THE ZETA–FUNCTION OF $x^4 + y^4 + z^4 = 0$

BERNDT E. SCHWERDTFEGER

per Violino due

Abstract. This note investigates the ζ–function of $x^4 + y^4 + z^4 = 0$, whose interesting factorization stimulated a closer look at its geometry and arithmetic.

Preface

This study was initiated by the question to find simple examples of curves with no rational points (that these exist had always puzzled me). It has two parts. In the first a conjecture is formulated, that the Jacobian variety J of the curve $C : x^4 + y^4 + z^4 = 0$ is isogenous to $E \times E \times E$, where E is the elliptic curve $y^2 = x^3 + x$. The second part provides the proof, based on Weil [7] and Faltings [2].

I want to thank Fritz Grunewald for pointing me to Weil's paper, when he learned about my conjecture [5]. Reminiscent of my Bielefeld time I dedicate this paper to *Violino due*.

Mainz, January 26, 2003 B. E. Schwerdtfeger

Introduction

Curves with no rational points always mystified me. So, some day in 1978, I set down to look for examples and tested some candidates, like $x^n + y^n + z^n = 0$.

The particular curve C that I looked at in more detail, $x^4 + y^4 + z^4 = 0$ over $\mathbb{F}_5$, had an unexpected form of its ζ–function: its numerator splits into a 3^{rd} power. When varying the ground field this structure of the ζ–function did not change – this led to the conjecture that the Jacobian variety of this curve is isogenous to $E \times E \times E$, where E is the elliptic curve $y^2 = x^3 + x$. So, a very innocent looking question triggered some far reaching speculations. But it seems that these were known to the classical authors, judging from some remarks by André Weil, but I have not studied this literature.

The first section 'On curves without rational points' contains my original manuscript [5]. It is rather elementary and I have only translated it with minor editing. It reflects the state of my knowledge when I came up with the conjecture. I was not endowed with particular theoretical insight at that time, besides knowing the mere definition of the ζ–function.

The second section revisits the subject and applies the tools that André Weil developed in his classical paper [7]. I have tried to keep this note self contained and not defer the reader to that paper, although she would certainly profit from reading it. The one exception is the theorem of Davenport and Hasse, the proof of which the reader will have to look up in Weil [7].

2010 *Mathematics Subject Classification.* Primary 11G20, 14G10; Secondary 11G05.
Key words and phrases. Zeta-function of curves, rational points, Gauss and Jacobi sums.
 version 1.0.527, March 4, 2015.

1. On curves without rational points

1.1. **A curve with no points.** In search for a curve without rational points I started with the following innocent looking polynomial

$$s_n(x,y,z) = x^n + y^n + z^n \qquad n \in \mathbb{Z},\ n \geq 1$$

This is an irreducible homogeneous polynomial over $\mathbb{Z}$ ($s_n(x,1,1) = x^n + 2$ is an Eisenstein polynomial, hence irreducible) and it is also absolutely irreducible in any characteristic not dividing n (and only there). The reducibility for $p \mid n$ is obvious. Let $p \nmid n$ be the characteristic (including 0), then for k algebraically closed the polynomial $x^n - (-y^n - 1) \in k(y)[x]$ is reducible, exactly when $y^n + 1$ is an ℓ–th power in $k(y)$ for all $\ell \mid n$, see Lang [4, VI, §9, Theorem 9.1]. Then $y^n + 1$ would have to be an ℓ–th power in $k[y]$ (Gauss lemma), but as $ny^{n-1} \neq 0$, $y^n + 1$ has no multiple roots, contradiction. s_n defines a curve over $\mathbb{Z}$:

$$V_n = \operatorname{Proj} \mathbb{Z}[x,y,z]/(x^n + y^n + z^n) \hookrightarrow \mathbf{P}_2/\mathbb{Z}$$

Of course $V_n/\mathbb{Z}$ is flat (which can be seen in an affine piece of $\mathbf{P}_2$, a local ring of V_n is free over $\mathbb{Z}_{(p)}$ for all primes, generically over $\mathbb{Q}$ anyhow). It is clear as well that V_n has singularities over $p \mid n$: $ds_n = 0$ in characteristic $p \mid n$, and $ds_n \neq 0$ for $p \nmid n$. Therefore $V_n/\mathbb{Z}[\frac{1}{n}]$ is a complete, geometrically irreducible, smooth planar curve.

We have $V_1 \simeq \mathbf{P}_1/\mathbb{Z}$ and V_2 is a conic, of genus 0, and has a rational point over any finite field, and therefore is $\simeq \mathbf{P}_1/\mathbb{F}_p$, $\forall p \neq 2$ (V_2 is the first infinitesimal neighbourhood of V_1 in characteristic 2). We conclude that $V_2 \hookrightarrow \mathbf{P}_2/\mathbb{F}_p$ ($p \neq 2$) is only a 'twisted' embedding of the projective line in the plane.

In general, the genus of a curve of degree n satisfies

$$g(V_n) \leq \frac{(n-1)(n-2)}{2}$$

see Artin [1, XVI, §6, Theorem 12]. As we assume $p \nmid n$, the covering

$$\begin{aligned} V_n &\to \mathbf{P}_1/\mathbb{F}_p \\ (x,y,z) &\mapsto (x,z) \end{aligned}$$

is *tamely* ramified, and the n ramification points all have ramification index n. According to the Hurwitz formula, e.g. Weil [8, VIII, §4], Corollary to Proposition 14, we have

$$2g - 2 = n \cdot (-2) + n \cdot (n-1)$$

which gives

$$g(V_n) = \frac{(n-1)(n-2)}{2} \tag{1}$$

V_3 has a rational point everywhere (namely over $\mathbb{Z}$). Also, we see that $V_n(\mathbb{F}_2) \neq \varnothing$, $V_n(\mathbb{F}_3) \neq \varnothing$. The smallest numbers for a curve without rational points could therefore be $n = 4$, $p = 5$. In fact, we do have

$$V_4(\mathbb{F}_5) = \varnothing \tag{2}$$

V_4 has genus 3, by (1).

More generally we have $V_{p-1}(\mathbb{F}_p) = \varnothing \quad$ for $p \neq 2, 3$. Indeed, for all $x \in \mathbb{F}_p^\times$ we have $x^{p-1} = 1$ and $s_{p-1}(x,y,z) \neq 0$ for $(x,y,z) \neq 0$.

Another example is $V_4(\mathbb{F}_{29}) = \varnothing$.

1.2. **ζ–function formalism and rational points.** We recall the definition of the ζ–function of schemes of finite type $V/\mathbb{F}_q$ as an EULER product over its closed points. For these the residue class field extension $\kappa(v)/\mathbb{F}_q$ is finite, let $\deg(v) = [\kappa(v) : \mathbb{F}_q]$ be its degree (see SERRE [6] or for curves WEIL [8, VII, §6, Definition 8]).

Definition 1.1 (DEDEKIND ζ–function)**.**

$$Z(t) = \prod_{v \in \overline{V}} \frac{1}{1 - t^{\deg(v)}}$$

Here $\overline{V}$ is the set of *closed* points of the scheme $V/\mathbb{F}_q$.

This coincides with WEIL loc.cit. in the sense that $\zeta(s) = Z(q^{-s})$. Here $\zeta = \zeta_F$ is the ζ–function of the associated function field $F/\mathbb{F}_q$ of $V/\mathbb{F}_q$ as a global field (or **A**–field in WEIL's terminology [8]).

The 'logarithmic' derivative is

$$\frac{Z't}{Z} = \sum_{v \in \overline{V}} \deg(v) \frac{t^{\deg(v)}}{1 - t^{\deg(v)}} = \sum_{n \geq 1} \left(\sum_{v \in \overline{V}, \deg(v) | n} \deg(v) \right) t^n = \sum_{n \geq 1} c_n t^n$$

where the coefficient c_n is the number of rational points of V over $\mathbb{F}_{q^n}$:

$$c_n = \sum_{\deg(v) | n} \deg(v) = \operatorname{card} V(\mathbb{F}_{q^n})$$

This gives the link between the number of rational points on a curve and its ζ–function.

The ζ–function is a rational function, for curves see WEIL [8, VII, §6, Theorem 4]:

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

where L is a polynomial of degree $2g$, g the genus of $V/\mathbb{F}_q$, satisfying the functional equation [8, VII, §6, (8)]

$$L(t) = q^g t^{2g} L(1/qt)$$

Let the α_i be the (inverse) 'roots' of $L(t)$ and let $\sigma_1, \sigma_2, \ldots$ be the elementary symmetric functions of the $\alpha_1, \alpha_2, \ldots$:

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t) = \sum_{i=0}^{2g} (-1)^i \sigma_i t^i$$

The functional equation translates to

$$\sigma_{2g-i} = q^{g-i} \sigma_i \quad \text{for} \quad 0 \leq i \leq g \tag{3}$$

We obtain by logarithmic derivation

$$\frac{Z't}{Z} = \frac{t}{1-t} + \frac{qt}{1-qt} + \frac{L't}{L} = \frac{t}{1-t} + \frac{qt}{1-qt} - \sum_i \frac{\alpha_i t}{1 - \alpha_i t}$$

Comparison of the coefficients of t^n in the power series expansion now gives

$$c_n = \operatorname{card} V(\mathbb{F}_{q^n}) = 1 + q^n - s_n \tag{4}$$

with $s_n = \sum_i \alpha_i^n$. The symmetric s_n can be expressed as polynomials in the elementary symmetric functions σ_i (NEWTON–Polynomials). So, we can calculate the number of rational points from the coefficients of L and vice versa.

Note. For varieties of dim > 1 the rationality conjectured by WEIL in 1948 [7, p. 507] is a theorem of Bernard DWORK in 1959, see SERRE [6] for details and references.

1.3. **The ζ–function of $V_4/\mathbb{F}_5$.** Let L be the numerator of the ζ–function of $V_4/\mathbb{F}_p$. It is a polynomial of 6^{th} degree

$$L = 1 - \sigma_1 t + \sigma_2 t^2 - \sigma_3 t^3 + \sigma_4 t^4 - \sigma_5 t^5 + \sigma_6 t^6$$

the coefficients of which we are going to calculate. We have

$$s_1 = \sigma_1 \qquad s_2 = \sigma_1^2 - 2\sigma_2 \qquad s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \tag{5}$$

We make use of (4) and (5), as well as the ones from the functional equation (3) and get finally

$$\begin{aligned} \sigma_1 &= 1 + p - c_1 \\ \sigma_2 &= p + (c_1^2 + c_2)/2 - (1+p)c_1 \\ \sigma_3 &= (1+p)(c_1^2 + c_2)/2 - pc_1 - (c_1^3 + 3c_1c_2 + 2c_3)/6 \\ \sigma_4 &= p\sigma_2, \quad \sigma_5 = p^2\sigma_1, \quad \sigma_6 = p^3 \end{aligned} \tag{6}$$

We only need to determine the number of rational points over the prime field and its quadratic and cubic extensions. We only made use of the fact $g = 3$, so the above remains valid for any curve of genus 3 over $\mathbb{F}_p$.

Now let $p = 5$, then by (2) $c_1 = 0$ and $\sigma_1 = 6$.

1.3.1. *The field $\mathbb{F}_{25}$.* On each of the lines $x = 0$, $y = 0$, $z = 0$ we have 4 points, this contributes $3 \cdot 4 = 12$ points on these lines. For the remaining we must have $xyz \neq 0$, say $z = 1$. As the 4^{th} powers in $\mathbb{F}_{25}^\times$ are exactly the 6^{th} roots of unity, we have (ρ is a primitive 3^{rd} root of 1) either:

$$x^4 = \rho \quad \text{and} \quad y^4 = \rho^2$$
$$\text{or}$$
$$x^4 = \rho^2 \quad \text{and} \quad y^4 = \rho$$

so, in each case $4 \cdot 4 = 16$, in total 32 points. Together with the previous ones we get $c_2 = 32 + 12 = 44$ and $\sigma_2 = 5 + 22 = 27$.

1.3.2. *The field $\mathbb{F}_{125}$.* The 4^{th} powers in the cubic field consist of the $\frac{125-1}{4} = 31^{st}$ roots of unity. Say α with $\alpha^3 + \alpha = 1$ is a primitive one.

As the powers of α are $\neq -1$, there are no points on one of the lines $x = 0$, $y = 0$, $z = 0$. The question therefore is: when is (set $z = 1$):

$$\alpha^a + \alpha^b = -1$$

(of course $a \neq b$).

Perhaps one can solve this conceptually, a short (dull) computation gives the following relations

$$\begin{aligned} &\alpha^4 + \alpha^{24} = -1 \qquad \alpha^{20} + \alpha^{27} = -1 \qquad \alpha^7 + \alpha^{11} = -1 \\ &\alpha^3 + \alpha^{18} = -1 \qquad \alpha^{15} + \alpha^{28} = -1 \qquad \alpha^{13} + \alpha^{16} = -1 \end{aligned} \tag{7}$$

The first three relations follow from the trace being $\operatorname{tr}\ \alpha = \alpha + \alpha^5 + \alpha^{25} = 0$ after division by α and applying the Frobenius. For the other three relations (that are connected by applying the Frobenius), as well as for the fact that there are no others, an a priori explanation is missing.

Anyhow, we can count the number of rational points now. As there are 6 possibilities for $x^4 + y^4 = -1$ by (7), we get for the pair (x^4, y^4) 12, and for (x, y)

$4\cdot 4\cdot 12 = 192 = c_3$ and $\sigma_3 = 68$. These values substituted in the formulas for the coefficients (6) yield the following numerator of the ζ–function

$$\begin{aligned} L &= 1-6t+27t^2-68t^3+135t^4-150t^5+125t^6 \\ &= (1-2t+5t^2)^3 = (1-(1+2i)t)^3\,(1-(1-2i)t)^3 \end{aligned}$$

This structure really amazed me, when I found it [5].

1.4. **A Conjecture:** $J \sim E\times E\times E$.

Question: could this simple form of the ζ–function have been recognized earlier ?

There are two elliptic curves $E/\mathbb{F}_5$, $E'/\mathbb{F}_5$ with the numerator $1-2t+5t^2$ of the ζ–function, having the modular invariants $j(E) = -2 = 2^6\cdot 3^3$ and $j(E') = 1$. Affine Weierstrass models are respectively $E : y^2 = x^3+x$ and $E' : y^2 = x^3+x+2$. Is there a connection ?

After some more calculations over different ground fields and reflecting the 'coincidence' I came up with the following

Conjecture. *Let J be the* Jacobian *of V_4. We have $J \sim E\times E\times E$, and this isogeny also holds over other ground fields.*

2. The method of André Weil

I could have answered my questions in section 1.4 if I had known the method of André Weil in [7]. The conjecture would then follow over finite fields by a theorem of John Tate. The conjecture as stated can now also be shown to be correct by a theorem of Gerd Faltings (1983), proving a conjecture of Tate, which generalizes Tate's result from finite fields to number fields.

The nice idea that André Weil exploits in [7] consists in a systematic use of *multiplicative* characters $\lambda : \mathbb{F}_q^\times \to \mathbb{C}^\times$ and their *additive* Fourier analysis. The character group $\Lambda = \mathrm{Hom}(\mathbb{F}_q^\times, \mathbb{C}^\times)$ is cyclic of order $q-1$. By convention $\lambda(0) = 0$, except for the trivial character, which is the constant function 1 (including at 0).

Look at the number of solutions in $\mathbb{F}_q$ for $x^n = u$, let $N_n(u)$ be that number. He first remarks that $N_n(u) = N_d(u)$ for $d = (n, q-1)$, the g.c.d. of n and $q-1$. For $d \mid q-1$ the subgroup of characters of order d, $\Lambda_d = \{\lambda\in\Lambda \mid \lambda^d = 1\}$, is cyclic of order d and with the convention above we have

$$N_d(u) = \sum_{\lambda\in\Lambda_d} \lambda(u) = \begin{cases} 1 & \text{for } u = 0 \\ 0 & \text{for } u\neq 0 \text{ not a } d\text{-th power} \\ d & \text{for } u\neq 0 \text{ a } d\text{-th power} \end{cases} \tag{8}$$

With this method we can calculate all the relevant ζ-functions.

We will first collect the salient facts about Gauss and Jacobi sums, as these occur naturally in the course of counting points by Weil's method.

2.1. **Jacobi and Gauss' sums.**

Let $\tau : \mathbb{F}_q \to \mathbb{C}^\times$ be any additive character, $\tau(x+y) = \tau(x)\tau(y)$. The field $\mathbb{F}_q$ operates on the group of these characters by $\tau^x(y) = \tau(x.y)$, which makes it a vector space over $\mathbb{F}_q$, obviously of dimension 1. In the sequel any $\tau \neq 1$ will do. If several fields are under consideration, say $\mathbb{F}_{q'}/\mathbb{F}_q$, it is convenient to choose $\tau' = \tau\circ \mathrm{tr}$, where $\mathrm{tr} : \mathbb{F}_{q'} \to \mathbb{F}_q$ is the trace.

For complex valued functions $f : \mathbb{F}_q \to \mathbb{C}$ the FOURIER transform and the convolution are defined by the usual formulas:

$$\widehat{f}(x) = \sum_y f(y)\tau(xy)$$
$$f * g(x) = \sum_y f(y)g(x-y)$$

A convolution of *multiplicative* characters evaluated at a field element is called a JACOBI *sum*. We make the choice of WEIL in [7] and define

$$J(\lambda,\mu) = \sum_{u+v=-1} \lambda(u)\mu(v) = \lambda * \mu(-1)$$

Another common choice is $\lambda * \mu(1)$, which differs only by a sign, see (9).

Note. In Weil's notation $j(\lambda,\mu,\lambda^{-1}\mu^{-1}) = J(\lambda,\mu)$ for $\lambda \neq 1, \mu \neq 1, \lambda\mu \neq 1$.

It has these properties:

Proposition 2.1.

$$\lambda * \mu(x) = J(\lambda,\mu)\lambda\mu(-x) \tag{9}$$
$$J(\lambda,\mu) = J(\lambda,\lambda^{-1}\mu^{-1}) \qquad \lambda,\mu,\lambda\mu \neq 1 \tag{10}$$
$$J(\lambda,\lambda^{-1}) = -\lambda(-1) \qquad \lambda \neq 1 \tag{11}$$
$$J(1,\lambda) = 0 \qquad \lambda \neq 1 \tag{12}$$
$$J(1,1) = q \tag{13}$$

Proof. As to (9):

$$\lambda * \mu(x) = \sum \lambda(y)\mu(x-y) = \sum \lambda(-xy)\mu(x+xy) =$$
$$= \lambda\mu(-x)\sum \lambda(y)\mu(-1-y) = J(\lambda,\mu)\lambda\mu(-x)$$

As to (10):

$$J(\lambda,\lambda^{-1}\mu^{-1}) = \sum_{u+v=-1} \lambda(u)\lambda^{-1}\mu^{-1}(v) = \sum_{v\neq 0} \lambda(-1-v)\lambda\mu(v^{-1}) =$$
$$= \sum_{v\neq 0} \lambda(-\frac{1}{v}-1)\mu(v^{-1}) = \lambda * \mu(-1) = J(\lambda,\mu)$$

As to (11): $J(\lambda,\lambda^{-1}) = \sum_{v\neq 0} \lambda(-1-v)\lambda(v)^{-1} = \sum_{v\neq 0} \lambda(-1/v-1) = -\lambda(-1)$.

The relations (12), (13) are clear. □

We will need two more facts on the JACOBI sums: the representation of the JACOBI sum as a product of GAUSS sums, and the variance with the tower of field extensions above $\mathbb{F}_q$.

A GAUSS *sum* is by definition a FOURIER transform of a multiplicative character: $\widehat{\lambda}(x) = \sum_y \lambda(y)\tau(xy)$. As $\widehat{\lambda}(x) = \lambda(x)^{-1}\widehat{\lambda}(1)$, the variance with τ is clear and it is omitted from the notation. We define, with WEIL [7], $g(\lambda) = \widehat{\lambda}(1) = \sum_x \lambda(x)\tau(x)$.

Proposition 2.2.

$$g(\lambda)\overline{g(\lambda)} = q \qquad \lambda \neq 1 \tag{14}$$
$$\overline{g(\lambda)} = \lambda(-1)g(\lambda^{-1}) \tag{15}$$
$$J(\lambda,\mu) = \lambda\mu(-1)\frac{g(\lambda)g(\mu)}{g(\lambda\mu)} = \frac{1}{q}g(\lambda)g(\mu)g(\lambda^{-1}\mu^{-1}) \qquad \lambda,\mu,\lambda\mu \neq 1 \tag{16}$$

Proof. As to (14):

$$g(\lambda)\overline{g(\lambda)} = \sum_{x\neq 0}\sum_{y\neq 0}\lambda(xy^{-1})\tau(x-y) = \sum_{x\neq 0}\lambda(x)\sum_{y\neq 0}\tau(xy-y)$$

Now,

$$\sum_{y\neq 0}\tau(xy-y) = \begin{cases} -\tau(0) = -1 & x\neq 1 \\ q-1 & x=1 \end{cases}$$

therefore,

$$g(\lambda)\overline{g(\lambda)} = q-1-\sum_{x\neq 0,1}\lambda(x) = q$$

As to (15): $\overline{g(\lambda)} = \sum \lambda^{-1}(x)\tau(-x) = \lambda(-1)\sum\lambda^{-1}(-x)\tau(-x) = \lambda(-1)g(\lambda^{-1})$.

As to (16): $\widehat{\lambda}\cdot\widehat{\mu} = \widehat{\lambda * \mu}$ and by (9) therefore, $g(\lambda)g(\mu) = J(\lambda,\mu)\lambda\mu(-1)g(\lambda\mu)$. The second equation in (16) follows from (14) and (15). □

The variance with the tower of field extensions above $\mathbb{F}_q$ is the theorem of Davenport and Hasse:

Proposition 2.3. *Let $\mathbb{F}_{q'}/\mathbb{F}_q$ be an extension of degree n. Let the additive characters be chosen by $\tau' = \tau\circ\mathrm{tr}$. The norm $\mathrm{N}:\mathbb{F}_{q'}^{\times}\to\mathbb{F}_q^{\times}$ transports characters on $\mathbb{F}_q^{\times}$ to characters on $\mathbb{F}_{q'}^{\times}$. Then:*

$$-g(\lambda\circ\mathrm{N}) = (-g(\lambda))^n$$

Proof. We skip the proof, see Weil [7, (5)]. □

2.2. **The ζ–function of $V_4/\mathbb{F}_q$ revisited.** We return to the curve $C = V_4/\mathbb{F}_q$.

2.2.1. *The case $q\equiv 1 \pmod 4$.*

Let us look separately at the affine part $C_0 = \mathrm{Spec}\,\mathbb{F}_q[x,y]/(x^4+y^4+1)$ where $z\neq 0$ and the part at infinity $C_\infty = C - C_0$.

The number of points at infinity is:

$$N_\infty = \mathrm{card}\,C_\infty(\mathbb{F}_q) = N_4(-1) = 1+\chi(-1)+\chi^2(-1)+\chi^{-1}(-1) = 2(1+\chi(-1)),$$

as $\Lambda_4 = \{1,\chi,\chi^2,\chi^{-1}\}$, when χ is a primitive 4^{th} character, $\chi^4 = 1$; we have $\chi^2(-1) = 1$, as -1 is a square for $q\equiv 1 \pmod 4$.

The number of points in the affine part C_0 is:

$$N_0 = \mathrm{card}\,C_0(\mathbb{F}_q) = \sum_{u+v=-1}N_4(u)N_4(v) = \sum_{\lambda\in\Lambda_4}\sum_{\mu\in\Lambda_4}\sum_{u+v=-1}\lambda(u)\mu(v) =$$

the inner expression is a Jacobi sum, we use (12) in Prop.2.1 and get

$$= \sum_{\lambda\in\Lambda_4}\sum_{\mu\in\Lambda_4}J(\lambda,\mu) = J(1,1)+J(\chi,\chi)+J(\chi^2,\chi^2)+J(\chi^{-1},\chi^{-1})+$$
$$+2J(\chi,\chi^2)+2J(\chi^{-1},\chi^2)+2J(\chi,\chi^{-1})$$

Now, by (10), we have $J(\chi,\chi) = J(\chi,\chi^2)$. We define the shortcut $\pi = J(\chi,\chi)$, by (14) and (16) we have $\pi\overline{\pi} = q$. Putting in (11) and (13) as well, we get

$$N_0 = q+3\pi-1+3\overline{\pi}-2\chi(-1)$$

and for the number of all rational points

$$N = \mathrm{card}\,V_4(\mathbb{F}_q) = N_0+N_\infty = 1+q+3\pi+3\overline{\pi},$$

and similarly for any field extension

$$N_n = \operatorname{card} V_4(\mathbb{F}_{q^n}) = 1 + q^n + 3\pi_n + 3\overline{\pi}_n, \tag{17}$$

where $\pi_n = J(\chi_n, \chi_n)$ is built with $\chi_n = \chi \circ \mathrm{N} : \mathbb{F}_{q^n}^\times \to \mathbb{C}^\times$. By Davenport–Hasse we have $\pi_n = (-1)^{n-1}\pi^n$, therefore (17) implies:

$$\frac{L't}{L} = \sum_{n\geq 1}(N_n - 1 - q^n)t^n = 3\sum_{n\geq 1}(\pi^n + \overline{\pi}^n)(-1)^{n-1}t^n.$$

Let $Q(t) = (1+\pi t)(1+\overline{\pi}t)$, then

$$\frac{Q't}{Q} = \frac{\pi t}{1+\pi t} + \frac{\overline{\pi}t}{1+\overline{\pi}t} = \sum_{n\geq 1}(\pi^n + \overline{\pi}^n)(-1)^{n-1}t^n.$$

and this finally shows that $L = Q^3$ and the ζ–function of $V_4/\mathbb{F}_q$ is

$$Z(t) = \frac{(1+\pi t)^3(1+\overline{\pi}t)^3}{(1-t)(1-qt)} \qquad \text{for } q \equiv 1 \pmod 4 \tag{18}$$

2.2.2. *The case* $q \equiv 3 \pmod 4$.

Let $\gamma : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be the quadratic character and $\chi : \mathbb{F}_{q^2}^\times \to \mathbb{C}^\times$ be the bi-quadratic character as above.

In this case there are no points at infinity, $N_\infty = 0$, and $N_4(u) = N_2(u)$.

Therefore, $N = \operatorname{card} C(\mathbb{F}_q) = \sum_{u+v=-1} N_2(u)N_2(v) = J(1,1) + J(\gamma,\gamma) = q+1$, as now $J(\gamma,\gamma) = -\gamma(-1)$ and $\gamma(-1) = -1$, since $q \equiv 3 \pmod 4$. Similarly, for all odd degree extensions

$$N_{2n+1} = 1 + q^{2n+1}$$

For the even degree extensions, as $q^2 \equiv 1 \pmod 4$, we can apply the previous section 2.2.1 and get

$$N_{2n} = \operatorname{card} V_4(\mathbb{F}_{q^{2n}}) = 1 + q^{2n} + 3\pi_n + 3\overline{\pi}_n,$$

where again $\pi_n = (-1)^{n-1}\pi^n$, and $\pi = J(\chi,\chi)$ with $\pi\overline{\pi} = q^2$.

Now, as $q \equiv 3 \pmod 4$, we have $\chi^q = \chi^{-1}$, whereas

$$g(\chi) = \sum \chi(x)\tau(x) = \sum \chi(x^q)\tau(x^q) = \sum \chi^{-1}(x)\tau(x) = g(\chi^{-1}).$$

Therefore, $\pi = J(\chi,\chi) = J(\chi^{-1},\chi^{-1}) = \overline{\pi}$ and $\pi \in \mathbb{Z}$ is an integer with $\pi^2 = q^2$.

We build the analog power series as in 2.2.1, which now is even:

$$\frac{L't}{L} = 6\sum_{n\geq 1}\pi^n(-1)^{n-1}t^{2n} = 3\frac{2\pi t^2}{1+\pi t^2} = 3\frac{Q't}{Q}$$

where this time $Q(t) = 1 + \pi t^2$, and again $L = Q^3$. We still have to determine the sign of π: by [8, VII, § 6, Theorem 4], $L(1) = (1+\pi)^3$ is the number of divisor classes of degree 0 (otherwise put, $L(1) = \operatorname{card} J(\mathbb{F}_q)$), hence it is ≥ 0 and $\pi = +q$. So, the ζ–function of $V_4/\mathbb{F}_q$ is

$$Z(t) = \frac{(1+qt^2)^3}{(1-t)(1-qt)} \qquad \text{for } q \equiv 3 \pmod 4 \tag{19}$$

2.3. **The ζ–function of $E/\mathbb{F}_q$.** By the general formalism of ζ–functions (see section 1.2) the ζ–function of $E : y^2 = x^3 + x$ has the form

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)}$$

and we want to show that $P = Q$ with the polynomial Q from section 2.2.

2.3.1. *The case* $q \equiv 3 \pmod 4$.

This case can be dealt with by a simple direct counting argument. As -1 is not a square, the sets $\{x, -x\}$, where x runs thru all squares in $\mathbb{F}_q^\times$, covers $\mathbb{F}_q^\times$. Write $y^2 = x \cdot (x^2+1)$, then either x^2+1 is a square or not, so *either* $x \cdot (x^2+1)$ *or* $-x \cdot (x^2+1)$, but not both, is a square, such that for each set $\{x, -x\}$ you get exactly two y (x^2+1 can never be 0). The number of squares is $(q-1)/2$, so this gives $q-1$ points on the elliptic curve, plus the point $(0,0)$, and the one at infinity, results in card $E(\mathbb{F}_q) = q+1$, hence $P(t) = 1 + qt^2 = Q(t)$, and we are done.

2.3.2. *The case* $q \equiv 1 \pmod 4$.

There is no direct way to count, nor to apply the method of Weil, because the equation $y^2 = x^3 + x$ is not of the type considered in [7]. We will use a trick and apply Weil's method to an open, affine subset. If $O = (0:1:0)$ is the origin of the elliptic curve, then $E - \{O\} = \operatorname{Spec} \mathbb{F}_q[x,y]/(y^2 - x^3 - x)$ is affine and we will also remove the other rational point: $(x,y) = (0,0)$, that is we will study

$$U = E - \{O, (0,0)\} = \operatorname{Spec} \mathbb{F}_q[x, x^{-1}, y]/(y^2 - x^3 - x)$$

This affine ring in the function field $\mathbb{F}_q(x,y)$ has two other generators:

$$\mathbb{F}_q[x, x^{-1}, y] = \mathbb{F}_q[\frac{y}{x}, x - \frac{1}{x}]$$

this follows at once from

$$\left(\frac{y}{x}\right)^2 = x + \frac{1}{x}$$

We see that

$$\left(\frac{y}{x}\right)^4 = x^2 + 2 + \frac{1}{x^2} = (x - \frac{1}{x})^2 + 4$$

Let $E' : y'^2 = x'^4 - 4$ be another elliptic curve, then the affine piece

$$U' = E' - \{O'\} = \operatorname{Spec} \mathbb{F}_q[x', y']/(y'^2 - x'^4 + 4)$$

is isomorphic to U by the ring isomorphism

$$\begin{aligned} \varphi : \mathbb{F}_q[x', y'] &\longrightarrow \mathbb{F}_q[x, x^{-1}, y] \\ \varphi(x') &= \frac{y}{x} \\ \varphi(y') &= x - \frac{1}{x} \end{aligned}$$

the inverse being given by $\varphi^{-1}(x) = (x'^2 + y')/2$, $\varphi^{-1}(y) = x'(x'^2 + y')/2$.

The new curve E' is amenable to Weil's method and we have

$$\begin{aligned} \operatorname{card} E(\mathbb{F}_q) &= 2 + \operatorname{card} U(\mathbb{F}_q) = 2 + \operatorname{card} U'(\mathbb{F}_q) = \\ &= 2 + \sum_{u+v=4} N_4(u) N_2(-v) = 2 + \sum_{\lambda \in \Lambda_4} \sum_{\mu \in \Lambda_2} \sum_{u+v=4} \lambda(u)\mu(v) = \\ &= 2 + \sum_{\lambda \in \Lambda_4} \sum_{\mu \in \Lambda_2} \lambda * \mu(4) = 2 + \sum_{\lambda \in \Lambda_4} \sum_{\mu \in \Lambda_2} \lambda\mu(-4) J(\lambda, \mu) = \\ &= 2 + J(1,1) + \chi^{-1}(-4) J(\chi, \chi^2) + J(\chi^2, \chi^2) + \chi(-4) J(\chi^{-1}, \chi^2) = \\ &= 2 + q + \chi(-1)\chi^2(2)\pi - 1 + \chi(-1)\chi^2(2)\overline{\pi} = 1 + q + \pi + \overline{\pi} \end{aligned}$$

because $\chi(-1)\chi(2)^2 = 1$ by the *quadratic reciprocity* law.

As this implies that $P = (1 + \pi t)(1 + \overline{\pi} t) = Q$, we are done.

2.4. **Conclusion.** In 1983 Gerd FALTINGS proved several outstanding conjectures in a short paper [2], like the TATE conjectures, the SHAFAREVICH conjecture and the MORDELL conjecture. I am not going to explain these, as they are beyond the level of this note.

In particular, one of the corollaries of his is (see [3, §5, Corollary 2]):

Corollary 2.4. *Let A_1, A_2 be abelian varieties over K. The following are equivalent:*

(1) *A_1 and A_2 are isogenous.*
(2) *$T_\ell(A_1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq T_\ell(A_2) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ as $Gal(\overline{K}/K)$–modules.*
(3) *$L_v(A_1, s) = L_v(A_2, s)$ for almost all places v of K.*
(4) *$L_v(A_1, s) = L_v(A_2, s)$ for all v.*

The conclusion now is that $J \sim E \times E \times E/\mathbb{Q}$ follows from this, as we have seen in the previous sections condition (3) to be true.

REFERENCES

[1] Emil Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.
[2] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones math. **73** (1983), 349–366.
[3] ———, *Finiteness Theorems for Abelian Varieties over Number Fields*, Conference on Arithmetic Geometry, Arithmetic Geometry (Gary Cornell and Joseph H. Silverman, eds.), Springer, 1986, pp. 9–27.
[4] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, 2002.
[5] Berndt E. Schwerdtfeger, *Über Kurven ohne rationale Punkte*, August 1978, unpublished.
[6] Jean-Pierre Serre, *Zeta and L–Functions*, Arithmetical Algebraic Geometry, Proc. Conf. at Purdue Univ., Harper and Row, New York, 1965, pp. 82–92.
[7] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Am. Math. Soc. **55** (1949), 497–508, available at http://berndt-schwerdtfeger.de/wp-content/uploads/pdf/nf.pdf.
[8] ———, *Basic Number Theory*, Classics in Mathematics, Springer, Berlin, Heidelberg, New York, 1973, 1995.