

CONGRUENCES BETWEEN THE COEFFICIENTS OF THE TATE CURVE VIA FORMAL GROUPS

ANTONIOS BROUMAS

(Communicated by David E. Rohrlich)

ABSTRACT. Let $E_q : Y^2 + XY = X^3 + h_4X + h_6$ be the Tate curve with canonical differential, $\omega = dX/(2Y + X)$. If the characteristic is $p > 0$, then the Hasse invariant, H , of the pair (E_q, ω) should equal one. If $p > 3$, then calculation of H leads to a nontrivial separable relation between the coefficients h_4 and h_6 . If $p = 2$ or $p = 3$, Thakur related h_4 and h_6 via elementary methods and an identity of Ramanujan. Here, we treat uniformly all characteristics via explicit calculation of the formal group law of E_q . Our analysis was motivated by the study of the invariant A which is an infinite Witt vector generalizing the Hasse invariant.

1. INTRODUCTION

The Tate curve in characteristic either zero or positive is an elliptic curve with canonical Weierstrass model:

$$(1) \quad E_q : Y^2 + XY = X^3 + h_4X + h_6$$

$$\text{where } h_4 = -5S_3 \quad \text{and} \quad h_6 = -\frac{5S_3 + 7S_5}{12} \quad \text{for} \quad S_k = \sum_{n \geq 1} \frac{n^k}{1 - q^n}.$$

Note that the denominator appearing in the expression of h_6 is simply a notational convenience and in fact E_q is defined over $\mathbb{Z}[[q]]$. Hence, since all coefficients are integral, we can specialize to positive characteristic p for any prime p of our choice and obtain E_q defined over $\mathbb{F}_p[[q]]$.

In all positive characteristics the Hasse invariant of the pair (E_q, ω) for ω the canonical invariant differential, $\omega = dX/(2Y + X)$, is equal to 1. See [KM], 8.8, p. 258 and 12.4.2, p. 355. It turns out that if the characteristic is greater than 3, explicit calculation of H leads to a separable algebraic relation between h_4 and h_6 . If the characteristic is equal to 2 or 3, then H is identically one and no relation is thus obtained. However, in characteristic 2 we have $h_4 = h_6$, and in characteristic 3 we have $h_4 - h_4^2 + h_6 = 0$, relations produced in [T] by Thakur via elementary methods and an identity of Ramanujan.

Our goal is to provide a unified approach to the identities involving h_4 and h_6 . The starting point of this work is the following—one of many—alternative calculation-definition of the Hasse invariant involving the formal group of E_q : Let L

Received by the editors April 27, 1998.

1991 *Mathematics Subject Classification*. Primary 11F33; Secondary 11G07, 14G20.

Key words and phrases. Tate curve, Hasse invariant, formal group, p -typical, invariant A .

be a local parameter at the origin satisfying: $\omega = (1 + \dots)dL$. Then $H = H(E_q, \omega)$ is the coefficient of L^p in the power series denoting multiplication by p in the formal group of E_q calculated with respect to L . That is, $[p]_{\widehat{E}_q}[L] = H \cdot L^p + O[L^{2p}]$.

However, the formal group laws, $\widehat{E}_q[L_1, L_2]$, of the Tate curve and, $\widehat{\mathbb{G}}_m^-(l_1, l_2)$, of the multiplicative group scheme are isomorphic and for appropriate choices of local parameters, cf. (2.3), we have: $L = \alpha(l)$ for α a power series in l with coefficients in $\mathbb{F}[[q]]$. This leads to: $[p]_{\widehat{E}_q}(\alpha(l)) = \alpha(l^p)$ since $[p]_{\widehat{\mathbb{G}}_m^-}[l] = l^p$. Our plan is to calculate the formal group law \widehat{E}_q and the isomorphism α explicitly and obtain as byproduct the algebraic dependence of h_4 and h_6 in all positive characteristics.

The motivation for this paper was the calculation of the A invariant of the Tate curve. The A invariant, which is an infinite Witt vector, generalizes Hasse's invariant and is defined by: $F\eta = A\eta$ for η a basis of the first Witt vector cohomology group $H^1(E, W\mathcal{O}_E)$ and F the map in cohomology induced by the absolute Frobenius on the structure sheaf of E . If E is ordinary, $H^1(E, W\mathcal{O}_E)$ is isomorphic to the module of p -typical curves of the formal group \widehat{E} . In analogy to the canonical differential of the Tate curve, $\omega_{\text{can}} = dX/(2Y + X)$, with corresponding Hasse invariant equal to 1, there exists a canonical basis η_{can} of $H^1(E, W\mathcal{O}_E)$ and all our subsequent work can be viewed as a verification of the fact $A(E_{\text{Tate}}, \eta_{\text{can}}) = (1, 0, 0, \dots) = 1$ in $W(\mathbb{F}_p[[q]])$. More details on A will be published in [B].

2. FORMAL GROUPS

2.1. Foundations. We restrict ourselves to the one dimensional case. Unless specifically stated, the characteristic of R is not necessarily positive. See [H] for a comprehensive account. A formal group law \widehat{G} over a ring R is a double power series in $R[[l_1, l_2]]$ starting with $l_1 + l_2$ and satisfying the associativity condition: $\widehat{G}(l_1, \widehat{G}(l_2, l_3)) = \widehat{G}(\widehat{G}(l_1, l_2), l_3)$. A homomorphism from a formal group law \widehat{G} to a formal group law \widehat{F} is a power series α without constant term satisfying $\alpha(\widehat{G}(l_1, l_2)) = \widehat{F}(\alpha(l_1), \alpha(l_2))$. An isomorphism is a homomorphism possessing a left and right inverse.

For E an elliptic curve and L a choice of local parameter at the identity, $\widehat{E}(L_1, L_2)$ is the corresponding formal group law and it can be calculated explicitly up to any desired accuracy following the algorithm in [S], Ch. IV, §1.

2.2. The formal group of the Tate curve. The Tate curve E_q given in (1) is a rigid analytic group over $\mathbb{Z}[[q]]$ isomorphic to the rigid analytic group $\mathbb{G}_m/q^{\mathbb{Z}}$ over $\mathbb{Z}[[q]]$. Hence, for every local field K and for every q of absolute value smaller than 1, $|q| < 1$, we have $K^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(K)$. See [DR], Ch. VII, and [R], §3. In fact for u a multiplicative parameter of K the isomorphism is explicitly given as equation (29) in [R], p. 26:

$$(2) \quad u \mapsto (X(u), Y(u)) = \left(\sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n \geq 1} \frac{n}{1 - q^n}, \sum_{n \in \mathbb{Z}} \frac{q^{2n} u^2}{(1 - q^n u)^3} + \sum_{n \geq 1} \frac{n}{1 - q^n} \right).$$

2.3. Formal group law isomorphism. The isomorphism above results in an isomorphism of formal group laws $\widehat{\mathbb{G}}_m/q^{\mathbb{Z}}$ and \widehat{E}_q . We make this isomorphism explicit after we specify local parameters.

The formal group of the rigid analytic group $\mathbb{G}_m/q^{\mathbb{Z}}$ is isomorphic to the formal group of \mathbb{G}_m . See [DR], 1.12, p. 296/154. Let $l = l(u) = 1 - 1/u$ be our choice of local parameter at the identity of the rigid analytic space \mathbb{G}_m . Then $u = u(l) = 1/(1 - l)$ and we can calculate the formal group law $\widehat{\mathbb{G}}_m$ with respect to the local parameter l :

$$(3) \quad \widehat{\mathbb{G}}_m(l_1, l_2) = l(u_1, u_2) = l(u(l_1) \cdot u(l_2)) = l_1 + l_2 - l_1 l_2.$$

Note that in order to use the integrality of the existing classical formulae the choice of local parameter had to be a power series in $t = u - 1$ with $\mathbb{Z}[[q]]$ coefficients and leading term $\pm t$ but otherwise arbitrary. Our particular choice, $l = t - t^2 + t^3 - t^4 + \dots$ will simplify the subsequent calculations.

Now let us choose as our local parameter at the identity of the Tate curve: $L = -X/Y$. Again L could have been any power series in X/Y invertible over $\mathbb{Z}[[q]]$ and our particular choice was made in order to simplify the presentation. In our notation formulae 30 and 31 in [R], p. 27, which are a direct consequence of equation 29 in [R] reproduced above as equation (2), read as:

$$(4) \quad X = \frac{1}{l^2} - \frac{1}{l} + O[l^2] \text{ and } Y = \frac{-1}{l^3} + \frac{1}{l^2} + O[l]$$

and the formal group laws $\widehat{E}_q(L_1, L_2)$ and $\widehat{\mathbb{G}}_m(l_1, l_2)$ calculated with respect to the local parameters L for the former and l for the latter are isomorphic via α satisfying:

$$(5) \quad \alpha(\widehat{\mathbb{G}}_m(l_1, l_2)) = \widehat{E}_q(\alpha(l_1), \alpha(l_2)) \text{ and}$$

$$(6) \quad L = -\left(\frac{X(l)}{Y(l)}\right) = \alpha(l) = l + O[l^5] \text{ and } l = \alpha^{-1}(L) = L + O[L^5].$$

3. MAIN CALCULATION

Note that the equation defining E_q and the power series α have integral coefficients and so we can specialize to any characteristic $p > 0$.

In all cases: (a) our choice of local parameter at the identity is $L = -X/Y$ and (b) the calculation of the series $[p]_{\widehat{E}_q}$ can be either carried out directly by repeated application of the corresponding formal group law or by expansion with respect to the chosen local parameter of the rational formulae of multiplication by p on E_q .

3.1. The case: $p \geq 5$. In this case we have two ways to obtain the desired relation. Note that the canonical differential $\omega = dX/(2Y + X)$ is equal to $(1 + \dots)dL$. Hence, the multiplication by p in the formal group calculated with respect to L , see [KM], 12.4, p. 353-354, is equal to:

$$(7) \quad \begin{aligned} [p]_{\widehat{E}_q}(L) &= H(E_q, \omega)L^p + \dots \\ &= \alpha\left([p]_{\widehat{\mathbb{G}}_m}(\alpha^{-1}(L))\right) = \alpha\left([p]_{\widehat{\mathbb{G}}_m}(L + \dots)\right) = \alpha(L^p + \dots) \\ &= L^p + \dots \end{aligned}$$

Now using either Deuring's algorithm to calculate H , or Silverman's algorithm to calculate \widehat{E}_q and subsequently $[p]_{\widehat{E}_q}$, see [D] and [S], loc. cit., we produce a nontrivial separable relation between h_4 and h_6 , the coefficients of the canonical Weierstrass model of E_q . To see this, change Weierstrass models for E_q to $y^2 = f(x)$ for $x = X + 1/12$ and $y = Y + X/2$ and work with: $E_q : y^2 = x^3 + (h_4 - 1/48)x +$

$(h_6 - h_4/12 + 1/864)$. Then calculate H as the coefficient of x^{p-1} in the expansion of $(f(x))^{(p-1)/2}$ and obtain:

$$(8) \quad 1 = H = \sum_{3i+j=p-1, i+j \leq \frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!j! \left(\frac{p-1}{2} - i - j\right)!} \left(h_4 - \frac{1}{48}\right)^j \left(h_6 - \frac{h_4}{12} + \frac{1}{864}\right)^{\frac{p-1}{2} - i - j}$$

binding h_4 and h_6 separably algebraically. Similarly we treat below the cases $p = 2$ and $p = 3$.

3.2. Characteristic 2. In this case the formal group law is:

$$(9) \quad \begin{aligned} \widehat{E}_q(L_1, L_2) = & L_1 + L_2 + L_1L_2 + h_4(L_1^2L_2^4 + L_1^4L_2^2) \\ & + h_6(L_1L_2^6 + L_1^6L_2) + (h_4 + h_6)(L_1^2L_2^5 + L_1^5L_2^2 + L_1^3L_2^4 + L_1^4L_2^3) \\ & + h_4(L_1^2L_2^6 + L_1^6L_2^2) + (h_4 + h_6)(L_1^3L_2^5 + L_1^5L_2^3 + L_1^4L_2^4) \\ & + O[L_1^mL_2^n, m+n \geq 9] \end{aligned}$$

and the multiplication by 2 is given by:

$$(10) \quad [2]_{\widehat{E}_q}(L) = L^2 + (h_4 + h_6)L^8 + O[L^{10}].$$

Proceeding as in (7), equating $\alpha\left([2]_{\widehat{G}_m}(\alpha^{-1}(L))\right) = L^2 + O[L^{10}]$ we obtain $h_4 + h_6 = 0$ and taking advantage of the denominator 12 appearing in the definition of h_6 we have: $S_3 \equiv S_5$ modulo 8.

3.3. Characteristic 3. In this case the formal group law is:

$$(11) \quad \begin{aligned} \widehat{E}_q(L_1, L_2) = & L_1 + L_2 - L_1L_2 + h_4(L_1L_2^4 + L_1^4L_2 - L_1^2L_2^3 - L_1^3L_2^2) \\ & + h_4(L_1L_2^5 + L_1^5L_2 + L_1^2L_2^4 + L_1^4L_2^2) \\ & + h_4(L_1L_2^6 + L_1^6L_2 - L_1^2L_2^5 - L_1^5L_2^2 - L_1^3L_2^4 - L_1^4L_2^3) \\ & + h_4(L_1L_2^7 + L_1^7L_2 - L_1^2L_2^6 - L_1^6L_2^2 - L_1^3L_2^5 - L_1^5L_2^3 - L_1^4L_2^4) \\ & + (h_4 + h_4^2)(L_1L_2^8 + L_1^8L_2 - L_1^3L_2^6 - L_1^6L_2^3) \\ & + (-h_4 + h_4^2)(L_1^4L_2^5 + L_1^5L_2^4) \\ & + (-h_6)(L_1^3L_2^6 + L_1^6L_2^3) + (-h_4)(L_1^2L_2^7 + L_1^7L_2^2) \\ & + O[L_1^mL_2^n, m+n \geq 10] \end{aligned}$$

and the multiplication by 3 is given by:

$$(12) \quad [3]_{\widehat{E}_q}(L) = L^3 + (h_4 - h_4^2 + h_6)L^9 + O[L^{10}].$$

Comparing with $\alpha\left([3]_{\widehat{G}_m}(\alpha^{-1}(L))\right) = L^3 + O[L^{15}]$ we conclude $h_4 - h_4^2 + h_6 = 0$, resulting in: $7S_3 + 6S_3^2 + 2S_5 = 0$ modulo 9.

ACKNOWLEDGEMENTS

I would like to thank Dr. Douglas Ulmer for all insightful conversations, Dr. Dinesh Thakur for presenting me the question which was originated in his paper, [T], and Dr. John Tate and Dr. Felipe Voloch for their continuous direction and encouragement.

REFERENCES

- [B] A. Broumas, The invariant A and the moduli problem $\text{Ig}(p^n)$, in preparation.
- [DR] P. Deligne, M. Rapoport, Les schemas des modules de courbes elliptiques, in *Modular functions in one variable II*, *Lecture Notes in Math.* **349** 143-316, Springer-Verlag (1973). MR **49**:2762
- [D] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197-272. MR **3**:104f
- [H] M. Hazewinkel, Formal groups and applications, *Pure and Applied Math.* **78** Academic Press (1978). MR **82a**:14020
- [KM] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Princeton Univ. Press (1985). MR **86i**:11024
- [R] P. Roquette, Analytic theory of elliptic functions over local fields, Vandehoeck and Ruprecht, Göttingen (1970). MR **41**:5376
- [S] J. Silverman, The arithmetic of elliptic curves, *Graduate Texts in Math.* **106** Springer-Verlag (1986). MR **87g**:11070
- [T] D. Thakur, Automata style proof of Voloch's result on transcendence, *Journal of Number Theory* **58** (1996) 60-62. MR **98a**:11100

MATHEMATICAL SCIENCES RESEARCH INSTITUTE, 1000 CENTENNIAL DR., BERKELEY, CALIFORNIA 94720

E-mail address: antonios_m@yahoo.com