London Mathematical Society ISSN 1461–1570

ON POLYNOMIAL INTERPOLATIONS RELATED TO VERHEUL HOMOMORPHISMS

TAKAKAZU SATOH

Abstract

The Verheul homomorphism is a group homomorphism from a finite subgroup of the multiplicative group of a field to an elliptic curve. The hardness of computation of the Verheul homomorphism was shown by Verheul to be closely related to the hardness of the computational Diffie–Hellman problem. Let $p \geqslant 5$ be a prime, and let N be a prime satisfying $\sqrt{12p} < N < 2p/\sqrt{3}$, where $N \neq p$. Let E be an ordinary elliptic curve over $\mathbb{F}_p$, and let $C \subset E$ be a cyclic subgroup of order N. Let H be the group of all Nth roots of unity (contained in the algebraic closure of $\mathbb{F}_p$), and let φ be the Verheul isomorphism from H to C. We consider a polynomial P such that $P(z)$ is the X-coordinate of $\varphi(z)$ for all $z \in H - \{1\}$. We show that, for at least approximately 58% of pairs (E, C), none of the coefficients of the non-constant terms of P vanishes.

1. *Introduction*

Cryptographic protocols and primitives based on number-theoretic algorithms are now being widely deployed. However, many important problems still remain open. So far, most of the results are based on widely believed assumptions, such as the hardness of integer factorizations. On the other hand, some researchers are trying to prove circumstantial evidence for the hardness of these number-theoretic problems without any unproved assumptions. Although their cryptographic implication is not clear, these results have their own interest from a mathematical point of view.

Let us see one of theorems of this type, which concerns elliptic curve discrete logarithms. Let $E/\mathbb{F}_p$ be an elliptic curve, and assume that $p \geqslant 7$. We denote the X-coordinate function on E by ξ. Choose $\beta \in E$ of order $N \in \mathbb{N}$. Lange and Winterhof [**9**, Proposition 2] proved that for a given $S \subset \{1, \ldots, [N/4]\}$, any polynomial $F(X) \in \mathbb{F}_p[X]$ satisfying

$$F(\xi(n\beta)) = n \qquad \text{and} \qquad F(\xi(2n\beta)) = 2n, \qquad \text{for all } n \in S,$$

has degree not less than $\#S/4$. See also work by Lange and Winterhof [**7**, **8**], Kiltz and Winterhof [**5**] and Satoh [**14**] for more results. However, unlike the finite field discrete logarithms case, where we have an explicit formula (see, for example, Wells [**20**], Mullen and White [**12**] and Niederreiter [**13**]), these results on elliptic curve discrete logarithms have obtained only estimates of the degrees of the interpolating polynomials. They can be very sparse, so that they might be evaluated quickly. The purpose of this paper is to study polynomial interpolation related to the Verheul isomorphism, and to show that all non-constant term coefficients are nonzero for some significant proportion of elliptic curves and

Received 29 November 2005, revised 14 March 2006; *published* 27 April 2006.
2000 Mathematics Subject Classification 11Y16, 11T71, 11F11.

https://doi.org/10.1112/S1461157000001224 Published Online by Cambridge University Press

their cyclic subgroups. Of course, proving such a result does not imply the hardness of computing the Verheul homomorphism. However, it is definitely not bad (and is necessary) to confirm that elliptic curve cryptosystems based on the hardness of the Diffie–Hellman problem are not vulnerable against at least straightforward evaluation of sparse polynomial interpolations.

Now we introduce the Verheul isomorphism. In [19], E. Verheul proved the following remarkable result.

> *Let G_1, G_2, H be cyclic groups, all of the same order, this order having known factorization (for example, prime order). Assume the existence of efficient algorithms to compute*: (i) *a group isomorphism from G_1 to G_2*, (ii) *a non-degenerate bilinear pairing from $G_1 \times G_2$ to H, and* (iii) *a group isomorphism from H to G_1. Then the computational Diffie–Hellman problems on H, G_1 and G_2 are efficiently computable.*

He constructed such maps in the case that G_1 and G_2 are cyclic subgroups of the N-torsion points of certain supersingular curves defined over $\mathbb{F}_p$, and that H is a certain subgroup of $\mathbb{F}_{p^3}^{\times}$. Since the Diffie–Hellman problem on $H \subset \mathbb{F}_{p^3}^{\times}$ is believed to be hard, he states that a hypothesis that there exists a feasible algorithm to compute an isomorphism from H to G_1 is unlikely to be correct [19, p. 196]. Following Koblitz and Menezes [6], we call a group homomorphism from a finite subgroup of the multiplicative group of a field to an elliptic curve the *Verheul homomorphism*.

Our main result is summarized as follows (see Theorem 5.3 for the precise statement). Let $p \geqslant 5$ be a prime, and $E/\mathbb{F}_p$ an ordinary elliptic curve. Let N be a prime satisfying $\sqrt{12p} < N < (2/\sqrt{3})p$. Let ζ be a primitive Nth root of unity (in $\mathbb{F}_p^a$, the algebraic closure of $\mathbb{F}_p$), and let $\beta \in E$ be of order N and put $C := \langle \beta \rangle$. Let φ be the Verheul isomorphism such that $\varphi(\zeta) = \beta$. We consider a polynomial $P(z) \in \mathbb{F}_p^a[z]$ satisfying $P(z) = \xi(\varphi(z))$ for all $z \in \langle \zeta \rangle - \{1\}$ and $P(1) = 0$. Such a polynomial exists, due to Lagrange's polynomial interpolation formula. Clearly, $\deg P \leqslant N - 1$. In this paper, we show that $\deg P = N - 1$, and that none of coefficients of P vanishes for about 58% of pairs (E, C).

We sketch our method of proof. For simplicity, assume that $N \equiv 1 \mod 6$ in the introduction. Let $\alpha(E, \beta, \zeta, m) \in \mathbb{F}_p^a$ be the coefficient of z^m in the above $P(z)$; that is,

$$\xi(n\beta) = \sum_{m=0}^{N-1} \alpha(E, \beta, \zeta, m)\zeta^{nm} \qquad \text{for } 1 \leqslant n \leqslant N-1$$

and

$$\sum_{m=0}^{N-1} \alpha(E, \beta, \zeta, m) = 0.$$

Our plan is to relate

$$\prod_{m=1}^{N-1} \alpha(E, \beta, \zeta, m)$$

to a special value of a rational function h on the modular curve of level N. Then the number of zeros of h, counting with multiplicity, is the number of poles of h, which will be proved to be approximately $N^2/6$. This leads to the upper bound of a number of level-N structures for which at least one of $\alpha(E, \beta, \zeta, m)$ is zero.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

In order to construct the modular function h mentioned above, first we compute a polynomial interpolation of the Verheul isomorphism for a level-N structure corresponding to

$$\tau \in \Gamma_0(N) \setminus \mathcal{H} \cong X_0(N)(\mathbb{C}).$$

Here $\mathcal{H} := \{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\}$ is the upper half plane. For an even integer $k \geqslant 4$, let E_k be the Eisenstein series of weight k normalized as $E_k(i\infty) = 1$. For the elliptic curve

$$Y^2 = X^3 - \frac{1}{2^4 3} E_4(\tau) X + \frac{1}{2^5 3^3} E_6(\tau)$$

and the point $B(\tau)$ given by

$$\left(-\frac{1}{4\pi^2} \wp(1/N; \tau)\,,\ \frac{1}{(2\pi i)^3} \wp'(1/N; \tau) \right),$$

consider a polynomial interpolation

$$\xi(nB(\tau)) = \sum_{m=0}^{N-1} A_m(\tau) \exp\left(\frac{2\pi i n m}{N}\right)$$

such that $\sum_{m=0}^{N-1} A_m(\tau) = 0$. We show in Section 4 that the function $A_m(\tau)$ is a modular form of weight two for $\Gamma_1(N)$. However, the product $\prod_{m=1}^{N-1} A_m$ is a modular form of weight $2(N-1)$ for the larger group $\Gamma_0(N)$. Its Fourier coefficients are integral except for finitely many prime ideals. We have its explicit expression by the holomorphic Eisenstein series of weight two. Let Δ be Ramanujan's delta, which is a cusp form of weight 12. Dividing $\prod_{m=1}^{N-1} A_m$ by $\Delta^{(N-1)/6}$, we obtain a modular function for $\Gamma_0(N)$, which is regarded as a rational function h on $X_0(N)(\mathbb{C})$. Since Δ has only one simple zero at $\infty \in X_0(1)$, this function h is holomorphic except for cusps 0 and ∞, and it has $(N+1)(N-1)/6$ zeros over $X_0(N)(\mathbb{C})$. (Recall that $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)] = N+1$ since N is a prime.) By the Deuring lifting theory, for a given level-N structure (E, C), we can choose $\tau \in \mathcal{H}$ and a prime ideal $\mathfrak{p}$ lying above p, for which $\overline{h(\tau)} = \prod_{m=1}^{N-1} \alpha(E, \beta, \zeta, m)$. On the other hand, reduction does not increase the orders of poles under certain conditions. This implies that $\prod_{m=1}^{N-1} \alpha(E, \beta, \zeta, m)$ can be zero in at most $(N^2-1)/6$ places.

However, the affine curve $\Phi_N(X, Y) = 0$ gives a singular model of $X_0(N)$. At a singular point, we cannot talk about the order of the zeros. What is worse, in the case that $C = E(\mathbb{F}_p)$, the level-N structure (E, C) *always* corresponds to a singular point of the curve $\Phi_N(X, Y) = 0$. To overcome this problem, we use the classical language of valuations. Let $\mathcal{K}$ be a function field of one variable with an exact constant field k, and let M be its smooth model. Recall that the set of equivalence classes of valuations on $\mathcal{K}$ which is trivial on k is in one-to-one correspondence to the set of $\mathrm{Gal}(k^a/k)$ orbits of the points on M. For an imaginary quadratic $\tau \in \mathcal{H}$, we define a valuation $\overline{\mathrm{ord}_\tau}$ on the function field of the curve defined by the coefficient-wise reduction $\overline{\Phi_N}(X, Y) = 0$. Thus we can talk about the order of a zero for a rational function at the point corresponding to a reduction of τ without handling a smooth model of $X_0(N)$, even if τ corresponds a singular point.

The paper is organized as follows. Section 2 summarizes the basic properties of Eisenstein series of weight two, which are more or less immediate consequences of work by Hecke [**2**]. In Section 3, we construct valuations on the reduced modular curve. As a byproduct, we obtain Corollary 3.14 on singular values on a certain modular function for $\Gamma_0(N)$ which is not covered by Schertz [**15**]. In Section 4, we compute $A_m(\tau)$ explicitly, and prove that we can apply the results of Section 3 to $\Delta^{-(N-1)/6} \prod_{m=1}^{N-1} A_m$. Finally, we prove our main result, namely Theorem 5.3, in Section 5.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

NOTATION. We denote the X-coordinate function on E by ξ. We put

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \mid c \equiv 0 \bmod N \right\}$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \bmod N \right\}.$$

We denote the trivial Dirichlet character modulo N by χ_0. Let χ be a Dirichlet character modulo N. For

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

we write $\chi(d)$ as $\chi(M)$. With this convention, it holds that $\chi(MM') = \chi(M)\chi(M')$ for $M, M' \in \Gamma_0(N)$. A bar stands for reduction with respect to a prime ideal which should be clear by context, whereas the complex conjugate is denoted by $\check{}$. (Also, the symbol π is always $3.14\ldots$.) We let $\mathbf{e}(z) := \exp(2\pi i z)$. For an even $k \geqslant 4$, we denote by E_k the Eisenstein series of weight k normalized as $E_k(\tau) = 1 + O(q)$. As usual, $\Phi_N(X, Y)$ is the Nth modular polynomial.

2. *The Eisenstein series for congruence subgroups*

This section summarizes some properties on Eisenstein series of weight two. They are more or less immediate consequences of [2]. Let N be a fixed prime. The group $\mathrm{GL}(2, \mathbb{R})$ acts on the upper half plane $\mathcal{H}$ by

$$M\langle\tau\rangle = \frac{a\tau + b}{c\tau + d},$$

where $\tau \in \mathcal{H}$ and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{R})$. For an integer k, a function f on $\mathcal{H}$ and $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{R})$, we define $f|_k M$ by

$$(f|_k M)(\tau) := (ad - bc)^{k/2}(c\tau + d)^{-k} f(M\langle\tau\rangle).$$

We denote the $\mathbb{C}$-vector space of holomorphic modular forms of weight k for $\Gamma_0(N)$ and the Dirichlet character χ modulo N by $M_k(\Gamma_0(N), \chi)$ and, likewise, the $\mathbb{C}$-vector space of holomorphic modular forms of weight k for $\Gamma_1(N)$ by $M_k(\Gamma_1(N)))$. Define

$$\tilde{G}_{u,v}(\tau, s) = \sum_{\substack{(\alpha,\beta)\neq(0,0) \\ (\alpha,\beta)\equiv(u,v) \bmod N}} \frac{1}{(\alpha\tau + \beta)^2 |\alpha\tau + \beta|^s}.$$

This is absolutely convergent for $\mathrm{Re}(s) > 0$, and in fact it has a meromorphic continuation to the whole s-plane. For $(u, v) \in \mathbb{Z}^2$, we define the Eisenstein series of weight two by

$$G_{(u,v)}(\tau) = \tilde{G}_{u,v}(\tau, 0).$$

Since we let $s = 0$ after analytic continuation,

$$G_{(u,v)}|_2 M = G_{(u,v)M} \qquad \text{for } M \in \mathrm{SL}(2, \mathbb{Z}). \tag{2.1}$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Let $\delta(x) := 1$ for $x \in \mathbb{Z}$ and $\delta(x) := 0$ otherwise. Hecke [2, (13)] proved that

$$\begin{aligned} G_{(u,v)}(\tau) = &-\frac{\pi}{N^2 \operatorname{Im}\tau} + \delta\left(\frac{u}{N}\right) \sum_{\substack{n \neq 0 \\ n \equiv v \bmod N}} \frac{1}{n^2} \\ &- \frac{4\pi^2}{N^2} \sum_{n=1}^{\infty} \left(\sum_{\substack{dd' = n \\ d \equiv u \bmod N}} |d'| \mathbf{e}\left(\frac{vd'}{N}\right) \right) \mathbf{e}\left(\frac{n\tau}{N}\right). \end{aligned} \tag{2.2}$$

Put $\sigma_1(n) := \sum_{d \mid n} d$. We also note that

$$\mathbf{E}_2(\tau) := -\frac{3}{\pi \operatorname{Im}\tau} + 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) \mathbf{e}(n\tau)$$

is a (non-holomorphic) Eisenstein series with respect to $\mathrm{SL}(2, \mathbb{Z})$ of weight two. It is easy to verify that

$$G_{(0,0)}(\tau) = -\frac{\pi}{N^2 y} + \frac{\pi^2}{3N^2} - \frac{8\pi^2}{N^2} \sum_{n=1}^{\infty} \left(\sum_{0 < d \mid n} d \right) \mathbf{e}(n\tau) = \frac{\pi^2}{3N^2} \mathbf{E}_2(\tau). \tag{2.3}$$

For a non-trivial Dirichlet character χ modulo N, we put

$$\begin{aligned} E_\chi &:= -\frac{N^2}{4\pi^2} \cdot \frac{1}{2} \sum_{t=1}^{N-1} \chi^{-1}(t) G_{(0,t)}; \\ E^\chi &:= -\frac{N^2}{4\pi^2} \cdot \frac{1}{2} \sum_{t=1}^{N-1} \chi^{-1}(t) G_{(t,0)}. \end{aligned} \tag{2.4}$$

The transformation formula (2.1) implies that

$$E_\chi |_2 M = \chi(M) E_\chi \qquad \text{for } M \in \Gamma_0(N) \tag{2.5}$$

and

$$E^\chi = E_\chi |_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2.6}$$

For an odd character χ (that is, $\chi(-1) = -1$), it is trivial to see that $E_\chi = E^\chi = 0$. (Note that $G_{(u,v)} = G_{-(u,v)}$.) When χ is a non-trivial even character, we have

$$\begin{aligned} E^\chi(\tau) &= \frac{1}{2} \sum_{t=1}^{N-1} \chi^{-1}(t) \left(\frac{1}{4\pi y} + \sum_{n=1}^{\infty} \left(\sum_{\substack{dd' = n \\ d \equiv t \bmod N}} |d'| \right) \mathbf{e}\left(\frac{n\tau}{N}\right) \right) \\ &= \sum_{n=1}^{\infty} \left(\sum_{0 < d \mid n} \frac{n}{d} \chi^{-1}(d) \right) \mathbf{e}\left(\frac{n\tau}{N}\right). \end{aligned} \tag{2.7}$$

Hence E^χ is holomorphic on $\mathcal{H}$. On the contrary, the function defined by

$$\mathcal{E}^{\chi_0} := -\frac{N^2}{4\pi^2} \cdot \frac{1}{2} \sum_{t=1}^{N-1} G_{(t,0)} \tag{2.8}$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

is not holomorphic because

$$\mathcal{E}^{\chi_0}(\tau) = \frac{N-1}{8\pi y} + \sum_{n=1}^{\infty}\Big(\sum_{N\nmid d\,|\,n}\frac{n}{d}\Big)\mathbf{e}\Big(\frac{n\tau}{N}\Big). \tag{2.9}$$

However,

$$E^{\chi_0}(\tau) := \mathcal{E}^{\chi_0}(\tau) + \frac{N-1}{24}\mathbf{E}_2(\tau)$$

is holomorphic on $\mathcal{H}$. Noting that

$$\sum_{d\,|\,n} d - \sum_{d\,|\,\frac{n}{N}} d = \sum_{d\,|\,n}\frac{n}{d} - \sum_{N\,|\,\frac{n}{d}} d = \sum_{d\,|\,n}\frac{n}{d} - \sum_{N\,|\,d'\,|\,n}\frac{n}{d'} = \sum_{N\nmid d\,|\,n}\frac{n}{d}$$

we see that

$$-\frac{1}{24}\Big(\mathbf{E}_2\Big(\frac{\tau}{N}\Big) - \mathbf{E}_2(\tau)\Big) = \mathcal{E}^{\chi_0}(\tau) \tag{2.10}$$

and thus

$$\begin{aligned} E^{\chi_0} &= \frac{1}{24}\Big(N\mathbf{E}_2(\tau) - \mathbf{E}_2\Big(\frac{\tau}{N}\Big)\Big) \\ &= \frac{N-1}{24} + \sum_{n=1}^{\infty}\Big(\sum_{d\,|\,n} d\chi_0(d)\Big)\mathbf{e}\Big(\frac{n\tau}{N}\Big). \end{aligned} \tag{2.11}$$

Let $\mathfrak{g}(\chi) := \sum_{t=1}^{N-1}\chi(t)\mathbf{e}(t/N)$ be the Gauss sum. Recall that

$$\sum_{t=1}^{N-1}\chi(t)\mathbf{e}\Big(\frac{td}{N}\Big) = \chi^{-1}(d)\mathfrak{g}(\chi)$$

for any *non-trivial* character χ, regardless of whether $\gcd(d, N) = 1$ or not. Hence

$$E_\chi(\tau) = -\frac{N^2}{4\pi^2}L(2,\chi^{-1}) + \mathfrak{g}(\chi^{-1})\sum_{n=1}^{\infty}\Big(\sum_{0<d\,|\,n} d\chi(d)\Big)\mathbf{e}(n\tau) \tag{2.12}$$

which shows that E_χ is holomorphic on $\mathcal{H}$. Therefore, $E_\chi \in M_2(\Gamma_0(N), \chi)$ by (2.5). As to the trivial character, define E_{χ_0} by

$$E_{\chi_0} := \mathcal{E}_{\chi_0} + \frac{N-1}{24}\mathbf{E}_2 \tag{2.13}$$

where

$$\mathcal{E}_{\chi_0} := \mathcal{E}^{\chi_0}|_2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = -\frac{N^2}{4\pi^2}\cdot\frac{1}{2}\sum_{t=1}^{N-1}G_{(0,t)}. \tag{2.14}$$

Then $\mathcal{E}_{\chi_0}|_2 M = \mathcal{E}_{\chi_0}$ for all $M \in \Gamma_0(N)$. It is easy to see that $E_{\chi_0}|_2 M = E_{\chi_0}$ for all $M \in \Gamma_0(N)$. Since

$$E_{\chi_0} = E^{\chi_0}|_2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

the function E_{χ_0} is holomorphic on $\mathcal{H}$. Thus, $E_{\chi_0} \in M_2(\Gamma_0(N), \chi_0)$. The Fourier expansion of E_{χ_0} is

$$E_{\chi_0}(\tau) = \frac{1}{24}\big(N\mathbf{E}_2(\tau) - N^2\mathbf{E}_2(N\tau)\big) = \frac{N - N^2}{24} - N\sum_{n=1}^{\infty}\Big(\sum_{d\,|\,n} d\,\chi_0(d)\Big)\mathbf{e}(n\tau). \tag{2.15}$$

3. *Reductions of modular functions*

We show some results on the reduction of modular functions for $\Gamma_0(N)$, which are crucial in the later sections. Let h be a modular function for $\Gamma_0(N)$ whose Fourier coefficients satisfy certain arithmeticity conditions. For a prime ideal $\mathfrak{p}$ of an algebraic number field, we define the reduction $\overline{h}$ of h modulo $\mathfrak{p}$, which is a rational function on the singular model of $X_0(N)$ defined by the Nth modular polynomial Φ_N. We also define a valuation $\overline{\mathrm{ord}}_{\tau_0}$ for some $\tau_0 \in \mathcal{H}$. This valuation may be regarded as a point on a smooth model of the reduction of $X_0(N)$. Our object is to show that the order of a zero (or a pole) at a cusp is preserved under the reduction, and that $h(\tau_0) \not\equiv 0 \bmod \mathfrak{p}$ if $\overline{\mathrm{ord}}_{\tau_0}\overline{h} = 0$. We note that the case where $(j(\tau_0), j(N\tau_0))$ is a singular point is important for cryptographic applications. These results would follow as instances of the general theory. Perhaps the most sophisticated language for such purposes employs the p-adic modular forms introduced by Katz [4]. However, we use rather more classical language, which gives a more straightforward description. A major difficulty is that the modular polynomial gives a singular model of fields of modular functions. So we work with function fields of modular curves and their spots, rather than (smooth or non-smooth models of) modular curves.

We recall some basic facts on extensions of a valuation. Let (k, v) be a (not necessarily complete) valuation field, and let $K := k(\alpha)$ be a simple algebraic extension of k. We denote the minimum polynomial of α by $f(X) \in k[X]$. Let $f(X) = f_1(X)\cdots f_n(X)$ be the irreducible factorization of $f(X)$ over k_v, the completion of k at v. Then v has n extensions $v_1, \ldots, v_n$. Explicitly, given $u(X) \in k[X]$, we have

$$v_i(u(\alpha)) = v\left(N_{k_v(\alpha_i)/k_v}(u(\alpha_i))\right)^{1/\deg f_i} \tag{3.1}$$

for $i = 1, \ldots, n$, where α_i is a root of $f_i(X) = 0$. The product of the ramification index of v_i and the degree of the residue field extension is $\deg f_i$. (See, for example, [18, Chapters 4 and 6] for more details.)

Let N be a prime, and let $\Phi_N(X, Y)$ be the Nth modular polynomial. It is known that

$$\Phi_N(X, Y) = X^{N+1} + Y^{N+1} + \sum_{m,n=0}^{N} a_{mn}X^mY^n$$

with suitable $a_{mn} \in \mathbb{Z}$ (depending on N). Moreover, $a_{NN} = -1$ and $a_{mn} = a_{nm}$; that is, $\Phi_N(X, Y) = \Phi_N(Y, X)$. Let $\mathcal{A}(N)$ be the field of modular functions with respect to $\Gamma_0(N)$. Then

$$\mathcal{A}(N) = \mathbb{C}(j, j\circ[N]) \cong \mathbb{C}(X)[Y]/\langle\Phi_N(X, Y)\rangle,$$

where the isomorphism is given by $j \to X$ and $j\circ[N] \to$ (the class of) Y. The subfield $\mathcal{A}(1)$ of $\mathcal{A}(N)$ corresponds to $\mathbb{C}(X)$. Let $x := X^{-1}$ and $y := Y^{-1}$. The spot corresponding to the cusp ∞ of $\mathcal{A}(1)$ is the x-adic valuation.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

In terms of x and y, the above isomorphism is

$$\mathcal{A}(N) = \mathbb{C}(j, j \circ [N]) \cong \mathbb{C}(x)[y]/\langle \varphi_N(x, y) \rangle$$

where

$$\varphi_N(x, y) := x^{N+1} y^{N+1} \Phi_N(x^{-1}, y^{-1}) \left(= x^{N+1} + y^{N+1} + \sum_{m,n=0}^{N} a_{mn} x^{N+1-m} y^{N+1-n} \right).$$

Let F be a field satisfying $\mathrm{char}(F) \nmid N$. By Igusa [3], Φ_N is irreducible over F. So φ_N is also irreducible over F. For simplicity, we denote the field $F(X)[Y]/\langle \Phi_N(X, Y) \rangle$ by $\mathcal{B}(N)_F$, the class of Y in $\mathcal{B}(N)_F$ by $\tilde{Y}$, and the class of Y^{-1} in $\mathcal{B}(N)_F$ by $\tilde{y}$. We understand that $\mathcal{B}(1)_F = F(X)$. Since $j(\tau) - 1/q \in \mathbb{Z}[[q]]$, there exists a unique $\omega(T) \in 1 + T\mathbb{Z}[[T]]$ satisfying $(j \circ [N])^{-1} = (1/j)^N \omega(1/j)$.

LEMMA 3.1. *There exist two additive valuations on $\mathcal{B}(N)_F$, denoted by* ord_0 *and* ord_∞ *respectively, which are extensions of the x-adic order* ord_x. *They are given by*

$$\mathrm{ord}_\infty u(x, \tilde{y}) = \mathrm{ord}_T u(T, T^N \omega(T)) \tag{3.2}$$

and

$$\mathrm{ord}_0 u(x, \tilde{y}) = \mathrm{ord}_T u(T^N \omega(T), T) \tag{3.3}$$

for $u(x, y) \in F(x, y)$, where T is an indeterminate and ord_T *is the T-adic order on the field of the formal Laurent series $F((T))$. The ramification indices of* ord_0 *and* ord_∞ *are N and* 1, *respectively.*

Proof. Let $A_i(x) \in \mathbb{Z}[x]$ be the coefficient of y^i in $\varphi_N(x, y)$. So we have

$$A_{N+1}(x) = 1 + \sum_{m=0}^{N} a_{m0} x^{N+1-m},$$

$$A_0(x) = x^{N+1} \qquad \text{and} \qquad x \mid A_i(x) \quad \text{for } 0 \leqslant i \leqslant N.$$

Let $\varphi_N^{(\infty)}(x, y) := y - x^N \omega(x)$. Since $\varphi_N(j^{-1}, (j \circ [N])^{-1}) = 0$, we see that $\varphi_N^{(\infty)} \mid \varphi_N$. Put

$$\varphi_N^{(0)} := \varphi_N / \varphi_N^{(\infty)},$$

and write

$$\varphi_N^{(0)} = \sum_{i=0}^{N} \alpha_i(x) y^i.$$

Then $\alpha_N(x) = A_{N+1}(x)$ and $\alpha_0(x) = -x\omega(x)^{-1}$ (note that $\omega(T) \in \mathbb{Z}[[T]]^\times$). Let ν be the least positive integer satisfying $x \nmid \alpha_\nu(x)$ (in $F[[x]]$). Suppose that $\nu < N$. Then $A_{\nu+1}(x) = \alpha_\nu(x) - x^N \omega(x) \alpha_{\nu+1}(x)$ is not divisible by x, which is a contradiction. Hence $\nu = N$; that is, $x \mid \alpha_i(x)$ for $0 \leqslant i \leqslant N - 1$.

Since $\alpha_N(x) = A_{N+1}(x) \equiv 1 \bmod x$, the polynomial $\varphi_N^{(0)}(x, y)$ is irreducible over $F((x))$ by Eisenstein's irreducibility criterion. Hence there are two valuations of $\mathcal{B}(N)_F$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

lying above v_x. We denote the (multiplicative) valuations corresponding to $\varphi_N^{(\infty)}$ and $\varphi_N^{(0)}$ by v_∞ and v_0, respectively. Now (3.2) is an immediate consequence of (3.1). Clearly, v_∞ is unramified. Let e_0 be the ramification index of v_0. We see that

$$v_0(\tilde{y}) = v_x\big(x\omega(x)^{-1}/A_{N+1}(x)\big)^{1/N} = v_x(x)^{1/N}$$

by (3.1). Hence $e_0 \geqslant N$. On the other hand, $\deg_y \varphi_N^{(0)}(x, y) = N$, which implies that $e_0 \leqslant N$. Thus $e_0 = N$ and $v_0(\tilde{y})$ generates the value group of v_0. So, v_0 is a $\tilde{y}$-adic valuation. Noting that $\varphi_N(x, y) = \varphi_N(y, x)$, we see that $x = \tilde{y}^N\omega(\tilde{y})$ when $\tilde{y}$ is a root of $\varphi_N^{(0)}(x, \tilde{y}) = 0$. This proves (3.3). □

Remark 3.2. In the case of $F = \mathbb{C}$, the additive valuation ord_0 is the order of the zero at the cusp 0 of the compact Riemann surface $X_0(N)(\mathbb{C})$, and ord_∞ is that at the cusp ∞.

Definition 3.3. For a subring R of $\mathbb{C}$, we denote by $\mathcal{A}(N)_R$ the ring of automorphic functions h for $\Gamma_0(N)$ that is holomorphic on $\mathcal{H}$, and that satisfies $h(\tau) \in R((q))$ and $h(-1/\tau) \in R((q^{1/N}))$.

Lemma 3.4. *Let R be a subring of $\mathbb{C}$, and let $h \in \mathcal{A}(N)_R$. Then there exists a polynomial $u(X, Y) \in R[X, Y]$ satisfying*

$$(\partial_Y \Phi_N)(j, j\circ[N])h = u(j, j\circ[N]). \tag{3.4}$$

Here, ∂_Y stands for partial differentiation with respect to Y.

Proof. By a similar proof to that used by Cox [1, Proposition 12.7(ii)], there exists $u(X, Y) \in \mathbb{C}[X, Y]$ satisfying (3.4). Without loss of generality, we can assume that $\deg_Y u \leqslant N$. Put $t := \deg_X u$. Let $u(X, Y) = \sum_{m=0}^{t}\sum_{n=0}^{N} b_{mn}X^mY^n$. Since $h \in \mathcal{A}(N)_R$, we see that

$$\sum_{m=0}^{t}\sum_{n=0}^{N} b_{mn}j(\tau)^m j\,(N\tau)^n \in R((q)) \tag{3.5}$$

and

$$\sum_{m=0}^{t}\sum_{n=0}^{N} b_{mn}j(\tau)^m j\left(\frac{\tau}{N}\right)^n \in R((q^{1/N})) \tag{3.6}$$

by (3.4) and the automorphic property of j. By induction on t, we prove that $b_{mn} \in R$ for all $0 \leqslant m \leqslant t$ and $0 \leqslant n \leqslant N$. We see that $b_{t,N}, \ldots, b_{t,1} \in R$, from (3.6). Then $b_{t,0} + b_{t-1,N} \in R$ by (3.6) and

$$b_{t,0}j(\tau)^t + \sum_{m=0}^{t-1}\sum_{n=0}^{N} b_{mn}j(\tau)^m j(N\tau)^n \in R((q))$$

by (3.5). Therefore $b_{t-1,N} \in R$, and thus $b_{t,0} \in R$. Then we obtain

$$\sum_{m=0}^{t-1}\sum_{n=0}^{N} b_{mn}j(\tau)^m j\,(N\tau)^n \in R((q))$$

and

$$\sum_{m=0}^{t-1}\sum_{n=0}^{N} b_{mn}j(\tau)^m j\left(\frac{\tau}{N}\right)^n \in R((q^{1/N})).$$

Repeating this process, we complete the proof. □

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

In what follows, we let K be an algebraic number field, and let $\mathfrak{p}$ be its prime ideal not dividing N. We denote by R the ring of $\mathfrak{p}$-integral elements of K, and put $k := R/\mathfrak{p}R$. We need the fact that Φ_N is separable. This has been proved by Igusa [3], but we can prove it by the following elementary argument. The irreducible polynomial $\varphi_N^{(0)}$ is separable as a polynomial of y since $\mathrm{char}(k) \nmid \deg \varphi_N^{(0)}$. Thus $\varphi_N^{(0)}$ has no repeated factor over $k((x))$. Clearly, $\varphi_N^{(0)}$ and $\varphi_N^{(\infty)}$ are coprime. Thus φ_N is separable, and so is Φ_N. In either event, $\overline{\partial_Y \Phi_N}(X, \tilde{Y})$ is a non-zero element of $\mathcal{B}(N)_k$.

For notational consistency, we write ord_∞ and ord_0 as $\overline{\mathrm{ord}}_\infty$ and $\overline{\mathrm{ord}}_0$, respectively in the case of $\mathrm{char}(F) > 0$.

DEFINITION 3.5. Let $h \in \mathcal{A}(N)_R$. The reduction $\overline{h}$ of h modulo $\mathfrak{p}$ is defined to be

$$\frac{\overline{u}(X, \tilde{Y})}{\overline{\partial_Y \Phi_N}(X, \tilde{Y})} \in \mathcal{B}(N)_k$$

where u is as in (3.4) and a bar on a polynomial stands for its coefficient-wise reduction. (Note that for $g(X, Y) \in R[X, Y]$, we have $g(j, j \circ [N]) = \overline{g}(X, \tilde{Y})$.)

THEOREM 3.6. *Let w be an additive valuation on $\mathcal{B}(1)_k$ $(= k(X))$ which does not belong to the infinite spot. Let $h \in \mathcal{A}(N)_R$. Then*

$$\sum_{v \mid w} v(\overline{h}) \geqslant 0,$$

where $\sum_{v \mid w}$ stands for summation over additive valuations v of $\mathcal{B}(N)_k$ whose restrictions to $\mathcal{B}(1)_k$ are w.

Proof. By Igusa [3], the extension $\mathcal{B}(N)_k/\mathcal{B}(1)_k$ is the Galois extension. On the other hand, recall that the Galois group $G := \mathrm{Gal}(\mathcal{B}(N)_k/\mathcal{B}(1)_k)$ acts transitively on the set of valuations whose restrictions to $\mathcal{B}(1)_k$ are w. Take any such a valuation v_0. Let n be the order of the stabilizer group of v_0. This is independent of the choice of v_0. Then

$$\begin{aligned}
\sum_{v \mid w} v(\overline{h}) &= n^{-1} \sum_{\sigma \in G} v(\sigma(\overline{h})) \\
&= n^{-1} v\left(\prod_{\sigma \in G} \sigma(\overline{h}) \right) \\
&= n^{-1} w\left(N_{\mathcal{B}(N)_k/\mathcal{B}(1)_k}(\overline{h}) \right) \\
&= n^{-1} w\left(\overline{N_{\mathcal{A}(N)_K/\mathcal{A}(1)_K}(h)} \right).
\end{aligned}$$

(Note that $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ and $\Phi_N(X, Y)$ is monic in Y.) Since h is holomorphic on $\mathcal{H}$, the function $N_{\mathcal{A}(N)_K/\mathcal{A}(1)_K}(h)$ is a polynomial in the j function. Hence $\overline{N_{\mathcal{A}(N)_K/\mathcal{A}(1)_K}(h)}$ is a polynomial in X. Our assertion follows from the assumption that w does not belong to the infinite spot. □

PROPOSITION 3.7. *Let $h \in \mathcal{A}(N)_R$. Let*

$$h(\tau) = \sum_{n \in \mathbb{Z}} c_n q^n \qquad \text{and} \qquad h(-1/\tau) = \sum_{n \in \mathbb{Z}} c'_n q^{n/N}$$

be the q-expansions of h at the cusps. Then

$$\overline{\mathrm{ord}}_\infty \overline{h} = \min\{n : c_n \not\equiv 0 \bmod \mathfrak{p}\}; \tag{3.7}$$

$$\overline{\mathrm{ord}}_0 \overline{h} = \min\{n : c'_n \not\equiv 0 \bmod \mathfrak{p}\}. \tag{3.8}$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Proof. Let $u \in R[X, Y]$ be as in (3.4). Note that

$$\partial_Y \Phi_N(X, Y) = (N+1)Y^N - NX^N Y^{N-1} + \sum_{m=0}^{N-1} N a_{mN} X^m Y^{N-1} + \sum_{m=0}^{N} \sum_{n=0}^{N-2} (n+1) a_{m,n+1} X^m Y^n.$$

There exists $\lambda_\infty(T) \in 1 + T\mathbb{Z}[[T]]$ such that

$$\partial_Y \Phi_N(T^{-1}, T^{-N}\omega(T)^{-1}) = T^{-N^2}\lambda_\infty(T).$$

Indeed, the lowest-degree term in $\partial_Y \Phi_N(T^{-1}, T^{-N}\omega(T)^{-1})$ comes from $(N+1)Y^N$ and $NX^N Y^{N-1}$. Since $\omega(0) = 1$, the coefficient of T^{-N^2} is $(N+1) - N = 1$. In particular,

$$\overline{\mathrm{ord}}_\infty \overline{\partial_Y \Phi_N}(X, \tilde{Y}) = -N^2.$$

Write

$$u(T^{-1}, T^{-N}\omega(T)^{-1}) = \sum_{n \in \mathbb{Z}} \beta_n T^n \tag{3.9}$$

with $\beta_n \in R$. Then

$$\overline{u}(T^{-1}, T^{-N}\omega(T)^{-1}) = \sum_{n \in \mathbb{Z}} \overline{\beta_n} T^n.$$

Therefore

$$\overline{\mathrm{ord}}_\infty \overline{h} = \min\{n : \beta_n \not\equiv 0 \bmod \mathfrak{p}\} + N^2.$$

On the other hand, (3.4) and (3.9) give

$$j^{N^2}\lambda_\infty(1/j)h = \sum_{n \in \mathbb{Z}} \beta_n j^{-n}.$$

Comparing q-expansions, we see that

$$-N^2 + \min\{n : c_n \not\equiv 0 \bmod \mathfrak{p}\} = \min\{n : \beta_n \not\equiv 0 \bmod \mathfrak{p}\}.$$

This proves (3.7). A proof for (3.8) is similar. In other words, we have

$$\partial_Y \Phi_N(T^{-N}\omega(T)^{-1}, T^{-1}) = T^{-N^2-N+1}\lambda_0(T) \qquad \text{with } \lambda_0(T) \in N + T\mathbb{Z}[[T]].$$

Note that N is invertible in F. Letting

$$u(T^{-N}\omega(T)^{-1}, T^{-1}) = \sum_{n \in \mathbb{Z}} \beta'_n T^n,$$

we obtain

$$\overline{\mathrm{ord}}_0 \overline{h} = \min\{n : \beta'_n \not\equiv 0 \bmod \mathfrak{p}\} + N^2 + N - 1.$$

On the other hand,

$$j\Big(\frac{\tau}{N}\Big)^{N^2+N-1} \lambda_0\Big(\frac{1}{j(\tau/N)}\Big) h\Big(\frac{-1}{\tau}\Big) = \sum_{n \in \mathbb{Z}} \beta'_n j\Big(\frac{\tau}{N}\Big)^n.$$

Expanding this equality by $q^{1/N}$, we have

$$-(N^2 + N - 1) + \min\{n : c'_n \not\equiv 0 \bmod \mathfrak{p}\} = \min\{n : \beta'_n \not\equiv 0 \bmod \mathfrak{p}\}. \qquad \square$$

In order to consider reductions at non-cusp points, we introduce the following terminology.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

DEFINITION 3.8. Let K be an algebraic number field, and $\mathfrak{p}$ a prime ideal which does not divide N. Let R be the ring of $\mathfrak{p}$-integral elements of K, and put $k := R/\mathfrak{p}R$. An imaginary quadratic $\tau_0 \in \mathcal{H}$ is said to be $(\mathfrak{p}, N)$-*admissible* if it satisfies the following conditions (3.10) and (3.11), and it is said to be $(\mathfrak{p}, N)$-*proper* if it satisfies all the following conditions (3.10) through (3.12).

(3.10) $j(\tau_0) \in K$ and $j(N\tau_0) \in K$.

(3.11) There exists $P(T) \in TR[[T]]$ satisfying $j(N\tau) = j(N\tau_0) + P(j(\tau) - j(\tau_0))$.

(3.12) $((\partial_Y \Phi_N)(j(\tau_0) + T, j(N\tau_0) + P(T)))^{-1} \in R((T))$. (Equivalently, the leading coefficient of the power series $(\partial_Y \Phi_N)(j(\tau_0)+T, j(N\tau_0)+P(T))$ is an invertible element of R.)

For a $(\mathfrak{p}, N)$-admissible τ_0, we define a valuation $\overline{\mathrm{ord}}_{\tau_0}$ on $\mathcal{B}(N)_k$ by

$$\overline{\mathrm{ord}}_{\tau_0}(u) = \mathrm{ord}_T\, u(\overline{j(\tau_0)} + T, \overline{j(N\tau_0)} + \overline{P}(T))$$

for $u \in k(X, \tilde{Y}) = \mathcal{B}(N)_k$.

THEOREM 3.9. *Under the notation in the above definition, assume that τ_0 is $(\mathfrak{p}, N)$-proper and that τ_0 is not an elliptic fixed point for $\mathrm{SL}(2, \mathbb{Z})$. Assume that $h \in \mathcal{A}(N)_R$ and $\overline{\mathrm{ord}}_{\tau_0}\overline{h} = 0$. Then $h(\tau_0) \in R^\times$.*

Proof. Since τ_0 is not an elliptic fixed point, $j'(\tau_0) \neq 0$ and $j(\tau) - j(\tau_0)$ is a local parameter at τ_0. Hence $h(\tau)$ is expanded to a power series of $j(\tau) - j(\tau_0)$. Take u as in (3.4). Then

$$h(\tau) = \frac{u(j(\tau), j(N\tau_0) + P(j(\tau) - j(\tau_0)))}{(\partial_Y \Phi_N)(j(\tau), j(N\tau_0) + P(j(\tau) - j(\tau_0)))}.$$

By the condition (3.12), we have the Laurent expansion

$$\sum_{m=M}^{\infty} c_m T^m := \frac{u(j(\tau_0) + T, j(N\tau_0) + P(T))}{(\partial_Y \Phi_N)(j(\tau_0) + T, j(N\tau_0) + P(T))} \in R((T)), \tag{3.13}$$

where $M \in \mathbb{Z}$ and $c_M \neq 0$. However, h is holomorphic at τ_0 and M must be non-negative. Then $h(\tau_0) = c_0$. On the other hand, by the definition of the reduction,

$$\overline{h}(\overline{j(\tau_0)} + T, \overline{j(N\tau_0)} + \overline{P}(T)) = \sum_{m=0}^{\infty} \overline{c_m} T^m.$$

Thus $\overline{\mathrm{ord}}_{\tau_0}\overline{h} = 0$ implies that $c_0 \notin \mathfrak{p}$. □

In order to show the properness of $\tau_0 \in \mathcal{H}$, we need the following lemmas.

LEMMA 3.10. *Let E be a CM elliptic curve defined over an algebraic number field K. Let $\mathfrak{p}$ be a prime ideal of K, and assume that E has ordinary reduction at $\mathfrak{p}$, and that $N \notin \mathfrak{p}$. Let $G_0, \ldots, G_N$ be the subgroups of E of order N. Put $A := \{j(E/G_i) : 0 \leqslant i \leqslant N\}$. Then the restriction of the reduction modulo $\mathfrak{p}$ map to A is injective.*

Proof. Note that E/G_i also has ordinary reduction at $\mathfrak{p}$, and that E/G_i is the canonical lift of $\overline{E/G_i}$. Hence the reduction modulo $\mathfrak{p}$ map induces an isomorphism

$$\mathrm{Hom}(E/G_m, E/G_n) \cong \mathrm{Hom}(\overline{E/G_m}, \overline{E/G_n}),$$

by [**11**, Corollary V.3.4]. Now $\overline{j(E/G_m)} = \overline{j(E/G_n)}$ implies that $\mathrm{Hom}(E/G_m, E/G_n)$ has an isogeny of degree 1, which is an isomorphism. Thus $j(E/G_m) = j(E/G_n)$. □

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

LEMMA 3.11. *Let $\tau_0 \in \mathcal{H}$ be an imaginary quadratic number. Assume that τ_0 is not an elliptic fixed point for* $\mathrm{SL}(2,\mathbb{Z})$, *and that $(\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0)) \neq 0$. Let p be a prime different from N, and put $K := \mathbb{Q}(j(\tau_0), j(N\tau_0))$. Let $\mathfrak{p}$ be a prime ideal of K dividing p, and let R be the valuation ring of $\mathfrak{p}$-adic valuation on K. Assume moreover that an elliptic curve (defined over K) whose j-invariant is $j(\tau_0)$ has ordinary reduction at $\mathfrak{p}$. Then τ_0 is $(\mathfrak{p}, N)$-proper.*

Proof. The condition (3.10) is trivially satisfied. Put $d := (\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0))$. Let $\gamma_0, \gamma_1, \ldots, \gamma_N$ be a system of representatives for $\Gamma_0(N) \setminus \mathrm{SL}(2,\mathbb{Z})$. Recall that

$$\Phi_N(j(\tau), Y) = \prod_{i=0}^{N} (Y - j(N\gamma_i\langle\tau\rangle)). \tag{3.14}$$

By Lemma 3.10, $d \neq 0$ implies that $d \in R^\times$. Put $P_1(T) := 0$, and define $P_n(T)$ by Newton's iterative root-finding recurrence formula; that is,

$$P_{n+1}(T) := P_n(T) - \frac{\Phi_N(j(\tau_0) + T, j(N\tau_0) + P_n(T))}{(\partial_Y \Phi_N)(j(\tau_0) + T, j(N\tau_0) + P_n(T))}$$

for $n \geqslant 2$. By induction on n, we see that $(\partial_Y \Phi)(j(\tau_0) + T, j(N\tau_0) + P_n(T)) \in R[[T]]^\times$, and that $P_{n+1}(T) \in TR[[T]]$. Therefore the limit $P(T)$ of the sequence $\{P_n(T)\}_{n=1}^{\infty}$ belongs to $TR[[T]]$. The non-vanishing lowest-degree term in $(\partial_Y \Phi_N)(j(\tau_0)+T, j(N\tau_0)+P(T))$ is the constant term $d \in R^\times$. This proves (3.12). Moreover, $P(T)$ is the unique formal power series in $T\mathbb{C}[[T]]$ satisfying $\Phi_N(j(\tau_0) + T, j(N\tau_0) + P(T)) = 0$ and $P(0) = 0$. Since j and $j \circ [N]$ are holomorphic on $\mathcal{H}$ and $j'(\tau_0) \neq 0$, there exists a (converging) power series $Q(T) \in T\mathbb{C}[[T]]$ satisfying $j(N\tau) = j(N\tau_0) + Q(j(\tau) - j(\tau_0))$. Letting $T := j(\tau) - j(\tau_0)$, we have $\Phi_N(j(\tau_0) + T, j(N\tau_0) + Q(T)) = 0$. By the uniqueness of P, we conclude that $P = Q$. Hence (3.11) holds. □

Now we consider the case $(\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0)) = 0$. Again, let

$$\gamma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_1, \ldots, \gamma_N$$

be a system of representatives for $\Gamma_0(N) \setminus \mathrm{SL}(2,\mathbb{Z})$. By (3.14) and [**16**, p. 248], reordering the γ_i if necessary, we may assume that

$$j(N\tau_0) = j(N\gamma_1\langle\tau_0\rangle) \neq j(N\gamma_i\langle\tau_0\rangle) \qquad \text{for } i \geqslant 2. \tag{3.15}$$

Put $\mathfrak{F} := \mathbb{Q}(\tau_0)$. We denote the maximal order of $\mathfrak{F}$ by $\mathfrak{O}$. Assume that τ_0 is not an elliptic fixed point for $\mathrm{SL}(2,\mathbb{Z})$. Then $\mathfrak{O}^\times = \{\pm 1\}$ and $j'(\tau_0) \neq 0$. Take $\beta \in \mathfrak{O} - \mathbb{Z}$ satisfying $N_{\mathfrak{F}/\mathbb{Q}}(\beta) = N^2$. (If no such β exists, then $\partial_Y \Phi_N(j(\tau_0), j(N\tau_0)) \neq 0$. See again [**16**, p. 248]). Put $\delta_{\mathfrak{F},N} := 4(\mathrm{Im}\,\beta)^2$. This is an integer that is independent of the choice of β, by the assumption that $\mathfrak{O}^\times = \{\pm 1\}$.

LEMMA 3.12. *Let $\tau_0 \in \mathcal{H}$ be an imaginary quadratic number which is not an elliptic fixed point for* $\mathrm{SL}(2,\mathbb{Z})$.

(i) *The quotient $a_1 := j'(N\tau_0)/j'(\tau_0)$ is an algebraic number.*

(ii) *Let $\mathfrak{p}$ be a prime ideal of an algebraic number field containing a_1. Assume that*

$$j(\tau_0)(j(\tau_0) - 1728) \not\equiv 0 \bmod \mathfrak{p} \quad \textit{and} \quad j(N\tau_0)(j(N\tau_0) - 1728) \not\equiv 0 \bmod \mathfrak{p}. \tag{3.16}$$

Then $\mathrm{ord}_{\mathfrak{p}}\, a_1 = 0$.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Proof. Since $j' = 2\pi i(E_4^2 E_6/\Delta)$, we see that

$$a_1 = \zeta \frac{j(N\tau_0)^{2/3}\sqrt{j(N\tau_0)-1728}}{j(\tau_0)^{2/3}\sqrt{j(\tau_0)-1728}} \cdot \left(\frac{\Delta(N\tau_0)}{\Delta(\tau_0)}\right)^{1/6}$$

where ζ is one of the sixth roots of unity. By [**10**, Chapter 12, Theorem 4], the quotient $\Delta(N\tau_0)/\Delta(\tau_0)$ is an algebraic integer dividing N^{12}. This proves all the assertions. □

LEMMA 3.13. *Let p be a prime satisfying $p \nmid N$. Let $\tau_0 \in \mathcal{H}$ be an imaginary quadratic number satisfying $(\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0)) = 0$ and $p \nmid \delta_{\mathfrak{F},N}$. Put*

$$a_1 := Nj'(N\tau_0)/j'(\tau_0) \qquad \text{and} \qquad K := \mathbb{Q}(\tau_0, j(\tau_0), j(N\tau_0), a_1).$$

Let $\mathfrak{p}$ be a prime ideal of K dividing p, and let R be the valuation ring of $\mathfrak{p}$-adic valuation on K. Assume that (3.16) holds, and that an elliptic curve (defined over K) whose j-invariant is $j(\tau_0)$ has ordinary reduction at $\mathfrak{p}$. Then τ_0 is $(\mathfrak{p}, N)$-proper.

Proof. We first note that K is an algebraic number field by Lemma 3.12(i). We also note that (3.16) implies that τ_0 is not an elliptic fixed point for $\mathrm{SL}(2,\mathbb{Z})$, and therefore $j'(\tau_0) \neq 0$. Differentiating $\Phi_N(j(\tau), j(N\tau)) = 0$ by τ, we obtain

$$(\partial_X \Phi_N)(j, j\circ[N])j' + N(\partial_Y \Phi_N)(j, j\circ[N])j'\circ[N] = 0 \tag{3.17}$$

and

$$\begin{aligned}(\partial_{XX}\Phi_N)(j, j\circ[N])j'^2 &+ 2N(\partial_{XY}\Phi_N)(j, j\circ[N])j'j'\circ[N]\\ &+ N^2(\partial_{YY}\Phi_N)(j, j\circ[N])j'^2\circ[N]\\ &+ (\partial_X\Phi_N)(j, j\circ[N])j''\\ &+ N^2(\partial_Y\Phi_N)(j, j\circ[N])j''\circ[N] = 0.\end{aligned} \tag{3.18}$$

Evaluating (3.17) at τ_0, we obtain

$$(\partial_X \Phi_N)(j(\tau_0), j(N\tau_0))j'(\tau_0) + N(\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0))j'(N\tau_0) = 0. \tag{3.19}$$

Because $j'(\tau_0) \neq 0$ and because of (3.19), we see that $(\partial_X \Phi_N)(j(\tau_0), j(N\tau_0)) = 0$. Then, evaluating (3.18) at τ_0 and dividing by $j'(\tau_0)^2$ ($\neq 0$), we obtain

$$\begin{aligned}(\partial_{XX}\Phi_N)(j(\tau_0), j(N\tau_0)) &+ 2N(\partial_{XY}\Phi_N)(j(\tau_0), j(N\tau_0))\frac{j'(N\tau_0)}{j'(\tau_0)}\\ &+ N^2(\partial_{YY}\Phi_N)(j(\tau_0), j(N\tau_0))\frac{j'(N\tau_0)^2}{j'(\tau_0)^2} = 0.\end{aligned} \tag{3.20}$$

It is straightforward to verify that

$$\Phi_N(T + j(\tau_0), a_1 T + j(N\tau_0)) \equiv 0 \bmod T^3 \qquad \text{in } R[T]. \tag{3.21}$$

On the other hand, differentiating (3.14) by Y twice, we find that

$$(\partial_{YY}\Phi_N)(j(\tau_0), j(N\tau_0)) = 2\prod_{i=2}^{N}(j(N\tau_0) - j(N\gamma_i\langle\tau_0\rangle)).$$

For $M := \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{GL}^+(2,\mathbb{R})$, let $J(M,\tau) := \det(M)^{-1/2}(c\tau + d)$. Differentiating (3.14) by τ, we have

$$j'(\tau)(\partial_X\Phi_N)(j(\tau), Y) = -\sum_{i=0}^{N} J(g_N\gamma_i, \tau)^{-2} j'(N\gamma_i\langle\tau\rangle)\prod_{n\neq i}(Y - j(N\gamma_n\langle\tau\rangle)),$$

where $g_N := \left(\begin{smallmatrix} N & 0 \\ 0 & 1\end{smallmatrix}\right)$.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Differentiating this by Y, we obtain

$$j'(\tau)(\partial_{XY}\Phi_N)(j(\tau),Y) = -\sum_{i=0}^{n} J(g_N\gamma_i,\tau)^{-2} j'(N\gamma_i\langle\tau\rangle) \sum_{n\neq i} \prod_{\substack{m\neq n\\ m\neq i}} (Y - j(N\gamma_m\langle\tau\rangle)).$$

Substituting τ by τ_0 and Y by $j(N\tau_0)$, we obtain

$$\begin{aligned} &j'(\tau_0)(\partial_{XY}\Phi_N)(j(\tau_0), j(N\tau_0)) \\ &\qquad = -\big(Nj'(N\tau_0) + J(g_N\gamma_i,\tau_0)^{-2} j'(N\gamma_i\langle\tau_0\rangle)\big) \prod_{m=2}^{N} (j(N\tau_0) - j(N\gamma_m\langle\tau_0\rangle)). \end{aligned}$$

Therefore

$$(\partial_Y\Phi_N)(T + j(\tau_0), a_1T + j(N\tau_0)) \equiv b_1b_2T \bmod T^2$$

with

$$\begin{aligned} b_1 &:= \prod_{m=2}^{N} (j(N\tau_0) - j(N\gamma_m\langle\tau_0\rangle)); \\ b_2 &:= \frac{1}{j'(\tau_0)}\big(Nj'(N\tau_0) - J(g_N\gamma_1,\tau_0)^{-2} j'(N\gamma_1\langle\tau_0\rangle)\big). \end{aligned}$$

We shall prove that $b_1b_2 \in R^\times$. Once this has been proved, (3.12) obviously holds and (3.11) follows from an argument similar to that used in the proof of the preceding lemma. However, this time we put $P_1(T) := a_1T$. Then

$$T^{-1}(\partial_Y\Phi_N)(j(\tau_0) + T, j(N\tau_0) + P_n(T)) \in R[[T]]^\times$$

under the condition that $b_1b_2 \in R^\times$, and therefore

$$P_{n+1}(T) \in R[[T]] \qquad \text{and} \qquad P_{n+1}(T) \equiv P_1(T) \bmod T^2$$

by (3.21).

By Lemma 3.10, we see that $b_1 \in R^\times$. We prove that $b_2 \in R^\times$. By the first equality in (3.15), there exists $M \in \mathrm{SL}(2,\mathbb{Z})$ satisfying

$$N\gamma_1\langle\tau_0\rangle = M\langle N\tau_0\rangle. \tag{3.22}$$

Since j' is a modular function of weight two, we have

$$\begin{aligned} &Nj'(N\tau_0) - J(g_N\gamma_1,\tau_0)^{-2} j'(N\gamma_1\langle\tau_0\rangle) \\ &\qquad = Nj'(N\tau_0) - \frac{J(M, g_N\langle\tau_0\rangle)^2}{J(g_N\gamma_1,\tau_0)^2} j'(N\tau_0) \\ &\qquad = Nj'(N\tau_0) - \frac{J(Mg_N,\tau_0)^2}{J(g_N,\tau_0)^2 J(g_N\gamma_1,\tau_0)^2} j'(N\tau_0) \\ &\qquad = N\left(1 - \left(\frac{J(Mg_N,\tau_0)}{J(g_N\gamma_1,\tau_0)}\right)^2\right) j'(N\tau_0). \end{aligned}$$

In order to compute $J(Mg_N,\tau_0)/J(g_N\gamma_1,\tau_0)$, we follow the method used in the proof of [**15**, Satz 3.6]. By (3.22), there exists $\alpha \in \mathfrak{F} := \mathbb{Q}(\tau_0)$ satisfying $\alpha g_N\gamma_1\binom{\tau_0}{1} = Mg_N\binom{\tau_0}{1}$.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Put $\tilde{M} := N\gamma_1^{-1} g_N^{-1} M g_N$, which belongs to $\mathrm{Mat}(2, \mathbb{Z})$. Then we have

$$N\alpha \begin{pmatrix} \tau_0 \\ 1 \end{pmatrix} = \tilde{M} \begin{pmatrix} \tau_0 \\ 1 \end{pmatrix}. \tag{3.23}$$

This implies that $N\alpha \in \mathrm{End}(\mathbb{Z} + \tau_0\mathbb{Z}) \subset \mathfrak{O}$, and that $N_{\mathfrak{F}/\mathbb{Q}}(N\alpha) = (\det \tilde{M})^2 = N^2$. Moreover,

$$\tilde{M}\langle \tau_0 \rangle = \tau_0 \tag{3.24}$$

by (3.23). Now

$$\begin{aligned} J(Mg_N, \tau_0) &= J(Ng_N\gamma_1\tilde{M}, \tau_0) \\ &= J(g_N\gamma_1, (N\tilde{M})\langle\tau_0\rangle) J(N\tilde{M}, \tau_0) \\ &= J(g_N\gamma_1, \tau_0) J(\tilde{M}, \tau_0) \qquad \text{(by (3.24))}. \end{aligned}$$

Noting that $\det \tilde{M} = N^2$, we see that $J(\tilde{M}, \tau_0) = \alpha$ by (3.23). Therefore

$$\frac{J(Mg_N, \tau_0)}{J(g_N\gamma_1, \tau_0)} = \alpha.$$

Eventually, we have obtained

$$b_2 = a_1(1 - \alpha^2).$$

Here $a_1 \in R^\times$ by Lemma 3.12(ii). Since $N\alpha \in \mathfrak{O}$ and $p \nmid N$, we have $\alpha \in R$. Let $\breve{\alpha}$ be the complex conjugate of α and assume that $\mathrm{ord}_{\mathfrak{p}}(1-\alpha^2) > 0$. Noting that $\delta_{\mathfrak{F},N} = N^2(\alpha - \breve{\alpha})^2$, we see that

$$0 < \mathrm{ord}_{\mathfrak{p}}(1 - \alpha^2)(1 - \breve{\alpha}^2) = \mathrm{ord}_{\mathfrak{p}}(\alpha - \breve{\alpha})^2 = \frac{1}{\mathrm{ord}_{\mathfrak{p}}\, p} \mathrm{ord}_p\, \delta_{\mathfrak{F},N},$$

which contradicts the assumption that $p \nmid N\delta_{\mathfrak{F},N}$. Therefore $b_2 \in R^\times$. This completes the proof. □

Although it is not used in the rest of this paper, we show an application of Lemma 3.13 which may be of independent interest. Put $d := (\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0))$ for simplicity. In [**15**, Satz 3.5 and its remark below], Schertz proved that a value of a modular function with the Fourier coefficients in $\mathbb{Q}$ at an imaginary quadratic $\tau_0 \in \mathcal{H}$ lie in $\mathbb{Q}(j(\tau_0), j(N\tau_0))$, provided that $d \neq 0$. There, the condition that $d \neq 0$ was crucial. Our Theorem 3.9 and Lemma 3.13 can handle the case where $d = 0$.

Corollary 3.14. *Let $\tau_0 \in \mathcal{H}$ be a non-elliptic fixed point for $\mathrm{SL}(2, \mathbb{Z})$. Let K be a finite-degree extension of $\mathbb{Q}(\tau_0, j(\tau_0), j'(N\tau_0)/j'(\tau_0))$. Assume that $(\partial_Y \Phi_N)(j(\tau_0), j(N\tau_0)) = 0$. Then for any $h \in \mathcal{A}(N)_K$, we have $h(\tau_0) \in K$.*

Proof. Indeed, there are infinitely many prime ideals $\mathfrak{p}$ which satisfy the assumptions of Lemma 3.13. That is, τ_0 is $(\mathfrak{p}, N)$-proper. Then, as in the proof of Theorem 3.9, there exists $c(T) \in K((T))$ satisfying $h(\tau) = c(j(\tau) - j(\tau_0))$. But h is holomorphic on H. Hence $c(T) \in K[[T]]$ and $h(\tau_0) = c(0) \in K$. Note that $j(N\tau_0) \in \mathbb{Q}(j(\tau_0))$ since $\Phi_N(j(\tau_0), Y) = 0$ has only one double root and the other roots are simple roots. □

4. *Fourier expansion of the Weierstrass function*

In this section, we compute the Fourier expansion of the Weierstrass $\wp$-function over the points t/N for $0 < t < N$. More explicitly, we compute functions $A_0(\tau), \ldots, A_{N-1}(\tau)$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

satisfying

$$-\frac{1}{4\pi^2}\wp\Big(\frac{t}{N};\tau\Big)=\sum_{m=0}^{N-1}A_m(\tau)\mathbf{e}\Big(\frac{mt}{N}\Big)$$

for $t=1,\dots,N-1$ and

$$0=\sum_{m=0}^{N-1}A_m(\tau).$$

We express $A_m(\tau)$ in terms of the Eisenstein series E_χ defined in Section 2. We begin with a simple lemma which links roots of unity and the Dirichlet characters.

LEMMA 4.1. *Let χ be the Dirichlet character modulo N and let $m\in\mathbb{Z}$. Put*

$$c_{m,\chi}=\frac{\mathfrak{g}(\chi^{-1})}{N-1}\chi(m), \tag{4.1}$$

where $\mathfrak{g}(\chi^{-1})$ is the Gauss sum. Then, for integers d and m,

$$\sum_\chi c_{m,\chi}\chi(d)=\begin{cases}\mathbf{e}\Big(\dfrac{md}{N}\Big) & (N\nmid dm),\\ 0 & (N\mid dm),\end{cases} \tag{4.2}$$

where (and in what follows) $\sum_\chi$ stands for a summation over all Dirichlet characters modulo N.

Proof. The assertion for the case $N\mid dm$ is obvious. Assume that $N\nmid dm$. Orthogonality of the Dirichlet characters gives

$$\begin{aligned}\sum_\chi c_{d,\chi}\chi(m)&=\frac{1}{N-1}\sum_\chi\left(\sum_{t=1}^{N-1}\chi^{-1}(t)\mathbf{e}\Big(\frac{t}{N}\Big)\chi(d)\right)\chi(m)\\&=\mathbf{e}\Big(\frac{dm}{N}\Big).\end{aligned}$$

□

LEMMA 4.2. *We have*

$$A_m=\begin{cases}2\displaystyle\sum_\chi c_{-m,\chi}E_{\chi^{-1}} & (m\neq 0),\\ 2E_{\chi_0} & (m=0).\end{cases}$$

Proof. Clearly,

$$A_m(\tau)=\sum_{t=1}^{N-1}\mathbf{e}\Big(-\frac{mt}{N}\Big)\left(-\frac{1}{4\pi^2}\wp\Big(\frac{t}{N};\tau\Big)\right).$$

Recall that

$$\wp(z;\tau)=\sum_{\substack{(\alpha,\beta)\in\mathbb{Z}^2\\(\alpha,\beta)\neq(0,0)}}\left(\frac{1}{(z-(\alpha\tau+\beta))^2}-\frac{1}{(\alpha\tau+\beta)^2}\right).$$

Hecke has proved [2, (14)] that

$$N^{-2}\wp\left(\frac{u\tau+v}{N};\tau\right)=G_{(u,v)}(\tau)-G_{(0,0)}(\tau). \tag{4.3}$$

(Note that the exponent of N on the left-hand side should be -2, not 2 as in Hecke's paper.)

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

In the case of $m \neq 0$, we have

$$\begin{aligned} A_m(\tau) &= \sum_{t=1}^{N-1} \mathbf{e}\Big(-\frac{mt}{N}\Big) \frac{-N^2}{4\pi^2} \left(G_{(0,t)} - G_{(0,0)}\right) \\ &= 2\left(c_{-m,\chi_0}\left(E_{\chi_0} - \frac{N-1}{24}\mathbf{E}_2\right) + \sum_{\chi \neq \chi_0} c_{-m,\chi} E_{\chi^{-1}}\right) - \frac{1}{12}\mathbf{E}_2 \end{aligned}$$

by (4.2), (2.4), (2.14) and (2.13). Since $\mathfrak{g}(\chi_0) = -1$ and

$$c_{d,\chi_0} = \begin{cases} \dfrac{-1}{N-1} & (d \not\equiv 0 \bmod N), \\ 0 & (d \equiv 0 \bmod N), \end{cases}$$

we see that $A_m(\tau) = 2\sum_\chi c_{-m,\chi} E_{\chi^{-1}}$. The formula for A_0 is an immediate consequence of (2.14) and (2.13). □

Definition 4.3. For an algebraic number field K, we denote by $K_{[2,N]}$ the field generated by

$$\left\{\mathbf{e}\Big(\frac{1}{N-1}\Big), \mathbf{e}\Big(\frac{1}{N}\Big)\right\} \cup \bigcup_{\chi:\text{even}} \left\{\mathfrak{g}(\chi), \frac{1}{\pi^2} L(2,\chi)\right\}$$

over K.

Proposition 4.4. *Let F_N be the product*

$$\prod_{m=1}^{N-1} A_m.$$

Then F_N is a non-zero element of $M_{2(N-1)}(\Gamma_0(N), \chi_0)$. The Fourier coefficients of F_N and $F_N|_{2(N-1)} \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ belong to $\mathbb{Q}_{[2,N]}$, and they are $\mathfrak{p}$-integral where $\mathfrak{p}$ is any prime ideal of $\mathbb{Q}_{[2,N]}$ not dividing $3(N-1)$.

Proof. For $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we see that

$$\begin{aligned} F_N|_{2(N-1)} M &= \prod_{m=1}^{N-1} \left(2\sum_\chi c_{-m,\chi} E_{\chi^{-1}}|_2 M\right) \\ &= \prod_{m=1}^{N-1} \left(2\sum_\chi c_{-m,\chi} \chi^{-1}(M) E_{\chi^{-1}}\right). \end{aligned}$$

It follows immediately from the definition (4.1) of $c_{d,\chi}$ that

$$c_{-m,\chi}\chi(d) = c_{-dm,\chi} \qquad \text{for } d \nmid N.$$

Let d' be an integer satisfying $dd' \equiv 1 \bmod N$. Then

$$F_N|_{2(N-1)} M = \prod_{m=1}^{N-1} \left(2\sum_\chi c_{-d'm,\chi} E_{\chi^{-1}}\right) = F_N.$$

Denote by $M_2(\Gamma_1(N))$ the space of modular forms of weight 2 with respect to $\Gamma_1(N)$. By the direct sum decomposition $M_2(\Gamma_1(N)) = \bigoplus_\chi M_2(\Gamma_0(N), \chi)$, we see that A_m is

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

a non-zero function. Hence F_N is non-zero. The assertion on the Fourier coefficients of F_N follows from (2.12) and (2.15). On the other hand, the assertion on the Fourier coefficients of $F_N|_{2(N-1)}\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ follows from (2.7) and (2.11) and

$$\begin{aligned} F_N|_{2(N-1)}\begin{pmatrix}0&1\\-1&0\end{pmatrix} &= \prod_{m=1}^{N-1} A_m|_2\begin{pmatrix}0&1\\-1&0\end{pmatrix} \\ &= \prod_{m=1}^{N-1}\left(2\sum_{\chi} c_{-m,\chi}E_{\chi^{-1}}|_2\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right) \\ &= \prod_{m=1}^{N-1}\left(2\sum_{\chi} c_{-m,\chi}E^{\chi^{-1}}\right). \end{aligned}$$

□

5. *Cryptographic application*

We apply results developed in the previous sections to elliptic curves over $\mathbb{F}_q$ where q is a power of prime $p \geqslant 5$. Throughout this section, $N \geqslant 5$ is a prime satisfying $p \nmid N-1$.

For an imaginary quadratic $\tau \in \mathcal{H}$, we define an elliptic curve E_τ by

$$Y^2 = X^3 - \frac{1}{2^4 3}\frac{E_4(\tau)}{\Delta^{1/3}(\tau)}X + \frac{1}{2^5 3^3}\frac{E_6(\tau)}{\Delta^{1/2}(\tau)}.$$

Here, for a divisor δ of 24, we explicitly put

$$\Delta^{1/\delta}(\tau) := \mathbf{e}(\tau/\delta)\prod_{n=1}^{\infty}(1-\mathbf{e}(n\tau))^{24/\delta}.$$

The complex numbers

$$a_4(\tau) := \frac{E_4(\tau)}{\Delta^{1/3}(\tau)} \qquad \text{and} \qquad a_6(\tau) := \frac{E_6(\tau)}{\Delta^{1/2}(\tau)}$$

are in fact algebraic integers. Put $k_\tau := \mathbb{Q}(a_4(\tau), a_6(\tau))$. The discriminant of E_τ is 1, and the j-invariant of E_τ is $j(\tau)$. In particular, E_τ has good reduction at any prime ideal $\mathfrak{p}$ of k_τ which does not divide 6. The map $\mathcal{P}_\tau$, defined by

$$\mathcal{P}_\tau(z) := \left(-\frac{1}{4\pi^2}\frac{\wp(z;\tau)}{\Delta^{1/6}(\tau)},\ \frac{1}{(2\pi i)^3}\frac{\wp'(z;\tau)}{\Delta^{1/3}(\tau)}\right),$$

induces an isomorphism between $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ and E_τ. Let C_τ be the cyclic subgroup of E_τ generated by $\mathcal{P}_\tau(1/N)$.

Now, let E be an elliptic curve over $\mathbb{F}_p$ given by the short Weierstrass form, and let C be its cyclic subgroup of order N. Let B be a generator of C, and let ζ be one of the Nth primitive roots of unity. Let ξ be the X-coordinate function. There uniquely exist constants $\alpha(E, B, \zeta, m)$ for $0 \leqslant m < N$ satisfying

$$\xi(nB) = \sum_{m=0}^{N-1}\alpha(E, B, \zeta, m)\zeta^{-nm}$$

for $1 \leqslant n \leqslant N-1$ and

$$\sum_{m=0}^{N-1}\alpha(E, B, \zeta, m) = 0.$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Put

$$Z_{E,C} := \#\{m : 1 \leqslant m < N,\ \alpha(E, B, \zeta, m) = 0\}.$$

As the notation suggests, $Z_{E,C}$ is independent of the choice of B and ζ. For $\mu, \nu \in (\mathbb{Z}/N\mathbb{Z})^\times$, it is easy to observe that

$$\alpha(E, \nu B, \zeta^\mu, m) = \alpha(E, B, \zeta, \nu^{-1}\mu m).$$

Moreover, let E' be an elliptic curve (also given by the short Weierstrass form) which is isomorphic to E under an isomorphism $\varphi : (x, y) \to (\gamma^2 x, \gamma^3 y)$ defined over $\mathbb{F}_p^a$. Then

$$\alpha(\varphi(E), \varphi(B), \zeta, m) = \gamma^2 \alpha(E, B, \zeta, m).$$

Therefore, $Z_{E,C}$ depends only on an isomorphism class of the level-N structure (E, C). Let $\mathcal{X}(N)$ be the set of the isomorphism classes of (E, C) which satisfies the condition that E is ordinary and that $j(E)(j(E) - 1728) \neq 0$.

Note that $\mathcal{X}(N)$ is a finite set. By the Deuring lifting theorem, there exist an algebraic number field K and a prime ideal $\mathfrak{p}$ dividing p such that for each $(E, C) \in \mathcal{X}(N)$ there exists an imaginary quadratic $\tau \in \mathcal{H}$ with the following properties.

(1) $K \supset \mathbb{Q}\left(j(N\tau), (\Delta(N\tau)/\Delta(\tau))^{1/6}, \sqrt{-3}\right)$.
(2) $C_\tau \subset E(K)$.
(3) $j(E_\tau/C_\tau) = j(N\tau)$.
(4) There exists an isomorphism $\varphi : \overline{E_\tau} \to E$.
(5) $\varphi(\overline{C_\tau}) = C$.
(6) $\overline{\mathrm{End}(E_\tau)} = \mathrm{End}(\overline{E_\tau}) \cong \mathrm{End}(E)$.

For each pair $(E, C) \in \mathcal{X}(N)$, choose (and fix) $\tau \in \mathcal{H}$ as above and denote it by $t(E, C)$. We denote the residue field of $\mathfrak{p}$ by k. We begin with estimating a number of isomorphism classes of E which might correspond to non-proper τ.

Lemma 5.1. *Let N be a prime number different from p.*

(i) *If $N > \sqrt{12p}$, then there are at most two (up to isomorphisms over $\mathbb{F}_p^a$) ordinary elliptic curves E defined over $\mathbb{F}_p$ which contains a cyclic subgroup C of order N satisfying $j(E/C) = 0$.*

(ii) *If $N > 2\sqrt{p}$, then there are at most two (up to isomorphisms over $\mathbb{F}_p^a$) ordinary elliptic curves E defined over $\mathbb{F}_p$ which contains a cyclic subgroup C of order N satisfying $j(E/C) = 1728$.*

Proof. (i) Let E' be an elliptic curve defined over $\mathbb{F}_p$ such that $j(E') = 0$. An isogeny $E \to E/C \cong E'$ maps a non-trivial point of order p in E to that in E' because $p \nmid \#C$. Hence E' is ordinary, and we obtain $p \equiv 1 \bmod 3$. We denote the pth power Frobenius endomorphism by φ. First, we show that there exists $C' \subset E'$ such that C' is an eigenspace of φ^6 and $j(E'/C') = j(E)$. Indeed, there exists an isogeny $f \in \mathrm{Hom}_{\mathbb{F}_p^a}(E', E)$ satisfying $\deg f = N$. This isogeny f is defined over some finite extension $\mathbb{F}_{p^r}$ of $\mathbb{F}_p$. Then the characteristic equations of φ^r on these curves are the same (cf. [16, pp. 236–237]; see also [17, Theorem III.7.7]). The quotient field of their endomorphism ring is $\mathbb{Q}(\sqrt{-3})$. Let λ and λ' be the images of φ^p on E and E', respectively, in $\mathbf{Q}(\sqrt{-3})$. Then we have either $\lambda^r = \lambda'^r$ or $\check{\lambda}^r = \lambda'^r$. Hence either λ/λ' or $\check{\lambda}/\lambda'$ is an rth root of the unity in $\mathbb{Q}(\sqrt{-3})$. Hence $r \mid 6$. Let C' be the kernel of f'. Then C' is defined over $\mathbb{F}_{p^6} \supset \mathbb{F}_{p^r}$. This means that C' is an eigenspace of φ^6 in $E'[N]$, a two-dimensional vector space over $\mathbb{F}_N$.

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Now we assume that there are three curves defined over $\mathbb{F}_p$ satisfying the condition of the assertion of the lemma. Then there exist three distinct eigenspaces of φ^6 in $E'[N]$. Hence a matrix representation of φ^6 on $E'[N]$ is a scalar matrix. Let $\alpha, \beta \in \mathbb{Q}(\sqrt{-3})$ be the characteristic roots of φ ($\in \mathrm{End}(E')$). Then it is necessary that $\alpha^6 \equiv \beta^6 \bmod N$. Since $p \equiv 1 \bmod 3$, without loss of generality we may put

$$\alpha := u + \frac{-1+\sqrt{-3}}{2}v \qquad \text{and} \qquad \beta := u + \frac{-1-\sqrt{-3}}{2}v$$

where u and v are integers satisfying

$$u^2 - uv + v^2 = p. \tag{5.1}$$

Then

$$\begin{aligned}\alpha^6 - \beta^6 &= \left(\left(u - \frac{v}{2}\right) + \frac{\sqrt{-3}}{2}v\right)^6 - \left(\left(u - \frac{v}{2}\right) - \frac{\sqrt{-3}}{2}v\right)^6 \\ &= 3\sqrt{-3}uv(u-v)(u+v)(u-2v)(2u-v). \end{aligned} \tag{5.2}$$

Therefore, $\alpha^6 \equiv \beta^6 \bmod N$ implies that N divides one of u, v, $u \pm v$, $2u - v$ or $2v - u$ since $N > \sqrt{12p} \geqslant \sqrt{60}$. On the other hand, (5.1) restricts

$$|u| \leqslant \frac{2}{\sqrt{3}}\sqrt{p} \qquad \text{and} \qquad |v| \leqslant \frac{2}{\sqrt{3}}\sqrt{p}.$$

This contradicts $N > \sqrt{12p}$.

The proof of part (ii) is similar, and in fact a bit easier. In this case we work over $\mathbb{Q}(\sqrt{-1})$. Instead of (5.2), we obtain

$$\alpha^4 - \beta^4 = 8\sqrt{-1}uv(u+v)(u-v)$$

where $p = u^2 + v^2 \equiv 1 \bmod 4$. □

Lemma 5.2. *Let $(E, C) \in \mathcal{X}(N)$ and put $\tau := t(E, C)$. Assume that $N < \frac{2}{\sqrt{3}}p$ and that*

$$j(N\tau)(j(N\tau) - 1728) \not\equiv 0 \bmod \mathfrak{p}.$$

Then τ is $(\mathfrak{p}, N)$-proper.

Proof. In the case of $(\partial_Y \Phi_N)(j(\tau), j(N\tau)) \neq 0$, the assertion follows from Lemma 3.11 (regardless of the magnitude of N). Now assume that $(\partial_Y \Phi_N)(j(\tau), j(N\tau)) = 0$. Put $\mathfrak{F} := \mathbb{Q}(\tau)$ and choose ω so that $\mathbb{Z} + \omega\mathbb{Z}$ is the maximal order $\mathfrak{O}$ of $\mathfrak{F}$. Without loss of generality, we may assume that the minimal equation of ω is $\omega^2 + b\omega + c = 0$ where $b = 0$ or $b = 1$. Assume that $\beta := x + y\omega \in \mathfrak{O} - \mathbb{Z}$ satisfy $N_{\mathfrak{F}/\mathbb{Q}}(\beta) = N^2$. This is equivalent to $x^2 + bxy + cy^2 = N^2$. Then $\delta_{\mathfrak{F},N} = (4c - b^2)y^2$. By Lemma 3.13, it suffices to show that $p \nmid \delta_{\mathfrak{F},N}$. Since $\overline{E_\tau}$ is ordinary, the prime p splits in $\mathfrak{F}$ into two *different* prime ideals. Hence $p \nmid (4c - b^2)$. Suppose that $p \mid y$. Since $y \neq 0$, this implies that $|y| \geqslant p$. Thus, we obtain $\frac{3}{4}p^2 \leqslant N^2$, a contradiction. Therefore $p \nmid y$. □

Theorem 5.3. *Let N be a prime satisfying $\sqrt{12p} < N < \frac{2}{\sqrt{3}}p$. Then*

$$\frac{\#\{(E, C) \in \mathcal{X}(N) : Z_{E,C} = 0\}}{\#\mathcal{X}(N)} \geqslant \left(1 - \frac{8}{11\sqrt{3}} - \frac{76}{11p}\right)\left(1 - \frac{12}{11p + 12}\right).$$

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

Proof. Let $(E, C) \in \mathcal{X}(N)$ and put $\tau := t(E, C)$, $B_\tau := \overline{\mathcal{P}_\tau(1/N)}$ and $\zeta := \overline{\mathbf{e}(1/N)}$. Then

$$\alpha(E_\tau, B_\tau, \zeta, m) = \overline{\left(\frac{A_m(\tau)}{\Delta^{1/6}(\tau)}\right)} \tag{5.3}$$

for $1 \leqslant n < N$. (Note that $\alpha(E_\tau, B_\tau, \zeta, m)$ is $\mathfrak{p}$-integral.) Consider a function h defined by

$$h := \begin{cases} \dfrac{1}{\Delta^{(N-1)/6}} \displaystyle\prod_{m=1}^{N-1} A_m & (N \equiv 1 \bmod 6), \\ \dfrac{1}{\Delta^{(N+1)/6}} A_0^2 \displaystyle\prod_{m=1}^{N-1} A_m & (N \equiv -1 \bmod 6). \end{cases} \tag{5.4}$$

Then h is a modular function for $\Gamma_0(N)$, which is holomorphic on $\mathcal{H}$ by Proposition 4.4. Put $\nu := [(N+1)/6]$. The orders of the poles of h at the cusps are at most ν at ∞ and $N\nu$ at 0. By Proposition 3.7, we have $\overline{\mathrm{ord}}_0 \overline{h} \geqslant -\nu N$ and $\overline{\mathrm{ord}}_\infty \overline{h} \geqslant -\nu$. Put

$$\mathcal{U}(N) := \big\{(E, C) \in \mathcal{X}(N) : \text{All cyclic subgroups } C' \text{ in } E \text{ of order } N \text{ satisfy } j(E/C') \neq 0 \text{ and } j(E/C') \neq 1728\big\}.$$

We see that $t(E, C)$ is $(\mathfrak{p}, N)$-proper for $(E, C) \in \mathcal{U}(N)$ by Lemma 5.2. Put

$$S_1 := \big\{\overline{\mathrm{ord}}_{t(E,C)} : (E, C) \in \mathcal{U}(N)\big\}$$

and let S_2 be the complement set of $S_1 \cup \{\overline{\mathrm{ord}}_0, \overline{\mathrm{ord}}_\infty\}$ in the set of valuations on $\mathcal{B}(N)_k$. Then $\mathrm{Gal}(\mathcal{B}(N)_k/\mathcal{B}(1)_k)$ acts not only on S_1 but also on S_2. (This is why we introduced C' in the definition of $\mathcal{U}(N)$ instead of using C.) By Theorem 3.6,

$$\sum_{v \in S_2} v(\overline{h}) \geqslant 0.$$

Hence $v(\overline{h}) > 0$ holds for at most $(N+1)\nu$ valuations v in S_1.

Suppose that $\overline{\mathrm{ord}}_\tau \overline{h} = 0$ where $\tau := t(E, C)$ with some $(E, C) \in \mathcal{U}(N)$. Since $N < (2/\sqrt{3})p$, it is clear that $p \nmid (N-1)$. Then Theorem 3.9 yields $h(\tau) \not\equiv 0 \bmod \mathfrak{p}$. Hence (5.3) and (5.4) imply that

$$\prod_{m=1}^{N-1} \alpha(E_\tau, B_\tau, \zeta, m) \neq 0 \qquad \text{for } N \equiv 1 \bmod 6,$$

and that

$$\alpha(E_\tau, B_\tau, \zeta, 0)^2 \prod_{m=1}^{N-1} \alpha(E_\tau, B_\tau, \zeta, m) \neq 0 \qquad \text{for } N \equiv -1 \bmod 6.$$

In either case, $Z_{E,C} = Z_{\overline{E_\tau}, \overline{C_\tau}} = 0$.

There are at most $p/12 + 2$ supersingular j values. Thus there at least $(11/12)p - 4$ ordinary j values in $\mathbb{F}_p$ other than 0 and 1728. Then

$$\#\mathcal{U}(N) \geqslant ((11/12)p - 6)(N+1)$$

by the assumption that $N > \sqrt{12p}$ and Lemma 5.1. Note that the correspondence

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

$t : (E, C) \to \tau$ is at most two-to-one. Therefore

$$\frac{\#\{(E,C) \in \mathcal{U}(N) : Z_{E,C} = 0\}}{\#\mathcal{X}(N)} \geqslant \frac{\left(\frac{11}{12}p - 6\right)(N+1) - 2^{\frac{(N+1)^2}{6}}}{\left(p - \left[\frac{p}{12}\right]\right)(N+1)}$$
$$\geqslant \left(1 - \frac{8}{11\sqrt{3}} - \frac{76}{11p}\right)\left(1 - \frac{12}{11p+12}\right). \qquad \square$$

Acknowledgement. The author would like to thank Igor Semaev and Steven Galbraith for valuable discussions.

References

1. D. A. Cox, *Primes of the form $x^2 + ny^2$* (Wiley, New York, 1989). 143
2. E. Hecke, 'Theorie der eisensteinschen riehen höherer stufe und ihre anwendung auf funktionentheorie und arithmetik', *Abh. Math. Sem. Hamburg* 5 (1927) 199–224. 137, 138, 139, 151
3. J. Igusa, 'Fibre systems of jacobian varieties. III Fibre systems of elliptic curves', *Amer. J. Math.* 81 (1959) 453–476. 142, 144
4. N. M. Katz, 'p-adic properties of modular schemes and modular forms', *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lect. Notes in Math. 350 (Springer, Berlin, 1973) 69–190. 141
5. E. Kiltz and A. Winterhof, 'On the interpolation of bivariate polynomials related to the Diffie–Hellman mapping', *Bull. Austral. Math. Soc.* 69 (2004) 305–315. 135
6. N. Koblitz and A. Menezes, 'Pairing-based cryptography at high security levels', *Cryptograhy and Coding 2005*, ed. N. P. Smart, Lect. Notes in Comput. Sci. 3796 (Springer, Berlin/Heidelberg, 2005) 13–36. 136
7. T. Lange and A. Winterhof, 'Polynomial interpolation of the elliptic curve and XTR discrete logarithm', *Proc. COCOON 2002*, ed. O. H. Ibarra and L. Zhang, Lect. Notes in Comput Sci. 2387 (Springer, Berlin/Heidelberg, 2002) 137–143. 135
8. T. Lange and A. Winterhof, 'Interpolation of the discrete logarithm in $\mathbb{F}_q$ by boolean functions and by polynomials in several variables modulo a divisor of $q-1$', *Discrete Appl. Math.* 128 (2003) 193–206. 135
9. T. Lange and A. Winterhof, 'Interpolation of the elliptic curve Diffie–Hellman mapping', *Proc. AAECC 2003*, ed. M. Fossorier, T. Høholdt and A. Poli, Lect. Notes in Comput. Sci. 2643 (Springer, Berlin/ Heidelberg, 2003) 51–60. 135
10. S. Lang, *Elliptic functions*, Grad. Texts in Math. 112 (Springer, Berlin/Heidelberg, 1987). 148
11. W. Messing, *The crystals associated to Barsotti–Tate groups: with applications to Abelian schemes*, Lect. Notes in Math. 264 (Springer, Berlin/Heidelberg/New York, 1972). 146
12. G. L. Mullen and D. White, 'A polynomial representation for logarithms in $gf(q)$', *Acta Arith.* 47 (1986) 255–261. 135
13. H. Niederreiter, 'A short proof for explicit formulas for discrete logarithms in finite fields', *Appl. Alg. Eng. Comm. Comput.* 1 (1990) 55–57. 135

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press

14. T. Satoh, 'On degrees of polynomial interpolation related to elliptic curve cryptography', *Proc. International Workshop on Coding and Cryptograpy* (*WCC 2005*), ed. Ø. Ytrehus, Lecture Notes in Comput. Sci. 3969 (Springer, Berlin/Heidelberg, 2006) 55–61. 135

15. R. Schertz, 'Die singulären werte der weberschen funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3', *J. Reine Angew. Math.* 286/287 (1976) 46–74. 137, 149, 150

16. R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* 7 (1995) 219–254. 147, 154

17. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. 106 (Springer, Berlin/Heidelberg/New York, 1985). 154

18. A. D. Thomas, *Zeta-functions: an introduction to algebraic geometry*, Research Notes in Math. 12 (Pitman Publishing, London/San Francisco, 1977). 141

19. E. R. Verheul, 'Evidence that XTR is more secure than supersingular elliptic curve cryptosystems', *Advances in cryptology - EUROCRYPT 2001* (ed. B. Pfitzmann), Lecture Notes in Comput. Sci. 2045 (Springer, Berlin/Heidelberg, 2001) 195–210. 136

20. A. L. Wells, Jr, 'A polynomial form for logarithms modulo a prime', *IEEE Trans. IT* 30 (1984) 845–846. 135

Takakazu Satoh `satojlms@mathpc-satoh.math.titech.ac.jp`
`http://mathpc-satoh.math.titech.ac.jp/en/TkkzSatoh.html`

Department of Mathematics
Tokyo Institute of Technology
Tokyo, 152-8551
Japan

https://doi.org/10.1112/S1461157000001224 Published online by Cambridge University Press