J. Math. Soc. Japan
Vol. 39, No. 2, 1987

# Heegner points and the modular curve of prime level

By Benedict H. GROSS

(Received Nov. 30, 1985)

The purpose of this note is to show how Heegner points can be used to study the geometry of the modular curve $X=X_0(N)$ when $N$ is prime. For example, we will show that the classical model for $X$ in $\boldsymbol{P}^1\times\boldsymbol{P}^1$ given by the zeroes of the $N^{\text{th}}$ modular polynomial has only ordinary double points as singularities. We will also consider a specific fibre system of elliptic curve over $X$ when $N\equiv 3 \pmod 4$ and relate the fibres over certain Heegner points to $\boldsymbol{Q}$-curves.

I wish to thank R. Rumely, J. Tate, and D. Zagier for suggesting some of the problems considered in this paper.

## §1. Function theory.

Let $N$ be a prime. The curve $Y=Y_0(N)$ is defined over $\boldsymbol{Q}$ and classifies elliptic curves with an $N$-isogeny. If $F$ is any field of characteristic zero the points of $Y$ rational over $F$ correspond to diagrams

$$x=(\phi : E \rightarrow E'),$$

where $E$ and $E'$ are elliptic curves over $F$ and $\phi$ is an $F$-rational (cyclic) isogeny of degree $N$. The complex points of $Y$ may be identified with the Riemann surface $\mathfrak{H}/\Gamma_0(N)$ [**5**, §1].

The curve $Y$ is non-singular, but is not complete. We denote its compactification $X=X_0(N)$; this is obtained by adjoining the two cusps $\infty$ and $0$ which correspond to diagrams $(\phi : E\rightarrow E')$ of degenerate elliptic curves where the kernel of $\phi$ meets each geometric component of $E$ [**1**, pp. 150-151]. We will call the points $x$ of $Y$ affine points of $X$; if $x$ is a complex affine point we let $\tau$ be a pre-image of $x$ in $\mathfrak{H}$ and $q=e^{2\pi i\tau}$.

The complex function field of $X$ consists of the modular functions $f(\tau)$ for $\Gamma_0(N)$ which are meromorphic on the extended upper half-plane. A function $f$ lies in the rational function field $\boldsymbol{Q}(X)$ if and only if the Fourier coefficients in its expansion at $\infty : f(\tau)=\sum a_n q^n$ are all rational numbers [**1**, p. 306]. The field $\boldsymbol{Q}(X)$ is known to be generated over $\boldsymbol{Q}$ by the functions

$$
(1.1) \qquad \begin{cases} j = j(E) = j(\tau) = q^{-1}+744+196884q+\cdots \\ j_N = j(E') = j(-1/N\tau) = j(N\tau) = q^{-N}+744+\cdots. \end{cases}
$$

A further element in the function field $\boldsymbol{Q}(X)=\boldsymbol{Q}(j, j_N)$ is the modular unit

$$
(1.2) \qquad u = \frac{\Delta(\tau)}{\Delta(N\tau)}
$$

with divisor $(N-1)\{(0)-(\infty)\}$. If $m=\gcd(N-1, 12)$, then an $m^{\text{th}}$ root of $u$ lies in $\boldsymbol{Q}(X)$; this function has the Fourier expansion

$$
(1.3) \qquad t = \sqrt[m]{u} = q^{(1-N)/m}\prod_{n\geq 1}\left(\frac{1-q^n}{1-q^{nN}}\right)^{24/m} = \left(\frac{\eta(\tau)}{\eta(N\tau)}\right)^{24/m}.
$$

When $N-1$ divides 12, so $m=N-1$, the function $t$ is a Hauptmodul for the curve $X$ (which has genus 0).

The canonical involution $w=w_N$ of $X$ takes the diagram $x=(\phi: E\to E')$ to the diagram $w(x)=(\phi^\vee: E'\to E)$, where $\phi^\vee$ is the dual isogeny. We denote its action on modular functions by $g\to g_N$, so

$$
g_N(x) = g(w(x)) = g(-1/N\tau).
$$

This is in agreement with our notation in (1.1), and $(j_N)_N=j$. Since

$$
(1.4) \qquad \eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)
$$

(where the square root has positive real part), we find from formula (1.3) the relation

$$
(1.5) \qquad t\cdot t_N = N^{12/m}.
$$

We note that the functions $j$, $j_N$, $t$, and $t_N$ all lie in the affine co-ordinate ring of $Y$

$$
(1.6) \qquad R_{\boldsymbol{Q}} = H^0(Y, \mathcal{O}_Y) = H^0(X-\{\infty, 0\}, \mathcal{O}_X)
$$

as they are regular outside the cusps. By (1.5), $t$ and $t_N$ are units in this $\boldsymbol{Q}$-algebra.

## § 2. Heegner points.

We say the affine point $x=(\phi: E\to E')$ is a Heegner point of $X$ if $\mathrm{End}(E)=\mathrm{End}(E')=\mathcal{O}$ is an order of conductor prime to $N$ in an imaginary quadratic field $K$. Then the field $K(x)$ is a finite abelian extension of $K$, the ring class field of conductor $\boldsymbol{c}=\mathrm{cond}(\mathcal{O})$, and the values $j(x)$, $j_N(x)$, $t(x)$ are all algebraic integers of $K(x)$ [**5**, § 4].

Over the complex numbers, a Heegner point $x$ is described by the order $\mathcal{O}$, invertible ideal $\mathfrak{n}$ of index $N$ in $\mathcal{O}$ which annihilates $\ker\phi$, and the class $[\mathfrak{a}]$ of the projective $\mathcal{O}$-module $H_1(E, \boldsymbol{Z})$ in $\mathrm{Pic}(\mathcal{O})$. We have

$$x = (E(\boldsymbol{C})=\boldsymbol{C}/\mathfrak{a} \underset{\phi}{\rightarrow} E'(\boldsymbol{C})=\boldsymbol{C}/\mathfrak{a}\mathfrak{n}^{-1}).$$

The involution $w$ acts on Heegner points by the formula:

$$w(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \bar{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}]) \tag{2.1}$$

where $\alpha \mapsto \bar{\alpha}$ is the non-trivial involution of $K$ over $\boldsymbol{Q}$. The Artin isomorphism of global class field theory $\mathfrak{b} \rightarrow \sigma_{\mathfrak{b}}$ gives an isomorphism $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(K(x)/K)$ and this group acts on Heegner points by the formula

$$\sigma_{\mathfrak{b}}(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]). \tag{2.2}$$

Finally, if $x=(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ then

$$t(x) = \sqrt[m]{\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{a}\bar{\mathfrak{n}})}} \tag{2.3}$$

generates the ideal $(\bar{\mathfrak{n}}A)^{12/m}$, where $A$ is the ring of integers in $K(x)$.

## § 3. The fixed points of $w$.

We say a Heegner point $x$ has discriminant $D$ if $D=\mathrm{disc}(\mathcal{O})$.

PROPOSITION 3.1. *The fixed points of $w$ on $X$ consists of those Heegner points whose discriminants $D$ divide $-4N$ and are divisible by $N$.*

PROOF. If $w(x)=x$ then $E \simeq E'$ over $\boldsymbol{C}$ and the isogeny $\phi: E \rightarrow E'$ gives rise to a complex multiplication $\alpha$ of $E$ of degree $N$. Since $\ker\phi$ is identified with $\ker\phi^{\vee}$, the trace $\alpha+\bar{\alpha}=t$ is divisible by $N$. But the discriminant $D$ of $\mathcal{O}=\mathrm{End}(E)$ divides the discriminant of the sub-order $\boldsymbol{Z}[\alpha]$, which is equal to $t^2-4N<0$. If $N>3$ we must have $t=0$ and $D$ divides $-4N$. If $N=3$ then $t=0$, $\pm 3$ and $D$ divides $-12$; if $N=2$ then $t=0$, $\pm 2$ and $D$ divides $-8$. Since in all cases the conductor of $\mathcal{O}$ is prime to $N$, $x$ is a Heegner point of discriminant $D$ dividing $-4N$.

Conversely, if $x$ is such a Heegner point, the ideal $\mathfrak{n}=\bar{\mathfrak{n}}$ is principal in $\mathcal{O}$, and $w(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])=(\mathcal{O}, \bar{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}])=(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$. Hence $x$ is fixed by $w$.

We have the following table of discriminants dividing $-4N$, with the class numbers of the respective orders. These class numbers give the number of fixed points in each orbit for $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

| $N$ | $D$ | $h(D)$ |
|---|---|---|
| 2 | $-4$ | 1 |
| | $-8$ | 1 |
| $N\equiv 3\ (4)$ | $-N$ | $h(-N)$ |
| | $-4N$ | $h(-4N)=\begin{cases} h(-N) & \text{if } N=3 \text{ or } N\equiv 7\ (8) \\ 3h(-N) & \text{if } N\equiv 3\ (8),\ N>3 \end{cases}$ |
| $N\equiv 1\ (4)$ | $-4N$ | $h(-4N)$ |

We wish to distinguish the two orbits of fixed points when $N=2$ or $N\equiv 3\ (4)$. In these cases $m=\gcd(N-1, 12)$ divides 6, and we have the following

PROPOSITION 3.2. *Assume $N=2$ or $N\equiv 3\ (4)$ and $x$ is fixed by $w$. Then*

$$t(x)=\begin{cases} -N^{6/m} & \text{if } \operatorname{disc}(x)=-N \text{ (or } -4 \textit{ when } N=2) \\ +N^{6/m} & \text{if } \operatorname{disc}(x)=-4N. \end{cases}$$

PROOF. Since $x$ is fixed by $w$, we have

$$t(x)^2=t(x)t_N(x)=N^{12/m}$$

by (1.5). Hence $t(x)=\pm N^{6/m}$ takes integral values at each fixed point, so it takes the *same* value at each point in a Galois orbit. It therefore suffices to show $t(x)<0$ for one point $x$ of discriminant $-N$ (or $-4$) and $t(x)>0$ for one point $x'$ of discriminant $-4N$. We will do this for $N\equiv 3\ (4)$, and leave the case when $N=2$ to the reader.

If we take $[\mathfrak{a}]=[\mathcal{O}]$ then $x$ is represented by the point $\tau=1/2+i/(2\sqrt{N})$ in $\mathfrak{H}$, which solves the equation $Nz^2-Nz+(N+1)/4=0$ of discriminant $-N$, and $x'$ is represented by the point $\tau'=i/\sqrt{N}$, which solves the equation $Nz^2+1=0$ of discriminant $-4N$. Hence

$$q=-e^{-\pi/\sqrt{N}}<0$$

$$q'=e^{-2\pi/\sqrt{N}}>0.$$

Since

$$t=q^{(1-N)/m}\prod_{n\geq 1}\left(\frac{1-q^n}{1-q^{nN}}\right)^{24/m}$$

with $(1-N)/m$ odd and $24/m$ even, we see that $\operatorname{sign} t(x)=\operatorname{sign} q$ is negative and $\operatorname{sign} t(x')=\operatorname{sign} q'$ is positive.

## § 4. The modular equation.

The functions $j$ and $j_N$ define a morphism over $\boldsymbol{Q}$

$$\pi : X \longrightarrow Z \subset \boldsymbol{P}^1 \times \boldsymbol{P}^1 \qquad (4.1)$$
$$x \longmapsto (j(x),\ j_N(x))$$

whose image is the correspondence $Z$ defined by the vanishing of the classical modular polynomial of level $N$: $\phi(j, j_N)=0$. The polynomial $\phi(u, v)$ is symmetric, has integral coefficients, and is absolutely irreducible [**1**, pp. 283-284]. More precisely, it has the form

$$\phi(u, v) = u^{N+1}+v^{N+1}-u^N v^N + \sum_{0 \leq m, n \leq N} a_{m,n} u^m v^n . \qquad (4.2)$$

Hence the correspondence $Z$ is symmetric of bidegree $N+1$ and has intersection $2N$ with the diagonal in $\boldsymbol{P}^1 \times \boldsymbol{P}^1$.

Kronecker established two important results on the polynomial $\phi(u, v)$. The first i the famous congruence

$$\phi(u, v) \equiv (u^N - v)(u - v^N) \qquad (\mathrm{mod}\ N) \qquad (4.3)$$

and the second is a factorization of $\phi(u, u)$. Let $D$ be a negative discriminant and define [**6**, § 4]

$$f_{|D|}(x) = \prod_{D=df^2} \prod_{\substack{\tau \in \mathfrak{H}/SL_2(\boldsymbol{Z}) \\ \mathrm{disc}(\tau)=d}} (x - j(\tau))^{1/\mathrm{Aut}(\tau)} . \qquad (4.4)$$

Thus the roots of $f_{|D|}(x)$ are the singular moduli with multiplication by the order of discriminant $D$. Then Kronecker showed that

$$\phi(u, u) = - \prod_{\substack{t \in \boldsymbol{Z} \\ t^2 < 4N}} f_{4N-t^2}(u) . \qquad (4.5)$$

Since $w$ induces the involution $(u, v) \mapsto (v, u)$ of $Z$, its fixed points all lie on the diagonal. By Proposition 3.1, these correspond to the roots of $f_{4N}(x)$ when $N$ is odd and of $f_8(x) f_4(x)^2$ when $N=2$. The other roots of $\phi(u, u)$ in (4.5) all occur with multiplicity 2, and we shall show that they are double points on $Z$. More generally, we have the following description of the singularities of $Z$.

PROPOSITION 4.6. *The correspondence $Z$ is non-singular, except at the image*

$$\pi(\infty) = \pi(0) = (\infty, \infty)$$

*of the two cusps of $X$ and at the images*

$$\pi(x) = \pi(x') = (j(\mathfrak{a}),\ j(\mathfrak{a}\mathfrak{n}^{-1}))$$

*of the pairs of Heegner points $x=(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, $x'=(\mathcal{O}, \bar{\mathfrak{n}}, [\mathfrak{a}])$ where $\mathfrak{n} \neq \bar{\mathfrak{n}}$ but*

$[\mathfrak{n}]=[\bar{\mathfrak{n}}]$ *in* Pic($\mathcal{O}$). *At each singularity* $(u, v)$ *the curve* $Z$ *has an ordinary double point.*

NOTES. 1) The result in 4.6 was obtained by Dwork [**2**, lemma 8.16] using $N$-adic methods. Moreover, Dwork shows that the affine singularities of $Z$ are the canonical liftings, in the sense of Serre and Tate, of the ordinary moduli on the intersection of the two components in characteristic $N$. This result also follows from Proposition 4.6; indeed, each singularity is an integral point $(u, v)$ whose co-ordinates satisfy

$$\left.\begin{array}{l} v \equiv u^N \\ u \equiv v^N \end{array}\right\} \quad (\mathrm{mod}\ NA)$$

where $A$ is the ring of integers in $K(x)$. This congruence follows from (2.2) and the definition of the Artin symbol. Since $\mathfrak{n}\neq\bar{\mathfrak{n}}$, the reduction of $u$ and $v$ are ordinary moduli in the field of $N^2$ elements.

2) The double points of $Z$ which lie on the diagonal are the images of the cusps and those Heegner points $x=(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ where $\mathfrak{n}\neq\bar{\mathfrak{n}}$ and $\mathfrak{n}=(\alpha)$ is principal in $\mathcal{O}$.

3) The function $t$ distinguishes the pairs of points $x\neq x'$ over each double point of $Z$, by the remarks following (2.3). This shows that $t$ is *not* a polynomial in $j$ and $j_N$. The affine ring of $Y$ over $\boldsymbol{Q}$ is equal to the integral closure of the ring $\boldsymbol{Q}[j, j_N]/\phi(j, j_N)$ in its quotient field $\boldsymbol{Q}(X)=\boldsymbol{Q}(j, j_N)$, as $Y$ is the normalization of the affine curve

$$Z^{\mathrm{aff}} = Z-\{(\infty, \infty)\} = \mathrm{Spec}\,\boldsymbol{Q}[j, j_N]/\phi(j, j_N).$$

We now turn to the proof of Proposition 4.6.

PROOF. The covering $\pi: X\to Z$ is generically 1-to-1 and is given by the rule "forget the isogeny $\phi$". Hence $X$ is the normalization of $Z$ and its genus $g$ is given by the formula

$$g = N^2-\sum_{z\in Z}\delta(z),$$

where $N^2$ is the arithmetic genus of $Z$ and $\delta(z)$ is a local term which is positive if and only if $z$ is a singular point on $Z$ [**9**, Ch. IV]. If $z=\pi(x)=\pi(x')$ with $x\neq x'$, we have $\delta(z)\geqq 1$ with equality if and only if $z$ is an ordinary double point.

To prove Proposition 4.6 we will count the number $s$ of pairs of Heegner points which occur therein and will show that

$$g = N^2-s-1. \tag{4.7}$$

Hence $\sum\delta(z)=s+1$, so $\delta(z)=1$ for each obvious singularity and $\delta(z)=0$ at all other points of $Z$.

If $x=(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ is of the type discussed in the proposition, then the ideal $\mathfrak{n}^2=(\alpha)$ is principal and prime to $\bar{\mathfrak{n}}$. Then $N(\alpha)=N^2$ and $\mathrm{Tr}(\alpha)=t$ is prime to $N$; the ring $\mathcal{O}$ contains the order $\boldsymbol{Z}[\alpha]$ of discriminant $t^2-4N^2$. There are $w(d)$ choices for the generator $\alpha$, which all give the same ideal $\mathfrak{n}$, and $h(d)$ choices for $[\mathfrak{a}]$ once the pair $(\mathcal{O}, \mathfrak{n})$ has been fixed. Hence

$$s=\sum_{\substack{|t|\in \boldsymbol{Z}\\ t\leq 2N\\ (t,N)=1}}\sum_{t^2-4N^2=df^2}\frac{h(d)}{w(d)}=\frac{1}{2}\sum_{\substack{|t|\in \boldsymbol{Z}\\ t\leq 2N\\ (t,N)=1}}H(4N^2-t^2)$$

where $H(|D|)$ is the Hurwitz class number.

But Kronecker established the class number relation

$$\sum_{\substack{t\in \boldsymbol{Z}\\ t^2\leq 4n}}H(4n-t^2)=\sum_{\substack{n=dd'\\ d>0}}\max(d, d')$$

with $H(0)=-1/12=\zeta_{\boldsymbol{Q}}(-1)$. Taking $n=N^2$ and separating out the terms $t$ with $t\equiv 0 \pmod N$, we find

$$s=N^2+\frac{N}{2}-\frac{H(4N^2)}{2}-H(3N^2)-H(0).$$

Hence

$$N^2-s-1=\frac{N-13}{12}+\frac{\left(1-\left(\frac{-4}{N}\right)\right)}{4}+\frac{\left(1-\left(\frac{-3}{N}\right)\right)}{3}.$$

But the right hand side is equal to the genus $g$ of $X$ (one can show this by considering the ramification in the covering $X_0(N)\underset{j}{\to}X_0(1)\cong \boldsymbol{P}^1$ and using Hurwitz's formula), so we have established (4.7).

## § 5. A fibre system of elliptic curves.

In this section we will assume that $N\equiv 3 \pmod 4$ and $N>3$. We will define a fibre system $E$ of elliptic curves over $X=X_0(N)$, with degenerations at the cusps and Heegner points of discriminant $-3$. We will show that the complex points of $E$ can be identified with a certain elliptic modular surface defined by Shioda, which answers a question posed in [8, pp. 57-58].

Recall the classical modular forms of level 1:

$$c_4=1+240\sum_{n\geq 1}\sigma_3(n)q^n$$

$$c_6=-1+504\sum_{n\geq 1}\sigma_5(n)q^n$$

$$\Delta=\eta^{24}=q\prod_{n\geq 1}(1-q^n)^{24}.$$

These have weights 4, 6, and 12 respectively and satisfy $c_4^3-c_6^2=1728\Delta$. Define the meromorphic function $e=e(\tau)$ on $\mathfrak{H}$ by the following expression, where $\eta\circ N(\tau)=\eta(N\tau)$:

$$(5.1)\qquad \begin{cases} N\equiv 7\ (24) & e=\eta\cdot\eta\circ N/j^{2/3}=\eta^{17}\cdot\eta\circ N/c_4^2 \\ N\equiv 11\ (24) & e=\eta\cdot\eta\circ N/(j-1728)^{1/2}=\eta^{13}\cdot\eta\circ N/c_6 \\ N\equiv 19\ (24) & e=\eta\cdot\eta\circ N/j^{2/3}(j-1728)^{1/2}=\eta^{29}\cdot\eta\circ N/c_4^2c_6 \\ N\equiv 23\ (24) & e=\eta\cdot\eta\circ N. \end{cases}$$

Then $e(\gamma\tau)=(c\tau+d)e(\tau)$ for all elements $\gamma$ in the subgroup

$$(5.2)\qquad \Gamma_0'(N)=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in SL_2(\boldsymbol{Z}) : c\equiv 0\ (N),\ \left(\frac{d}{N}\right)=+1\right\}.$$

Hence $e(\tau)^2$ is a meromorphic form of weight 2 for the group $\Gamma_0(N)=\Gamma_0'(N)\times\langle\pm 1\rangle$.

We define modular functions on $X_0(N)$ over $\boldsymbol{Q}$ by taking

$$(5.3)\qquad \begin{cases} f_4=c_4/e^4 \\ f_6=c_6/e^6 \\ f_{12}=\Delta/e^{12}=\sqrt{\dfrac{\Delta(\tau)}{\Delta(N\tau)}}\cdot\begin{cases} j(\tau)^8 \\ (j(\tau)-1728)^6 \\ j(\tau)^8(j(\tau)-1728)^6 \\ 1 \end{cases} \begin{matrix} N\equiv 7 \\ N\equiv 11 \\ N\equiv 19 \\ N\equiv 23 \end{matrix}\Bigg\}\ (\mathrm{mod}\ 24)\,. \end{cases}$$

Then $f_4, f_6$, and $f_{12}$ lie in $R=H^0(Y, \mathcal{O}_Y)$, and $f_{12}$ is a unit once the points with $j=0$ or $j=1728$ have been removed.

We define a cubic curve $E$ over $R$ by the (non-homogeneous) equation

$$(5.4)\qquad E : v^2=u^3-\frac{f_4}{2^4 3}u-\frac{f_6}{2^5 3^3}.$$

This has the invariant differential $\omega=du/2v$ with invariants

$$\begin{aligned} c_4(E,\omega)&=f_4 \\ c_6(E,\omega)&=f_6 \\ \Delta(E,\omega)&=f_{12} \\ j(E)&=j\,. \end{aligned}$$

Hence $E$ defines a fibre system of elliptic curves over $Y$, once the appropriate points in the base where $j=0$, 1728 and $f_{12}$ is not invertible have been removed. Our first task will be to see at which of these points $E$ has good reduction.

LEMMA 5.5. 1) *If* $N\equiv 11\ (12)$ *then* $E$ *has good reduction at all points of* $Y$.

2) *If* $N\equiv 7\ (12)$ *then* $E$ *has good reduction at all points of* $Y$ *except the two Heegner points of discriminant* $-3$. *At these points,* $E$ *has bad reduction of type* IV*.

PROOF. 1) If $N\equiv 23\,(24)$ there is nothing to prove, as $f_{12}$ is a unit in $R$ and $\omega$ is a Néron differential over $Y$. If $N\equiv 11\,(24)$, we must show $E$ has good reduction at each of the $(N+1)/2$ points $x$ where $j=1728$. The key point is that $\mathrm{ord}_x(j-1728)=2$. If $\pi$ is a uniformizing parameter in the local ring $R_x$ at $x$, then the differential $\omega'=\pi\omega$ has invariants

$$\begin{aligned} c_4(E,\omega') &= c_4(j-1728)^2/\eta^4\cdot\eta\circ N^4\cdot\pi^4 \\ c_6(E,\omega') &= c_6(j-1728)^3/\eta^6\cdot\eta\circ N^6\cdot\pi^6 \\ \Delta(E,\omega') &= t(j-1728)^6/\pi^{12} \end{aligned}$$

in $R_x$, with $\Delta(E,\omega')$ in $R_x^*$. Hence $E$ has good reduction at $x$.

2) If $N\equiv 7\,(24)$ we must show $E$ has good reduction at each of the $(N-1)/3$ points $x$ where $j=0$ which are not Heegner points of discriminant $-3$ $(j_N(x)\neq 0)$. The key point is that $\mathrm{ord}_x(j)=3$. If $\pi$ is a uniformizing parameter in the local ring $R_x$, then the differential $\omega'=\pi^2\omega$ has invariants

$$\begin{aligned} c_4(E,\omega') &= c_4 j^{8/3}/\eta^4\cdot\eta\circ N^4\cdot\pi^8 \\ c_6(E,\omega') &= c_6 j^4/\eta^6\cdot\eta\circ N^6\cdot\pi^{12} \\ \Delta(E,\omega') &= t^3 j^8/\pi^{24} \end{aligned}$$

in $R_x$, with $\Delta(E,\omega')\in R_x^*$. Hence $E$ has good reduction at $x$. When $N\equiv 19\,(24)$ this argument handles the points where $j=0$ and $j_N\neq 0$, and the argument of 1) handles the points where $j=1728$.

At the points $x$ where $j=j_N=0$, which are Heegner points of discriminant $-3$, the function $j$ has a simple zero and $\mathrm{ord}_x(\Delta(E,\omega))=8$. Hence $E$ has potentially good reduction of type IV*.

The equation (5.4) defines an elliptic curve over the field $\boldsymbol{Q}(X)$. We have discussed the reduction of $E$ at the affine places of this field; at the two cusps we have the following;

LEMMA 5.6. *$E$ has bad reduction at $\infty$ of type $\mathrm{I}_1$ and bad reduction at $0$ of type $\mathrm{I}_N$. The reduction at $\infty$ is split over $\boldsymbol{Q}$, and at $0$ it is split by the quadratic extension $\boldsymbol{Q}(\sqrt{-N})$.*

PROOF. Let $q=e^{2\pi i\tau}$ be the standard uniformizing parameter at $\infty$, and write $e(\tau)=\pm q^a+\cdots$ with $a\geqq 1$. The differential $\omega'=\omega/q^a$ has invariants

$$\begin{aligned} c_4(E,\omega') &= q^{4a}f_4 = 1+\cdots \\ c_6(E,\omega') &= q^{6a}f_6 = -1+\cdots \\ \Delta(E,\omega') &= q^{12a}f_{12} = q+\cdots \\ j(E) = j &= \frac{1}{q}+\cdots. \end{aligned}$$

Hence the reduction is of type $\mathrm{I}_1$ at $\infty$, split over $\boldsymbol{Q}$.

To study the reduction at 0, we conjugate the curve $E$ by the involution $w$ of $X$ and study the reduction at $\infty$. By (1.4) and (5.1) we have

$$\frac{e(-1/N\tau)}{\tau}=(\sqrt{-N})^a(q^b+\cdots)$$

with $a\equiv 1 \pmod 4$ and $b\geqq 1$. Let $\omega_1$ be the conjugate differential on $E_1=w(E)$ with invariants $(f_4)_N$, $(f_6)_N$, and $(f_{12})_N$ and put $\omega_1'=\omega_1/q^b$. We find

$$c_4(E_1, \omega_1')=(\sqrt{-N})^{4a}+\cdots$$
$$c_6(E_1, \omega_1')=-(\sqrt{-N})^{6a}+\cdots$$
$$\Delta(E_1, \omega_1')=(\sqrt{-N})^{12a}q^N+\cdots$$
$$j(E_1)=j_N=\frac{1}{q^N}+\cdots.$$

Hence the reduction is of type $\mathrm{I}_N$, split by $\boldsymbol{Q}(\sqrt{-N})$.

If $\Gamma\subset SL_2(\boldsymbol{Z})$ is a subgroup of finite index which does not contain $\langle\pm 1\rangle$, Shioda [8] has defined an elliptic modular surface $B_\Gamma$ over the complex curve $\mathfrak{H}^*/\Gamma$. $B_\Gamma$ is the minimal regular compactification of the complex elliptic surface:

$$\boldsymbol{C}\times\mathfrak{H}^0/\boldsymbol{Z}^2\rtimes\Gamma \longrightarrow \mathfrak{H}^0/\Gamma$$

where $\mathfrak{H}^0$ is the upper half-plane minus the $\Gamma$-orbits of elliptic points.

Let $B$ denote the minimal regular model for $E$ over $X=X_0(N)$.

PROPOSITION 5.7. *The complex elliptic surface $B(\boldsymbol{C})\to X(\boldsymbol{C})$ is analytically isomorphic to Shioda's modular surface $B_\Gamma\to\mathfrak{H}^*/\Gamma$ where $\Gamma=\Gamma_0'(N)$.*

PROOF. We will give an analytic isomorphism over the open curve where $j\neq 0$, 1728, $\infty$. The result then follows from the uniqueness of a minimal regular model.

The isomorphism is given by mapping $(z, \tau)\in\boldsymbol{C}\times\mathfrak{H}$ to the co-ordinates $(u, v)$ of $E$, with

$$u=\frac{\wp(z, \tau)}{(2\pi i e(\tau))^2}$$
$$2v=\frac{\wp'(z, \tau)}{(2\pi i e(\tau))^3}$$
$$\omega=\frac{du}{2v}=2\pi i e(\tau)dz.$$

Here $\wp$ and $\wp'$ are the functions of Weierstrass:

$$\wp(z, \tau) = z^{-2} + \sum_{\substack{\alpha \in \boldsymbol{Z}+\boldsymbol{Z}\tau \\ \alpha \neq 0}} \{(z+\alpha)^{-2} - \alpha^{-2}\}$$

$$\wp'(z, \tau) = -2 \sum_{\alpha \in \boldsymbol{Z}+\boldsymbol{Z}\tau} (z+\alpha)^{-3}.$$

Since $\wp$ is a meromorphic Jacobi form of weight 2 and index 0:

$$\wp\left(\frac{z}{c\tau+d}, \frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 \wp(z, \tau) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z})$$

$$\wp(z+\lambda\tau+\mu, \tau) = \wp(z, \tau) \qquad (\lambda, \mu) \in \boldsymbol{Z}^2$$

we see the map factors through the quotient $B_\Gamma$, and gives an analytic isomorphism.

As an added dividend of the proof of (5.7), we see that the integral period lattice of the curve $(E_x, \omega_x)$ at a point $x$ in $Y$ is given by:

(5.8) $$L(\omega_x) = 2\pi i e(\tau)(\boldsymbol{Z}+\boldsymbol{Z}\tau).$$

## § 6. A rational $N$-isogeny and the representable moduli problem.

We retain the notion of the previous section. In particular, $N \equiv 3\,(4)$ and $E$ is the elliptic curve over the affine curve obtained by removing the Heegner points of discriminant $-3$ from $Y = Y_0(N)$. (We will be a little sloppy below and refer to $E$ as an elliptic curve over $Y$, which is correct only when $N \equiv 11\,(12)$). We let $B$ denote the minimal regular model for $E$ over the complete curve $X = X_0(N)$.

Define the elliptic curve $F$ over $Y$ by first conjugating $E$ by the involution $w$ of the base then twisting by the quadratic extension $Y(\sqrt{-N})$. Let $\omega'$ be the conjugate differential on $E' = w(E)$ and $\nu$ the differential on $F$ which corresponds to $\omega'/\sqrt{-N}$. We then have

$$c_4(F, \nu) = N^2 (f_4)_N$$
$$c_6(F, \nu) = -N^3 (f_6)_N$$
$$\Delta(F, \nu) = N^6 (f_{12})_N$$
$$j(F) = j_N.$$

PROPOSITION 6.1. *There is a unique $N$-isogeny $\phi: E \to F$ over $Y$ such that $\phi^*(\nu) = \omega$.*

PROOF. An analysis similar to the proof of (5.7) shows that the lattice of $(F_x, \nu_x)$ at a point $x$ is given by

$$L(\nu_x) = 2\pi i e(\tau)(\boldsymbol{Z}(1/N)+\boldsymbol{Z}\tau) = \frac{2\pi i e(\tau)}{N}(\boldsymbol{Z}+\boldsymbol{Z}N\tau).$$

Since this contains $L(\omega_x)$ with index $N$, we obtain an analytic isogeny $\phi: E(\boldsymbol{C})\to F(\boldsymbol{C})$ over $Y(\boldsymbol{C})$ with the desired properties. This extends to the minimal regular compactifications over $X(\boldsymbol{C})$, and is algebraic. To show $\phi$ is rational over $\boldsymbol{Q}$, we let $\sigma$ be any automorphism of $\boldsymbol{C}$. Then

$$\omega = \omega^\sigma = \phi^*(\nu)^\sigma = (\phi^\sigma)^*(\nu^\sigma) = (\phi^\sigma)^*(\nu).$$

Hence $\phi-\phi^\sigma$ acts trivially on the cotangent space of $F$, so $\phi=\phi^\sigma$.

Let $\phi^\vee: F\to E$ be the dual isogeny over $Y$, and let $Y[\ker\phi^\vee]$ be the étale abelian extension obtained by adjoining the co-ordinates of any point in the kernel of $\phi^\vee$. Let $Y_1=Y_1(N)$ be the affine curve which classifies elliptic curves together with a point of order $N$ over $\boldsymbol{Q}$; then there is a natural covering map

$$\pi : Y_1 \longrightarrow Y$$

which is abelian of degree $(N-1)/2$ with Galois group $(\boldsymbol{Z}/N)^*/\pm 1\simeq(\boldsymbol{Z}/N)^{*2}$, and étale away from the Heegner points of discriminant $-3$. Our main result in this section is the following.

PROPOSITION 6.2. *The covering* $Y[\ker\phi^\vee]$ *has degree* $(N-1)/2$ *and is isomorphic to* $Y_1$. *The representation of the Galois group of* $Y[\ker\phi^\vee]/Y$ *in* $(\boldsymbol{Z}/N)^*=\mathrm{Aut}(\ker\phi^\vee)$ *has image equal to* $(\boldsymbol{Z}/N)^{*2}$.

PROOF. It is clear that $Y[\ker\phi^\vee]$ contains $Y_1$; so it suffices to verify that the co-ordinates of a point in $\ker\phi^\vee$ are in the ring of modular functions for $\Gamma_1(N)$ with rational Fourier coefficients.

Since $NL(\nu_x)=2\pi i e(\tau)(\boldsymbol{Z}+\boldsymbol{Z}N\tau)$ is contained with index $N$ in $L(\omega_x)$, we find that co-ordinates for the point $2\pi i e(\tau)\cdot\tau \bmod NL(\nu_x)$ in the kernel of the dual isogeny are given by

$$u = \frac{\wp(\tau, N\tau)}{(2\pi i e(\tau))^2}, \qquad v = \frac{\wp'(\tau, N\tau)}{2\cdot(2\pi i e(\tau))^3}.$$

A simple calculation shows that the functions $f(\tau)=\wp(\tau, N\tau)/(2\pi i)^2$ and $g(\tau)=\wp'(\tau, N\tau)/(2\cdot(2\pi i)^3)$ are modular forms of weight 2 and 3 for

$$\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} : c\equiv 0\,(N),\ a\equiv d\equiv 1\,(N)\right\}$$

which have rational Fourier coefficients in terms of the parameter $q=e^{2\pi i\tau}=e^{2\pi i N\tau/N}$ at $\infty$. Since the same is true for $e^2$ and $e^3$, $u$ and $v$ are elements of the rational function field of $X_1(N)$ over $\boldsymbol{Q}$, which are regular for $\tau$ with $j(\tau)\neq 0$, 1728, $\infty$.

The representation has image in $(\boldsymbol{Z}/N)^{*2}$, as this is the unique subgroup of index 2 and order $(N-1)/2$ in $(\boldsymbol{Z}/N)^*$.

COROLLARY 6.3. *The covering* $Y[\ker\phi]$ *has degree* $N-1$ *and is isomorphic to* $Y_1(\sqrt{-N})$.

If $A$ is a $\boldsymbol{Q}$-algebra, then the fibre $E_a \xrightarrow{\phi_a} F_a$ of our family over each point $a\in Y(A)$ defines an $N$-isogeny between elliptic curves over $A$ such that $\ker\check{\phi}_a$ trivializes over an étale extension of degree dividing $(N-1)/2$ of each geometric component. In fact, the family

$$\begin{array}{ccc} E & \xrightarrow{\ \phi\ } & F \\ & {\scriptstyle\pi}\searrow \quad \swarrow & \\ & Y & \end{array}$$

represents this (rigid) functor on $\boldsymbol{Q}$-algebras: any isogeny of degree $N$ with this property arises as one of the fibres of this family (away from the Heegner points of discriminant $-3$).

Let $\underline{\omega}=\pi_*\Omega^1_{E/Y}$; then $e$ is a meromorphic section of $\underline{\omega}$ with poles only when $j=0$, 1728. When $N\equiv 23\,(24)$, $e$ is regular and non-zero, so gives a trivialization of the line bundle $\underline{\omega}$ over $Y$.

We now have enough information to identify the fibres of the family $E\to Y$ over the fixed points $x$ of $w$ which have discriminant $-N$. Recall from Proposition 3.2 that at each such point we have

$$t(x) = -N^{6/m}$$

where $m=2$ if $N\equiv 2\,(3)$ and $m=6$ if $N\equiv 1\,(3)$.

LEMMA 6.4 (Rumely [7]). *If* $x\in Y$ *has complex multiplication by* $K$, *then the torsion points of* $E_x$ *are rational over* $K^{\mathrm{ab}}$.

PROOF. The condition that $x$ has complex multiplication by $K$ is just that $\tau\in K\cap\mathfrak{H}$. Then the torsion points of $E$ are given by the values of arithmetic automorphic functions at $\tau$, by (5.7). Shimura's reciprocity law guarantees that these values lie in $K^{\mathrm{ab}}$.

LEMMA 6.5. *If* $x$ *is fixed by* $w$ *and has discriminant* $-N$, *then* $E_x$ *is a* $\boldsymbol{Q}$*-curve and* $\boldsymbol{Q}(x, \ker\check{\phi}_x)$ *has degree* $(N-1)/2$ *over* $\boldsymbol{Q}(x)=\boldsymbol{Q}(j(E_x))$.

PROOF. By lemma 6.4, $E_x$ is a $K=\boldsymbol{Q}(\sqrt{-N})$-curve; since $\boldsymbol{Q}(x)$ has degree $h$ over $\boldsymbol{Q}$ by the results in § 3, $E_x$ is defined over the field of its modulus and is a $\boldsymbol{Q}$-curve. The same is true for $F_x$, which is isogenous to $E_x$ over $\boldsymbol{Q}(x)$.

In [4, 14.1.2] we determined the structure of the Galois representation on the $N$-torsion in the rational $N$-isogeny for all $\boldsymbol{Q}$-curves. The character always has order divisible by $(N-1)/2$, so is equal to a character of order $(N-1)/2$ in this case.

Recall that $E(N)$ is the unique $\boldsymbol{Q}$-curve with good reduction outside $N$ and minimal discriminant $(-N^3)$ over $\boldsymbol{Q}(x)$. The representation on its $N$-torsion is given by $\omega_N^{(3N-1)/4}$, where $\omega_N$ is the character giving the Galois action on $N^{\text{th}}$ roots of unity.

PROPOSITION 6.6. 1) *If* $N\equiv 7\,(8)$ *then* $E_x\cong E(N)$ *and* $F_x\cong E(N)^{\sqrt{-N}}$.
2) *If* $N\equiv 3\,(8)$ *then* $E_x\cong E(N)^{\sqrt{-N}}$ *and* $F_x\cong E(N)$.

PROOF. The unique $\boldsymbol{Q}$-curve whose $N$-torsion representation has order $(N-1)/2$ is equal to

$$\begin{cases} E(N)^{\sqrt{-N}} & \text{if } N\equiv 7\,(8) \\ E(N) & \text{if } N\equiv 3\,(8). \end{cases}$$

In particular, $E_x$ always has good reduction at the places of $\boldsymbol{Q}(x)$ not dividing $N$. In the next section we will see this is true for the fibre $E_x$ over a point of $Y$ where $j(x)$ is an algebraic integer.

## § 7. Integral models.

Assume first that $N$ is an arbitrary prime. Let $\underline{S}$ be the ring $\boldsymbol{Z}[j, j_N]/\phi(j, j_N)$ and let $\underline{R}$ be the integral closure of $\underline{S}$ in its quotient field $\boldsymbol{Q}(X)$. We obtain models for $Z^{\text{aff}}$ and $Y$ over $\boldsymbol{Z}$ by taking the affine schemes:

$$\underline{Z}^{\text{aff}} = \operatorname{Spec}(\underline{S}), \qquad \underline{Y} = \operatorname{Spec}(\underline{R}). \tag{7.1}$$

The arithmetic surface $\underline{Y}$ is normal, and is known to be regular outside the supersingular points in characteristic $N$ where $j=0, 1728$ [**1**, p. 284]. The arguments of § 4 can be extended to show that $\underline{Y}[1/N]$ is smooth over $\boldsymbol{Z}[1/N]$.

A modular function $f$ for $\Gamma_0(N)$ lies in $\underline{R}$ if and only if $f$ is regular on $\mathfrak{H}$ and the Fourier coefficients of $f$ at both cusps are integers. Thus $f=\sum a_n q^n$ and $f_N=\sum b_n q^n$ have integral Fourier expansions at $\infty$. The elements $t$ and $t_N$ lie in $\underline{R}$, and are units in $\underline{R}[1/N]$.

When $N-1$ divides 12, so $X$ has genus 0, we have

$$\underline{R} = \boldsymbol{Z}[t, t_N]/(tt_N = N^{12/(N-1)}). \tag{7.2}$$

This ring is regular when $N=13$; otherwise there is a singularity of type $A_{k-1}$ (with $k=12/(N-1)$) at the unique supersingular point $t=t_N=0$ in characteristic $N$. Fricke [**3**, Ch. 9] gives formulae for $j$ and $j_N$ as polynomials in $t$ and $t_N$; for example

$$(7.3) \qquad \begin{cases} N=2 & j=t+2^8\cdot 3+2^4\cdot 3t_2+t_2^2 \\ N=3 & j=t+2^2\cdot 3^3\cdot 7+2\cdot 3^3\cdot 5t_3+2^2\cdot 3^2t_3^2+t_3^3. \end{cases}$$

Now assume $N\equiv 3 \pmod 4$ and $N>3$. We will extend the fibre system $E\to Y$ to a system of elliptic curves $\underline{E}$ over $\underline{Y}[1/N]$. We will also discuss the reduction of $\underline{E}$ at the two primes dividing $N$ in $\underline{R}$, corresponding to the two irreducible components $Z_\infty$ and $Z_0$ in $\underline{Y}\otimes\boldsymbol{Z}/N$. These components are indexed by the cusps they contain; the ordinary points on $Z_\infty$ correspond to elliptic curves with multiplicative subgroups of order $N$. We label the prime ideals with residue rings the affine rings of $Z_\infty$ and $Z_0$ by $N_\infty$ and $N_0$ respectively; then $\underline{R}/N_\infty\simeq\boldsymbol{Z}/N[j]$ and $\underline{R}/N_0\simeq\boldsymbol{Z}/N[j_N]$.

PROPOSITION 7.4. *The curves $\underline{E}$ and $\underline{F}$ have good reduction over $\underline{Y}[1/N]$ and $\underline{\phi}:\underline{E}\to\underline{F}$ extends to an N-isogeny over this base. The kernel of $\phi^\vee$ is an étale group scheme which splits over the extension $\underline{Y}_1[1/N]$ of degree* $(N-1)/2$.

As for the reduction at $N$, we will prove the following.

PROPOSITION 7.5. *The curve $\underline{E}$ has good reduction* $(\mathrm{mod}\, N_\infty)$ *and the reduction of* $(\underline{E}, \omega)$ *over $\underline{R}/N_\infty$ has invariants*

$$\begin{aligned} c_4 &\equiv j^a(j-1728)^{a'}f_{ss}(j)^2 \\ c_6 &\equiv -j^b(j-1728)^{b'}f_{ss}(j)^3 \\ \Delta &\equiv j^c(j-1728)^{c'}f_{ss}(j)^6 \\ j &\equiv j, \end{aligned}$$

*where $f_{ss}(j)$ is the monic supersingular polynomial* $(\mathrm{mod}\, N)$ *with the possible factor $(j)(j-1728)$ removed and the exponents $a$, $a'$, $b$, $b'$ and $c$, $c'$ are given by the following table.*

| $N$ | $a$ | $a'$ | $b$ | $b'$ | $c$ | $c'$ |
|---|---|---|---|---|---|---|
| $\equiv 7\ (24)$ | 3 | 1 | 4 | 2 | 8 | 3 |
| $\equiv 11\ (24)$ | 1 | 3 | 1 | 5 | 2 | 9 |
| $\equiv 19\ (24)$ | 3 | 3 | 4 | 5 | 8 | 9 |
| $\equiv 23\ (24)$ | 1 | 1 | 1 | 2 | 2 | 3 |

NOTE. The reduction of $\underline{E}$ has modular interpretation over the ordinary points of the component $Z_\infty$. It represents ordinary curves in characteristic $N$ such that the kernel of $(\mathrm{Fr})^\vee=(\mathrm{Ver})$ splits over an extension of degree dividing $(N-1)/2$, or equivalently with Hasse invariant a square. The number of points of such a curve over a finite field $\boldsymbol{F}_q$ has the form $1+q-a$, where $\left(\frac{a}{N}\right)=+1$.

We now turn to the proofs of Propositions 7.4 and 7.5, in the simplest case when $N\equiv 23\,(24)$. In that case, $f_4$, $f_6$ and $f_{12}=t$ lie in $\underline{R}$ and $f_{12}$ is a unit in $\underline{R}[1/N]$. Hence equation (5.4) defines an elliptic curve over $\underline{E}$ over $\underline{Y}[1/6N]$. The curve $\underline{F}$ is also defined over this base.

LEMMA 7.6. *The curves $\underline{E}$ and $\underline{F}$ have good reduction at the prime ideals $2\underline{R}$ and $3\underline{R}$.*

PROOF. We first claim there are functions $f_2\in\underline{R}/3\underline{R}$ and $f_1\in\underline{R}/2\underline{R}$ such that

$$\begin{cases} f_2^2\equiv f_4 & \bmod 3 \\ f_2^3\equiv -f_6 & \bmod 3^2, \end{cases}$$

$$\begin{cases} f_1^4\equiv f_4 & \bmod 2^3 \\ f_1^6\equiv -f_6 & \bmod 2^2. \end{cases}$$

To define $f_2$ and $f_1$ we recall the modular forms $b_2\,(\bmod 3)$ and $a_1\,(\bmod 2)$ which have weights 2 and 1 and put

$$f_2=b_2/e^2,\qquad f_1=a_1/e.$$

Since $b_2^2\equiv c_4\,(\bmod 3)$, $b_2^3\equiv -c_6\,(\bmod 3^2)$, $a_1^4\equiv c_4\,(\bmod 2^3)$ and $a_1^6\equiv -c_6\,(\bmod 2^2)$, these functions have the desired properties.

To discuss the reduction of $\underline{E}$ $(\bmod 3\underline{R})$, we change co-ordinates in (5.4) by taking $u=w+(f_2/3)$. Then

$$v^2=w^3+f_2w^2+\left(\frac{2^4f_2^2-f_4}{2^43}\right)w+\left(\frac{2^5f_2^3-2\cdot 3f_2f_4-f_6}{2^53^3}\right)$$

is an equation with coefficients in $\underline{R}[1/2]$ with discriminant $t\in\underline{R}[1/N]^*$. To see that the coefficients are integral at 3, we use the previous congruences for $f_2$:

$$2^4f_2^2-f_4\equiv f_2^2-f_4\equiv 0 \qquad \bmod 3\underline{R}$$

$$2^5f_2^3-2\cdot 3f_2f_4-f_6\equiv 5f_2^3-6f_2^3-f_6\equiv 0 \qquad \bmod 9\underline{R}.$$

Thus the coefficient of $w$ lies in $\underline{R}[1/2]$ and the constant coefficient lies in $\frac{1}{3}\underline{R}[1/2]$. If this coefficient does not lie in $\underline{R}[1/2]$, the reduction is of type II* at $3\underline{R}$ and the conductor $f=4$. But this is impossible, as $\underline{E}$ achieves good reduction once the points in $\ker\phi$ are rational, and this occurs over an extension of degree $N-1$. Since $N\equiv 2\,(3)$ this extension cannot be wildly ramified at $\underline{3}$, so the original reduction can not have conductor $f>2$. Hence $\underline{E}$, and the $N$-isogenous curve $\underline{F}$, have good reduction at $3\underline{R}$.

To discuss the reduction at $2\underline{R}$, we change co-ordinates in (5.4) by $v=v'+\frac{f_1}{2}u'$, $u=u'+\frac{f_1^2}{12}$. Then

$$(v')^2+f_1u'v'=(u')^3+\Big(\frac{-f_4}{2^4 3}+\frac{f_1^4}{2^4 3}\Big)u'+\Big(\frac{-f_6}{2^5 3^3}+\frac{f_1^2}{2^2 3}\Big(\frac{-f_4}{2^4 3}\Big)+\frac{f_1^6}{2^6 3^3}\Big)$$

is an equation with coefficients in $\underline{R}[1/3]$ and discriminant $t\in\underline{R}[1/N]^*$. To see that the coefficients are integral at 2, we use the previous congruences for $f_1$:

$$\begin{aligned} -f_4+f_1^4 &\equiv 0 \qquad (\mathrm{mod}\ 2^3)\\ -2f_6-3f_1^2f_4+f_1^6 &= -2f_6+f_1^2(f_1^4-3f_4)\\ &= -2(f_6+f_1^2f_4+4g) \qquad g\in\underline{R}\\ &\equiv 0 \qquad (\mathrm{mod}\ 2^3). \end{aligned}$$

Hence the coefficient of $u'$ lies in $\frac{1}{2\cdot 3}\underline{R}$ and the constant coefficient lies in $\frac{1}{2^3\cdot 3^3}\underline{R}$. If these coefficients are not 2-integral, the reduction of $\underline{E}$ has type $\mathrm{I}_0^*$, $\mathrm{III}^*$, or $\mathrm{II}^*$ at the prime $2\underline{R}$ and conductor $f=8$, 5, or 4. But this is impossible, as $F$ and hence the isogenous curve $E$ achieve good reduction over the extension splitting $\ker\phi^\vee$, which has degree $(N-1)/2$. Since $N\equiv 3\,(4)$, this extension cannot be wildly ramified at $\underline{2}$, so the original reduction cannot have conductor $f>2$. Hence $\underline{E}$ and the $N$-isogenous $\underline{F}$ have good reduction at $2\underline{R}$.

This completes the proof of (7.4), as $\phi$ is an isogeny of degree $N$, which is invertible on $Y[1/N]$. Hence $\ker\phi^\vee$ is étale; since it is split by $Y_1$ over $Y$, it is split by the normal extension $\underline{Y}_1[1/N]$ of $\underline{Y}[1/N]$. Proposition 7.5 follows almost immediately from the congruence (which holds for all primes $N$):

(7.7) $$u\equiv\prod_{E_i}\{j-j(E_i)\}^{24/e_i} \qquad (\mathrm{mod}\ N_\infty)$$

where $u=\Delta(\tau)/\Delta(N\tau)$ is the modular unit, the product is taken over all supersingular elliptic curves in characteristic $N$, and $e_i=|\mathrm{Aut}(E_i)|$. We leave the details to the reader.

We end with some remarks on the rank of the elliptic curve $\underline{E}$ at various fibres of $\underline{Y}[1/N_0]$. The Mordell-Weil group of $E$ over $Y=\underline{Y}\otimes\boldsymbol{Q}$ is trivial; this follows from a calculation of $h^{1,1}$ for the complex elliptic surface $B(\boldsymbol{C})$ over $X(\boldsymbol{C})$ and a consideration of the degenerate fibres, as in Shioda [8]. One can also show, by analytic methods, that $h^{2,0}$ for this surface is equal to the dimension $d$ of the space of cusp forms of weight 3 for $\Gamma_0'(N)$. In fact

(7.8)
$$d=\begin{cases}\dfrac{N-1}{6} & N\equiv 7\,(12)\\ \dfrac{N-5}{6} & N\equiv 11\,(12),\end{cases}$$

and the subspace of forms with complex multiplication, which has dimension $h(-N)$, was studied extensively by Hecke. If $k$ is an algebraically closed field of characteristic $l\neq 0$, $N$ then the rank of $\underline{E}$ over the base $\underline{Y}\otimes k$ is bounded above by $2d$; when $\left(\frac{l}{N}\right)=-1$ the Tate conjectures suggest that it should be bounded below by $2h(-N)$. Finally, let $\boldsymbol{F}$ be the finite field with $N^2$ elements; then the Tate conjectures suggest that the rank of $\underline{E}$ over the base $\underline{Y}[1/N_0]\otimes\boldsymbol{F}$ should be bounded below by $h(-N)$.

## Bibliography


[1] P. Deligne and M. Rapoport, Les schémas de modules des courbes elliptiques, Proceedings on Modular Functions (1972), Vol. II, Lecture Notes in Math., **349**, Springer, 1973, pp. 143-316.
[2] B. Dwork, $P$-adic cycles, Publ. Math. I. H. E. S., **37** (1969), 27-115.
[3] R. Fricke, Die Elliptischen Funktionen und Ihre Anwendungen, Zweiter Teil, Teubner, Berlin, 1922.
[4] B. Gross, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Math., **776**, Springer, 1980.
[5] B. Gross, Heegner points on $X_0(N)$, Modular Forms (ed. R. A. Rankin), Ellis Horwood, 1984, pp. 87-106.
[6] B. Gross and D. Zagier, On singular moduli, J. Reine Angew. Math., **355** (1985), 191-220.
[7] R. Rumely, A formula for the Grössencharacter of a parametrized elliptic curve, J. Number Theory, **17** (1983), 389-402.
[8] T. Shioda, On elliptic modular surfaces, J. Math. Soc. Japan, **24** (1972), 20-59.
[9] J.-P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959.



Benedict H. Gross
Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138
U. S. A.