Resultants and discriminants of multiplication polynomials for elliptic curves

Harry Schmidt
(with Appendix by Jung Kyu Canci and Harry Schmidt)

May 11, 2015

Abstract

In this article, we prove that the resultant of the standard multiplication polynomials A_n, B_n of an elliptic curve in the form $y^2 = x^3 + ax + b$ is $(16\Delta)^{\frac{n^2(n^2-1)}{6}}$, where $\Delta = -(4a^3 + 27b^2)$ is the discriminant of the curve. We give an application to good reduction of an associated Lattès map. We also prove a similar result for the discriminant of the largest squarefree factor of B_n.

1 Introduction

If a, b are elements of a field of characteristic not 2 or 3 with

$$\Delta = -(4a^3 + 27b^2) \neq 0,$$

then the equation

$$y^2 = x^3 + ax + b \tag{1}$$

defines an elliptic curve. It is well-known, see for example [Si1], Exercise 3.7 (p.105), that for each natural number n there are polynomials $A_n, B_n \neq 0$ in x such that multiplication by n sends the point $P = (x, y)$ to a point whose x-coordinate is $\frac{A_n(x)}{B_n(x)}$. The classical literature studied such things in detail, but mainly for the Weierstrass model with an extra coefficient 4 in (1); there we see functions ψ_n, ϕ_n. See among others Fricke [F, pp.184-196], Halphen [H, pp. 96-106] and Tannery and Molk [TM, pp.100-105]. For example

$$A_1(x) = x, \quad B_1(x) = 1, \quad A_2(x) = x^4 - 2ax^2 - 8bx + a^2, \quad B_2(x) = 4(x^3 + ax + b). \tag{2}$$

In general they are usually normalized by their leading terms

$$A_n(x) = x^{n^2} + \cdots, \quad B_n(x) = n^2 x^{n^2-1} + \ldots. \tag{3}$$

2010 Mathematics Subject Classification: 14H52, 11F30.

Key words: Elliptic curves, Fourier coefficients of automorphic forms

(see [Si1, Exercise 3.7(b)]). More terms seem to be difficult to find in the literature, classical or otherwise, and in connexion with another investigation Masser and Zannier [MZ] have recently found that

$$A_n(x) = x^{n^2} - \kappa_n a x^{n^2-2} - \lambda_n b x^{n^2-3} + \cdots, \quad B_n(x) = n^2 x^{n^2-1} + \mu_n a x^{n^2-3} + \cdots \tag{4}$$

where

$$\kappa_n = \frac{n^2(n^2-1)}{6}, \quad \lambda_n = \frac{2n^2(n^4-1)}{15}, \quad \mu_n = \frac{n^2(n^2-1)(n^2+6)}{30}. \tag{5}$$

With more work a few more early coefficients could be found but they get increasingly complicated, and it seems hopeless to obtain similar expressions for late coefficients like the constant terms.

A fundamental property is that A_n, B_n are coprime (see also [Si1, Exercise 3.7(c)]), which if $n \geq 2$ is equivalent to the non-vanishing of the resultant $\mathrm{res}(A_n, B_n)$. Here we mean this in a formal sense as if B_n had degree n^2-1 (see for example [L2, p.200]). It seems that no-one has ever calculated $\mathrm{res}(A_n, B_n)$ explicitly. As the resultant is given by a complicated Sylvester determinant looking like

$$\begin{vmatrix} 1 & 0 & -\kappa_n a & -\lambda_n b & \dots \\ 0 & 1 & 0 & -\kappa_n a & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \\ n^2 & 0 & \mu_n a & ? & \dots \\ 0 & n^2 & 0 & \mu_n a & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{vmatrix} \tag{6}$$

for (4), the task would at first sight seem difficult. Nevertheless it is what we do in the present paper, with a result that may initially seem surprisingly simple.

Theorem 1.1. *For natural numbers $n \geq 2$ we have*

$$\mathrm{res}(A_n, B_n) = (16\Delta)^{\frac{n^2(n^2-1)}{6}}.$$

It is a natural step from resultants to discriminants, and as B_n is known to play a major role in the study of torsion points it may seem justified to ask for its discriminant. Unfortunately if $n > 1$ then B_n is not squarefree and so this discriminant vanishes. But it can be shown (see [Si1, Exercise 3.7(a)]) that we have

$$B_n = B_n^{*2} \quad (n \text{ odd}) \tag{7}$$

$$B_n = B_n^{*2}/C \quad (n \text{ even}) \tag{8}$$

for a polynomial B_n^* unique up to sign, where $C = C(x) = x^3 + ax + b$. Here B_n^* is squarefree, at least in characteristic 0. In particular C divides B_n and B_n^* when n is even. We calculate the discriminant disc B_n^* (also in the formal sense - see also [L2, p.204]), at least up to sign, as follows.

Theorem 1.2. *For natural numbers $n \geq 2$ we have*

$$\text{disc } B_n^* \;=\; \pm n^{\frac{n^2-3}{2}}(16\Delta)^{\frac{(n^2-1)(n^2-3)}{24}} \quad (n \text{ odd}),$$

$$\text{disc } B_n^* \;=\; \pm n^{\frac{n^2}{2}} 2^{-(n^2-2)}(16\Delta)^{\frac{n^2(n^2+2)}{24}} \quad (n \text{ even}).$$

We can determine the signs (which are independent of the choice of B_n^*) in Theorem 1.2 but that involves messier calculations, so we just quote the results with a hint at the proof also later.

After using Fourier expansions to establish these results we came across Exercise 6.23(e) in Silverman's dynamical book [Si3, p.383], which gives the resultant in Theorem 1.1, at least up to an undetermined sign. During our proof we had already noted that the resultant up to undetermined powers of $-1, 2, 3$ could be found relatively simply without Fourier. And it turns out that the primes $2, 3$ can be eliminated using the Tate form, thus supplying a similar proof of the Exercise. But this requires certain integrality assertions which are not easy to track down in the literature (see section 8 below).

However it seems that such purely arithmetic techniques do not extend to the discriminant in Theorem 1.2; at best they give in place of the displayed powers of 2 and n only some undetermined product of primes p dividing n. Even more recently we also came across Lemma 1 of Stark [St, p.354] which implies our Theorem 1.2 when n is odd (see also Exercise 1.14(b) of Silverman's second elliptic book [Si2, p.88]). His proof seems rather different using the Kronecker Limit Formula. We think it useful to publish our unified proof for general n, and it is hardly any more work to include our original proof of Theorem 1.1; in fact we deduce Theorem 1.2 from Theorem 1.1 rather quickly. Also in section 6 we comment on how Theorem 1.2 is related to the conjecture made in [BH], p. 31.

Here is how the proofs are arranged. In section 2 we show with comparatively simple arguments that the general shape of Theorems 1 and 2 is not too surprising. In particular we get Theorem 1.1 up to powers of $-1, 2, 3$. Then in section 3 we set the stage for the main calculations, which involve Fourier expansions of elliptic functions and modular forms. These are carried out in section 4 to prove Theorem 1.1. Here some work can be saved thanks to the transcendence of π! We could use similar calculations to prove Theorem 1.2 but to avoid too many complications we first give some auxiliary resultants in section 5. At last in section 6 we prove Theorem 1.2. Then in section 7 we translate our results from $x^3 + ax + b$ in (1) to the more classical Weierstrass form $4x^3 - g_2x - g_3$ and the Legendre form $x(x-1)(x-\lambda)$ investigated in [MZ].

And finally in section 8 we pass to the Tate form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{9}$$

as mentioned, this leads purely arithmetically to Theorem 1.1 up to sign. It also leads to a version of Proposition 6.55 of [Si3, p.362] about good reduction of the Lattès map ϕ_n

of degree n^2 for the Tate curve E: namely if $n \geq 2$ and our ground field has a discrete ultrametric valuation with respect to which (9) is minimal, then ϕ_n has good reduction if and only if E has good reduction. This is proven in the Appendix where the arguments belong to the theory of good reduction of rational maps.

Finally a comment on the characteristic of the ground field seems to be in place. All formulae appearing are identities and Theorem 1.1 and 1.2 are valid for a, b in an arbitrary field simply by specialization. However A_n^W, B_n^W in section 7 are elements in $\mathbb{Z}[\frac{g_2}{4}, \frac{g_3}{4}, x]$ so it seems that it *a priori* doesn't make sense to ask for any properties in characteristic 2. In contrast $A_n^L, B_n^L, B_n^{L*} \in \mathbb{Z}[x, \lambda]$ (see [MZ], section 2) and the formulae in section 7 are valid in any characteristic. The same holds for A_n^T, B_n^T in section 8 but B_n^{T*} can carry a denominator 2 for n even. We would need to replace B_n^{T*} by $2B_n^{T*}$ to make sense of the discriminant in characteristic 2 which is then identically zero.

I thank my research supervisor David Masser for suggesting these problems and his advice on the preparation of this article, and Joseph Silverman and John Tate for valuable correspondence.

2 Algebraic preparations

The following observation gives quite quickly the general shape of the resultant.

Lemma 2.1. *For each natural number $n \geq 2$ there are integers c_n, c_n^* and $k_n \geq 0, k_n^* \geq 0$, depending only on n, such that*

$$\mathrm{res}(A_n, B_n) = c_n \Delta^{k_n}, \quad \mathrm{disc}\ B_n^* = c_n^* \Delta^{k_n^*}.$$

Further there are integers d_n and $l_n \geq 0$, depending only on n, such that

$$\mathrm{res}(C, B_n) = d_n \Delta^{l_n}, \quad (n \text{ odd})$$

$$\mathrm{res}(C, B_n/C) = d_n \Delta^{l_n}. \quad (n \text{ even})$$

Proof. It is known that $A_n(x), B_n(x)$ and even $B_n^*(x)$ lie in $\mathbf{Z}[x, a, b]$ (again see [Si1, Exercise 3.7(a)]). As $C(x)$ is monic this is also true of $B_n(x)/C(x)$ when n is even. Thus it will suffice to prove the lemma when a, b are independent variables over $\mathbf{Q}$. Now the first resultant can be denoted by $R_n(a, b)$ in $\mathbf{Q}[a, b]$. If we specialize a, b to any a_0, b_0 algebraic over $\mathbf{Q}$ then the resultant specializes too, and if it is zero then we must have $\Delta(a_0, b_0) = 0$, where $\Delta(a, b) = -(4a^3 + 27b^2)$. By the Hilbert Nullstellensatz (see for example [L2, p.380]) there is a positive integer $m = m_n$ and a Q_n in $\mathbf{Q}[a, b]$ such that $\Delta(a, b)^m = Q_n(a, b)R_n(a, b)$. Since $\Delta(a, b)$ is irreducible it follows that $R_n(a, b) = c\Delta(a, b)^k$ for some rational $c = c_n$ and some non-negative integer $k = k_n$. Finally since $R_n(a, b)$ is actually in $\mathbf{Z}[a, b]$ and $\Delta(a, b)$ is primitive in $\mathbf{Z}[a, b]$ it follows that c is in $\mathbf{Z}$, and this settles $\operatorname{res}(A_n, B_n)$. The same arguments work for disc B_n^* because we are in zero characteristic.

Similar arguments work for $\operatorname{res}(C, B_n)$ provided we can show that the two polynomials are coprime. But this is clear, because $C = \frac{1}{4}B_2$ vanishes at the x-coordinates of points $P \neq O$ with $2P = O$ and in the same way B_n with $nP = O$; as n is odd both are not simultaneously possible. And likewise for B_n/C with $nP = O$ but $2P \neq O$; this quotient is also in $\mathbf{Z}[x, a, b]$ because C is monic. □

We could go a bit further and verify by homogeneity arguments (assigning x, a, b the usual weights 1,2,3 respectively in (6))) that here $k_n = \kappa_n$ as in Theorem 1.1, but the details are not quite straightforward and the calculations of section 3 will anyway deliver this with relatively little effort. The real purpose of these calculations is to get at c_n. In fact for any prime $p \neq 2$ the equation $y^2 = x^3 - x$ over $\mathbf{F}_p$ defines an elliptic curve with $\Delta = -4$, and so if p divides c_n then $\operatorname{res}(A_n, B_n) = 0$ would contradict the coprimality (known for $p \neq 2, 3$). Thus c_n is composed at most of powers of 2 and 3.

We can even deal with 2 and 3 in a similar way by passing to the Tate curve $y^2 + y = x^3 - x$, and that would yield Theorem 1.1 up to sign; however this step is a bit more delicate and we postpone it to section 8. In fact all we need to know in the sequel is that c_n is a rational number depending only on n. Similar remarks apply for k_n^*, l_n. But for c_n^*, d_n we have to be more careful, because the zeroes of C and B_n can coalesce. However this happens only if the characteristic divides $6n$, so all we could conclude in general is that c_n^*, d_n are composed at most of powers of primes dividing $6n$. It may be found a little surprising that c_n^* is essentially a power of n (and we will see that $d_n = n^6$ when n is even).

Lemma 2.2. *For all natural numbers n we have*

$$4(A_n^3 + aA_nB_n + bB_n^3)B_n = B_{2n}.$$

Proof. For a point $P = (x, y)$ on our elliptic curve we calculate $2nP$ as $2(nP)$. We find

$$\frac{A_{2n}}{B_{2n}} = \frac{A_2(\frac{A_n(x)}{B_n(x)})}{B_2(\frac{A_n(x)}{B_n(x)})} = \frac{A}{B}, \tag{10}$$

where by (2)

$$A = A_n^4 - 2aA_n^2B_n^2 - 8bA_nB_n^3 + a^2B_n^4, \quad B = 4(A_n^3 + aA_nB_n^2 + bB_n^3)B_n.$$

Now in (10) A_{2n}, B_{2n} are coprime, and the degree of A is at most $4n^2 = (2n)^2$ which is already the degree of A_{2n}. It follows that A_{2n}, A are equal up to constants, and by checking the leading coefficients using (3) we deduce equality. So also $B_{2n} = B$, which is what we want. □

For the sequel we record some properties of resultants. For polynomials $A = a\prod_\alpha(x-\alpha)$ of degree $r \geq 1$ and $B = b\prod_\beta(x-\beta)$ of degree $s \geq 1$ we have

$$\mathrm{res}(A,B) = a^s b^r \prod_{\alpha,\beta}(\alpha-\beta) = a^s \prod_\alpha B(\alpha) = (-1)^{rs} b^r \prod_\beta A(\beta) \tag{11}$$

(see for example [L2, p.202]). These make clear the multiplicativity in both A and B separately; and also

$$\mathrm{res}(A,B) = \mathrm{res}(A, B+\tilde{A}) = \mathrm{res}(A+\tilde{B}, B) \tag{12}$$

for any $\tilde{A}, \tilde{B}$ such that $B+\tilde{A}$ also has degree s, $A+\tilde{B}$ also has degree r, as well as $\tilde{A}(\alpha) = 0$ for all α and $\tilde{B}(\beta) = 0$ for all β.

3 Analytic preparations

From now on the coefficients a, b in(1)will be complex numbers. In fact we start with an element τ of the upper half-plane and the corresponding lattice $\Lambda(\tau) = \mathbf{Z}+\mathbf{Z}\tau$ in $\mathbf{C}$. One defines the corresponding Weierstrass function $\wp(z) = \wp(z;\tau)$ and the corresponding map P from $\mathbf{C}/\Lambda(\tau)$ to an elliptic curve $E = E(\tau)$ defined by(1), where $P(z) = (\wp(z), \frac{1}{2}\wp'(z))$ with the usual convention that $P(z)$ is the group origin for every z in the lattice. Here

$$a = a(\tau) = -\frac{1}{4}g_2(\tau), \quad b = b(\tau) = -\frac{1}{4}g_3(\tau) \tag{13}$$

for the standard Eisenstein series g_2, g_3. This is a group isomorphism between $\mathbf{C}/\Lambda(\tau)$ and the complex points $E(\tau)(\mathbf{C})$ ([Si1, p.158]). We also define

$$e_1 = e_1(\tau) = \wp\left(\frac{\tau}{2}\right), \quad e_2 = e_2(\tau) = \wp\left(\frac{1}{2}\right), \quad e_3 = e_3(\tau) = \wp\left(\frac{\tau+1}{2}\right). \tag{14}$$

It is well-known that

$$C(x) = x^3 + ax + b = (x-e_1)(x-e_2)(x-e_3). \tag{15}$$

Now recall the polynomials A_n, B_n corresponding to the curve $E(\tau)$. We write $\mathcal{C}_n$ for the set

$$\mathcal{C}_n = \{(r,s) \in \mathbf{Z}^2; 0 \leq r, s < n, (r,s) \neq (0,0)\}. \tag{16}$$

Lemma 3.1. *For all natural numbers n we have*

$$B_n(x) = \prod_{\mathcal{C}_n}\left(x - \wp\left(\frac{r\tau+s}{n}\right)\right) \tag{17}$$

and

$$\begin{aligned}
A_n(x) - e_1 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ odd}, s \text{ even}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right) \qquad (18) \\
A_n(x) - e_2 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ even}, s \text{ odd}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right) \\
A_n(x) - e_3 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ odd}, s \text{ odd}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right).
\end{aligned}$$

Proof. The zeros of B_n are the x-coordinates $x(P)$ of the points $P \neq O$ on $E(\tau)$ with $nP = O$. These are the $\wp\left(\frac{r\tau+s}{n}\right)$ and we can restrict here to $\mathcal{C}_n$. Now $x(P) = x(Q)$ is equivalent to $P = \pm Q$. So each value turns up exactly twice except if n is even, when the three values (14) each turn up once. By (15) this corresponds precisely to (7) and (8) and we deduce (17).

Again using (15) on Lemma 2.2 we see that

$$4(A_n - e_1 B_n)(A_n - e_2 B_n)(A_n - e_3 B_n)B_n \; = \; B_{2n}.$$

Thus the $(2n)^2$ zeroes $\wp\left(\frac{r\tau+s}{2n}\right)$ of B_{2n} are distributed between those of $A_n - e_1 B_n$, $A_n - e_2 B_n$, $A_n - e_3 B_n$ and B_n. Clearly we get a zero of B_n if and only if r and s are both even. Also $A_n(x) - e_1 B_n(x) = 0$ for $x = x(P)$ is equivalent to $x(nP) = e_1$ and so $\wp\left(\frac{r\tau+s}{2}\right) = \wp\left(\frac{\tau}{2}\right)$ by (14). This in turn is equivalent to r odd and s even. Similarly for the remaining two factors. □

Finally we need some Fourier expansions in $q = e^{2\pi i\tau}$. We have

$$\frac{1}{(2\pi i)^{12}}(g_2^3 - 27g_3^2) = q\prod_{l=1}^{\infty}(1 - q^l)^{24}$$

whose leading term suffices for us, in the form

$$\Delta = -(4a^3 + 27b^2) = \frac{g_2^3 - 27g_3^2}{16} = \frac{(2\pi i)^{12}}{16}q + \cdots . \qquad (19)$$

Then

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) \; = \; \frac{1}{12} + \sum_{m \in \mathbf{Z}} \frac{Qq^m}{(1 - Qq^m)^2} - 2\sum_{k=1}^{\infty} \frac{kq^k}{1 - q^k},$$

where $Q = e^{2\pi i z}$. Putting $z = \frac{r\tau+s}{n}$ for (r, s) in $\mathcal{C}_n$ we deduce not quite as in [L1, p.66]

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau + s}{n};\tau\right) \; = \; \frac{1}{12} + \frac{q^{\frac{r}{n}}\zeta_n^s}{(1 - q^{\frac{r}{n}}\zeta_n^s)^2} + \sum_{k=1}^{\infty}\sum_{m=1}^{\infty} kq^{mk}(q^{\frac{rk}{n}}\zeta_n^{sk} + q^{-\frac{rk}{n}}\zeta_n^{-sk} - 2),$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$. But here the leading term or terms are not so clear.

If $r \neq 0$ then $|q^{\frac{r}{n}}\zeta_n^s| < 1$ so we can expand

$$\frac{q^{\frac{r}{n}}\zeta_n^s}{(1-q^{\frac{r}{n}}\zeta_n^s)^2} = \sum_{k=1}^{\infty} k(q^{\frac{r}{n}}\zeta_n^s)^k$$

and we get a power series in $q^{\frac{1}{n}}$ of the form

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau+s}{n};\tau\right) \;=\; \frac{1}{12} + q^{\frac{r}{n}}\zeta_n^s + q^{\frac{n-r}{n}}\zeta_n^{-s} + \cdots, \tag{20}$$

where the remaining terms involve $q^{\frac{t}{n}}$ with $t > \min\{r, n-r\}$.

If $r = 0$ then we get

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau+s}{n};\tau\right) \;=\; \frac{1}{12} + \frac{\zeta_n^s}{(1-\zeta_n^s)^2} + \cdots, \tag{21}$$

where the remaining terms involve $q^{\frac{t}{n}}$ with $t > 0$.

Finally we need the well-known

$$\prod_{s=1}^{n-1}(1-\zeta_n^s) = n \tag{22}$$

which is proved by evaluating $\prod_{s=1}^{n-1}(X-\zeta_n^s) = \frac{X^n-1}{X-1}$ at $X = 1$. Similarly

$$\prod_{s=1}^{n-1}(1+\zeta_n^s) = 1, \quad (n \text{ odd}) \tag{23}$$

$$\prod_{s=0, s\neq\frac{n}{2}}^{n-1}(1+\zeta_n^s) = n. \quad (n \text{ even}) \tag{24}$$

4 Proof of Theorem 1.1

In view of Lemma 2.1 and (19) it suffices to calculate the leading term of the resultant $\mathrm{res}(A_n, B_n)$ in our Fourier case (13).

In (11) we can use (17) to factorize $B = B_n$ but we have not yet factorized A_n; however by (12) the resultant is also $\mathrm{res}(A_n - eB_n, B_n)$ for any complex number e. It is most convenient here to choose $e = e_1$; then we can use (18).

This leads to the basic formula

$$\mathrm{res}(A_n, B_n) \;=\; (2\pi i)^{2n^2(n^2-1)}(n^2)^{n^2} \prod_{(r,s)\in\mathcal{C}_n} \prod_{\substack{(r',s')\in\mathcal{C}_{2n} \\ r' \text{ odd},\ s' \text{ even}}} f(r', s', r, s), \tag{25}$$

where

$$f(r',s',r,s) \ = \ \frac{1}{(2\pi i)^2}\left(\wp\left(\frac{r'\tau+s'}{2n}\right)-\wp\left(\frac{r\tau+s}{n}\right)\right). \tag{26}$$

Next we examine (26) using (20) and (21). The $\frac{1}{12}$ disappears; and as r' is odd the only way to get a constant term is with $r=0$. This term is then $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$. Taking the product over $s=1,\ldots,n-1$ gives $(-1)^{n-1}\frac{1}{n^2}\zeta_n^{\frac{n(n-1)}{2}}$ using (22), and then the product over the n^2 pairs (r',s') in (25) gives

$$(n^2)^{-n^2}. \tag{27}$$

This cancels with one of the outside factors in (25).

It remains to consider the (26) outside $r=0$, so that (20) holds for both parts. To ease notation we write $s'=2t$, so that $t=0,\ldots,n-1$. We find now

$$f(r',s',r,s) \ = \ q^{\frac{r'}{2n}}\zeta_n^t+q^{\frac{2n-r'}{2n}}\zeta_n^{-t}-q^{\frac{2r}{2n}}\zeta_n^s-q^{\frac{2n-2r}{2n}}\zeta_n^{-s}+\cdots, \tag{28}$$

where all other powers of $q^{\frac{1}{2n}}$ exceed $M=\min\{R',R\}$ for

$$R'=\min\{r',2n-r'\}, \quad R=\min\{2r,2n-2r\}.$$

We claim that this minimum

$$M=\min\{r',2n-r',2r,2n-2r\} \tag{29}$$

is attained at exactly one of the four elements, so that exactly one of the four terms on the right of (28) is the leading term, then involving $q^{\frac{M}{2n}}$.

Note that R is even but R' is odd because r' is odd. In particular $R'\neq R$.

If $R'<R$ then $M=R'$ and so the above claim can be false only if $M=r'=2n-r'$. But then $n=r'$ is odd and $M=n$, and as $R\leq n$ we must have $R<n=M=R'$, a contradiction.

Similarly if $R'>R$ then $M=R$ and the claim can be false only if $M=2r=2n-2r$. But then $n=2r$ is even and $M=n$, and as $R'\leq n$ we must have $R'<n=M=R$, another contradiction.

So the above claim regarding (29) is verified.

It follows from this discussion that if $R'<R$ then $q^{\frac{M}{2n}}\zeta_n^{\pm t}$ is the leading term in (28) while if $R'>R$ then we get $-q^{\frac{M}{2n}}\zeta_n^{\pm s}$. Furthermore the ± do not depend on t,s. These latter both range unrestrictedly from 0 to $n-1$ and so taking the product over t,s kills off the roots of unity. Taking the further product over r,r' we end up with some $(-1)^{\sigma_n}q^{k_n^*}$. Here σ_n is the number of (r,s,r',s') with $R'>R$. If n is even then σ_n is even due to the range of t (or s); while if n is odd, then σ_n is even because we may pair a given r with $n-r\neq r$.

So the product in (25) outside $r = 0$ is simply $q^{k_n^*}$. Combining this with the above result (27) for $r = 0$ we end up with $(2\pi i)^{2n^2(n^2-1)} q^{k_n^*}$ as the leading term of $\mathrm{res}(A_n, B_n)$.

On the other hand by Lemma 2.1 and (19) this leading term is $c_n \left(\frac{(2\pi i)^{12}}{16} q\right)^{k_n}$. It follows that $k_n^* = k_n$ and

$$16^{k_n} (2\pi i)^{2n^2(n^2-1)-12k_n} = c_n.$$

However c_n is rational and π is transcendental and therefore we must have $k_n = \frac{n^2(n^2-1)}{6}$ which is just κ_n from (5). Thus also $c_n = 16^{\kappa_n}$ and this completes the proof of Theorem 1.1.

Of course our appeal to the transcendence of π could be avoided here by directly verifying that our exponent of q, which comes out from the above as the sum of (29) over the range in (25), is κ_n. We leave this to the reader. The verification is slightly easier if one uses $A_n - e_2 B_n$ rather than $A_n - e_1 B_n$ in (18), when (29) becomes the more symmetric $\min\{r', n - r', r, n - r\}$.

5 Some more resultants

We could calculate the discriminant of B_n^* in Theorem 1.2 by deducing its zeros from (17) and using the standard product formula. But this leads to long and involved calculations which we prefer to avoid. Instead we first calculate the other resultants in Lemma 2.1.

Lemma 5.1. *We have*

$$\mathrm{res}(C, B_n) = \Delta^{\frac{n^2-1}{2}}, \quad (n \text{ odd})$$

$$\mathrm{res}(C, B_n/C) = n^6 \Delta^{\frac{n^2-4}{2}}. \quad (n \text{ even})$$

Proof. Of course we go back to Fourier.

We start with n odd. We have

$$\mathrm{res}(C, B_n) \;=\; (2\pi i)^{6(n^2-1)} (n^2)^3 \prod_{(r,s)\in\mathcal{C}_n} \prod_{(r',s')\in\mathcal{C}_2} f(r', s', r, s), \tag{30}$$

where now

$$f(r', s', r, s) \;=\; \frac{1}{(2\pi i)^2} \left(\wp\left(\frac{r'\tau + s'}{2}\right) - \wp\left(\frac{r\tau + s}{n}\right)\right).$$

Now the right-hand sides of (20) and (21) for $n = 2$ read simply $\frac{1}{12} + 2q^{\frac{1}{2}} + \cdots$ for $(r', s') = (1, 0)$, and $\frac{1}{12} - 2q^{\frac{1}{2}} + \cdots$ for $(r', s') = (1, 1)$, and $\frac{1}{12} - \frac{1}{4}$ for $(r', s') = (0, 1)$.

From these with $r' = 0$ we get constant terms $-\frac{1}{4}$ if $r \geq 1$ and

$$-\frac{1}{4} - \frac{\zeta_n^s}{(1 - \zeta_n^s)^2} \;=\; -\frac{(1 + \zeta_n^s)^2}{4(1 - \zeta_n^s)^2}$$

if $r = 0$. Taking the product over (r, s) using (22) and (23) gives $n^{-2}2^{-2(n^2-1)}$.

Another constant term arises from $r' = 1$ and $r = 0$, namely $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$, and taking the product over s', s gives an additional $(n^{-2})^2$; thus so far we have a constant term

$$(n^{-2})^3 2^{-2(n^2-1)} \tag{31}$$

which partly cancels with one of the outside factors in (30).

There remain the terms with $r' = 1$ and $r \geq 1$, which give

$$(-1)^{s'} 2q^{\frac{1}{2}} - q^{\frac{r}{n}}\zeta_n^s - q^{\frac{n-r}{n}}\zeta_n^{-s} + \cdots . \tag{32}$$

As n is odd the leading term here has coefficient $-\zeta_n^{\pm s}$ with ± independent of s. Now $\prod_{s=0}^{n-1} \zeta_n^s = 1$ so this kills the root of unity; and the minus sign is killed by the two values of s'. Thus taking the product yields just 1 for the coefficient, and together with (31) we find $\operatorname{res}(C, B_n) = (2\pi i)^{6(n^2-1)}2^{-2(n^2-1)}q^{l_n^*} + \cdots$. Comparing with Lemma 2.1 and using again transcendence we conclude $l_n^* = l_n = \frac{n^2-1}{2}$ and $d_n = 1$ as required.

Now for n even. This time we have

$$\operatorname{res}(C, B_n/C) \;=\; (2\pi i)^{6(n^2-4)}(n^2)^3 \prod_{(r,s)\in\mathcal{C}_n^*} \prod_{(r',s')\in\mathcal{C}_2} f(r', s', r, s),$$

with f as above, where now $\mathcal{C}_n^*$ is $\mathcal{C}_n$ as in (16) but without $(r, s) = (\frac{n}{2}, 0), (0, \frac{n}{2}), (\frac{n}{2}, \frac{n}{2})$ corresponding to points of order 2.

As above with $r' = 0$ we get constant terms $-\frac{1}{4}$ if $r \geq 1$ and

$$-\frac{1}{4} - \frac{\zeta_n^s}{(1-\zeta_n^s)^2} \;=\; -\frac{(1+\zeta_n^s)^2}{4(1-\zeta_n^s)^2}$$

if $r = 0$. Taking the product over (r, s) using (22) and now (24) gives $2^{-2(n^2-4)}$.

Another constant term arises from $r' = 1$ and $r = 0$, namely $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$, and taking the product over s', s gives an additional $16(n^{-2})^2$; thus so far we have a constant term

$$(n^{-2})^2 2^{-2(n^2-6)}. \tag{33}$$

There remain the terms with $r' = 1$ and $r \geq 1$, which give again (32). Now n is even. If $r \neq \frac{n}{2}$ then the leading term here has coefficient $-\zeta_n^{\pm s}$ with ± independent of s. Now $\prod_{s=0}^{n-1} \zeta_n^s = -1$ so this kills the root of unity; and the two minus signs are killed by the two values of s'. Thus taking the product yields just 1 for the coefficient. But if $r = \frac{n}{2}$ then we get three leading terms with a coefficient $(-1)^{s'}2 - \zeta_n^s - \zeta_n^{-s}$. This is $(1 - \zeta_n^s)(1 - \zeta_n^{-s})$ for $s' = 0$ and $-(1 + \zeta_n^s)(1 + \zeta_n^{-s})$ for $s' = 1$. Taking the product using (22) and (24) yields $(\frac{n}{2})^4$ for the coefficient.

So together with (33) we find $\operatorname{res}(C, B_n/C) = (2\pi i)^{6(n^2-4)}2^{-2(n^2-4)}n^6 q^{l_n^*}$. Comparing with Lemma 2.1 and using again transcendence we conclude $l_n^* = l_n = \frac{n^2-4}{2}$ and $d_n = n^6$ as required. □

6 Proof of Theorem 1.2

We start by expressing $A_n = A_n(x)$ in terms of $B_n = B_n(x)$ and its derivatives.

Lemma 6.1. *For all natural numbers n we have*

$$n^2 A_n B_n \ = \ n^2 x B_n^2 - B_n B_n' C' - 2(B_n B_n'' - B_n'^2)C.$$

Proof. Again it is enough to prove this over the complex numbers; indeed in view of the coefficients n^2 it may not be so useful in positive characteristic (even though it is true there). There we have the Weierstrass σ-function $\sigma(z) = \sigma(z;\tau)$. It is well-known (see for example [F, p.184]) that

$$\frac{\sigma(nz)}{\sigma(z)^{n^2}} = \psi_n(\wp(z), \wp'(z)),$$

where the square of the right-hand side is $B_n(\wp(z))$. So squaring, then logarithmically differentiating to get the Weierstrass ζ-function, then again differentiating to involve $\wp(nz) = \frac{A_n(\wp(z))}{B_n(\wp(z))}$ we end up after a short calculation with the desired result after writing $x = \wp(z)$. □

We will now prove Theorem 1.2 for n odd. Substituting $B_n = B_n^{*2}$ in Lemma 6.1 we obtain $n^2 A_n = A + \tilde{A}$ for $\tilde{A} = 4(B_n^*)'^2 C$ and a polynomial A of degree at most n^2 and divisible by B_n^*. Also $\tilde{A}$ has the same degree n^2 as $n^2 A_n$. So taking the resultant of both sides with B_n and using (12) we get

$$(n^2)^{n^2-1}\mathrm{res}(A_n, B_n) = \mathrm{res}(n^2 A_n, B_n) = \mathrm{res}(\tilde{A}, B_n) = 4^{n^2-1}\mathrm{res}((B_n^*)'^2 C, B_n)$$

because B_n^* vanishes at the zeroes of B_n. Using multiplicativity we see that the last resultant is

$$\mathrm{res}(C, B_n)\mathrm{res}((B_n^*)', B_n^*)^4 \ = \ \mathrm{res}(C, B_n)(n \text{ disc } B_n^*)^4$$

because the leading coefficient of B_n^* is $\pm n$. Finally substituting in our values from Theorem 1.1 and Lemma 5.1 we end up with

$$(\text{disc } B_n^*)^4 = (n^2)^{n^2-3}(16\Delta)^{\frac{(n^2-1)(n^2-3)}{6}}.$$

The required result follows from this by taking fourth roots and using Lemma 2.1. We have calculated the sign ± in the statement of Theorem 1.2 to be $(-1)^{\frac{n-1}{2}}$ for n odd by directly using Fourier expansion. This is in accordance to the conjecture in [BH], p.31.

Now for n even, it is convenient to substitute $B_n = CB_n^{**2}$ in Lemma 6.1, where $B_n^{**} = B_n^*/C$. We obtain $n^2 A_n = A + \tilde{A}$ for

$$\tilde{A} = C'^2 B_n^{**2} + 4C^2(B_n^{**})'^2$$

and a polynomial A of degree at most n^2 and as before divisible by $B_n^* = CB_n^{**}$. Also $\tilde{A}$ has the same degree n^2 as $n^2 A_n$. Taking the resultant of both sides with B_n we get as above

$$(n^2)^{n^2-1}\mathrm{res}(A_n, B_n) = \mathrm{res}(\tilde{A}, B_n) = \mathrm{res}(\tilde{A}, C)\mathrm{res}(\tilde{A}, B_n^{**2}) \qquad (34)$$

because B_n^* still vanishes at the zeroes of B_n.

Now we evaluate each resultant on the right-hand side of (34).

First $C'^2 B_n^{**2}$ also has degree n^2 and so

$$\mathrm{res}(\tilde{A}, C) = \mathrm{res}(C'^2 B_n^{**2}, C) = \mathrm{res}(C', C)^2 \mathrm{res}(B_n^{**2}, C) = n^6 \Delta^{\frac{n^2}{2}} \qquad (35)$$

by Lemma 5.1.

Similarly

$$\mathrm{res}(\tilde{A}, B_n^{**2}) = \mathrm{res}(4C^2(B_n^{**})'^2, B_n^{**2}) = 4^{n^2-4}\mathrm{res}(C, B_n^{**2})^2 (n\mathcal{D})^4 = 4^{n^2-4} n^{16} \Delta^{n^2-4} \mathcal{D}^4 \qquad (36)$$

again by Lemma 5.1, where $\mathcal{D} = \mathrm{disc}\ B_n^{**}$. However we are aiming at

$$\mathrm{disc}\ B_n^* = (-1)^{\frac{n}{2}} n^{-1} \mathrm{res}(CB_n^{**}, C'B_n^{**} + C(B_n^{**})') \qquad (37)$$

which by multiplicativity and (12) is

$$(-1)^{\frac{n}{2}} n^{-1} \mathrm{res}(C, C'B_n^{**})\mathrm{res}(B_n^{**}, C(B_n^{**})') \;=\; \Delta\ \mathrm{res}(C, B_n^{**2})\mathcal{D} \;=\; n^6 \Delta^{\frac{n^2-2}{2}} \mathcal{D} \qquad (38)$$

once again by Lemma 5.1. Now combining this with Theorem 1.1 and (34),(35) and (36) we end up with

$$(\mathrm{disc}\ B_n^*)^4 = n^{2n^2} 2^{-4(n^2-2)} (16\Delta)^{\frac{n^2(n^2+2)}{6}}. \qquad (39)$$

Again taking fourth roots we complete the proof of Theorem 1.2.
We see that from (38),(39) and (37) follows that

$$\mathcal{D} = \pm n^{\frac{n^2}{2}-6} 2^{n^2-2} (16\Delta)^{\frac{(n^2-4)(n^2-6)}{24}}.$$

In fact a more elaborate calculation again using Fourier expansion directly shows that the ± in Theorem 1.2 (as well as for $\mathcal{D}$) is given by $(-1)^{\frac{n-2}{2}}$ (n even). We remark that we checked all results appearing in this article with Mathematica for small n. Further it seems that the conjecture as stated in [BH],p.31 is wrong. In order to compare the conjecture with our result we notice that the authors study the discriminant of f_n with $f_n = B_n^{**}/2$ (n even) and with (11) we have disc $f_n = 2^{-n^2+6}\mathcal{D}$. We see however that the error lies just in the determination of the sign for n even. Possibly this may be explained by the authors accidentally omitting the sign $(-1)^{\frac{d(d-1)}{2}}$, with d the degree of f_n, in their explicit computations. For $f_n = B_n^*$ (n odd) this sign is equal to 1.

7 Weierstrass and Legendre curves

The first of these is defined by the equation $y^2 = 4x^3 - g_2x - g_3$. Now defining $A_n^W = A_n^W(x)$, $B_n^W = B_n^W(x)$ again with respect to the action of multiplication by n on the x-coordinate, so that

$$\wp(nz) = \frac{A_n^W(\wp(z))}{B_n^W(\wp(z))}$$

for the corresponding Weierstrass function, and again normalizing the numerator to be monic, we have no change except for the substitution of the form (13). Thus we find the even simpler form

$$\operatorname{res}(A_n^W, B_n^W) = (g_2^3 - 27g_3^2)^{\frac{n^2(n^2-1)}{6}}.$$

And with

$$B_n^W = B_n^{W*2} \quad (n \text{ odd})$$
$$B_n^W = 4B_n^{W*2}/(4x^3 - g_2x - g_3) \quad (n \text{ even})$$

we find

$$\operatorname{disc} B_n^{W*} = \pm n^{\frac{n^2-3}{2}}(g_2^3 - 27g_3^2)^{\frac{(n^2-1)(n^2-3)}{24}} \quad (n \text{ odd}),$$
$$\operatorname{disc} B_n^{W*} = \pm n^{\frac{n^2}{2}} 2^{-(n^2-2)}(g_2^3 - 27g_3^2)^{\frac{n^2(n^2+2)}{24}} \quad (n \text{ even}).$$

The Legendre curve is defined by the equation $y^2 = x(x-1)(x-\lambda)$. Now defining $A_n^L = A_n^L(x)$, $B_n^L = B_n^L(x)$ with respect to the action of multiplication by n on the x-coordinate, and again normalizing the numerator to be monic, we have

$$A_n^L(x) = A_n(x + \frac{1}{3}(\lambda+1)), \quad B_n^L(x) = B_n(x + \frac{1}{3}(\lambda+1)) \tag{40}$$

and the substitution

$$a = -\frac{1}{3}(\lambda^2 - \lambda + 1), \quad b = -\frac{1}{27}(\lambda-2)(\lambda+1)(2\lambda-1)$$

(see [MZ] for more about these polynomials). We find

$$\operatorname{res}(A_n^L, B_n^L) = (4\lambda(\lambda-1))^{\frac{n^2(n^2-1)}{3}}.$$

And finally with

$$B_n^L = B_n^{L*2} \quad (n \text{ odd})$$
$$B_n^L = B_n^{L*2}/(x(x-1)(x-\lambda)) \quad (n \text{ even})$$

we find

$$\operatorname{disc} B_n^{L*} = \pm n^{\frac{n^2-3}{2}}(4\lambda(\lambda-1))^{\frac{(n^2-1)(n^2-3)}{12}} \quad (n \text{ odd}),$$
$$\operatorname{disc} B_n^{L*} = \pm n^{\frac{n^2}{2}} 2^{-(n^2-2)}(4\lambda(\lambda-1))^{\frac{n^2(n^2+2)}{12}} \quad (n \text{ even}).$$

8 Tate form

We saw that the Tate form is given by (9). This can be reduced to $y^2 = x^3 + ax + b$ as in [Si1, pp.46,48] with $a = -27c_4, b = -54c_6$ both complicated polynomials in $\mathcal{R} = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$; here the old variables are expressed in terms of the new as

$$36x + 3b_2, 216y + 108a_1x + 108a_3 \tag{41}$$

respectively, for some b_2 in $\mathcal{R}$. Thus multiplication by n on x is still given by polynomials $A_n^T = A_n^T(x), B_n^T = B_n^T(x)$, and again normalizing the numerator to become monic we find

$$A_n^T(x) = 36^{-n^2}(A_n(36x + 3b_2) - 3b_2B_n(36x + 3b_2)), \quad B_n^T(x) = 36^{-n^2+1}B_n(36x + 3b_2), \tag{42}$$

the latter also looking like $n^2x^{n^2-1} + \cdots$.

Taking into account the various appearances of 36, and using another property of resultants (see for example Exercise 2.7(a) of [Si3, p.75] with $\beta = \gamma = 0, \delta = 1$) we find the nice form

$$\mathrm{res}(A_n^T, B_n^T) = (\Delta^T)^{\kappa_n}, \tag{43}$$

where $\Delta^T = \frac{1}{1728}(c_4^3 - c_6^2)$, by definition the discriminant of (9), is an even more complicated polynomial still in $\mathcal{R}$ (with 26 terms). Similarly with

$$B_n^T = B_n^{T*2} \quad (n \text{ odd})$$

$$B_n^T = 4B_n^{T*2}/B_2^T \quad (n \text{ even})$$

for $B_2^T = 4x^3 + b_2x^2 + 2b_4x + b_6$ and the standard b_4, b_6 in $\mathcal{R}$ [Si1, p.59] we find

$$\mathrm{disc}\ B_n^{T*} = \pm n^{\frac{n^2-3}{2}}(\Delta^T)^{\frac{(n^2-1)(n^2-3)}{12}} \quad (n \text{ odd}),$$

$$\mathrm{disc}\ B_n^{T*} = \pm n^{\frac{n^2}{2}}2^{-(n^2-2)}(\Delta^T)^{\frac{n^2(n^2+2)}{12}} \quad (n \text{ even}).$$

Now (43) has an application in good reduction, but we must first pause to prove that $A_n^T(x), B_n^T(x)$ lie in $\mathcal{R}[x]$. This seems not to be explicitly in the literature, even though it is known to the experts; indeed from (42) it looks unlikely at first sight. But Tate pointed out that it follows from Proposition 4 of his paper [MT, p.681] with Mazur. Here we supply a slightly more direct proof.

Again by [Si1, p.59] we have $A_2^T = x^4 - b_4x^2 - 2b_6x - b_8$ for the standard b_8 in $\mathcal{R}$. We can then proceed by induction using the relations in [Si1, p.216]. These imply for $n \geq 2$ that

$$x_{n-1} + x_{n+1} = S(x, x_n), \quad x_{n-1}x_{n+1} = P(x, x_n),$$

where $x_m = x(mQ)$ for the generic point $Q = (x, y)$ on $y^2 = x^3 + ax + b$ and

$$S(x, z) = \frac{2(x + z)(a + xz) + 4b}{(x + z)^2 - 4xz}, \quad P(x, z) = \frac{(xz - a)^2 - 4b(x + z)}{(x + z)^2 - 4xz}.$$

We make the change of variables as in (41) to land on (9) and solve for the new x_{n-1}, x_{n+1} to find

$$x_{n-1} + x_{n+1} = S^T(x, x_n), \quad x_{n-1}x_{n+1} = P^T(x, x_n)$$

with

$$\begin{aligned} S^T(x,z) &= \frac{1}{36}S(36x+3b_2, 36z+3b_2) - \frac{1}{6}b_2 \\ P^T(x,z) &= \frac{1}{1296}P(36x+3b_2, 36z+3b_2) - \frac{1}{432}b_2 S(36x+3b_2, 36z+3b_2) + \frac{1}{144}b_2^2. \end{aligned}$$

Now setting

$$x_m = \frac{A_m^T}{B_m^T} = \frac{x^{m^2} + \cdots}{m^2 x^{m^2-1} + \cdots}$$

and comparing the resulting denominator and numerator we obtain

$$B_{n-1}^T B_{n+1}^T = (A_n^T - xB_n^T)^2$$

and similarly (with mild surprise at the disappearance of the denominators) that

$$A_{n-1}^T B_{n+1}^T + A_{n+1}^T B_{n-1}^T, \quad A_{n-1}^T A_{n+1}^T$$

lie in $\mathcal{R}[x, A_n^T, B_n^T]$.

As A_{n-1}^T is monic, the second above shows that if A_{n-1}^T, A_n^T, B_n^T are over $\mathcal{R}$ then so is A_{n+1}^T; and then the first does the same for B_{n+1}^T. This suffices for the induction step.

Incidentally a similar argument shows that for the Legendre model both $A_n^L(x), B_n^L(x)$ lie in $\mathbf{Z}[x, \lambda]$ as mentioned in [MZ]; this is not directly clear from (40) because of the denominator 3.

At this point we interrupt to indicate how to prove Theorem 1.1 up to sign starting only from $\mathrm{res}(A_n, B_n) = c_n\Delta^{\kappa_n}$ as in section 2 with $k_n = \kappa_n$ and c_n composed at most of primes 2,3. As above we deduce only

$$\mathrm{res}(A_n^T, B_n^T) = 16^{-\kappa_n} c_n (\Delta^T)^{\kappa_n}, \tag{44}$$

in place of (43). Now it is a fact that Δ^T is a primitive polynomial; in fact 5 of the 26 terms have coefficient ±1. It follows that $c_n = 16^{\kappa_n} c_n^T$ for c_n^T also in $\mathbf{Z}$. If 2 or 3 divides c_n^T then we look at $y^2 + y = x^3 - x$ over $\mathbf{F}_2$ or $\mathbf{F}_3$ with $\Delta^T = -37$, and then (44) would imply $\mathrm{res}(A_n^T, B_n^T) = 0$ again contradicting coprimality.

In connexion with the Appendix we make a remark about translation by a point $P = (\xi, \eta)$ of order 2. Here

$$B_2^T(\xi) = 4\xi^3 + b_2\xi^2 + 2b_4\xi + b_6 = 0. \tag{45}$$

From [Si1] (p.59) we find that x becomes

$$\frac{A_P^T(x)}{B_P^T(x)} = \xi - \frac{\delta}{x - \xi}$$

with $\delta = a_1\eta - 3\xi^2 - 2a_2\xi - a_4$ (here $2\eta + a_1\xi + a_3 = 0$). But now there seems to be no obvious way to normalize A_P^T, B_P^T; for example ξ is probably not in the integral closure of $\mathcal{R}$. However from (8.4) we see that 4ξ (as well as b_6/ξ if $\xi \neq 0$) is; and if we take

$$A_P^T(x) = 4(\xi x - \xi^2 - \delta), \quad B_P^T(x) = 4(x - \xi)$$

then we also find that even $2(\xi^2 + \delta)$, which is $-4\xi^2 - b_2\xi - b_4$ or $b_4 + \frac{b_6}{\xi}$, is in the closure.

Then $\rho = \operatorname{res}(A_P^T, B_P^T)$ satisfies

$$\rho^3 + c_4\rho^2 + 256\Delta^T = 0. \tag{46}$$

This is not so nice in characteristic 2, and over $\mathbf{F}_2[a_1, a_2, a_3, a_4, a_6]$ we should normalize differently. Then $a_1 \neq 0$ otherwise we are in the supersingular case and P does not exist, and with

$$A_P^T(x) = a_1(\xi x - \xi^2 - \delta), \quad B_P^T(x) = a_1(x - \xi)$$

we get $a_1\xi = a_3$ and $a_1(\xi^2 + \delta)$ the square root of $a_1(a_3^3 + a_1a_2a_3^2 + a_1a_4^2 + a_1^2a_3a_4 + a_1^3a_6)$ in the closure; and simply

$$\rho^2 = \Delta^T. \tag{47}$$

In fact, all is much nicer for Legendre when the three $\frac{A_P^L(x)}{B_P^L(x)}$ are

$$\frac{\lambda}{x}, \quad \frac{x-\lambda}{x-1}, \quad \lambda\frac{x-1}{x-\lambda}.$$

Appendix (with Jung Kyu Canci)

Recall that a rational map $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ is called a *Lattès map* if there exists an elliptic curve E, a morphism $\Phi\colon E \to E$, and a finite separable covering $\pi\colon E \to \mathbb{P}_1$ such that the map ϕ fits in the following diagram

$$\begin{tikzcd}
E \arrow[r, "\Phi"] \arrow[d, "\pi"'] & E \arrow[d, "\pi"] \\
\mathbb{P}_1 \arrow[r, "\phi"] & \mathbb{P}_1.
\end{tikzcd} \tag{48}$$

The study of these type of maps has a long history. See [Mil] for an introduction to Lattès maps.

From an arithmetical point of view they are important because information about preperiodic points of a Lattès map associated to a multiplication by n-map $[n]\colon E \to E$ gives information about the torsion points of E.

From an analytic point of view they are important because they are postcritically finite maps, i.e. the set of critical points is contained in the set of preperiodic points. In other words the full forward orbit of each critical point is finite. See [Si3, Chapter 6] for more information about this. Over $\mathbb{C}$, the study of the forward orbits of the critical points is very important because it gives information about the dynamical behavior of a holomorphic map. Furthermore, the family of Lattès maps represents a very exceptional set of postcritically finite maps (see [BBLPP, Thurston's Rigidity]).

Following Milnor's definitions in [Mil], we can divide Lattès maps into two groups: the flexible Lattès maps and the rigid Lattès maps. A flexible Lattès map is characterized by the property that by varying the elliptic curve E continuously we obtain other Lattès maps which are not conformally conjugate to it. More practically, it is a map as in diagram (48) where the map Φ is of the form $\Phi(P) = [n](P) + Q$ for $n \in \mathbb{Z}$, $Q \in E$ and π is a double covering with $\pi(P) = \pi(-P)$ for all $P \in E$. A Lattès map which is not flexible is called a rigid Lattès map.

Let K be a field equipped with a discrete valuation v and k the respective residue field. Further let $\phi\colon \mathbb{P}_1(K) \to \mathbb{P}_1(K)$ be a morphism defined over K. We say that ϕ has good reduction at v if there exists a morphism $\phi_v\colon \mathbb{P}_1(k) \to \mathbb{P}_1(k)$ that fits in the following commutative diagram:

$$\begin{tikzcd}
\mathbb{P}_1(K) \arrow[r, "\phi"] \arrow[d, "\sim"'] & \mathbb{P}_1(K) \arrow[d, "\sim"] \\
\mathbb{P}_1(k) \arrow[r, "\phi_v"] & \mathbb{P}_1(k)
\end{tikzcd}$$

where $\tilde{}$ denotes the reduction modulo v map.

As an application of Theorem 1 and its generalization to the Tate form in section 8, we prove the following proposition. It can be seen as an improvement of [Si3, Proposition 6.55] since it removes the condition on n (and the proof is valid in all characteristic).

Proposition 1. *Let K be a field equipped with a non-archimedean valuation v and k the corresponding residue field. Let E be an elliptic curve given by an equation in Tate form defined over K. Let $\phi\colon \mathbb{P}_1(K) \to \mathbb{P}_1(K)$ be a flexible Lattès map associated to E where the corresponding π is also defined over K. Suppose that E has good reduction at v. Then there exists an $f \in \mathrm{PGL}_2(K)$ such that $\phi^f = f \circ \phi \circ f^{-1}$ has good reduction at v.*

Proof of Proposition 1. In Silverman's book [Si3, Proposition 6.51] it is proven that the Q appearing in the definition of flexible Lattès maps should be a torsion point of order dividing 2.

Since a priori π is not the projection on the x–coordinate we have to pass to a conjugate $\phi^f = f \circ \phi \circ f^{-1}$ where $f \in \mathrm{PGL}_2(K)$. Indeed, by [Si3, Proposition 6.51], there exists an automorphism $f \in \mathrm{PGL}_2(K)$ such that ϕ^f fits into a diagram of the type (48) where π now is the projection on the x–coordinate. Furthermore since E has good reduction it can be seen by standard arguments that we can conjugate with another $f \in \mathrm{PGL}_2(K)$ such that E is given by a minimal Tate equation with respect to v and π is still the projection on the x–coordinate. If Q is the identity element and n^2 the degree of the Lattès map, then $\phi^f(x) = \frac{A_n^T(x)}{B_n^T(x)}$ (where we are using the notation as in section 8 and the affine notation for the endomorphism ϕ). From the arguments in section 8 follows that the polynomials $A_n^T(x)$ and $B_n^T(x)$ have v–integer coefficients and $A_n^T(x)$ is monic of degree n^2. By [Si3, Theorem 2.15], the map $\phi^f(x)$ has good reduction if and only if the resultant $\mathrm{res}(A_n^T(x), B_n^T(x))$ is a v–unit. But this follows immediately from (8.2).

Suppose now that Q is not the identity element. We define the addition by Q map as $\psi(P) = P + Q$. Since $\psi(-P) = -\psi(P)$ it has a Lattès map ϕ_Q sitting in the following commutative diagram

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}_1 \arrow[r, "\phi_Q"] & \mathbb{P}_1,
\end{tikzcd} \tag{49}$$

where x denotes the projection down to the x coordinate. We want to show that ϕ_Q has good reduction if the chosen model for E in (49) has good reduction. To show the desired property we look at the following bigger diagram.

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "\sim"'] & E \arrow[d, "\sim"] \\
\widetilde{E} \arrow[r, "\widetilde{\psi}"] \arrow[d, "x"'] & \widetilde{E} \arrow[d, "x"] \\
\mathbb{P}_1(k) \arrow[r, "\widetilde{\phi_Q}"] & \mathbb{P}_1(k)
\end{tikzcd}$$

where $\widetilde{\psi}$ denotes the addition by $\widetilde{Q}$ map (by abuse of notation we use $\widetilde{\ }$ also for reduction on the curve). This map has an associated Lattès map $\widetilde{\phi_Q}$. The upper diagram commutes because reduction modulo v is a homomorphism of groups since E has good reduction. The lower small diagram commutes simply because of the definition of Lattès maps. Now reducing modulo v so applying $\widetilde{\ }$ and then projecting down to the x coordinate can be performed in the reverse order if suitably interpreted in the case of the identity element. We draw yet another diagram

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}_1(K) \arrow[r, "\phi_Q"] \arrow[d, "\tilde{}"'] & \mathbb{P}_1(K) \arrow[d, "\tilde{}"] \\
\mathbb{P}_1(k) \arrow[r, "\widetilde{\phi_Q}"] & \mathbb{P}_1(k)
\end{tikzcd}$$

where now the commutativity of the upper small diagram is given by definition and the commutativity of the big one by the previous remark about reversing the order of projecting and reducing. We want to verify the commutativity of the small lower diagram. We start at E in the left upper corner and go down by projecting to the x coordinate. Then we apply ϕ_Q and afterwards $\tilde{}$. By commutativity of the big diagram and the upper small one this is the same as applying the map x reducing modulo v and then applying $\widetilde{\phi_Q}$. Hence we get the equality $\tilde{} \circ \phi_Q \circ x = \widetilde{\phi_Q} \circ \tilde{} \circ x$. Since x is surjective it follows that $\tilde{} \circ \phi_Q = \widetilde{\phi_Q} \circ \tilde{}$ which is the desired commutativity of the lower small diagram. It follows that the Lattès map ϕ_Q has good reduction (a fact also consistent with (46) and (47)). This concludes the proof since good reduction is preserved under composition. □

References

[BBLPP] E. Brezin, R. Byrne, J. Levy, K. Pilgrim, and K. Plummer, *A census of rational maps,* Conformal Geometry and Dynamics 4 (2000), 35-74.

[BH] I. Burhanuddin and M. Huang, *Elliptic curve torsion points and division poynomials.*, Computational aspects of algebraic curves Lecture Notes Ser. Comput. **13** World Sci. Publ., Hackensack, NJ (2005), 13 -37.

[F] R. Fricke, *Elliptische Funktionen II*, Teubner, Leipzig and Berlin 1922.

[H] G.-H. Halphen, *Fonctions elliptiques I*, Gauthier-Villars, Paris 1888.

[L1] S. Lang, *Elliptic functions*, Springer 1987.

[L2] S. Lang, *Algebra*, Addison-Wesley 1993.

[MZ] D. Masser and U. Zannier, *Bicyclotomic polynomials and impossible intersections* to appear in Journal de Théorie des Nombres de Bordeaux, 26pp.

[MT] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), 663-688.

[Mil] J. Milnor. *On Lattès maps.* In Dynamics on the Riemann Sphere, A Bodil Branner Festschrift, Hjorth and Petersen, editors, pages 9-43, Eur. Math. Soc

[Si1] J.H. Silverman, *The arithmetic of elliptic curves*, Springer 1986, GTM **241**.

[Si2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer 1994, GTM **151**.

[Si3] J.H. Silverman, *The arithmetic of dynamical systems*, Springer 2007, GTM **106**.

[St] H.M. Stark, *The Coates-Wiles Theorem revisited*, in *Number theory related to Fermat's last theorem* (Cambridge MA, 1981), Progress Math. **26**, Birkhauser 1982 (pp.349-362).

[TM] J. Tannery and J. Molk, *Fonctions elliptiques III*, Gauthier-Villars, Paris 1893.

Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland (*Harry.Schmidt@unibas.ch*).