manuscript No.
(will be inserted by the editor)

On Colmez's product formula for periods of CM-abelian varieties

Andrew Obus

Received: date / Accepted: date

Abstract Colmez conjectured a product formula for periods of abelian varieties with complex multiplication by a field K, analogous to the standard product formula in algebraic number theory. He proved this conjecture up to a rational power of 2 for $K/\mathbb{Q}$ abelian. In this paper, we complete the proof of Colmez for $K/\mathbb{Q}$ abelian by eliminating this power of 2. Our proof relies on analyzing the Galois action on the De Rham cohomology of Fermat curves in mixed characteristic $(0,2)$, which in turn relies on understanding the stable reduction of $\mathbb{Z}/2^n$-covers of the projective line, branched at three points.

Keywords Fermat curve · Stable reduction · Product formula

Mathematics Subject Classification (2000) 11G20 · 11G15 · 14H25 · 14H30 · 14K22 · 32G20

1 Introduction

The *product formula* in algebraic number theory states that, given an algebraic number $x \neq 0$ in a number field K, the product of $|x|$ as $|\cdot|$ ranges over all inequivalent absolute values of K (appropriately normalized) is equal to 1. In logarithmic form, the sum of $\log|x|$ as $|\cdot|$ ranges over all inequivalent absolute values is 0. In [3], Colmez asked whether an analogous product formula might hold for periods of algebraic varieties, and conjectured that it would hold for periods of abelian varieties with complex multiplication (CM-abelian varieties). He proved that, for abelian varieties with complex multiplication by *abelian* extensions of $\mathbb{Q}$, such a product formula holds (in

The author was supported by an NSF Postdoctoral Research Fellowship in the Mathematical Sciences. Final editing of this work was undertaken during a fellowship at the Max Planck Institute for Mathematics in Bonn.

Columbia University, Department of Mathematics, 2990 Broadway, MC 4403, New York, NY 10027
Tel.: +1-212-854-6240
Fax: +1-212-854-8962
E-mail: andrewobus@gmail.com

logarithmic form) up to an (unknown) rational multiple of $\log 2$ ([3, Théorème 0.5 and discussion after Conjecture 0.4]). A key step in this proof was provided by work of Coleman and McCallum ([2], [1]) on understanding stable models of quotients of Fermat curves in mixed characteristic $(0,p)$, where p is an odd prime. These quotients are $\mathbb{Z}/p^n$-covers of the projective line, branched at three points. The unknown rational multiple of $\log 2$ was necessary in [3] precisely because the stable models of $\mathbb{Z}/2^n$-covers of the projective line, branched at three points, in mixed characteristic $(0,2)$, were not well-understood at the time. This problem was solved by the author in [7], where a complete description of the stable models of such covers was given. In this paper, we use the results of [7] to complete the proof of Colmez's product formula for abelian extensions of $\mathbb{Q}$ by eliminating the multiple of $\log 2$ in question.

Colmez first looks at the example of $2\pi i$, which is a period for the variety $\mathbb{G}_m$, rather than for an abelian variety. For each prime p, one can view $2\pi i$ as an element t_p of Fontaine's ring of periods $\mathbf{B}_p$, and its p-adic absolute value is $|t_p|_p = p^{1/(1-p)}$. The archimedean absolute value $|\cdot|_\infty$ is the standard one, so $|2\pi i|_\infty = 2\pi$. The logarithm of the product of all of these absolute values is

$$\log 2\pi - \sum_{p<\infty} \frac{\log p}{p-1}.$$

This sum does not converge, but formally, it is equal to $\log 2\pi - \frac{\zeta'(1)}{\zeta(1)}$, where ζ is the Riemann zeta function. Using the functional equation of ζ (and ignoring the Γ factors), we obtain $\log 2\pi - \frac{\zeta'(0)}{\zeta(0)}$, which is equal to 0. In this sense, we can say that the product formula holds for $2\pi i$.

The above method can be adapted to give a definition of what it means to take the logarithm of the product of all the absolute values of a period, and thus to give a product formula meaning. Many subtleties arise, and the excellent and thorough introduction to [3] discusses them in detail. We will not attempt to recreate this discussion. Instead, we will just note that Colmez shows that the product formula for periods of CM-abelian varieties with complex multiplication by an abelian extension of $\mathbb{Q}$ (in logarithmic form) is equivalent to the formula

$$ht(a) = Z(a^*, 0) \tag{1.1}$$

for all $a \in \mathscr{CM}^{ab}$ ([3, Théorème II.2.12(iii)]). Here, $\mathscr{CM}^{ab}$ is the vector space of $\mathbb{Q}$-valued, locally constant functions $a : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathbb{Q}$ such that, if c represents complex conjugation, then $a(g) + a(cg)$ does not depend on $g \in G_{\mathbb{Q}}$. Such a function can be decomposed into a $\mathbb{C}$-linear combination of Dirichlet characters whose L-functions do not vanish at 0. If $a \in \mathscr{CM}^{ab}$ then we define $a^* \in \mathscr{CM}^{ab}$ by $a^*(g) = a(g^{-1})$. Also, $Z(\cdot, 0)$ is the unique $\mathbb{C}$-linear function on $\mathscr{CM}^{ab} \otimes \mathbb{C}$ equal to $\frac{L'(\chi,0)}{L(\chi,0)}$ when its argument is a Dirichlet character χ whose L-function does not vanish at 0. Lastly, $ht(\cdot)$ is a $\mathbb{C}$-linear function on $\mathscr{CM}^{ab} \otimes \mathbb{C}$ related to Faltings heights of abelian varieties (see [3, Théorème 0.3] for a precise definition, also [10]).

Colmez shows ([3, Proposition III.1.2, Remarque on p. 676]) that

$$Z(a^*, 0) - ht(a) = \sum_{p \text{ prime}} w_p(a) \log p, \tag{1.2}$$

where $w_p : \mathscr{C}\mathscr{M}^{ab} \to \mathbb{Q}$ is a $\mathbb{Q}$-linear function (depending on p) that will be defined in §2. He then further shows that $w_p(a) = 0$ for all $p \geq 3$ and all $a \in \mathscr{C}\mathscr{M}^{ab}$ ([3, Corollaire III.2.7]). Thus (1.1) is correct up to a adding a rational multiple of $\log 2$. Our main theorem (Theorem 3.9) states that $w_2(a) = 0$ for all $a \in \mathscr{C}\mathscr{M}^{ab}$, thus proving (1.1).

We note that, in light of the expression (1.1), Colmez's formula is fundamentally about relating periods of CM-abelian varieties to logarithmic derivatives of L-functions. That this can be expressed as a product formula is aesthetically pleasing, but the main content is encapsulated by (1.1).

In §2, we define w_p and show how it is related to De Rham cohomolgy of Fermat curves. In §3.1, we write down the important properties of the stable model of a certain quotient of the Fermat curve F_{2^n} of degree 2^n ($n \geq 2$) over $\mathbb{Q}_2$, and we discuss the monodromy action on the stable reduction. In §3.2, we show how knowledge of this stable model, along with the monodromy action, allows us to understand the Galois action on the De Rham cohomology of F_{2^n}. In §3.3, we show how this is used to prove that $w_2(a) = 0$. Lastly, in §4, we collect some technical power series computations that are used in §3.2, but would interrupt the flow of the paper if included there.

1.1 Conventions

The letter p always represents a prime number. If $x \in \mathbb{Q}/\mathbb{Z}$, then $\langle x \rangle$ is the unique representative for x in the interval $[0, 1)$. The standard p-adic valuation on $\mathbb{Q}$ is denoted v_p, and the subring $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ consists of the elements $x \in \mathbb{Q}$ with $v_p(x) \geq 0$. If K is a field, then $\overline{K}$ is its algebraic closure and G_K is its absolute Galois group.

2 Galois actions on De Rham cohomology

The purpose of this section is to define the function $w_p(a)$ from (1.2). In order to make this definition, one must first consider a particular rational factor of the Jacobian of the mth Fermat curve (where m is related to a). This factor will have complex multiplication, and we will choose a de Rham cohomology class that is an eigenvector for this complex multiplication. One can then define the "p-adic valuation" of such a cohomology class, and this valuation essentially determines $w_p(a)$.

Recall that the action of $G_{\mathbb{Q}}$ on roots of unity gives a homomorphism $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$. This factors through $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, giving an isomorphism $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$, called the *cyclotomic character*. Multiplication by the cyclotomic character gives a well-defined action of $G_{\mathbb{Q}}$ on $\mathbb{Q}/\mathbb{Z}$, factoring through $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$.

The following definitions are from [3, III]. Recall that $\mathscr{C}\mathscr{M}^{ab}$ is the vector space of $\mathbb{Q}$-valued, locally constant functions $a : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathbb{Q}$ such that, if c represents complex conjugation, then $a(g) + a(cg)$ does not depend on $g \in G_{\mathbb{Q}}$ ([3, p. 627]). For $r \in \mathbb{Q}/\mathbb{Z}$, define an element $a_r \in \mathscr{C}\mathscr{M}^{ab}$ by

$$a_r(g) = \langle gr \rangle - \frac{1}{2}.$$

One can show that the a_r generate $\mathscr{C}\mathscr{M}^{ab}$ as a $\mathbb{Q}$-vector space. For $r \in \mathbb{Q}/\mathbb{Z}$, set $v_p(r) = \min(v_p(\langle r \rangle), 0)$, and set

$$r_{(p)} = p^{-v_p(r)} r \in \mathbb{Q}/\mathbb{Z}. \tag{2.1}$$

Set

$$V_p(r) = \begin{cases} 0 & r \in \mathbb{Z}_{(p)}/\mathbb{Z} \\ (\langle r \rangle - \frac{1}{2}) v_p(r) - \frac{1}{(p-1)p^{-v_p(r)-1}} (\langle \frac{r_{(p)}}{p} \rangle - \frac{1}{2}) & \text{otherwise,} \end{cases}$$

where $\frac{r_{(p)}}{p}$ is the unique element of $\mathbb{Z}_{(p)}/\mathbb{Z}$ such that $\frac{r_{(p)}}{p} \cdot p = r_{(p)}$.

Let $q = (\rho, \sigma, \tau) \in (\mathbb{Q}/\mathbb{Z})^3$, such that $\rho + \sigma + \tau = 0$ and none of ρ, σ, or τ are 0. Let m be a positive integer such that $m\rho = m\sigma = m\tau = 0$. Let $\varepsilon_q = \langle \rho \rangle + \langle \sigma \rangle + \langle \tau \rangle - 1$. Let F_m be the mth Fermat curve, that is, the smooth, proper model of the affine curve over $\mathbb{Q}$ given by $u^m + v^m = 1$, and let J_m be its Jacobian. Write $\langle \rho \rangle = \frac{a}{m}$ and $\langle \sigma \rangle = \frac{b}{m}$. Consider the closed differential form

$$\eta_{m,q} := m \langle \rho + \sigma \rangle^{\varepsilon_q} u^a v^b \frac{v}{u} d\left(\frac{u}{v}\right)$$

on F_m. We can view its De Rham cohomology class as a class $\omega_{m,q} \in H^1_{DR}(J_m) \cong H^1_{DR}(F_m)$ over $\mathbb{Q}$. It turns out that there is a particular rational factor J_q of J_m with complex multiplication, and a class $\omega_q \in H^1_{DR}(J_q)$, such that the pullback of ω_q to J_m is $\omega_{m,q}$. Furthermore, ω_q is an eigenvector for the complex multiplication on J_q. As is suggested by the notation, the pair (J_q, ω_q) depends only on q, not on m, up to isomorphism ([3, p. 674]).

Now, $G_{\mathbb{Q}}$ acts diagonally on $(\mathbb{Q}/\mathbb{Z})^3$ by the cyclotomic character. If $\gamma \in G_{\mathbb{Q}}$, then $J_q = J_{\gamma q}$ ([3, p. 674]). Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, which gives rise to an embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. If γ lies in the inertia group $I_{\mathbb{Q}_p} \subseteq G_{\mathbb{Q}_p} \subseteq G_{\mathbb{Q}}$, then γ acts on J_q, and thus on $H^1_{DR}(J_q, \overline{\mathbb{Q}}_p)$. We have $\gamma^* \omega_q = \beta_\gamma(q) \omega_{\gamma q}$ where the constant $\beta_\gamma(q)$ lies in some finite extension of $\mathbb{Q}_p$ ([3, pp. 676-7]). We also note that $I_{\mathbb{Q}_p}$ acts on $H^1_{DR}(F_m, \overline{\mathbb{Q}}_p) \cong H^1_{DR}(J_m, \overline{\mathbb{Q}}_p)$ via its action on F_m. One derives

$$\gamma^* \omega_{m,q} = \beta_\gamma(q) \omega_{m,\gamma q}. \tag{2.2}$$

If K is a p-adic field with a valuation v_p, then there is a notion of p-adic valuation of $\omega \in H^1_{DR}(A)$ whenever A is a CM-abelian variety defined over K and ω is an eigenvector for the complex multiplication ([3, p. 659]—note that ω_q is such a class). By abuse of notation, we also write this valuation as v_p. It has the property that, if $c \in K$, then $v_p(c\omega) = v_p(c) + v_p(\omega)$.

Lemma 2.1 *If $\gamma \in I_{\mathbb{Q}_p}$, then $v_p(\omega_q) - v_p(\omega_{\gamma q}) = v_p(\beta_\gamma(q))$.*

Proof By [3, Théorème II.1.1], we have $v_p(\omega_q) = v_p(\gamma^* \omega_q)$. The lemma then follows from the definition of $\beta_\gamma(q)$.

Let $b_q = a_\rho + a_\sigma + a_\tau \in \mathscr{C}\mathscr{M}^{ab}$. There is a unique linear map $w_p : \mathscr{C}\mathscr{M}^{ab} \to \mathbb{Q}$ such that

$$w_p(b_q) = v_p(\omega_q) - V_p(q)$$

([3, Corollaire III.2.2]). This is the map w_p from (1.2). Recall from §1 that Colmez showed $w_p(a) = 0$ for all $p \geq 3$ and all $a \in \mathscr{C}\mathscr{M}^{ab}$. In Theorem 3.9, we will show that $w_2(a) = 0$ for all $a \in \mathscr{C}\mathscr{M}^{ab}$.

3 Fermat curves

In general, a branched Galois cover $f : Y \to X := \mathbb{P}^1$ defined over $\mathbb{Q}_p$ does not necessarily have good reduction. However, assuming that $2g(X)+r \geq 3$ (where r is the number of branch points), one can always find a finite extension $K/\mathbb{Q}_p$ with valuation ring R, and a *stable model* $f^{st} : Y_R \to X_R$ for the cover (i.e., f^{st} is a finite map of flat R-curves whose generic fiber is f, and where Y^{st} has reduced, stable fibers, considering the specializations of the ramification points of f as marked points). The special fiber $\overline{f} : \overline{Y} \to \overline{X}$ of f^{st} is called the *stable reduction* of the cover. Furthermore, there is an action of $G_{\mathbb{Q}_p}$ on $\overline{f}$ (called the *monodromy action*), given by reducing its canonical action on f, and this action factors through $\mathrm{Gal}(K/\mathbb{Q}_p)$. For more details, see [4], [9], [6].

Calculating the stable reduction and monodromy action of a cover can be difficult, even when the Galois group is simple (see, e.g., [5], where Lehr and Matignon calculate the stable reduction and monodromy action of $\mathbb{Z}/p$-covers branched at arbitrarily many equidistant points). Restricting to three branch points can simplify matters. A major result of Coleman and McCallum ([2]) calculated the stable reduction of all cyclic covers of $\mathbb{P}^1$ branched at three points, when $p \neq 2$. From this, the monodromy action was calculated in [1], which sufficed to prove Colmez's product formula up to the factor of $\log 2$. The case $p = 2$ (for three-point covers) is somewhat more complicated, and requires new techniques by the author in [7]. Enough details are given in [7] to calculate the monodromy action explicitly, which we do to the extent we need to in §3.1. The work in §3.2 and §3.3 mimics the work in [1] and [3], respectively, to show how a knowledge of the monodromy action leads to a proof of the product formula.

3.1 The monodromy action

Fix $n \geq 2$. Let $f : Y \to X := \mathbb{P}^1$ be the branched cover given birationally by the equation $y^{2^n} = x^a(x-1)^b$, defined over $\mathbb{Q}_2$, where x is a fixed coordinate on $\mathbb{P}^1$. Assume for this entire section that a is odd, that $1 \leq v_2(b) \leq n-2$, and that $0 < a, b < 2^n$. Set $s = n - v_2(b)$ (this makes 2^s the branching index of f at $x = 1$). Thus $s \geq 2$. Let $K/\mathbb{Q}_2$ be a finite extension, with valuation ring R, over which f admits a stable model $f^{st} : Y^{st} \to X^{st}$. Let k be the residue field of K. We write $I_{\mathbb{Q}_2} \subseteq G_{\mathbb{Q}_2}$ for the inertia group. Let $\overline{f} : \overline{Y} \to \overline{X}$ be the special fiber of f^{st} (called the *stable reduction* of f). We focus on the monodromy action of the inertia group $I_{\mathbb{Q}_2}$ on $\overline{f}$. Throughout this section we write v for the valuation on K satisfying $v(2) = 1$. We will allow finite extensions of K as needed.

The following proposition is the result that underlies our entire computation.

Proposition 3.1 ([7], Lemma 7.8)

(i) There is exactly one irreducible component $\overline{X}_b$ of $\overline{X}$ above which $\overline{f}$ is generically étale.
(ii) Furthermore, $\overline{f}$ is étale above $\overline{X}_b^{sm}$, i.e., the smooth points of $\overline{X}$ that lie on $\overline{X}_b$.

(iii) *Let*

$$d = \frac{a}{a+b} + \frac{\sqrt{2^n bi}}{(a+b)^2}.$$

and extend K finitely (if necessary) so that K contains d, as well as an element e such that $v(e) = n - \frac{s}{2} + \frac{1}{2}$. Here, i can be either square root of -1 and $\sqrt{2^n bi}$ can be either square root of $2^n bi$. Then, in terms of the coordinate x, the K-points of X that specialize to $\overline{X}_b^{sm}$ form a closed disc of radius $|e|$ centered at d.

(iv) *For each k-point $\overline{u}$ of $\overline{X}_b^{sm}$, the K-points of X that specialize to $\overline{u}$ form an open disc of radius $|e|$.*

Remark 3.2 The result [7, Lemma 7.8] is more general, in that it proves an analogous statement when 2 is replaced by any prime p. Such a result was already shown in [1] when p is an odd prime (with some restrictions in the case $p = 3$). In [7, Lemma 7.8], k is assumed to be algebraically closed, but as long as we restrict to k-points in Proposition 3.1(iv), everything works.

For any K-point w in the closed disc from Proposition 3.1(iii), write $\overline{w}$ for its specialization to $\overline{X}_b$, which is a k-point. For such a w, if t is defined by $x = w + et$, then $\hat{\mathcal{O}}_{X^{st},\overline{w}} = R[[t]]$, where $\hat{\mathcal{O}}_{X^{st},\overline{w}}$ is the completion of the local ring $\mathcal{O}_{X^{st},\overline{w}}$ at its maximal ideal. The variable t is called a *parameter* for $\hat{\mathcal{O}}_{X^{st},\overline{w}}$. One thinks of $R[[t]]$ as the ring of functions on the open unit disc $|t| < 1$, which corresponds to the open disc $|x - w| < |e|$.

For $\gamma \in I_{\mathbb{Q}_2}$, let $\chi(\gamma) \in \mathbb{Z}_2^\times$ be the cyclotomic character applied to γ. Maintain the notation d from Proposition 3.1.

Lemma 3.3 *Fix $\gamma \in I_{\mathbb{Q}_2}$. Let a' (resp. b') be the integer between 0 and $2^n - 1$ congruent to $\chi(\gamma)a$ (resp. $\chi(\gamma)b$) modulo 2^n. Let*

$$d' = \frac{a'}{a'+b'} + \frac{\sqrt{2^n b'i}}{(a'+b')^2}$$

(here i is the same square root of -1 chosen in the definition of d, but $\sqrt{2^n b'i}$ can be either choice of square root). Then we have $\overline{\gamma(d)} = \overline{d'}$.

Proof We first claim that

$$d' \equiv \frac{a}{a+b} + \chi(\gamma)^{-3/2} \frac{\sqrt{2^n bi}}{(a+b)^2} \pmod{2^n}, \tag{3.1}$$

where $\sqrt{2^n bi}$ is chosen as in the definition of d, as long as the square root of $\chi(\gamma)$ is chosen correctly. One verifies easily that

$$\frac{a'}{a'+b'} \equiv \frac{a}{a+b} \pmod{2^n}. \tag{3.2}$$

One also sees easily that

$$\frac{\sqrt{2^n b'i}}{(a'+b')^2} \equiv \frac{1}{\chi(\gamma)^2} \frac{\sqrt{2^n b'i}}{(a+b)^2} \pmod{2^n}. \tag{3.3}$$

Now,

$$\sqrt{2^n b' i} = \sqrt{2^n(\chi(\gamma)b + r)i} = \chi(\gamma)^{1/2}\sqrt{2^n bi}\sqrt{1 + \frac{r}{\chi(\gamma)b}}, \tag{3.4}$$

where r is some integer divisible by 2^n, where $\sqrt{1+\frac{r}{\chi(\gamma)b}}$ is chosen to be no further from 1 than from -1, where $\sqrt{2^n bi}$ is chosen as in the definition of d, and where $\chi(\gamma)^{1/2}$ is chosen to make the equality work. But $v\left(\frac{r}{\chi(\gamma)b}\right) \geq s$, and thus

$$v\left(\sqrt{1+\frac{r}{\chi(\gamma)b}} - 1\right) \geq s - 1 \geq \frac{s}{2}$$

(recall that we assume $s \geq 2$). Since $v(\sqrt{2^n bi}) = n - \frac{s}{2}$, it follows from (3.4) that

$$\sqrt{2^n b' i} \equiv \chi(\gamma)^{1/2}\sqrt{2^n bi} \pmod{2^n}.$$

Combining this with (3.2) and (3.3) proves the claim.

Now,

$$\gamma(d) = \frac{a}{a+b} + \zeta_\gamma \frac{\sqrt{2^n bi}}{(a+b)^2},$$

where ζ_γ is a fourth root of unity that depends on γ. In particular,

$$\zeta_\gamma = \begin{cases} \pm i & \chi(\gamma) \equiv 3 \pmod 4 \\ \pm 1 & \chi(\gamma) \equiv 1 \pmod 4. \end{cases}$$

In both cases, one computes that $\zeta_\gamma \equiv \chi(\gamma)^{-3/2} \pmod 2$. So

$$\gamma(d) \equiv \frac{a}{a+b} + \chi(\gamma)^{-3/2}\frac{\sqrt{2^n bi}}{(a+b)^2} \pmod{2^{n-\frac{s}{2}+1}}. \tag{3.5}$$

Combining this with (3.1), we obtain that

$$\gamma(d) \equiv d' \pmod{2^{\min(n, n-\frac{s}{2}+1)}}.$$

Since $s \geq 2$, this implies

$$\gamma(d) \equiv d' \pmod{2^{n-\frac{s}{2}+1}}.$$

By Proposition 3.1(iv), $\gamma(d)$ and d' specialize to the same point, and we are done.

Remark 3.4 Note that $v(d) = v(d') = 0$ and $v(d-1) = v(d'-1) = n - s$.

Combining Proposition 3.1 and Lemma 3.3, and using the definitions of d, d', e, and γ therein, we obtain:

Corollary 3.5 *If $x = d + et$, then t is a parameter for Spec $\hat{\mathcal{O}}_{X^{st},\overline{d}}$. Likewise, if $x = d' + et'$, then t' is a parameter for Spec $\hat{\mathcal{O}}_{X^{st},\overline{\gamma(d)}}$.*

3.2 Differential forms

Maintain the notation of §3.1, including d, d', e, and γ. All De Rham cohomology groups will be assumed to have coefficients in K.

As in §2, let $q=(\rho,\sigma,\tau)\in(\mathbb{Q}/\mathbb{Z})^3$, such that $\rho+\sigma+\tau=0$. Furthermore, suppose $\langle\rho\rangle=\frac{a}{2^n}$ with a odd and $\langle\sigma\rangle=\frac{b}{2^n}$ with $1\le v(b)\le n-2$. Set $\varepsilon_q=\langle\rho\rangle+\langle\sigma\rangle+\langle\tau\rangle-1$. Let F_{2^n} be the Fermat curve given by $u^{2^n}+v^{2^n}=1$, defined over $\mathbb{Q}_2$, and let J_{2^n} be its Jacobian. Let $\omega_{2^n,q}$ be the element of $H^1_{DR}(F_{2^n})\cong H^1_{DR}(J_{2^n})$ given by the differential form

$$\eta_{2^n,q}=2^n\langle\rho+\sigma\rangle^{\varepsilon_q}u^av^b\frac{v}{u}d\left(\frac{u}{v}\right).$$

Recall that this is the pullback of a cohomology class ω_q on a rational factor J_q of J_{2^n}. One can rewrite $\eta_{2^n,q}$ as

$$\langle\rho+\sigma\rangle^{\varepsilon_q}u^{a-2^n}v^{b-2^n}d(u^{2^n})$$

(cf. [1, (1.2)]). Making the substitution $y=u^av^b$ and $x=u^{2^n}$ shows that $\eta_{2^n,q}$ (and thus $\omega_{2^n,q}$) descends to the curve Y given by the equation $y^{2^n}=x^a(x-1)^b$ (which we will also call $F_{2^n,a,b}$), and is given in (x,y)-coordinates by

$$\eta_{2^n,q}=\frac{\langle\rho+\sigma\rangle^{\varepsilon_q}}{x(1-x)}ydx.$$

If $\gamma\in I_{\mathbb{Q}_2}$, then $\langle\gamma\rho\rangle=\frac{a'}{2^n}$ and $\langle\gamma\sigma\rangle=\frac{b'}{2^n}$, where a' and b' are as in Lemma 3.3. Letting $\gamma\in I_{\mathbb{Q}_2}$ act on $(\mathbb{Q}/\mathbb{Z})^3$ diagonally via the cyclotomic character, we define $\eta_{2^n,\gamma q}$, $\omega_{2^n,\gamma q}$, and $\omega_{\gamma q}$ as above. Now, $\eta_{2^n,\gamma q}$ (and thus $\omega_{2^n,\gamma q}$) descends to the curve $F_{2^n,a',b'}$ given by the equation $(y')^{2^n}=x^{a'}(x-1)^{b'}$, where $y'=u^{a'}v^{b'}$. Then $\eta_{2^n,\gamma q}$ is given in (x,y')-coordinates by

$$\eta_{2^n,\gamma q}=\frac{\langle\gamma\rho+\gamma\sigma\rangle^{\varepsilon_{\gamma q}}}{x(1-x)}y'dx.$$

Note that we can identify $F_{2^n,a',b'}$ with $F_{2^n,a,b}$ via $y'=y^hx^j(1-x)^k$, where h, j, and k are such that $a'=ha+2^nj$ and $b'=hb+2^nk$.

Recall from (2.2) that, for each $\gamma\in I_{\mathbb{Q}_2}$, there exists $\beta_\gamma(q)\in K$ (after a possible finite extension of K) such that $\gamma^*\omega_{2^n,q}=\beta_\gamma(q)\omega_{2^n,\gamma q}$ in $H^1_{DR}(J_{2^n})$. We will compute $\beta_\gamma(q)$ by viewing $\omega_{2^n,q}$ and $\omega_{2^n,\gamma q}$ as cohomology classes on $F_{2^n,a,b}=F_{2^n,a',b'}$.

The following proposition relies on calculations from §4.

Proposition 3.6 (cf. [1], Corollary 7.6) *We have*

$$v(\beta_\gamma(q))=v(\langle\rho\rangle)(\langle\rho\rangle-\langle\gamma\rho\rangle)+v(\langle\sigma\rangle)(\langle\sigma\rangle-\langle\gamma\sigma\rangle)+v(\langle\tau\rangle)(\langle\tau\rangle-\langle\gamma\tau\rangle).$$

Proof We work with the representatives $\eta_{2^n,q}$ and $\eta_{2^n,\gamma q}$ of $\omega_{2^n,q}$ and $\omega_{2^n,\gamma q}$ on the curve $F_{2^n,a,b}=F_{2^n,a',b'}$.

If $x=d+et$, then Proposition 4.6 defines (after a possible finite extension of R) a power series $\alpha(t)\in R[[t]]$ such that

$$\alpha(t)^{2^n}=x^a(x-1)^bd^{-a}(d-1)^{-b}$$

(Remark 4.7). Corollary 4.8 defines $\tilde{\alpha}(t) = \frac{d(1-d)\alpha(t)}{x(1-x)} \in R[[t]]$ (after substituting $x = d+et$), and shows that the valuation of the coefficient of t^ℓ in $\tilde{\alpha}(t)$ is $\frac{1}{2}S(\ell)$, the number of ones in the base 2 expansion of ℓ. Since $y^{2^n} = x^a(x-1)^b$, we have

$$\eta_{2^n,q} = \frac{\sqrt[2^n]{d^a(d-1)^b}\langle\rho+\sigma\rangle^{\varepsilon_q}\tilde{\alpha}(t)}{d(1-d)}\,e\,dt = \mu d^{\langle\rho\rangle-1}(d-1)^{\langle\sigma\rangle-1}\langle\rho+\sigma\rangle^{\varepsilon_q}\tilde{\alpha}(t)e\,dt, \tag{3.6}$$

where μ is some root of unity and $d^{\langle\rho\rangle}$, $(d-1)^{\langle\sigma\rangle}$. are calculated using some choices of 2^nth roots.

Likewise, letting d' be as in Lemma 3.3 and setting $x' = d'+et'$, we have

$$\eta_{2^n,\gamma q} = \mu'(d')^{\langle\gamma\rho\rangle-1}(d'-1)^{\langle\gamma\sigma\rangle-1}\langle\gamma\rho+\gamma\sigma\rangle^{\varepsilon_{\gamma q}}\tilde{\alpha}'(t')e\,dt', \tag{3.7}$$

where μ' is some root of unity, and $\tilde{\alpha}'(t')$ is some power series in t' whose coefficients have the *same* valuations as the coefficients of $\tilde{\alpha}(t)$ (Remark 4.9).

By Corollary 3.5, t (resp. t') is a parameter for Spec $\hat{\mathcal{O}}_{X^{st},\overline{d}}$ (resp. Spec $\hat{\mathcal{O}}_{X^{st},\overline{\gamma(d)}}$). Since the map $Y^{st} \to X^{st}$ is completely split above $\overline{d}$ (Proposition 3.1(ii)), we can also view t as a parameter for Spec $\hat{\mathcal{O}}_{Y^{st},\overline{u}}$ for any point $\overline{u} \in \overline{Y}$ above $\overline{d}$. Then t' can be viewed as a parameter for Spec $\hat{\mathcal{O}}_{Y^{st},\gamma(\overline{u})}$. Write $\eta_{2^n,q} = \sum_{\ell=0}^\infty z_\ell t^\ell dt$ and $\eta_{2^n,\gamma q} = \sum_{\ell=0}^\infty z'_\ell (t')^\ell dt'$. By [1, Theorem 4.1] (setting $q=1$ in that theorem),

$$v(\beta_\gamma(q)) = \lim_{i\to\infty} v\left(\frac{z_{\ell_i}}{z'_{\ell_i}}\right),$$

where ℓ_i is any sequence such that $\lim_{i\to\infty} v(z_{\ell_i}) - v(\ell_i+1) = -\infty$. Take $\ell_i = 2^i-1$. Then, by Remark 3.4, Corollary 4.8, (3.6), and (3.7), we have

$$v(z_{\ell_i}) = (n-s)(\langle\sigma\rangle-1) - n\varepsilon_q + \frac{i}{2} + (n - \frac{s}{2} + \frac{1}{2})$$

and

$$v(z'_{\ell_i}) = (n-s)(\langle\gamma\sigma\rangle-1) - n\varepsilon_{\gamma q} + \frac{i}{2} + (n - \frac{s}{2} + \frac{1}{2}).$$

So

$$v(\beta_\gamma(q)) = (n-s)(\langle\sigma\rangle - \langle\gamma\sigma\rangle) + n(\varepsilon_{\gamma q} - \varepsilon_q).$$

Some rearranging shows that this is equal to

$$n(\langle\gamma\rho\rangle - \langle\rho\rangle) + s(\langle\gamma\sigma\rangle - \langle\sigma\rangle) + n(\langle\gamma\tau\rangle - \langle\tau\rangle),$$

which is equal to the expression in the proposition.

3.3 Finishing the product formula

If $\gamma \in I_{\mathbb{Q}_2}$ and $r \in \mathbb{Q}/\mathbb{Z}$, then let $w_{2,\gamma}(r) = w_2(a_r) - w_2(a_{\gamma r})$, where the terms on the right hand side are defined in §2. The following result is an important consequence of Proposition 3.6.

Corollary 3.7 *Let $\gamma \in I_{\mathbb{Q}_2}$. If $q = (\rho, \sigma, \tau) \in (\mathbb{Q}/\mathbb{Z})^3$ with $\rho + \sigma + \tau = 0$, and none of $\langle \rho \rangle$, $\langle \sigma \rangle$, or $\langle \tau \rangle$ is $\frac{1}{2}$, then $w_{2,\gamma}(\rho) + w_{2,\gamma}(\sigma) + w_{2,\gamma}(\tau) = 0$.*

Proof This has already been proven in [3, Lemme III.2.5] when any of ρ, σ, or τ is in $\mathbb{Z}_{(2)}/\mathbb{Z}$, so we assume otherwise. Furthermore, [3, Lemme III.2.6] states that $w_{2,\gamma}(\alpha) = w_{2,\gamma}(\alpha')$ whenever $\alpha - \alpha' \in \mathbb{Z}_{(2)}/\mathbb{Z}$. For each $\alpha \in (\mathbb{Q}/\mathbb{Z})$, there is a unique $\alpha' \in \mathbb{Q}/\mathbb{Z}$ such that $\alpha - \alpha' \in \mathbb{Z}_{(2)}/\mathbb{Z}$ and $\langle \alpha' \rangle = \frac{j}{k}$, where k is a power of 2. Furthermore, if $\rho + \sigma + \tau = 0$, then $\rho' + \sigma' + \tau' = 0$. So we may assume that the denominators of ρ, σ, and τ are powers of 2.

Let n be minimal such that $\langle \rho \rangle = \frac{a}{2^n}$, $\langle \sigma \rangle = \frac{b}{2^n}$, and $\langle \tau \rangle = \frac{c}{2^n}$, with $a, b, c \in \mathbb{Z}$. Then $n \geq 3$. Assume without loss of generality that $v_2(b) \geq \max(v_2(a), v_2(c))$. Then a and c must be odd, and $1 \leq v(b) \leq n-2$ (cf. §3.2—recall that we assume that $\langle \sigma \rangle \notin \{0, \frac{1}{2}\}$).

One can then copy the proof of [3, Lemme III.2.5], with our Proposition 3.6 substituting for [1, Corollary 7.6]. In more detail,

$$w_{2,\gamma}(\rho) + w_{2,\gamma}(\sigma) + w_{2,\gamma}(\tau) = w_2(b_q) - w_2(b_{\gamma q}).$$

Using the definitions from §2, this is equal to

$$V_2(b_{\gamma q}) - V_2(b_q) + v_2(\omega_q) - v_2(\omega_{\gamma q}),$$

which is equal to

$$V_2(b_{\gamma q}) - V_2(b_q) - v(\beta_\gamma(q)),$$

by Lemma 2.1. By Proposition 3.6 and the fact that $\rho_{(2)}$, $(\gamma\rho)_{(2)}$, $\sigma_{(2)}$, $(\gamma\sigma)_{(2)}$, $\tau_{(2)}$, and $(\gamma\tau)_{(2)}$ are all zero (Equation (2.1)), this is equal to zero.

Corollary 3.8 *For all $\gamma \in I_{\mathbb{Q}_2}$ and r in $\mathbb{Q}/\mathbb{Z}$, we have $w_{2,\gamma}(r) = 0$.*

Proof If $\langle r \rangle \in \{0, \frac{1}{2}\}$, then $r = \gamma r$, thus $w_{2,\gamma}(r) = 0$ by definition. We also have $w_{2,\gamma}(-r) = -w_{2,\gamma}(r)$ for all $r \in \mathbb{Q}/\mathbb{Z}$ (this follows from plugging $(\rho, \sigma, \tau) = (r, -r, 0)$ into Corollary 3.7, unless $\langle r \rangle = \frac{1}{2}$, in which case it is obvious). Plugging any triple $(a, b, -(a+b))$ into Corollary 3.7 then shows that

$$w_{2,\gamma}(a) + w_{2,\gamma}(b) = w_{2,\gamma}(a+b),$$

as long as none of $\langle a \rangle$, $\langle b \rangle$, or $\langle a+b \rangle$ is $\frac{1}{2}$.

We now claim that, if $k > 4$ is even, and if $a \in \mathbb{Q}/\mathbb{Z}$ satisfies $\langle a \rangle = \frac{1}{k}$, then $w_{2,\gamma}(ja) = jw_{2,\gamma}(a)$ for $1 \leq j \leq \frac{k}{2} - 1$ and for $\frac{k}{2} + 1 \leq j \leq k$. Admitting the claim, we set $j = k$ to show that $w_{2,\gamma}(a) = 0$, which in turn shows that $w_{2,\gamma}(ja) = 0$ for all j above. Since any $r \in ([0,1) \cap \mathbb{Q}) \backslash \{\frac{1}{2}\}$ is the fractional part of some such ja, the claim implies the corollary.

To prove the claim, we note by additivity of $w_{2,\gamma}$ that $w_{2,\gamma}(ja) = jw_{2,\gamma}(a)$ for $1 \le j \le \frac{k}{2} - 1$. By additivity again (using $(\frac{k}{2} - 1)a$ and $2a$, neither of which has fractional part $\frac{1}{2}$), we have $w_{2,\gamma}((\frac{k}{2}+1)a) = (\frac{k}{2}+1)w_{2,\gamma}(a)$. Then, additivity shows that $w_{2,\gamma}(ja) = jw_{2,\gamma}(a)$ for $\frac{k}{2}+1 \le j \le k$.

Theorem 3.9 *We have $w_2(a) = 0$ for all $a \in \mathscr{C}\mathscr{M}^{ab}$.*

Proof This follows from Corollary 3.8 exactly as [3, Corollaire III.2.7] follows from [3, Lemme III.2.6(i)].

Theorem 3.9 completes the proof of Colmez's product formula when the field of complex multiplication is an abelian extension of $\mathbb{Q}$.

Remark 3.10 Colmez already proved Corollary 3.8 when $r \in \frac{1}{8}\mathbb{Z}_{(2)}/\mathbb{Z}$ ([3, Lemma III.2.8]). This was used to give a geometric proof of the Chowla-Selberg formula ([3, III.3]).

4 Computations

The results of this section are used only in the proof of Proposition 3.6.

4.1 Base 2 expansions

Let $S(\ell)$ be the sum of the digits in the base 2 expansion of ℓ, or ∞ if $\ell \in \mathbb{Q}\setminus\{0,1,2,\ldots\}$. It is clear that $S(\ell) = 1$ iff ℓ is an integer and a power of 2. Note also that if ℓ_1 and ℓ_2 are positive integers whose ratio is a power of 2, then $S(\ell_1) = S(\ell_2)$.

Lemma 4.1 *If ℓ_1 and ℓ_2 are nonnegative integers, then $S(\ell_1+\ell_2) \le S(\ell_1)+S(\ell_2)$. Equality never holds if $\ell_1 = \ell_2$. Furthermore, if ℓ is a positive integer, there are exactly $2^{S(\ell)} - 2$ ordered pairs of positive integers (ℓ_1, ℓ_2) such that $\ell_1 + \ell_2 = \ell$ and $S(\ell_1) + S(\ell_2) = S(\ell)$.*

Proof The first two assertions are clear from the standard addition algorithm. Now, for positive integers ℓ_1 and ℓ_2, we have $S(\ell_1+\ell_2) = S(\ell_1)+S(\ell_2)$ exactly when no carrying takes place in the addition of ℓ_1 and ℓ_2 in base 2. This happens when ℓ_1 is formed by taking a nonempty, proper subset of the 1's in the base 2 expansion of ℓ, and converting them to zeros. There are $2^{S(\ell)-2}$ such subsets, proving the lemma.

The following lemma gathers several elementary facts. The somewhat strange phrasings will pay off in §3. Notice that all inequalities are phrased in terms of something being less than or equal to $\frac{1}{2}S(\ell)$.

Lemma 4.2 *Let ℓ be a positive integer.*

(i) $2S(\frac{\ell}{4}) - 2 \le \frac{1}{2}S(\ell)$ *iff $\ell \ge 4$ is a power of 2.*
(ii) $S(\frac{\ell}{2}) - 1 \le \frac{1}{2}S(\ell)$ *iff $S(\ell) \le 2$ and ℓ is even.*

(iii) *There are exactly* $2^{S(\ell)}-2$ *ordered pairs of positive integers* (ℓ_1,ℓ_2) *such that* $\ell_1+\ell_2=\ell$ *and* $\frac{1}{2}S(\ell_1)+\frac{1}{2}S(\ell_2)\leq\frac{1}{2}S(\ell)$.

(iv) *If* ℓ_1 *and* ℓ_2 *are distinct positive integers such that* $2(\ell_1+\ell_2)=\ell$, *then* $S(\ell_1)+S(\ell_2)-1\leq\frac{1}{2}S(\ell)$ *iff* $S(\ell_1)=S(\ell_2)=1$ *and* $S(\ell)=2$.

(v) *If* ℓ_1, ℓ_2, *and* ℓ_3 *are positive integers, not all distinct, such that* $\ell_1+\ell_2+\ell_3=\ell$, *then it is never the case that* $\frac{1}{2}S(\ell_1)+\frac{1}{2}S(\ell_2)+\frac{1}{2}S(\ell_3)\leq\frac{1}{2}S(\ell)$.

(vi) *If* ℓ_1 *and* ℓ_2 *are distinct positive integers such that* $\ell_1+3\ell_2=\ell$, *then it is never the case that* $\frac{1}{2}S(\ell_1)+\frac{3}{2}S(\ell_2)\leq\frac{1}{2}S(\ell)$.

(vii) *If* ℓ_1, ℓ_2, *and* ℓ_3 *are distinct positive integers such that* $\ell_1+\ell_2+2\ell_3=\ell$, *then it is never the case that* $\frac{1}{2}S(\ell_1)+\frac{1}{2}S(\ell_2)+S(\ell_3)\leq\frac{1}{2}S(\ell)$.

(viii) *If* ℓ_1, ℓ_2, ℓ_3, *and* ℓ_4 *are distinct nonnegative integers such that* $\ell_1+\ell_2+\ell_3+\ell_4=\ell$, *then it is never the case that* $\frac{1}{2}S(\ell_1)+\frac{1}{2}S(\ell_2)+\frac{1}{2}S(\ell_3)+\frac{1}{2}S(\ell_4)+1\leq\frac{1}{2}S(\ell)$.

Proof Parts (i) and (ii) are easy, using that $S(\ell/4)$ and $S(\ell/2)$ are either equal to $S(\ell)$ or ∞. Part (iii) follows from Lemma 4.1. Part (iv) follows from that fact that $S(\ell)=S(\ell_1+\ell_2)\leq S(\ell_1)+S(\ell_2)$. Parts (v), (vi), (vii), and (viii) also follow from Lemma 4.1.

4.2 Power series

As in §3, let $f:Y\to X=\mathbb{P}^1$ be the branched cover of smooth curves given birationally by $y^{2^n}=x^a(x-1)^b$ where a is odd, $1\leq v_2(b)\leq n-2$, and $0<a,b<2^n$. Throughout this section, we take $K/\mathbb{Q}_2$ to be a finite extension over which f admits a stable model, and R to be the ring of integers of K. We will take further finite extensions of K and R as necessary. The valuation v on K (and any finite extension) is always normalized so that $v(2)=1$. Throughout this section, we fix a square root i of -1 in K. We let $f^{st}:Y^{st}\to X^{st}$ be the stable model of f, and $\overline{f}:\overline{Y}\to\overline{X}$ its stable reduction (§3.1).

Set $d=\frac{a}{a+b}+\frac{\sqrt{2^nbi}}{(a+b)^2}$, and $s:=n-v_2(b)\geq 2$. Let $\overline{d}$ be the specialization of d in $\overline{X}$. Let e be any element of R with valuation $n-\frac{s}{2}+\frac{1}{2}$. If $x=d+et$, then t is a parameter of $\hat{\mathscr{O}}_{X^{st},\overline{d}}$ (Corollary 3.5). We set

$$g(x)=x^a(x-1)^bd^{-a}(d-1)^{-b}.$$

Note that $g(d)=1$.

Lemma 4.3 *Expanding out* $g(x)$ *in terms of* t *yields an expression of the form*

$$\gamma(t):=g(d+et)=\sum_{\ell=0}^{\infty}c_\ell t^\ell$$

where $c_0=1$, $v(c_2)=n$, $\frac{c_1^2}{c_2}\equiv 2^{n+1}i \pmod{2^{n+2}}$, *and* $v(c_\ell)>n+\frac{1}{2}S(\ell)$ *for all* $\ell\geq 3$. *In particular,* $v(c_1)=n+\frac{1}{2}$.

Remark 4.4 Of course, the "series" above is actually just a polynomial.

Proof The claim at the beginning of the proof of the $p = 2$ part of [7, Lemma C.2] proves everything except the statement for $\ell \geq 3$. The continuation of the proof of *loc. cit.* leads to

$$v(c_\ell) = n + 1 + \frac{\ell - 2}{2}(s+1) - v(\ell) > n + \ell - 1 - v(\ell)$$

(recall, $s \geq 2$). It is easy to see that $\ell > 1 + v(\ell) + \frac{1}{2}S(\ell)$ for $\ell \geq 3$, from which the lemma follows.

We wish to understand the 2^nth root of $\gamma(t)$. It turns out that it is easier to do this by first taking a 2^{n-2}th root, and then a 4th root.

Lemma 4.5 *After possibly replacing R by a finite extension, the power series $\gamma(t) = \sum_{\ell=0}^{\infty} c_\ell t^\ell$ from Lemma 4.3 has a 2^{n-2}nd root in $R[[t]]$ of the form*

$$\delta(t) = \sum_{\ell=0}^{\infty} d_\ell t^\ell,$$

where $d_0 = 1$, $v(d_2) = 2$, $\frac{d_1^2}{d_2} \equiv 8i \pmod{16}$, and $v(d_\ell) > 2 + \frac{1}{2}S(\ell)$ for $\ell \geq 3$. In particular, $v(d_1) = \frac{5}{2}$.

Proof Let $w = \gamma(t) - 1$. Binomially expanding $(1+w)^{1/2^{n-2}}$ gives

$$\delta(t) = 1 + \frac{w}{2^{n-2}} + \sum_{j=2}^{\infty} \binom{1/2^{n-2}}{j} w^j.$$

The valuation of $\binom{1/2^{n-2}}{j}$ is

$$S(j) - j - j(n-2) = S(j) + j - jn.$$

On the other hand, the valuation of c_ℓ (the coefficient of t^ℓ in w) is at least $n + \frac{1}{2}S(\ell) - \frac{1}{2}$ (Lemma 4.3, the equality only holds for $\ell = 2$). So, by Lemma 4.1, the coefficient of t^ℓ in w^j for $j \geq 2$ has valuation greater than $jn + \frac{1}{2}S(\ell) - \frac{j}{2}$ (equality could only occur if $\ell = 2j$, but in fact, does not, because $j(n + \frac{1}{2}S(2) - \frac{1}{2}) > jn + \frac{1}{2}S(2j) - \frac{j}{2}$). Combining everything, the coefficient of t^ℓ in $\binom{1/2^{n-2}}{j} w^j$ (for $j \geq 2$) has valuation greater than $S(j) + \frac{j}{2} + \frac{1}{2}S(\ell)$, which is at least $2 + \frac{1}{2}S(\ell)$.

Thus, for the purposes of the lemma, we may replace $\delta(t)$ by $1 + \frac{w}{2^{n-2}}$. The lemma then follows easily from Lemma 4.3.

Proposition 4.6 *After possibly replacing R by a finite extension, the power series $\delta(t) = \sum_{\ell=0}^{\infty} d_\ell t^\ell$ from Lemma 4.5 has a 4th root in $R[[t]]$ of the form*

$$\alpha(t) = \sum_{j=0}^{\infty} a_\ell t^\ell,$$

where $a_0 = 1$, and

$$a_\ell \equiv d_1^\ell (1+i)^{S(\ell) - 5\ell} \pmod{(1+i)^{S(\ell)+1}}.$$

In particular, $v(a_\ell) = \frac{1}{2}S(\ell)$.

Remark 4.7 Note that $\alpha(t)$ is a 2^nth root of

$$g(d+et) = x^a(x-1)^b d^{-a}(d-1)^{-b},$$

where $x = d+et$.

Proof (of Proposition 4.6) By Proposition 3.1(ii), the stable model f^{st} of f splits completely above $\hat{\mathscr{O}}_{X^{st},\overline{d}} = R[[t]]$. Thus, by [8, Proposition 3.2.3 (2)], $x^a(x-1)^b$ (when written in terms of t) is a 2^nth power in $R[[t]]$. This does not change when it is multiplied by the constant $d^{-a}(d-1)^{-b}$ (as long as we extend R appropriately), so we see that $\alpha(t)$ lives in $R[[t]]$ (this can also be shown using an explicit computation with the binomial theorem).

We have the equation

$$\left(1+\sum_{\ell=1}^{\infty} a_\ell t^\ell\right)^4 \equiv 1+\sum_{\ell=1}^{\infty} d_\ell t^\ell. \tag{4.1}$$

We prove the proposition by strong induction, treating the base cases $\ell = 1$, 2 separately. Recall that $v(d_1) = \frac{5}{2}$ and $v(d_2) = 2$. For $\ell = 1$, we obtain from (4.1) that $d_1 = 4a_1$, so

$$a_1 = \frac{d_1}{4} \equiv d_1(1+i)^{-4} \pmod{(1+i)^2}.$$

For $\ell = 2$, we obtain

$$d_2 = 4a_2 + 6a_1^2 = 4a_2 + \frac{3}{8}d_1^2,$$

so $a_2 = \frac{d_2}{4} - \frac{3}{32}d_1^2$. Using that $\frac{d_1^2}{d_2} \equiv 8i \pmod{16}$ (Lemma 4.5), one derives that $\frac{d_2}{4} \equiv \frac{d_1^2}{32i} \pmod{2}$. Thus,

$$a_2 \equiv (-i-3)\frac{d_1^2}{32} \equiv d_1^2(1+i)^{-9} \pmod{(1+i)^2},$$

proving the proposition for $\ell = 2$.

Now, suppose $\ell > 2$. Then (4.1) yields (setting $a_j = 0$ for any $j \notin \mathbb{Z}$, and with all ℓ_i assumed to be positive integers):

$$\begin{aligned} d_\ell = {} & 4a_\ell + 6a_{\ell/2}^2 + 4a_{\ell/3}^3 + a_{\ell/4}^4 + \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell_2}} 12a_{\ell_1}a_{\ell_2} + \sum_{\substack{\ell_1+\ell_2+\ell_3=\ell \\ \ell_1<\ell_2<\ell_3}} 24a_{\ell_1}a_{\ell_2}a_{\ell_3} \\ & + \sum_{\substack{\ell_1+2\ell_2=\ell \\ \ell_1\neq\ell_2}} 12a_{\ell_1}a_{\ell_2}^2 + \sum_{\substack{\ell_1+3\ell_2=\ell \\ \ell_1\neq\ell_2}} 4a_{\ell_1}a_{\ell_2}^3 + \sum_{\substack{\ell_1+\ell_2+\ell_3+\ell_4=\ell \\ \ell_1<\ell_2<\ell_3<\ell_4}} 24a_{\ell_1}a_{\ell_2}a_{\ell_3}a_{\ell_4} \\ & + \sum_{\substack{\ell_1+\ell_2+2\ell_3=\ell \\ \ell_1<\ell_2,\ell_3\neq\ell_1,\ell_3\neq\ell_2}} 12a_{\ell_1}a_{\ell_2}a_{\ell_3}^2 + \sum_{\substack{2\ell_1+2\ell_2=\ell \\ \ell_1<\ell_2}} 6a_{\ell_1}^2 a_{\ell_2}^2. \end{aligned}$$

or

$$a_\ell = -\frac{1}{4}d_\ell + \frac{3}{2}a_{\ell/2}^2 + a_{\ell/3}^3 + \frac{1}{4}a_{\ell/4}^4 + \sum_{\substack{\ell_1+\ell_2=\ell\\ \ell_1<\ell_2}} 3a_{\ell_1}a_{\ell_2} + \sum_{\substack{\ell_1+\ell_2+\ell_3=\ell\\ \ell_1<\ell_2<\ell_3}} 6a_{\ell_1}a_{\ell_2}a_{\ell_3}$$
$$+ \sum_{\substack{\ell_1+2\ell_2=\ell\\ \ell_1\neq\ell_2}} 3a_{\ell_1}a_{\ell_2}^2 + \sum_{\substack{\ell_1+3\ell_2=\ell\\ \ell_1\neq\ell_2}} a_{\ell_1}a_{\ell_2}^3 + \sum_{\substack{\ell_1+\ell_2+\ell_3+\ell_4=\ell\\ \ell_1<\ell_2<\ell_3<\ell_4}} 6a_{\ell_1}a_{\ell_2}a_{\ell_3}a_{\ell_4}$$
$$+ \sum_{\substack{\ell_1+\ell_2+2\ell_3=\ell\\ \ell_1<\ell_2,\ell_3\neq\ell_1,\ell_3\neq\ell_2}} 3a_{\ell_1}a_{\ell_2}a_{\ell_3}^2 + \sum_{\substack{2\ell_1+2\ell_2=\ell\\ \ell_1<\ell_2}} \frac{3}{2}a_{\ell_1}^2a_{\ell_2}^2.$$

Since we need only determine a_ℓ modulo $(1+i)^{S(\ell)+1}$, and all terms on the right hand side have half-integer valuation, we can ignore all terms with valuation greater than $\frac{1}{2}S(\ell)$. Using the inductive hypothesis, along with Lemmas 4.5 and 4.2 (v), (vi), (vii), and (viii), we obtain

$$a_\ell \equiv \frac{3}{2}a_{\ell/2}^2 + \frac{1}{4}a_{\ell/4}^4 + \sum_{\substack{\ell_1+\ell_2=\ell\\ \ell_1<\ell_2}} 3a_{\ell_1}a_{\ell_2} + \sum_{\substack{2\ell_1+2\ell_2=\ell\\ \ell_1<\ell_2}} \frac{3}{2}a_{\ell_1}^2a_{\ell_2}^2 \pmod{(1+i)^{S(\ell)+1}}. \tag{4.2}$$

If ℓ is a power of 2 (i.e., $S(\ell)=1$), then by Lemma 4.2 (i)–(iv), the induction hypothesis, and (4.2), we have

$$a_\ell \equiv \frac{3}{2}a_{\ell/2}^2 + \frac{1}{4}a_{\ell/4}^4 \equiv d_1^\ell\left(\frac{3}{2}(1+i)^{2-5\ell} + \frac{1}{4}(1+i)^{4-5\ell}\right)$$
$$\equiv d_1^\ell(3i-1)(1+i)^{-5\ell} \equiv d_1^\ell(1+i)^{1-5\ell} \pmod{(1+i)^2},$$

thus proving the proposition for such ℓ.

For all other ℓ, we have (by Lemma 4.2 (i), the induction hypothesis, and (4.2)) that

$$a_\ell \equiv \frac{3}{2}a_{\ell/2}^2 + \sum_{\substack{\ell_1+\ell_2=\ell\\ \ell_1<\ell_2}} 3a_{\ell_1}a_{\ell_2} + \sum_{\substack{2\ell_1+2\ell_2=\ell\\ \ell_1<\ell_2}} \frac{3}{2}a_{\ell_1}^2a_{\ell_2}^2 \pmod{(1+i)^{S(\ell)+1}}. \tag{4.3}$$

By Lemma 4.2 (ii) and (iv), the first and last terms matter only when $S(\ell)=2$ and ℓ is even, in which case their combined contribution is

$$3d_1^\ell(1+i)^{4-5\ell} \pmod{(1+i)^3},$$

which is trivial. So in any case, we need only worry about the middle term. By Lemma 4.2 (iii), the middle term is the sum of $2^{S(\ell)-1}-1$ subterms, each congruent to

$$3d_1^\ell(1+i)^{S(\ell)-5\ell} \pmod{(1+i)^{S(\ell)+1}}.$$

Since $S(\ell)\geq 2$, this sum is in turn congruent to

$$d_1^\ell(1+i)^{S(\ell)-5\ell} \pmod{(1+i)^{S(\ell)+1}},$$

proving the proposition.

Corollary 4.8 *In the notation of Proposition 4.6, the power series*

$$\tilde{\alpha}(t) := \frac{d(1-d)\alpha(t)}{x(1-x)} = \frac{d(1-d)\alpha(t)}{(d+et)(1-d-et)}$$

has the form

$$\sum_{i=0}^{\infty} \tilde{a}_\ell t^\ell,$$

where $\tilde{a}_0 = 1$ *and* $v(\tilde{a}_\ell) = v(a_\ell) = \frac{1}{2}S(\ell)$ *for all* ℓ*.*

Proof Recall that $v(1-d) = n-s$ (Remark 3.4), that $v(e) = n - \frac{s-1}{2}$, and that we assume $2 \leq s \leq n-1$. Set $\mu = -\frac{e}{d}$ and $\nu = \frac{e}{1-d}$. Then $v(\mu) = n - \frac{s-1}{2} > 1$ and $v(\nu) = \frac{s+1}{2} > 1$. Expanding $\tilde{\alpha}(t)$ out as a power series yields

$$\tilde{\alpha}(t) = \alpha(t)(1+\mu t+\mu^2 t^2+\cdots)(1+\nu t+\nu^2 t^2+\cdots) = \alpha(t)(1+\xi_1 t+\xi_2 t^2+\cdots),$$

where $v(\xi_\ell) > \ell$ for all ℓ. The constant term is 1, so $\tilde{a}_0 = 1$. The coefficient of t^ℓ is

$$\tilde{a}_\ell = a_\ell + \xi_\ell + \sum_{j=1}^{\ell-1} a_{\ell-j}\xi_j.$$

We know $v(a_\ell) = \frac{1}{2}S(\ell)$. We have seen that $v(\xi_\ell) > \ell > \frac{1}{2}S(\ell)$. Also, for $1 \leq j \leq \ell-1$, we have

$$v(a_{\ell-j}\xi_j) > \frac{1}{2}S(\ell-j)+j > \frac{1}{2}S(\ell-j)+\frac{1}{2}S(j) \geq \frac{1}{2}S(\ell).$$

By the non-archimedean property, we conclude that $v(\tilde{a}_\ell) = \frac{1}{2}S(\ell)$.

Remark 4.9 Note that $v(\tilde{a}_\ell)$ does not depend on a or b.

Acknowledgements I thank Pierre Colmez, Dick Gross, Johan de Jong, Melissa Liu, and Shouwu Zhang for useful conversations. In particular, I thank Michel Matignon for pointing me in the direction of this question. I also thank the referee for useful expository suggestions.

References

1. Coleman, Robert. On the Frobenius matrices of Fermat curves. In: *p*-adic analysis (Trento, 1989), Lecture Notes in Math. 1454, pp. 173–193. Springer, Berlin (1990)
2. Coleman, Robert; McCallum, William. Stable reduction of Fermat curves and Jacobi sum Hecke characters. J. Reine Angew. Math. 385, 41–101 (1988)
3. Colmez, Pierre. Périodes des variétés abéliennes à multiplication complexe. Ann. of Math. (2) 138, no. 3, 625–683 (1993)
4. Deligne, Pierre; Mumford, David. The irreducibility of the space of curves of given genus. Inst. Hautes Études Sci. Publ. Math. 36, 75–109 (1969)
5. Lehr, Claus; Matignon, Michel. Wild monodromy and automorphisms of curves. Duke Math. J. 135, no. 3, 569–586 (2006)
6. Liu, Qing. Stable reduction of finite covers of curves. Compos. Math. 142, no. 1, 101–118 (2006)
7. Obus, Andrew. Fields of moduli of three-point *G*-covers with cyclic *p*-Sylow, I, to appear in Algebra Number Theory. http://arxiv.org/abs/0911.1103v5 (2011)
8. Raynaud, Michel. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. Invent. Math. 116, no. 1-3, 425–462 (1994)
9. Raynaud, Michel. Specialization des revêtements en caractéristique $p > 0$. Ann. Sci. École Norm. Sup. (4) 32, no. 1, 87–126 (1999)
10. Yang, Tonghai. The Chowla-Selberg formula and the Colmez conjecture. Canad. J. Math. 62, no. 2, 456–472 (2010)