 of 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 $j_h\colon Y_h \to Z_h$ 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 $j'\colon E\times E \to Y$ necessary to compute cohomology (as virtual $A_3 \times \mathrm{Gal}_{\mathbb{F}_q}$-representation) is twisted to the torsor $j'_h\colon Y'_h = E \times E_h \to Y_h$ given by

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

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

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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

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

For $q=p^e$ not divisible by 3, we will need the trace $\operatorname{tr}(\tau F|\mathrm{H}_c^*(E\times E_h)^{\mu_3})$, 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

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

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

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

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, $(\xi,\lambda,\mu)\in H_{3,h}(\overline{\mathbb{F}}_q)$ 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 $H_{3,h}(\overline{\mathbb{F}}_q)$ 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

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

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press

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:

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

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 proofs of Theorem 1.2 and of Proposition 5.10 based on (5.2) and (5.3):

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

References

[ABR15] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, *Shifted convolution and the Titchmarsh divisor problem over $F_q[t]$*. Philos. Trans. Roy. Soc. A **373**(2015), no. 2040, 20140308, 18 pp. http://dx.doi.org/10.1098/rsta.2014.0308

[BaB15] E. Bank and L. Bary-Soroker, *Prime polynomial values of linear functions in short intervals*. J. Number Theory **151**(2015), 263–275. http://dx.doi.org/10.1016/j.jnt.2014.12.016

[Bar12] L. Bary-Soroker, *Hardy–Littlewood tuple conjecture over large finite fields*. Int. Math. Res. Not. **2014**, no. 2, 568–575. http://dx.doi.org/10.1093/imrn/rns249

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

[BeP09] A. O. Bender and P. Pollack, *On quantitative analogues of the Goldbach and twin prime conjectures over $F_q[t]$*. 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 Mathématiques, **43**(1919), 100–104, 124–128.

[Car15] D. Carmon, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic 2*. Philos. Trans. Roy. Soc. A **373**(2015), 20140315, 14 pp. http://dx.doi.org/10.1098/rsta.2014.0311

[Cas15] A. Castillo, Ch. Hall, R. J. Lemke Oliver, P. Pollack, and L. Thompson, *Bounded gaps between primes in number fields and function fields*. Proc. Amer. Math. Soc. 143(2015), no. 7, 2841–2856. http://dx.doi.org/10.1090/S0002-9939-2015-12554-3

[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. Math.-Phys.-Chem. **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*. Compos. Math. **152**(2016), no. 12, 2525–2544. http://dx.doi.org/10.1112/S0010437X16007570

[FK88] E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjecture*. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3, Springer-Verlag, Berlin, 1988. http://dx.doi.org/10.1007/978-3-662-02541-3

[Gra15] A. Granville, *Primes in intervals of bounded length*. Bulletin of the AMS **52**(2015), 171–222. http://dx.doi.org/10.1090/S0273-0979-2015-01480-1

[GrT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math. **167**(2008), no. 2, 481–547. http://dx.doi.org/10.4007/annals.2008.167.481

[GTZ12] B. Green, T. Tao, and T. Ziegler, *An inverse theorem for the Gowers* $U^{s+1}[N]$*-norm*. Ann. of Math. **176**(2012), no. 2, 1231–1372. http://dx.doi.org/10.4007/annals.2012.176.2.11

[Hal06] C. Hall, *L-functions of twisted Legendre curves*. J. Number Theory **119**(2006), no. 1, 128–147. http://dx.doi.org/10.1016/j.jnt.2005.10.004

[HL23] G. H. Hardy and 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. http://dx.doi.org/10.1007/BF02403921

[HM17] D. Hast and V. Matei, *Higher moments of arithmetic functions in short intervals: a geometric perspective*. International Mathematics Research Notices, rnx310. http://dx.doi.org/10.1093/imrn/rnx310

[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. http://dx.doi.org/10.1007/BF01465095

[Kat12a] N. M. Katz, *On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor*. Int. Math. Res. Not. IMRN **2013**, no. 14, 3221–3249. http://dx.doi.org/10.1093/imrn/rns143

[Kat12b] ———, *Witt vectors and a question of Keating and Rudnick*. Int. Math. Res. Not. IMRN **2013**, no. 16, 3613–3638. http://dx.doi.org/10.1093/imrn/rns144

[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. IMRN **2014**, no. 1, 259–288. http://dx.doi.org/10.1093/imrn/rns220

[KRG16] J. P. Keating and E. Roditty-Gershon, *Arithmetic correlations over large finite fields*. Int. Math. Res. Not. IMRN **2016**, 860–874. http://dx.doi.org/10.1093/imrn/rnv157

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*. 2017. http://www.lmfdb.org [Online; accessed 28 September 2017].

[May15] J. Maynard, *Small gaps between primes*. Ann. of Math. (2), **181**(2015), 383–413. http://dx.doi.org/10.4007/annals.2015.181.1.7

[Pol08] P. Pollack, *An explicit approach to Hypothesis H for polynomials over finite fields*. In: Anatomy of integers, CRM Proceedings and Lecture Notes, 46, American Mathematical Society, 2008, pp. 47–64.

[Pol14] D. H. J. Polymath, *New equidistribution estimates of Zhang type*, Algebra & Number Theory, **8** (2014), no. 9, 2067–2199. http://dx.doi.org/10.2140/ant.2014.8.2067

[Ser73] J.-P. Serre, *A Course in arithmetic*. Graduate Texts in Mathematics, 7, Springer-Verlag, New York-Heidelberg, 1973.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*. Second ed., Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009. http://dx.doi.org/10.1007/978-0-387-09494-6

[Sk01] A. Skorobogatov, *Torsors and rational points*. Cambridge Tracts in Mathematics, 144, Cambridge University Press, Cambridge, 2001. http://dx.doi.org/10.1017/CBO9780511549588

[Su17] A. V. Sutherland, *Sato-Tate distributions*. 2017. arxiv:1604.01256v4

[Zha14] Y. Zhang, *Bounded gaps between primes*. Ann. of Math. **179**(2014), no. 3, 1121–1174. http://dx.doi.org/10.4007/annals.2014.179.3.7

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, 6997801 Tel Aviv, Israel
Email: barylior@post.tau.ac.il

Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Straße 6–8, 60325 Frankfurt am Main, Germany
Email: stix@math.uni-frankfurt.de

https://doi.org/10.4153/CJM-2018-018-9 Published online by Cambridge University Press