Math. Ann. 271, 269–304 (1985)

Mathematische Annalen

On the Picard-Fuchs Equation and the Formal Brauer Group of Certain Elliptic *K*3-Surfaces

Jan Stienstra[1] and Frits Beukers[2]

1 Department of Mathematics, University of Utrecht, Budapestlaan 6, NL-3508 TA Utrecht, The Netherlands
2 Department of Mathematics, University of Leiden, Wassenaarse Weg 80, NL-2333 AL Leiden, The Netherlands

Introduction

In this paper we study some 1-parameter commutative formal group laws connected with a Weierstrass equation

$$(W) \qquad Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

with coefficients $a_i=a_i(t)$ in the polynomial ring $\mathbb{Z}[t]$ and having non-constant discriminant $\Delta=\Delta(t)$ and j-invariant $J=J(t)$ [29].

First we treat (W) as a family of (complex) elliptic curves. The periods of the elliptic curve varying in this family satisfy a second order linear differential equation: the Picard-Fuchs equation of (W) [18, 22]. We prove that the condition

(0.1) *Eq.* (W) *reduces modulo* t *to* $Y^2Z+XYZ=X^3$,

implies that the Picard-Fuchs equation admits locally about $t=0$ a unique solution $f(t)=\sum f_nt^{n-1}$ in $\mathbb{Z}[\![t]\!]$ with $f_1=1$ [Theorem (1.5)].

Let $\ell(t)=\sum n^{-1}f_nt^n$ and let D be the greatest common divisor of the coefficients of the polynomial $\Delta(t)$. We prove that the assumption

$$(0.2) \qquad \textit{degree } a_i(t)\leqq 2i \quad \textit{for} \quad i=1,\ldots,6$$

in combination with (0.1), implies that the power series

$$\mathcal{G}(t_1,t_2)\overset{\text{def}}{=}\ell^{-1}(\ell(t_1)+\ell(t_2))$$

has coefficients in $\mathbb{Z}[1/D]$, i.e. $\ell(t)$ is the logarithm of a 1-parameter commutative formal group law $\mathcal{G}(t_1,t_2)$ over $\mathbb{Z}[1/D]$ [Theorem (3.4)].

In the second part of the paper we give another interpretation of the formal group law $\mathcal{G}(t_1,t_2)$. For this we fix a prime number $p\geqq 5$ and assume besides (0.1) and (0.2) also

(0.3) Δ *is not constant* mod p, *i.e.* $p\nmid D$

(0.4) *neither* $gcd(g_2(t)^3 \bmod p,\ g_3(t)^2 \bmod p)$ *nor*

$$gcd(t^{24}g_2(t^{-1})^3 \bmod p,\ t^{24}g_3(t^{-1})^2 \bmod p)$$

is divisible by the twelfth power of a non-constant polynomial in $\mathbb{F}_p[t]$.

Here $g_2(t)$ and $g_3(t)$ are the Weierstrass g-invariants of (W) [29]; these are polynomials in $\mathbb{Z}[t, 1/6]$ of degree $\leqq 8$ and $\leqq 12$ respectively. Consider the elliptic curve over $\mathbb{F}_p(t)$ given by the equation (W) mod p. Let $\mathscr{X}_p$ be its Néron minimal model [23]. Then $\mathscr{X}_p$ is a $K3$-surface over $\mathbb{F}_p$. Artin and Mazur [2] associated with such a surface a 1-dimensional commutative formal group over $\mathbb{F}_p$, called the formal Brauer group of $\mathscr{X}_p$ and denoted $\mathscr{B}r_{\hat{\mathscr{X}}_p}$. We prove in Sect. 6:

Main Theorem. *If* (0.1)–(0.4) *hold, then* $\mathscr{G}(t_1, t_2) \bmod p$ *is a formal group law for* $\mathscr{B}r_{\hat{\mathscr{X}}_p}$. □

By means of Cartier-Dieudonné theory and crystalline cohomology one can connect $\mathscr{B}r_{\hat{\mathscr{X}}_p}$ with the zeta-function of $\mathscr{X}_p/\mathbb{F}_p$. Thus one finds a link between the solution $f(t)$ of the Picard-Fuchs equation of the elliptic pencil (W) and the zeta-function of the surface $\mathscr{X}_p/\mathbb{F}_p$. This link can be expressed very concretely by congruences similar to the Atkin-Swinnerton-Dyer congruences for elliptic curves over $\mathbb{Q}$ [10]. The result is as follows. Let

$$Z(\mathscr{X}_p/\mathbb{F}_p; T) = 1/((1-T)(1-p^2T)P_2(T))$$

be the zeta-function of $\mathscr{X}_p/\mathbb{F}_p$. The polynomial $P_2(T)$ has integral coefficients, constant term 1 and degree 22. Assume it can be factored, $P_2(T) = P_{21}(T)P_{22}(T)$ such that $P_{21}(T) \in \mathbb{Z}[T]$, $P_{22}(p^{-1}T) \in \mathbb{Z}[T]$, $P_{21}(0) = P_{22}(0) = 1$. Write $P_{21}(T) = 1 + \alpha_1 T + \ldots + \alpha_\nu T^\nu$. Then the congruences are:

$$f_{mp^r} + \alpha_1 f_{mp^{r-1}} + \alpha_2 f_{mp^{r-2}} + \ldots + \alpha_\nu f_{mp^{r-\nu}} \equiv 0 \bmod p^r \tag{0.5}$$

for all $m, r \geqq 1$ (convention: $f_n = 0$ if $n \notin \mathbb{N}$). In order to keep the number of terms in (0.5) small one wants $P_{22}(T)$ to have a large degree. A useful factor $P_{22}(T)$ of $P_2(T)$ can be found by looking at the algebraic cycles on the surface $\mathscr{X}_p \otimes \bar{\mathbb{F}}_p$ (over the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$).

In the third part of the paper we have worked out a few concrete examples. Among other things we obtain congruences which relate the numbers

$$\sum_k \binom{n}{k}^2 \binom{n+k}{k}, \quad \sum_k \binom{n}{k}^3, \quad \text{and} \quad \sum_k \binom{n}{k}^2 \binom{2k}{k}$$

to the decomposition of rational primes in the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(\sqrt{-3})$, respectively, as well as to the cusp forms of weight 3

$$q \prod_{n \geqq 1} (1-q^{4n})^6,$$

$$q \prod_{n \geqq 1} (1-q^n)^2 (1-q^{2n})(1-q^{4n})(1-q^{8n})^2$$

$$q \prod_{n \geqq 1} (1-q^{2n})^3 (1-q^{6n})^3$$

[see Theorems (13.1), (13.8), (14.2)]. The numbers $\sum_k \binom{n}{k}^2 \binom{n+k}{k}$ became famous through Apéry's proof of the irrationality of $\zeta(2)$ and $\zeta(3)$ [30]. We obtain these congruences by studying elliptic pencils on appropriate models of the $K3$-surfaces, of which the lattice of transcendental cycles has rank 2 and intersection form

equivalent to $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, respectively $\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$, respectively $\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}$. These models may also be interesting for other purposes.

In the appendix we have assembled the facts in formal group theory which are used in the paper.

Part I

1

Consider the family of complex elliptic curves described by Eq. (W), parametrized by the set $\mathbb{C}_\Delta = \{t \in \mathbb{C} | \Delta(t) \neq 0\}$. Let E_t denote the fiber over t. The canonical invariant regular 1-form on this elliptic curve E_t is

$$\omega_t = dx/(2y + a_1 x + a_3), \tag{1.1}$$

where $x = X/Z$, $y = Y/Z$; often we write just ω instead of ω_t.

Let U be a simply connected open subset of $\mathbb{C}_\Delta$ and let t_0 be a point in U. For every $t \in U$ there is a canonical isomorphism $H_1(E_{t_0}, \mathbb{Z}) \simeq H_1(E_t, \mathbb{Z})$, carrying a cycle along a path in U from t_0 to t. Given $\gamma_{t_0} \in H_1(E_{t_0}, \mathbb{Z})$ we denote its image in $H_1(E_t, \mathbb{Z})$ by γ_t and then write γ for the collection $\{\gamma_t\}_{t \in U}$. With γ one associates the holomorphic function $\int_\gamma \omega$ on U which assigns to t the period of ω_t along γ_t:

$$\left(\int_\gamma \omega\right)(t) = \int_{\gamma_t} \omega_t .$$

This function can be extended to a multi-valued function on $\mathbb{C}_\Delta$, or to a univalent function on the universal covering of $\mathbb{C}_\Delta$ [18, 22].

The function $\int_\gamma \omega$ satisfies a second order linear differential equation, independent of γ and U. This is the Picard-Fuchs equation of the elliptic pencil (W) [18, 22]. The following classical method for deriving this equation can be found in [18, p. 34]. Let g_2 and g_3 be the Weierstrass g-invariants of (W), i.e. [29]:

$$\begin{aligned} 12 g_2 &= (a_1^2 + 4a_2)^2 - 24(a_1 a_3 + 2a_4), \\ 216 g_3 &= -(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(a_1 a_3 + 2a_4) - 216(a_3^2 + 4a_6). \end{aligned} \tag{1.2}$$

Then the functions $\Omega = \sqrt{g_3/g_2} \int_\gamma \omega$ are in fact (multi-valued) functions of the j-invariant J of (W), which satisfy the differential equation

$$\frac{d^2\Omega}{dJ^2} + \frac{1}{J}\frac{d\Omega}{dJ} + \frac{(31J - 4)\Omega}{144J^2(J-1)^2} = 0. \tag{1.3}$$

Substituting $\Omega = \sqrt{g_3/g_2} \int_\gamma \omega$ and the expression for J as function of t one can thus derive the differential equation for $\int_\gamma \omega$ as function of t. For the examples in Part III we shall present more practical ways for obtaining the Picard-Fuchs equation (see Sects. 11 and 10).

The Picard-Fuchs equation can be written as

(1.4) with
$$\mathfrak{L}\eta = 0$$
$$\mathfrak{L} = L_2\frac{d^2}{dt^2} + L_1\frac{d}{dt} + L_0 \in \mathbb{Z}\left[t, \frac{d}{dt}\right],$$

normalized so that the polynomials L_0, L_1, L_2 have no common non-trivial factor in $\mathbb{Z}[t]$.

(1.5) **Theorem.** *Assume that condition* (0.1) *for equation* (W) *is satisfied. Put* $c_4 = 12g_2$ *[cf.* (1.2) *and* [29]*]. Let*

$$F\left(\frac{5}{12}, \frac{1}{12}, 1; z\right) = \sum_{k=0}^{\infty}\binom{-5/12}{k}\binom{-1/12}{k}z^k$$

be the hypergeometric function with parameters 5/12, 1/12, 1 [19]. *Set*

$$f(t) = c_4(t)^{-1/4}F\left(\frac{5}{12}, \frac{1}{12}, 1; \frac{1}{J(t)}\right).$$

Then

$$\mathfrak{L}f(t) = 0, \quad f(t) \in \mathbb{Z}[[t]], \quad f(0) = 1$$

and f is the only solution of the Picard-Fuchs equation which is holomorphic at $t=0$ and satisfies $f(0)=1$.

Proof. Recall that $J = g_2^3/(g_2^3 - 27g_3^2)$ and $c_4 = 12g_2$. Hence

$$f(t) = (3\sqrt{2})^{-1}\sqrt{g_2/g_3}\,\dot{\theta},$$

where $\theta = (1-1/J)^{1/4}F(5/12, 1/12, 1; 1/J)$. The function θ is a solution of (1.3) in the neighborhood of $J=\infty$. Assumption (0.1) implies that J has a pole at $t=0$. Thus we see that $f(t)$ is indeed a solution of the Picard-Fuchs equation in the neighborhood of $t=0$ i.e. $\mathfrak{L}f=0$. Notice that (0.1) also implies $c_4(0)=1$, and hence $f(0)=1$.

In order to show that $f(t)$ has a power series expansion with integral coefficients we are going to check:

(i) $$c_4(t)^{-1/4} \in \mathbb{Z}[[t]],$$

(ii) $$J(t)^{-1} \in 12^3\mathbb{Z}[[t]],$$

(iii) $$F(5/12, 1/12, 1; 12^3 z) \in \mathbb{Z}[[z]].$$

For (i) we write

$$c_4^{-1/4} = a_1^{-1}\cdot(1+4a_2a_1^{-2})^{-1/2}\cdot(1-24(a_1a_3+2a_4)(a_1^2+4a_2)^{-2})^{-1/4}.$$

The result then follows from the observation: $a_1(0)=1$, $a_2(0)=\ldots=a_6(0)=0$, $(1+4z)^{-1/2} \in \mathbb{Z}[[z]]$, and $(1-24z)^{-1/4} \in \mathbb{Z}[[z]]$.

For (ii) one only has to notice: $c_4(0)=1$ and $J^{-1} = 12^3\Delta c_4^{-3}$ (cf. [29]). Result (iii) is correct, because $\binom{-5/12}{k}\binom{-1/12}{k}12^{3k}$ is an integer for every k.

A second solution of the Picard-Fuchs equation. independent of f, has the form

$$f(t)\log(J(t)^{-1})+g(t)$$

with $g(t)$ holomorphic about $t=0$ [19]. Hence, $f(t)$ is the unique holomorphic solution about $t=0$ with $f(0)=1$. □

(1.6) *Remark.* Actually $f(t)$ equals $\int_\gamma \omega$ where γ is a so-called vanishing cycle at $t=0$.

(1.7) *Remark.* The statement that a power series $h(t)=\sum h_n t^n$ satisfies $\mathfrak{Q}h=0$, is equivalent to the statement that the sequence of coefficients $(h_0, h_1, \ldots, h_n, \ldots)$ is the solution of a certain linear recurrence relation over $\mathbb{Z}$. The fact that this recurrence relation has only one complex solution starting with 1 [namely the sequence of coefficients of $f(t)$ (1.5)], means that by the recurrence relation each term of a solution, in any ring of characteristic 0, is uniquely determined by the preceding terms. Thus, for instance, $f(t)$ is also the unique power series solution of the Picard-Fuchs equation with p-adic coefficients and constant term 1.

2

In order to fully exploit the integrality of Eq. (W) one has to consider the smooth proper scheme $\mathscr{E}$ over $\mathrm{Spec}(\mathbb{Z}[t, 1/\Delta])$, which is defined by (W). The family of complex elliptic curves, which we considered in the previous section, is obtained by pulling $\mathscr{E}\to\mathrm{Spec}(\mathbb{Z}[t, 1/\Delta])\to\mathrm{Spec}\mathbb{Z}$ back along the map induced by $\mathbb{Z}\hookrightarrow\mathbb{C}$. Also the Picard-Fuchs equation arises as a pull-back; to be precise, the Gauss-Manin connection

$$\nabla: \mathbb{Z}[t, 1/\Delta, d/dt]\to\mathrm{End}(H^1_{DR}(\mathscr{E}/\mathbb{Z}[t, 1/\Delta]))$$

makes differential operators act on cohomology classes, in such a way that the operator $\mathfrak{Q}$ (1.4) annihilates the cohomology class $[\omega]$ of the 1-form ω (1.1):

$$\nabla(\mathfrak{Q})[\omega]=0 \tag{2.1}$$

[22, 17].

Now let $\mathscr{E}\hat{}$ be the completion of $\mathscr{E}$ at the $\mathbb{Z}[t, 1/\Delta]$-rational point $(0, 1, 0)$, which is the 0-section for the group structure on $\mathscr{E}$. Traditionnally one takes $u=-X/Y$ as a (formal) coordinate on $\mathscr{E}\hat{}$ [29]. The 1-form ω has on $\mathscr{E}\hat{}$ a power series expansion

$$\omega=\sum_{n\geq 1} q_n u^{n-1}du\,. \tag{2.2}$$

The coefficients q_n in this expansion can be written as integral polynomials in $a_1, \ldots, a_6$ and $q_1=1$ [see [29]; in fact one can show

$q_n=$coefficient of x^{n-1} in $\sum_{m=0}^{[n/2]}\binom{n-1-m}{m}(a_1x+a_3)^{n-1-2m}(x^3+a_2x^2+a_4x+a_6)^m$

[32], but we shall not use this quite explicit description here]. In the situation considered here $a_1, \ldots, a_6$ are elements of $\mathbb{Z}[t]$, and hence all q_n are in $\mathbb{Z}[t]$ too.

The construction of the Gauss-Manin connection is such that in $H^1_{DR}(\mathscr{E}'/\mathbb{Z}[t, 1/\Delta])$ one has

$$\nabla(\mathfrak{L})[\omega] = \text{cohomology class of the 1-form } \sum \mathfrak{L}(q_n)u^{n-1}du\,.$$

[17].

Vanishing of this cohomology class means that $\sum \mathfrak{L}(q_n)u^{n-1}du$ is an exact 1-form, equal to dg for some $g \in \mathbb{Z}[t, 1/\Delta][\![u]\!]$. Thus one finds:

(2.3) **Theorem** (Katz [17]). *In the above situation one has for every n:*

$$\mathfrak{L}q_n \equiv 0 \bmod n\mathbb{Z}[t, 1/\Delta]\,. \quad \square$$

By construction each $\mathfrak{L}q_n$ is a polynomial. Letting D be the greatest common divisor of the coefficients of the polynomial $\Delta(t)$ we may therefore restate (2.3) as:

(2.3bis) $$\mathfrak{L}q_n \equiv 0 \bmod n\mathbb{Z}[1/D][t] \text{ for all } n\,.$$

So the polynomials q_n are solutions of what one might call "Picard-Fuchs congruence differential equations". These should, of course, be intimately related to the solution $\mathscr{f}(t)$ of the actual Picard-Fuchs equation [at least if (0.1) holds]. And, indeed, the situation is as follows.

(2.4) **Theorem.** *Assume that condition* (0.1) *is satisfied. Let p be a prime number which does not divide all coefficients of* $\Delta(t)$.

Then there exists a unique power series $H(t) \in \mathbb{Z}[\![t]\!]$ *such that*

(2.4.1) $$\text{for all } n\text{: } q_n(t) \equiv H(t)q_{n/p}(t^p) \bmod p^s \text{ if } p^s | n\,,$$

(2.4.2) $$\mathscr{f}(t) = H(t)\cdot H(t^p)\cdot H(t^{p^2})\cdot \ldots = \prod_{i \geqq 0} H(t^{p^i})\,.$$

Proof. The expansion of the group structure of the cubic (W) in terms of the coordinate $u = -X/Y$ is a 1-parameter commutative formal group law over $\mathbb{Z}[t]$ with logarithm $\sum n^{-1}q_n u^n$ (see the appendix for some of the main facts about formal groups). Equation (W) reduces modulo t to $Y^2Z + XYZ = X^3$. Consequently, the 1-form ω is modulo t equal to $du/(1-u)$. Whence, $q_n(0) = 1$ for all n.

Instead of $\mathbb{Z}[t]$ we use $\mathbb{Z}_p[\![t]\!]$ as ground ring ($\mathbb{Z}_p$ = p-adic integers). This ring is a complete local ring, with residue field $\mathbb{F}_p$, which can be endowed with an endomorphism σ, lifting Frobenius, by setting $\sigma|\mathbb{Z}_p = id$ and $\sigma(t) = t^p$. Being 1 mod t q_p is invertible in $\mathbb{Z}_p[\![t]\!]$. Theorem (A.8) in the appendix now shows the existence of a power series $H(t)$ in $\mathbb{Z}_p[\![t]\!]$ for which (2.4.1) holds. Note that $H(0) = 1$.

Put $g(t) = \prod_{i \geqq 0} H(t^{p^i}) \in \mathbb{Z}_p[\![t]\!]$. Then (2.4.1) implies for all $s > r \geqq 1$:

$$\begin{aligned} q_{p^{r+s}} &\equiv H(t)\cdot H(t^p)\cdot \ldots \cdot H(t^{p^{s-1}})\cdot q_{p^r}(t^{p^s}) \bmod p^{r+1} \\ &\equiv g(t) \bmod (p^{r+1}, t^{p^s})\,. \end{aligned}$$

Combining this with (2.3bis) we get

$$\mathfrak{L}g \equiv 0 \bmod (p^{r+1}, t^{p^s}) \quad \text{for all} \quad s > r \geqq 1\,,$$

and hence $\mathfrak{L}g = 0$ and $g = \mathscr{f}$ (1.5), (1.7). So (2.4.2) also holds.

To see that $H(t)$ is unique and has coefficients in $\mathbb{Z}$ one may notice that $H(t) = \mathscr{f}(t)/\mathscr{f}(t^p)$. $\square$

3

Throughout this section we assume that (0.1) and (0.2) are satisfied. This implies for the polynomials q_n, defined in (2.2), that

$$q_n(0)=1 \text{ for all } n, \tag{3.1}$$

$$\text{degree } q_n \leqq 2n-2 \text{ for all } n; \tag{3.2}$$

indeed, (3.1) follows from the observation that (0.1) makes the differential ω reduce to $du/(1-u)$ modulo t, and (3.2) follows from (0.2) because q_n is a homogeneous polynomials of weight $n-1$ in $a_1, \ldots, a_6$ if a_i gets weight i.

(3.3) *Definition.* We set

$$\varrho_n = \text{coefficient of } t^{n-1} \text{ in } q_n$$

and then define

$$\imath(t)=\sum_{n\geqq 1} n^{-1}\varrho_n t^n$$

$$\varphi(t_1,t_2)=\imath^{-1}(\imath(t_1)+\imath(t_2)).$$

We also define

$$\ell(t)=\sum_{n\geqq 1} n^{-1}\lambda_n t^n,$$

where $\lambda(t)=\sum \lambda_n t^{n-1}$ is the power series expansion of the function $\lambda(t)$ given in (1.5), and we set

$$\mathcal{G}(t_1,t_2)=\ell^{-1}(\ell(t_1)+\ell(t_2)).$$

(3.4) **Theorem.** *Assume that conditions* (0.1) *and* (0.2) *for Eq.* (W) *are satisfied. Let* D *be the greatest common divisor of the coefficients of the polynomial* $\Delta(t)$, *the discriminant of* (W).

Then:

(i) $$\imath(t)\equiv\ell(t)\equiv t \bmod \text{degree } 2$$

(ii) $$\varphi(t_1,t_2)\in\mathbb{Z}[\![t_1,t_2]\!]$$

(iii) $$\imath^{-1}(\ell(t))\in\mathbb{Z}[1/D][\![t]\!]$$

(iv) $$\mathcal{G}(t_1,t_2)\in\mathbb{Z}[1/D][\![t_1,t_2]\!].$$

In other words: $\varphi(t_1,t_2)$ *is a* 1*-parameter commutative formal group law over* $\mathbb{Z}$ *with logarithm* $\imath(t)$, $\mathcal{G}(t_1,t_2)$ *is a* 1*-parameter commutative formal group law over* $\mathbb{Z}[1/D]$ *with logarithm* $\ell(t)$ *and these two formal group laws are strictly isomorphic over* $\mathbb{Z}[1/D]$.

(See the appendix for a brief survey of some facts in formal group theory.)

Proof. (i) is obvious and (iv) follows immediately from (ii) and (iii).

To prove (ii) it suffices to show that $\varphi(t_1,t_2)$ lies in $\mathbb{Z}_p[\![t_1,t_2]\!]$ for every prime number p. Fix a prime p. Since the polynomials $q_n(t)$ are the coefficients in the

logarithm of a 1-parameter formal group law, Theorem (A.8) in the appendix shows that there exist polynomials $S_i(t)$ in $\mathbb{Z}_p[t]$ such that

$$q_{mp^r}(t)+\sum_{i=1}^{r} p^{i-1}S_i(t)q_{mp^{r-i}}(t^{p^i})\equiv 0 \bmod p^r \quad \text{for all } m,r\geqq 1$$
$$=0 \qquad\qquad \text{for } m=1 \text{ and all } r. \tag{1}$$

This relation in combination with (3.2) shows: degree $S_i(t)\leqq 2p^i-2$. Focussing on the coefficient of t^{mp^r-1} in (1) we see that for all $m,r\geqq 1$

$$q_{mp^r}+\sum_{i=1}^{r} p^{i-1}A_i q_{mp^{r-i}}\equiv 0 \bmod p^r, \tag{2}$$

where A_i is the coefficient of t^{p^i-1} in $S_i(t)$. Using (A.8) we can now conclude that $\varkappa(t)$ is the logarithm of a formal group law over $\mathbb{Z}_p$. This proves (ii) (for an alternative proof compare with Sect. 5).

For (iii) we show $\varkappa^{-1}(\ell(t))\in\mathbb{Z}_p[\![t]\!]$ for all primes p not dividing D. Fix p, $p\nmid D$. Recall from the proof of (2.4)

$$q_{p^{r+s}}\equiv f(t) \bmod (p^{r+1},t^{p^s}) \quad \text{for all} \quad s>r\geqq 1$$

and substitute this result in (1), taking $m=p^s$,:

$$f(t)+\sum_{i=1}^{r} p^{i-1}S_i(t)f(t^{p^i})\equiv 0 \bmod (t^{p^s},p^r). \tag{3}$$

Let s tend to ∞ and focus on the coefficient of t^{np^r-1} in (3). We see

$$f_{np^r}+\sum_{i=1}^{r} p^{i-1}A_i f_{np^{r-i}}\equiv 0 \bmod p^r. \tag{4}$$

This holds for all n and r. The combination of (2) and (4) implies, according to (A.9), that the power series $\varkappa^{-1}(\ell(t))$ has coefficients in $\mathbb{Z}_p$. This proves (iii). □

Part II

4

Let k be a perfect field of characteristic different from 2 and 3. Again we start with a Weierstrass equation

$$(4.1) \qquad Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3,$$

but in this and the next section we take coefficients $a_i=a_i(t)$ from the polynomial ring $k[t]$. We fix a positive integer N and assume

(4.2.1) the discriminant $\Delta=\Delta(t)$ of (4.1) is not constant

(4.2.2) degree $a_i(t)\leqq Ni$ for $i=1,\ldots,6$

(4.2.3) neither $gcd(g_2(t)^3,g_3(t)^2)$ nor

$$gcd(t^{12N}g_2(t^{-1})^3,t^{12N}g_3(t^{-1})^2)$$

is divisible by the twelfth power of a non-constant polynomial in $k[t]$;

here g_2 and g_3 are the Weierstrass g-invariants of (4.1) (1.2); they are polynomials of degree $\leqq 4N$ respectively $\leqq 6N$. Note that here we do not assume that the j-invariant is non-constant.

Equation (4.1) defines a surface in $\mathbb{P}^2_{\mathcal{k}} \times \mathbb{A}^1_{\mathcal{k}}$ (X, Y, Z are homogeneous coordinates on the projective plane $\mathbb{P}^2_{\mathcal{k}}$ and t is a coordinate on the affine line $\mathbb{A}^1_{\mathcal{k}}$). To complete this surface with a fiber above $t=\infty$ one takes the Weierstrass equation

$$\overline{(4.1)} \qquad \bar{Y}^2\bar{Z} + \bar{a}_1\bar{X}\bar{Y}\bar{Z} + \bar{a}_3\bar{Y}\bar{Z}^2 = \bar{X}^3 + \bar{a}_2\bar{X}^2\bar{Z} + \bar{a}_4\bar{X}\bar{Z}^2 + \bar{a}_6\bar{Z}^3$$

with coefficients $\bar{a}_i = \bar{t}^{Ni} a_i(\bar{t}^{-1})$ in $\mathcal{k}[\bar{t}]$ and one glues the two surfaces defined by (4.1) and $\overline{(4.1)}$ above $\mathrm{Spec}(\mathcal{k}[t, t^{-1}])$ and $\mathrm{Spec}(\mathcal{k}[\bar{t}, \bar{t}^{-1}])$ via the identification

$$(4.3) \qquad \bar{t} = t^{-1}, \quad \bar{X} = t^{-2N}X, \quad \bar{Y} = t^{-3N}Y, \quad \bar{Z} = Z.$$

The result is a complete surface $\mathcal{X}'$ over $\mathcal{k}$ together with a map $\varepsilon' : \mathcal{X}' \to \mathbb{P}^1_{\mathcal{k}}$ whose fibers are curves of arithmetic genus 1. This surface $\mathcal{X}'$ may have singularities. In order to resolve these singularities we look at the Néron minimal model of (4.1), where (4.1) is viewed as an elliptic curve over the function field $\mathcal{k}(t)$ of $\mathbb{P}^1_{\mathcal{k}}$ (see [23, 24]). This Néron minimal model, call it $\mathcal{X}$, is a complete non-singular surface over $\mathcal{k}$ equipped with an elliptic pencil $\varepsilon : \mathcal{X} \to \mathbb{P}^1_{\mathcal{k}}$. By inspection of the constructions in [23] one checks that the hypotheses in (4.2) imply that there is a morphism $\pi : \mathcal{X} \to \mathcal{X}'$ [the point is that in the given circumstances the transformation which locally puts (4.1) and $\overline{(4.1)}$ in Néron's standard form [23, III, Sect. 7], are defined over the local rings i.e. the integer h in loc. cit. Proposition 4 is zero]. The morphism π is a resolution of the singularities of $\mathcal{X}'$. It is also compatible with the elliptic pencils on $\mathcal{X}$ and $\mathcal{X}'$ and, in fact, the pencil $\varepsilon' : \mathcal{X}' \to \mathbb{P}^1_{\mathcal{k}}$ is the Jacobian Weierstrass fibration for $\varepsilon : \mathcal{X} \to \mathbb{P}^1_{\mathcal{k}}$.

Remark. A slightly different method for resolving the singularities of $\mathcal{X}'$ is explained in [16]. This method seems to require a possible extension of the ground field $\mathcal{k}$. Néron's minimal model is however defined over the ground field we started with [24]. This fact may be important when we come to the use of zeta-functions.

The normal bundle to the 0-section of the pencil $\varepsilon' : \mathcal{X}' \to \mathbb{P}^1_{\mathcal{k}}$ is spanned above $\mathrm{Spec}(\mathcal{k}[t])$ by X/Y and above $\mathrm{Spec}(\mathcal{k}[\bar{t}])$ by $\bar{X}/\bar{Y}$. So its degree as a line bundle on $\mathbb{P}^1_{\mathcal{k}}$ is N. The same is true for the pencil ε on $\mathcal{X}$. Using [8, Theorem 2] one can now compute the canonical bundle $K_{\mathcal{X}}$ and the irregularity $\dim \mathrm{Pic}^0_{\mathcal{X}/\mathcal{k}}$. From this one finds:

if $N=1$ then $\mathcal{X}$ is a rational surface

if $N=2$ then $\mathcal{X}$ is a $K3$-surface.

5

The hypotheses for this section are the same as for Sect. 4, except that we assume from now on $N=2$, i.e. $\mathcal{X}$ is a $K3$-surface.

We are interested in the formal Brauer group $\mathcal{B}r_{\mathcal{X}}$ of the $K3$-surface $\mathcal{X}$ [1, 2]. In [1] Artin presents the construction of a 1-parameter formal group law for $\mathcal{B}r_{\mathcal{X}}$, in terms of the data of the Weierstrass equation (4.1). His construction is as follows.

Let

$$u_1 \oplus u_2 = u_1 + u_2 - a_1 u_1 u_2 + \ldots \in \mathcal{k}[t]\,[\![u_1, u_2]\!] \tag{5.1}$$

be the formal power series expansion of the addition law on the cubic (4.1), in the coordinate $u = -X/Y$ about the point $(0, 1, 0)$ [29]. Then Artin [1, p. 551] gives a formal group law $\varphi(s_1, s_2)$ for $\mathcal{B}r_{\mathcal{X}}$ as solution of the equation

$$t^{-1}s_1 \oplus t^{-1}s_2 = t^{-1}\varphi(s_1, s_2) \oplus f(s_1, s_2) \oplus t^{-2}\bar{f}(s_1, s_2) \tag{5.2}$$

with $\varphi(s_1, s_2) \in \mathcal{k}[\![s_1, s_2]\!]$, $f(s_1, s_2) \in \mathcal{k}[t]\,[\![s_1, s_2]\!]$,

$$\bar{f}(s_1, s_2) \in \mathcal{k}[t^{-1}]\,[\![s_1, s_2]\!], \quad f(0,0) = \bar{f}(0,0) = 0\,.$$

Since $\oplus$ is ordinary addition plus higher order terms, one can indeed solve $\varphi(s_1, s_2)$ from (5.2) by induction.

Both (5.1) and (5.2) make sense, and (5.2) remains solvable, if we treat the coefficients a_{ij} of

$$a_i(t) = a_{i0} + a_{i1}t + \ldots + a_{i,2i}t^{2i} \quad (i = 1, \ldots, 6)\,,$$

as indeterminates and replace $\mathcal{k}$ by the polynomial ring $R = \mathbb{Z}[a_{1,0}, \ldots, a_{6,12}]$. We can now make things more explicit by using the fact that

$$u_1 \oplus u_2 = L^{-1}(L(u_1) + L(u_2)) \tag{5.3.1}$$

with

$$L(u) = \sum_{n \geqq 1} n^{-1} q_n u^n \in \mathbb{Q}[a_{1,0}, \ldots, a_{6,12}, t]\,[\![u]\!], \tag{5.3.2}$$

obtained from the power series expansion of the 1-form associated with the cubic (4.1) (over $R[t]$):

$$\omega = dx/(2y + a_1 x + a_3) = \sum_{n \geqq 1} q_n u^{n-1} du \tag{5.3.3}$$

($x = X/Z$, $y = Y/Z$, $u = -X/Y$). Combining (5.3.1) with (5.2) one finds

$$L(t^{-1}s_1) + L(t^{-1}s_2) = L(t^{-1}\varphi(s_1, s_2)) + L(f(s_1, s_2)) + L(t^{-2}\bar{f}(s_1, s_2))\,. \tag{5.4}$$

Focus on the coefficient of t^{-1} in (5.4). Let

$$\varrho_n = \text{coefficient of } t^{n-1} \text{ in } q_n \tag{5.5}$$

$$\imath(s) = \sum_{n \geqq 1} n^{-1} \varrho_n s^n \in \mathbb{Q}[a_{1,0}, \ldots, a_{6,12}]\,[\![s]\!]\,. \tag{5.6}$$

The coefficient of t^{-1} on the right-hand side of (5.4) is $\imath(\varphi(s_1, s_2))$ and on the left-hand side it is $\imath(s_1) + \imath(s_2)$. Consequently,

$$\varphi(s_1, s_2) = \imath^{-1}(\imath(s_1) + \imath(s_2))\,, \tag{5.7}$$

i.e. $\imath(s)$ is the logarithm of $\varphi(s_1, s_2)$, whereas $\varphi(s_1, s_2)$ is a 1-parameter commutative formal group law over R which lifts Artin's group law for $\mathcal{B}r_{\mathcal{X}}$.

(5.8) *Remark.* The above argument is also correct in characteristic 2 or 3, provided one knows somehow that the Weierstrass equation, which one wants to consider,

belongs to a $K3$-surface. We used the hypothesis $\mathrm{char}(k) \neq 2, 3$ only to have (4.2.3) (with $N=2$) as a criterion for recognizing Weierstrass equations belonging to $K3$-surfaces.

(5.9) *Remark.* If (4.1) is in fact the reduction modulo p of an equation (W) defined over $\mathbb{Z}$, then one may use in the above constructions the data from (W) instead of those from the universal lifting of (4.1) to the polynomial ring R. The notations in the above constructions then get the same meaning as in Part I.

6

It is time to put the results of Sect. 3 and 5 together. The situation is as follows. We are given a Weierstrass equation

$$\text{(W)} \qquad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_i = a_i(t)$ in $\mathbb{Z}[t]$. We are also given a prime number $p \geqq 5$. We assume:

(6.1.1) the j-invariant J of (W) is not constant, i.e. $J \in \mathbb{Q}(t) \setminus \mathbb{Q}$.

(6.1.2) the discriminant Δ of (W) is not constant mod p, i.e. $\Delta \notin \mathbb{Z} + p\mathbb{Z}[t]$.

(6.1.3) Equation (W) reduces modulo t to $Y^2Z + XYZ = X^3$.

(6.1.4) degree $a_i(t) \leqq 2i$ for $i = 1, \ldots, 6$.

(6.1.5) neither $gcd(g_2(t)^3 \bmod p, g_3(t)^2 \bmod p)$ nor

$$gcd(t^{24}g_2(t^{-1})^3 \bmod p, t^{24}g_3(t^{-1})^2 \bmod p)$$

is divisible by the twelfth power of a non-constant polynomial in $\mathbb{F}_p[t]$.

The constructions in Sect. 4 can be applied to the equation $((\text{W}) \bmod p)$. They produce a $K3$-surface over $\mathbb{F}_p$, which we denote by $\mathscr{X}_p$ (to indicate the dependence on p). Section 5 leads to a formal group law for the formal Brauer group $\mathscr{B}r_{\hat{\mathscr{X}}_p}$, which turns out to be the reduction mod p of the group law $\varphi(t_1, t_2)$ over $\mathbb{Z}$, which was constructed directly from (W) in Sect. 3. And then Theorem (3.4) shows that $\varphi(t_1, t_2)$ is, over $\mathbb{Z}[1/D]$, strictly isomorphic to the formal group law $\mathscr{G}(t_1, t_2)$ whose logarithm $\ell(t)$ is the integral of the solution $f(t)$ of the Picard-Fuchs equation of the elliptic pencil (W). Thus we have proved:

(6.2) **Main Theorem.** *$\mathscr{G}(t_1, t_2) \bmod p$ is a formal group law for $\mathscr{B}r_{\hat{\mathscr{X}}_p}$.* □

(6.3) *Remark.* This theorem is also correct in characteristic 2 and 3 provided $\mathscr{X}_p$ is a $K3$-surface.

7

The situation is as in the previous section. In order to extract arithmetical information from our main theorem (6.2) we are going to study the action of Frobenius on the Cartier-Dieudonné module of $\mathscr{B}r_{\hat{\mathscr{X}}_p}$. We refer to the appendix for a survey of the relevant facts in Dieudonné theory.

First assume $\mathscr{X}_p$ is not supersingular [14, II(7.2a)]. According to [2, (4.3)] the Cartier-Dieudonné module of $\mathscr{B}\mathscr{r}_{\mathscr{X}_p}$ is equal to $H^2(\mathscr{X}_p, \mathscr{W}\mathscr{O})$, the second cohomology group of the sheaf of Witt vectors on $\mathscr{X}_p$. This identification includes the action of Frobenius F. As $\mathscr{X}_p$ is not supersingular, $H^2(\mathscr{X}_p, \mathscr{W}\mathscr{O})$ is a free $\mathbb{Z}_p$-module of rank h (= height $\mathscr{B}\mathscr{r}_{\mathscr{X}_p}$; see [14]). Since we work over the prime field $\mathbb{F}_p$, Frobenius acts $\mathbb{Z}_p$-linearly. Let

$$g_1(T) = T^h + \gamma_1 T^{h-1} + \gamma_2 T^{h-2} + \ldots + \gamma_h$$

be the characteristic polynomial of F on $H^2(\mathscr{X}_p, \mathscr{W}\mathscr{O})$. Here $\gamma_1, \ldots, \gamma_h$ are p-adic integers. Put $\gamma_i = 0$ for $i > h$. Then (6.2) and (A.14) in the appendix lead to

$$\text{(7.1)} \qquad \phi_{mp^r} + \gamma_1 \phi_{mp^{r-1}} + \gamma_2 \phi_{mp^{r-2}} + \ldots + \gamma_r \phi_m \equiv 0 \bmod p^r$$

for all $m, r \geqq 1$ (convention: $\phi_n = 0$ if $n \notin \mathbb{Z}$). We prefer, however, congruences with ordinary integers instead of p-adics. To achieve this goal we use the fact that, since $\mathscr{X}_p$ is not supersingular, $H^2(\mathscr{X}_p, \mathscr{W}\mathscr{O})$ is a direct summand of the second crystalline cohomology group $H^2_{\text{cris}}(\mathscr{X}_p/\mathbb{Z}_p)$ of $\mathscr{X}_p$; more precisely [14, II(7.2)]

$$H^2_{\text{cris}}(\mathscr{X}_p/\mathbb{Z}_p) = H^2(\mathscr{X}_p, \mathscr{W}\mathscr{O}) \oplus H^1(\mathscr{X}_p, \mathscr{W}\Omega^1) \oplus H^0(\mathscr{X}_p, \mathscr{W}\Omega^2).$$

This is compatible with the action of Frobenius. Let

$$\bar{P}_2(T) = T^{22} + \beta_1 T^{21} + \ldots + \beta_{22}$$

respectively

$$g_2(T) = T^{22-h} + \delta_1 T^{21-h} + \ldots + \delta_{22-h}$$

be the characteristic polynomials of F acting on $H^2_{\text{cris}}(\mathscr{X}_p/\mathbb{Z}_p)$ respectively

$$H^1(\mathscr{X}_p, \mathscr{W}\Omega^1) \oplus H^0(\mathscr{X}_p, \mathscr{W}\Omega^2);$$

both spaces are free $\mathbb{Z}_p$-modules. Then, of course, $\bar{P}_2(T) = g_1(T) g_2(T)$. It is known that the eigenvalues of F on $H^1(\mathscr{X}_p, \mathscr{W}\Omega^1) \oplus H^0(\mathscr{X}_p, \mathscr{W}\Omega^2)$ have p-adic valuation $\geqq 1$ [14, II(3.5)]. Whence $\delta_i \in p^i \mathbb{Z}_p$ for all i. Thus we can derive from (7.1):

$$\text{(7.2)} \qquad \sum_n \beta_n \phi_{mp^{r-n}} = \sum_i \left(\delta_i \sum_{n \geqq i} \gamma_{n-i} \phi_{mp^{(r-i)-(n-i)}} \right) \equiv 0 \bmod p^r$$

for all $m, r \geqq 1$. Crystalline cohomology (tensored with $\mathbb{Q}$) is a good Weil cohomology theory [5]. So the characteristic polynomials of Frobenius acting on $H^*_{\text{cris}}(\mathscr{X}_p/\mathbb{Z}_p)$ can be read off from the zeta-function of $\mathscr{X}_p/\mathbb{F}_p$ and they have rational integer coefficients. In the present case one has

$$Z(\mathscr{X}_p/\mathbb{F}_p; T) = 1/((1-T)(1-p^2T)(1+\beta_1 T + \ldots + \beta_{22} T^{22})).$$

Next assume $\mathscr{X}_p$ supersingular. Then $\mathscr{B}\mathscr{r}_{\mathscr{X}_p}$ is isomorphic to the additive formal group $\mathbb{G}_a$ [1, (0.3)]; [14, (7.2)]. This implies by (A.14):

$$\text{(7.3)} \qquad \phi_n \equiv 0 \bmod p^r \quad \text{if} \quad p^r | n.$$

On the other hand, for a supersingular $K3$-surface all eigenvalues of F on H^2_{cris} have p-adic valuation 1 [14, II(7.2)]. So (7.2) is also correct in the supersingular case. Thus, after all, the distinction between supersingular and non-supersingular disappears. We have shown:

(7.4) **Theorem.** *Consider the situation of the previous section. Let*

$$Z(\mathscr{X}_p/\mathbb{F}_p; T) = 1/((1-T)(1-p^2T)P_2(T))$$

be the zeta-function of $\mathscr{X}_p/\mathbb{F}_p$,

$$P_2(T) = 1+\beta_1 T+\beta_2 T^2+ \ldots +\beta_{22}T^{22} \in \mathbb{Z}[T].$$

Let $f(t)=\sum f_n t^{n-1} \in \mathbb{Z}[[t]]$ *be the solution of the Picard-Fuchs equation of the elliptic pencil* (W) *with* $f_1=1$. *Then one has for all* $m, r \geqq 1$:

$$f_{mp^r}+\beta_1 f_{mp^{r-1}}+\beta_2 f_{mp^{r-2}}+ \ldots +\beta_{22} f_{mp^{r-22}} \equiv 0 \bmod p^r. \quad \square$$

Using once more the argument by which (7.2) was derived from (7.1), one can reduce the number of terms in the congruences:

(7.5) **Corollary.** *In the situation of the theorem suppose* $P_2(T)=P_{21}(T)P_{22}(T)$ *with*

$$P_{21}(T)=1+\alpha_1 T+ \ldots +\alpha_\nu T^\nu \in \mathbb{Z}[T] \quad \text{and} \quad P_{22}(p^{-1}T) \in \mathbb{Z}[T].$$

Then: for all $m, r \geqq 1$:

$$f_{mp^r}+\alpha_1 f_{mp^{r-1}}+\alpha_2 f_{mp^{r-2}}+ \ldots +\alpha_\nu f_{mp^{r-\nu}} \equiv 0 \bmod p^r. \quad \square$$

In practice one finds a useful factor $P_{22}(T)$ of $P_2(T)$ by looking at the algebraic cycles on $\mathscr{X}_p/\bar{\mathbb{F}}_p$ (12.2.1).

Part III

In this third part of the paper we present a few concrete examples. In our work on these examples we were strongly guided by the explicit equations in the paper of Beauville [4], classifying semi-stable elliptic pencils over $\mathbb{P}^1$ with four singular fibres, by the paper of Shioda and Inose [27] on complex $K3$-surfaces with Picard number 20 and by discussions with Peters about double covers of $\mathbb{P}^2$, branched along a singular sextic curve.

The sections hereafter are organized as follows. In Sect. 8 we describe three $K3$-surfaces. In Sect. 9 we give elliptic pencils on these surfaces and in Sect. 10 we solve the corresponding Picard-Fuchs equations, without first explicitly determining these differential equations. For the sake of completeness we determine in Sect. 11 the Picard-Fuchs equations of the given elliptic pencils. Section 12 is devoted to the zeta-functions of the three $K3$-surfaces. In Sect. 13 we give the resulting congruences for the coefficients of the solutions of the Picard-Fuchs equations. Finally, in Sect. 14 we present a connection with modular forms.

8

The surfaces we want to consider, arise as smooth complete models of branched double covers of $\mathbb{P}^2$, with branch locus equal to a curve of degree six. For the ground field we allow any field of characteristic different from 2. Table 1 lists the names of the surfaces and the corresponding branch loci; for pictures see Fig. 1.

Table 1

Surface	Branch locus in $\mathbb{P}^2$
$\mathscr{A}$	$XYZ(X-Y)(Y-Z)(Z-X)=0$
$\mathscr{A}'$	$XYZ(X-Y)(XY-Z^2)=0$
$\mathscr{B}$	$XYZ(X+Y)(Y+Z)(Z+X)=0$
$\mathscr{C}$	$XYZ(X+Y+Z)(XY+YZ+ZX)=0$

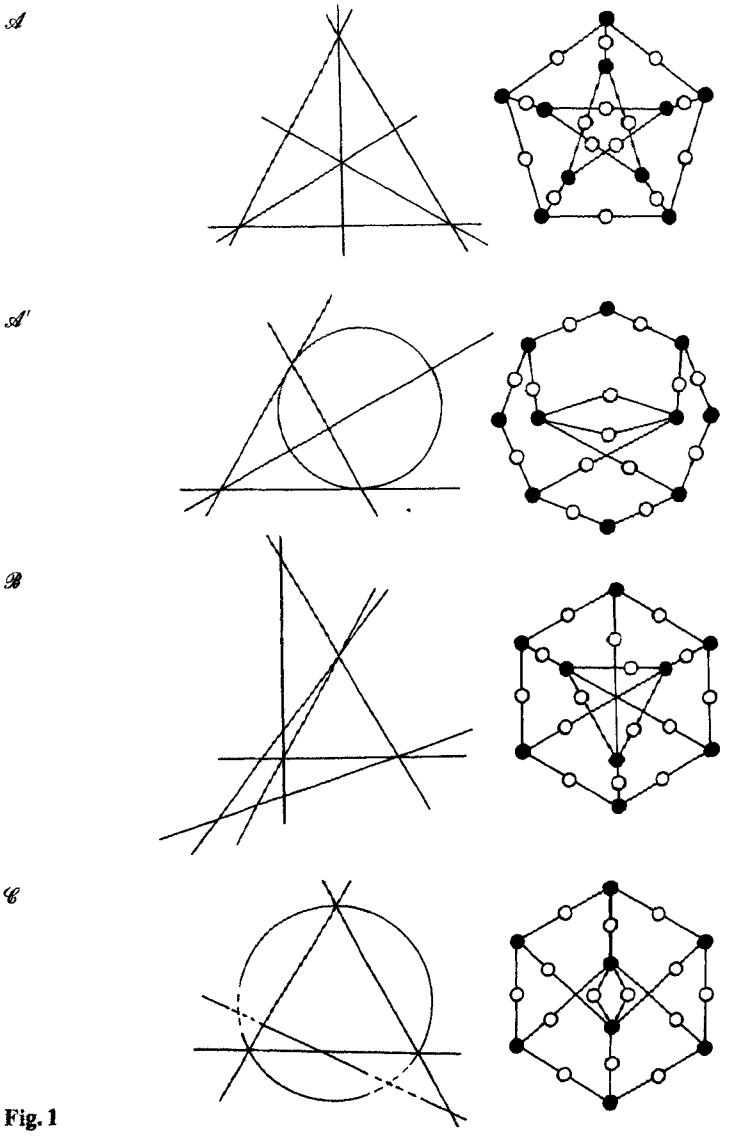

Fig. 1

For these singular sextics the smooth complete model of the corresponding branched double cover of $\mathbb{P}^2$ can be constructed as follows (also see [3]). First blow up $\mathbb{P}^2$ at the triple points of the curves. Except for case $\mathscr{A}'$, the total transform of the branch locus has only ordinary double points. In case $\mathscr{A}'$ the total transform has still two triple points and we blow these up again to get a total transform with only ordinary double points. So now we have in all cases a total transform with only double points. Its components have, however, odd multiplicities. We must blow up the double points in order to get a total transform of the original branch locus whose only singularities are double points, at which a component of odd and one of even multiplicity meet. In Fig. 1 we have depicted beside the original branch loci also the dual graphs of their total transforms after the above blowing up process; the vertices •, respectively ○, correspond to components of odd, respectively even, multiplicity. The desired smooth surface is then the double cover of the blown up $\mathbb{P}^2$, with branch locus consisting of all components of odd multiplicity of the total transform of the original sextic curve (i.e. the •'s).

Let $\mathscr{X}$ be any of the surfaces $\mathscr{A}$, $\mathscr{A}'$, $\mathscr{B}$, $\mathscr{C}$. Let $\mathscr{D}$ be the corresponding sextic curve in $\mathbb{P}^2$ and let $\phi: \mathscr{X} \to \mathbb{P}^2$ be the natural morphism. Then $\phi^{-1}(\mathscr{D})$ is a union of rational curves, each with self-intersection -2, meeting exactly as described by the graphs in Fig. 1 [each vertex, • as well as ○, represents a component of $\phi^{-1}(\mathscr{D})$]. Furthermore, $\mathscr{X} \setminus \phi^{-1}(\mathscr{D})$ is a smooth affine surface in $\mathbb{A}^3$, for which we fix the following equations:

$$
\begin{aligned}
&\text{for } \mathscr{A}: \quad s^2 = xy(x-y)(y-1)(1-x)\\
&\text{for } \mathscr{A}': \quad s^2 = xy(x-y)(xy-1)\\
&\text{for } \mathscr{B}: \quad s^2 = -xy(x+y)(y+1)(1+x)\\
&\text{for } \mathscr{C}: \quad s^2 = xy(x+y+1)(xy+y+x).
\end{aligned}
\tag{8.1}
$$

To see that these surfaces are $K3$-surfaces one may consult the general theory in [3], or check that the Weierstrass equations in Table 3 satisfy the criteria of Sect. 4.

(8.2) *Remark.* The graph in case $\mathscr{A}'$ is exactly the dual graph of the picture at the bottom of p. 131 in [27]. The graph in case $\mathscr{A}$ also appears in [31]. We shall see in Sect. 12 that (over $\mathbb{C}$) the surfaces $\mathscr{A}'$ and $\mathscr{A}$ are indeed isomorphic to the $K3$-surface with Néron-Severi lattice of rank 20 and discriminant 4.

(8.3) **Proposition.** *The surfaces $\mathscr{A}'$ and $\mathscr{A}$ are isomorphic over every field of characteristic different from 2.*

Proof. Consider the birational quadratic transformation on $\mathbb{P}^2$ given by

$$(X, Y, Z) \mapsto (YZ - Z^2, XZ - Z^2, XY - Z^2)$$

It transforms the branch locus for $\mathscr{A}'$ to that for $\mathscr{A}$. [Notice here that the transformation blows up the points $(1,1,1)$, $(1,0,0)$, and $(0,1,0)$, and that of these points the first one is a double point of the branch locus and that the other two are triple points. So the exceptional curves coming from $(1,0,0)$ and $(0,1,0)$ are components of the transformed branch locus.] Thus we see that $\mathscr{A}'$ and $\mathscr{A}$ are birationally equivalent. Being $K3$-surfaces they are therefore isomorphic. □

Table 2

Surface	Family of cubics on $\mathbb{P}^2$
$\mathscr{A}'$	$XYZ-\tau(X-Y)(XY-Z^2)=0$
$\mathscr{A}(1)$	$XYZ-\tau(X-Y)(Y-Z)(Z-X)=0$
$\mathscr{A}(2)$	$X(Y-Z)(Z-X)-\tau(X-Y)YZ=0$
$\mathscr{B}$	$XYZ+\tau(X+Y)(Y+Z)(Z+X)=0$
$\mathscr{C}$	$XYZ-\tau(X+Y+Z)(XY+YZ+ZX)=0$

(τ is the parameter of the family, X, Y, Z are homogeneous coordinates on $\mathbb{P}^2$)

9

There are various ways for constructing elliptic pencils on the surfaces $\mathscr{A}, \mathscr{A}', \mathscr{B}, \mathscr{C}$. The pencils we want to consider here are all obtained from families of cubic curves on $\mathbb{P}^2$, which meet the branch locus correctly so as to lift to the double cover, i.e. on the blown up $\mathbb{P}^2$ (Sect. 8) the proper transform of the generic cubic in the family intersects only components of even multiplicity of the total transform of the branch locus. Table 2 gives a list of the surfaces and of the families of cubics on $\mathbb{P}^2$, which we want to use.

With exception of the first family in case $\mathscr{A}$, these equations have been taken from Beauville's list of stable families of cubics over $\mathbb{P}^1$ [4]. We refer to loc. cit. for their modular interpretation. If one blows up the nine (possibly infinitely near) base points of the families in Table 2, one finds elliptic pencils lying on rational surfaces. Our $K3$-surfaces are double covers of these rational surfaces, branched along two of the four singular fibres. In down to earth terms this means that in the equations the parameter τ is replaced by t^2; or also that the pencil on the $K3$-surface $\mathscr{X}$ ($=\mathscr{A}', \mathscr{A}, \mathscr{B}$ or $\mathscr{C}$) is given by the morphism $\mathscr{X}\to\mathbb{P}^1$ which on the affine part with Eq. (8.1) is described by $t=xys^{-1}$ [respectively, for the second pencil on $\mathscr{A}$ by $t=x(y-1)(1-x)s^{-1}$].

Remark. In cases $\mathscr{B}$ and $\mathscr{C}$ we use in fact the same family of cubics; indeed, replacing in case $\mathscr{B}$ τ by $\tau/(\tau-1)$ one finds the equation of case $\mathscr{C}$. But, when $\mathscr{B}$ and $\mathscr{C}$ are constructed as "branched double covers of this family", the branching occurs

Table 3

$\mathscr{A}'$	$X=U^2-VW$, $Y=U^2$, $Z=t^{-2}UV$; $V^2W+UVW+t^4VW^2=U^3+t^4U^2W$.
$\mathscr{A}(1)$	$X=VW-U^2$, $Y=-t^2UW-U^2$, $Z=-t^{-2}UV-U^2$; $V^2W+UVW-t^4VW^2=U^3$.
$\mathscr{A}(2)$	$X=-t^2VW$, $Y=-t^2UW+U^2$, $Z=-UV$; $V^2W+(1-t^2)UVW-t^2VW^2=U^3-t^2U^2W$.
$\mathscr{B}$	$X=t^2UW+U^2$, $Y=VW-U^2$, $Z=t^{-2}UV+U^2$; $V^2W+(1+2t^2)UVW+t^4VW^2=U^3$.
$\mathscr{C}$	$X=t^2(t^2-1)UW+U^2$, $Y=-(t^2-1)VW-U^2$, $Z=-t^{-2}UV+U^2$; $V^2W+(1-3t^2)UVW-t^4(t^2-1)VW^2=U^3$.

along different singular fibres. The surfaces $\mathscr{B}$ and $\mathscr{C}$ are not isomorphic, as we shall clearly see in Sect. 12.

It turns out that each of the five equations in Table 2 can be put in Weierstrass form by means of a quadratic transformation on $\mathbb{P}^2$. Table 3 shows in each case the appropriate transformation and the resulting Weierstrass equation for the pencil on the $K3$-surface (i.e. with t^2 instead of τ).
These Weierstrass equations satisfy the conditions of (6.1). So the results of Parts I and II apply to these five elliptic pencils.

10

We now determine the solutions, which are holomorphic at $t=0$, of the Picard-Fuchs equations of the elliptic pencils listed in Table 2 (with τ replaced by t^2). We work in the complex analytic setting.

Notice that all examples, except $\mathscr{A}(2)$, have equations of the form $XYZ - t^2Q(X, Y, Z)=0$; also $\mathscr{A}(2)$ can be put in this form by substituting $Y'=Y-Z$ and $Z'=Z-X$:

$$XY'Z'-t^2(-(Y'+Z')(Z'+X)(X+Y'+Z'))=0\,.$$

Assume $|t|$ sufficiently small and non-zero. Then an argument as in [6, p. 52], involving Poincaré's residue theorem, shows that the integral

$$\frac{1}{2\pi i}\iint_{|x|=|y|=1}\frac{dx\,dy}{xy-t^2Q(x,y,1)} \tag{10.1}$$

is equal to a period of the elliptic curve $XYZ-t^2Q(X, Y, Z)=0$. Hence (10.1) gives a solution of the Picard-Fuchs equation of the pencil in a neighborhood of $t=0$. Its power series expansion is:

$$\frac{1}{2\pi i}\iint_{|x|=|y|=1}\frac{dx\,dy}{xy-t^2Q(x,y,1)}=\sum_{n\geqq 0}t^{2n}\left(\frac{1}{2\pi i}\iint\frac{Q(x,y,1)^n}{x^{n+1}y^{n+1}}\,dx\,dy\right)$$
$$=2\pi i\sum_{n\geqq 0}f_{2n+1}t^{2n}$$

with

$$f_{2n+1}=\text{coefficient of } X^nY^nZ^n \text{ in } Q(X,Y,Z)^n\,.$$

Thus we see that the power series $f(t)=\sum f_{2n+1}t^{2n}$ is the solution of the Picard-Fuchs equation, which is holomorphic at $t=0$ and has $f(0)=1$; that is, the solution we studied in Parts I and II.

Table 4 gives a formula for the coefficients f_{2n+1} of $f(t)$ in each of the five cases. It is quite straightforward to derive these formulas, using the combinatorial identities

$$\sum_k(-1)^k\binom{n}{k}^3=\begin{cases}0 & \text{if } n \text{ is odd}\\ (-1)^m\dfrac{(3m)!}{(m!)^3} & \text{if } n=2m\end{cases}\quad[34,\text{ p. }121]$$

$$\sum_{a+b=C}\binom{A}{a}\binom{B}{b}=\binom{A+B}{C}.$$

Table 4

Pencil	f_{2n+1}
$\mathscr{A}'$	0 if n is odd, $\binom{2m}{m}^2$ if $n=2m$
$\mathscr{A}(1)$	0 if n is odd, $(-1)^m\binom{2m}{m}\binom{3m}{m}$ if $n=2m$
$\mathscr{A}(2)$	$(-1)^n\sum_k\binom{n}{k}^2\binom{n+k}{k}$
$\mathscr{B}$	$(-1)^n\sum_k\binom{n}{k}^3$
$\mathscr{C}$	$\sum_k\binom{n}{k}^2\binom{2k}{k}$

The functions we find in cases $\mathscr{A}'$ and $\mathscr{A}(1)$ are very classical; namely

$$\sum_{m\geqq 0}\binom{2m}{m}^2 t^{4m}=F\left(\frac{1}{2},\frac{1}{2},1;16t^4\right) \tag{10.2.1}$$

$$\sum_{m\geqq 0}(-1)^m\frac{(3m)!}{(m!)^3}t^{4m}=F\left(\frac{1}{3},\frac{2}{3},1;-27t^4\right), \tag{10.2.2}$$

where $F(\frac{1}{2},\frac{1}{2},1;z)$ respectively $F(\frac{1}{3},\frac{2}{3},1;z)$ are the hypergeometric series with parameters 1/2, 1/2, 1 respectively 1/3, 2/3, 1. This result agrees with the fact that Table 3 exhibits these pencils as "fourfold coverings" of the pencils

$$V^2W+UVW+\varrho VW^2=U^3+\varrho U^2W$$

respectively

$$V^2W+UVW+\varrho VW^2=U^3.$$

The Picard-Fuchs equations of the latter two pencils were determined in [25] (fibre combination, up to permutation, $I_1I_4I_1^*$ respectively $I_1IV^*I_3$). The novelty of our result is that $\int F(1/2,1/2,1;16t^4)dt$ and $\int F(1/3,2/3,1;-27t^4)dt$ are the logarithms of 1-parameter formal group laws over $\mathbb{Z}$ [see (3.4); note: the discriminants of the pencils $\mathscr{A}'$ and $\mathscr{A}(1)$ are $t^{16}(16t^4-1)$ and $t^{12}(27t^4+1)$].

11

The Picard-Fuchs equations of the pencils in cases $\mathscr{A}'$ and $\mathscr{A}(1)$ can easily be derived from (10.2). In this section we shall determine the Picard-Fuchs equations of the remaining pencils. Our goal is to derive the recurrence relations given in Table 7. We work again in the complex analytic setting.

Our method works for semi-stable elliptic pencils over $\mathbb{P}^1$, i.e. elliptic pencils, of which all singular fibres are of multiplicative type [this excludes $\mathscr{A}(1)$ because this pencil has a type IV fibre]. Let $\varepsilon:\mathscr{S}\to\mathbb{P}^1$ be a semi-stable elliptic pencil; think of it

as described by a pair of Weierstrass equations like (4.1) and $\overline{(4.1)}$ together with the identification rules of (4.3). Let $\Xi \subset \mathbb{P}^1$ be the set of critical points of the pencil. Assume $\infty \in \Xi$. Put $\Xi^* = \Xi \setminus \{\infty\}$, $\mathscr{S}^* = \mathscr{S} \setminus \varepsilon^{-1}(\infty)$, $\mathbb{A}^1 = \mathbb{P}^1 \setminus \{\infty\}$ ($\approx \mathbb{C}$) and let $\varepsilon^* : \mathscr{S}^* \to \mathbb{A}^1$ be the restriction of ε. The Picard-Fuchs equation of the pencil ε^* has singularities at all points of Ξ (including ∞). The semi-stability hypothesis implies that the j-invariant J has poles at the points of Ξ. Two independent solutions of the Picard-Fuchs equation in a neighborhood of a point $\xi \in \Xi$ can therefore be given by

$$c_4^{-1/4} F\left(\frac{5}{12}, \frac{1}{12}, 1; \frac{1}{J}\right) \quad \text{and} \quad c_4^{-1/4} \log\left(\frac{1}{J}\right) F\left(\frac{5}{12}, \frac{1}{12}, 1; \frac{1}{J}\right) + G$$

with G holomorphic at ξ (1.5); here c_4 is the c_4-invariant of the pencil ε^*. The semi-stability hypothesis implies that $c_4(\xi) \neq 0$ if $\xi \in \Xi^*$, and hence, that the local exponents of the Picard-Fuchs equation at ξ are 0, 0. Near ∞ we have to use the coordinate $\bar{t} = t^{-1}$. By hypothesis we know that the polynomial $\bar{c}_4(\bar{t}) = \bar{t}^{4N} c_4(\bar{t}^{-1})$ (4.3) does not vanish at $\bar{t} = 0$ (i.e. $\deg c_4 = 4N$). So the local exponents of the Picard-Fuchs equation at ∞ are N, N.

Besides the singularities at the points of Ξ, the Picard-Fuchs equation may have apparent singularities (e.g. [15, (16.4)]). Let A be the number of apparent singularities and let Λ be the sum of the local exponents at these points. Then Λ is an integer $\geqq 2A$ (loc. cit.). By Fuch's identity for the local exponents one knows

$$2N - \sharp(\Xi) + \Lambda - A = -2$$

[15, Sect. 15.4]. Thus, in particular, if the pencil ε has $2N+2$ singular fibres, then there are no apparent singularities. This condition is satisfied by the pencils listed in Table 2 (with τ), since they have four singular fibres and $N = 1$, as well as by their double covers (with t^2 instead of τ), which have six singular fibres and $N = 2$.

From now on assume $\sharp(\Xi) = 2N + 2$. Then there are no apparent singularities. Since the local exponents at the points of Ξ are 0, 0, the Picard-Fuchs equation must be of the form

$$\eta'' + \left(\sum_{\xi \in \Xi^*} \frac{1}{t - \xi}\right) \eta' + \left(\sum_{\xi \in \Xi^*} \frac{a_\xi}{t - \xi}\right) \eta = 0 \tag{11.1}$$

[15, Sect. 15.4]. The fact that the equation has a regular singular point at ∞ with local exponents N, N, yields $\sum a_\xi = 0$ and $\sum \xi a_\xi = N^2$. More relations between the a_ξ's can be obtained by substituting the Taylor series expansion of $c_4^{-1/4} F(5/12, 1/12, 1; 1/J)$, in powers of t, into (11.1). Thus one can easily determine the a_ξ's. Of course, if one happens to know the first few terms of a power series solution of (11.1) in a neighborhood of 0, like we do in the examples, this information can also be used to determine the a_ξ's.

In Table 5 one finds the location and the number of components of the singular fibres for the pencils listed in Table 2 behind $\mathscr{A}(2)$, $\mathscr{B}$, $\mathscr{C}$ (also see [4]). Table 6 gives the corresponding Picard-Fuchs equations. Note that these results are for the pencils in Table 2 i.e. with τ; for the pencils on the $K3$-surfaces one should replace τ by t^2.

Table 5

Pencil	Singular fibres at	Number of components
$\mathscr{A}(2)$	$\tau=0,\ \infty$, roots of $\tau^2-11\tau-1=0$	5, 5, 1, 1
$\mathscr{B}$	$\tau=0,\ \infty,\ 1,\ -1/8$	6, 3, 2, 1
$\mathscr{C}$	$\tau=0,\ \infty,\ 1,\ 1/9$	6, 2, 3, 1

Table 6

Pencil	Picard-Fuchs equation $\left(\text{note: } ' = \frac{d}{d\tau}\right)$
$\mathscr{A}(2)$	$\tau(\tau^2-11\tau-1)\eta''+(3\tau^2-22\tau-1)\eta'+(\tau-3)\eta=0$
$\mathscr{B}$	$\tau(\tau-1)(8\tau+1)\eta''+(24\tau^2-14\tau-1)\eta'-(8\tau+2)\eta=0$
$\mathscr{C}$	$\tau(\tau-1)(9\tau-1)\eta''+(27\tau^2-20\tau+1)\eta'+(9\tau-3)\eta=0$

Table 7

$u_n=\sum_k \binom{n}{k}^2\binom{n+k}{k}$	satisfies	$(n+1)^2u_{n+1}=(11n^2+11n+3)u_n+n^2u_{n-1}$
$u_n=\sum_k \binom{n}{k}^3$	satisfies	$(n+1)^2u_{n+1}=(7n^2+7n+2)u_n+8n^2u_{n-1}$
$u_n=\sum_k \binom{n}{k}^2\binom{2k}{k}$	satisfies	$(n+1)^2u_{n+1}=(10n^2+10n+3)u_n-9n^2u_{n-1}$

For a power series solution $\sum u_n\tau^n$ such a differential equation is equivalent to a recurrence relation for the coefficients. Thus we find recurrence relations for the numbers of Table 4; see Table 7.

Thus we recover Apéry's recurrence for $\sum\binom{n}{k}^2\binom{n+k}{k}$ and Cusick's recurrence for $\sum\binom{n}{k}^3$ [30, 6]. The third recurrence and its solution are, as far as we know, new.

12

In this section we work over various ground fields. We write therefore $\mathscr{X}/k$ or $\mathscr{X}_k$ when considering the surface $\mathscr{X}$ over the field k. We assume $\operatorname{char} k\neq 2$ and, when dealing with the surface $\mathscr{C}$, also $\operatorname{char} k\neq 3$. When there is no need to distinguish between the surfaces $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$ we call them simply $\mathscr{X}$.

Our objective is to compute the zeta-functions $Z(\mathscr{A}/\mathbb{F}_p;T)$ and $Z(\mathscr{B}/\mathbb{F}_p;T)$ for p prime $\neq 2$ and $Z(\mathscr{C}/\mathbb{F}_p;T)$ for $p\neq 2,3$. Recall

$$Z(\mathscr{X}/\mathbb{F}_p;T)=1/((1-T)(1-p^2T)P_2(T)) \tag{12.1}$$

Table 8. (k algebraically closed)

Pencil	Fibre combination	Discriminant	#sections
$\mathscr{A}_t(2)$	$\begin{pmatrix} I_{10}I_{10}I_1I_1I_1I_1 & \text{if } \operatorname{char} k \neq 5 \\ I_{10}I_{10}IIII & \text{if } \operatorname{char} k = 5 \end{pmatrix}$	$t^{10}(t^4-11t^2-1)$	$\geqq 5$
$\mathscr{B}_t$	$\begin{pmatrix} I_{12}I_6I_2I_2I_1I_1 & \text{if } \operatorname{char} k \neq 3 \\ I_{12}I_6IIIIII & \text{if } \operatorname{char} k \neq 3 \end{pmatrix}$	$t^{12}(t^2-1)^2(8t^2+1)$	$\geqq 6$
$\mathscr{C}_t$	$I_{12}I_4I_3I_3I_1I_1$	$t^{12}(t^2-1)^3(9t^2-1)$	$\geqq 6$

with $P_2(T) \in \mathbb{Z}[T]$, $\deg P_2(T) = 22$ and $P_2(0) = 1$. First we determine a factor of $P_2(T)$ "coming from algebraic cycles", by looking at an elliptic pencil on $\mathscr{X}/\bar{\mathbb{F}}_p$ ($\bar{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$). Table 8 shows for some of the elliptic pencils taken from Table 2 ($\tau = t^2$) the types of the singular fibres, the discriminants and a lower bound for the group of sections (Recall [20] that type I_1 (respectively II) is a rational curve with an ordinary double point (respectively cusp), that type III has two rational components touching at one point and that I_n, for $n \geqq 2$, is a cycle of n $\mathbb{P}^1$'s. The fibres above $t = 0$ and $t = \infty$ are visible in the graphs of Fig. 1 as the outer and the inner cycle, respectively. The intersections appear in the graphs as the connections between these cycles).

By a theorem of Shioda [26] one knows that, given an elliptic pencil on $\mathscr{X}/\bar{\mathbb{F}}_p$, the algebraic equivalence classes of the fibre, of the zero section and of the components of the singular fibres which do not meet the zero section, are linearly independent elements in the Néron-Séveri group $NS(\mathscr{X}/\bar{\mathbb{F}}_p)$ modulo torsion. From Table 8 we see that this gives a 20-dimensional subspace of $NS(\mathscr{X}/\bar{\mathbb{F}}_p)\otimes\mathbb{Q}$ ($\subset H^2_{\text{cris}}(\mathscr{X}/W(\bar{\mathbb{F}}_p))\otimes\mathbb{Q}$). The action of Frobenius on this space is p times the map induced by the endomorphism of the surface $\mathscr{X}$ itself which raises coordinates to the p^{th} power [14]. One easily sees what this map does to the given basis: all elements are fixed, except for two components of the fibre above $t = \infty$ if $p \equiv 2 \bmod 3$ and $\mathscr{X} = \mathscr{C}$; in the exceptional case the two components are interchanged. Thus we get:

$$P_2(T) = (1-pT)^{19}(1-\varepsilon pT)P_{21}(T) \tag{12.2.1}$$

with

$$\begin{aligned} \varepsilon &= -1 \quad \text{if } p \equiv 2 \bmod 3 \text{ and } \mathscr{X} = \mathscr{C} \\ &\quad +1 \quad \text{otherwise.} \end{aligned} \tag{12.2.2}$$

The factor $P_{21}(T)$ is a quadratic polynomial in $\mathbb{Z}[T]$. In order to determine this factor we first take a closer look at the complex surface $\mathscr{X}_{\mathbb{C}}$ and then apply a result of Shioda and Inose [27].

Table 8 and [27, (1.2)] show that the Picard number of $\mathscr{X}_{\mathbb{C}}$ ($= \operatorname{rank} NS(\mathscr{X}_{\mathbb{C}})$) is 20, and hence the lattice of transcendental cycles on $\mathscr{X}_{\mathbb{C}}$, $\mathscr{T}_{\mathscr{X}/\mathbb{C}}$, has rank 2. One knows that $\mathscr{T}_{\mathscr{X}/\mathbb{C}}$ is an even positive definite lattice. Table 8 and [27, (1.3)] show that the discriminant of $\mathscr{T}_{\mathscr{X}/\mathbb{C}}$ equals 4 respectively 8 respectively 12 or 3 for $\mathscr{X} = \mathscr{A}$ respectively $\mathscr{B}$ respectively $\mathscr{C}$. Hence the intersection matrix is equivalent to

$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ for $\mathscr{X}=\mathscr{A}$, to $\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$ for $\mathscr{X}=\mathscr{B}$. We shall see later that for $\mathscr{X}=\mathscr{C}$ it is equivalent to $\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}$. According to Shioda and Inose [27] $K3$-surfaces with Picard number 20 are classified by their lattice of transcendental cycles. So for the surfaces $\mathscr{A}_{\mathbb{C}}$ and $\mathscr{B}_{\mathbb{C}}$ we know where they fit into this classification.

The surface corresponding to the lattice $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ is described in [27] as the non-singular complete model of $E_1 \times E_2/\langle\sigma\rangle$ where E_j $(j=1,2)$ is the elliptic curve $y_j^2=x_j^3-x_j$ and σ is the automorphism of order 4 given by

$$\sigma((x_1,y_1),(x_2,y_2))=((-x_1,iy_1),(-x_2,-iy_2)) \quad (i=\sqrt{-1}).$$

The isomorphism of this surface with our $\mathscr{A}'_{\mathbb{C}}$, and hence with $\mathscr{A}_{\mathbb{C}}$ [cf. (8.3)], is easily described as follows. Consider the affine surface $\mathscr{A}'_0$ in $\mathbb{C}^3$ given by the equation $s^2=xy(x-y)(xy-1)$. Then $\mathscr{A}'_{\mathbb{C}}$ is the non-singular completion of $\mathscr{A}'_0$ (8.1). Define a rational map $\varphi: E_1 \times E_2 \to \mathscr{A}'_0$ by

$$\varphi((x_1,y_1),(x_2,y_2))=(x_1x_2, x_1/x_2, y_1y_2x_1/x_2)\,(=(x,y,s)).$$

Then φ obviously factors through $E_1 \times E_2/\langle\sigma\rangle$ and induces the desired isomorphism between the non-singular complete models.

Let us take a closer look at the surface $\mathscr{C}$. The quadratic transformation on $\mathbb{P}^2$, given by

$$\begin{aligned} U&=\omega YZ+\omega XZ-\omega^2XZ-\omega^2XY \\ V&=\omega YZ+\omega Y^2-\omega^2Y^2-\omega^2XY \\ W&=YZ-\omega^2XY \end{aligned}$$

with ω a primitive cube root of 1, transforms the curve

$$XYZ(X+Y+Z)(XY+YZ+ZX)=0$$

to $(U^3-W^3)(V^3-W^3)=0$. Thus we see that $\mathscr{C}$ is, over any field containing a primitive cube root of 1, isomorphic to the non-singular complete model of the branched double covering of $\mathbb{P}^2$ branched along $(U^3-W^3)(V^3-W^3)=0$; that is, it is isomorphic to the Kummer surface associated with $E \times E$, where E is the elliptic curve $y^2=x^3-1$. Thus we also know where $\mathscr{C}_{\mathbb{C}}$ fits into the classification. It corresponds to $\begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}$ (cf. [27, Theorem 2] and note that $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ is the only even rank 2 lattice of discriminant 3).

Knowing where the surface $\mathscr{X}_{\mathbb{C}}$ fits into the classification of Shioda and Inose, we can use [27, Sect. 6] to compute the zeta-function of $\mathscr{X}/\mathbb{F}_q$, when $\mathbb{F}_q$ is a sufficiently large field of characteristic p. In loc. cit. the zeta-function of $\mathscr{X}/\mathbb{F}_q$ is expressed in terms of the zeta-function of a model of the elliptic curve $C_{\mathscr{X}/\mathbb{C}}$, with

$$C_{\mathscr{A}/\mathbb{C}}=\mathbb{C}/\mathbb{Z}+\mathbb{Z}i, \quad C_{\mathscr{B}/\mathbb{C}}=\mathbb{C}/\mathbb{Z}+\mathbb{Z}\sqrt{-2}, \quad C_{\mathscr{C}/\mathbb{C}}=\mathbb{C}/\mathbb{Z}+\mathbb{Z}\omega$$

$(i=\sqrt{-1}, \omega=(-1+\sqrt{-3})/2)$. The elliptic curve $C_{\mathscr{X}/\mathbb{C}}$ has complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-d})$, where $d=1$ for $\mathscr{X}=\mathscr{A}$, respectively $d=2$ for

$\mathscr{X}=\mathscr{B}$, respectively $d=3$ for $\mathscr{X}=\mathscr{C}$. The curve $C_{\mathscr{C}/\mathbb{C}}$ has a model $C_{\mathscr{X}}$ defined over $\mathbb{Q}$ with good reduction outside the primes dividing $2d$: for instance, take $C_{\mathscr{A}}$: $y^2=x^3-x$, respectively $C_{\mathscr{B}}$: $y^2=x^3-4x^2+2x$, respectively $C_{\mathscr{C}}$: $y^2=x^3+1$ [the curves $C_{\mathscr{A}}$ and $C_{\mathscr{C}}$ are well-known; for $C_{\mathscr{B}}$ see Exercises IV(4.5) and (4.12) in [33] and compare with [13]]. The zeta-function of $C_{\mathscr{X}}/\mathbb{F}_p$ ($p\nmid 2d$) is equal to [21]

$$Z(C_{\mathscr{C}}/\mathbb{F}_p;T)=(1-\pi T)(1-\bar{\pi}T)/(1-T)(1-pT), \tag{12.3.1}$$

where $\pi\bar{\pi}=p$ and

$$\pi=\sqrt{-p} \quad \text{if } p \text{ does not split in } \mathbb{Q}(\sqrt{-d}), \tag{12.3.2}$$

$$\pi \text{ prime in } \mathbb{Q}(\sqrt{-d}) \quad \text{if } p \text{ splits in } \mathbb{Q}(\sqrt{-d}). \tag{12.3.3}$$

At this point it is not necessary for our purpose to remove the ambiguity in π due to the presence of roots of unity in $\mathbb{Q}(\sqrt{-d})$.

As a consequence of (12.3.1) one has for $q=p^r$:

$$Z(C_{\mathscr{X}}/\mathbb{F}_q;T)=(1-\pi^rT)(1-\bar{\pi}^rT)/(1-T)(1-qT). \tag{12.4}$$

Shioda and Inose [27, p. 134] show that for appropriately chosen q one then has

$$Z(\mathscr{X}/\mathbb{F}_q;T)=1/((1-T)(1-qT)^{20}(1-q^2T)(1-\pi^{2r}T)(1-\bar{\pi}^{2r}T)). \tag{12.5}$$

Hence, if $P_{21}(T)$ is as in (12.2) and $P_{21}(T)=(1-\lambda_1T)(1-\lambda_2T)$, then $\lambda_1^r=\pi^{2r}$ and $\lambda_2^r=\bar{\pi}^{2r}$. So, $\lambda_1=\varrho\pi^2$ and $\lambda_2=\pm\bar{\varrho}\bar{\pi}^2$ where ϱ is a root of unity. Note that this absorbs the ambiguity we left in the determination of π.

If p does not split in $\mathbb{Q}(\sqrt{-d})$, then $\pi^2=\bar{\pi}^2=-p$ and the only possibilities for $\lambda_1+\lambda_2$ are 0, $\pm p$, $\pm 2p$, while $\lambda_1\lambda_2$ may be $\pm p^2$ if $\lambda_1+\lambda_2=0$, and $\lambda_1\lambda_2=p^2$ otherwise.

If p splits in $\mathbb{Q}(\sqrt{-d})$, then π^{2r} is a non-rational number lying in the quadratic fields $\mathbb{Q}(\sqrt{-d})$ and $\mathbb{Q}(\lambda_1)$. So $\mathbb{Q}(\lambda_1)=\mathbb{Q}(\sqrt{-d})$, and $\varrho\in\mathbb{Q}(\sqrt{-d})$. Moreover, $\lambda_2=\bar{\varrho}\bar{\pi}^2$ and, hence, $\lambda_1\lambda_2=p^2$. So, if p splits in $\mathbb{Q}(\sqrt{-d})$, we find the following possibilities for $\lambda_1+\lambda_2$:

surface $\mathscr{A}$: let $p=a^2+b^2$, $a,b\in\mathbb{Z}$; then $\lambda_1+\lambda_2=\pm 2(a^2-b^2)$ or $\pm 4ab$.

surface $\mathscr{B}$: let $p=a^2+2b^2$, $a,b\in\mathbb{Z}$; then $\lambda_1+\lambda_2=\pm 2(a^2-2b^2)$.

surface $\mathscr{C}$: let $p=a^2+3b^2$, $a,b,\in\mathbb{Z}$; then

$$\lambda_1+\lambda_2=\pm 2(a^2-3b^2) \quad \text{or} \quad \pm(a^2-6ab-3b^2) \quad \text{or} \quad \pm(a^2+6ab-3b^2).$$

In order to finally remove all ambiguities we estimate the number $^{\sharp}\mathscr{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on the surface $\mathscr{X}$, for $q=p$ and $q=p^2$ (not necessarily the same q as above). From the zeta-function $Z(\mathscr{X}/\mathbb{F}_q;T)$ one gets

$$^{\sharp}\mathscr{X}(\mathbb{F}_q)=1+q^2+19q+\varepsilon^rq+\lambda_1^r+\lambda_2^r \tag{12.6}$$

if $q=p^r$, and ε is as in (12.2.2).

On the other hand, viewing $\mathscr{A}$ as a branched double covering of $\mathbb{P}^2$ one can see a group of order 4 (respectively of order 8 if $q\equiv 1 \bmod 4$) which operates on $\mathscr{A}/\mathbb{F}_q$; namely, the group generated by the automorphism of $\mathscr{A}$ which interchanges the two sheets of the covering and by the automorphism of $\mathscr{A}$ induced by $(X,Y,Z)\mapsto(Z-Y,Z-X,Z)$ in $\mathbb{P}^2$ [respectively and the one induced by $(X,Y,Z)\mapsto(Y,X,Z)$]. The points of $\mathscr{A}/\mathbb{F}_q$ not lying above the branch curve $XYZ(X-Y)(Y-Z)(Z-X)=0$ or the line $X+Y=Z$, have a trivial stabilizer. So,

Table 9

Surface	α_1	α_2	Prime p $(a, b \in \mathbb{Z})$
$\mathscr{A}$	0	$-p^2$	$p \equiv 3 \bmod 4$
	$2p-4a^2$	p^2	$p=a^2+b^2,\ a \equiv 1 \bmod 2$
$\mathscr{B}$	0	$-p^2$	$p \equiv 5$ or $7 \bmod 8$
	$2p-4a^2$	p^2	$p=a^2+2b^2$
$\mathscr{C}$	0	$-p^2$	$p \equiv 5 \bmod 6$
	$2p-4a^2$	p^2	$p=a^2+3b^2$

modulo 4 (respectively modulo 8 if $q \equiv 1 \bmod 4$) the number $^{\#}\mathscr{A}(\mathbb{F}_q)$ is equal to the number of points above the branch curve plus those above the line $X+Y=Z$. The points above the branch curve can easily be counted, especially if one uses the graph of Fig. 1 for book keeping. This number equals $(q+1)$ times the number of •'s plus $(q-1)$ times the number of ○'s; so it is $25q-5$. Above the line $X+Y=Z$ one finds $q-3$ more points if $q \equiv 3 \bmod 4$ (respectively $q-5$ more points if $q \equiv 1 \bmod 4$). Combining this estimate of $^{\#}\mathscr{A}(\mathbb{F}_q)$ with (12.6) we get $\lambda_1+\lambda_2 \equiv 2 \bmod 8$ if $p \equiv 1 \bmod 4$, and $\lambda_1+\lambda_2 \equiv 0 \bmod 4$, $\lambda_1^2+\lambda_2^2 \equiv 2 \bmod 8$ if $p \equiv 3 \bmod 4$. Comparing this result with our previous information about λ_1 and λ_2 we can remove all ambiguity: for $\mathscr{A}/\mathbb{F}_p$ the factor $P_{21}(T)$ equals $(1-p^2T^2)$ if $p \equiv 3 \bmod 4$; it equals $1-2(a^2-b^2)T+p^2T^2$ if $p \equiv 1 \bmod 4$, $p=a^2+b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \bmod 2$.

For the surfaces $\mathscr{B}$ and $\mathscr{C}$ one can argue in the same way, using a group of order 6 which operates on $\mathscr{B}$ and $\mathscr{C}$; namely the group generated by the automorphism which interchanges the sheets of the double covering and by the automorphism induced by $(X, Y, Z) \to (Y, Z, X)$ in $\mathbb{P}^2$. Further details are left to the reader. The result is shown in Table 9, where we have tabulated the coefficients of the polynomial $P_{21}(T)=1+\alpha_1 T+\alpha_2 T^2$ (so, $\alpha_1 = -\lambda_1-\lambda_2$, $\alpha_2=\lambda_1\lambda_2$).

13

Putting together results of Sects. 7, 10, and 12 we obtain:

(13.1) **Theorem.** *Let $\{u_n\}$ be one of the five sequences given by the following expressions*

I $$u_{4m+1}=\binom{2m}{m}^2, \qquad u_{4m-1}=0$$

II $$u_{4m+1}=(-1)^m\binom{2m}{m}\binom{3m}{m}, \qquad u_{4m-1}=0$$

III $$u_{2m+1}=(-1)^m\sum_k\binom{m}{k}^2\binom{m+k}{k}$$

IV $$u_{2m+1}=(-1)^m\sum_k\binom{m}{k}^3$$

V $$u_{2m+1}=\sum_k\binom{m}{k}^2\binom{2k}{k}$$

and in all cases $u_n = 0$ if n is even. Let $M = 4$ in cases I, II, III; *let $M = 2$ in case* IV; *let $M = 3$ in case* V.

Then for every prime number p, not dividing M, and for all $m, r \in \mathbb{N}$ we have the congruences:

$$u_{mp^r} + (2p - 4a^2)u_{mp^{r-1}} + p^2 u_{mp^{r-2}} \equiv 0 \bmod p^r$$

$$\text{if } \left(\frac{-M}{p}\right) = 1 \text{ and } p = a^2 + Mb^2,\ a, b \in \mathbb{Z}$$

$$u_{mp^r} - p^2 u_{mp^{r-2}} \equiv 0 \bmod p^r \quad \text{if} \quad \left(\frac{-M}{p}\right) = -1;$$

here $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi-Legendre symbol. □

(13.2) *Remark.* It turns out that in case V one also has $u_n \equiv 0 \bmod 3^r$ if $n \equiv 0 \bmod 3^r$; see (14.15).

(13.3) *Remark.* The congruences $u_p \equiv 0 \bmod p$ for primes p with $\left(\frac{-M}{p}\right) = -1$ can also be proved directly by means of the symmetry properties of the recurrence relations in Table 7.

(13.4) *Remark.* Note that the expressions I, II, III in (13.1) all three yield for $u_p \bmod p$ the same value, namely $0 \bmod p$ if $p \equiv 3 \bmod 4$ and $\binom{\frac{1}{2}(p-1)}{\frac{1}{4}(p-1)}^2 \bmod p$ if $p \equiv 1 \bmod 4$. The congruences for u_p given in (13.1) for the cases I, II, III follow also immediately from Gauss' $\binom{\frac{1}{2}(p-1)}{\frac{1}{4}(p-1)} \equiv 2a \bmod p$ if $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, $a \equiv 1 \bmod 4$ [9].

(13.5) *Remark.* When one tests the given congruences with actual numbers one discovers that the sequence $\{u_n\}$ in case III satisfies its congruences in fact modulo higher powers of p: we checked, with $m = \frac{1}{2}(p-1)$,

$$\sum_k \binom{m}{k}^2 \binom{m+k}{k} \equiv \begin{cases} 0 \bmod p^2 & \text{if} \quad p \equiv 3 \bmod 4 \\ 4a^2 - 2p \bmod p^2 & \text{if} \quad p = a^2 + 4b^2,\ a, b \in \mathbb{Z} \end{cases}$$

for all primes $p > 3$ and $\leqq 181$. Similar "super congruences" were observed in a few other examples [7], but they do not hold for the cases $\neq$ III of (13.1). Recently, professor Dwork informed us that, using properties of the p-adic Γ-function, he had proved $\binom{-1/2}{\frac{1}{2}(p-1)}^2 \equiv 4a^2 - 2p \bmod p^2$ if $p = a^2 + 4b^2$, p prime, $a, b \in \mathbb{Z}$. At present we have no further explanation for these super congruences. They seem, however, to be important for choosing a formal group law for the formal Brauer group which can also be used in the description of the formal completion of the second Chow group [28, (17.15)].

One can also present a global version of the congruences of (13.1). For these we need the L-series

(13.6) $$L_{\mathfrak{X}}(s) = \prod_p (1 + \alpha_{1,p,\mathfrak{X}} p^{-s} + \alpha_{2,p,\mathfrak{X}} p^{-2s})^{-1}$$

with $\alpha_{1,p,\mathscr{X}}$ and $\alpha_{2,p,\mathscr{X}}$ as tabulated in Table 9 for the prime p and the surface $\mathscr{X}$ ($=\mathscr{A}$, $\mathscr{B}$ or $\mathscr{C}$); we put $\alpha_{1,2,\mathscr{X}}=\alpha_{2,2,\mathscr{X}}=\alpha_{2,3,\mathscr{C}}=0$ and $\alpha_{1,3,\mathscr{C}}=3$.

The global congruences are most elegantly formulated by saying that two elements of the multiplicative group of formal Dirichlet series,

$$\text{(13.7.1)} \qquad \mathrm{DS}^{(0)}=\Big\{\sum_{n\geqq 1} a_n n^{-s} \mid a_n\in\mathbb{Z} \text{ for all } n, a_1=1\Big\},$$

belong to the same coset of the subgroup

$$\text{(13.7.2)} \qquad \mathrm{DS}^{(1)}=\Big\{\sum_{n\geqq 1} a_n n^{-s} \mid a_n\in n\mathbb{Z} \text{ for all } n, a_1=1\Big\}.$$

Then the global version of (13.1) is:

(13.8) **Theorem.** *Let* $\{u_n\}$ *be as in* (13.1) *and* $L_{\mathscr{X}}(s)$ *be as in* (13.6). *Then*

$$\sum_{n\geqq 1} u_n n^{-s}\equiv L_{\mathscr{X}}(s) \text{ modulo } \mathrm{DS}^{(1)},$$

where $\mathscr{X}=\mathscr{A}$ *in cases* I, II, III; $\mathscr{X}=\mathscr{B}$ *in case* IV; $\mathscr{X}=\mathscr{C}$ *in case* V. □

14

In this final section we take a closer look at the L-series $L_{\mathscr{X}}(s)$ of (13.6). Let

$$\begin{aligned}\Phi_4(q)&=q\prod_{n\geqq 1}(1-q^{4n})^6\\ \text{(14.1)}\qquad \Phi_2(q)&=q\prod_{n\geqq 1}(1-q^n)^2(1-q^{2n})(1-q^{4n})(1-q^{8n})^2\\ \Phi_3(q)&=q\prod_{n\geqq 1}(1-q^{2n})^3(1-q^{6n})^3.\end{aligned}$$

(14.2) **Theorem.** *The Dirichlet series expansion of* $L_{\mathscr{A}}(s)$ *respectively* $L_{\mathscr{B}}(s)$ *respectively* $L_{\mathscr{C}}(s)$ *has the same coefficients as the power series expansion of* $\Phi_4(q)$ *respectively* $\Phi_2(q)$ *respectively* $\Phi_3(q)$.

Proof. We prove the three statements simultaneously, but remark that the result for $\Phi_4(q)$ is in fact already known from [38].

First we notice that, in the notation of [13] and [12],

$$\text{(14.2.1)} \qquad \Phi_M(e^{2\pi iz})\in S_3(\Gamma_0(4M),\varepsilon_M),$$

where the character $\varepsilon_M:(\mathbb{Z}/4M\mathbb{Z})^*\to\{\pm 1\}$ is defined by

$$\varepsilon_M(d \bmod 4M)=\left(\frac{M}{|d|}\right)(-1)^{1/2(d-1)}$$

for $d\in\mathbb{Z}$ with $(d,4M)=1$. The proof of (14.2.1) is almost identical with the proof of Theorem 1 in [13], the only difference being that, as the weight of our forms is odd, a sign $(-1)^{1/2(d-1)}$ survives the computations and has to be incorporated in the character.

Obviously, $S_3(\Gamma_0(4M),\varepsilon_M)$ is contained in the space of cusp forms of weight 3 with respect to the group $\Gamma_0(16)\cap\Gamma_1(4)$ if $M=4$, respectively $\Gamma_1(8)$ if $M=2$,

respectively $\Gamma_0(12)\cap\Gamma_1(6)$ if $M=3$. These three spaces of cusp forms are 1-dimensional, as one can see as follows. Note that

$$\Gamma_0(16)\cap\Gamma_1(4)=\begin{pmatrix}4&0\\0&1\end{pmatrix}^{-1}\Gamma_4(4)\begin{pmatrix}4&0\\0&1\end{pmatrix}$$

and

$$\Gamma_0(12)\cap\Gamma_1(6)=\begin{pmatrix}2&0\\0&1\end{pmatrix}^{-1}\Gamma_2(6)\begin{pmatrix}2&0\\0&1\end{pmatrix}$$

in the notation of [35]. The spaces $S_3(\Gamma_4(4))$, $S_3(\Gamma_1(8))$, and $S_3(\Gamma_2(6))$ are 1-dimensional, as is shown by the computations in [35, (3.4), (3.7)] and [12, Theorem (2.25)]. Thus we see

$$\dim S_3(\Gamma_0(4M),\varepsilon_M)=1 \quad \text{for} \quad M=4,2,3\,.$$

Theorem (3.43) of [12] shows now that the Dirichlet series associated with $\Phi_M(q)$ is equal to the Euler product $\prod_p (1-c_M(p)p^{-s}+\varepsilon_M(p)p^{2-2s})^{-1}$ with $c_M(p)$ equal to the coefficient of q^p in the expansion of $\Phi_M(q)$. To finish the proof of Theorem (14.2) one has to check that $-c_M(p)$ and $\varepsilon_M(p)p^2$ coincide with the values of α_1 and α_2 in Table 9. For $\varepsilon_M(p)p^2$ this is clearly correct. To determine $c_M(p)$ one can successfully apply formulas of Jacobi and Macdonald:

$$\eta(X)^3=\sum_{n\equiv 1(4)} nX^{n^2/8} \quad [36,\ (0.7)]$$

$$\eta(X^{1/2})^2\eta(X)^{-1}\eta(X^2)^2=\sum_{n\equiv 1(3)} nX^{n^2/6} \quad [36,\ (6b)\ \text{on p. } 138],$$

where $\eta(X)=X^{1/24}\prod_{n\geq 1}(1-X^n)$ is Dedekind's η-function. One finds indeed $c_M(p)=0$ if $\left(\frac{-M}{p}\right)=-1$ and $c_M(p)=4a^2-2p$ if $\left(\frac{-M}{p}\right)=1$ and $p=a^2+Mb^2$, $a,b\in\mathbb{Z}$; also $c_3(3)=-3$. □

(14.3) **Corollary.** *Let* $\varphi_M(q)=\int \Phi_M(q)q^{-1}dq$ *and*

$$H_M(t_1,t_2)=\varphi_M^{-1}(\varphi_M(t_1)+\varphi_M(t_2))\,.$$

Then $H_M(t_1,t_2)$ *is a formal group law over* $\mathbb{Z}$ *and for every prime number* p, *not dividing* $2M$, $H_M(t_1,t_2)\bmod p$ *is a formal group law for the formal Brauer group of the K3-surface* $\mathscr{X}/\mathbb{F}_p$, *where* $\mathscr{X}=\mathscr{A}$ *if* $M=4$, $\mathscr{X}=\mathscr{B}$ *if* $M=2$, $\mathscr{X}=\mathscr{C}$ *if* $M=3$.

Proof. This follows from (14.2) and the theory explained in Sect. 7 and the appendix. □

We arrived at the conclusion of Corollary (14.3) after first calculating the zeta functions of the surfaces $\mathscr{A},\mathscr{B},\mathscr{C}$, but without invoking our main theorem (6.2). However, as we shall show next, one can derive (14.3) also from (6.2), without calculating zeta functions. This method works also for other subgroups of $\mathrm{Sl}_2(\mathbb{Z})$.

Let Γ be a subgroup of finite index in $\mathrm{Sl}_2(\mathbb{Z})$ satisfying

(14.4) Γ has no elliptic elements; all parabolic elements of Γ have trace 2; $\mu=[\mathrm{PSl}_2(\mathbb{Z}):\Gamma]$ is divisible by 12 and $\mathscr{H}^*/\Gamma$ is a curve of genus 0.

(where $\mathscr{H}$ = complex upper half plane; $\mathscr{H}^* = \mathscr{H} \cup \{i\infty\} \cup \mathbb{Q}$). Attached to Γ is the elliptic modular surface B_Γ [26]. Fix a uniformizing parameter $t = t(z)$ on $\mathscr{H}^*/\Gamma$ and a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{14.5}$$

with coefficients a_i in $\mathbb{C}[t]$, for the canonical elliptic pencil on B_Γ. Because of assumption (14.4) the singular fibers of (14.5) are situated above the points $t(c)$ with c a cusp of Γ and the fiber above $t(c)$ is of type $I_{\nu(c)}$, where $\nu(c)$ is the width of the cusp c i.e. the ramification index of the map $\mathscr{H}^*/\Gamma \to \mathscr{H}^*/\mathrm{Sl}_2(\mathbb{Z})$ at c. Moreover, the discriminant $\Delta(t)$ of (14.5) is $\prod_c (t - t(c))^{\nu(c)}$ where the product is taken over a full set of inequivalent cusps of Γ, except possibly one where $t(z)$ has a pole. If $t(z)$ is finite at all cusps, then the degree of $\Delta(t)$ equals μ.

For $z \in \mathscr{H}$, the fiber of (14.5) above $t(z)$ is, by construction of B_Γ, isomorphic to the elliptic curve with period lattice $\mathbb{Z} \oplus \mathbb{Z}z$. A Weierstrass model for the latter curve is

$$Y^2 = 4X^3 - g_2(z)X - g_3(z), \tag{14.6}$$

in which $g_2(z)$ and $g_3(z)$ are the standard Eisenstein series of weight 4 and 6 respectively. The discriminant of (14.6) is equal to $\eta(z)^{24} = q \prod_{n \geqq 1} (1-q^n)^{24}$ with $q = e^{2\pi i z}$. Tate's formulas [29] show that passing from (14.6) to (14.5) multiplies the canonical 1-form, and hence the period lattice, with $\eta(z)^2 \Delta(t(z))^{-1/12}$. Here it should be noticed that the zeros and poles of $\Delta(t(z))$ are located in the cusps or have order divisible by 12, and that therefore $\Delta(t(z))^{1/12}$ can be chosen to be a one-valued holomorphic function on $\mathscr{H}$.

(14.7) **Theorem.** *If* (14.4) *is satisfied, then* $\eta(z)^2 \Delta(t(z))^{-1/12}$ *is a modular form of weight one with respect to* Γ. *It has a zero of order* $\mu/12$ *at the points* $z \in \mathscr{H}^*$ *for which* $t(z) = \infty$.

Proof. Put $G(z) = \eta(z)^2 \Delta(t(z))^{-1/12}$. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ one has, in view of the transformation behavior of $\eta(z)$, $(cz+d)^{-1} G(Az) = v(A) G(z)$, with $v(A)$ a twelfth root of unity independent of z. On the other hand, the lattices $G(z)(\mathbb{Z} \oplus \mathbb{Z}z)$ and $(cz+d)^{-1} G(Az)(\mathbb{Z} \oplus \mathbb{Z}z)$ are equal, since both equal the period lattice of the fiber of (14.5) above $t(z) = t(Az)$. Since this holds for all $z \in \mathscr{H}$, we must have $v(A) = 1$. So $G(z)$ transforms under Γ as a modular form of weight one.

Next we check that $G(z)$ is holomorphic at the cusps of Γ, i.e. $(-cz+a)G(z)$ is in the neighborhood of a/c a holomorphic function of the local parameter

$$q = \exp(2\pi i v^{-1}(dz - b)(-cz + a)^{-1}),$$

where v is the width of the cusp a/c and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$. If $t(a/c) \neq \infty$, then $(-cz+a)^{12} \eta(z)^{24}$ and $\Delta(t(z))$ both depend holomorphically on q and both have a zero of order v. If $t(a/c) = \infty$, then $(-cz+a)^{12} \eta(z)^{24}$ still has a zero of order v, but $\Delta(t(z))$ gets a pole of order $\deg \Delta(t) = \mu - v$. In any case, $(-cz+a)G(z)$ is a holomorphic function of q. If $t(a/c) = \infty$, it even has a zero of order $\mu/12$ at a/c. If

$t(z)$ has a (simple) pole at a point z_0 in $\mathscr{H}$, then $\eta(z)$ is holomorphic and non-zero at z_0, while $\Delta(t(z))$ is meromorphic with a pole of order $\deg \Delta(t) = \mu$. So, $G(z)$ has a zero of order $\mu/12$ at z_0. □

Let as before $G(z) = \eta(z)^2 \Delta(t(z))^{-1/12}$ and let a/c be a cusp of Γ. In the preceding proof it was shown that $(-cz+a)G(z)$ is, in the neighborhood of a/c, a holomorphic function of the local parameter q and also, that $(-cz+a)G(z)$ is a period of the fiber of (14.5) above $t(z)$. The periods of (14.5) are solutions of the Picard-Fuchs equation associated with the pencil (14.5), and in the neighborhood of $t(a/c)$ there is, up to scalar multiples, exactly one such which is holomorphic. Let $f(t)$ be such a holomorphic non-zero solution. Then:

$$f(t(z)) = \lambda(-cz+a)\eta(z)^2 \Delta(t(z))^{-1/12} \tag{14.8}$$

with $\lambda \in \mathbb{C}$.

(14.9) **Theorem.** *Assume* (14.4). *Let a/c be a cusp of Γ and let $f(t)$ be a holomorphic non-zero solution near $t(a/c)$ of the Picard-Fuchs equation of* (14.5). *Let N be a positive integer such that $\Gamma \subset \Gamma_0(N)$ and let $b, d \in \mathbb{Z}$ be such that $ad - bc = 1$. Define the function $r(z)$ on $\mathscr{H}^*$ by*

$$r(z) = t((aNz+b)/(cNz+d)).$$

Set

$$\Gamma' = \begin{pmatrix} aN & b \\ cN & d \end{pmatrix} \Gamma \begin{pmatrix} aN & b \\ cN & d \end{pmatrix}^{-1}$$

which is again a subgroup of index μ in $\mathrm{Sl}_2(\mathbb{Z})$. Then:

(i) *$r(z)$ is a modular function with respect to Γ'.*

(ii) *$f(r(z))$ is a modular form of weight one with respect to Γ'.*

(iii) *If $\mu \geqq 24$, then $f(r(z))\dfrac{dr(z)}{dz}$ is a cusp form of weight three with respect to Γ'.*

Proof. (i) follows from the fact that $t(z)$ is a modular function with respect to Γ. (ii) is an easy consequence of (14.7) and (14.8). (iii). It follows from (i) and (ii) that $f(r(z))\dfrac{dr(z)}{dz}$ transforms like a cusp form of weight 3. It is holomorphic on $\mathscr{H}^*$, because $f(r(z))$ has a zero of order $\dfrac{\mu}{12} \geqq 2$ at the points where $r(z)$ has a (simple) pole. Vanishing at the cusps is also easily checked. □

Assume from now on besides (14.4) also

(14.10.1) $\mu = 24$

(14.10.2) the function $r(z)$ of (14.9) admits in the neighborhood of $i\infty$ a power series expansion in the local coordinate $q = e^{2\pi i z/\nu}$ with coefficients in $\mathbb{Z}$, constant term 0 and linear term q (ν is the width of the cusp $i\infty$ of Γ')

(14.10.3) the coefficients a_i of (14.5) lie in $\mathbb{Z}[t]$ and satisfy the conditions (0.1) and (0.2)

(14.10.4) the function $f(t)$ in (14.9) is chosen so that $f(0) = 1$.

The hypotheses (14.4) and (14.10.1) imply that the space of cusp forms of weight 3 for Γ' is 1-dimensional and that B_Γ is a $K3$-surface with Picard number 20 (see [12] and [26]). Hypotheses (14.10.3/4) ensure that that the results of Parts I and II of this paper apply to the model (14.4) of B_Γ and to the function $f(t)$. Finally, (14.10.2) allows one to rewrite (14.9)(iii) as

$$f(\psi(q))d\psi(q) = \Phi(q)\frac{dq}{q} \tag{14.11}$$

in which, upon substituting $q = e^{2\pi i z/\nu}$, $\Phi(q)$ is a cusp form of weight 3 with respect to Γ' and $\psi(q) = r(z)$.

Relation (14.11) expresses that $\psi(q)$ is an isomorphism between the formal group laws with logarithms $\int f(t)dt$ and $\int \Phi(q)q^{-1}dq$, respectively. Theorem (6.2) states that the first group law, reduced modulo p, is a group law for the formal Brauer group of $B_\Gamma/\mathbb{F}_p$ (assuming good reduction at p). From the above discussion we can now conclude:

(14.12) **Theorem.** *Let the assumptions and notations be as in* (14.4)–(14.11). *Then the formal group law with logarithm* $\int \Phi(q)q^{-1}dq$ *is, after reduction modulo p, a group law for the formal Brauer group of the K3-surface* $B_\Gamma/\mathbb{F}_p$ *(assuming good reduction at p).* □

In [37] Oda also investigates the connection between certain cusp forms of weight 3 and the formal Brauer groups of the appropriate elliptic modular surfaces. His results are only formulated for the principal congruence subgroups of $\mathrm{Sl}_2(\mathbb{Z})$, but, on the other hand, his methods, which are completely different from ours, do not require that the surface is a $K3$-surface, or that the base curve has genus 0. Moreover, they provide similar connections between cusp forms of higher weights and higher Artin-Mazur formal groups of certain varieties. Theorem (14.12) shows such results also for a few other subgroups of $\mathrm{Sl}_2(\mathbb{Z})$, at least for forms of weight 3. It may be quite well possible that our method also generalises to higher dimensions, but we have not yet studied this question.

Let us return to the examples. By considering the way in which the pencils $\mathscr{A}'$ and $\mathscr{C}$ were constructed from some of Beauville's pencils (see Sect. 9 and [4]) and the modular interpretation of the latter, one can easily see that the surfaces $\mathscr{A}$ and $\mathscr{C}$, equipped with the pencils $\mathscr{A}'$ respectively $\mathscr{C}$ given in Table 2 ($\tau = t^2$), are in fact the elliptic modular surfaces associated with the groups $\Gamma_0(16)\cap\Gamma_1(4)$ respectively $\Gamma_0(12)\cap\Gamma_1(6)$. As for $\mathscr{B}$, this surface should carry an elliptic pencil exhibiting it as the elliptic modular surface for $\Gamma_1(8)$. Unfortunately this pencil seems not visible in our model of $\mathscr{B}$.

In order to apply (14.9) and (14.11) to the pencil $\mathscr{A}'$ and the group $\Gamma_0(16)\cap\Gamma_1(4)$ we take: $\Gamma = \Gamma' = \Gamma_0(16)\cap\Gamma_1(4)$, $\begin{pmatrix} aN & b \\ cN & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 16 & 0 \end{pmatrix}$,

$$r(z) = \eta(16z)^4\eta(4z)^2\eta(8z)^{-6}, \qquad t(z) = r(-1/16z), \qquad q = e^{2\pi i z},$$

$$\begin{cases} \psi(q) = q\prod_{n\geq 1}(1+q^{8n-4})^{-2}(1+q^{8n})^2, \\ \Phi(q) = \Phi_4(q) = q\prod_{n\geq 1}(1-q^{4n})^6 \quad \text{[cf. (14.1), (14.2.1)]} \\ f(t) = F(\tfrac{1}{2},\tfrac{1}{2},1;16t^4) = \sum_{m\geq 0}\binom{2m}{m}^2 t^{4m} \quad \text{[cf. (10.2.1)]}. \end{cases} \tag{14.13}$$

A Weierstrass model for $\mathscr{A}'$ is given in Table 3. It has a singular fiber of type I_{16} at $t=0$, one of type I_4 at $t=\infty$ and four of type I_1 at $t=\pm\frac{1}{2}, \pm\frac{1}{2}i$.

A set of inequivalent cusps of $\Gamma_0(16)\cap\Gamma_1(4)$ is $0, \frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, i\infty$ and the width of the cusp is 16, 4, 1, 1, 1, 1 respectively. One easily checks that $r(z)$ is a modular function for $\Gamma_0(16)\cap\Gamma_1(4)$ (cf. the computations in the proof of [13, Theorem 1]). Moreover, the function $t(z)$ maps $0, \frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, i\infty$ to $0, \infty, -\frac{i}{2}, \frac{i}{2}, -\frac{1}{2}, \frac{1}{2}$ respectively. So it matches the cusps and the singular fibers correctly. Therefore the data of (14.13) do satisfy relation (14.11).

Similar considerations apply to the elliptic pencil $\mathscr{C}$ and the group $\Gamma_0(12)\cap\Gamma_1(6) = \Gamma = \Gamma'$. We take

$$r(z)=\eta(12z)^4\eta(2z)^2\eta(6z)^{-2}\eta(4z)^{-4}, \quad t(z)=r(-1/12z),$$

$$\text{(14.14)}\quad \begin{cases} \psi(q)=q\prod_{n\geq 1}(1+q^{6n})^4(1-q^{6n})^2(1+q^{2n})^{-4}(1-q^{2n})^{-2} \\ \Phi(q)=\Phi_3(q)=q\prod_{n\geq 1}(1-q^{2n})^3(1-q^{6n})^3 \quad [(14.1), (14.2.1)] \\ f(t)=\sum_{m\geq 0}\left(\sum_k \binom{m}{k}^2\binom{2k}{k}\right)t^{2m} \quad \text{(Table 4)}. \end{cases}$$

Again these data satisfy the relation

$$f(\psi(q))d\psi(q)=\Phi(q)\frac{dq}{q}.$$

(14.15) *Remark.* The resulting isomorphisms between formal groups over $\mathbb{Z}$ provide (alternative) proofs for the congruences of (13.8) for the cases I and V. In particular they yield the congruences mentioned in Remark (13.2), which did not follow from our proof of (13.1) because of the bad reduction of the pencil $\mathscr{C}$ at the prime 3.

Appendix

In this appendix we have assembled a few facts about 1-parameter commutative formal group laws (henceforth abbreviated to 1-CFGL). Hazewinkel's book [10] is our main reference for these matters.

(A.1) Let R be a ring (by which we mean "commutative ring with unit"). A 1-CFGL over R is a power series $G(u,v)$ in $R[\![u,v]\!]$ which satisfies

$$\text{(A.1.1)}\quad \begin{aligned} &G(u,v)\equiv u+v \bmod \deg 2, \\ &G(G(u,v),w)=G(u,G(v,w)), \\ &G(u,v)=G(v,u). \end{aligned}$$

(A.2) The two simplest examples over any ring are the additive 1-CFGL $\mathbb{G}_a(u,v)=u+v$ and the multiplicative 1-CFGL $\mathbb{G}_m(u,v)=u+v+uv$. Other important examples are provided by the power series expansion of the addition law on cubics (elliptic curves); see (A.7).

(A.3) Two 1-CFGL's $G(u,v)$ and $\bar{G}(u,v)$ are said to be isomorphic over R if there exist are power series $\psi(u) \in R[[u]]$ and a unit $a \in R^*$ such that

(A.3.1) $\qquad \psi(u) \equiv au \bmod \deg 2, \qquad \psi(G(u,v)) = \bar{G}(\psi(u), \psi(v))$.

If one can choose $a=1$ then one says that $G(u,v)$ and $\bar{G}(u,v)$ are strictly isomorphic over R.

(A.4) If R is a $\mathbb{Q}$-algebra, then every 1-CFGL $G(u,v)$ over R is strictly isomorphic to $\mathbb{G}_a(u,v)$ (cf. [10, (1.6.2)], [11, Theorem 1]). This means that there is a power series $\ell(u) \in R[[u]]$ such that

(A.4.1) $\qquad \ell(u) \equiv u \bmod \deg 2, \qquad G(u,v) = \ell^{-1}(\ell(u) + \ell(v))$.

(A.5) Following [10] we say that a ring R has characteristic zero (char $R=0$), if the natural map $R \to R \otimes \mathbb{Q}$ is injective.

(A.6) If R is a ring of characteristic 0, one can apply the result of (A.4) to the ring $R \otimes \mathbb{Q}$ and thus show that for every 1-CFGL $G(u,v)$ over R there is a power series $\ell(u) \in R \otimes \mathbb{Q}[[u]]$ for which (A.4.1) holds. It can be shown that $\ell(u)$ has the form $\sum_{n \geq 1} n^{-1} b_n u^n$ with $b_n \in R$ for all n [11, Theorem 1 and Proposition (1.1)]. The series $\ell(u)$, uniquely determined by the 1-CFGL $G(u,v)$, is called the logarithm of $G(u,v)$.

(A.7) For example, the logarithm of $\mathbb{G}_m(u,v)$ is $\log(1+u) = -\sum n^{-1}(-u)^n$. Let us also consider the example of the 1-CFGL associated with the cubic equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

over the ring $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Associated with this cubic is the 1-form $\omega = dx/(2y + a_1x + a_3)$, where $x = X/Z$ and $y = Y/Z$. The 1-form has a power series expansion $\omega = \sum q_n u^{n-1} du$, in terms of the coordinate $u = -X/Y$, with coefficients q_n in R [29]. Then the series $\sum n^{-1} q_n u^n$ is the logarithm of a 1-CFGL over R, and this 1-CFGL is the power series expansion of the group structure on the cubic about the point $(0,1,0)$ [29, 10].

Given such a cubic Weierstrass equation over an arbitrary ring, one obtains its 1-CFGL from the universal case by specialization of the coefficients $a_1, \ldots, a_6$.

In practice one rather works with the logarithm of a 1-CFGL instead of the power series expansion of the 1-CFGL itself. The following theorem gives on the one hand a good criterion for recognizing logarithms of 1-CFGL's and on the other hand it provides interesting conclusions about the coefficients of a series in $R \otimes \mathbb{Q}[[u]]$ if one knows somehow that the series is the logarithm of a 1-CFGL over R (char $R=0$)

(A.8) **Theorem.** *Let p be a prime number and $\mathbb{Z}_{(p)} = \left\{ \dfrac{n}{m} \,\middle|\, n, m \in \mathbb{Z}, p \nmid m \right\}$. Let R be a $\mathbb{Z}_{(p)}$-algebra of characteristic 0, equipped with an endomorphism $\sigma : R \to R$ such that $\sigma(a) \equiv a^p \bmod pR$ for all $a \in R$ (σ is a "lifting of Frobenius"). Let $\ell(u) = \sum_{n \geq 1} n^{-1} b_n u^n$ with all b_n in R and $b_1 = 1$.*

Then the following statements are equivalent.

(i) *$\ell(u)$ is the logarithm of a 1-CFGL over R.*

(ii) $\ell^{-1}(\ell(u) + \ell(v)) \in R[[u,v]]$.

(iii) *There exist elements s_i in R, for $i \in \mathbb{N}$, such that*

$$b_{mp^r} + s_1\sigma(b_{mp^{r-1}}) + ps_2\sigma^2(b_{mp^{r-2}}) + \ldots + p^{r-1}s_r\sigma^r(b_m) \equiv 0 \bmod p^r \qquad (*)$$

for all $m, r \geqq 1$.

(iv) *There exist elements s_i in R, for $i \in \mathbb{N}$, such that $(*)$ holds for all $m, r \geqq 1$ and such that for all $r \geqq 1$*

$$b_{p^r} + s_1\sigma(b_{p^{r-1}}) + ps_2\sigma^2(b_{p^{r-2}}) + \ldots + p^{r-1}s_r\sigma^r(b_1) = 0\,. \qquad (**)$$

Assume furthermore that R is p-adically complete and that b_p is invertible in R. Then the above statements are also equivalent to

(v) *There exists an element H in R such that for all $m, r \geqq 1$*

$$b_{mp^r} \equiv H\sigma(b_{mp^{r-1}}) \bmod p^r \qquad (***)$$

Proof. (i) $\Leftrightarrow$ (ii) by definition [see (A.6)]. The implication (iii) $\Rightarrow$ (ii) is exactly part (i) of the functional equation lemma in [10], while (ii) $\Rightarrow$ (iii) is shown in [10, Proposition (20.1.3)]. The implications (iv) $\Rightarrow$ (iii) and (v) $\Rightarrow$ (iii) are trivial. The proofs of (iii) $\Rightarrow$ (iv) and (iii) $\Rightarrow$ (v) will be given in (A.10) and (A.11). □

(A.9) **Theorem.** *Let p, R, and σ be as in* (A.8). *Let $G(u, v)$ and $\bar{G}(u, v)$ be two* 1-CFGL's *over R with respective logarithms $\ell(u) = \sum n^{-1}b_n u^n$ and $\hbar(u) = \sum n^{-1}c_n u^n$. Let furthermore elements $s_i \in R$ be given, for $i \in \mathbb{N}$, such that formula $(*)$ of* (A.8) *holds for all $m, r \geqq 1$. Then the following statements are equivalent.*

(i) *$G(u, v)$ and $\bar{G}(u, v)$ are strictly isomorphic over R.*

(ii) $\ell^{-1}(\hbar(u)) \in R[\![u]\!]$.

(iii) $c_{mp^r} + s_1\sigma(c_{mp^{r-1}}) + ps_2\sigma^2(c_{mp^{r-2}}) + \ldots + p^{r-1}s_r\sigma^r(c_m) \equiv 0 \bmod p^r$ *holds for all $m, r \geqq 1$.*

Proof. (i) $\Leftrightarrow$ (ii) is obvious; (ii) $\Leftrightarrow$ (iii) is shown in parts (ii) and (iii) of the functional equation lemma.

(A.10) We prove that (A.8)(iii) implies (A.8)(iv). Define the series $\hbar(u) = \sum n^{-1}c_n u^n$ in $R \otimes \mathbb{Q}[\![u]\!]$ by

(A.10.1) $\qquad c_n = b_n$ if n is a power of p, $c_n = 0$ otherwise.

Assume (A.8)(iii) holds. Then (A.9)(iii) is obviously also correct, and therefore $\ell^{-1}(\hbar(u))$ and $\hbar^{-1}(\ell(u))$ are power series with coefficients in R. Looking at the proof of [10, Proposition (20.1.3)] we see that we can find new elements s_i in R such that

(A.10.2) $\qquad c_{mp^r} + s_1\sigma(c_{mp^{r-1}}) + ps_2\sigma^2(c_{mp^{r-2}}) + \ldots + p^r s_r\sigma^r(c_m) = 0$

holds for all $m, r \geqq 1$. (A.10.1) and the implication (ii) $\Rightarrow$ (iii) in (A.9) (with ℓ and $\hbar$ interchanged) now show that with these new s_i's (iv) in (A.8) is satisfied. □

(A.11) We prove (iii) $\Rightarrow$ (v) in (A.8), assuming R p-adically complete and b_p invertible in R. Using the elements s_i of (iii) we construct a sequence

$H_1, H_2, \ldots, H_j, \ldots$ in R such that for all $j \geqq 1$ one has

$$b_{mp^r} \equiv H_j \sigma(b_{mp^{r-1}}) \bmod p^{\min(r,j)} \quad \text{for all } m, r \geqq 1. \tag{1}_j$$

$$H_j \equiv H_{j-1} \bmod p^j \quad (\text{take } H_0 = 1). \tag{2}_j$$

The sequence $\{H_j\}_{j \geqq 1}$ will then converge in R to an element H with the desired property (***).

In view of (*) we take $H_1 = -s_1$. Suppose now we have H_j for which $(1)_j$ and $(2)_j$ hold and let us construct H_{j+1}. First note that $H_1 \equiv b_p \bmod p$, and that therefore $H_1, \ldots, H_j$ are invertible in R. From $(1)_j$ one gets

$$\sigma^i(b_{mp^{r-1}}) \equiv [\sigma(H_j) \cdot \sigma^2(H_j) \cdot \ldots \cdot \sigma^{i-1}(H_j)]^{-1} \sigma(b_{mp^{r-1}}) \bmod p^{\min(r-i+1,\, j)} \tag{3}$$

for all m, r, i with $m \geqq 1$, $r \geqq 1$.

Combining (3) and (*) we get for all $m \geqq 1$ and $r > j$:

$$\begin{aligned} b_{mp^r} &\equiv -s_1 \sigma(b_{mp^{r-1}}) - p s_2 \sigma^2(b_{mp^{r-2}}) - \ldots - p^j s_{j+1} \sigma^{j+1}(b_{mp^{r-j-1}}) \\ &\equiv H_{j+1} \sigma(b_{mp^{r-1}}) \bmod p^{j+1} \end{aligned}$$

with

$$H_{j+1} = -s_1 - \sum_{i=2}^{j+1} p^{i-1} s_i [\sigma(H_j) \cdot \sigma^2(H_j) \cdot \ldots \cdot \sigma^{i-1}(H_j)]^{-1} \tag{4}_j$$

So we have constructed $H_{j+1} \in R$ so that $(1)_{j+1}$ holds. Using $(4)_j$, $(4)_{j-1}$ and $(2)_j$ one can easily check that $(2)_{j+1}$ is also satisfied. The proof of (A.8) (iii) $\Rightarrow$ (v) is complete. □

(A.12) Let k be a perfect field of characteristic $p > 0$, $\mathscr{W}$ its ring of Witt vectors and σ the Frobenius automorphism of $\mathscr{W}$ [10]. The Dieudonné ring $\mathscr{D}$ over k is, by definition, the non-commutative $\mathscr{W}$-algebra with unit, generated by two elements F and V, subject to the rules

$$FV = VF = p, \qquad Fa = \sigma(a)F, \qquad aV = V\sigma(a) \quad \text{for all} \quad a \in \mathscr{W}.$$

For example, if k is the prime field $\mathbb{F}_p$, then $\mathscr{W}$ is the ring of p-adic integers $\mathbb{Z}_p$, σ is the identity map and $\mathscr{D}$ is the (commutative!) ring $\mathbb{Z}_p[F, V]/(FV - p)$.

Cartier-Dieudonné theory assigns to every commutative formal group law G over k a $\mathscr{D}$-module $\mathbb{D}(G)$, called the Cartier-Dieudonné module or covariant Dieudonné module of G or the module of p-typical curves on G [10]. This module is V-adically complete and separated [i.e. $\mathbb{D}(G) = \varprojlim \mathbb{D}(G)/V^n\mathbb{D}(G)$], it has no V-torsion and $\mathbb{D}(G)/V\mathbb{D}(G)$ is a finite dimensional vector space over k.

One of the main theorems in this theory asserts that two formal group laws over k are isomorphic if and only if the corresponding Cartier-Dieudonné modules are isomorphic [10, (27.7.10)].

(A.13) Let k be a perfect field of positive characteristic and let $\bar{G}(u, v)$ be a 1-CFGL over k, not isomorphic to the additive 1-CFGL $\mathbb{G}_a$. Then the Cartier-Dieudonné module $\mathbb{D}(\bar{G})$ is a free $\mathscr{W}$-module of finite rank h (= height of $\bar{G}$; [10, (28.3.10)]). Moreover, $\mathbb{D}(\bar{G})/V\mathbb{D}(\bar{G})$ is a 1-dimensional k-vector space. It follows that $\mathbb{D}(\bar{G})$ has a $\mathscr{W}$-basis of the form $\omega, V\omega, \ldots, V^{h-1}\omega$. Expressing $F\omega$ in terms of this basis

one obtains a relation

$$F\omega = a_1\omega + a_2 V\omega + \ldots + a_h V^{h-1}\omega \tag{A.13.1}$$

with $a_1, \ldots, a_h \in \mathcal{W}$. Now define the sequence $\{b_n\}_{n\geq 1}$ in $\mathcal{W}$ by

$$\begin{aligned} &b_1 = 1,\ b_n = 0 \text{ if } n \text{ is not a power of } p, \\ &b_{p^r} = \sum_{i=1}^{h} p^{i-1}\sigma^{i-1}(a_i)\sigma^i(b_{p^{r-i}}) \quad \text{for} \quad r \geqq 1. \end{aligned} \tag{A.13.2}$$

Then, according to Theorem (A.8), the series $\ell(u) = \sum n^{-1} b_n u^n$ is the logarithm of a 1-CFGL $\tilde{G}(u, v)$ over $\mathcal{W}$. Reducing the coefficients of $\tilde{G}(u, v)$ modulo p one obtains a 1-CFGL over k. The Cartier-Dieudonné module of the latter is isomorphic to $\mathbb{D}(\bar{G})$ (see [10, (26.5.9)]). Hence $\tilde{G}(u, v) \bmod p$ is isomorphic to $\bar{G}(u, v)$.

(A.14) Let $G(u, v)$ be a 1-CFGL over $\mathbb{Z}_p$, with logarithm $\lambda(u) = \sum n^{-1} c_n u^n$. Put $\bar{G}(u, v) = G(u, v) \bmod p$.

If $\bar{G}(u, v)$ is isomorphic to $\mathbb{G}_a$ over $\mathbb{F}_p$, then one must have $c_n \equiv 0 \bmod p^r$ if $p^r | n$ [10, Sect. 5.8] or [11, Theorem 1 and Proposition (1.1)].

Assume henceforth that $\bar{G}(u, v)$ is not isomorphic to $\mathbb{G}_a$. Take a basis of $\mathbb{D}(\bar{G})$ of the form $\omega, V\omega, \ldots, V^{h-1}\omega$ and define $a_1, \ldots, a_h$ in $\mathbb{Z}_p$ by (A.13.1). Now that we are working over $\mathbb{Z}_p$, we have $\sigma = id$ and F is a linear endomorphism of $\mathbb{D}(\bar{G})$ (A.12). Linear algebra therefore shows that $T^h - a_1 T^{h-1} - p a_2 T^{h-2} - \ldots - p^{h-1} a_h$ is the characteristic polynomial of F acting on $\mathbb{D}(\bar{G})$. This gives an intrinsic characterisation of $a_1, \ldots, a_h$. Now construct the 1-CFGL $\tilde{G}(u, v)$ over $\mathbb{Z}_p$ as in (A.13). Then $\tilde{G}(u, v) \bmod p$ is isomorphic, over $\mathbb{F}_p$, to $\bar{G}(u, v) = G(u, v) \bmod p$. According to [10, (22.1.10/11)] this implies that $G(u, v)$ and $\tilde{G}(u, v)$ are strictly isomorphic over $\mathbb{Z}_p$. Combining (A.13.2) and (A.9) we may conclude that for all $m, r \geqq 1$ we have

$$c_{mp^r} - a_1 c_{mp^{r-1}} - p a_2 c_{mp^{r-2}} - \ldots - p^{h-1} a_h c_{mp^{r-h}} \equiv 0 \bmod p^r. \tag{A.14.1}$$

Acknowledgements. We want to thank Chris Peters and Matthijs Coster for inspiring discussions about the examples.

References

1. Artin, M.: Supersingular $K3$-surfaces. Ann. Sci. Ec. Norm. Super. **7**, 543–568 (1974)
2. Artin, M., Mazur, B.: Formal groups arising from algebraic varieties. Ann. Sci. Ec. Norm. Super. **10**, 87–132 (1977)
3. Barth, W., Peters, C., Van de Ven, A.: Compact complex surfaces. Ergebnisse der Mathematik 3. Folge, Bd. 4. Berlin, Heidelberg, New York: Springer 1984
4. Beauville, A.: Les familles stables de courbes elliptiques sur $\mathbb{P}^2$ admettant quatre fibres singulières. C.R. Acad. Sci. Paris **294**, 657 (1982)
5. Berthelot, P., Ogus, A.: Notes on crystalline cohomology. Mathematical Notes 21. Princeton: Princeton University Press 1978
6. Beukers, F.: Irrationality of π^2, periods of an elliptic curve and $\Gamma_1(5)$. In: Approximations diophantiennes et nombres transcendants, Luminy 1982, Progress in Mathematics 31. Basel, Boston, Stuttgart: Birkhäuser 1983
7. Beukers, F.: Arithmetical properties of Picard-Fuchs equations. Sém. de Theorie des Nombres, Paris 1982–1983, Progress in Mathematics 51. Basel, Boston, Stuttgart: Birkhäuser 1984

8. Bombieri, E., Mumford, D.: Enriques classification of surfaces in char. p. II. In: Complex analysis and algebraic geometry (Bailey, Shioda, T., eds.) Cambridge: 1977
9. Gauss, C.: Werke, Band II, pp. 87–91.
10. Hazewinkel, M.: Formal groups and applications. New York: Academic Press 1978
11. Honda, T.: On the theory of commutative formal groups. J. Math. Soc. Japan **22**, 213–246 (1970)
12. Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Iwanami Shoten Publishers and Princeton: Princeton University Press 1971
13. Honda, T., Miyawaki, I.: Zeta-functions of elliptic curves of 2-power conductor. J. Math. Soc. Japan **26**, 362–373 (1974)
14. Illusie, L.: Complexe de De Rham-Witt et cohomologie cristalline. Ann. Sci. Ecol. Norm. Super. **12**, 501–661 (1979)
15. Ince, E.: Ordinary differential equations. New York: Dover 1927
16. Kas, A.: Weierstrass normal forms and invariants of elliptic surfaces. Trans. Am. Math. Soc. **225**, 259–266 (1977)
17. Katz, N.: Expansion coefficients as approximate solutions of differential equations. Cohomologie p-adique. Astérisque 119–120 (1984)
18. Klein, F.: Vorlesungen über die Theorie der elliptischen Modulfunktionen, ausgearbeitet und vervollständigt von R. Fricke. Leipzig 1892
19. Klein, F.: Vorlesungen über die hypergeometrische Funktion. Grundlehren der mathematischen Wissenschaften, Bd. 39. Berlin, Heidelberg, New York: Springer 1981
20. Kodaira, K.: On compact analytic surfaces. II. Ann. Math. **77**, 563–626 (1963)
21. Lang, S.: Elliptic functions. New York: Addison-Wesley 1973
22. Manin, Yu.: Rational points on algebraic curves over function fields. Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963) A.M.S. Transl. Ser. 2, **50**, 189–234
23. Néron, A.: Modèles mininaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S. **21** (1964)
24. Raynaud, M.: Modèles de Néron. C.R. Acad. Sci. Paris Sér. A **262**, 345 (1966)
25. Schmickler-Hirzbruch, U.: Elliptische Flächen über $\mathbb{P}^1\mathbb{C}$ mit drei Ausnahmefasern und die hypergeometrische Differentialgleichung. Diplomarbeit, Universität Bonn 1978
26. Shioda, T.: On elliptic modular surfaces. J. Math. Soc. Japan **24**, 20–59 (1972)
27. Shioda, T., Inose, H.: On singular $K3$-surfaces. In: Complex analysis and algebraic geometry. (Baily, Shioda, T., eds.) Cambridge 1977
28. Stienstra, J.: Cartier-Dieudonné theory for Chow groups. J. Reine Angew. Math. **355**, 1–166 (1985)
29. Tate, J.: The arithmetic of elliptic curves. Invent. Math. **23**, 179–206 (1974)
30. Van der Poorten, A.: A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. Math. Intell. **1**, 195–203 (1978)
31. Vinberg, E.: The two most algebraic $K3$-surfaces. Math. Ann. **265**, 1–21 (1983)
32. Beukers, F.: Une formule explicite dans la théorie des courbes elliptiques. Preprint (1984)
33. Hartshorne, R.: Algebraic geometry. Graduate Text in Mathematics, Vol. 52. Berlin, Heidelberg, New York: Springer 1977
34. MacMahon: Combinatory analysis. New York: Chelsea 1066
35. Cox, D., Parry, W.: Torsion in elliptic curves over $k(t)$. Compositio Math. **41**, 337–354 (1980)
36. Macdonald, I.: Affine root systems and Dedekind's η-function. Invent. Math. **15**, 91–143 (1972)
37. Oda, T.: Formal groups attached to elliptic modular forms. Invent. Math. **61**, 81–102 (1980)
38. Schoeneberg, B.: Über den Zusammenhang der Eisensteinschen Reihen und Thetareihen mit der Diskriminante der elliptischen Funktionen. Math. Ann. **126**, 177–184 (1953)

Received April 18, 1984; in revised form September 17, 1984