Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

A Brauer–Siegel theorem for Fermat surfaces over finite fields

Richard Griffon

Abstract

We prove an analogue of the Brauer–Siegel theorem for Fermat surfaces over a finite field $\mathbb{F}_q$. Namely, letting $\mathcal{F}_d$ be the Fermat surface of degree d over $\mathbb{F}_q$ and $p_g(\mathcal{F}_d)$ be its geometric genus, we show that, for $d \to \infty$ ranging over the set of integers coprime with q, one has

$$\log\left(|\operatorname{Br}(\mathcal{F}_d)| \cdot \operatorname{Reg}(\mathcal{F}_d)\right) \sim \log q^{p_g(\mathcal{F}_d)} \sim \frac{\log q}{6} \cdot d^3.$$

Here, $\operatorname{Br}(\mathcal{F}_d)$ denotes the Brauer group of $\mathcal{F}_d$ and $\operatorname{Reg}(\mathcal{F}_d)$ the absolute value of a Gram determinant of the Néron–Severi group $\operatorname{NS}(\mathcal{F}_d)$ with respect to the intersection form.

1. *Introduction*

We prove an analogue for certain surfaces over a finite field of the classical Brauer–Siegel theorem, which asserts that, in families of number fields k of bounded degree, the product of the class number h_k and of the regulator of units R_k is of order of magnitude $\sqrt{\Delta_k}$, where Δ_k denotes the absolute value of the discriminant of k. More precisely,

Theorem 1.1 (Brauer–Siegel). *When k runs through a sequence of number fields, whose degrees over $\mathbb{Q}$ are bounded and whose discriminants Δ_k grow to infinity, one has*

$$\log(h_k \cdot R_k) \sim \log \sqrt{\Delta_k} \qquad (\text{as } \Delta_k \to \infty).$$

The proof of Theorem 1.1 (see [**Lan94**, Chap. XVI]) is analytic in that it uses properties of the Dedekind zeta functions $\zeta_k(s)$ of the number fields k in the sequence. There are two main ingredients to it: the first is the analytic class number formula, which relates $h_k \cdot R_k$ to the residue ζ_k^* of $\zeta_k(s)$ at its pole at $s = 1$, and the second is the asymptotic estimate $\log \zeta_k^* = o\big(\log \sqrt{\Delta_k}\big)$ obtained by studying the behaviour of $\zeta_k(s)$ around $s = 1$.

In the analogy between number fields and function fields of curves over finite fields, Theorem 1.1 has the following translation (see [**Ina50**], or [**GL78**] for a similar statement):

Theorem 1.2 (Inaba). *Given a finite field $\mathbb{F}_q$, when C runs through a sequence of smooth projective and geometrically connected curves over $\mathbb{F}_q$, whose gonalities are bounded and whose genera g_C grow to infinity, one has*

$$\log\left|\operatorname{Jac}_C(\mathbb{F}_q)\right| \sim \log q^{g_C}, \qquad (\text{as } g_C \to \infty),$$

where Jac_C denotes the Jacobian variety of C over $\mathbb{F}_q$.

The analogy with Theorem 1.1 becomes evident upon noting that $\operatorname{Jac}_C(\mathbb{F}_q)$ is isomorphic to the divisor class group of $\mathbb{F}_q(C)$, and that no regulator of units appears in this setting. The proof

2010 *Mathematics Subject Classification* 11G25, 11T24, 14G10, 14J25 (primary), 14G15, 11J71 (secondary).

of Theorem 1.2 is analytic too, this time using the Hasse–Weil zeta functions $\zeta(C/\mathbb{F}_q, s)$ of the curves C in the sequence. Both Theorem 1.1 and Theorem 1.2 have been recently generalised: for example, see [**TV02**] for a study of the consequences of weakening the hypothesis of bounded degree in Theorem 1.1 (respectively, of bounded gonality in Theorem 1.2).

In this article, we prove an analogue of Theorems 1.1 and 1.2 for a sequence of *surfaces* over a finite field. More precisely, given a finite field $\mathbb{F}_q$, consider for all integers $d \geq 2$, the Fermat surface $\mathcal{F}_d$ of degree d, *i.e.* the hypersurface of $\mathbb{P}^3$ over $\mathbb{F}_q$ given by:

$$\mathcal{F}_d : \qquad X_0^d + X_1^d + X_2^d + X_3^d = 0.$$

To ensure that $\mathcal{F}_d$ is smooth and geometrically irreducible, we always assume that d is prime to q. Let $\mathrm{NS}(\mathcal{F}_d)$ be the Néron–Severi group of $\mathcal{F}_d$ over $\mathbb{F}_q$, it is known to be a finitely generated torsion-free abelian group (see [**Mil80**, Chap. V] and [**Shi87**]). It is endowed with the intersection form (a nondegenerate bilinear pairing), and one can then define the *regulator of* $\mathcal{F}_d$ to be the Gram determinant

$$\mathrm{Reg}(\mathcal{F}_d) := \left|\det\left[(C_i \cdot C_j)\right]_{1\leq i,j\leq \rho}\right| \in \mathbb{Z} \smallsetminus \{0\},$$

where $C_1, \ldots, C_\rho$ are divisors on $\mathcal{F}_d$ whose classes form a $\mathbb{Z}$-basis of $\mathrm{NS}(\mathcal{F}_d)$. This construction is reminiscent of the definition of the regulator of units of a number field as a determinant.

Besides, recall that the Brauer group $\mathrm{Br}(\mathcal{F}_d)$ is defined as the group of similarity classes of Azumaya algebras over $\mathcal{F}_d$ (see [**Gro68a**], [**Gro68b**], [**Mil80**]). For our purpose, it is sufficient to know that $\mathrm{Br}(\mathcal{F}_d)$ classifies algebraic objects on $\mathcal{F}_d$ that are everywhere étale locally trivial but not globally trivial. It is thus a distant relative of the class group of a number field k, which classifies ideals that are everywhere locally principal, but not necessarily globally so. The Brauer groups of Fermat surfaces has been shown to be finite (see [**SK79**], [**Tat66**], [**Mil75**]).

Our main result in this article (see Corollary 7.2) is the following asymptotic estimate on the product $|\mathrm{Br}(\mathcal{F}_d)| \cdot \mathrm{Reg}(\mathcal{F}_d)$ in terms of the geometric genus $p_g(\mathcal{F}_d)$ of $\mathcal{F}_d$:

THEOREM 1.3. *Let $\mathbb{F}_q$ be a finite field and, for any integer $d \geq 2$ that is coprime to q, consider the d-th Fermat surface $\mathcal{F}_d$ over $\mathbb{F}_q$. With notations as above, one has*

$$\log\big(|\mathrm{Br}(\mathcal{F}_d)| \cdot \mathrm{Reg}(\mathcal{F}_d)\big) \sim \log q^{p_g(\mathcal{F}_d)} \qquad (d \to \infty), \tag{1}$$

where $p_g(\mathcal{F}_d)$ denotes geometric genus of $\mathcal{F}_d$.

It then follows from an easy estimate of $p_g(\mathcal{F}_d)$ that, when $d \to \infty$, one has

$$\log\big(|\mathrm{Br}(\mathcal{F}_d)| \cdot \mathrm{Reg}(\mathcal{F}_d)\big) \sim \frac{\log q}{6} \cdot d^3;$$

thus revealing that the product $|\mathrm{Br}(\mathcal{F}_d)| \cdot \mathrm{Reg}(\mathcal{F}_d)$ grows exponentially fast with d.

Let us outline the proof of Theorem 1.3: in view of the analogy with Theorem 1.1, we proceed in two main steps. For any integer $d \geq 2$ coprime with q, denote by $\zeta(\mathcal{F}_d/\mathbb{F}_q, s)$ the Hasse–Weil zeta function of $\mathcal{F}_d$. Putting $T = q^{-s}$, Weil's work [**Wei49**] shows that

$$\zeta(\mathcal{F}_d/\mathbb{F}_q, s) = \frac{1}{(1-T) \cdot P_2(\mathcal{F}_d/\mathbb{F}_q, T) \cdot (1-q^2T)}, \tag{2}$$

where $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ is an explicit polynomial with integral coefficients (see section 2.3 for details). The Artin–Tate conjecture for surfaces provides a (conjectural) analogue of the

class number formula (see [Tat66], [Tat94], [Mil75], and section 2.1). For the Fermat surfaces $\mathcal{F}_d$, this conjecture has been proved by Katsura and Shioda (see [SK79], [Shi87]). Recall that the special value of $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ at $T = q^{-1}$ is defined as follows: we let $\rho := \mathrm{ord}_{T=q^{-1}} P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ and put

$$P_2^*(\mathcal{F}_d/\mathbb{F}_q) := \left.\frac{P_2(\mathcal{F}_d/\mathbb{F}_q, T)}{(1-qT)^\rho}\right|_{T=q^{-1}} \in \mathbb{Z}[q^{-1}] \subset \mathbb{Q}.$$

The Artin–Tate conjecture implies that $\rho = \mathrm{rk}\,\mathrm{NS}(\mathcal{F}_d)$ and that $P_2^*(\mathcal{F}_d/\mathbb{F}_q)$ has the following interpretation (see section 2.4):

$$P_2^*(\mathcal{F}_d/\mathbb{F}_q) = \frac{|\,\mathrm{Br}(\mathcal{F}_d)| \cdot \mathrm{Reg}(\mathcal{F}_d)}{q^{p_g(\mathcal{F}_d)}}. \tag{3}$$

The second step of the proof of Theorem 1.3 then consists in proving suitable bounds on $P_2^*(\mathcal{F}_d/\mathbb{F}_q)$. More precisely, (3) tells us that Theorem 1.3 will follow from an estimate of the shape $\log P_2^*(\mathcal{F}_d/\mathbb{F}_q) = o\big(\log q^{p_g(\mathcal{F}_d)}\big)$ when $d \to \infty$. We prove a more precise statement:

THEOREM 1.4. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $\varepsilon \in (0, 1/4)$. For any integer $d \geq 2$ prime to q, as $d \to \infty$, one has:*

$$-c_1 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon} \leq \frac{\log P_2^*(\mathcal{F}_d/\mathbb{F}_q)}{\log q^{p_g(\mathcal{F}_d)}} \leq c_2 \cdot \frac{\log\log d}{\log d}, \tag{4}$$

where c_1, c_2 are positive constants that depend at most on q, p and ε.

Theorem 1.4 is a by-product of our main technical results (Theorems 5.1 and 6.2), whose proofs occupy most of sections 5 and 6. Both rely on the explicit expression of $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ obtained by Weil. The upper bound in (4) is relatively straightforward (see section 5) but the lower bound is more demanding (see section 6): let us give a rough sketch of our strategy.

By construction, the special value has the shape:

$$P_2^*(\mathcal{F}_d/\mathbb{F}_q) = \frac{(\text{integer prime to } q)}{q^{w_q(d)}} \quad \text{for a certain exponent } w_q(d) \in \mathbb{Z}_{\geq 0}. \tag{5}$$

Upper bounds on $w_q(d)$ in terms of $p_g(\mathcal{F}_d)$ imply lower bounds on $\log P_2^*(\mathcal{F}_d/\mathbb{F}_q)$: to prove the one in (4), we are to show that $w_q(d) = o\big(p_q(\mathcal{F}_d)\big)$ as $d \to \infty$. An argument "à la Liouville" gives the trivial upper bound: $w_q(d) = O\big(p_q(\mathcal{F}_d)\big)$ (see Proposition 6.1), and we improve on this as follows. The special value $P_2^*(\mathcal{F}_d/\mathbb{F}_q)$ is given as a product of algebraic numbers related to Jacobi sums: we keep track of the contribution of each factor of this product to the denominator in (5) by making use of Stickelberger's theorem. In Theorem 6.4, we thus obtain an explicit expression of $w_q(d)$ in terms of combinatorial data related to the action of q on $\mathbb{Z}/d\mathbb{Z}$ by multiplication. An average equidistribution statement, proved in section 4 (Theorem 4.1), then allows us to conclude that $w_q(d) = o\big(p_q(\mathcal{F}_d)\big)$ as $d \to \infty$ (see Theorem 6.2).

The proof of Theorem 1.3 is put together in section 7 (see Corollary 7.2 there).

In passing, we prove an upper bound on the rank of $\mathrm{NS}(\mathcal{F}_d)$ (see Corollary 5.3):

THEOREM 1.5. *For a given finite field $\mathbb{F}_q$, let $\mathcal{F}_d$ be the d-th Fermat surface over $\mathbb{F}_q$. We denote by $\rho(\mathcal{F}_d/\mathbb{F}_q)$ the rank of the Néron–Severi group of $\mathcal{F}_d/\mathbb{F}_q$. One has*

$$\rho(\mathcal{F}_d/\mathbb{F}_q) \ll_q \frac{d^3}{\log d} \qquad (d \to \infty). \tag{6}$$

The implied constant is effective and depends only on q.

This bound on the rank of Néron–Severi groups appears to be new. It improves greatly on the "geometric" rank bound of Igusa (see [Igu60]) which only yields that $\rho(\mathcal{F}_d/\mathbb{F}_q) \ll d^3$. Moreover, the bound (6) is "asymptotically optimal" in the sense that there exists an infinite sequence of integers d' prime to q such that $\rho(\mathcal{F}_{d'}/\mathbb{F}_q) \gg_q {d'}^3/(\log d')$ as $d' \to \infty$ (see Proposition 5.4).

General notations – For any finite set X, we denote the cardinality of X by $|X|$. If $f(x), g(x)$ are functions of a variable x going to ∞, $f(x) \sim g(x)$ means that $\lim_{x\to\infty} f(x)/g(x) = 1$; and $f(x) \ll_a g(x)$ means that $f(x) \leq C_a g(x)$ for some real constant $C_a > 0$ depending at most on a parameter a. If $q \geq 1$ and $d \geq 2$ are coprime integers, we let $\langle q\rangle_d \subset (\mathbb{Z}/d\mathbb{Z})^\times$ denote the subgroup generated by q mod d. The order of $\langle q\rangle_d$, *i.e.* the multiplicative order of q mod d, is denoted by $o_q(d)$.

2. *Special values of zeta functions of Fermat surfaces*

In this section, we quickly review useful facts about zeta functions of surfaces over finite fields and conjectures about them. We also recall the definitions of Fermat surfaces and known results about their zeta functions. The main goal of this section is to reduce Theorem 1.3 to a statement about the special value of the zeta functions of $\mathcal{F}_d$ (see Proposition 2.6).

Let $\mathbb{F}_q$ be a finite field of characteristic p, and let $\mathcal{S}$ be a smooth projective and geometrically irreducible surface over $\mathbb{F}_q$. We write $\overline{\mathcal{S}} = \mathcal{S} \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. For a prime number $\ell \neq p$, denote by $\mathrm{H}^i(\mathcal{S})$ the i-th ℓ-adic étale cohomology space $\mathrm{H}^i_{ét}(\overline{\mathcal{S}}, \mathbb{Q}_\ell)$.

Let $\mathrm{NS}(\overline{\mathcal{S}})$ be the group of divisors on $\overline{\mathcal{S}}$ modulo algebraic equivalence. The *Néron–Severi group* $\mathrm{NS}(\mathcal{S})$ is defined to be the image of the Picard group $\mathrm{Pic}(\mathcal{S})$ in $\mathrm{NS}(\overline{\mathcal{S}})$. Since the base field $\mathbb{F}_q$ is finite, another possible definition is to let $\mathrm{NS}(\mathcal{S}) := \mathrm{NS}(\overline{\mathcal{S}})^{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}$, the $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-invariant subgroup of $\mathrm{NS}(\overline{\mathcal{S}})$ (see [PTvL15, Prop. 6.2]).

The so-called "Theorem of the base" asserts that $\mathrm{NS}(\overline{\mathcal{S}})$, and therefore $\mathrm{NS}(\mathcal{S})$, is a finitely generated abelian group (see Chapter V in [Mil80]). The rank $\rho(\mathcal{S}/\mathbb{F}_q)$ of $\mathrm{NS}(\mathcal{S})$ is called the *Picard number* of $\mathcal{S}$. Moreover, the Néron–Severi group is endowed with the intersection form $(- \cdot -)$, which is a nondegenerate bilinear pairing: if $D_1, \dots, D_\rho$ is a set of divisors on $\mathcal{S}$ whose classes generate $\mathrm{NS}(\mathcal{S})$ modulo torsion, we define the *regulator of* $\mathcal{S}$ to be

$$\mathrm{Reg}(\mathcal{S}/\mathbb{F}_q) := \left|\det\left(D_i \cdot D_j\right)_{1\leq i,j\leq\rho}\right| \in \mathbb{Z} \smallsetminus \{0\}. \tag{2.1}$$

The *Brauer group of* $\mathcal{S}$ can be defined in (at least) two ways: one can define $\mathrm{Br}(\mathcal{S}/\mathbb{F}_q)$ as the group of similarity classes of Azumaya algebras over $\mathcal{S}$ (see [Gro68a]) which, when $\mathcal{S}$ is smooth and projective, is isomorphic to the "cohomological" Brauer group

$$\mathrm{Br}(\mathcal{S}/\mathbb{F}_q) := \mathrm{H}^2_{ét}(\mathcal{S}, \mathbb{G}_m) = \mathrm{H}^2_{ét}(\mathcal{S}, \mathcal{O}_{\mathcal{S}}^\times), \tag{2.2}$$

see [Gro68b], [Mil80, Chap. V].

It is conjectured, but not known in general, that $\mathrm{Br}(\mathcal{S}/\mathbb{F}_q)$ is finite (see [Tat66]).

2.1. *Zeta functions of surfaces and their special values*

A priori, the zeta function of $\mathcal{S}$ is defined as the formal power series

$$Z(\mathcal{S}/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{+\infty} \frac{|\mathcal{S}(\mathbb{F}_{q^n})|}{n} \cdot T^n\right) \in \mathbb{Q}[[T]]$$

where $|\mathcal{S}(\mathbb{F}_{q^n})|$ denotes the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{S}$. By the Weil conjectures (which are now proved, see [Del74]), it is known that $Z(\mathcal{S}/\mathbb{F}_q, T)$ is actually a rational function of T:

more precisely, $Z(\mathcal{S}/\mathbb{F}_q, T)$ can be written as

$$Z(\mathcal{S}/\mathbb{F}_q, T) = \frac{P_1(T) \cdot P_3(T)}{P_0(T) \cdot P_2(T) \cdot P_4(T)},$$

with $P_i(T) = \det\left(1 - \mathrm{Fr}^* \cdot T \;\middle|\; \mathrm{H}^i(\mathcal{S})\right)$, where Fr^* is the endomorphism of $\mathrm{H}^i(\mathcal{S})$ induced by the action of the geometric Frobenius on $\overline{\mathcal{S}}$. It is also known that the polynomials $P_i(T)$ have integral coefficients, are independent of the choice of $\ell \neq p$, and that their reciprocal roots are algebraic integers of absolute value $q^{i/2}$ in any complex embedding (the so-called Riemann hypothesis for $Z(\mathcal{S}/\mathbb{F}_q, T)$). For more details about these facts, the reader can consult [**Mil80**].

If $\mathcal{S}$ is geometrically irreducible, one has $P_0(T) = 1 - T$ and $P_4(T) = 1 - q^2T$. Furthermore, by Poincaré duality, $P_3(T) = P_1(qT)$ and, as soon as $\mathcal{S}$ has a trivial Picard variety, $P_1(T) = P_3(T) = 1$. Finally, any nonsingular surface $\mathcal{S}$ of degree d in $\mathbb{P}^3$ has

$$\deg P_2(T) = \dim \mathrm{H}^2(\mathcal{S}) = (d-1)(d^2 - 3d + 3) + 1. \tag{2.3}$$

Let us study the analytic behaviour of $P_2(\mathcal{S}/\mathbb{F}_q, T)$ at $T = q^{-1}$ (that is, the behaviour of $s \mapsto Z(\mathcal{S}/\mathbb{F}_q, q^{-s})$ at $s = 1$). First, we call the order of vanishing of $P_2(T)$ at $T = q^{-1}$ the *analytic rank* ρ of $\mathcal{S}$. Second, we define the *special value at* $T = q^{-1}$ to be

$$P_2^*(\mathcal{S}/\mathbb{F}_q, q^{-1}) := \left.\frac{P_2(\mathcal{S}/\mathbb{F}_q, T)}{(1 - qT)^\rho}\right|_{T=q^{-1}}.$$

By definition, $P_2^*(\mathcal{S}/\mathbb{F}_q, q^{-1})$ is a nonzero rational number, and the Riemann hypothesis for $P_2(\mathcal{S}/\mathbb{F}_q, T)$ implies that $P_2^*(\mathcal{S}/\mathbb{F}_q, q^{-1})$ is positive.

Inspired by the conjectures of Birch and Swinnerton-Dyer for elliptic curves, Tate and Artin–Tate conjectured that these quantities have a "geometric" interpretation:

Conjecture 2.1 (Artin–Tate). Let $\mathcal{S}$ be a projective smooth and geometrically irreducible surface over a finite field $\mathbb{F}_q$, $p_g(\mathcal{S})$ be the geometric genus of $\mathcal{S}$ and let $\rho(\mathcal{S}/\mathbb{F}_q)$ denote the rank of the Néron–Severi group $\mathrm{NS}(\mathcal{S})$ of $\mathcal{S}$. Then

(1) The Néron–Severi group has rank $\rho(\mathcal{S}/\mathbb{F}_q) = \mathrm{ord}_{T=q^{-1}} P_2(\mathcal{S}/\mathbb{F}_q, T)$,
(2) The Brauer group $\mathrm{Br}(\mathcal{S})$ is finite,
(3) The special value $P_2^*(\mathcal{S}/\mathbb{F}_q, q^{-1})$ admits the expression:

$$P_2^*(\mathcal{S}/\mathbb{F}_q, q^{-1}) = \frac{|\mathrm{Br}(\mathcal{S}/\mathbb{F}_q)| \cdot \mathrm{Reg}(\mathcal{S}/\mathbb{F}_q)}{q^{p_g(\mathcal{S})} \cdot |\mathrm{NS}(\mathcal{S})_{\mathrm{tors}}|^2} \cdot q^{\delta(\mathcal{S})}, \tag{2.4}$$

where $\delta(\mathcal{S}) = \dim \mathrm{H}^1(\mathcal{S}, \mathcal{O}_\mathcal{S}) - \dim \mathrm{PicVar}(\mathcal{S})$ is the "defect of smoothness" of the Picard variety of $\mathcal{S}$ (it is known that $\delta(\mathcal{S}) \leq p_g(\mathcal{S})$, see [**Tat66**]).

We refer to [**Tat66**, Conjecture C] for the original statement. Tate [**Tat94**] and Milne [**Mil75**] have subsequently proved that parts (1) to (3) are equivalent (see [**Ulm14**] for a nice survey). The full Conjecture 2.1 has been proved for certain surfaces over $\mathbb{F}_q$, among which Fermat surfaces (see below).

2.2. *Fermat surfaces*

For any positive integer d coprime to p, let $\mathcal{F}_d$ be the *d-th Fermat surface* over $\mathbb{F}_q$, whose equation in $\mathbb{P}^3$ is

$$\mathcal{F}_d : \qquad X_0^d + X_1^d + X_2^d + X_3^d = 0. \tag{2.5}$$

Thus defined, $\mathcal{F}_d$ is a smooth, projective and geometrically irreducible surface (since d is prime to q). These surfaces – and their higher dimensional analogues – have been studied in great detail, in particular by Shioda and his coauthors.

Let us recall the facts about $\mathcal{F}_d$ that are most relevant to our present goal (the reader is referred to [SK79], [Shi86], [Shi87] and [SSvL10] for detailed geometric information on $\mathcal{F}_d$). Like any nonsingular surface of degree d in $\mathbb{P}^3$, the Fermat surface $\mathcal{F}_d$ has geometric genus

$$p_g(\mathcal{F}_d) = \frac{(d-1)(d-2)(d-3)}{6} = \binom{d-1}{3}.$$

In particular, $p_g(\mathcal{F}_d) \sim d^3/6$ as $d \to \infty$. Furthermore, for any nonsingular surface $\mathcal{S}$ in $\mathbb{P}^3$, one knows that $\mathrm{NS}(\mathcal{S})$ is torsion-free, and that the Picard variety $\mathrm{PicVar}(\mathcal{S})$ is trivial (so that, in particular, the defect of smoothness $\delta(\mathcal{S})$ in (2.4) vanishes).

There is a natural action of $\Gamma_d := \mu_d(\overline{\mathbb{F}_q})^4/(\text{diagonal}) \subset \mathrm{Aut}_{\overline{\mathbb{F}_q}}(\mathcal{F}_d)$ on $\mathcal{F}_d$ via

$$\forall P = [x_0 : x_1 : x_2 : x_3] \in \mathcal{F}_d, \forall \boldsymbol{\zeta} = [\zeta_0 : \zeta_1 : \zeta_2 : \zeta_3] \in \Gamma_d, \quad \boldsymbol{\zeta} \cdot P = [\zeta_0 x_0 : \zeta_1 x_1 : \zeta_2 x_2 : \zeta_3 x_3].$$

Note that, when d divides $|\mathbb{F}_q^\times| = q-1$, the action of Γ_d on $\mathcal{F}_d$ is an action by $\mathbb{F}_q$-automorphisms (since then, all d-roots of unity in $\overline{\mathbb{F}_q}$ are $\mathbb{F}_q$-rational). In general though (*i.e.* d only assumed to be prime to q), the action of the q-th power Frobenius Fr_q on Γ_d is not trivial.

Instead of Γ_d, we will rather study its character group $\widehat{\Gamma_d}$ under the following "combinatorial" incarnation:

$$G_d := \left\{ \mathbf{a} = (a_0, \dots, a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 \;\middle|\; a_0 + \cdots + a_3 \equiv 0 \bmod d \right\} \simeq \widehat{\Gamma_d}. \tag{2.6}$$

2.3. *Zeta functions of Fermat surfaces*

The zeta functions of Fermat surfaces have been explicitly computed by Weil in [Wei49] as evidence towards his conjectures. We recall his result in this subsection but, before we do so, we need to introduce a few more notations which will be in force for the rest of the paper.

2.3.1. *The Teichmüller character and the action of q on G_d* Let p be a prime number; we fix, once and for all, an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ (of which all number fields are seen as subfields) and a prime ideal $\mathfrak{P}$ above p in the ring of integers $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$. The quotient field $\overline{\mathbb{Z}}/\mathfrak{P}$ is then an algebraic closure of $\mathbb{F}_p$: all the finite fields $\mathbb{F}_q$ of characteristic p involved in our computations will be seen as subfields of this algebraic closure. Let $\mu_{p'} \subset \overline{\mathbb{Q}}$ be the group of roots of unity whose order is prime to p. The reduction map $\overline{\mathbb{Z}} \to \overline{\mathbb{Z}}/\mathfrak{P} = \overline{\mathbb{F}_p}$ induces an isomorphism $\mu_{p'} \to \overline{\mathbb{F}_p}^\times$. We denote by $\mathbf{t} : \overline{\mathbb{F}_p}^\times \to \mu_{p'} \hookrightarrow \overline{\mathbb{Q}}^\times$ the inverse of this isomorphism: we call $\mathbf{t}$ the *Teichmüller character*, and we also denote by $\mathbf{t}$ the restrictions of $\mathbf{t}$ to the various finite fields $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$.

Let G_d be as in (2.6). There is a natural action of $(\mathbb{Z}/d\mathbb{Z})^\times$ on G_d by component-wise multiplication: for all $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ and all $\mathbf{a} = (a_0, \dots, a_3) \in G_d$, we let $t \cdot \mathbf{a} := (ta_0, \dots, ta_3)$. Since q is prime to d, the subgroup $\langle q \rangle_d \subset (\mathbb{Z}/d\mathbb{Z})^\times$ generated by q also acts on G_d by multiplication.

For any subset Λ of G_d which is stable under this action of q, we will denote by $\mathcal{O}_q(\Lambda)$ the set of orbits of Λ under multiplication by q. Given an orbit $\mathbf{A} \in \mathcal{O}_q(\Lambda)$, we will often have to make a choice of a representative $\mathbf{a} \in \Lambda$ of this orbit. To avoid repeating the sentence "[...] where $\mathbf{a}$ is a representative of the orbit $\mathbf{A}$", we will stick to the following convention: orbits in $\mathcal{O}_q(\Lambda)$ will always be denoted by an *uppercase bold* letter ($\mathbf{A}, \mathbf{B}$, ...) and we denote by the corresponding *lowercase bold* letter ($\mathbf{a}$, $\mathbf{b}$, ...) any choice of a representative in Λ of that orbit. For any orbit $\mathbf{A} \in \mathcal{O}_q(G_d)$, we let $|\mathbf{A}|$ be the length of $\mathbf{A}$; in other words, for any representative $\mathbf{a} = (a_0, \dots, a_3) \in \mathbf{A}$, one has $|\mathbf{A}| = \left|\{\mathbf{a}, q \cdot \mathbf{a}, \dots, q^n \cdot \mathbf{a}, \dots\}\right|$, or equivalently

$$|\mathbf{A}| = \min\left\{ n \in \mathbb{Z}_{\geq 1} \;\middle|\; \forall i \in \{0,1,2,3\},\ q^n \cdot a_i \equiv a_i \bmod d \right\}.$$

For any $\mathbf{a} \in G_d$, let $d_{\mathbf{a}} := d/\gcd(d, a_0, \dots, a_3)$: since q is prime to d, it is easy to see that $\mathbf{a} \mapsto d_{\mathbf{a}}$ is constant along an orbit under multiplication by q, and one checks that $|\mathbf{A}| = o_q(d_{\mathbf{a}})$ where,

for any integer $n \geq 2$ prime to q, $o_q(n)$ denotes the (multiplicative) order of q in $(\mathbb{Z}/n\mathbb{Z})^\times$. For any power q^v of q, by definition of the order, we see that $q^v\mathbf{a} \equiv \mathbf{a} \bmod d$ if and only if $o_q(d_\mathbf{a})$ divides v, *i.e.* $\mathbb{F}_{q^v}$ is an extension of $\mathbb{F}_{q^{|\mathbf{A}|}}$.

It is also easily checked that the pairing

$$(\mathbf{a}, \boldsymbol{\zeta}) \in G_d \times \Gamma_d \mapsto \mathbf{t}_\mathbf{a}(\boldsymbol{\zeta}) := \mathbf{t}(\zeta_0)^{a_0} \cdot \ldots \cdot \mathbf{t}(\zeta_3)^{a_3} \in \overline{\mathbb{Q}}^\times$$

induces the isomorphism $\widehat{\Gamma_d} \simeq G_d$ alluded to in (2.6). Moreover, this isomorphism takes the q-th power Frobenius action on Γ_d to the action of q by multiplication on G_d in the following sense:

$$\forall \mathbf{a} \in G_d, \forall \boldsymbol{\zeta} = [\zeta_0 : \cdots : \zeta_3] \in \Gamma_d, \quad \mathbf{t}_\mathbf{a}(\mathrm{Fr}_q(\boldsymbol{\zeta})) = \mathbf{t}_\mathbf{a}(\zeta_0^q, \ldots, \zeta_3^q) = \mathbf{t}_{q\cdot\mathbf{a}}(\zeta_0, \ldots, \zeta_3) = \mathbf{t}_{q\cdot\mathbf{a}}(\boldsymbol{\zeta}).$$

2.3.2. *Jacobi sums* To state Weil's result in a convenient form, we further need to introduce a specific "instantiation" of Jacobi sums. We make the convention that characters $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ are extended by $\chi(0) = 0$ unless χ is the trivial character, in which case we put $\chi(0) = 1$.

The classical results we need about characters of finite fields and Jacobi sums can be found in [**IR90**] and [**LN97**, Chap. 5].

Definition 2.2. For all $\mathbf{a} = (a_0, \ldots, a_3) \in G_d \smallsetminus \{(0,0,0,0)\}$ and all integers $s \in \mathbb{Z}_{\geq 1}$, define the following characters on $\mathbb{F}_Q^\times$ where $Q = q^{s\cdot|\mathbf{A}|}$:

$$\forall i \in \{0,1,2,3\},\ \boldsymbol{\chi}_i : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times,\ x \mapsto \left(\mathbf{t} \circ \mathbf{N}_{\mathbb{F}_Q/\mathbb{F}_{q^{|\mathbf{A}|}}}(x)\right)^{(q^{|\mathbf{A}|}-1)\cdot a_i/d},$$

where $\mathbf{N}_{\mathbb{F}_Q/\mathbb{F}_{q^{|\mathbf{A}|}}} : \mathbb{F}_Q \to \mathbb{F}_{q^{|\mathbf{A}|}}$ denotes the relative norm.

One then defines a Jacobi sum (relative to $\mathbb{F}_Q$) by

$$\mathbf{J}_Q(\mathbf{a}) = \frac{1}{Q-1} \sum_{\substack{x_0,\ldots,x_3 \in \mathbb{F}_Q^\times \\ x_0+\cdots+x_3=0}} \boldsymbol{\chi}_0(x_0)\boldsymbol{\chi}_1(x_1)\boldsymbol{\chi}_2(x_2)\boldsymbol{\chi}_3(x_3).$$

When $s = 1$, we denote $\mathbf{J}_{q^{|\mathbf{A}|}}(\mathbf{a})$ by $\mathbf{J}(\mathbf{a})$ for short. By convention, let $\mathbf{J}(0,0,0,0) = q$.

This normalisation of Jacobi sums is the same as that of Weil [**Wei49**] and of Shioda [**Shi87**]. Note that the characters $\boldsymbol{\chi}_i$ have order dividing d (actually, the exact order of $\boldsymbol{\chi}_i$ can be seen to be $d/\gcd(d, a_i)$) and that $\boldsymbol{\chi}_i$ is trivial if and only if $a_i = 0$. In particular, the sum $\mathbf{J}_Q(\mathbf{a})$ is an algebraic integer in the cyclotomic field $K := \mathbb{Q}(\zeta_d)$.

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ thus permutes the sums $\mathbf{J}_Q(\mathbf{a})$: let us identify $\mathrm{Gal}(K/\mathbb{Q})$ with $(\mathbb{Z}/d\mathbb{Z})^\times$ in the usual manner (with $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ corresponding to $\sigma_t \in \mathrm{Gal}(K/\mathbb{Q})$), then

$$\forall \mathbf{a} \in G_d, \forall t \in (\mathbb{Z}/d\mathbb{Z})^\times, \quad \sigma_t\left(\mathbf{J}_Q(\mathbf{a})\right) = \mathbf{J}_Q(t \cdot \mathbf{a}). \tag{2.7}$$

Furthermore, it is well-known that $|\mathbf{J}_Q(\mathbf{a})| = Q$ if and only if all $\boldsymbol{\chi}_i$ are non trivial and their product $\boldsymbol{\chi}_0 \cdot \ldots \cdot \boldsymbol{\chi}_3$ is trivial: we are thus led to introduce

$$G_d^\circ := \left\{(a_0, \ldots, a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 \;\middle|\; \forall i,\ a_i \neq 0 \text{ and } \sum a_i = 0\right\} = \left\{\mathbf{a} \in G_d \;\middle|\; \forall i,\ a_i \neq 0\right\}.$$

The subset $G_d^\circ \subset G_d$ is clearly stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$; it has cardinality $|G_d^\circ| = (d-1)(d^2-3d+3) = (d-1)^3 - 2d^2$. We also remark that $\mathbf{J}(q \cdot \mathbf{a}) = \mathbf{J}(\mathbf{a})$ and, more generally, that $\mathbf{J}(p \cdot \mathbf{a}) = \mathbf{J}(\mathbf{a})$. Finally, we recall the relation of Davenport–Hasse for Jacobi sums in the following form (see [**Wei49**], [**IR90**]):

$$\text{if } \mathbf{a} \in G_d \text{ and } s \geq 1 \text{ is an integer, then } \mathbf{J}_{q^{s|\mathbf{A}|}}(\mathbf{a}) = \left(\mathbf{J}_{q^{|\mathbf{A}|}}(\mathbf{a})\right)^s = \mathbf{J}(\mathbf{a})^s. \tag{2.8}$$

2.3.3. *Zeta functions of Fermat surfaces* We have now enough notations to state the result of Weil mentioned earlier (see [**Wei49**]):

THEOREM 2.3 (Weil). *Let $\mathbb{F}_q$ be a finite field and $d \geq 2$ be an integer, coprime with q. Let $G_d^\circ \subset G_d$ be as above. The Fermat surface $\mathcal{F}_d/\mathbb{F}_q$ defined by equation (2.5) has zeta function given by*

$$Z(\mathcal{F}_d/\mathbb{F}_q, T) = \frac{1}{(1-T)\cdot P_2(\mathcal{F}_d/\mathbb{F}_q, T)\cdot(1-q^2T)},$$

where, denoting by $\mathbf{J}(\mathbf{a}) = \mathbf{J}_{q^{|\mathbf{A}|}}(a_0, \dots, a_3)$ the Jacobi sum defined above,

$$P_2(\mathcal{F}_d/\mathbb{F}_q, T) = (1-qT)\cdot \prod_{\mathbf{A}\in\mathcal{O}_q(G_d^\circ)} \left(1 - \mathbf{J}(\mathbf{a})\cdot T^{|\mathbf{A}|}\right). \tag{2.9}$$

There are at least two ways to obtain this expression for $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$. One is by a direct "point-counting" argument (see [**Wei49**] or [**IR90**]). Another is via a more cohomological method: one can decompose $\mathrm{H}^2(\mathcal{F}_d)$ into subspaces that are stable for the induced action of G_d (see [**SK79**] or [**Kat81**, Coro. 2.4]). Note that the "usual" setting for the proof is to assume that d divides $q-1$ (in which case the action of G_d commutes to that of Fr_q), which is insufficient for our use since we need d to be arbitrarily large with respect to a fixed q. This explains the appearance of the action of q on the indexing set G_d° for the Jacobi sums: multiplication by q on G_d is the "combinatorial" version of the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on Γ_d (see subsection 2.3.1).

REMARK 2.4. If one considers the Fermat surface "with coefficients", that is to say the surface defined by

$$\mathcal{F}'_d : c_0X_0^d + c_1X_1^d + c_2X_2^d + c_3X_3^d = 0 \quad \text{with } c_i \in \mathbb{F}_q^\times,$$

one can also give an explicit expression of the zeta function. The only change in Theorem 2.3 is that

$$P_2(\mathcal{F}'_d/\mathbb{F}_q, T) = (1-qT)\cdot \prod_{\mathbf{A}\in\mathcal{O}_q(G_d^\circ)} \left(1 - \xi_{\mathbf{c}}(\mathbf{a})\cdot\mathbf{J}(\mathbf{a})\cdot T^{|\mathbf{A}|}\right),$$

where $\xi_{\mathbf{c}}(\mathbf{a}) = \prod_{i=0}^3 \boldsymbol{\chi}_i(c_i^{-1})$ is a d-th root of unity in $\overline{\mathbb{Q}}$.

The reader can check that our arguments to bound $P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1})$ would work just as well for $\mathcal{F}'_d$ (uniformly in the choice of coefficients c_i).

2.4. *Special values of zeta functions of Fermat surfaces*

We now introduce $G_d^* := \left\{\mathbf{a} \in G_d^\circ \;\middle|\; \mathbf{J}(\mathbf{a}) \neq q^{|\mathbf{A}|}\right\}$, the subset of G_d° parametrising the factors $1 - \mathbf{J}(\mathbf{a})T^{|\mathbf{A}|}$ of $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ that do not vanish at $T = q^{-1}$: this set G_d^* is obviously stable under the action of q; furthermore, a computation (as in Lemma 3.5 below) shows that the special value of $P_2(\mathcal{F}_d/\mathbb{F}_q, T)$ at $T = q^{-1}$ is:

$$P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1}) = \prod_{\mathbf{a}\in\mathcal{O}_q(G_d^\circ\smallsetminus G_d^*)} |\mathbf{A}| \cdot \prod_{\mathbf{A}\in\mathcal{O}_q(G_d^*)} \left(1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right). \tag{2.10}$$

On the other hand, $P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1})$ also has an expression in terms of algebro-geometric invariants of $\mathcal{F}_d$, indeed:

THEOREM 2.5 (Shioda). *Over $\mathbb{F}_q$, the Fermat surface $\mathcal{F}_d$ satisfies the Artin–Tate conjecture (Conjecture 2.1). In particular, its Brauer group $\mathrm{Br}(\mathcal{F}_d)$ is finite.*

Shioda proves that $\mathcal{F}_d/\mathbb{F}_q$ satisfies part (1) of Conjecture 2.1 (the so-called Tate conjecture), which is enough to prove that the full conjecture holds. His proof relies on the following two facts: first, if one knows that (1) holds for a surface $\mathcal{S}$ and if there is a dominant rational map $\mathcal{S} \dashrightarrow \mathcal{S}'$, then (1) also holds for $\mathcal{S}'$. Second, (1) is true for surfaces $\mathcal{S}$ that are products of curves $C_1 \times C_2$ by a famous result of Tate [**Tat94**]. In particular, (1) is known for all surfaces that are dominated by products of curves. Katsura and Shioda have explicitly constructed a dominant rational map $C_1 \times C_2 \dashrightarrow \mathcal{F}_d$ from a product of Fermat curves to $\mathcal{F}_d$. For more details, see [**SK79**].

The veracity of Conjecture 2.1 for $\mathcal{F}_d$ (in particular, part (3) of it) yields the following expression for $P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1})$ (see Proposition 5.2 of [**Shi87**]):

PROPOSITION 2.6 (Shioda). *Let $\mathbb{F}_q$ be a finite field. For any integer $d \geq 2$ that is prime to q, one has:*

$$P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1}) = \frac{|\operatorname{Br}(\mathcal{F}_d)| \cdot \operatorname{Reg}(\mathcal{F}_d)}{q^{p_g(\mathcal{F}_d)}}.$$

3. *A more general setting*

With the previous Proposition at hand, the proof of our main theorem (Theorem 1.3) reduces to proving the asymptotic bound on the special value $P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1})$ mentioned in the introduction (Theorem 1.4). To obtain such an asymptotic estimate, we rely on the explicit expression (2.10) for $P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1})$. Since we have other applications in mind for these bounds on special values, and since it will not lead to too many technical complications, we will consider a slightly more general and more flexible setting which we now describe.

3.1. *The polynomials $P(\Lambda, T)$*

Let $\mathbb{F}_q$ be a finite field of characteristic p. As above, for any integer $d \geq 2$ that is prime to p, we let

$$G_d = \left\{(a_0, \ldots, a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 \mid \textstyle\sum_{i=0}^3 a_i = 0\right\} \subset (\mathbb{Z}/d\mathbb{Z})^4.$$

Recall that $(\mathbb{Z}/d\mathbb{Z})^\times$ (and thus its subgroup $\langle q \rangle_d$) acts by multiplication on G_d. If $\Lambda \subset G_d$ is stable by multiplication by q, we denote by $\mathcal{O}_q(\Lambda)$ the set of orbits of Λ under this action. We will be interested in the following class of polynomials:

DEFINITION 3.1. Let Λ be a nonempty subset of G_d. We assume that Λ is stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ by multiplication. We then define the following polynomial

$$P(\Lambda, T) = \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \left(1 - \mathbf{J}(\mathbf{a}) \cdot T^{|\mathbf{A}|}\right) \in \mathbb{Z}[T],$$

where $\mathbf{J}(\mathbf{a}) = \mathbf{J}_{q^{|\mathbf{A}|}}(a_0, \ldots, a_3)$ is the Jacobi sum defined above (Definition 2.2).

Under the assumption that Λ is $(\mathbb{Z}/d\mathbb{Z})^\times$-stable, $P(\Lambda, T)$ indeed has integral coefficients because the Jacobi sums are algebraic integers and the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ on $\{\mathbf{J}(\mathbf{a})\}_{\mathbf{a} \in G_d}$ corresponds to the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ on G_d (see (2.7)). Note that $P(\Lambda, T)$ implicitly depends

on q, but we chose not to include it in the notation since q is considered to be fixed. Besides, we remark that $\deg P(\Lambda, T) = \left|\left\{\mathbf{a} \in \Lambda \;\middle|\; \mathbf{J}(\mathbf{a}) \neq 0\right\}\right| \leq |\Lambda|$.

We define the *special value of* $P(\Lambda, T)$ *at* $T = q^{-1}$ to be

$$P^*(\Lambda) := \left.\frac{P(\Lambda, T)}{(1-qT)^\rho}\right|_{T=q^{-1}}, \text{ where } \rho = \operatorname{ord}_{T=q^{-1}} P(\Lambda, T).$$

In other words, if we set $P^*_\Lambda(T) := P(\Lambda, T) \cdot (1-qT)^{-\rho} \in \mathbb{Z}[T]$, then $P^*(\Lambda) = P^*_\Lambda(q^{-1})$.

By construction, $P^*(\Lambda)$ is a nonzero element of $\mathbb{Z}[q^{-1}] \subset \mathbb{Q}$.

3.2. *Examples*

To justify our considering such objects, let us give a few examples of situations in which polynomials $P(\Lambda, T)$ naturally appear.

Example 3.2. As a first example, let us choose $\Lambda_{\mathcal{F}} = G_d$ for an integer $d \geq 2$ coprime with q. For any $\mathbf{a} \in G_d$, recall that

$$\mathbf{J}(\mathbf{a}) = \begin{cases} q & \text{if } \mathbf{a} = (0,0,0,0), \\ 0 & \text{if some (but not all) of the } a_i \text{ are } 0, \\ \text{of absolute value } q^{|\mathbf{A}|} & \text{if } \mathbf{a} \in G_d^\circ. \end{cases}$$

So that, from Weil's theorem (Theorem 2.3), we obtain

$$P(\Lambda_{\mathcal{F}}, T) = (1-qT) \cdot \prod_{\mathbf{A} \in \mathcal{O}_q(G_d^\circ)} \left(1 - \mathbf{J}(\mathbf{a}) \cdot T^{|\mathbf{A}|}\right) = P_2(\mathcal{F}_d/\mathbb{F}_q, T).$$

Notice that $\Lambda_{\mathcal{F}}$ is of size $|\Lambda_{\mathcal{F}}| = |G_d| = d^3 \sim 6 \cdot p_g(\mathcal{F}_d)$ when $d \to \infty$. This example is actually the one to which we will apply our main results (Theorems 5.1 and 6.2) in section 7.

Example 3.3. For an integer $d \geq 2$ coprime with q, consider a subgroup H of $\Gamma_d = \mu_d(\overline{\mathbb{F}_q})^4/(\text{diagonal})$ (see subsection 2.2). The finite group H acts on $\mathcal{F}_d$, and we let $\mathcal{S} := \mathcal{F}_d/H$ be the quotient of the Fermat surface $\mathcal{F}_d$ by this action. The resulting surface $\mathcal{S}$ is defined over $\mathbb{F}_q$ and is normal (but not necessarily smooth).

Let $\Lambda_H \subset G_d$ be the subgroup of G_d isomorphic to $H^\perp = \left\{\chi \in \widehat{\Gamma_d} \;\middle|\; \forall h \in H,\ \chi(h) = 1\right\}$ in the isomorphism $\widehat{\Gamma_d} \simeq G_d$. Being a subgroup of G_d, Λ_H is clearly nonempty and stable under multiplication by $(\mathbb{Z}/d\mathbb{Z})^\times$. Denote by $P_2(\mathcal{S}/F_q, T)$ the characteristic polynomial of the Frobenius Fr_q acting on $\mathrm{H}^2(\mathcal{S})$. A computation very similar to that of [**Ulm02**, §7] would show that

$$P_2(\mathcal{S}/\mathbb{F}_q, T) = P(\Lambda_H, T).$$

Our main results (Theorems 5.1 and 6.2) directly provide bounds in terms of $|\Lambda_H|$ on the special value $P^*(\Lambda_H)$ as $|\Lambda_H|$ (and thus d) tends to infinity.

Example 3.4. As a special case, for any integer $d \geq 2$ prime to q, consider the subgroup $H \subset \Gamma_d$ generated by $[\zeta^2 : \zeta : 1 : 1]$ and $[1 : \zeta : \zeta^3 : 1]$, for $\zeta \in \mu_d(\overline{\mathbb{F}_q})$ a primitive d-th root of unity. Set $\mathcal{S} := \mathcal{F}_d/H$ to be the quotient of the Fermat surface by the action of H. In [**Ulm02**], Ulmer has proved a number of facts about $\mathcal{S}$, among which the identity $P_2(\mathcal{S}/\mathbb{F}_q, T) = P(\Lambda_H, T)$, where $\Lambda_H \subset G_d$ is associated to H as in the example above.

The polynomial $P_2(\mathcal{S}/\mathbb{F}_q, T)$ is closely related to the L-function of the elliptic curve $E_d/\mathbb{F}_q(t)$ given by $y^2 + xy = x^3 - t^d$ (see *loc. cit.* for details). In this example, our upper and lower bounds on $P_2^*(\Lambda_H)$ have been proved by Hindry and Pacheco as the first example of a family

of elliptic curves over $\mathbb{F}_q(t)$ unconditionally satisfying an analogue of the Brauer–Siegel theorem (see [**HP16**, §7.4]). There are now five more examples of such families, by [**Gri16**].

3.3. *Two preliminary lemmas*

Let $\Lambda \subset G_d$ be a nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset. The next lemma provides an explicit expression for the special value $P^*(\Lambda)$ in terms of the following decomposition of Λ:

$$\Lambda = \Lambda_0 \sqcup \Lambda^* \sqcup \Lambda',$$

where $\Lambda_0 = \{\mathbf{a} \in \Lambda \mid \mathbf{J}(\mathbf{a}) = q^{|\mathbf{A}|}\}$, $\Lambda^* = \{\mathbf{a} \in \Lambda \mid |\mathbf{J}(\mathbf{a})| = q^{|\mathbf{A}|} \text{ but } \mathbf{J}(\mathbf{a}) \neq q^{|\mathbf{A}|}\}$, and $\Lambda' = \Lambda \smallsetminus (\Lambda_0 \sqcup \Lambda^*)$. Each of these subsets of Λ is stable under the action of q because the value of $\mathbf{J}(\mathbf{a})$ does not depend on the choice of representative $\mathbf{a} \in \mathbf{A}$. Notice that, if $\mathbf{A} \in \mathcal{O}_q(\Lambda')$ one has $\mathbf{J}(\mathbf{a}) = 0$ and that, if $(0,0,0,0) \in \Lambda$ then $(0,0,0,0) \in \Lambda_0$.

With this decomposition at hand, we can state:

LEMMA 3.5. *Notations being as above, the multiplicity of $T = q^{-1}$ as a root of $P(\Lambda, T)$ is equal to $|\mathcal{O}_q(\Lambda_0)|$ and the special value $P^*(\Lambda)$ can be expressed as:*

$$P^*(\Lambda) = P^*_\Lambda(q^{-1}) = \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda_0)} |\mathbf{A}| \cdot \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda^*)} \left(1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right). \tag{3.1}$$

Proof. For any orbit $\mathbf{A} \in \mathcal{O}_q(\Lambda)$, we let $g_{\mathbf{A}}(T) := 1 - \mathbf{J}(\mathbf{a})T^{|\mathbf{A}|}$ be the corresponding factor of $P(\Lambda, T)$. The polynomial $g_{\mathbf{A}}(T)$ vanishes at $T = q^{-1}$ if and only if $\mathbf{J}(\mathbf{a}) = q^{|\mathbf{A}|}$, in which case $T = q^{-1}$ is a simple root of $g_{\mathbf{A}}(T)$. This means that

$$\rho := \operatorname{ord}_{T=q^{-1}} P(\Lambda, T) = \sum_{\mathbf{A}} \operatorname{ord}_{T=q^{-1}} g_{\mathbf{A}}(T) = \left|\left\{\mathbf{A} \in \mathcal{O}_q(\Lambda) \mid \mathbf{J}(\mathbf{a}) = q^{|\mathbf{A}|}\right\}\right| = |\mathcal{O}_q(\Lambda_0)|,$$

as claimed. Now, by definition of $P^*_\Lambda(T)$ and by construction of the decomposition of Λ, it follows that

$$\begin{aligned} P^*_\Lambda(T) = \frac{P(\Lambda, T)}{(1-qT)^\rho} &= \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda_0)} \frac{1 - \mathbf{J}(\mathbf{a})T^{|\mathbf{A}|}}{1 - qT} \cdot \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda^* \sqcup \Lambda')} \left(1 - \mathbf{J}(\mathbf{a})T^{|\mathbf{A}|}\right) \\ &= \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda_0)} \frac{1 - (qT)^{|\mathbf{A}|}}{1 - qT} \cdot \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda^*)} \left(1 - \mathbf{J}(\mathbf{a})T^{|\mathbf{A}|}\right). \end{aligned}$$

Evaluating this expression at $T = q^{-1}$ yields the desired result. □

In the following lemma, we record a few useful facts about the action of q on subsets of G_d.

LEMMA 3.6. *Let $\Lambda \subset G_d$ be a nonempty subset which is stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ by multiplication. The following upper bounds hold:*

(i) $\displaystyle\sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} |\mathbf{A}| = |\Lambda| \leq |\Lambda|,$

(ii) $\displaystyle\sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} 1 = |\mathcal{O}_q(\Lambda)| \ll \log q \cdot \frac{|\Lambda|}{\log|\Lambda|},$

(iii) $\displaystyle\sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log|\mathbf{A}| \ll \log q \cdot \frac{|\Lambda| \cdot \log\log|\Lambda|}{\log|\Lambda|}.$

All the involved constants are absolute and effective.

Proof. The first assertion (i) follows directly from the fact that the set $\mathcal{O}_q(\Lambda)$ can be written as a disjoint union of orbits under the action of q.

To prove (ii) and (iii), we introduce the following notation: for any divisor d' of d, we let

$$\Lambda_{d'} := \left\{ \mathbf{a} = (a_0, \dots, a_3) \in \Lambda \;\middle|\; \gcd(d, a_0, \dots, a_3) = d/d' \right\}.$$

It is clear that $\Lambda = \bigsqcup_{d'|d} \Lambda_{d'}$ and that the action of q on Λ can be restricted to each $\Lambda_{d'}$, yielding the decomposition $\mathcal{O}_q(\Lambda) = \bigsqcup_{d'|d} \mathcal{O}_q(\Lambda_{d'})$. We remark that $\Lambda_1 \subset \{(0,0,0,0)\}$ and $|\mathcal{O}_q(\Lambda_1)| \leq 1$: in what follows, we thus concentrate on divisors $d' \geq 2$ of d. Any orbit $\mathbf{A}$ containing an element $\mathbf{a} \in \Lambda_{d'}$ has length $|\mathbf{A}| = |\langle q \rangle_{d'}| = o_q(d')$: this implies that $|\mathcal{O}_q(\Lambda_{d'})| = |\Lambda_{d'}|/o_q(d')$. We also note that, by definition of $o_q(d')$, d' divides $q^{o_q(d')} - 1$ so that $\log d' \leq o_q(d') \cdot \log q$.

Putting these remarks together, we see that

$$|\mathcal{O}_q(\Lambda)| = \sum_{d'|d} |\mathcal{O}_q(\Lambda_{d'})| \leq 1 + \sum_{\substack{d'|d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{o_q(d')} \leq 1 + \log q \cdot \sum_{\substack{d'|d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{\log d'}.$$

Let $X \in [2, d]$ be a parameter, we split the last sum into two parts, which we estimate separately:

$$\sum_{\substack{d'|d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{\log d'} = \sum_{\substack{d'|d \\ 2 \leq d' \leq X}} \frac{|\Lambda_{d'}|}{\log d'} + \sum_{\substack{d'|d \\ d' > X}} \frac{|\Lambda_{d'}|}{\log d'}.$$

To bound the first sum, we remark that for each $d' \mid d$ (with $d' \geq 2$), $\Lambda_{d'}$ is in one-to-one correspondence with a subset of $(\mathbb{Z}/d'\mathbb{Z})^3$ so that $|\Lambda_{d'}| \leq {d'}^3$. Since the function $y \mapsto y^3/\log y$ is increasing on $[2, X]$, the first sum satisfies

$$\sum_{\substack{d'|d \\ 2 \leq d' \leq X}} \frac{|\Lambda_{d'}|}{\log d'} \leq \sum_{\substack{d'|d \\ 2 \leq d' \leq X}} \frac{{d'}^3}{\log d'} \leq \frac{X^3}{\log X} \cdot \sum_{\substack{d'|d \\ 2 \leq d' \leq X}} 1 \leq \frac{X^3}{\log X} \cdot \sum_{2 \leq d' \leq X} 1 \leq \frac{X^4}{\log X}.$$

To treat the second sum, we use the decomposition $\Lambda = \bigsqcup_{d'|d} \Lambda_{d'}$ and the fact that $y \mapsto (\log y)^{-1}$ is decreasing on $[X, +\infty)$:

$$\sum_{\substack{d'|d \\ d' > X}} \frac{|\Lambda_{d'}|}{\log d'} \leq \sum_{\substack{d'|d \\ d' > X}} \frac{|\Lambda_{d'}|}{\log X} \leq \frac{1}{\log X} \cdot \sum_{d'|d} |\Lambda_{d'}| \leq \frac{|\Lambda_d|}{\log X}.$$

Summing the two contributions and choosing $X = |\Lambda|^{1/4}$ leads to

$$|\mathcal{O}_q(\Lambda)| \leq 1 + \log q \cdot \frac{X^4 + |\Lambda|}{\log X} \leq 1 + 8 \log q \cdot \frac{|\Lambda|}{\log |\Lambda|} \ll \log q \cdot \frac{|\Lambda|}{\log |\Lambda|}.$$

This proves part (ii) of the Lemma (with a hidden absolute constant $c_5 \leq 9$) and we finally turn to the proof of part (iii). Again, we use the decomposition of $\mathcal{O}_q(\Lambda)$ as the disjoint union of $\mathcal{O}_q(\Lambda_{d'})$ (with $d' \mid d$) and the fact that the orbits of $\mathbf{a} \in \Lambda_{d'}$ all have the same length $o_q(d')$:

$$\sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log |\mathbf{A}| = \sum_{\substack{d'|d \\ d' \geq 2}} \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda_{d'})} \log |\mathbf{A}| = \sum_{\substack{d'|d \\ d' \geq 2}} |\mathcal{O}_q(\Lambda_{d'})| \cdot \log o_q(d') = \sum_{\substack{d'|d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{o_q(d')} \cdot \log o_q(d').$$

We introduce a new parameter $Y \in [3, d)$ and we split the sum into two parts according to the size of d' with respect to Y. To bound the sum over "small divisors" d' of d (*i.e.* $d' \mid d$ and $2 \leq d' \leq Y$), we use that $\log o_q(d') \leq \log \phi(d') \leq \log Y$ and we obtain that

$$\sum_{\substack{d'|d \\ 2 \leq d' \leq Y}} \frac{|\Lambda_{d'}|}{o_q(d')} \cdot \log o_q(d') \leq \log Y \cdot \sum_{\substack{d'|d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{o_q(d')} = \log Y \cdot \sum_{\substack{d'|d \\ d' \geq 2}} |\mathcal{O}_q(\Lambda_{d'})| \leq |\mathcal{O}_q(\Lambda)| \cdot \log Y.$$

The sum over "large divisors" of d (those $d' \mid d$ such that $d' > Y$) is bounded from above as follows. As was noted earlier in the proof, we have $o_q(d') \geq \log d'/\log q$ for all $d' \mid d$. If $d' > Y$, this implies that $(\log o_q(d'))/o_q(d') \leq \log q \cdot (\log\log Y)/\log Y$ because $x \mapsto (\log x)/x$ is decreasing on $[3, +\infty)$. It follows that

$$\sum_{\substack{d' \mid d \\ d' > Y}} \frac{|\Lambda_{d'}|}{o_q(d')} \cdot \log o_q(d') \leq \sum_{\substack{d' \mid d \\ d' > Y}} \frac{\log o_q(d')}{o_q(d')} \cdot |\Lambda_{d'}| \leq \log q \cdot \frac{\log\log Y}{\log Y} \cdot \sum_{\substack{d' \mid d \\ d' > Y}} |\Lambda_{d'}|$$
$$\leq \log q \cdot \frac{\log\log Y}{\log Y} \cdot \sum_{d' \mid d} |\Lambda_{d'}| = \log q \cdot \frac{\log\log Y}{\log Y} \cdot |\Lambda|.$$

From part (ii) that we have just proved, we deduce that

$$\sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log|\mathbf{A}| = \sum_{\substack{d' \mid d \\ d' \geq 2}} \frac{|\Lambda_{d'}|}{o_q(d')} \cdot \log o_q(d') \leq |\mathcal{O}_q(\Lambda)| \cdot \log Y + \log q \cdot \frac{\log\log Y}{\log Y} \cdot |\Lambda|$$
$$\leq \log q \cdot |\Lambda| \cdot \left(\frac{c_5}{\log|\Lambda|} + \frac{\log\log Y}{\log Y} \right).$$

The claimed bound now follows on taking $Y = |\Lambda|^{1/3}$ (with an absolute constant $c_6 \leq 12$). □

4. *An equidistribution statement*

Let us temporarily turn to a more combinatorial problem and consider subsets of $\mathbb{Z}/d\mathbb{Z}$. The fractional part of $x \in \mathbb{R}$ will be denoted by $\{x\}$. The map $m \in \mathbb{Z}/d\mathbb{Z} \mapsto \{m/d\}$ is well-defined and allows us to view subsets of $\mathbb{Z}/d\mathbb{Z}$ as sequences in $[0, 1]$: we may then study the distribution of subsets H_d of $\mathbb{Z}/d\mathbb{Z}$ when d grows. Of course, given a random set $H_d \subset \mathbb{Z}/d\mathbb{Z}$, there is no reason why H_d should be particularly well-distributed in $\mathbb{Z}/d\mathbb{Z}$.

Nonetheless, if H_d is a subset of $(\mathbb{Z}/d\mathbb{Z})^\times$ that is "not too small", we show that its "translates" $g \cdot H_d$ by $g \in (\mathbb{Z}/d\mathbb{Z})^\times$ are, on average, equidistributed in $\mathbb{Z}/d\mathbb{Z}$. More precisely, our result is:

THEOREM 4.1. *Let $F : [0, 1] \to \mathbb{R}$ be a function of bounded total variation on $[0, 1]$ and denote by $\mathscr{V}(F)$ its total variation. Let $\mathscr{D} \subset \mathbb{Z}_{\geq 1}$ be an infinite set of positive integers. For all $d \in \mathscr{D}$, suppose we are given a subset H_d of $(\mathbb{Z}/d\mathbb{Z})^\times$ and an element $a_d \in (\mathbb{Z}/d\mathbb{Z})^\times$; assume that*

$$|H_d|/\log\log d \xrightarrow[\substack{d \in \mathscr{D} \\ d \to \infty}]{} +\infty.$$

Then, for all $\varepsilon \in (0, 1/4)$, when $d \in \mathscr{D}$ goes to $+\infty$, one has

$$\frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \left| \int_0^1 F(t)\,\mathrm{d}t - \frac{1}{|H_d|} \sum_{h \in H_d} F\left(\left\{ \frac{a_d \cdot gh}{d} \right\} \right) \right| \leq c_7 \cdot \mathscr{V}(F) \cdot \left(\frac{\log\log d}{|H_d|} \right)^{1/4-\varepsilon}. \quad (4.1)$$

The constant $c_7 > 0$ is effective and depends at most on $\varepsilon > 0$. In particular, note that this upper bound is entirely independent of the choice of a_d.

This equidistribution theorem constitutes the main analytic input in the proof of our lower bound on special values (see Theorem 6.2), and may be of interest for other applications. See Lemma 7.10 in [**HP16**] for a related statement. This result applies in particular to continuously differentiable functions $F : [0, 1] \to \mathbb{R}$, in which case $\mathscr{V}(F)$ is simply $\int_0^1 |F'(t)|\,\mathrm{d}t$.

The author thanks Igor Shparlinski for pointing out the necessity of the two coprimality conditions (*viz.* "$a_d \in (\mathbb{Z}/d\mathbb{Z})^\times$" and "$H_d \subset (\mathbb{Z}/d\mathbb{Z})^\times$") without which equidistribution may

fail. Note that the outer average on $(\mathbb{Z}/d\mathbb{Z})^\times$ is also necessary, as exemplified by the case where $d_N = q^N - 1$ (with $q \geq 2$ a fixed integer, $N \in \mathbb{Z}_{\geq 1}$), $a_{d_N} = 1$ and $H_{d_N} = \langle q \rangle_{d_N} \subset (\mathbb{Z}/d_N\mathbb{Z})^\times$ for which the term corresponding to $g = 1 \in (\mathbb{Z}/d_N\mathbb{Z})^\times$ in (4.1) is not necessarily small.

The proof of Theorem 4.1 will occupy the rest of the present section.

4.1. *Fourier transform on $\mathbb{Z}/d\mathbb{Z}$*

Fix a positive integer $d \geq 2$, any function $\psi : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ has a Fourier transform $\widehat{\psi} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ defined by

$$\forall y \in \mathbb{Z}/d\mathbb{Z}, \qquad \widehat{\psi}(y) := \sum_{x \in \mathbb{Z}/d\mathbb{Z}} \psi(x) \cdot \mathbf{e}\left(\tfrac{xy}{d}\right),$$

where $\mathbf{e}(x) := \mathrm{e}^{2i\pi x}$ for all $x \in \mathbb{R}$. In this context, an analogue of *Plancherel's equality* holds:

$$\sum_{y \in \mathbb{Z}/d\mathbb{Z}} |\widehat{\psi}(y)|^2 = d \cdot \sum_{x \in \mathbb{Z}/d\mathbb{Z}} |\psi(x)|^2, \tag{4.2}$$

or, with more evocative notations, $\|\widehat{\psi}\|_2^2 = d \cdot \|\psi\|_2^2$.

Let $H \subset \mathbb{Z}/d\mathbb{Z}$ be a nonempty subset and denote by $\mathbb{1} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{R}$ the characteristic function of H. Clearly, we have $\|\widehat{\mathbb{1}}\|_\infty = \widehat{\mathbb{1}}(0) = |H|$, so that $\psi_H := \mathbb{1}(.)/|H|$ satisfies $\|\widehat{\psi_H}\|_\infty = 1$, where $\|\psi'\|_\infty := \max_x |\psi'(x)|$ denotes the sup-norm of a function ψ'.

LEMMA 4.2. *Let $d \geq 3$ be an integer and $H \subset \mathbb{Z}/d\mathbb{Z}$. For any $\beta \in (0, 1]$ and any $k \in \mathbb{Z}$ such that $k \not\equiv 0 \bmod d$, one has*

$$\frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \left|\widehat{\psi_H}(kg)\right| \leq \beta + \frac{d}{\phi(d)} \cdot \frac{\gcd(k,d)}{\beta^2 \cdot |H|}, \tag{4.3}$$

Proof. Let us cut the sum into two parts according to the given parameter $\beta \in (0, 1]$:

$$\sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} |\widehat{\psi_H}(kg)| = \sum_{g \text{ s.t. } |\widehat{\psi_H}(kg)| \leq \beta} |\widehat{\psi_H}(kg)| + \sum_{g \text{ s.t. } |\widehat{\psi_H}(kg)| > \beta} |\widehat{\psi_H}(kg)|.$$

The first sum is clearly $\leq \beta \cdot |(\mathbb{Z}/d\mathbb{Z})^\times| = \beta \cdot \phi(d)$. Since $\|\widehat{\psi_H}(y)\|_\infty \leq 1$, the second sum is bounded by:

$$\sum_{\substack{g \in (\mathbb{Z}/d\mathbb{Z})^\times \text{ s.t.} \\ |\widehat{\psi_H}(kg)| > \beta}} |\widehat{\psi_H}(kg)| \leq 1 \cdot \left| \left\{ g \in (\mathbb{Z}/d\mathbb{Z})^\times \;\middle|\; |\widehat{\psi_H}(kg)| > \beta \right\} \right|.$$

For any $y \in \mathbb{Z}/d\mathbb{Z}$, there are at most $\gcd(k, d)$ elements $g \in (\mathbb{Z}/d\mathbb{Z})^\times$ such that $kg = y$, so that

$$\left| \left\{ g \in (\mathbb{Z}/d\mathbb{Z})^\times \;\middle|\; |\widehat{\psi_H}(kg)| > \beta \right\} \right| \leq \gcd(k, d) \cdot \left| \left\{ y \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\widehat{\psi_H}(y)| > \beta \right\} \right|.$$

By Plancherel's equality (4.2), we have

$$\beta^2 \cdot \left| \left\{ y \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\widehat{\psi_H}(y)| > \beta \right\} \right| \leq \|\widehat{\psi_H}\|_2^2 = d \cdot \|\psi_H\|_2^2 \leq d \cdot |H| \cdot \|\psi_H\|_\infty^2 \leq d \cdot |H|^{-1}.$$

From which it follows that

$$\sum_{g \text{ s.t. } |\widehat{\psi_H}(kg)| > \beta} |\widehat{\psi_H}(kg)| \leq \frac{d}{|H|} \cdot \frac{\gcd(k,d)}{\beta^2}.$$

Adding the two contributions, we deduce that

$$\frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} |\widehat{\psi_H}(kg)| \leq \beta + \frac{d}{\phi(d) \cdot |H|} \cdot \frac{\gcd(k,d)}{\beta^2},$$

which concludes the proof of the Lemma. □

In our application of Lemma 4.2, we will need the following result of analytic number theory:

LEMMA 4.3. *There is an absolute effective constant $c_8 > 0$ such that, for all integers $d \geq 3$, one has $\frac{d}{\phi(d)} \leq c_8 \cdot \log\log d$.*

Proof. It follows from the proof of Theorem 428 of [**HW08**] that

$$\frac{d}{\phi(d)} < \left(1 - \frac{1}{\log d}\right)^{-\log d/\log\log d} \cdot \Big(\prod_{p \leq \log d} \left(1 - \tfrac{1}{p}\right)\Big)^{-1},$$

(*cf.* p.470 in §XXII.9 there). A straightforward analysis shows that $(1-1/x)^{-x/\log x} \leq 1$ for all $x \in [1,\infty)$. Moreover, Mertens' formula (see Theorem 1.12 in [**Ten15**]) implies that

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{\mathrm{e}^{-\gamma}}{\log x} \cdot \left(1 + O\left(\frac{1}{\log x}\right)\right),$$

for all $x \geq 2$, where γ denotes the Euler-Mascheroni constant. Being a little more careful (as in *loc. cit.*, Theorem 1.10), one can even show that the constant in the "O" can be chosen $\leq 2(1+\log 4) < 5$. It follows easily that, for all d such that $\log d > 5$, we have

$$\frac{d}{\phi(d) \cdot \log\log d} < \mathrm{e}^{\gamma} \cdot \left(1 + O\left(\frac{1}{\log\log d}\right)\right)^{-1} \leq \mathrm{e}^{\gamma} \cdot \left(1 + \frac{2}{\log\log d}\right).$$

Therefore, there exists a constant $c_8' > 0$ such that $\frac{d}{\phi(d)} \leq c_8' \cdot \log\log d$ for all $d \geq 150$.

One concludes by adjusting the value of c_8' to accommodate the smaller values of d. For completeness, we note that $c_8 = 10\mathrm{e}^{\gamma}$ is a suitable choice of constant. □

4.2. *Tools from equidistribution theory*

Before passing to the proof of Theorem 4.1, we recall the following two results about distribution of sequences in $[0,1]$. The reader may consult [**KN74**, Chap. 2] for more details and for proofs. For any finite sequence $x_1, x_2, \ldots, x_N$ of N points in $[0,1]$, we define its *discrepancy* by

$$D((x_n)_{n=1}^N) := \sup_{I \subset [0,1]} \left| \mu(I) - \frac{1}{N} \left| \{ n \in [\![1, N]\!] \mid x_n \in I \} \right| \right|,$$

the supremum being taken over all intervals $I \subset [0,1]$, whose length is denoted by $\mu(I)$. The inequality below can be viewed as a quantitative version of Weyl's criterion for equidistribution:

PROPOSITION 4.4 (Inequality of Erdös–Turán). *Let $x_1, \ldots, x_N$ be a sequence of N points in $[0,1]$. Then, for all integers $K \geq 1$, the discrepancy $D((x_n)_{n=1}^N)$ is bounded by*

$$D((x_n)_{n=1}^N) \leq \frac{6}{K+1} + \frac{4}{\pi} \sum_{k=1}^{K} \frac{1}{k} \left| \frac{1}{N} \sum_{n=1}^{N} \mathrm{e}^{2i\pi \cdot k \cdot x_n} \right|. \tag{4.4}$$

The next proposition comes from the world of numerical integration and roughly states that the average of a well-behaved function on $[0,1]$ can be approximated by averaging its values at finitely many points, provided that these points are sufficiently well-distributed.

PROPOSITION 4.5 (Koksma's inequality). *Let $F : [0,1] \to \mathbb{R}$ be a function of bounded total variation on $[0,1]$, and $x_1, \dots, x_N$ be a sequence of N points in $[0,1]$ with discrepancy $D((x_n)_{n=1}^N)$. Then, one has*

$$\left| \int_0^1 F(t)\,\mathrm{d}t - \frac{1}{N} \sum_{n=1}^{N} F(x_n) \right| \leq \mathscr{V}(F) \cdot D((x_n)_{n=1}^N), \tag{4.5}$$

where $\mathscr{V}(F)$ denotes the total variation of F.

4.3. *Proof of Theorem 4.1*

Let hypotheses be as in the statement of Theorem 4.1. For any $d \in \mathscr{D}$, we let

$$\Theta_d(a_d, H_d) := \frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \left| \int_0^1 F(t)\,\mathrm{d}t - \frac{1}{|H_d|} \sum_{h \in H_d} F\left(\left\{ \frac{a_d \cdot gh}{d} \right\} \right) \right|.$$

If F is constant, there's nothing to prove, for then $\Theta_d(a_d, H_d) = 0$. If not, dividing throughout by $\mathscr{V}(F) \neq 0$, we may assume that F has total variation $\mathscr{V}(F) = 1$. Since $a_d \in (\mathbb{Z}/d\mathbb{Z})^\times$, one sees that $\Theta_d(a_d, H_d) = \Theta_d(1, H_d)$ by reindexing the outer sum; thus, we need only prove that $\Theta_d(1, H_d)$ satisfies the desired bound. Whenever it is necessary, we will assume that $d \in \mathscr{D}$ is big enough that $\log\log d$ is positive.

For any $g \in (\mathbb{Z}/d\mathbb{Z})^\times$, let $(x_h)_{h \in H_d}$ be the finite sequence defined by $x_h = \{gh/d\} \in [0,1]$ for all $h \in H_d$. We successively use Koksma's inequality (Proposition 4.5) and the Erdös–Turán inequality (Proposition 4.4) on $(x_h)_{h \in H_d}$ to get

$$\begin{aligned} \left| \int_0^1 F(t)\,\mathrm{d}t - \frac{1}{|H_d|} \sum_{h \in H_d} F\left(\left\{ \frac{gh}{d} \right\} \right) \right| &\leq \mathscr{V}(F) \cdot D((x_h)_{h \in H_d}) = D((x_h)_{h \in H_d}) \\ &\leq \frac{6}{K+1} + \frac{4}{\pi} \sum_{k=1}^{K} \frac{1}{k} \left| \frac{1}{|H_d|} \sum_{h \in H_d} \mathbf{e}\left(k \cdot \left\{ \frac{gh}{d} \right\} \right) \right|, \end{aligned} \tag{4.6}$$

for all integers $K \geq 1$.

Denote by $\mathbb{1} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{R}$ the characteristic function of $H_d \subset (\mathbb{Z}/d\mathbb{Z})^\times$ seen as a subset of $\mathbb{Z}/d\mathbb{Z}$, and set $\psi_d := \mathbb{1}(.)/|H_d|$ as in subsection 4.1. Since $y \mapsto \{y\}$ is a 1-periodic function, the inner sums in (4.6) can be written as Fourier coefficients of ψ_d:

$$\forall k \geq 1, \quad \frac{1}{|H_d|} \sum_{h \in H_d} \mathbf{e}\left(k \cdot \left\{ \frac{gh}{d} \right\} \right) = \frac{1}{|H_d|} \sum_{h' \in \mathbb{Z}/d\mathbb{Z}} \mathbb{1}(h') \cdot \mathbf{e}\left(\frac{kgh'}{d} \right) = \widehat{\psi_d}(kg).$$

Using this expression and averaging inequalities (4.6) over $g \in (\mathbb{Z}/d\mathbb{Z})^\times$ yields

$$0 \leq \Theta_d(1, H_d) \leq \frac{6}{K+1} + \frac{4}{\pi} \sum_{k=1}^{K} \frac{1}{k} \cdot \left(\frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} |\widehat{\psi_d}(kg)| \right).$$

We now pick an integer $K \geq 1$ such that $K < d$. We can use Lemma 4.2 with all $k \in [\![1, K]\!]$ and plug (4.3) in the last displayed inequality: we obtain that, for all $\beta \in (0, 1]$,

$$\sum_{k=1}^{K} \frac{1}{k} \cdot \left(\frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} |\widehat{\psi_d}(-kg)| \right) \leq \sum_{k=1}^{K} \frac{1}{k} \cdot \left(\beta + \frac{d}{\phi(d)} \cdot \frac{\gcd(k,d)}{\beta^2 \cdot |H_d|} \right)$$
$$\leq \beta \cdot \log(K+1) + \frac{d}{\phi(d)} \cdot \frac{(K+1)}{\beta^2 \cdot |H_d|},$$

because $\gcd(k,d)/k \leq 1$ for all $k \geq 1$. Setting $K' = K + 1$ and $f(d) := (\log\log d)/|H_d|$, we deduce from Lemma 4.3 that

$$\Theta_d(1, H_d) \leq \frac{6}{K'} + \frac{4\beta}{\pi} \cdot \log K' + \frac{4c_8 f(d)}{\pi} \cdot \frac{K'}{\beta^2}.$$

By the hypothesis about the growth of $|H_d|$, we see that $f(d) \to 0^+$ when $d \to \infty$. Choosing $K' = K + 1 = \lfloor \mathrm{e}^{1/4-\varepsilon} \cdot f(d)^{-1/4+\varepsilon} \rfloor$ and $\beta = (3\pi/2) \cdot (K' \log K')^{-1}$ leads to the bound:

$$\Theta_d(1, H_d) \leq 12 \cdot f(d)^{1/4-\varepsilon} + \frac{c_8}{9\pi^3} \cdot f(d)^{1/4+3\varepsilon} \cdot (1 - \log f(d))^2.$$

Noticing that one has $0 \leq 1 - \log y \leq (2\varepsilon)^{-1} \cdot y^{-2\varepsilon}$ for all $y \in (0, +\infty)$, straightforward manipulations imply the upper bound that was announced in Theorem 4.1:

$$\Theta_d(1, H_d) \leq \left(12 + \frac{c_8}{36\pi^3} \cdot \varepsilon^{-2} \right) \cdot f(d)^{1/4-\varepsilon},$$

with an explicit expression for the constant c_7. □

5. *Upper bounds on the special value and on the "analytic rank"*

We now come back to studying the size of special values $P^*(\Lambda)$ as defined in section 3.1. The purpose of this section is twofold: we first prove an upper bound on $P^*(\Lambda)$ in terms of $|\Lambda|$; second, we bound $\mathrm{ord}_{T=q^{-1}} P(\Lambda, T)$ from above. The latter allows us to deduce an estimate on the Picard number of Fermat surfaces.

THEOREM 5.1. *Let $\mathbb{F}_q$ be a finite field and $d \geq 2$ be an integer coprime with q. Given a nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset $\Lambda \subset G_d$, consider the polynomial $P(\Lambda, T) \in \mathbb{Z}[T]$ associated to Λ as in Definition 3.1. The special value $P^*(\Lambda)$ of $P(\Lambda, T)$ satisfies*

$$\log |P^*(\Lambda)| \ll \log q \cdot |\Lambda| \cdot \frac{\log\log|\Lambda|}{\log|\Lambda|}. \tag{5.1}$$

Here, the implicit constant is absolute and effective.

Proof. We take the logarithm of the explicit expression of $P^*(\Lambda)$ obtained in Lemma 3.5 and use the triangle inequality, noting that $|\mathbf{J}(\mathbf{a})| = q^{|\mathbf{A}|}$ when $\mathbf{a} \in \Lambda^*$:

$$\log |P^*(\Lambda)| = \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda_0)} \log |\mathbf{A}| + \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda^*)} \log \left| 1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}} \right|$$
$$\leq \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log |\mathbf{A}| + \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda^*)} \log \left(1 + \frac{|\mathbf{J}(\mathbf{a})|}{q^{|\mathbf{A}|}} \right)$$
$$\leq \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log |\mathbf{A}| + \log 2 \cdot |\mathcal{O}_q(\Lambda^*)| \leq \sum_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \log |\mathbf{A}| + \log 2 \cdot |\mathcal{O}_q(\Lambda)|.$$

The estimates in items (ii) and (iii) in Lemma 3.6 then lead to:

$$\log|P^*(\Lambda)| \leq c_6 \log q \cdot \frac{|\Lambda| \cdot \log\log|\Lambda|}{\log|\Lambda|} + c_5 \log 2 \cdot \frac{\log q \cdot |\Lambda|}{\log|\Lambda|}.$$

This upper bound on $\log|P^*(\Lambda)|$ is stronger than the desired one. For completeness, we note that crude bounds lead to $\log|P^*(\Lambda)| \leq c_2 \cdot \log q \cdot |\Lambda| \cdot \log\log|\Lambda|/\log|\Lambda|$, where $c_2 \leq 19$. □

We record the following upper bound on the order of vanishing of $P(\Lambda, T)$ at $T = q^{-1}$:

Proposition 5.2. *Given a nonempty subset $\Lambda \subset G_d$ which is stable under multiplication by $(\mathbb{Z}/d\mathbb{Z})^\times$, the multiplicity of $T = q^{-1}$ as a root of $P(\Lambda, T)$ satisfies*

$$\operatorname{ord}_{T=q^{-1}} P(\Lambda, T) \ll \log q \cdot \frac{|\Lambda|}{\log|\Lambda|}. \tag{5.2}$$

Here too, the implicit constant is absolute and effective.

Proof. Recall that $\operatorname{ord}_{T=q^{-1}} P(\Lambda, T) = |\mathcal{O}_q(\Lambda_0)|$, with $\Lambda_0 = \left\{\mathbf{a} \in \Lambda \;\middle|\; \mathbf{J}_{\mathbf{a}} = q^{|\mathbf{A}|}\right\}$ (see Lemma 3.5) and note that $|\mathcal{O}_q(\Lambda_0)| \leq |\mathcal{O}_q(\Lambda)| \leq c_5 \log q \cdot \frac{|\Lambda|}{\log|\Lambda|}$ by item (ii) in Lemma 3.6. □

This proposition implies an upper bound on the Picard number $\rho(\mathcal{F}_d/\mathbb{F}_q)$ of Fermat surfaces:

Corollary 5.3. *For any finite field $\mathbb{F}_q$ and any integer $d \geq 2$ coprime with q, let $\mathcal{F}_d$ be the Fermat surface surface over $\mathbb{F}_q$. The rank $\rho(\mathcal{F}_d/\mathbb{F}_q)$ of the Néron–Severi group $\mathrm{NS}(\mathcal{F}_d)$ satisfies*

$$\rho(\mathcal{F}_d/\mathbb{F}_q) \ll \frac{\log q \cdot d^3}{\log d}, \tag{5.3}$$

for some (small) absolute constant.

Proof. Choose $\Lambda_{\mathcal{F}} = G_d$ and note that $|\Lambda_{\mathcal{F}}| = d^3$ in this case. As we have seen in Example 3.2, one has $P(\Lambda_{\mathcal{F}}, T) = P_2(\mathcal{F}_d/\mathbb{F}_q, T)$. Part (1) of the Artin–Tate Conjecture 2.1 implies that $\rho(\mathcal{F}_d/\mathbb{F}_q)$ equals the "analytic rank" $\operatorname{ord}_{T=q^{-1}} P_2(\mathcal{F}_d/\mathbb{F}_q, T)$. The corollary is then a direct consequence of Proposition 5.2 above (and the implicit absolute constant c_3 can be chosen $c_3 \leq 3$). □

One may compare the bound (5.3) to the "geometric" bound of Igusa [**Igu60**] which states that $\rho(\mathcal{F}_d/\mathbb{F}_q) \leq \dim \mathrm{H}^2(\mathcal{F}_d)$, *i.e.*

$$0 \leq \rho(\mathcal{F}_d/\mathbb{F}_q) \leq \rho(\overline{\mathcal{F}_d}/\overline{\mathbb{F}_q}) \leq \dim \mathrm{H}^2(\mathcal{F}_d) = (d-1)(d^2-3d+3) \leq (d-1)^3.$$

Moreover, as its name suggests, this latter bound does not "see" the "growth" of the rank of the successive Néron–Severi groups $\mathrm{NS}(\mathcal{F}_d \times_{\mathbb{F}_q} k)$ in a tower of finite extensions $k/\mathbb{F}_q$. The bound in Corollary 5.3 does provide some insight about this growth: for fixed q and d, it yields that $\rho(\mathcal{F}_d \times_{\mathbb{F}_q} k) \ll_{q,d} [k : \mathbb{F}_q]$ as $[k : \mathbb{F}_q] \to \infty$.

We can also prove that (5.3) is asymptotically optimal:

Proposition 5.4. *For any finite field $\mathbb{F}_q$, there are infinitely many integers d', prime to q, such that*

$$\rho(\mathcal{F}_{d'}/\mathbb{F}_q) \gg_q \frac{d'^3}{\log d'},$$

where the implied constant is effective and depends only on q.

Proof. For any integer $n \geq 1$, put $d_n = q^n + 1$. For such d_n, Lemma 8.2 in [Ulm02] proves that $o_q(d_n) = 2n$. Moreover, a theorem of Shafarevich and Tate shows that $\mathbf{J}(\mathbf{a}) = q^{|\mathbf{A}|}$ for all $\mathbf{a} \in G^\circ_{d_n}$ (see [ST67] or [Ulm02, Prop. 8.1]). Combining this with part (1) of the Artin–Tate Conjecture 2.1 and Lemma 3.5, we see that

$$\rho(\mathcal{F}_{d_n}/\mathbb{F}_q) = \operatorname{ord}_{T=q^{-1}} P_2(\mathcal{F}_{d_n}/\mathbb{F}_q, T) = |\mathcal{O}_q(G_{d_n})|.$$

On the other hand, with an argument similar to the proof of Lemma 3.6, it is possible to bound $|\mathcal{O}_q(G_{d_n})|$ from below as follows. For any divisor d' of d_n, let $H_{d'} = \{(a_0, \dots, a_3) \in G_{d_n} \mid \gcd(d, a_0, \dots, a_3) = d_n/d'\}$. Then

$$|\mathcal{O}_q(G_{d_n})| \geq \sum_{\substack{d'|d \\ d' \geq 2}} \frac{|H_{d'}|}{o_q(d')} \geq \frac{1}{o_q(d_n)} \cdot \sum_{\substack{d'|d \\ d' \geq 2}} |H_{d'}| = \frac{|G_{d_n}| - 1}{o_q(d_n)} = \frac{d_n^3 - 1}{2n} \gg_q \frac{d_n^3}{\log d_n}.$$

This proves that the integers $(d_n)_{n \geq 1}$ satisfy the statement of the Proposition. □

6. *Lower bounds on $P^*(\Lambda)$*

In this section, we prove lower bounds on special values $P^*(\Lambda)$ as defined in section 3.1. For the rest of this section, we fix a finite field $\mathbb{F}_q$ of characteristic p. Let us start by giving a "trivial" lower bound on $P^*(\Lambda)$, which could be called a "Liouville type" lower bound:

PROPOSITION 6.1. *Let $d \geq 2$ be an integer coprime with q, and Λ be a nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset of G_d. The special value $P^*(\Lambda)$ of the polynomial $P(\Lambda, T)$ associated to Λ satisfies:*

$$\log |P^*(\Lambda)| \geq -\log q \cdot |\Lambda| \qquad \textit{i.e.} \qquad |P^*(\Lambda)| \geq \frac{1}{q^{|\Lambda|}}. \tag{6.1}$$

Proof. By definition, $P^*(\Lambda)$ is the value at $T = q^{-1}$ of a polynomial with integral coefficients, namely $P^*_\Lambda(T)$. Thus, it is obvious that $|P^*_\Lambda(q^{-1})| \in \mathbb{Z}[q^{-1}]$ is of the form $N/q^{\deg P^*_\Lambda(T)}$ for some integer $N \geq 0$ prime to q. Since $P^*_\Lambda(T)$ does not vanish at $T = q^{-1}$, the numerator N is actually positive. Hence $N \geq 1$ and the lower bound follows from the simple observation that $\deg P^*_\Lambda(T) \leq \deg P(\Lambda, T) \leq |\Lambda|$. □

The lower bound (6.1) is sometimes far from the truth. Indeed, assume that d divides $q^n + 1$ for some $n \in \mathbb{Z}_{\geq 1}$, then the theorem of Shafarevich and Tate mentioned above (see [ST67]) states that $\mathbf{J}(\mathbf{a}) = q^{|\mathbf{A}|}$ for all $\mathbf{a} \in G^\circ_d$. Therefore, in this case, for any $\Lambda \subset G_d$ as above, the set Λ^* is empty and, by Lemma 3.5, the special value $P^*(\Lambda)$ is a positive integer:

$$\log |P^*(\Lambda)| = \log \prod_{\Lambda \in \mathcal{O}_q(\Lambda_0)} |\mathbf{A}| \geq 0.$$

We now set out to prove a lower bound on $P^*(\Lambda)$ refining (6.1) in a more general case:

THEOREM 6.2. *Let $d \geq 2$ be an integer coprime with q, and Λ be a nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset of G_d. Assume that, for all $\varepsilon \in (0, 1/4)$, there exists $u \in (0, 1)$ such that*

$$\frac{1}{|\Lambda|} \cdot \left| \left\{ (a_0, \dots, a_3) \in \Lambda^\circ \;\middle|\; \max_i \{\gcd(d, a_i)\} > d^u \right\} \right| \leq c' \cdot \left(\frac{\log \log d}{\log d} \right)^{1/4 - \varepsilon}, \tag{$\mathcal{H}$}$$

for some constant c'. Then, for all $\varepsilon \in (0, 1/4)$, the special value $P^*(\Lambda)$ of the polynomial $P(\Lambda, T)$ satisfies

$$\log|P^*(\Lambda)| \gg -\log q \cdot |\Lambda| \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon}, \tag{6.2}$$

the implicit (positive) constant being effective (and depending at most on p, ε, u and c').

The rest of this section is devoted to the proof of Theorem 6.2. It will essentially consists in two parts: the first one has an algebraic flavour (see Theorem 6.4) while the second is more analytic (see subsection 6.2).

Remark 6.3. The extra hypothesis ($\mathcal{H}$) is used in the analytic part of the proof of Theorem 6.2 to ensure that there are "few" $(a_0, \dots, a_3) \in \Lambda^\circ$ with a "large" $\max_i\{\gcd(d, a_i)\}$ (see the end of subsection 6.2). For an arbitrary nonempty subset $\Lambda \subset G_d$ which is $(\mathbb{Z}/d\mathbb{Z})^\times$-stable, there is no *a priori* reason why ($\mathcal{H}$) should hold.

Nonetheless, if $d \geq 2$ is a prime number with $d \neq p$, ($\mathcal{H}$) is automatic for any $\Lambda \subset G_d$ because in this case the set of $(a_0, \dots, a_3) \in \Lambda^\circ$ such that $\max_i\{\gcd(d, a_i)\} > 1$ is empty. More importantly, as we will show in Lemma 7.1, a strong form of hypothesis ($\mathcal{H}$) holds for $\Lambda = G_d$ for any $d \geq 2$ coprime with q.

6.1. *Lower bound on products*

Our first step towards Theorem 6.2 will be to prove:

Theorem 6.4. *Let $d \geq 2$ be an integer coprime with q, and Λ be any nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset of G_d. The special value $P^*(\Lambda)$ satisfies*

$$\log|P^*(\Lambda)| \geq -\log q \cdot w_p(\Lambda, d) \qquad \textit{i.e.} \qquad |P^*(\Lambda)| \geq \frac{1}{q^{w_p(\Lambda,d)}}, \tag{6.3}$$

where $w_p(\Lambda, d)$ is given by $w_p(\Lambda, d) := \sum_{\mathbf{a}\in\Lambda^\circ} w_p(\mathbf{a}, d)$ with $\Lambda^\circ = \Lambda \cap G_d^\circ$ and

$$w_p(\mathbf{a}, d) := \frac{1}{\phi(d)} \sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times} \max\left\{0, \sum_{i=0}^{3}\left(-\frac{1}{2} + \frac{1}{|\langle p\rangle_d|}\sum_{\pi\in\langle p\rangle_d}\left\{\frac{a_i\pi g}{d}\right\}\right)\right\}.$$

We note the (surprising?) fact that $w_p(\Lambda, d)$ does not depend on q, but only on p. Of course, the usefulness of Theorem 6.4 relies on our ability to find a good upper bound on $w_p(\Lambda, d)$. This question is addressed the next subsection, where we prove that $w_p(\Lambda, d)$ is $o(|\Lambda|)$ as $|\Lambda| \to \infty$, under the assumption of hypothesis ($\mathcal{H}$).

Proof. As we have seen (in Lemma 3.5), the special value $P^*(\Lambda)$ associated to Λ has the following shape:

$$P^*(\Lambda) = \prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda_0)} |\mathbf{A}| \cdot \prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}\left(1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right) = (\text{integer}) \cdot \prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}\left(1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right).$$

From this, we deduce that

$$\log|P^*(\Lambda)| = \log|\text{integer}| + \log\prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}\left|1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right| \geq \log\prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}\left|1 - \frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right|,$$

and we shall now find lower bounds on the product $\Pi^*_\Lambda := \prod_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)} \left(1-\mathbf{J}(\mathbf{a})q^{-|\mathbf{A}|}\right)$ on the right-hand side. This product Π^*_Λ is a nonzero element of $\mathbb{Z}[q^{-1}]$ and we need to bound from above the exponent of q appearing in its denominator. We split the proof of Theorem 6.4 into three parts.

First, we recall the following result of Shioda concerning Jacobi sums (see Proposition 2.1 in [Shi87]). For the convenience of the reader, we give a proof in our notations below. Let $K := \mathbb{Q}(\zeta_d)$ be the d-th cyclotomic field and $\mathfrak{p}$ be the prime ideal of K that lies under $\mathfrak{P}$ (see section 2.3). We denote by $\mathrm{ord}_\mathfrak{p} : K^* \to \mathbb{Z}$ the $\mathfrak{p}$-adic valuation.

Lemma 6.5 (Shioda). *Let $\mathbb{F}_q$ be a finite field, $d \geq 2$ be an integer coprime with q, and $\mathbf{a} \in G_d$ be such that $|\mathbf{J}(\mathbf{a})| = q^{|\mathbf{A}|}$ (i.e. $\mathbf{a} \in G_d^\circ$). Set $v_\mathbf{A} = \mathrm{ord}_p(q^{|\mathbf{A}|}) = [\mathbb{F}_{q^{|\mathbf{A}|}} : \mathbb{F}_p]$. Then either $\mathbf{J}(\mathbf{a}) = q^{|A|}$, or*

$$\log \mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right) \geq -(\log q^{|\mathbf{A}|}) \cdot \sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times} \max\left\{0, 1-\frac{\mathrm{ord}_\mathfrak{p}\,\mathbf{J}(g\cdot\mathbf{a})}{v_\mathbf{A}}\right\}. \tag{6.4}$$

Proof. Fix a set $g_1 = 1, g_2, \ldots, g_s \in (\mathbb{Z}/d\mathbb{Z})^\times$ of coset representatives of $\langle p\rangle_d$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. Hence $s = \phi(d)/o_p(d)$ where $o_p(d) = |\langle p\rangle_d|$ is the multiplicative order of $p \bmod d$. For any $g \in (\mathbb{Z}/d\mathbb{Z})^\times$, we denote by $\sigma_g \in \mathrm{Gal}(K/\mathbb{Q})$ the corresponding automorphism of K in the usual isomorphism. Now let $\mathfrak{p}_i := (\sigma_{g_i})^{-1}(\mathfrak{p})$ for $i = 1, \ldots, s$: it is well-known that p decomposes as $p\cdot\mathbb{Z}[\zeta_d] = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$ in $\mathbb{Z}[\zeta_d]$ and that $\mathbf{N}\mathfrak{p}_i = \mathbf{N}\mathfrak{p} = p^{o_p(d)}$ for all i (see [IR90, Chap. 13]).

Noting that $\mathrm{ord}_\mathfrak{p}\, q^{|\mathbf{A}|} = v_\mathbf{A}$, it is clear that $q^{|\mathbf{A}|}\cdot\mathbb{Z}[\zeta_d]$ decomposes as $q^{|\mathbf{A}|}\cdot\mathbb{Z}[\zeta_d] = \prod_{i=1}^s \mathfrak{p}_i^{v_\mathbf{A}}$. Since $|\mathbf{J}(\mathbf{a})| = q^{|\mathbf{A}|} = p^{v_\mathbf{A}}$, the integral ideal of $\mathbb{Z}[\zeta_d]$ generated by $\mathbf{J}(\mathbf{a})$ is concentrated above p: its decomposition as a product of prime ideals takes the form $\mathbf{J}(\mathbf{a})\cdot\mathbb{Z}[\zeta_d] = \prod_{i=1}^s \mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}\mathbf{J}(\mathbf{a})}$. Further, for all $i \in [\![1, s]\!]$, one has $\mathrm{ord}_{\mathfrak{p}_i}\mathbf{J}(\mathbf{a}) = \mathrm{ord}_{\sigma_{g_i}^{-1}(\mathfrak{p})}\mathbf{J}(\mathbf{a}) = \mathrm{ord}_\mathfrak{p}(\sigma_{g_i}\mathbf{J}(\mathbf{a})) = \mathrm{ord}_\mathfrak{p}\mathbf{J}(g_i\cdot\mathbf{a})$, where the last equality follows from (2.7). Let us assume that $\mathbf{J}(\mathbf{a}) \neq q^{|\mathbf{A}|}$ and set

$$I_\mathbf{a} = \prod_{i=1}^s \mathfrak{p}_i^{\min\{v_\mathbf{A}, \mathrm{ord}_\mathfrak{p}\mathbf{J}(g_i\cdot\mathbf{a})\}} = \prod_{g\in(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d} (\sigma_g^{-1}\mathfrak{p})^{\min\{v_\mathbf{A}, \mathrm{ord}_\mathfrak{p}\mathbf{J}(g\cdot\mathbf{a})\}}.$$

By construction, $I_\mathbf{a}$ is an integral ideal of $\mathbb{Z}[\zeta_d]$ that divides the nonzero ideal generated by $(q^{|\mathbf{A}|} - \mathbf{J}(\mathbf{a}))$ in $\mathbb{Z}[\zeta_d]$. In particular, $\mathbf{N}I_\mathbf{a} \leq \mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{A}|} - \mathbf{J}(\mathbf{a}))$ in $\mathbb{Z}$, which yields

$$\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right) = \frac{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{A}|}-\mathbf{J}(\mathbf{a}))}{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{A}|})} \geq \frac{\mathbf{N}I_\mathbf{a}}{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{A}|})} = \frac{1}{q^{|\mathbf{A}|\cdot\phi(d)}\cdot(\mathbf{N}I_\mathbf{a})^{-1}}.$$

Together with a straightforward computation of $\mathbf{N}I_\mathbf{a}$, this inequality implies that

$$\log \mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right) \geq -\log q^{|\mathbf{A}|}\cdot o_p(d)\cdot\sum_{i=1}^s \max\left\{0, 1-\frac{\mathrm{ord}_\mathfrak{p}\mathbf{J}(g_i\cdot\mathbf{a})}{v_\mathbf{A}}\right\}.$$

Finally, since the elements g_i were chosen to be representatives of $(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d$ and since $\mathbf{J}(p^j\cdot\mathbf{a}) = \mathbf{J}(\mathbf{a})$ for all $j \geq 0$, the right-hand side of the above inequality can be rewritten as:

$$\begin{aligned} o_p(d)\cdot\sum_{i=1}^s \max\left\{0, 1-\frac{\mathrm{ord}_\mathfrak{p}\mathbf{J}(g_i\cdot\mathbf{a})}{v_\mathbf{A}}\right\} &= |\langle p\rangle_d|\cdot\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d} \max\left\{0, 1-\frac{\mathrm{ord}_\mathfrak{p}\mathbf{J}(g\cdot\mathbf{a})}{v_\mathbf{A}}\right\} \\ &= \sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times} \max\left\{0, 1-\frac{\mathrm{ord}_\mathfrak{p}\mathbf{J}(g\cdot\mathbf{a})}{v_\mathbf{A}}\right\}. \end{aligned}$$

Combining the last two displayed relations, the Lemma immediately follows. □

We also need a more explicit expression of the $\mathfrak{p}$-adic valuations $\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot\mathbf{a})$ appearing in the previous lemma:

LEMMA 6.6 (Stickelberger). *Let $\mathfrak{p}$ be as above. For any $\mathbf{b}=(b_0,\dots,b_3)\in G_d^\circ\subset G_d$, set $v_{\mathbf{B}}=\mathrm{ord}_p(q^{|\mathbf{B}|})=[\mathbb{F}_{q^{|\mathbf{B}|}}:\mathbb{F}_p]$. The $\mathfrak{p}$-adic valuation of the Jacobi sum $\mathbf{J}(\mathbf{b})$ is given by*

$$\frac{\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(\mathbf{b})}{v_{\mathbf{B}}}=\frac{1}{|\langle p\rangle_d|}\cdot\sum_{\pi\in\langle p\rangle_d}\left(3-\sum_{i=0}^{3}\left\{\frac{b_i\cdot\pi}{d}\right\}\right).$$

Proof. For the duration of the proof, we set $Q=q^{o_q(d)}$, $v=[\mathbb{F}_Q:\mathbb{F}_p]=\mathrm{ord}_p\,Q$ and $q'=q^{|\mathbf{B}|}$. The computation of the $\mathfrak{p}$-adic valuations of Gauss sums leading to Stickelberger's theorem (as in [**IR90**, Chap. 14] or [**Lan94**, IV, §3]) implies that the Jacobi sum $\mathbf{J}_Q(\mathbf{b})$ (relative to $\mathbb{F}_Q$) has $\mathfrak{p}$-adic valuation:

$$\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}_Q(\mathbf{b})=\sum_{j=0}^{v-1}\left(-1+\sum_{i=0}^{3}\left\{\frac{-b_i\cdot p^j}{d}\right\}\right).$$

Given the properties of $\mathrm{ord}_{\mathfrak{p}}$ and the relation of Davenport–Hasse (which here reads: $\mathbf{J}_Q(\mathbf{b})=\big(\mathbf{J}_{q'}(\mathbf{b})\big)^{[\mathbb{F}_Q:\mathbb{F}_{q'}]}$, see (2.8)), the expression above yields that

$$\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(\mathbf{b})=\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}_{q'}(\mathbf{b})=\frac{1}{[\mathbb{F}_Q:\mathbb{F}_{q'}]}\,\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}_Q(\mathbf{b})=\frac{1}{[\mathbb{F}_Q:\mathbb{F}_{q'}]}\sum_{j=0}^{v-1}\left(-1+\sum_{i=0}^{3}\left\{\frac{-b_i\cdot p^j}{d}\right\}\right). \tag{6.5}$$

We now rearrange this raw expression. First, there may be repetitions in the sum over j: since $v=\mathrm{lcm}([\mathbb{F}_q:\mathbb{F}_p],o_p(d))$, v is a multiple of $o_p(d)$. By construction, d divides $p^{o_p(d)}-1$ and any multiple thereof: it follows that we may reindex the sum over $j\in[\![0,v-1]\!]$ into a sum over $\pi\in\langle p\rangle_d$ and obtain

$$\sum_{j=0}^{v-1}\left(-1+\sum_{i=0}^{3}\left\{\frac{-b_i\cdot p^j}{d}\right\}\right)=\frac{v}{o_p(d)}\cdot\sum_{\pi\in\langle p\rangle_d}\left(-1+\sum_{i=0}^{3}\left\{\frac{-b_i\cdot\pi}{d}\right\}\right). \tag{6.6}$$

Secondly, we note that $\{-y\}=1-\{y\}$ for all $y\in\mathbb{R}\smallsetminus\mathbb{Z}$ and that $-b_i\cdot\pi/d$ is never an integer for $\pi\in\langle p\rangle_d$ and $\mathbf{b}\in G_d^\circ$. This leads to

$$\sum_{\pi\in\langle p\rangle_d}\left(-1+\sum_{i=0}^{3}\left\{\frac{-b_i\cdot\pi}{d}\right\}\right)=\sum_{\pi\in\langle p\rangle_d}\left(3-\sum_{i=0}^{3}\left\{\frac{b_i\cdot\pi}{d}\right\}\right). \tag{6.7}$$

To conclude, one only needs to combine (6.6) and (6.7) with (6.5), and to remember that

$$\frac{v}{o_p(d)\cdot[\mathbb{F}_Q:\mathbb{F}_{q'}]}=\frac{[\mathbb{F}_Q:\mathbb{F}_p]}{o_p(d)\cdot[\mathbb{F}_Q:\mathbb{F}_{q'}]}=\frac{[\mathbb{F}_{q'}:\mathbb{F}_p]}{o_p(d)}=\frac{v_{\mathbf{B}}}{|\langle p\rangle_d|}.$$

□

We can now finish the proof of Theorem 6.4. As was already noted at the beginning of this subsection, the desired lower bound on $P^*(\Lambda)$ follows from one on Π_Λ^*. Again by (2.7), the hypothesis that Λ be stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ implies the rationality of Π_Λ^*. In particular, we get:

$$\log|P^*(\Lambda)|\geq\log|\Pi_\Lambda^*|=\frac{\log\mathbf{N}_{K/\mathbb{Q}}(\Pi_\Lambda^*)}{[K:\mathbb{Q}]}=\frac{1}{[K:\mathbb{Q}]}\sum_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}\log\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(\mathbf{a})}{q^{|\mathbf{A}|}}\right).$$

We now use Lemma 6.5 on each term of the sum:

$$\begin{aligned}\log|\Pi_\Lambda^*| &\geq \frac{1}{[K:\mathbb{Q}]}\sum_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)} -\log(q^{|\mathbf{A}|})\cdot\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot\mathbf{a})}{v_{\mathbf{A}}}\right\}\\ &\geq \frac{-\log q}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\sum_{\mathbf{A}\in\mathcal{O}_q(\Lambda^*)}|\mathbf{A}|\cdot\max\left\{0,1-\frac{\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot\mathbf{a})}{v_{\mathbf{A}}}\right\}\\ &= \frac{-\log q}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\sum_{\mathbf{a}\in\Lambda^*}\max\left\{0,1-\frac{\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot\mathbf{a})}{v_{\mathbf{A}}}\right\}. \qquad (6.8)\end{aligned}$$

For all $\mathbf{b}\in G_d^\circ\subset G_d$, Lemma 6.6 implies that

$$1-\frac{\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(\mathbf{b})}{v_{\mathbf{B}}} = 1-\frac{1}{|\langle p\rangle_d|}\cdot\sum_{\pi\in\langle p\rangle_d}\left(3-\sum_{i=0}^{3}\left\{\frac{b_i\pi}{d}\right\}\right) = \sum_{i=0}^{3}\left(-\frac{1}{2}+\frac{1}{|\langle p\rangle_d|}\sum_{\pi\in\langle p\rangle_d}\left\{\frac{b_i\pi}{d}\right\}\right).$$

Plugging this into (6.8) with $\mathbf{b}=g\cdot\mathbf{a}\in\Lambda^*\subset G_d^\circ$ and exchanging the order of summation, we obtain

$$\log|\Pi_\Lambda^*|\geq -(\log q)\cdot\sum_{\mathbf{a}\in\Lambda^*}w_p(\mathbf{a},d)\geq -(\log q)\cdot\sum_{\mathbf{a}\in\Lambda^\circ}w_p(\mathbf{a},d) = -(\log q)\cdot w_p(\Lambda,d),$$

because the terms $w_p(\mathbf{a},d)$ that are added are nonnegative.

This concludes the proof of Theorem 6.4. □

6.2. *Proof of Theorem 6.2*

Let d and Λ be as in the statement of Theorem 6.2. Recall that $w_p(\Lambda,d)$ is the sum over all $\mathbf{a}\in\Lambda^\circ$ of $w_p(\mathbf{a},d)$, where for all $\mathbf{a}=(a_0,\dots,a_3)\in G_d^\circ$,

$$w_p(\mathbf{a},d)=\frac{1}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,\sum_{i=0}^{3}\left(-\frac{1}{2}+\frac{1}{|\langle p\rangle_d|}\sum_{\pi\in\langle p\rangle_d}\left\{\frac{a_i\pi g}{d}\right\}\right)\right\}.$$

In the course of proving Theorem 6.4 (see especially (6.8) and the following lines), we have essentially obtained the following alternative expression for $w_p(\mathbf{a},d)$:

$$w_p(\mathbf{a},d)=\frac{1}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot\mathbf{a})}{v_{\mathbf{A}}}\right\}.$$

Notice that $\operatorname{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot\mathbf{a})\geq 0$ since the Jacobi sum is an algebraic integer. We deduce that $w_p(\mathbf{a},d)$ satisfies a trivial upper bound:

$$\forall\mathbf{a}\in G_d^\circ,\qquad 0\leq w_p(\mathbf{a},d)\leq 1. \qquad (6.9)$$

Therefore, $w_p(\Lambda,d)$ satisfies $0\leq w_p(\Lambda,d)\leq|\Lambda|$. Proving Theorem 6.2 comes down to showing that, assuming ($\mathcal{H}$), $w_p(\Lambda;d)$ satisfies the improved upper bound:

$$w_p(\Lambda,d)=\sum_{\mathbf{a}\in\Lambda^\circ}w_p(\mathbf{a},d)\ll_{p,\varepsilon}|\Lambda|\cdot\left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon}$$

That is, we have to show that $w_p(\mathbf{a},d)$ is "often small". With the help of Theorem 4.1, we start by showing that this is indeed the case for certain $\mathbf{a}\in G_d^\circ$.

LEMMA 6.7. *Let $d \geq 2$ be an integer, coprime with q. For an element $\mathbf{a} = (a_0, \dots, a_3) \in G_d^\circ$, set $d_i = \gcd(d, a_i)$ and $d' = d/\max\{d_0, \dots, d_3\}$. Then, for all $\varepsilon \in (0, 1/4)$, one has*

$$w_p(\mathbf{a}, d) \leq c_9 \cdot \left(\frac{\log\log d'}{\log d'}\right)^{1/4-\varepsilon},$$

where the constant $c_9 > 0$ is effective and depends at most on p and ε.

Proof. Let $F : [0,1] \to \mathbb{R}$, $x \mapsto x$, and

$$\forall a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}, \qquad \theta_p(a,d) := \frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \left| \int_{[0,1]} F - \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} F\left(\left\{\frac{a\pi g}{d}\right\}\right) \right|. \quad (6.10)$$

Observe that, for all $a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ and for all common divisors δ of a and d, one has $\theta_p(a,d) = \theta_p(a/\delta, d/\delta)$. Indeed, $\langle p \rangle_{d/\delta}$ is the image of $\langle p \rangle_d$ under the natural surjective morphism $(\mathbb{Z}/d\mathbb{Z})^\times \to (\mathbb{Z}/(d/\delta)\mathbb{Z})^\times$, which leads to

$$\frac{1}{|\langle p \rangle_{d/\delta}|} \sum_{\pi' \in \langle p \rangle_{d/\delta}} \left\{\frac{(a/\delta)\pi'}{d/\delta}\right\} = \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} \left\{\frac{a\pi}{d}\right\},$$

and similarly for the outer average on $(\mathbb{Z}/d\mathbb{Z})^\times$ in (6.10). In particular, if we set $a' = a/\gcd(d,a)$ and $d' = d/\gcd(d,a)$, then we have $\theta_p(a,d) = \theta_p(a',d')$.

The upshot of this manipulation is that $\gcd(a',d') = 1$: we may now apply our equidistribution result (Theorem 4.1) on $\theta_p(a',d')$ with $H_{d'} := \langle p \rangle_{d'}$, seen as a subset of $(\mathbb{Z}/d'\mathbb{Z})^\times$. Then, one has $|H_{d'}| \geq \log d'/\log p$ because d' divides $p^{|H_{d'}|} - 1$, by definition of $o_p(d') = |\langle p \rangle_{d'}|$.

In this situation, Theorem 4.1 yields that, for all $a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$,

$$\theta_p(a',d') \leq c_7 \cdot (\log p)^{1/4-\varepsilon} \cdot E(d') \quad \text{where we have put } E(d') := \left(\frac{\log\log d'}{\log d'}\right)^{1/4-\varepsilon},$$

and where the constant c_7 depends at most on ε.

Now let $\mathbf{a} \in G_d^\circ$ be as in the statement of the Lemma. Since $\max\{0, y\} \leq |y|$ for all $y \in \mathbb{R}$, the triangle inequality gives that

$$w_p(\mathbf{a}, d) \leq \frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \left| \sum_{i=0}^{3} \left(-\frac{1}{2} + \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} \left\{\frac{a_i \pi g}{d}\right\} \right) \right| \leq \sum_{i=0}^{3} \theta_p(a_i, d).$$

Upon applying Theorem 4.1 to each $a_i \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ as in the previous paragraph, we get

$$w_p(\mathbf{a}, d) \leq \sum_{i=0}^{3} \theta_p(a_i, d) \leq c_7 \cdot (\log p)^{1/4-\varepsilon} \cdot \sum_{i=0}^{3} E(d/d_i) \leq 4c_7 \cdot (\log p)^{1/4-\varepsilon} \cdot E(d/\max_i\{d_i\}),$$

because $n \mapsto E(n)$ is a decreasing function. Taking $c_9 = 4c_7 \cdot (\log p)^{1/4-\varepsilon}$ concludes the proof. □

In the case that d is assumed to be prime, the proof of Theorem 6.2 follows directly from Lemma 6.7 without extra hypotheses on Λ. Indeed, for a prime d and for any nonempty $(\mathbb{Z}/d\mathbb{Z})^\times$-stable subset $\Lambda \subset G_d$, all the elements $\mathbf{a} = (a_0, \dots, a_3) \in \Lambda \cap G_d^\circ$ have $\max_i\{\gcd(d, a_i)\} = 1$. Thus, Lemma 6.7 implies that, for all $\varepsilon \in (0, 1/4)$, one has

$$w_p(\Lambda, d) = \sum_{\mathbf{a} \in \Lambda^\circ} w_p(\mathbf{a}, d) \leq \sum_{\mathbf{a} \in \Lambda^\circ} c_9 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon} \leq c_9 \cdot |\Lambda| \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon},$$

as claimed. In the general case, we use hypothesis ($\mathcal{H}$) to control the proportion of terms $\mathbf{a} \in \Lambda^\circ$ for which Lemma 6.7 provides no improvement on the trivial upper bound (6.9).

Proof of Theorem 6.2. Let $d \geq 2$ be any integer prime to q, $\Lambda \subset G_d$ be a nonempty subset which is $(\mathbb{Z}/d\mathbb{Z})^\times$-stable and satisfies hypothesis ($\mathcal{H}$), and $\varepsilon \in (0, 1/4)$. For $X \in (1, d)$, define two subsets of Λ°:

$$\Lambda^\bullet(X) = \Big\{(a_0, \dots, a_3) \in \Lambda^\circ \;\Big|\; \max_i\{\gcd(d, a_i)\} \leq X\Big\}$$

and $\Lambda^\dagger(X) := \Lambda^\circ \smallsetminus \Lambda^\bullet(X) = \big\{\mathbf{a} \in \Lambda^\circ \;\big|\; \max_i\{\gcd(d, a_i)\} > X\big\}$.

We start by cutting the sum $w_p(\Lambda, d)$ into two parts:

$$w_p(\Lambda, d) = \sum_{\mathbf{a}\in\Lambda^\circ} w_p(\mathbf{a}, d) = \sum_{\mathbf{a}\in\Lambda^\bullet(X)} w_p(\mathbf{a}, d) + \sum_{\mathbf{a}\in\Lambda^\dagger(X)} w_p(\mathbf{a}, d).$$

Since $w_p(\mathbf{a}, d)$ satisfies the trivial bound (6.9), the second sum is less than $|\Lambda^\dagger(X)|$. To bound the first sum, we make use of Lemma 6.7 and of the bound $|\Lambda^\bullet(X)| \leq |\Lambda|$; which yields

$$\sum_{\mathbf{a}\in\Lambda^\bullet(X)} w_p(\mathbf{a}, d) \leq \sum_{\mathbf{a}\in\Lambda^\bullet(X)} c_9 \cdot \left(\frac{\log\log(d/X)}{\log(d/X)}\right)^{1/4-\varepsilon} \leq c_9 \cdot |\Lambda| \cdot \left(\frac{\log\log(d/X)}{\log(d/X)}\right)^{1/4-\varepsilon}.$$

Summing the two contributions, we arrive at:

$$w_p(\Lambda, d) = \sum_{\mathbf{a}\in\Lambda^\circ} w_p(\mathbf{a}, d) \leq |\Lambda| \cdot \left(c_9 \cdot \left(\frac{\log\log(d/X)}{\log(d/X)}\right)^{1/4-\varepsilon} + \frac{|\Lambda^\dagger(X)|}{|\Lambda|}\right).$$

By Hypothesis ($\mathcal{H}$), for the given $\varepsilon \in (0, 1/4)$ there exists $u \in (0, 1)$ and a constant c' such that $|\Lambda^\dagger(d^u)|/|\Lambda| \leq c' \cdot \big(\frac{\log\log d}{\log d}\big)^{1/4-\varepsilon}$. Therefore, on choosing $X = d^u$, we obtain that

$$\frac{w_p(\Lambda, d)}{|\Lambda|} \leq \frac{c_9}{1-u} \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon} + c' \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon}.$$

Setting $c_1 = c_9/(1-u) + c' > 0$, we have proved the claimed lower bound on $P^*(\Lambda)$. □

7. *Conclusion*

Let us recapitulate the results we have obtained so far. Let $\mathbb{F}_q$ be a finite field of characteristic p, $d \geq 2$ be an integer prime to q and denote by $\mathcal{F}_d/\mathbb{F}_q$ the Fermat surface of degree d over $\mathbb{F}_q$. In the notations of sections 2.3 and 3.1, Theorem 2.3 and Example 3.2 show that $P_2(\mathcal{F}_d/\mathbb{F}_q, T) = P(G_d, T)$. On the one hand, the special value satisfies

$$P^*(G_d) = P_2^*(\mathcal{F}_d/\mathbb{F}_q, q^{-1}) = \frac{|\operatorname{Br}(\mathcal{F}_d)| \cdot \operatorname{Reg}(\mathcal{F}_d)}{q^{p_g(\mathcal{F}_d)}} \in \mathbb{Z}[q^{-1}] \smallsetminus \{0\}$$

by the Artin–Tate Conjecture (Theorem 2.5 and Proposition 2.6); hence one has

$$\frac{\log\big(|\operatorname{Br}(\mathcal{F}_d)| \cdot \operatorname{Reg}(\mathcal{F}_d)\big)}{\log q^{p_g(\mathcal{F}_d)}} = 1 + \frac{p_g(\mathcal{F}_d)}{|G_d|} \cdot \frac{\log|P^*(G_d)|}{\log q^{|G_d|}}. \tag{7.1}$$

On the other hand, provided that $\Lambda = G_d$ satisfies hypothesis ($\mathcal{H}$), we have proved that

$$\forall \varepsilon \in (0, 1/4), \quad -c_1 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon} \leq \frac{\log|P^*(G_d)|}{\log q^{|G_d|}} \leq c_2 \cdot \frac{\log\log|G_d|}{\log|G_d|}, \tag{7.2}$$

for some constants c_1, c_2 depending on q, p and ε (combine Theorems 5.1 and 6.2).

Since $|G_d| = d^3$ and $p_g(\mathcal{F}_d) \sim d^3/6$ as $d \to \infty$, the identity (7.1) and the inequalities (7.2) directly imply our main result (Theorem 1.3). Consequently, there only remains to prove that G_d indeed satisfies ($\mathcal{H}$) for any integer $d \geq 2$ coprime with q.

LEMMA 7.1. *Let $d \geq 2$ be an integer and, for $X \in (1, d)$, define the subset*

$$G_d^\dagger(X) := \left\{(a_0, \dots, a_3) \in G_d \;\middle|\; d > \max_i\{\gcd(d, a_i)\} > X\right\} \subset G_d^\circ.$$

Then, for all $u \in (0, 1)$, there exists a constant c_9 depending only on u such that

$$|G_d^\dagger(d^u)| \leq c_9 \cdot d^{-u/2} \cdot |G_d|. \tag{7.3}$$

In particular, G_d satisfies hypothesis ($\mathcal{H}$).

Proof. For any divisor g of d and $i \in [\![0, 3]\!]$, let $H_i(g)$ be the subgroup of G_d defined by

$$H_i(g) = \left\{(a_0, \dots, a_3) \in G_d \;\middle|\; a_i \equiv 0 \bmod g\right\}.$$

Since the group homomorphism $G_d \to \mathbb{Z}/g\mathbb{Z}$ given by $\mathbf{a} \mapsto a_i \bmod g$ is surjective with kernel $H_i(g)$, the isomorphism theorem yields that $|H_i(g)| = |G_d|/g = d^3/g$.

On the other hand, one has

$$\begin{aligned}|G_d^\dagger(X)| &= \sum_{\substack{g|d \\ X<g<d}} \left|\left\{\mathbf{a} \in G_d \middle| \max_i\{\gcd(d, a_i)\} = g\right\}\right| \leq \sum_{\substack{g|d \\ X<g<d}} \sum_{i=0}^{3} \left|\left\{\mathbf{a} \in G_d \middle| \gcd(d, a_i) = g\right\}\right| \\ &\leq \sum_{\substack{g|d \\ X<g<d}} \sum_{i=0}^{3} |H_i(g)| = \sum_{i=0}^{3} \sum_{\substack{g|d \\ X<g<d}} \frac{|G_d|}{g} \leq 4 \cdot \frac{|G_d|}{X} \cdot \left|\{g \in [\![X, d]\!] \text{ such that } g \mid d\}\right|.\end{aligned}$$

The set $\{g \in [\![X, d]\!] \text{ such that } g \mid d\}$ has less than $\tau(d)$ elements, where $\tau(d)$ denotes the number of divisors of d. Further more, a classical result states that for all $v > 0$, there is an explicit constant c_v such that $\tau(d) \leq c_v \cdot d^v$ for all $d \geq 2$ (see Theorem 325 and (18.1.3) in its proof in [**HW08**]). In particular, for $v = u/2 > 0$, we deduce from we have proved that

$$|G_d(d^u)| \leq 4 \cdot \frac{|G_d|}{d^u} \cdot \tau(d) \leq 4c_{u/2} \cdot d^{-u/2} \cdot |G_d|,$$

which is the claimed upper bound (7.3). Hypothesis ($\mathcal{H}$) for G_d follows directly from (7.3) since for all $\varepsilon \in (0, 1/4)$ and all $u \in (0, 1)$, one has $d^{-u/2} = o\big(\big(\frac{\log\log d}{\log d}\big)^{1/4-\varepsilon}\big)$ as $d \to \infty$. □

Finally, putting (7.1) and (7.2) together, we obtain a quantitative version of Theorem 1.3:

COROLLARY 7.2. *Let $\mathbb{F}_q$ be a finite field of characteristic p, and $\varepsilon \in (0, 1/4)$. For an integer $d \geq 2$ prime to q, as $d \to \infty$, one has*

$$\frac{\log\left(|\operatorname{Br}(\mathcal{F}_d)| \cdot \operatorname{Reg}(\mathcal{F}_d)\right)}{\log q^{p_g(\mathcal{F}_d)}} = 1 + \frac{\log P^*(G_d)}{\log q^{p_g(\mathcal{F}_d)}} = 1 + O\Big(\Big(\frac{\log\log d}{\log d}\Big)^{1/4-\varepsilon}\Big), \tag{7.4}$$

where the implicit constants is effective, and depends at most on q, p and ε.

Acknowledgements. This work is based on part of the author's PhD thesis [**Gri16**]. The author wishes to thank his advisor Marc Hindry for his support and many illuminating conversations. Thanks are also due to Peter Stevenhagen, Michael Tsfasman, Douglas Ulmer and the anonymous referee for carefully reading drafts of this work and for providing valuable suggestions. The author is indebted to Igor Shparlinski for pointing out a mistake in an earlier version. This article was written while being a postdoc at Universiteit Leiden whose financial support and great working conditions are gratefully acknowledged.

References

Del74 P. Deligne, 'La conjecture de Weil. I'. *Inst. Hautes Études Sci. Publ. Math.*, 43: pp. 273–307, 1974.

GL78 S. Gogia and I. Luthar, 'The Brauer-Siegel theorem for algebraic function fields'. *J. Reine Angew. Math.*, 299/300: pp. 28–37, 1978.

Gri16 R. Griffon, 'Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques'. PhD thesis. Université Paris Diderot, 2016.

Gro68a A. Grothendieck, 'Le groupe de Brauer. I. Algèbres d'Azumaya et interprétations diverses'. In *Dix exposés sur la cohomologie des schémas*, Vol. 3 of *Adv. Stud. Pure Math.*, pp. 46–66. North-Holland, 1968.

Gro68b A. Grothendieck, 'Le groupe de Brauer. II. Théorie cohomologique'. In *Dix exposés sur la cohomologie des schémas*, Vol. 3 of *Adv. Stud. Pure Math.*, pp. 67–87. North-Holland, 1968.

HP16 M. Hindry and A. Pacheco, 'An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic'. *Moscow Math. J.*, 16(1): pp. 45—93, 2016.

HW08 G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. Oxford University Press, 6th edition, 2008.

Igu60 J. Igusa, 'Betti and Picard numbers of abstract algebraic surfaces'. *Proc. Nat. Acad. Sci. U.S.A.*, 46: pp. 724–726, 1960.

Ina50 E. Inaba, 'Number of divisor classes in algebraic function fields'. *Proc. Japan Acad.*, 26(7): pp. 1–4, 1950.

IR90 K. Ireland and M. Rosen, *A classical introduction to modern number theory*, vol. 84 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1990.

Kat81 N. M. Katz, 'Crystalline cohomology, Dieudonné modules, and Jacobi sums'. In *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, vol. 10 of *Tata Inst. Fund. Res. Studies in Math.*, pp. 165–246. Tata Inst. Fundamental Res., 1981.

KN74 L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*. Wiley-Interscience, 1974.

Lan94 S. Lang, *Algebraic number theory*, vol. 110 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1994.

LN97 H. Lidl and H. Niederreiter, *Finite fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.

Mil75 J. S. Milne, 'On a conjecture of Artin and Tate'. *Ann. of Math. (2)*, 102(3): pp. 517–533, 1975.

Mil80 J. S. Milne, *Étale cohomology*, vol. 33 of *Princeton Mathematical Series*. Princeton University Press, 1980.

PTvL15 B. Poonen, D. Testa and R. van Luijk, 'Computing Néron-Severi groups and cycle class groups'. *Compos. Math.*, 151(4): pp. 713–734, 2015.

Shi86 T. Shioda, 'An explicit algorithm for computing the Picard number of certain algebraic surfaces'. *Amer. J. Math.*, 108(2): pp. 415–432, 1986.

Shi87 T. Shioda, 'Some observations on Jacobi sums'. In *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, vol. 12 of *Adv. Stud. Pure Math.*, pp. 119–135. North-Holland, 1987.

SK79 T. Shioda and T. Katsura, 'On Fermat varieties'. *Tôhoku Math. J. (2)*, 31(1): pp. 97–115, 1979.

SSvL10 M. Schütt, T. Shioda and R. van Luijk, 'Lines on Fermat surfaces.' *J. Number Theory*, 130(9): pp. 1939–1963, 2010.

ST67 I. Shafarevich and J. Tate, 'The rank of elliptic curves'. *Dokl. Akad. Nauk SSSR*, 175: pp. 770–773, 1967.

Tat94 J. Tate, 'Conjectures on algebraic cycles in l-adic cohomology'. In *Motives (Seattle, WA, 1991)*, vol. 55 of *Proc. Sympos. Pure Math.*, pp. 71–83. Amer. Math. Soc., 1994.

Tat66 J. Tate, 'On the conjectures of Birch and Swinnerton-Dyer and a geometric analog'. In *Séminaire Bourbaki, Vol. 9*, Exp. No. 306, pp. 415–440. Soc. Math. France, Paris, 1965/66.

Ten15 G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, vol. 163 of *Graduate Studies in Mathematics*. American Mathematical Society, 3rd edition, 2015.

TV02 M. Tsfasman and S. Vlăduţ, 'Infinite global fields and the generalized Brauer-Siegel theorem'. *Mosc. Math. J.*, 2(2): pp. 329–402, 2002.

Ulm02 D. Ulmer, 'Elliptic curves with large rank over function fields'. *Ann. of Math. (2)*, 155(1): pp. 295–315, 2002.

Ulm14 D. Ulmer, 'Curves and jacobians over function fields'. In Francesc Bars, Ignazio Longhi, and Fabien Trihan, editors, *Arithmetic Geometry over Global Function Fields*, pp. 281–337. Springer, 2014.

Wei49 A. Weil, 'Numbers of solutions of equations in finite fields'. *Bull. Amer. Math. Soc.* (55): pp. 497–508, 1949.

Richard Griffon
Mathematisch Instituut
Postbus 9512
2300 RA Leiden
Netherlands

r.m.m.griffon@math.leidenuniv.nl