# Contents

# Abstract

We consider elliptic curves defined over $\mathbb{Q}$. It is known that for a prime $p > 3$ quadratic twists permute the Kodaira classes, and curves belonging to a given class have the same conductor exponent. It is not the case for $p = 2$ and 3. We establish a refinement of the Kodaira classification, ensuring that the permutation property is recovered by *refined* classes in the cases $p = 2$ and 3. We also investigate the nonquadratic twists. In the last part of the paper we discuss the number of isogeny classes of curves for given conductors of some special forms. Representative numerical data are given in the tables.

*Acknowledgements.* The authors are grateful to the anonymous referee for a very careful reading of the manuscript. His or her detailed remarks made it possible to correct some inaccuracies.

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11G07, 14H52.
*Key words and phrases*: elliptic curves, conductors, twists, Kodaira classification.
Received 12.6.2008; revised version 15.1.2009.

# I. Twists

## 1. Introduction

**1.1. Preliminaries.** We consider elliptic curves $\mathcal{E}$ defined over $\mathbb{Q}$ and their quadratic twists $\mathcal{E} * d$, where $d$ is a squarefree integer. If curves $\mathcal{E}'$ and $\mathcal{E}''$ have the same Kodaira symbols for a prime $p$, it may occur that the Kodaira symbols of their twists $\mathcal{E}' * d$ and $\mathcal{E}'' * d$ are different. For this anomaly to occur it is necessary, but not sufficient, that $p = 2$ or 3.

In the present paper we establish a refinement of the local Kodaira classification of elliptic curves. Twist action on the (finite) set of *refined* classes is well-defined, indeed it defines a permutation in the sense that if curves belong to a common subclass, then their images, under a given twist, will also belong to one, and only one, subclass. Moreover, all the curves in a given subclass have the same local conductor. As a consequence, the behaviour of conductors under a twist is described in subsequent theorems.

Similar topics have been investigated by several authors.

I. Papadopoulos [Pa] considered elliptic curves defined over a discrete valuation ring. Denote by $v$ the valuation, and by $N$ the conductor of an elliptic curve. The most interesting case is when the residue characteristic of $v$ is 2 or 3.

Papadopoulos divided Kodaira classes of elliptic curves into subclasses with the property that $v(N)$ has a fixed value for all curves in a subclass. The subclasses are defined by triples $(v(c_4), v(c_6), v(\Delta))$, where $c_4$, $c_6$ and the discriminant $\Delta$ correspond to a minimal model of a curve, and sometimes by some additional conditions.

Papadopoulos did not investigate twists of elliptic curves.

In the present paper we give a further refinement of the classification of Papadopoulos. Our additional conditions are simplified versions of the original ones, since we consider the curves defined over $\mathbb{Q}$, i.e. the classification is achieved locally over the rings $\mathbb{Z}_p$ of $p$-adic integers.

S. Comalada [Co] divided the Kodaira classes into subclasses using some conditions on the coefficients $b_2, b_4, b_6, b_8$ of a minimal model of an elliptic curve. The subclasses are preserved by twists, in the sense that twists of all curves belonging to a subclass also belong to one subclass.

Thus it would appear that Comalada has already done all the work for this paper! It is not exactly so. The coefficients $b_2, b_4, b_6, b_8$ used by him correspond to a minimal model of a curve, called a $v$-normal model. The definition of a $v$-normal model is given by complicated conditions of Lemma 2 in [Co]. In general a $v$-normal model is not the reduced minimal model (usually used, see Cremona's tables [Cr2]). A $v$-normal model is not unique, and what is given is an explicit algorithm for determining a $v$-normal model from the reduced minimal one (and *vice versa*). Thus to apply the results of Comalada to an elliptic curve given by means of the reduced minimal model, some additional effort is necessary.

Moreover, Comalada did not determine the value of $v(N)$ for curves belonging to his subclass. He only gives the difference $v(N^\chi) - v(N)$, where $N^\chi$ is the conductor of the twisted curve. We, however, determine, for each subclass, both the numbers $v(N^\chi)$ and $v(N)$, and not just their difference.

Therefore the results of the present paper are not a simple translation of the results of Comalada (stated in the language of $v$-normal models) to the reduced minimal models.

Every squarefree integer $d$ can be written uniquely in the form

$$d = \varepsilon\eta p_1^* \cdots p_n^*,$$

where $\varepsilon = \pm 1,\ \eta = 1$ or $2,\ n \geq 0,\ p^* := (-1)^{(p-1)/2} \cdot p$, and $p_1, \ldots, p_n$ are different odd primes. Then the twist by $d$ is the product of the twists by $\varepsilon,\ \eta,\ p_1^*, \ldots, p_n^*$.

For a curve $\mathcal{E}$ its local Kodaira symbol for a prime $p$ does not change under the twist by $d$, provided $\gcd(D, p) = 1$, where $D$ is the discriminant of the field $\mathbb{Q}(\sqrt{d})$. Therefore it is sufficient to consider the following cases: $p = 2,\ d = -1$ or $2$, and $p > 2,\ d = p^*$. We investigate these cases separately in what follows. Next we describe in a similar way the action of nonquadratic twists on the Kodaira classes.

Our considerations are in fact local, and they can be generalized *mutatis mutandis* to elliptic curves defined over an arbitrary discrete valuation ring with a finite residue field.

In the second part of the paper we discuss some questions concerning conductors, and the number of curves with a given conductor. In the tables (based on the Cremona tables [Cr2]) we illustrate these questions giving related numerical data.

**1.2. Notation.** Let

$$E\ :\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad a_j \in \mathbb{Z},$$

be a Weierstrass model of an elliptic curve $\mathcal{E}$. We shall also use the notation $E = [a_1, a_2, a_3, a_4, a_6]$. Let $\Delta(E)$ be the discriminant of this model, and let the letters $b_2, b_4, b_6, b_8, c_4, c_6, j$ have the standard meaning (see the formulas below).

We have

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = (c_4^3 - c_6^2)/12^3, \tag{1.1}$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$$

and

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Finally, $j = c_4^3/\Delta(E)$.

In particular, if $a_1 = a_3 = 0$, i.e. if $E = [0, a_2, 0, a_4, a_6]$, then the above formulas simplify to

$$b_2 = 4a_2, \quad b_4 = 2a_4, \quad b_6 = 4a_6, \quad b_8 = 4a_2a_6 - a_4^2,$$
$$c_4 = 2^4(a_2^2 - 3a_4), \quad c_6 = -2^5(2a_2^3 - 9a_2a_4 + 27a_6).$$

Hence in this case

$$\Delta(E) = 2^4(a_2a_4 + a_6)^2 - 2^6(a_4^3 + a_2^3a_6 + 7a_6^2) + 2^8a_2a_4a_6. \tag{1.2}$$

Denote by $v_p(r)$ the $p$-adic valuation of the rational number $r$. We use the simpler notation $v(r)$ when the prime number $p$ is fixed.

If $p^k \mid a_j$, then we use the convenient notation of Tate $a_{j,k} := a_j/p^k$. We define $b_{j,k}$ and $c_{j,k}$ similarly.

By $N = N(\mathcal{E})$ we denote the conductor of the elliptic curve $\mathcal{E}$.

**1.3. The reduced minimal model of a curve.** Applying to the model $E = [a_1, a_2, a_3, a_4, a_6]$ the substitution

$$X = X' + r, \quad Y = Y' + sX' + t,$$

where $r, s, t \in \mathbb{Z}$, we get the model $E' = [a_1', a_2', a_3', a_4', a_6']$, where

$$a_1' = a_1 + 2s, \quad a_2' = a_2 - sa_1 + 3r - s^2, \quad a_3' = a_3 - ra_1 + 2t,$$

and $c_4' = c_4$, $c_6' = c_6$, hence $\Delta(E') = \Delta(E)$.

It follows that there are unique $r, s, t \in \mathbb{Z}$ such that $a_1', a_3' \in \{0, 1\}$, $a_2' \in \{-1, 0, 1\}$. We call such a model *reduced*.

Thus for every model $E$ there is a unique reduced model $E'$ with the same discriminant.

We call a model $E$ of an elliptic curve $\mathcal{E}$ *minimal* if $|\Delta(E)| \le |\Delta(E')|$ for every model $E'$ of $\mathcal{E}$. Since $\Delta(E') = u^{12}\Delta(E)$ for some positive integer $u$, the discriminant of a minimal model of $\mathcal{E}$ depends only on the curve $\mathcal{E}$. We call it the *discriminant* of the elliptic curve $\mathcal{E}$, and denote it by $\Delta(\mathcal{E})$.

It follows from the above that for every elliptic curve $\mathcal{E}$ there is a unique reduced minimal model.

Every model $E' = [a_1', a_2', a_3', a_4', a_6']$ of $\mathcal{E}$ can be obtained from a minimal one $E = [a_1, a_2, a_3, a_4, a_6]$ by a linear substitution of the form

$$X = u^2X' + r, \quad Y = u^3Y' + u^2sX' + t,$$

where $r, s, t, u \in \mathbb{Z}$, $u \ne 0$. Then

$$c_4' = u^4c_4, \quad c_6' = u^6c_6, \quad \Delta(E') = u^{12}\Delta(E) = u^{12}\Delta(\mathcal{E}).$$

Thus the model $E'$ is minimal iff the scaling factor $u$ satisfies $|u| = 1$.

**1.4. Some important lemmas.** The following well known lemmas will be frequently used in this paper. We include them for the convenience of the reader.

Lemma 1.1.

(i) *If $E = [a_1, a_2, a_3, a_4, a_6]$ is a minimal model of $\mathcal{E}$, then*

$$4 \mid N(\mathcal{E}) \quad \textit{iff} \quad a_1 \equiv a_3 \equiv 0 \pmod 2.$$

(ii) *If* $E = [a_1, a_2, a_3, a_4, a_6]$ *is the reduced minimal model of* $\mathcal{E}$, *then*

$$4 \mid N(\mathcal{E}) \quad \textit{iff} \quad a_1 = a_3 = 0.$$

Proof (J. E. Cremona [Cr1]). (i) It is known [Si1] that $4 \mid N(\mathcal{E})$ iff the reduced curve $E$ (mod 2) has a cusp iff

$$\Delta(E) \equiv c_4 \equiv 0 \pmod 2. \tag{1.3}$$

Since $c_4 = b_2^2 - 24b_4 \equiv b_2 \equiv a_1 \pmod 2$ and $b_6 \equiv a_3 \pmod 2$, we get, by (1.1),

$$\Delta(E) \equiv a_1 b_8 + a_3 + a_1 b_4 b_6 \pmod 2.$$

Consequently, (1.3) holds iff $\Delta(E) \equiv a_1 \equiv 0 \pmod 2$ iff $a_3 \equiv a_1 \equiv 0 \pmod 2$.

(ii) The claim follows from (i), since in the reduced minimal model we have $a_1, a_3 \in \{0, 1\}$. ■

Lemma 1.2. *Let* $E = [0, a_2, 0, a_4, a_6]$. *Then* $2^4 \mid \Delta(E)$, *and moreover*

$$2^4 \parallel \Delta(E) \quad \textit{iff} \quad a_2 a_4 + a_6 \equiv 1 \pmod 2,$$

*and* $2^6 \mid \Delta(E)$ *otherwise.*

*Proof.* The lemma follows directly from (1.2). ■

Lemma 1.3 (A. Kraus). *Let integers* $m, n$ *satisfy* $m^3 - n^2 \neq 0$ *and* $12^3 \mid m^3 - n^2$. *There exists a model* $E = [a_1, a_2, a_3, a_4, a_6]$ *such that* $c_4 = m$ *and* $c_6 = n$ *iff*

(i) $v_3(n) \neq 2$, *and*
(ii) *either* $n \equiv -1 \pmod 4$ *or* $m \equiv 0 \pmod{16}$, $n \equiv 0, 8 \pmod{32}$.

*Proof.* See [Kr, Proposition 2]. ■

Lemma 1.4 (J. E. Cremona). *Let* $c_4$ *and* $c_6$ *correspond to the model* $E = [a_1, a_2, a_3, a_4, a_6]$. *Then the reduced model* $E' = [a'_1, a'_2, a'_3, a'_4, a'_6]$ *of* $E$ *is uniquely determined by* $c_4$ *and* $c_6$.

*Proof* (see [Cr2, p. 46]). It is sufficient to determine consecutively the following integers, taking into account that $c'_4 = c_4$ and $c'_6 = c_6$:

$$\begin{aligned}
&b'_2 \equiv -c_4 \pmod{12}, \qquad b'_2 \in \{-4, -3, 0, 1, 4, 5\},\\
&b'_4 = (b'^2_2 - c_4)/24,\\
&b'_6 = (-b'^3_2 + 36 b'_2 b'_4 - c_6)/216,\\
&a'_1 \equiv b'_2 \pmod 2, \qquad a'_1 \in \{0, 1\},\\
&a'_3 \equiv b'_6 \pmod 2, \qquad a'_3 \in \{0, 1\},\\
&a'_2 = (b'_2 - a'_1)/4,\\
&a'_4 = (b'_4 - a'_1 a'_3)/2,\\
&a'_6 = (b'_6 - a'_3)/4. \ ■
\end{aligned}$$

Lemma 1.5. *Let* $E' = [a'_1, a'_2, a'_3, a'_4, a'_6]$ *and* $E'' = [a''_1, a''_2, a''_3, a''_4, a''_6]$ *be models of curves* $\mathcal{E}'$ *and* $\mathcal{E}''$, *respectively. Then* $\mathcal{E}' = \mathcal{E}''$ *iff*

$$u'^4 c_4(E') = u''^4 c_4(E''), \qquad u'^6 c_6(E') = u''^6 c_6(E'') \qquad \textit{for some } u', u'' \in \mathbb{N}.$$

*Proof.* $\Rightarrow$ Assume that $\mathcal{E}' = \mathcal{E}''$ and let $E = [a_1, a_2, a_3, a_4, a_6]$ be a minimal model of the curve. Then

$$c_4' = u_1^4 c_4, \quad c_6' = u_1^6 c_6 \quad \text{for some } u_1 \in \mathbb{N},$$
$$c_4'' = u_2^4 c_4, \quad c_6'' = u_2^6 c_6 \quad \text{for some } u_2 \in \mathbb{N}.$$

It is sufficient to take $u' = u_2$ and $u'' = u_1$.

$\Leftarrow$ Let $E_1'$ and $E_1''$ be the models obtained from $E'$ and $E''$, respectively, by linear substitutions with the scaling factors $u'$ and $u''$, respectively. Then, by the assumption,

$$c_4(E_1') = u'^4 c_4(E') = u''^4 c_4(E'') = c_4(E_1''),$$

and similarly $c_6(E_1') = c_6(E_1'')$.

Consequently, by Lemma 1.4, the reduced models of $E_1'$ and $E_1''$ are the same. Hence $E_1'$ and $E_1''$ are models of the same curve, thus also $E'$ and $E''$ are models of the same curve. ∎

Lemma 1.6. *Let $E = [a_1, a_2, a_3, a_4, a_6]$ be a model of an elliptic curve $\mathcal{E}$. This model is minimal iff for every $u > 1$ satisfying*

$$u^4 \mid c_4, \quad u^6 \mid c_6, \quad u^{12} \mid \Delta(E) \tag{1.4}$$

*the numbers $m = c_4/u^4$ and $n = c_6/u^6$ do not satisfy at least one of the conditions* (i), (ii) *of Lemma* 1.3.

*Proof.* $\Rightarrow$ Assume that there is $u > 1$ such that (1.4) holds and the numbers $m, n$ defined in the lemma satisfy conditions (i), (ii) of Lemma 1.3.

Then, by Lemma 1.3, there is a model $E' = [a_1', a_2', a_3', a_4', a_6']$ of some elliptic curve $\mathcal{E}'$ such that $c_4' = m$, $c_6' = n$, i.e. $c_4 = u^4 c_4', c_6 = u^6 c_6'$ and $\Delta(E) = u^{12}\Delta(E')$.

From Lemma 1.5 we get $\mathcal{E} = \mathcal{E}'$, which contradicts the minimality of $E$, since $u > 1$.

$\Leftarrow$ If the model $E$ is not minimal, then there is a linear substitution with the scaling factor $u$, $|u| > 1$, such that (1.4) holds, which maps $E$ on a model $E'$ with $c_4' = c_4/u^4$, $c_6' = c_6/u^6$. Hence, by Lemma 1.3, the numbers $m = c_4'$, $n = c_6'$ satisfy the conditions (i), (ii) of this lemma. ∎

## 2. The case $p = 2$ and $d = -1$

**2.1. Table 2.1.** We give a refinement of the Kodaira classification of elliptic curves defined over $\mathbb{Q}$ based on Table IV in [Pa], which we slightly change and adapt to our situation. The set of all curves $\mathcal{E}$ with a fixed Kodaira symbol for $p = 2$ is partitioned into specific classes corresponding to the triples $V(E) = (v(c_4), v(c_6), v(\Delta))$, where $E$ is a minimal model of $\mathcal{E}$. We know that $\Delta \neq 0$, but for some curves it may happen that $c_4 = 0$ or $c_6 = 0$. Since $v(0) = \infty$, the first or the second term in the triple $V(E)$ can be $\infty$.

We denote e.g. by III(5, 7, 8) the class of all curves $\mathcal{E}$ with Kodaira symbol III for $p = 2$ satisfying $v(c_4) = 5, v(c_6) = 7, v(\Delta) = 8$, where $c_4, c_6, \Delta$ correspond to a minimal model of $\mathcal{E}$.

There is an exception: for curves with Kodaira symbol $\mathrm{I}_\nu$, $\nu \geq 0$, we use the nonminimal models given by Lemma 2.1 below.

It turns out that in general there are several classes with the same triple $V(E)$ and with different Kodaira symbols. The additional conditions indicated in the third column of Table 2.1 determine to which class a curve belongs. The notation of the form (3)&(4)′ means that Condition 3 holds, and Condition 4 does not.

For example, the triple $V(E) = (5, 7, 8)$ appears in Table 2.1 only once, so no additional condition is given in the third column and in the corresponding line. On the other hand, the triple $V(E) = (5, 5, 4)$ appears twice in the classes with Kodaira symbols II and III. Condition 1 decides to which class the curve in question belongs. The valuation of the conductor $v(N)$ is the same for all curves in a refined Kodaira class. It is known that $0 \le v(N) \le 8$ (see [Ser] and [LRS]).

**2.2. Additional conditions.** Below we give a more precise description of the contents of Table 2.1. First we state and discuss the additional conditions. In particular, we show which conditions are preserved under the twist by $-1$, and which are not.

From the Tate classification of elliptic curves [Ta] it follows that $4 \nmid N(\mathcal{E})$ iff the Kodaira symbol of $\mathcal{E}$ is $\mathrm{I}_\nu$ for some $\nu \ge 0$. Therefore, by Lemma 1.1, we have $a_1 = a_3 = 0$ for the reduced minimal model of $\mathcal{E}$ iff the Kodaira symbol of $\mathcal{E}$ is not $\mathrm{I}_\nu,\ \nu \ge 0$.

To get $a_1 = a_3 = 0$ also for curves with Kodaira symbol $\mathrm{I}_\nu,\ \nu \ge 0$, we consider the nonminimal models of these curves given by the following lemma.

Lemma 2.1. *If the reduced minimal model $E = [a_1, a_2, a_3, a_4, a_6]$ of a curve $\mathcal{E}$ satisfies $(a_1, a_3) \ne (0, 0)$, then the linear substitution*

$$X' = 4X, \qquad Y' = 8Y + 4a_1X + 4a_3$$

*with the scaling factor $u = 2$ leads to the nonminimal model*

$$E' = [a_1', a_2', a_3', a_4', a_6'] = [0, a_1^2 + 4a_2, 0, 8(a_1a_3 + 2a_4), 16(a_3^2 + 4a_6)]$$

*with $a_1' = a_3' = 0$. Then $c_4' = 2^4c_4,\ c_6' = 2^6c_6,\ \Delta(E') = 2^{12}\Delta(E)$.*

*Proof.* Direct verification. ∎

In view of Lemma 2.1, the classes of curves with Kodaira symbols $\mathrm{I}_\nu,\ \nu \ge 0$, will also be denoted using the nonminimal models:

$$\begin{aligned} &\mathrm{I}_0(0,0,0) = \mathrm{I}_0(4,6,12)', \\ &\mathrm{I}_0(\nu,3,0) = \mathrm{I}_0(4+\nu,9,12)', \quad \nu \ge 4, \\ &\mathrm{I}_\nu(0,0,\nu) = \mathrm{I}_\nu(4,6,12+\nu)', \quad \nu \ge 1, \end{aligned}$$

where the prime ′ indicates that the triple $V(E)$ corresponds to the nonminimal model given in Lemma 2.1.

The models with $a_1 = a_3 = 0$ are very convenient for the investigation of quadratic twists. Namely, if $E = [0, a_2, 0, a_4, a_6]$, then twisting of $E$ by a squarefree integer $d$ gives the model

$$E' := E * d = [0, da_2, 0, d^2a_4, d^3a_6],$$

which is not minimal in general. Hence $c_4' = d^2c_4,\ c_6' = d^3c_6,\ \Delta(E') = d^6\Delta(E)$. Consequently, if $V(E) = (v_1, v_2, v_3)$, then $V(E') = (v_1 + 2\delta, v_2 + 3\delta, v_3 + 6\delta)$, where $\delta = v_p(d) = 0$ or 1, since $d$ is squarefree. In particular, $V(E * (-1)) = V(E)$, since $v_p(-1) = 0$.

Lemma 2.2. *A model $E$ satisfying*

$$\text{(i) } V(E) = (4, 6, \geq 12), \quad \textit{respectively,} \quad \text{(ii) } V(E) = (\geq 8, 9, 12)$$

*is minimal iff*

$$\text{(i) } c_{6,6} \equiv 1 \pmod 4, \qquad \textit{respectively,} \quad \text{(ii) } c_{6,9} \equiv -1 \pmod 4.$$

*Proof.* By Lemma 1.6, the model $E$ is minimal iff there is no model $E'$ with $c_4' = c_4/2^4$, $c_6' = c_6/2^6$, $\Delta(E') = \Delta(E)/2^{12}$.

Obviously $v_3(c_6) = v_3(c_6/2^6)$, hence it is sufficient to consider only the condition (ii) of Lemma 1.3.

(i) From $v(c_6) = 6$ it follows that $c_{6,6}$ is odd. Then, by Lemma 1.3, there is no model $E'$ with $c_6' = c_{6,6}$ iff $c_{6,6} \equiv 1 \pmod 4$.

(ii) From $v(c_4) \geq 8$ we get $c_{4,4} \equiv 0 \pmod{16}$. From $v(c_6) = 9$ we deduce that $c_{6,9} \equiv \pm 1 \pmod 4$. Then, by Lemma 1.3, there is no model $E'$ with $c_4' \equiv 0 \pmod{16}$ and $c_{6,9} \equiv -1 \pmod 4$. ∎

In view of Lemma 2.2, we state

Condition 0. *Assume that $V(E) = (4, 6, \geq 12)$ or $(\geq 8, 9, 12)$. The condition is:*

$$\begin{aligned} c_{6,6} &\equiv 1 \pmod 4 \quad \textit{if} \quad V(E) = (4, 6, \geq 12), \\ c_{6,9} &\equiv -1 \pmod 4 \quad \textit{if} \quad V(E) = (\geq 8, 9, 12). \end{aligned}$$

Condition 0 makes it possible to distinguish the curves in the class:

- $\mathrm{I}_0(4, 6, 12)'$ from those in $\mathrm{I}_4^*(4, 6, 12)$;
- $\mathrm{I}_0(\nu, 9, 12)'$ from those in $\mathrm{II}^*(\nu, 9, 12)$, where $\nu \geq 8$;
- $\mathrm{I}_\nu(4, 6, 12+\nu)'$ from those in $\mathrm{I}_{4+\nu}^*(4, 6, 12+\nu)$, where $\nu \geq 1$.

Thus a curve with a model $E$ satisfying the assumptions of Condition 0 belongs to Case 1 or 2 if it satisfies Condition 0, and to Case $> 2$ otherwise. See Table 2.1.

Lemma 2.3. *A model $E$ satisfies Condition 0 iff the twisted model $E' := E * (-1)$ does not satisfy this condition.*

*Proof.* We have $V(E) = V(E')$ and $c_6 = -c_6'$. Obviously, $c_6$ satisfies Condition 0 iff $-c_6$ does not satisfy it. ∎

This lemma explains the first three lines in Table 2.2.

To state the next additional conditions we need the following notation. For a model $E = [0, a_2, 0, a_4, a_6]$ let

$$\begin{aligned} F(X) &:= X^3 + a_2X^2 + a_4X + a_6, \\ G(X) &:= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8 \\ &= 3X^4 + 4a_2X^3 + 6a_4X^2 + 12a_6X + (4a_2a_6 - a_4^2). \end{aligned}$$

Let us observe that $G'(X) = 12\,F(X) \equiv 0 \pmod 4$.

From the definition of the polynomials $F(X)$ and $G(X)$ for a model $E$ with $a_1 = a_3 = 0$ it follows that if the substitution $X \mapsto X + r$ leads to the model $E^{(r)}$ with the corresponding polynomials $F^{(r)}(X)$ and $G^{(r)}(X)$, then

$$F^{(r)}(X) := F(X+r) \quad \text{and} \quad G^{(r)}(X) := G(X+r).$$

Consequently, the additional conditions stated below, using the polynomials $F(X)$ and $G(X)$, do not depend on the minimal model chosen. Therefore we can apply the conditions to a minimal model chosen arbitrarily.

For the twisted model $E_d := E*d = [0, da_2, 0, d^2a_4, d^3a_6]$ denote by $F_d(X)$ and $G_d(X)$ the corresponding polynomials. Then

$$F_d(dX) = d^3F(X) \quad \text{and} \quad G_d(dX) = d^4G(X).$$

In particular,

$$F_{-1}(X) = -F(-X) \quad \text{and} \quad G_{-1}(X) = G(-X).$$

Choose $w$ satisfying $w \equiv a_4 \pmod 2$. It is easy to verify that $F(w) \pmod 4$ does not depend on the $w$ chosen.

Condition 1. *$F(w) \equiv 2$ or $3 \pmod 4$ for $w \equiv a_4 \pmod 2$.*

Let us observe that

$$F(a_4) = a_4^3 + a_2a_4^2 + a_4^2 + a_6 \equiv a_2a_4 + a_6 \pmod 2.$$

Then, by Lemma 1.2, $F(a_4)$ is odd iff $v(\Delta) = 4$.

Hence Condition 1 can be stated in the following equivalent form:

$$F(a_4) \equiv \begin{cases} 3 \pmod 4 & \text{if } v(\Delta) = 4, \\ 2 \pmod 4 & \text{if } v(\Delta) > 4. \end{cases} \tag{2.1}$$

Let $E$ satisfy $V(E) = (\geq 4, 5, 4)$ or $(4, \geq 7, 6)$. Then $E$ belongs to Case 3 iff Condition 1 is satisfied, and to Case $> 3$ otherwise. For the proof, see [Pa, Proposition 1].

Lemma 2.4. *For a model $E$ let $E' := E * (-1)$ be its twist by $-1$.*

(i) *If $v(\Delta) = 4$, then exactly one of the models $E$ and $E'$ satisfies Condition 1.*
(ii) *If $v(\Delta) > 4$, then $E$ and $E'$ satisfy or do not satisfy Condition 1 simultaneously.*

*Proof.* For both models $E$ and $E'$, $a_4$ is the same, and $a_4 \equiv -a_4 \pmod 2$. Moreover, $\Delta(E) = \Delta(E')$. Then $F_{-1}(a_4) \equiv F_{-1}(-a_4) = -F(a_4) \pmod 4$. Hence $F(a_4) \equiv F_{-1}(a_4) \pmod 4$ iff $F(a_4)$ is even iff $v(\Delta) > 4$. The lemma follows from (2.1). ∎

Condition 1 makes it possible to distinguish curves in the class:

- $\mathrm{II}(4,5,4)$ from those in $\mathrm{III}(4,5,4) \cup \mathrm{IV}(4,5,4)$;
- $\mathrm{II}(5,5,4)$ from those in $\mathrm{III}(5,5,4)$;
- $\mathrm{II}(\nu,5,4)$ from those in $\mathrm{IV}(\nu,5,4)$, where $\nu \geq 6$;
- $\mathrm{II}(4,\nu,6)$ from those in $\mathrm{III}(4,\nu,6)$, where $\nu \geq 7$.

See Table 2.1.

To distinguish curves in the class $\mathrm{III}(4,5,4)$ from those in $\mathrm{IV}(4,5,4)$ the next condition will be applied.

Choose $w$ satisfying $w \equiv a_4 \pmod 2$. It is easy to verify, using $G'(X) \equiv 0 \pmod 4$, that $G(w) \pmod 8$ does not depend on the $w$ chosen, and that $G(w) \equiv 0 \pmod 4$.

CONDITION 2. *$G(w) \equiv 4 \pmod 8$ for $w \equiv a_4 \pmod 2$.*

Assume that $V(E) = (4,5,4)$ and that $E$ belongs to Case $\geq 4$. Then $E$ belongs to Case 4 iff Condition 2 is satisfied. See [Pa, Proposition 2].

LEMMA 2.5. *Assume that $V(E) = (4,5,4)$. Condition 2 is satisfied by a model $E$ iff it is satisfied by the twisted model $E * (-1)$.*

*Proof.* Since $w \equiv -w \equiv a_4 \pmod 2$, we have $G(w) \equiv G(-w) \pmod 8$. The lemma follows from the equality $G_{-1}(w) = G(-w)$. ∎

Condition 2 makes it possible to distinguish curves belonging to the class III$(4,5,4)$ from those in IV$(4,5,4)$. The twist by $-1$ maps both these classes into II$(4,5,4)$. See Table 2.1. This lemma explains lines 4 and 5 in Table 2.2.

To state the next conditions we need the following lemma.

LEMMA 2.6. *Let $V(E) = (4,6,8)$ or $V(E) = (\nu,7,8)$ with $\nu \geq 6$. Then*

(i) *The congruence $G(X) \equiv 0 \pmod{32}$ has a solution $w \equiv a_4 \pmod 2$. Moreover, $G(w') \equiv 0 \pmod{32}$ iff $w' \equiv w \pmod 4$.*

(ii) *Choose $w$ satisfying $G(w) \equiv 0 \pmod{32}$. Then $F(w) \equiv 4 \pmod 8$, and $F(w) \pmod{16}$ does not depend on the $w$ chosen.*

*Proof.* Without loss of generality we can assume that $E = [0, a_2, 0, a_4, a_6]$ is the reduced minimal model, thus $a_2 = 0$ or $\pm 1$.

(i) We consider several cases and subcases. We collect the information on $a_2, a_4, a_6$, and then determine all solutions of $G(X) \equiv 0 \pmod{32}$.

From the definition of $G(X)$ it follows that if $G(w) \equiv 0 \pmod 2$, then $w \equiv a_4 \pmod 2$.

I. Let $V(E) = (4,6,8)$.

(a) Assume that $a_2 = 0$. Then $G(X) = 3X^4 + 6a_4X^2 + 12a_6X - a_4^2$. From $v(c_4) = 4$ and $c_4 = -2^4 \cdot 3\, a_4$ it follows that $a_4$ is odd. From $v(c_6) = 6$ and $c_6 = -2^5 \cdot 3^3\, a_6$ it follows that $a_6 = 2a_{6,1},\ a_{6,1}$ odd. Then

$$\Delta = (c_4^3 - c_6^2)/12^3 = -2^6(a_4^3 + 27a_{6,1}^2)$$

and $v(\Delta) = 8$ implies that $a_4^3 + 27a_{6,1}^2 \equiv 4 \pmod 8$, i.e. $a_4 \equiv 1 \pmod 8$.

Consequently, if $G(w) \equiv 0 \pmod 2$ then $w$ is odd.

For every odd $w$ we have $a_4 + w^2 \equiv 2 \pmod 8$, hence $(a_4 + w^2)^2 \equiv 4 \pmod{32}$. Now

$$G(w) = 3(w^2 + a_4)^2 - 4a_4^2 + 24a_{6,1}w \equiv 3 \cdot 4 - 4 + 24a_{6,1}w \equiv 8(1 + 3a_{6,1}w) \pmod{32}.$$

Hence $G(w) \equiv 0 \pmod{32}$ iff $1 + 3a_{6,1}w \equiv 0 \pmod 4$, iff $w \equiv a_{6,1} \pmod 4$. Thus all solutions of the congruence $G(w) \equiv 0 \pmod{32}$ are given by $w \equiv a_{6,1} \pmod 4$.

(b) Assume that $a_2 = \pm 1$. From $c_4 = 2^4(1 - 3a_4)$ and $v(c_4) = 4$ it follows that $c_{4,4} = 1 - 3a_4$ is odd, i.e. $a_4$ is even, hence $a_6$ is even, by Lemma 1.2. From $c_6 = -2^6(a_2 - 9a_2a_{4,1} + 27a_{6,1})$ and $v(c_6) = 6$ it follows that $c_{6,6} = c_6/2^6 = -(a_2 - 9a_2a_{4,1} + 27a_{6,1})$ is odd, i.e. $a_{4,1} \equiv a_{6,1} \pmod 2$.

We have

$$\Delta = \frac{2^6}{3^3}\,(c_{4,4}^3 - c_{6,6}^2).$$

From $v(\Delta) = 8$ it follows that $c_{4,4}^3 - c_{6,6}^2 \equiv 4 \pmod 8$, hence $c_{4,4} \equiv 5 \pmod 8$. Then $c_{4,4} = 1 - 3a_4$ implies that $a_4 \equiv 4 \pmod 8$, i.e. $a_{4,1} \equiv 2 \pmod 4$, hence $a_{6,1} \equiv 0 \pmod 2$. Therefore $a_{4,1} = 2a_{4,2}$, $a_{4,2}$ odd, and $a_{6,1} = 2a_{6,2}$.

Consequently, if $G(w) \equiv 0 \pmod 2$, then $w$ is even, $w = 2w_1$.

In view of $a_4 \equiv a_6 \equiv 0 \pmod 4$, we have

$$G(w) = G(2w_1) \equiv 16w_1^4 + 16(a_{6,2} + a_{4,2}) \equiv 16(w_1 + a_{6,2} + 1) \pmod{32}.$$

Consequently, $G(2w_1) \equiv 0 \pmod{32}$ iff $w_1 \equiv a_{6,2} + 1 \pmod 2$ iff $w = 2w_1 \equiv a_{6,1} + 2 \pmod 4$.

Thus all solutions of the congruence $G(w) \equiv 0 \pmod{32}$ are given by $w \equiv a_{6,1} + 2 \pmod 4$.

II. Let $V(E) = (\nu, 7, 8)$, $\nu \geq 6$.

(a) Assume that $a_2 = 0$. From $v(c_4) = \nu \geq 6$ and $c_4 = -2^4 \cdot 3\, a_4$ it follows that $4 \,|\, a_4$, $a_4 = 4a_{4,2}$. From $v(c_6) = 7$ and $c_6 = -2^5 \cdot 3^3\, a_6$ it follows that $2^2 \parallel a_6$, i.e. $a_6 = 4a_{6,2}$, $a_{6,2}$ odd.

Hence if $G(w) \equiv 0 \pmod 2$, then $w$ is even, $w = 2w_1$.

In view of $a_4 \equiv a_6 \equiv 0 \pmod 4$, we have

$$G(w) = G(2w_1) \equiv 16w_1^4 - 16a_{4,2}^2 \equiv 16(w_1 - a_{4,2}) \pmod{32}.$$

Consequently, $G(2w_1) \equiv 0 \pmod{32}$ iff $w_1 \equiv a_{4,2} \pmod 2$, i.e. $w \equiv a_{4,1} \pmod 4$.

Thus all solutions of the congruence $G(w) \equiv 0 \pmod{32}$ are given by $w \equiv a_{4,1} \pmod 4$.

(b) Assume that $a_2 = \pm 1$. From $c_4 = 2^4(1 - 3a_4)$ we get $1 - 3a_4 \equiv 4 \pmod 8$ if $v(c_4) = 6$, and $1 - 3a_4 \equiv 0 \pmod 8$ if $v(c_4) > 6$. Hence

$$a_4 \equiv \begin{cases} -1 \pmod 8 & \text{if } v(c_4) = 6, \\ \phantom{-}3 \pmod 8 & \text{if } v(c_4) > 6. \end{cases} \tag{2.2}$$

From $c_6 = -2^5(2a_2^3 - 9a_2a_4 + 27a_6)$ and $v(c_6) = 7$ it follows that $2a_2^3 - a_2a_4 + 3a_6 \equiv 4 \pmod 8$. Hence, by (6),

$$a_6 \equiv \begin{cases} 3a_2 \pmod 8 & \text{if } v(c_4) = 6, \\ -a_2 \pmod 8 & \text{if } v(c_4) > 6. \end{cases} \tag{2.3}$$

From (2.2) it follows that $a_4$ is odd. Hence if $G(w) \equiv 0 \pmod 2$, then $w$ is odd.

For every odd $w$ we have $w^2 - a_4 \equiv 2 \pmod 4$, hence $(w^2 - a_4)^2 \equiv 4 \pmod{32}$.

Moreover, from (2.2) and (2.3) it follows that $3a_4 + a_2a_6 \equiv 0 \pmod 8$ and $a_2 + 3a_6 \equiv \pm 2a_2 \pmod 8$. Consequently, in view of $w^2 \equiv 1 \pmod 8$, we get

$$\begin{aligned} G(w) &= 3(w^2 - a_4)^2 - 4a_4^2 + 4a_2w^3 + 12a_4w^2 + 12a_6w + 4a_2a_6 \\ &\equiv 3 \cdot 4 + 4w(a_2 + 3a_6) - 4 + 4(3a_4 + a_2a_6) \equiv 8(1 \pm a_2w) \pmod{32}. \end{aligned}$$

It follows that $G(w) \equiv 0 \pmod{32}$ iff

$$w \equiv \begin{cases} -a_2 \pmod 4 \\ \phantom{-}a_2 \pmod 4 \end{cases} \equiv \begin{cases} \phantom{-}a_6 \pmod 4 & \text{if } v(c_4) = 6, \\ -a_6 \pmod 4 & \text{if } v(c_4) > 6. \end{cases}$$

For convenience we collect the solutions $w$ of the congruence $G(w) \equiv 0 \pmod{32}$ obtained above. They always satisfy $w \equiv a_4 \pmod 2$, and $w \pmod 4$ is unique.

| Case | $a_2$ | $a_4 \pmod 8$ | $a_6 \pmod 8$ | $w \pmod 4$ | $c_4$ |
|---|---|---|---|---|---|
| I(a) | $0$ | $1$ | $\pm 2$ | $a_{6,1}$ | |
| I(b) | $\pm 1$ | $4$ | $0$ or $4$ | $a_{6,1}+2$ | |
| II(a) | $0$ | $0$ or $4$ | $4$ | $a_{4,1}$ | |
| II(b) | $\pm 1$ | $-1$ | $3a_2$ | $-a_2$ | $v(c_4)=6$ |
| | | $3$ | $-a_2$ | $a_2$ | $v(c_4)>6$ |

(ii) We prove that $F(w) \equiv 4 \pmod 8$ considering the table above case by case.

In the case I(a) we have $w \equiv a_{6,1} \equiv \pm 1 \pmod 4$. Hence

$$F(w) = w^3 + a_4 w + a_6 \equiv w + w + 2a_{6,1} \equiv 2(w + a_{6,1}) \equiv 4 \pmod 8.$$

In the case I(b) we have $a_4 \equiv a_6 \equiv 0 \pmod 4$ and $w \equiv a_{6,1} + 2 = 2(a_{6,2}+1) \pmod 4$ is even. Hence

$$F(w) = w^3 + a_2 w^2 + a_4 w + a_6 \equiv a_2 w^2 + a_6 \equiv 4(1 + a_{6,2})^2 + 4a_{6,2} \equiv 4 \pmod 8.$$

In the case II(a), we have $a_4 \equiv 0 \pmod 4$, $a_6 \equiv 4 \pmod 8$ and $w \equiv a_{4,1} = 2a_{4,2} \pmod 4$ is even. Hence

$$F(w) = w^3 + a_4 w + a_6 \equiv a_6 \equiv 4 \pmod 8.$$

In the case II(b) $w$ is odd. Hence

$$F(w) = w^3 + a_2 w^2 + a_4 w + a_6 \equiv w(1 + a_4) + (a_2 + a_6) \pmod 8.$$

If $v(c_4) = 6$, then we get

$$F(w) \equiv -a_2(1 + a_4) + (a_2 + 3a_2) \equiv 4a_2 \equiv 4 \pmod 8.$$

If $v(c_4) > 6$, then we get

$$F(w) \equiv a_2(1 + a_4) + (a_2 - a_2) \equiv 4a_2 \equiv 4 \pmod 8.$$

Thus $F(w) \equiv 4 \pmod 8$ in every case.

Since the solution $w$ of the congruence $G(X) \equiv 0 \pmod{32}$ is unique modulo 4, to prove the uniqueness of $F(w) \pmod{16}$ it is sufficient to prove that $F(w+4) \equiv F(w) \pmod{16}$.

We have

$$F(w+4) = F(w) + 4(3w^2 + 2a_2 w + a_4).$$

Consequently, to prove the claim it is sufficient to show that

$$3w^2 + 2a_2 w + a_4 \equiv 0 \pmod 4.$$

This can be easily verified considering the above table case by case. ■

Condition 3. *Assume that* $V(E) = (4, 6, 8)$ *or* $V(E) = (\nu, 7, 8)$, *where* $\nu \geq 6$, *and let* $G(w) \equiv 0 \pmod{32}$. *The condition is:* $F(w) \equiv 12 \pmod{16}$.

Assume that $E$ satisfies the assumptions of Condition 3. Then $E$ belongs to Case 6 iff Condition 3 is satisfied, and belongs to Case $> 6$ otherwise. See [Pa, Proposition 3]. See Table 2.1.

Let us remark that our Condition 3 is simpler than that in [Pa]. In our case the congruence $G(X) \equiv 0 \pmod{32}$ always has a solution. Moreover, we need this condition only for some particular triples $V(E)$. It leads to some simplifications in our case. In general it is also possible that sometimes $F(w) \equiv 8 \pmod{16}$.

Lemma 2.7. *Assume that* $V(E) = (4,6,8)$ *or* $(\nu,7,8)$ *with* $\nu \geq 6$, *and let* $E' := E*(-1)$. *Then exactly one of the models* $E$ *and* $E'$ *satisfies Condition* 3.

*Proof.* Let $G(w) \equiv 0 \pmod{32}$, where $w \equiv a_4 \pmod 2$. Then for the twisted model $E'$ the value of $a_4$ is the same, and $F_{-1}(-w) = -F(w)$.

Therefore $F_{-1}(-w) = -F(w) \equiv 4 \pmod 8$, by Lemma 2.6. Consequently, exactly one of the numbers $F(w)$ and $F_{-1}(-w)$ is $\equiv 12 \pmod{16}$. Hence exactly one of the models $E$ and $E'$ satisfies Condition 3. ■

Condition 3 makes it possible to distinguish curves belonging to the class:

- $\mathrm{I}_0^*(6,7,8)$ from those in $\mathrm{I}_1^*(6,7,8)$;
- $\mathrm{I}_0^*(\nu,7,8)$ from those in $\mathrm{IV}^*(\nu,7,8)$, where $\nu \geq 7$;
- $\mathrm{I}_0^*(4,6,8)$ from those in $\mathrm{I}_1^*(4,6,8) \cup \mathrm{IV}^*(4,6,8)$.

See Table 2.1.

The following condition makes it possible to distinguish curves belonging to the class $\mathrm{I}_1^*(4,6,8)$ from those in $\mathrm{IV}^*(4,6,8)$.

Condition 4. *Assume that* $V(E) = (4,6,\nu)$, *where* $\nu \geq 8$. *By Lemma* 2.6, *and Lemma* 3.9, *below, there is* $w \equiv a_4 \pmod 2$ *such that* $G(w) \equiv 0 \pmod{32}$ *and* $w \pmod 4$ *is unique. The condition is:* $a_2 - w \equiv 1 \pmod 4$.

Assume that $E$ belongs to Case $\geq 7$, and satisfies the assumptions of Lemma 2.6. Then $E$ belongs to Case 7 iff Condition 4 is satisfied. See [Pa, Proposition 4].

Lemma 2.8. *If* $E$ *satisfies the assumptions of Condition* 4 *and* $E' := E*(-1)$, *then exactly one of the models* $E$ *and* $E'$ *satisfies Condition* 4.

*Proof.* From $v(c_4) = 4$ it follows that $a_2^2 - 3a_4$ is odd, i.e. $a_2 - a_4$ is odd.

By Lemma 2.6 there is $w \equiv a_4 \pmod 2$ such that $G(w) \equiv 0 \pmod{32}$. Hence $a_2 - w$ is odd. Then $-w \equiv a_4 \equiv a_4' \pmod 2$ and $G_{-1}(-w) = G(w) \equiv 0 \pmod{32}$.

Thus Condition 4 for $E$ says that $a_2 - w \equiv 1 \pmod 4$, and for $E'$ that $a_2' - (-w) = -a_2 + w \equiv 1 \pmod 4$, i.e. $a_2 - w \equiv -1 \pmod 4$. Since $a_2 - w$ is odd, exactly one of these congruences holds, and the lemma follows. ■

Condition 4 makes it possible to distinguish curves in the class:

- $\mathrm{I}_1^*(4,6,8)$ from those in $\mathrm{IV}^*(4,6,8)$;
- $\mathrm{I}_2^*(4,6,10)$ from those in $\mathrm{III}^*(4,6,10)$;
- $\mathrm{I}_3^*(4,6,11)$ from those in $\mathrm{II}^*(4,6,11)$.

See Tables 2.1 and 2.2.

Applying Conditions 0–4, as described above, we can determine to which class a curve belongs, with one exception. Namely, there are classes $\mathrm{I}_2^*(6,\nu,12)$ and $\mathrm{I}_3^*(6,\nu,12)$, where $\nu \geq 10$, which belong to the same Case 7.

To distinguish curves in these classes we apply the next condition. It is not stated explicitly in [Pa].

Condition 5. *Assume that* $V(E) = (6, \nu, 12)$, *where* $\nu \geq 10$. *The condition is:* $c_{4,6} \equiv -1 \pmod 4$.

Lemma 2.9. *Let* $V(E) = (6, \nu, 12)$, *where* $\nu \geq 10$. *Then* $E$ *belongs to the class* $\mathrm{I}_2^*(6, \nu, 12)$ *iff Condition* 5 *is satisfied, and to* $\mathrm{I}_3^*(6, \nu, 12)$ *iff* $c_{4,6} \equiv 1 \pmod 4$.

*Proof.* We are going to apply Step 7 of the algorithm of Tate (see [Ta]). Thus we have to replace the model $E$ by a model $E' = [0, a_2', 0, a_4', a_6']$ satisfying $2 \parallel a_2'$. We consider two cases.

1) Let $a_2 = \pm 1$. We make the substitution $X \mapsto X - a_2$, which does not change the values of $c_4$, $c_6$ and $\Delta$. We get the model

$$E' = [0, a_2', 0, a_4', a_6'] = [0, -2a_2, 0, 1 + a_4, -a_2 a_4 + a_6].$$

Since $c_4 = c_4' = 2^4(4 - 3a_4')$ and $v(c_4) = 6$, we have $8 \mid a_4'$, hence $a_4' = 8a_{4,3}'$.

Similarly from

$$c_6 = c_6' = -2^5(2a_2'^3 - 9a_2' a_4' + 27a_6') = -2^5(16a_{2,1}'(1 - 9a_{2,1}'\, a_{4,3}') + 27a_6')$$

and $v(c_6) \geq 10$ we deduce that $2^4 \mid a_6'$.

The polynomial

$$P(T) = T^3 + a_{2,1}' T^2 + a_{4,2}' T + a_{6,3}' \pmod 2,$$

appearing in the Tate algorithm, in our case takes the form $P(T) = T^3 + T^2 \pmod 2$. It has a double root $T = 0$, and a single root $T = -1$.

Then, according to Step 7 of the algorithm, we have to consider the polynomial

$$Y^2 + a_{3,2}' Y - a_{6,4}' \pmod 2,$$

i.e. the polynomial $Y^2 - a_{6,4}' \pmod 2$ in our case. It has a double root, and we can translate $Y$, if necessary, so that the root is $Y = 0$.

Namely, if $a_{6,4}' \equiv 1 \pmod 2$, i.e. if $a_6' \equiv 16 \pmod{32}$, we make the substitution $Y \mapsto Y + 4$, and get the model $E'' = [0, a_2', 8, a_4', a_6' - 16]$. Here $a_6'' = a_6' - 16 \equiv 0 \pmod{32}$, i.e. $a_{6,4}'' \equiv 0 \pmod 2$. In other words, we can assume that $2^5 \mid a_6'$.

Now the algorithm says that the Kodaira symbol of $E'$ (hence also of $E$) is $\mathrm{I}_2^*$ if the polynomial

$$a_{2,1}' X^2 + a_{4,3}' X + a_{6,5}' \pmod 2,$$

i.e. $X^2 + a_{4,3}' X + a_{6,5}' \pmod 2$, has distinct roots, and is not $\mathrm{I}_2^*$ (hence $\mathrm{I}_3^*$ in our case) if it has a double root.

This polynomial has distinct roots iff $a_{4,3}' \equiv 1 \pmod 2$, and has a double root iff $a_{4,3}' \equiv 0 \pmod 2$.

Since $c_4 = c_4' = 2^4(4 - 3a_4')$, it follows that $c_{4,6} = 1 - 6a_{4,3}'$. Hence

$$c_{4,6} \equiv \begin{cases} -1 \pmod 4 \\ \phantom{-}1 \pmod 4 \end{cases} \quad \text{iff} \quad a_{4,3}' \equiv \begin{cases} 1 \pmod 2, \\ 0 \pmod 2, \end{cases}$$

and the lemma follows in this case.

2) Let $a_2 = 0$. We proceed similarly. Making the substitution $X \mapsto X + 2$, which does not change $c_4, c_6$ and $\Delta$, we get the model

$$E' = [0, a'_2, 0, a'_4, a'_6] = [0, 6, 0, 12 + a_4, 8 + 2a_4 + a_6].$$

Since

$$c_4 = c'_4 = 2^4(a'^2_2 - 3a'_4) = 2^4(36 - 3a'_4),$$

from $v(c_4) = 6$ we deduce that $8 \mid a'_4$, hence $a'_4 = 8a'_{4,3}$.

Similarly from

$$c_6 = c'_6 = -2^5(2a'^3_2 - 9a'_2a'_4 + 27a'_6) = -2^5\, 3^3(2^4(1 - a'_{4,3}) + a'_6)$$

and from $v(c_4) \geq 10$ we conclude that $2^4 \mid a'_6$. We can assume that $2^5 \mid a'_6$, making the substitution $Y \mapsto Y + 4$ if necessary.

Proceeding as in the first case we deduce that the Kodaira symbol of $E$ is $\mathrm{I}_2^*$ if $a'_{4,3}$ is odd, i.e. if $a'_4 \equiv 8 \pmod{16}$, and is $\mathrm{I}_3^*$ if $a'_4 \equiv 0 \pmod{16}$.

Since $c_4 = 2^6(9 - 6a'_{4,3})$, we get

$$c_{4,6} \equiv \begin{cases} -1 \pmod 4 \\ \phantom{-}1 \pmod 4 \end{cases} \quad \text{iff} \quad a'_4 \equiv \begin{cases} 8 \pmod{16}, \\ 0 \pmod{16}, \end{cases}$$

which proves the lemma in the second case. ■

This lemma explains the last two lines in Table 2.2.

**2.3. Table 2.2.** In Table 2.2 we describe the action of the twist by $-1$ on the refined Kodaira classes with $v(N) \leq 4$. In the consecutive columns of the table there are classes with $v(N) = 0, 1, 2, 3$ and 4, respectively. In every line there is a class and its image under the twist by $-1$.

It turns out that the class $\mathrm{II}(4, 5, 4)$ is the (disjoint!) union of the twists of the classes $\mathrm{III}(4, 5, 4)$ and $\mathrm{IV}(4, 5, 4)$. We denote these subsets of $\mathrm{II}(4, 6, 8)$ by $\mathrm{II}(4, 6, 8)a$ and $\mathrm{II}(4, 6, 8)b$, respectively.

By Lemma 2.5, the curves in the subset II(4,5,4)$a$ satisfy Condition 2, and those in $\mathrm{II}(4, 5, 4)b$ do not.

The same remark concerns the class $\mathrm{I}_0^*(4, 6, 8)$, which is the disjoint union of the images under the twist by $-1$ of the classes $\mathrm{I}_1^*(4, 6, 8)$ and $\mathrm{IV}^*(4, 6, 8)$. We denote these subsets by $\mathrm{I}_0^*(4, 6, 8)a$ and $\mathrm{I}_0^*(4, 6, 8)b$, respectively.

By Lemma 2.8 the curves belonging to the first subset satisfy Condition 4, and those belonging to the second one do not.

**2.4. Main Theorem.** The above considerations lead to the following theorem.

THEOREM 2.1. *Let $\mathcal{E}_{-1} := \mathcal{E} * (-1)$.*

(i) *If $v(N(\mathcal{E})) > 4$, then both curves $\mathcal{E}$ and $\mathcal{E}_{-1}$ belong to the same refined Kodaira class. Hence $v(N(\mathcal{E})) = v(N(\mathcal{E}_{-1}))$.*

(ii) *If $v(N(\mathcal{E})) \leq 4$, then $\mathcal{E}$ and $\mathcal{E}_{-1}$ belong to distinct refined Kodaira classes. More precisely, $v(N(\mathcal{E})) = 4$ iff $v(N(\mathcal{E}_{-1})) < 4$.*

*Proof.* The result follows immediately from Table 2.1 and Lemmas 2.3, 2.4, 2.5, 2.7 and 2.8.

For example, if $\mathcal{E}$ belongs to $\mathrm{II}(4,6,7)$ then in the corresponding line in Table 2.1 there is no additional condition. Therefore $\mathcal{E}_{-1}$ belongs to the same class. Moreover, in the fourth column of Table 2.1 we have $v(N)=7$. Thus Theorem 2.1 holds for the curves in the class $\mathrm{II}(4,6,7)$.

On the other hand, if $\mathcal{E}$ belongs to $\mathrm{IV}^*(4,6,8)$, then from Table 2.1 we see that $v(N)=2$ and the corresponding model satisfies neither Condition 3 nor Condition 4.

By Lemmas 2.7 and 2.8, the twisted model $E' := E*(-1)$ satisfies both these conditions. Therefore from Table 2.1 we see that $\mathcal{E}_{-1}$ does not belong to $\mathrm{I}_1^*(4,6,8)$, hence it belongs to $\mathrm{I}_0^*(4,6,8)$. Consequently, $v(N(\mathcal{E}_{-1}))=4$. This proves Theorem 2.1 for curves in $\mathrm{IV}^*(4,6,8)$.

The proof for the remaining classes is similar.

The action of twist by $-1$ on refined Kodaira classes with $v(N)\le 4$ is described in Table 2.2. ∎

## 3. The case $p=2$ and $d=2$

**3.1. Table 3.1.** If $V(E)=(v_1,v_2,v_3)$, then $V(E*2)=(v_1+2,v_2+3,v_3+6)$, thus the triples corresponding to the models $E$ and $E*2$ are distinct. Therefore a curve $\mathcal{E}$ and its twist $\mathcal{E}' := \mathcal{E}*2$ belong to distinct refined Kodaira classes.

In Table 3.1 we describe the twists by 2 of all curves given in Table 2.1. There are small differences between these tables made to get a better presentation.

The action of the twist by 2 on classes still requires further clarification, which motivates the lemmas given below. The corresponding reference is given in the last column of Table 3.1.

### 3.2. Lemmas

Lemma 3.1. *Let $E=[0,a_2,0,a_4,a_6]$ be the reduced minimal model of a curve $\mathcal{E}$. Assume that $V(E)=(4,\nu,6)$ with $\nu\ge 7$. Then $E$ satisfies Condition* 1 *iff $E' := E*2$ does not satisfy Condition* 5. *Hence*

$$\begin{aligned}\mathcal{E}\in \mathrm{II}(4,\nu,6) \quad &\textit{iff}\quad \mathcal{E}*2\in \mathrm{I}_3^*(6,\nu+3,12),\\ \mathcal{E}\in \mathrm{III}(4,\nu,6) \quad &\textit{iff}\quad \mathcal{E}*2\in \mathrm{I}_2^*(6,\nu+3,12).\end{aligned}$$

*Proof.* We have

$$E' := E*2 = [0,2a_2,0,4a_4,8a_6] =: [0,a_2',0,a_4',a_6'],$$

and hence $V(E')=(6,\nu+3,12)$ with $\nu+3\ge 10$.

From $c_4=2^4(a_2^2-3a_4)$ and $v(c_4)=4$ we get

$$a_2\not\equiv a_4 \pmod 2. \tag{3.1}$$

Since $v(\Delta(E))=6>4$, Condition 1 for $E$ takes the form

$$F(a_4)=a_4^3+a_2a_4^2+a_4^2+a_6\equiv 2 \pmod 4. \tag{3.2}$$

Since $c_4'=2^4(a_2'^2-3a_4')=2^6(a_2^2-3a_4)$, Condition 5 for $E'$ says that $c_{4,6}'\equiv -1 \pmod 4$, i.e. $a_2^2+a_4\equiv -1 \pmod 4$. Consequently, in view of (3.1), Condition 5′ for $E'$ is

$$a_2^2+a_4\equiv 1 \pmod 4. \tag{3.3}$$

Since $a_2a_4$ is even, by (3.1), from $v(c_6) \geq 7$ we get $2a_2^3 - 9a_2a_4 + 27a_6 \equiv 0 \pmod 4$, i.e. $2a_2 + a_2a_4 - a_6 \equiv 0 \pmod 4$.

Hence

$$\begin{aligned} F(a_4) &\equiv a_4^3 + a_2a_4^2 + a_4^2 + a_2a_4 + 2a_2 \\ &\equiv a_4(a_4+1)(a_2+a_4) + 2a_2 \pmod 4. \end{aligned}$$

Since $a_2 + a_4$ is odd and $a_4(a_4+1)$ is even we get

$$F(a_4) \equiv a_4(a_4+1) + 2a_2 \pmod 4.$$

Now $2a_2 \equiv 2a_2^2 \pmod 4$ and $a_4^2 + a_2^2 \equiv 1 \pmod 4$, by (3.1). Consequently,

$$F(a_4) \equiv a_4^2 + a_4 + 2a_2^2 \equiv (a_4^2 + a_2^2) + (a_4 + a_2^2) \equiv a_2^2 + a_4 + 1 \pmod 4.$$

Therefore $F(a_4) \equiv 2 \pmod 4$ iff $a_2^2 + a_4 \equiv 1 \pmod 4$, i.e. (3.2) is equivalent to (3.3).

In other words, $E$ satisfies Condition 1 iff $E'$ does not satisfy Condition 5. ∎

Lemma 3.2.

(i) *The class* $\mathrm{II}(\nu, 6, 6)$ *with* $\nu \geq 6$ *is the disjoint union of the classes* $\mathrm{I}_0(\nu+2, 9, 12)'$ *and* $\mathrm{II}^*(\nu+2, 9, 12)$, *both twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{II}(\nu, 6, 6)$, $\nu \geq 6$. *Then*

$$\begin{aligned} \mathcal{E} &\in \mathrm{I}_0(\nu+2, 9, 12)' * 2 \quad \textit{iff} \quad c_{6,6} \equiv \phantom{-}1 \pmod 4, \\ \mathcal{E} &\in \mathrm{II}^*(\nu+2, 9, 12) * 2 \quad \textit{iff} \quad c_{6,6} \equiv -1 \pmod 4. \end{aligned}$$

*Proof.* (i) From $\mathcal{E} \in \mathrm{II}(\nu, 6, 6)$ we get $V(E * 2) = (\nu+2, 9, 12)$. The triple $(\nu+2, 9, 12)$ appears in Table 3.1 twice with the Kodaira symbols $\mathrm{I}_0$ and $\mathrm{II}^*$. Therefore

$$\mathcal{E} * 2 \in \mathrm{I}_0(\nu+2, 9, 12)' \cup \mathrm{II}^*(\nu+2, 9, 12).$$

From $\mathcal{E} = (\mathcal{E} * 2) * 2$ we get the first part of the lemma.

(ii) To prove the second one we describe how Condition 0 (which is used to distinguish curves in the classes $\mathrm{I}_0(\nu+2, 9, 12)'$ and $\mathrm{II}^*(\nu+2, 9, 12)$) changes under the twist by 2.

Let $E' := E * 2 = [0, 2a_2, 0, 4a_4, 8a_6]$. Then $E'$ is a model of $\mathcal{E}'$ satisfying $V(E') = (\nu+2, 9, 12)$. Moreover, this model is not minimal if $\mathcal{E}' \in \mathrm{I}_0(\nu+2, 9, 12)'$, and is minimal if $\mathcal{E}' \in \mathrm{II}^*(\nu+2, 9, 12)$.

In view of Lemma 1.6, the model $E'$ is minimal iff the numbers $m = c'_{4,4}$ and $n = c'_{6,6}$ do not satisfy the condition (ii) of Lemma 1.3:

$$n \equiv -1 \pmod 4 \quad \text{or} \quad m \equiv 0 \pmod{16}, \ n \equiv 0, 8 \pmod{32},$$

i.e.

$$c'_{6,6} \equiv -1 \pmod 4 \quad \text{or} \quad c'_{4,4} \equiv 0 \pmod{16}, \ c'_{6,6} \equiv 0, 8 \pmod{32}. \tag{3.4}$$

In our case we have $v(c'_4) = \nu + 2 \geq 8$, hence $v(c'_{4,4}) = v(c'_4) - 4 \geq 4$. Thus $c'_{4,4} \equiv 0 \pmod{16}$.

From $v(c'_6) = 9$ we get $v(c'_{6,6}) = v(c'_6) - 6 = 3$. Then $c'_{6,6} \equiv \pm 8 \pmod{32}$.

Consequently, (3.4) is not satisfied iff $c'_{6,6} \equiv -8 \pmod{32}$, equivalently iff $c_{6,6} \equiv -1 \pmod 4$, since $c'_6 = 8c_6$, i.e. $c'_{6,6} = 8c_{6,6}$.

Thus the model $E'$ is minimal iff $c_{6,6} \equiv -1 \pmod 4$, and it is not minimal iff $c_{6,6} \equiv 1 \pmod 4$. This proves the lemma. ■

Lemma 3.3. *Let $E = [0, a_2, 0, a_4, a_6]$ be the reduced minimal model of a curve $\mathcal{E} \in \mathrm{I}_0^*(\nu, 8, 10)$, $\nu \geq 6$. Let the polynomials $F(X), G(X)$ correspond to this model. Define $a := (a_4 + a_2^2)/2 - a_2$. Then the minimal model $E' = [0, a_2', 0, a_4', a_6']$ of the twisted curve $\mathcal{E}' := \mathcal{E} * 2$ satisfies*

(i) *Condition* 1 *iff* $F(a) \equiv -8 \pmod{2^5}$ (*and* $F(a) \equiv 8 \pmod{2^5}$ *otherwise*).
(ii) *Condition* 2 *iff* $G(a) \equiv 2^6 \pmod{2^7}$ (*and* $G(a) \equiv 0 \pmod{2^7}$ *otherwise*).

*Proof.* From $\mathcal{E} = \mathcal{E}' * 2$ we get $V(E') = (\nu - 2, 5, 4)$, $\nu \geq 6$. Then $E' * 2 = [0, 2a_2', 0, 4a_4', 8a_6']$ is a minimal model of $\mathcal{E}$, which is not reduced in general. To get the reduced one, we make the substitution $X \mapsto X - a_2'$, which leads to the reduced minimal model

$$\widetilde{E} = [0, -a_2', 0, 4a_4' - a_2'^2, a_2'^3 - 4a_2'a_4' + 8a_6'].$$

Since the reduced minimal model is unique, we get $\widetilde{E} = E$, hence

$$a_2 = -a_2', \quad a_4 = 4a_4' - a_2'^2, \quad a_6 = a_2'^3 - 4a_2'a_4' + 8a_6',$$

It follows in particular that $a_4' = (a_4 + a_2^2)/4$.

Let $F_1(X), G_1(X)$ be polynomials corresponding to the model $E'$, and $F_2(X)$, $G_2(X)$ to the model $E' * 2$. Since the shift $X \mapsto X - a_2'$ leads from the model $E' * 2$ to the model $\widetilde{E} = E$, we obtain the equalities

$$F_2(X - a_2') = F(X), \qquad G_2(X - a_2') = G(X).$$

Moreover,

$$F_2(2X) = 8F_1(X), \qquad G_2(2X) = 16G_1(X).$$

Consequently,

$$F(a) = F\left(\frac{a_4 + a_2^2}{2} - a_2\right) = F(2a_4' + a_2') = F_2(2a_4') = 8F_1(a_4'),$$

and similarly $G(a) = 16G_1(a_4')$.

Condition 1 for the model $E'$ says that $F_1(a_4') \equiv -1 \pmod 4$ (and $F_1(a_4') \equiv 1 \pmod 4$ otherwise), hence it is equivalent to $F(a) \equiv -8 \pmod{32}$ (and $F(a) \equiv 8 \pmod{32}$ otherwise).

Condition 2 for the model $E'$ says that $G_1(a_4') \equiv 4 \pmod 8$ (and $G_1(a_4') \equiv 0 \pmod 8$ otherwise), hence it is equivalent to $G(a) \equiv 2^6 \pmod{2^7}$ (and $G(a) \equiv 0 \pmod{2^7}$ otherwise).

Let us remind ourselves that Conditions 1 and 2 do not depend on a minimal model chosen. Therefore we can use the minimal model $E'$ of $\mathcal{E}'$ even in the case where it is not reduced. ■

Lemma 3.4.

(i) *The class* $\mathrm{I}_0^*(6, 8, 10)$ *is the disjoint union of the classes* $\mathrm{II}(4, 5, 4)$, $\mathrm{III}(4, 5, 4)$ *and* $\mathrm{IV}(4, 5, 4)$, *all twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}_0^*(6,8,10)$. *Then*

$$\begin{aligned} &\mathcal{E} \in \mathrm{II}(4,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv -8 \pmod{32}, \\ &\mathcal{E} \in \mathrm{III}(4,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv 8 \pmod{32} \textit{ and } G(a) \equiv 2^6 \pmod{2^7}, \\ &\mathcal{E} \in \mathrm{IV}(4,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv 8 \pmod{32} \textit{ and } G(a) \equiv 0 \pmod{2^7}, \end{aligned}$$

*where* $a = (a_4 + a_2^2)/2 - a_2$.

*Proof.* (i) For the minimal model $E'$ of $\mathcal{E}' := \mathcal{E} * 2$ we have $V(E') = (4,5,4)$. The triple $(4,5,4)$ appears in Table 3.1 three times, with Kodaira symbols II, III and IV. Therefore

$$\mathcal{E} * 2 \in \mathrm{II}(4,5,4) \cup \mathrm{III}(4,5,4) \cup \mathrm{IV}(4,5,4).$$

This proves the first part of the lemma.

(ii) To prove the second part, let us observe that Conditions 1 and 2 make it possible to decide to which of the three classes the curve $\mathcal{E}'$ belongs.

Applying Lemma 3.3 we get the result. ∎

Proofs of the next two lemmas are quite analogous to the proof of Lemma 3.4, therefore we omit them.

Lemma 3.5.

(i) *The class* $\mathrm{I}_0^*(7,8,10)$ *is the disjoint union of the classes* $\mathrm{II}(5,5,4)$ *and* $\mathrm{III}(5,5,4)$, *both twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}_0^*(7,8,10)$. *Then*

$$\begin{aligned} &\mathcal{E} \in \mathrm{II}(5,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv -8 \pmod{32}, \\ &\mathcal{E} \in \mathrm{III}(5,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv 8 \pmod{32}, \end{aligned}$$

*where* $a = (a_4 + a_2^2)/2 - a_2$.

Lemma 3.6.

(i) *The class* $\mathrm{I}_0^*(\nu,8,10)$, $\nu \geq 8$, *is the disjoint union of the classes* $\mathrm{II}(\nu-2,5,4)$ *and* $\mathrm{IV}(\nu-2,5,4)$ *both twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}_0^*(\nu,8,10)$. *Then*

$$\begin{aligned} &\mathcal{E} \in \mathrm{II}(\nu-2,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv -8 \pmod{32}, \\ &\mathcal{E} \in \mathrm{IV}(\nu-2,5,4) * 2 \quad \textit{iff} \quad F(a) \equiv 8 \pmod{32}, \end{aligned}$$

*where* $a = (a_4 + a_2^2)/2 - a_2$.

Lemma 3.7. *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}_4^*(6,9,14)$. *Let the polynomials* $F(X), G(X)$ *correspond to this model. Define* $\widehat{a} := (a_6 - a_2a_4)/8 - 5a_2$. *Then the minimal model* $E' = [0, a_2', 0, a_4', a_6']$ *of the twisted curve* $\mathcal{E}' := \mathcal{E} * 2$ *satisfies*

(i) *Condition* 3 *iff* $F(\widehat{a}) \equiv -2^5 \pmod{2^7}$ (*and* $F(\widehat{a}) \equiv 2^5 \pmod{2^7}$ *otherwise*).

(ii) *Condition* 4 *iff* $\widehat{a} \equiv -(2 + 3a_2) \pmod 8$.

*Proof.* We proceed similarly to the proof of Lemma 3.3.

From $\mathcal{E} = \mathcal{E}' * 2$ we get $V(E') = (4, 6, 8)$. Then $E' * 2 = [0, 2a_2', 0, 4a_4', 8a_6']$ is a minimal model of $\mathcal{E}$, which is not reduced in general. The substitution $X \mapsto X - a_2'$ leads to the reduced minimal model

$$\widetilde{E} = [0, -a_2', 0, 4a_4' - a_2'^2, a_2'^3 - 4a_2'a_4' + 8a_6'].$$

By the uniqueness of the reduced minimal model, we get $\widetilde{E} = E$. Hence

$$a_2' = -a_2, \quad a_4' = (a_4 + a_2^2)/4, \quad a_6' = (a_6 - a_2a_4)/8.$$

Let $F_1(X), G_1(X)$ be polynomials corresponding to the model $E'$, and $F_2(X)$, $G_2(X)$ to the model $E' * 2$. Then

$$F_2(X - a_2') = F(X), \quad G_2(X - a_2') = G(X),$$
$$F_2(2X) = 8F_1(X), \quad G_2(2X) = 16G_1(X).$$

(i) To state Condition 3 for $E'$ we have to find a solution $w'$ of the congruence $G_1(w') \equiv 0 \pmod{32}$. By Lemma 2.6, we can take $w' = a_{6,1}' + 2a_2'$. Then Condition 3 for $E'$ says that $F_1(w') \equiv -4 \pmod{16}$, and we have $F_1(w') \equiv 4 \pmod{16}$ otherwise. Now,

$$2w' = a_6' + 4a_2' = \widehat{a} + 5a_2 - 4a_2 = \widehat{a} + a_2.$$

Therefore

$$F_1(w') = \tfrac{1}{8}F_2(2w') = \tfrac{1}{8}F_2(\widehat{a} + a_2) = \tfrac{1}{8}F(\widehat{a}).$$

Consequently, Condition 3 is equivalent to

$$F(\widehat{a}) \equiv -2^5 \pmod{2^7},$$

and otherwise we have $F(\widehat{a}) \equiv 2^5 \pmod{2^7}$.

(ii) Condition 4 for $E'$ says that $a_2' - w' \equiv 1 \pmod 4$, where $w'$ satisfies $G_1(w') \equiv 0 \pmod{32}$. By the first part of the proof, we can take

$$w' = a_{6,1}' + 2a_2' = (\widehat{a} + a_2)/2.$$

Consequently, Condition 4 is equivalent to

$$-a_2 - (\widehat{a} + a_2)/2 \equiv 1 \pmod 4, \quad \text{i.e.} \quad \widehat{a} \equiv -(2 + 3a_2) \pmod 8. \blacksquare$$

LEMMA 3.8.

(i) *The class* $\mathrm{I}_4^*(6, 9, 14)$ *is the disjoint union of the classes* $\mathrm{I}_0^*(4, 6, 8)$, $\mathrm{I}_1^*(4, 6, 8)$ *and* $\mathrm{IV}^*(4, 6, 8)$, *all twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}_4^*(6, 9, 14)$. *Then*

$$\begin{aligned} \mathcal{E} \in \mathrm{I}_0^*(4,6,8) * 2 \quad &\textit{iff} \quad F(\widehat{a}) \equiv -2^5 \pmod{2^7}, \\ \mathcal{E} \in \mathrm{I}_1^*(4,6,8) * 2 \quad &\textit{iff} \quad F(\widehat{a}) \equiv 2^5 \pmod{2^7} \textit{ and } \widehat{a} \equiv -(2+3a_2) \pmod 8, \\ \mathcal{E} \in \mathrm{IV}^*(4,6,8) * 2 \quad &\textit{iff} \quad F(\widehat{a}) \equiv 2^5 \pmod{2^7} \textit{ and } \widehat{a} \not\equiv -(2+3a_2) \pmod 8, \end{aligned}$$

*where* $\widehat{a} := (a_6 - a_2a_4)/8 - 5a_2$.

*Proof.* (i) The minimal model $E'$ of $\mathcal{E}' := \mathcal{E} * 2$ satisfies $V(E') = (4,6,8)$. The triple $(4,6,8)$ appears in Table 3.1 three times, with Kodaira symbols $\mathrm{I}_0^*$, $\mathrm{I}_1^*$ and $\mathrm{IV}^*$. Therefore

$$\mathcal{E} * 2 \in \mathrm{I}_0^*(4,5,4) \cup \mathrm{I}_1^*(4,5,4) \cup \mathrm{IV}^*(4,5,4).$$

This proves the first part of the lemma.

(ii) To prove the second part, let us observe that Conditions 3 and 4 make it possible to decide to which of the three classes the curve $\mathcal{E}'$ does belong.

Applying Lemma 3.7 we get the result. ∎

Now we extend Lemma 2.6 to the triples $(4,6,\nu)$, with $\nu \geq 9$.

Lemma 3.9. *Let $V(E) = (4,6,\nu)$, where $\nu \geq 9$. Then*

(i) *The congruence $G(X) \equiv 0 \pmod{32}$ has a solution $w \equiv a_4 \pmod 2$. Moreover, $G(w') \equiv 0 \pmod{32}$ iff $w' \equiv w \pmod 4$.*
(ii) *Choose $w$ satisfying $G(w) \equiv 0 \pmod{32}$. Then $F(w) \equiv 0 \pmod 8$, and $F(w) \pmod{16}$ does not depend on the $w$ chosen.*

*Proof.* We adapt the proof of Lemma 2.6 to the present situation.

(i) (a) Assume that $a_2 = 0$. From $c_4 = -2^4 \cdot 3\, a_4$ and $v(c_4) = 4$ it follows that $a_4$ is odd. From $c_6 = -2^5 \cdot 3^3\, a_6$ and $v(c_6) = 6$ it follows that $a_6 = 2a_{6,1},\ a_{6,1}$ odd.

From $\Delta = (c_4^3 - c_6^2)/12^3 = -2^6(a_4^3 + 27a_{6,1}^2)$ and $v(\Delta) \geq 9$ it follows that $a_4^3 + 27a_{6,1}^2 \equiv 0 \pmod 8$, i.e. $a_4 \equiv 5 \pmod 8$.

If $G(w) \equiv 0 \pmod 2$ then $3w^4 - a_4^2 \equiv 0 \pmod 2$, i.e. $w$ is odd. Hence $a_4 + w^2 \equiv 6 \pmod 8$, and so $(a_4 + w^2)^2 \equiv 4 \pmod{32}$.

Consequently,

$$G(w) = 3(w^2 + a_4)^2 - 4a_4^2 + 24a_{6,1}w \equiv 8(1 + 3a_{6,1}w) \pmod{32}.$$

It follows that $G(w) \equiv 0 \pmod{32}$ iff $1 + 3a_{6,1}w \equiv 0 \pmod 4$ iff $w \equiv a_{6,1} \pmod 4$.

(b) Assume that $a_2 = \pm 1$. From $c_4 = 2^4(1 - 3a_4)$ and $v(c_4) = 4$ it follows that $c_{4,4} = 1 - 3a_4$ is odd. Then $a_4$ is even, and $a_6$ is even, by Lemma 1.2. From $c_6 = -2^6(a_2 - 9a_2a_{4,1} + 27a_{6,1})$ and $v(c_6) = 6$ it follows that $c_{6,6} = c_6/2^6 = -(a_2 - 9a_2a_{4,1} + 27a_{6,1})$ is odd, i.e. $a_{4,1} \equiv a_{6,1} \pmod 2$.

From $\Delta = \frac{2^6}{3^3}(c_{4,4}^3 - c_{6,6}^2)$ and $v(\Delta) \geq 9$ it follows that $c_{4,4}^3 - c_{6,6}^2 \equiv 0 \pmod 8$. Hence $c_{4,4} = 1 - 3a_4 \equiv 1 \pmod 8$, so $a_4 \equiv 0 \pmod 8$, and $a_{4,1} \equiv a_{6,1} \pmod 2$ implies that $a_6 \equiv 0 \pmod 4$.

Consequently, if $G(w) \equiv 0 \pmod 2$, then $w$ is even, $w = 2w_1$.

In view of $a_4 \equiv 0 \pmod 8$ and $a_6 \equiv 0 \pmod 4$, we have

$$G(w) = G(2w_1) \equiv 48w_1^4 + 4a_2a_6 \equiv 16(w_1 + a_{6,2}) \pmod{32}.$$

Therefore $G(w) \equiv 0 \pmod{32}$ iff $w_1 \equiv a_{6,2} \pmod 2$ iff $w =\equiv a_{6,1} \pmod 4$.

Thus we have proved that in both cases

$$G(w) \equiv 0 \pmod{32} \quad \text{iff} \quad w \equiv a_{6,1} \pmod 4.$$

For convenience we collect in the following table the information obtained.

| $a_2$ | $a_4$ (mod 8) | $a_{6,1}$ (mod 2) | $w$ (mod 4) |
|---|---|---|---|
| 0 | 5 | 1 | $a_{6,1}$ |
| $\pm 1$ | 0 | 0 | $a_{6,1}$ |

(ii) If $a_2 = 0$ then

$$F(w) = w^3 + a_4 w + a_6 \equiv 6w + a_6 = 2(3w + a_{6,1}) \equiv 0 \pmod 8,$$

since $w \equiv a_{6,1} \pmod 4$ and $a_{6,1}$ is odd.

Let $a_2 = \pm 1$. Then $a_{6,1}$ is even, $a_{6,1} = 2a_{6,2}$. From $w \equiv a_{6,1} \pmod 4$ we get $w^2 \equiv a_{6,1}^2 \pmod 8$. Consequently,

$$F(w) \equiv a_2 w^2 + a_6 \equiv a_2 a_{6,1}^2 + 2a_{6,1} \equiv 4(a_{6,2}^2 + a_{6,2}) \equiv 0 \pmod 8.$$

To prove the last part of the lemma it is sufficient to prove that $F(w+4) \equiv F(w) \pmod{16}$. Since

$$F(w+4) - F(w) = 4(3w^2 + 2a_2 w + a_4),$$

it is sufficient to verify that

$$3w^2 + 2a_2 w + a_4 \equiv 0 \pmod 4.$$

This follows immediately from the table above. ■

Lemma 3.10. *Let $E = [0, a_2, 0, a_4, a_6]$ be the reduced minimal model of a curve $\mathcal{E} \in \mathrm{I}_6^*(6, 9, \nu)$, $\nu = 16$ or $17$. Then the minimal model $E' = [0, a_2', 0, a_4', a_6']$ of the twisted curve $\mathcal{E}' := \mathcal{E} * 2$ satisfies Condition 4 iff $(a_6 - a_2 a_4)/16 \equiv -(1 + a_2) \pmod 4$.*

*Proof.* It is sufficient in the proof of Lemma 3.7 to use Lemma 3.9 in place of Lemma 2.6, and $w' = a_{6,1}'$ in place of $w' = a_{6,1}' = 2a_2'$. Then Condition 4 for $E'$ says that $a_2' - w' \equiv 1 \pmod 4$, which is equivalent to $(a_6 - a_2 a_4)/16 \equiv -(1 + a_2) \pmod 4$. ■

The next two lemmas follow immediately from Lemma 3.10.

Lemma 3.11.

(i) *The class $\mathrm{I}_6^*(6, 9, 16)$ is the disjoint union of the classes $\mathrm{I}_2^*(4, 6, 10)$ and $\mathrm{III}^*(4, 6, 10)$, both twisted by 2.*

(ii) *Let $E = [0, a_2, 0, a_4, a_6]$ be the reduced minimal model of a curve $\mathcal{E} \in \mathrm{I}_6^*(6, 9, 16)$. Then*

$$\mathcal{E} \in \mathrm{I}_2^*(4,6,10) * 2 \quad \textit{iff} \quad (a_6 - a_2 a_4)/16 \equiv -(1 + a_2) \pmod 4,$$
$$\mathcal{E} \in \mathrm{III}^*(4,6,10) * 2 \quad \textit{iff} \quad (a_6 - a_2 a_4)/16 \not\equiv -(1 + a_2) \pmod 4,$$

*where $a = (a_4 + a_2^2)/2 - a_2$.*

Lemma 3.12.

(i) *The class $\mathrm{I}_7^*(6, 9, 17)$ is the disjoint union of the classes $\mathrm{I}_3^*(4, 6, 11)$ and $\mathrm{II}^*(4, 6, 11)$, both twisted by 2.*

(ii) *Let $E = [0, a_2, 0, a_4, a_6]$ be the reduced minimal model of a curve $\mathcal{E} \in \mathrm{I}_7^*(6, 9, 17)$. Then*

$$\mathcal{E} \in \mathrm{I}_3^*(4,6,11) * 2 \quad \textit{iff} \quad (a_6 - a_2 a_4)/16 \equiv -(1 + a_2) \pmod 4,$$
$$\mathcal{E} \in \mathrm{II}^*(4,6,11) * 2 \quad \textit{iff} \quad (a_6 - a_2 a_4)/16 \not\equiv -(1 + a_2) \pmod 4,$$

*where $a = (a_4 + a_2^2)/2 - a_2$.*

Lemma 3.13.

(i) *The class* $\mathrm{I}^*_{4+\nu}(6,9,14+\nu)$, *where* $\nu \geq 4$, *is the disjoint union of the classes* $\mathrm{I}_{\nu-4}(4,6,8+\nu)'$ *and* $\mathrm{I}^*_{\nu}(4,6,8+\nu)$, *both twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{I}^*_{4+\nu}(6,9,14+\nu)$, $\nu \geq 4$. *Then*

$$\mathcal{E} \in \mathrm{I}_{\nu-4}(4,6,8+\nu)' * 2 \quad \textit{iff} \quad c_{6,9} \equiv \phantom{-}1 \pmod 4,$$
$$\mathcal{E} \in \mathrm{I}^*_{\nu}(4,6,8+\nu) * 2 \quad \textit{iff} \quad c_{6,9} \equiv -1 \pmod 4.$$

*Proof.* (i) Let $\mathcal{E} = \mathcal{E}' * 2$ and let $E'$ be a minimal model of $\mathcal{E}'$. Then $V(E') = (4,6,8+\nu)$. The triple $(4,6,8+\nu)$, $\nu \geq 4$, appears in Table 3.1 twice with Kodaira symbols $\mathrm{I}_{\nu-4}$ and $\mathrm{I}^*_{\nu}$. This proves the first part of the lemma.

(ii) We have $\mathcal{E} \in \mathrm{I}_{\nu-4}(4,6,8+\nu)' * 2$ iff $\mathcal{E}' \in \mathrm{I}_{\nu-4}(4,6,8+\nu)'$ iff the model $E'$ satisfies Condition 0, i.e. $c'_{6,6} \equiv 1 \pmod 4$. Since $c_6 = 8c'_6$, Condition 0 for $E'$ is equivalent to $c_{6,6} \equiv 8 \pmod{32}$, i.e. to $c_{6,9} \equiv 1 \pmod 4$. This proves the lemma, because in every case $c_{6,9}$ is odd. ■

Lemma 3.14.

(i) *The class* $\mathrm{II}^*(8,10,14)$ *is the disjoint union of the classes* $\mathrm{I}^*_0(6,7,8)$ *and* $\mathrm{I}^*_1(6,7,8)$, *both twisted by* 2.

(ii) *Let* $E = [0, a_2, 0, a_4, a_6]$ *be the reduced minimal model of a curve* $\mathcal{E} \in \mathrm{II}^*(8,10,14)$. *Then*

$$\mathcal{E} \in \mathrm{I}^*_0(6,7,8) * 2 \quad \textit{iff} \quad \begin{cases} F(a_{4,2}) \equiv -2^5 \pmod{2^7} & \textit{if } a_2 = 0, \\ F(a_2) \equiv -2^5 \pmod{2^7} & \textit{if } a_2 = \pm 1. \end{cases}$$

$$\mathcal{E} \in \mathrm{I}^*_1(6,7,8) * 2 \quad \textit{iff} \quad \begin{cases} F(a_{4,2}) \equiv \phantom{-}2^5 \pmod{2^7} & \textit{if } a_2 = 0, \\ F(a_2) \equiv \phantom{-}2^5 \pmod{2^7} & \textit{if } a_2 = \pm 1. \end{cases}$$

*Proof.* (i) Let $\mathcal{E} = \mathcal{E}' * 2$ and let $E' = [0, a'_1, 0, a'_4, a'_6]$ be the reduced minimal model of $\mathcal{E}'$. Then $V(E') = (6,7,8)$, and the triple $(6,7,8)$ appears in Table 3.1 twice with Kodaira symbols $\mathrm{I}^*_0$ and $\mathrm{I}^*_1$. This proves the first part of the lemma.

(ii) We have $\mathcal{E} \in \mathrm{I}^*_0(6,7,8) * 2$ iff $\mathcal{E}' \in \mathrm{I}_0(6,7,8)$ iff $E'$ satisfies Condition 3, where $E'$ is a minimal model of $\mathcal{E}'$.

Let $F(X), G(X)$ be the polynomials corresponding to the model $E$, and $F_1(X), G_1(X)$ to the model $E'$. By Lemma 2.6 we have $G_1(w') \equiv 0 \pmod{32}$, where

$$w' = \begin{cases} a'_{4,1} & \text{if } a'_2 = 0, \\ -a'_2 & \text{if } a'_2 = \pm 1. \end{cases} \tag{3.5}$$

Condition 3 for $E'$ says that $F_1(w') \equiv -4 \pmod{16}$.

We have $F_1(X) = \frac{1}{8}F(2X + a'_2)$, and $a'_2 = -a_2$, $a'_4 = (a_4 + a_2^2)/4$ (see the proof of Lemma 3.7). Consequently, Condition 3 for $E'$ is equivalent to

$$F(a_{4,2}) \equiv -\,2^5 \pmod{2^7} \quad \text{if } a_2 = 0,$$
$$F(a_2) \equiv -\,2^5 \pmod{2^7} \quad \text{if } a_2 = \pm 1. \ ■$$

Lemma 3.15.

(i) *The class* $\mathrm{II}^*(\nu,10,14)$, *where* $\nu \geq 9$, *is the disjoint union of the classes* $\mathrm{I}_0^*(\nu-2,7,8)$ *and* $\mathrm{IV}^*(\nu-2,7,8)$, *both twisted by* 2.

(ii) *Let* $E=[0,a_2,0,a_4,a_6]$ *be the reduced minimal model of a curve* $\mathcal{E}\in \mathrm{II}^*(\nu,10,14)$. *Then*

$$\mathcal{E}\in \mathrm{I}_0^*(\nu-2,7,8)*2 \quad \textit{iff} \quad \begin{cases} F(a_{4,2})\equiv -2^5 \pmod{2^7} & \textit{if } a_2=0,\\ F(-3a_2)\equiv -2^5 \pmod{2^7} & \textit{if } a_2=\pm 1.\end{cases}$$

$$\mathcal{E}\in \mathrm{IV}^*(\nu-2,7,8)*2 \quad \textit{iff} \quad \begin{cases} F(a_{4,2})\equiv \ \ 2^5 \pmod{2^7} & \textit{if } a_2=0,\\ F(-3a_2)\equiv \ \ 2^5 \pmod{2^7} & \textit{if } a_2=\pm 1.\end{cases}$$

*Proof.* The proof goes along the lines of the proof of Lemma 3.14, with one exception: In the case $a_2'=\pm1$ we now have $w'=a_2'$, by Lemma 2.6. Consequently,

$$F_1(w')=\tfrac{1}{8}F(2a_2'+a_2')=\tfrac{1}{8}F(3a_2')=\tfrac{1}{8}F(-3a_2). \ \blacksquare$$

**3.3. Main Theorem.** The above considerations lead to the following theorem.

Theorem 3.1. *Let* $\mathcal{E}_2 := \mathcal{E}*2$.

(i) *If* $v(N(\mathcal{E}))>6$, *then* $v(N(\mathcal{E}_2))=v(N(\mathcal{E}))$. *Moreover, the corresponding Kodaira classes are:*

| $\mathcal{E}$ | II | III | $\mathrm{I}_2^*$ | $\mathrm{III}^*$ |
|---|---|---|---|---|
| $\mathcal{E}_2$ | $\mathrm{I}_2^*$ | $\mathrm{III}^*$ | II | III |

(ii) *If* $v(N(\mathcal{E}))\leq 6$, *then* $v(N(\mathcal{E}_2))\leq 6$. *More precisely,* $v(N(\mathcal{E}))=6$ *iff* $v(N(\mathcal{E}_2))<6$.

*Proof.* The theorem follows imediately from Table 3.1 and Lemmas 3.1–3.15.

For example, if $\mathcal{E}$ belongs to the class $\mathrm{I}_0^*(6,8,10)$, then $v(N(\mathcal{E}))=6$. By Lemma 3.4, $\mathcal{E}_2$ belongs to one of the classes $\mathrm{II}(4,5,4)$, $\mathrm{III}(4,5,4)$ or $\mathrm{IV}(4,5,4)$, hence $v(N(\mathcal{E}_2))=4,3$ or 2, by the corresponding lines of Table 3.1.

If $\mathcal{E}$ belongs to the class $\mathrm{I}_2^*(6,9,13)$, then $\mathcal{E}_2 \in$II(4,6,7), by Table 3.1. Moreover, $v(N(\mathcal{E}))=7$ and $v(N(\mathcal{E}_2))=7$.

The proof in the remaining cases is similar. $\blacksquare$

## 4. The case $p=3$ and $d=-3$

**4.1. Table 4.1.** Table 4.1 shows the Kodaira classes (for $p=3$) of curves $\mathcal{E}$, refined in such a way that every subclass is mapped by the twist by $-3$ onto some other subclass. Moreover, all curves in a subclass have conductors divisible by the same power of 3. We define $f_3 := v(N(E))$ and $f_3' := v(N(E'))$, where $E' := E*(-3)$. It is known that $0\leq v(N(E))\leq 5$ (see [Ser] and [LRS]).

**4.2. Additional conditions and comments.** We now deal with reduction modulo 3, so we may assume $a_1=a_3=0$ in the Weierstrass model (minimal locally at $p=3$). As noted earlier, this simplifies computations considerably.

Only two valuation triples are problematic, namely $V(E)=(\nu,3,3)$ with $\nu\geq 2$ (corresponding to Kodaira symbols II and III), and $V(E)=(\nu,6,9)$ with $\nu\geq 4$ (corresponding to Kodaira symbols III* and IV*). All other valuation triples uniquely define the Kodaira symbol (see [Pa, Table II]).

Lemma 4.1. *For every $\nu \geq 2$ the twist by $-3$ gives a one-to-one correspondence between the set of curves $\mathcal{E}_1$ with a minimal model $E_1$ satisfying $V(E_1) = (\nu, 3, 3)$, and the set of curves $\mathcal{E}_2$ with a minimal model $E_2$ satisfying $V(E_2) = (\nu + 2, 6, 9)$.*

*Proof.* Let $E_1$ be as stated. Then $V(E_1 * (-3)) = (\nu + 2, 3 + 3, 3 + 6) = (\nu + 2, 6, 9)$.

Conversely, given $E_2$ as above, we have $V(E_2 * (-3)) = ((\nu + 2) + 2, 6 + 3, 9 + 6) = (\nu + 4, 9, 15)$. This triple does not correspond to any minimal model, by [Pa, Table II]. Therefore $V(E_2 * (-3)) = ((\nu + 4) - 4, 9 - 6, 15 - 12) = (\nu, 3, 3) = V(E_1)$.

The correspondence is one-to-one, since $(\mathcal{E}_j * (-3)) * (-3) = \mathcal{E}_j$ for $j = 1, 2$. ■

Let us recall Conditions $\mathrm{P}_2$ and $\mathrm{P}_5$ used by Papadopoulos [Pa]:

$\mathrm{P}_2$ : $c_{6,3}^2 + 2 \equiv 3c_{4,2} \pmod 9$, provided $V(E) = (\nu, 3, 3)$, $\nu \geq 2$.
$\mathrm{P}_5$ : $c_{6,6}^2 + 2 \equiv 3c_{4,4} \pmod 9$, provided $V(E) = (\nu, 6, 9)$, $\nu \geq 4$.

Lemma 4.2. *Let $E$ be a minimal model such that $V(E) = (\nu, 3, 3)$ with $\nu \geq 2$. Then $E$ satisfies Condition $\mathrm{P}_2$ iff $E' := E * (-3)$ satisfies Condition $\mathrm{P}_5$.*

*Proof.* By Lemma 4.1, we have $V(E') = (\nu + 2, 6, 9)$. Moreover, $c_4' = 9c_4$ and $c_6' = -27c_6$. Hence $c_{4,4}' = c_{4,2}$ and $c_{6,6}' = -c_{6,3}$. Consequently, $c_{6,3}^2 + 2 - 3c_{4,2} = c_{6,6}'^2 + 2 - 3c_{4,4}'$. Thus Condition $\mathrm{P}_2$ holds for $E$ iff Condition $\mathrm{P}_5$ holds for $E'$. ■

**4.3. Main Theorem.** The above considerations lead to the following theorem.

Theorem 4.1. *Let $\mathcal{E}_{-3} := \mathcal{E} * (-3)$.*

(i) *If $v(N(\mathcal{E})) > 2$, then $v(N(\mathcal{E}_{-3})) = v(N(\mathcal{E}))$.*
(ii) *If $v(N(\mathcal{E})) < 2$, then $v(N(\mathcal{E}_{-3})) = 2$, and $\mathcal{E}_{-3}$ has Kodaira symbol $\mathrm{I}_\nu^*$ for some $\nu \geq 0$.*
(iii) *$v(N(\mathcal{E})) = v(N(\mathcal{E}_{-3})) = 2$ iff $\mathcal{E}$ has Kodaira symbol* III *or* III*.

*Proof.* The theorem follows immediately from Table 4.1. ■

Corollary 4.1.

(i) *If the curve $\mathcal{E}$ has Kodaira symbol* III *or* III* *for $p = 3$, and $\mathcal{E}'$ is isogenous with $\mathcal{E}$, then the Kodaira symbol of $\mathcal{E}'$ belongs to the set* {III, III*}.
(ii) *Also the set* {II, IV, II*, IV*} *of Kodaira symbols is preserved under isogenies.*

*Proof.* (i) From Table 4.1 it follows that $v(N(\mathcal{E})) = 2$, hence $v(N(\mathcal{E}')) = 2$, since conductors do not change under isogenies.

Assume that the Kodaira symbol of $\mathcal{E}'$ is neither III nor III*. Then from Table 4.1 it must be $\mathrm{I}_\nu^*$ for some $\nu \geq 0$. Therefore the twist $\mathcal{E}' * (-3)$ must have Kodaira symbol $\mathrm{I}_\nu$, and hence $v(N(\mathcal{E}' * (-3))) = 0$ or 1.

On the other hand, from Theorem 4.1(iii) we know that $v(N(\mathcal{E} * (-3))) = 2$. This constitutes a contradiction, since twists commute with isogenies: by the assumption on $\mathcal{E}$ and $\mathcal{E}'$, the twists $\mathcal{E} * (-3)$ and $\mathcal{E}' * (-3)$ must be isogenous, so they must have the same conductor.

(ii) The claim follows from the observation that $v(N(\mathcal{E})) \geq 3$ iff the Kodaira symbol of $\mathcal{E}$ belongs to the set {II, IV, II*, IV*} (see Table 4.1). ■

**5. The case $p > 3$.** Table 5.1 shows the classes of curves $\mathcal{E}$ and their twists by $p^*$. The present situation is easiest of all. One can assume $a_1 = a_3 = 0$ in the Weierstrass equations, thereby making twist data easy to compute. Most pertinent, however, is the fact that for $p > 3$ valuation triples uniquely determine the Kodaira symbol—without exception. Consequently, all the necessary information can be determined easily, if not directly, from the data in Table I of Papadopoulos [Pa]. Despite the trivial nature of the computations (which amount to nothing more than looking at valuation triples in Table I of [Pa] and noting that each twist satisfies $V(E*p) = V(E) + (2,3,6)$) we would nonetheless wish the paper to be as self-contained as possible. For the convenience of the reader we present the relevant data in Table 5.1.

## 6. Nonquadratic twists

**6.1. General remarks.** Let $\mathcal{E}$, $\mathcal{E}'$ be elliptic curves defined over $\mathbb{Q}$. Every isomorphism $\sigma : \mathcal{E} \to \mathcal{E}'$ defined over the algebraic closure of $\mathbb{Q}$ is called a *twist*. Then we say that the curve $\mathcal{E}'$ is a *twist* of $\mathcal{E}$.

We considered above only quadratic twists $\mathcal{E} \to \mathcal{E} * d$, i.e. isomorphisms defined over quadratic fields $\mathbb{Q}(\sqrt{d})$, where $d \neq 0$ is taken modulo squares. For every $\mathcal{E}$ and every $d \in \mathbb{Z}$, $d \neq 0$ there is a uniquely defined quadratic twist $\mathcal{E} * d$. Namely, if $E = [0, a_2, 0, a_4, a_6]$ is a model of $\mathcal{E}$, then $E * d := [0, da_2, 0, d^2a_4, d^3a_6]$ is a model of the twisted curve $\mathcal{E} * d$.

It is known that for some curves there are also twists defined over fields of degrees greater than 2 (see [Si1, Proposition 5.4]).

More precisely, for curves $\mathcal{E}$ satisfying $c_6 = 0$ (or equivalently, $j = 1728$) there are quartic twists $\mathcal{E} *_4 d$, where $d$ is a nonzero integer taken modulo fourth powers. Namely, such a curve has a model $E = [0, 0, 0, a_4, 0]$. Then $E *_4 d := [0, 0, 0, da_4, 0]$ is a model of $\mathcal{E} *_4 d$.

For curves $\mathcal{E}$ satisfying $c_4 = 0$ (or equivalently, $j = 0$) there are sextic twists $\mathcal{E} *_6 d$, where $d$ is a nonzero integer taken modulo sixth powers. Namely, such a curve has a model $E = [0, 0, 0, 0, a_6]$. Then $E *_6 d := [0, 0, 0, 0, da_6]$ is a model of $\mathcal{E} *_6 d$.

From the definitions it follows that if $E = [0, a_2, 0, a_4, a_6]$ is a model of $\mathcal{E}$, then the corresponding twists by $d$ give the following mappings:

$$\begin{aligned} \text{The quadratic twist:} \quad & (X, Y) \mapsto (dX, d^{3/2}Y). \\ \text{The quartic twist:} \quad & (X, Y) \mapsto (d^{1/2}X, d^{3/4}Y). \\ \text{The sextic twist:} \quad & (X, Y) \mapsto (d^{1/3}X, d^{1/2}Y). \end{aligned}$$

These twists are defined over the fields $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt[4]{d})$ and $\mathbb{Q}(\sqrt[6]{d})$, respectively.

There are the following obvious relations between twists:

$$(\mathcal{E} * d_1) * d_2 = \mathcal{E} * (d_1 d_2)$$

(and similar formulas for quartic and sextic twists),

$$\mathcal{E} * d^2 = \mathcal{E}, \quad \mathcal{E} *_4 d^4 = \mathcal{E}, \quad \mathcal{E} *_6 d^6 = \mathcal{E}, \quad \mathcal{E} *_4 d^2 = \mathcal{E} * d, \quad \mathcal{E} *_6 d^3 = \mathcal{E} * d.$$

We can also define the cubic twist $\mathcal{E} *_3 d := \mathcal{E} *_6 d^2$ for curves satisfying $c_4 = 0$, but we shall not use it. The cubic twist by $d$ corresponds to the mapping $(X, Y) \mapsto (d^{2/3}X, dY)$ defined over the cubic field $\mathbb{Q}(\sqrt[3]{d})$.

We shall describe the action of nonquadratic twists on Kodaira classes in the cases $p=2,\ p=3$ and $p>3$ separately.

**6.2. Quartic twists in the case $p=2$.** For convenience we use the following notation. For a nonzero integer $a$ let $\mathrm{odd}(a):=a/2^{v_2(a)}$, i.e. $\mathrm{odd}(a)$ is the maximal odd divisor of $a$ with the same sign as $a$.

Let $E=[0,0,0,a_4,0]$. Then $c_4=-2^4\cdot 3a_4$ and $\Delta(E)=-2^6a_4^3$. Consequently, $\mathrm{odd}(c_4)=-3\cdot\mathrm{odd}(a_4)\equiv\mathrm{odd}(a_4)\equiv\pm1 \pmod 4$.

Let $E':=E*_4(-1)=[0,0,0,a_4',0]$, where $a_4'=-a_4$. Then $\mathrm{odd}(c_4')=-\mathrm{odd}(c_4)$.

Condition 1 for $E$ says that $F(a_4)\equiv 2 \pmod 4$, i.e. $a_4^3+a_4^2\equiv 2 \pmod 4$. Equivalently $a_4\equiv 1 \pmod 4$.

Condition 5 for $E$ says that $c_{4,6}\equiv -1 \pmod 4$, equivalently, $a_{4,2}\equiv -1 \pmod 4$.

From Table 2.1 we find that there are six Kodaira classes with $c_6=0$, i.e. with $\nu=v(c_6)=\infty$:

| Kodaira class | Additional condition | $f$ |
|---|---|---|
| $\mathrm{II}(4,\infty,6)$ | $a_4\equiv 1 \pmod 4$ | 6 |
| $\mathrm{III}(4,\infty,6)$ | $a_4\equiv -1 \pmod 4$ | 5 |
| $\mathrm{III}(5,\infty,9)$ | $a_{4,1}\equiv \pm1 \pmod 4$ | 8 |
| $\mathrm{I}_2^*(6,\infty,12)$ | $a_{4,2}\equiv 1 \pmod 4$ | 6 |
| $\mathrm{I}_3^*(6,\infty,12)$ | $a_{4,2}\equiv 1 \pmod 4$ | 5 |
| $\mathrm{III}^*(7,\infty,15)$ | $a_{4,3}\equiv \pm1 \pmod 4$ | 8 |

The classes $\mathrm{III}(5,\infty,9)$ and $\mathrm{III}^*(7,\infty,15)$ can each be divided into two subclasses, according to the residue of $\mathrm{odd}(a_4)$ modulo 4:

$$\begin{aligned}
\mathrm{III}(5,\infty,9)^- &:= \{\mathcal{E}\in \mathrm{III}(5,\infty,9) : a_{4,1}\equiv -1 \pmod 4\},\\
\mathrm{III}(5,\infty,9)^+ &:= \{\mathcal{E}\in \mathrm{III}(5,\infty,9) : a_{4,1}\equiv 1 \pmod 4\},\\
\mathrm{III}^*(7,\infty,15)^- &:= \{\mathcal{E}\in \mathrm{III}^*(7,\infty,15) : a_{4,3}\equiv -1 \pmod 4\},\\
\mathrm{III}^*(7,\infty,15)^+ &:= \{\mathcal{E}\in \mathrm{III}^*(7,\infty,15) : a_{4,3}\equiv 1 \pmod 4\}
\end{aligned}$$

Now it is easy to describe the action of quartic twists by $-1$ on these Kodaira classes:

| $\mathcal{E}$ | $\mathcal{E}*_4(-1)$ | $\mathcal{E}*(-1)$ | Conductor exponents | | |
|---|---|---|---|---|---|
| $\mathrm{II}(4,\infty,6)$ | $\mathrm{III}(4,\infty,6)$ | $\mathrm{II}(4,\infty,6)$ | 6 | 5 | 6 |
| $\mathrm{III}(5,\infty,9)^-$ | $\mathrm{III}(5,\infty,9)^+$ | $\mathrm{III}(5,\infty,9)^-$ | 8 | 8 | 8 |
| $\mathrm{I}_2^*(6,\infty,12)$ | $\mathrm{I}_3^*(6,\infty,12)$ | $\mathrm{I}_2^*(6,\infty,12)$ | 6 | 5 | 6 |
| $\mathrm{III}^*(7,\infty,15)^-$ | $\mathrm{III}^*(7,\infty,15)^+$ | $\mathrm{III}^*(7,\infty,15)^-$ | 8 | 8 | 8 |

It is also easy to describe the action of quartic twists by 2 on the Kodaira classes, taking into account that $a_4'=2a_4$, hence $\mathrm{odd}(a_4')=\mathrm{odd}(a_4)$:

| $\mathcal{E}$ | $\mathcal{E}*_4 2$ | $\mathcal{E}*2$ | $\mathcal{E}*_4 8$ | Cond. exp. | | | |
|---|---|---|---|---|---|---|---|
| $\mathrm{II}(4,\infty,6)$ | $\mathrm{III}(5,\infty,9)^+$ | $\mathrm{I}_3^*(6,\infty,12)$ | $\mathrm{III}^*(7,\infty,15)^+$ | 6 | 8 | 5 | 8 |
| $\mathrm{III}(4,\infty,6)$ | $\mathrm{III}(5,\infty,9)^-$ | $\mathrm{I}_2^*(6,\infty,12)^-$ | $\mathrm{III}^*(7,\infty,15)^-$ | 5 | 8 | 6 | 8 |

From these tables we immediately get the following result.

Theorem 6.1. *Let $\mathcal{E}$ satisfy $j = 1728$, and let $p = 2$. Then $v(N(\mathcal{E})) \in \{5, 6, 8\}$. Moreover:*

(i) *$v(N(\mathcal{E})) = 5$ iff $v(N(\mathcal{E} *_4 (-1))) = 6$.*
(ii) *$v(N(\mathcal{E})) = 8$ iff $v(N(\mathcal{E} *_4 (-1))) = 8$.*
(iii) *$v(N(\mathcal{E})) = 8$ iff $v(N(\mathcal{E} *_4 2)) < 8$.*

**6.3. Sextic twists in the case $p = 2$.** For $\mathcal{E}$ satisfying $j = 0$ there is a model $E = [0, 0, 0, 0, a_6]$. Then $c_6 = -2^5 \cdot 3^3 a_6$ and $\Delta(E) = -2^4 \cdot 3^3 a_6^2$. Consequently, $\mathrm{odd}(c_6) = -3^3 \cdot \mathrm{odd}(a_6) \equiv \mathrm{odd}(a_6) \equiv \pm 1 \pmod 4$.

Let $E' := E *_6 d = [0, 0, 0, 0, a_6']$. Then $a_6' = da_6$. Hence $\mathrm{odd}(a_6') = \mathrm{odd}(d) \cdot \mathrm{odd}(a_6)$.

Condition 0 for $E$ says that $c_{6,9} \equiv -1 \pmod 4$, equivalently $a_{6,4} \equiv -1 \pmod 4$.

In the case $v(\Delta) = 4$, i.e. for $a_6$ odd, Condition 1 for $E$ says that $F(a_4) \equiv 3 \pmod 4$. Equivalently, $a_6 \equiv -1 \pmod 4$.

Condition 3 for $E$ says that if $G(w) \equiv 0 \pmod{32}$, then $F(w) \equiv 12 \pmod{16}$. In our case $G(X) = 3X^4 + 12a_6 X$, so we can choose $w = 0$, and then Condition 3 takes the form $a_6 \equiv 12 \pmod{16}$, i.e. $a_{6,2} \equiv -1 \pmod 4$.

From Table 2.1 we find that there are nine Kodaira classes with $c_4 = 0$, i.e. with $\nu = v(c_4) = \infty$:

| Kodaira class | Additional condition | $f$ |
|---|---|---|
| $\mathrm{I}_0(\infty, 9, 12)'$ | $a_{6,4} \equiv -1 \pmod 4$ | 0 |
| $\mathrm{II}(\infty, 5, 4)$ | $a_6 \equiv -1 \pmod 4$ | 4 |
| $\mathrm{II}(\infty, 6, 6)$ | $a_{6,1} \equiv \pm 1 \pmod 4$ | 6 |
| $\mathrm{IV}(\infty, 5, 4)$ | $a_6 \equiv 1 \pmod 4$ | 2 |
| $\mathrm{I}_0^*(\infty, 7, 8)$ | $a_{6,2} \equiv -1 \pmod 4$ | 4 |
| $\mathrm{I}_0^*(\infty, 8, 10)$ | $a_{6,3} \equiv \pm 1 \pmod 4$ | 6 |
| $\mathrm{IV}^*(\infty, 7, 8)$ | $a_{6,2} \equiv 1 \pmod 4$ | 2 |
| $\mathrm{II}^*(\infty, 9, 12)$ | $a_{6,4} \equiv 1 \pmod 4$ | 4 |
| $\mathrm{II}^*(\infty, 10, 14)$ | $a_{6,5} \equiv \pm 1 \pmod 4$ | 6 |

As above, we divide the classes $\mathrm{II}(\infty, 6, 6)$, $\mathrm{I}_0^*(\infty, 8, 10)$ and $\mathrm{II}^*(\infty, 10, 14)$ into two subclasses each, according to the residue modulo 4 of $\mathrm{odd}(a_6)$. We denote the subclasses using superscripts $+$ and $-$, as above.

From $(-1)^3 = -1$ it follows that

$$\mathcal{E} *_6 (-1) = \mathcal{E} *_6 (-1)^3 = \mathcal{E} * (-1),$$

i.e. the sextic twists by $-1$ coincide with the quadratic twists by $-1$. These last twists have been described above in Tables 2.1 and 2.2.

Namely, if $E = [0, 0, 0, 0, a_6]$ and $E' := E * (-1) = [0, 0, 0, 0, a_6']$, $a_6' = -a_6$, then $\mathrm{odd}(a_6') = -\mathrm{odd}(a_6)$, and consequently the quadratic twist by $-1$ acts on Kodaira classes as follows:

| $\mathcal{E}$ | $\mathcal{E}' := \mathcal{E} * (-1)$ | $f$ | $f'$ |
|---|---|---|---|
| $\mathrm{I}_0(\infty, 9, 12)'$ | $\mathrm{II}^*(\infty, 9, 12)$ | 0 | 4 |
| $\mathrm{II}(\infty, 5, 4)$ | $\mathrm{IV}(\infty, 5, 4$ | 4 | 2 |
| $\mathrm{II}(\infty, 6, 6)^-$ | $\mathrm{II}(\infty, 6, 6)^+$ | 6 | 6 |
| $\mathrm{I}_0^*(\infty, 7, 8)$ | $\mathrm{IV}^*(\infty, 7, 8)$ | 4 | 2 |
| $\mathrm{I}_0^*(\infty, 8, 10)^-$ | $\mathrm{I}_0^*(\infty, 8, 10)^+$ | 6 | 6 |
| $\mathrm{II}^*(\infty, 10, 14)^-$ | $\mathrm{II}^*(\infty, 10, 14)^+$ | 6 | 6 |

It is easy to describe the action of sextic twists by 2 on Kodaira classes taking into account that $a_6' = 2a_6$, hence $\mathrm{odd}(a_6') = \mathrm{odd}(a_6)$:

| $\mathcal{E}$ | $\mathrm{II}(\infty, 5, 4)$ | $\mathrm{IV}(\infty, 5, 4)$ | 4 | 2 |
|---|---|---|---|---|
| $\mathcal{E} *_6 2$ | $\mathrm{II}(\infty, 6, 6)^-$ | $\mathrm{II}(\infty, 6, 6)^+$ | 6 | 6 |
| $\mathcal{E} *_6 4$ | $\mathrm{I}_0^*(\infty, 7, 8)$ | $\mathrm{IV}^*(\infty, 7, 8)$ | 4 | 2 |
| $\mathcal{E} *_6 8$ | $\mathrm{I}_0^*(\infty, 8, 10)^-$ | $\mathrm{I}_0^*(\infty, 8, 10)^+$ | 6 | 6 |
| $\mathcal{E} *_6 16$ | $\mathrm{I}_0(\infty, 9, 12)'$ | $\mathrm{II}(\infty, 9, 12)$ | 0 | 4 |
| $\mathcal{E} *_6 32$ | $\mathrm{II}^*(\infty, 10, 14)^-$ | $\mathrm{II}^*(\infty, 10, 14)^+$ | 6 | 6 |

In the last column of the table, the corresponding conductor exponents are given.

From these tables we immediately get the following result.

THEOREM 6.2. *Let $\mathcal{E}$ satisfy $j = 0$, and let $p = 2$. Then $v(N(\mathcal{E})) \in \{0, 2, 4, 6\}$. Moreover:*

(i) $v(N(\mathcal{E})) < 4$ *iff* $v(N(\mathcal{E} *_6 (-1))) = 4$.
(ii) $v(N(\mathcal{E})) = 6$ *iff* $v(N(\mathcal{E} *_6 (-1))) = 6$.
(iii) $v(N(\mathcal{E})) < 6$ *iff* $v(N(\mathcal{E} *_6 2)) = 6$.

If $q > 2$ is a prime, then $q^* = (-1)^{(q-1)/2} q \equiv 1 \pmod 4$. Hence $q^* \cdot \mathrm{odd}(a_6) \equiv \mathrm{odd}(a_6) \pmod 4$. Consequently, sextic twists by $q^*$ do not change Kodaira classes.

**6.4. Quartic twists in the case $p = 3$.** For $\mathcal{E}$ satisfying $j = 1728$ there is a model $E = [0, 0, 0, a_4, 0]$. Then $c_4 = -2^4 \cdot 3 \cdot a_4$. Hence $v(c_4) = v(a_4) + 1$.

From Table 4.1 we see that there are four Kodaira classes satisfying $c_6 = 0$, i.e. $\nu = v(c_6) = \infty$:

$$\mathrm{I}_0(1, \infty, 0), \quad \mathrm{III}(2, \infty, 3), \quad \mathrm{I}_0^*(3, \infty, 6), \quad \mathrm{III}^*(4, \infty, 9),$$

with the conductor exponents equal to $0, 2, 2, 2$, respectively.

For $d$ not divisible by 3 we have $E' := E *_4 d = [0, 0, 0, da_4, 0]$ and $v(da_4) = v(a_4)$. Then $v(c_4') = v(c_4)$, and consequently these four Kodaira classes are invariant under quartic twists by $d$.

Now let $d = 3$. Then $v(da_4) = 1 + v(a_4)$. Hence $v(c_4') = 1 + v(c_4)$. Consequently, the quartic twists by 3 map the four Kodaira classes as follows:

$$\mathrm{I}_0(1, \infty, 0) \mapsto \mathrm{III}(2, \infty, 3) \mapsto \mathrm{I}_0^*(3, \infty, 6) \mapsto \mathrm{III}^*(4, \infty, 9) \mapsto \mathrm{I}_0(1, \infty, 0).$$

From this we immediately get

THEOREM 6.3. *Let $\mathcal{E}$ satisfy $j = 1728$ and let $p = 3$. Then $v(N(\mathcal{E})) \in \{0, 2\}$. Moreover, $v(N(\mathcal{E})) = 0$ implies $v(N(\mathcal{E} *_4 3)) = 2$.*

**6.5. Sextic twists in the case $p = 3$.** For $\mathcal{E}$ satisfying $j = 0$ there is a model $E = [0, 0, 0, 0, a_6]$. Then $c_6 = -2^5 \cdot 3^3 a_6$ and $\Delta(E) = -2^4 \cdot 3^3 a_6^2$. Hence $v(\Delta) = 2v(c_6) - 3$ and $v(c_6) = 3 + v(a_6)$.

From Table 4.1 we see that there are eight Kodaira classes satisfying $c_4 = 0$, i.e. $\nu = v(c_4) = \infty$:

$$\mathrm{II}(\infty, 3, 3), \quad \mathrm{II}(\infty, 4, 5), \quad \mathrm{III}(\infty, 3, 3), \quad \mathrm{IV}(\infty, 5, 7),$$
$$\mathrm{IV}^*(\infty, 6, 9), \quad \mathrm{IV}^*(\infty, 7, 11), \quad \mathrm{III}^*(\infty, 6, 9), \quad \mathrm{II}^*(\infty, 8, 13).$$

Since $c_4 = 0$, Condition $\mathrm{P}_2$ for $E$ says that $c_{6,3}^2 + 2 \equiv 0 \pmod 9$, provided $V(E) = (\infty, 3, 3)$. Equivalently, $a_6 \equiv \pm 1 \pmod 9$.

Similarly, Condition $\mathrm{P}_5$ for $E$ says that $c_{6,6}^2 + 2 \equiv 0 \pmod 9$, provided $V(E) = (\infty, 6, 9)$. Equivalently, $a_{6,3} \equiv \pm 1 \pmod 9$.

It turns out that the sextic twist by 3, and also by $d$ not divisible by 3, can change the Kodaira class, in general. To describe the situation, we divide the eight Kodaira classes given above into subclasses as follows.

We use the following notation. For a nonzero integer $a$ let

$$3\text{-free}(a) := a/3^{v_3(a)}.$$

Thus 3-free$(a)$ is the maximal divisor of $a$ not divisible by 3 and with the same sign as $a$.

Every integer $d$ not divisible by 3 satisfies exactly one of the following six congruences:

$$d \equiv \pm 1, \ \pm 2, \ \pm 4 \pmod 9.$$

For every Kodaira class $\mathbb{K} = \mathbb{K}(\infty, v(c_6), v(\Delta))$ as above we define the subclasses

$$\mathbb{K}(\infty, v(c_6), v(\Delta))^k := \{\mathcal{E} \in \mathbb{K} : 3\text{-free}(a_6) \equiv \pm 2^k \pmod 9\},$$

where $k$ is taken modulo 3.

Let us observe that the subclass $\mathrm{II}(\infty, 3, 3)^0$ is empty, because no curve belonging to $\mathrm{II}(\infty, 3, 3)$ satisfies Condition $\mathrm{P}_2$, i.e. 3-free$(a_6) = a_6 \not\equiv \pm 1 \pmod 9$.

Similarly, the subclass $\mathrm{IV}^*(\infty, 6, 9)^0$ is empty.

On the other hand, since every curve in $\mathrm{III}(\infty, 3, 3)$ satisfies Condition $\mathrm{P}_2$, we have $\mathrm{III}(\infty, 3, 3) = \mathrm{III}(\infty, 3, 3)^0$. Similarly, $\mathrm{III}^*(\infty, 3, 3) = \mathrm{III}^*(\infty, 3, 3)^0$, etc.

For simplicity we denote a subclass of the form $\mathbb{K}(\infty, v(c_6), v(\Delta))^k$ by $\mathbb{K}(v(c_6))^k$, since $v(\Delta)$ is uniquely determined by $v(c_6)$.

If $\mathcal{E} \in \mathbb{K}(m)^k$, then $\mathcal{E} *_6 3 \in \mathbb{K}'(m+1)^k$, where $m - 3$ is taken modulo 6, and $\mathcal{E} *_6 2 \in \mathbb{K}''(m)^{k+1}$, where $k + 1$ is taken modulo 3, and $\mathbb{K}'$, $\mathbb{K}''$ are appropriate Kodaira symbols. It turns out that these symbols are uniquely determined by $\mathbb{K}$, $k$ and $m$. We collect the results in the following table:

| | $\mathcal{E}$ | $\mathcal{E} *_6 3$ | $\mathcal{E} *_6 3^2$ | $\mathcal{E} *_6 3^3$ | $\mathcal{E} *_6 3^4$ | $\mathcal{E} *_6 3^5$ |
|---|---|---|---|---|---|---|
| $\mathcal{E}$ | $\mathrm{III}(3)^0$ | $\mathrm{II}(4)^0$ | $\mathrm{IV}(5)^0$ | $\mathrm{III}^*(6)^0$ | $\mathrm{IV}^*(7)^0$ | $\mathrm{II}^*(8)^0$ |
| $\mathcal{E} *_6 2$ | $\mathrm{II}(3)^1$ | $\mathrm{II}(4)^1$ | $\mathrm{IV}(5)^1$ | $\mathrm{IV}^*(6)^1$ | $\mathrm{IV}^*(7)^1$ | $\mathrm{II}^*(8)^1$ |
| $\mathcal{E} *_6 4$ | $\mathrm{II}(3)^2$ | $\mathrm{II}(4)^2$ | $\mathrm{IV}(5)^2$ | $\mathrm{IV}^*(6)^2$ | $\mathrm{IV}^*(7)^2$ | $\mathrm{II}^*(8)^2$ |

The corresponding conductor exponents are

| | | | | | |
|---|---|---|---|---|---|
| 2 | 5 | 5 | 2 | 5 | 5 |
| 3 | 5 | 5 | 3 | 5 | 5 |
| 3 | 5 | 5 | 3 | 5 | 5 |

From this table it follows that

| $\mathcal{E}$ | II(3) | II(4) | IV$^*$(6) | IV$^*$(7) |
|---|---|---|---|---|
| $\mathcal{E} *_6 3$ | II(4) | IV(5) | IV$^*$(7) | II$^*$(8) |

For other Kodaira classes $\mathbb{K}(m)$ the sextic twists by 3 of curves in a given class can belong to distinct classes.

Similarly, the Kodaira classes II(4), IV(5), IV$^*$(7) and II$^*$(8) are invariant under the sextic twist by 2. Moreover, the classes III(3) and III$^*$(6) are mapped by the sextic twist by 2 into the classes II(3) and IV$^*$(6), respectively.

From the above tables we get the following result.

Theorem 6.4. *Let $\mathcal{E}$ satisfy $j = 0$, and let $p = 3$. Then $v(N(\mathcal{E})) \in \{2, 3, 5\}$. Moreover,*

(i) *If $v(N(\mathcal{E})) = 2$ then $v(N(\mathcal{E} *_6 2)) = 3$.*
(ii) *If $v(N(\mathcal{E})) = 3$ then $v(N(\mathcal{E} *_6 2)) \leq 3$.*
(iii) *$v(N(\mathcal{E})) = 5$ iff $v(N(\mathcal{E} *_6 2)) = 5$.*
(iv) *If $v(N(\mathcal{E})) < 5$ then $v(N(\mathcal{E} *_6 3)) = 5$.*

Now we discuss the sextic twists by an arbitrary nonzero integer $d$. We have $d = 3^m d_1$, where $3 \nmid d_1$ and $d_1 \equiv \pm 2^k \pmod 9$, $0 \leq k \leq 2$.

Therefore

$$\mathcal{E} *_6 d = (\mathcal{E} *_6 3^m) *_6 2^k,$$

and we can here replace $m$ by its residue modulo 6. Hence the Kodaira subclass containing $\mathcal{E} *_6 d$ can be determined from the table above, if we know to which subclass the curve $\mathcal{E}$ belongs.

It follows that for a curve belonging to a subclass $\mathbb{K}(m)^k$ we can obtain a curve belonging to any other subclass by applying the sextic twist by a number of the form $2^k 3^m$, where $0 \leq k \leq 2$, $0 \leq m \leq 5$.

**6.6. Quartic and sextic twists in the case $p > 3$.** For $p > 3$ and $j = 0$ or 1728 the Kodaira class of a curve is uniquely determined by $v_p(\Delta)$. For $d$ not divisible by $p$ the quartic and sextic twists by $d$ do not change $v_p(\Delta)$. Therefore such twists do not change Kodaira classes.

Thus it is sufficient to consider quartic and sextic twists by $p$. Let $\Delta_4$ and $\Delta_6$ be the discriminants of $E *_4 p$ and $E *_6 p$, respectively. Then $\Delta_4 = p^3\Delta$ and $\Delta_6 = p^2\Delta$, where $\Delta$ is the discriminant of $E$. Consequently, these twists determine the following cyclic permutations of the Kodaira classes:

- The quartic twists by $p$:

$$\mathrm{I}_0 \mapsto \mathrm{III} \mapsto \mathrm{I}_0^* \mapsto \mathrm{III}^*.$$

- The sextic twists by $p$:

$$\mathrm{I}_0 \mapsto \mathrm{II} \mapsto \mathrm{IV} \mapsto \mathrm{I}_0^* \mapsto \mathrm{IV}^* \mapsto \mathrm{II}^*.$$

In both cases we have

$$v_p(N(\mathcal{E})) = \begin{cases} 0 & \text{if } \mathcal{E} \in \mathrm{I}_0, \\ 2 & \text{otherwise.} \end{cases}$$

# II. Conductors

We now discuss some questions concerning conductors of elliptic curves defined over $\mathbb{Q}$. We also supply some numerical data, based on the tables of Cremona [Cr2], which may give some suggestions how to answer these questions.

## 7. Observations concerning conductors

**7.1. Which numbers are conductors?** The tables of elliptic curves are ordered according to the values of conductors $N$ of the curves. Looking at the tables one observes immediately that not every positive integer is a conductor. More precisely, the following necessary condition for $N$ to be a conductor is known:

$$\text{If } N \text{ is a conductor, then} \quad 2^9 \nmid N,\ 3^6 \nmid N,\ p^3 \nmid N \quad \text{for } p > 3. \tag{7.1}$$

It is natural to ask the following more precise questions:

1) Does the set of conductors contain a subset of positive density?
2) Does the set of conductors which are prime numbers contain a subset of positive relative density, with respect to the set of all prime numbers?

More precisely, the issue is whether the number

$$\limsup_{X\to\infty} \frac{\#\{N \le X : N \text{ is a prime conductor}\}}{\pi(X)}$$

is positive, where $\pi(X)$ is the number of prime numbers not exceeding $X$.

We do not know the answers to any of these questions. Nevertheless, we can deduce from (7.1) that the density of the set of conductors (if it exists) is less than 1. Define

$$\mathrm{Cond}(X) := \{N \le X : N \text{ is a conductor}\}.$$

We have

Theorem 7.1. *For the set* Cond$(X)$ *of conductors not greater than* $X$ *the following estimate from above holds:*

$$\#\,\mathrm{Cond}(X) \le 0.984039X + o(X).$$

*Proof.* By (7.1), we have

$$\begin{aligned}\#\,\mathrm{Cond}(X) &\le \#\{N \le X : 2^9 \nmid N,\ 3^6 \nmid N,\ p^3 \nmid N \text{ for } p > 3\} \\ &= \Big(1 - \frac{1}{2^9}\Big)\Big(1 - \frac{1}{3^6}\Big)\prod_{p>3}\Big(1 - \frac{1}{p^3}\Big)X + o(X).\end{aligned}$$

Now

$$\left(1-\frac{1}{2^9}\right)\left(1-\frac{1}{3^6}\right)\prod_{p>3}\left(1-\frac{1}{p^3}\right)=\left(1+\frac{1}{2^3}+\frac{1}{2^6}\right)\left(1+\frac{1}{3^3}\right)\prod_{p\geq 2}\left(1-\frac{1}{p^3}\right)$$
$$=\frac{511}{432}\,\zeta(3)^{-1}\approx 0.984039,$$

and the theorem follows. ■

Consequently, the set of numbers which are not conductors contains a subset of positive density:

$$\#\{N\leq X : N \text{ is not a conductor}\}\geq 0.015961X+o(X).$$

Only partial results are known concerning the prime numbers which are conductors (see [Ha], [Set]).

We do not even know whether there are infinitely many prime numbers which are conductors (respectively, which are not conductors).

Table 7.1 collects numerical data on the numbers of conductors belonging to some intervals. They show that the proportion of conductors in consecutive intervals of one thousand numbers each, is decreasing very slowly. On the other hand, the number of prime conductors is decreasing much faster.

Basing on these data one may expect that more than 2/3 of primes are not conductors, and more than 1/2 of all positive integers are conductors.

**7.2. Curves with conductors differing by a prime power.** We shall investigate the sets $\mathcal{E}(N)$ of elliptic curves with conductors of the form $N=p^k m$, where a prime $p$ and a positive integer $m$ not divisible by $p$ are fixed, and

$$\begin{aligned}0\leq k\leq 8 &\quad \text{if } p=2,\\ 0\leq k\leq 5 &\quad \text{if } p=3,\\ 0\leq k\leq 2 &\quad \text{if } p>3.\end{aligned}$$

We shall rather count the classes of the isogenous curves, than the curves themselves. Kenku [Ke] has proved that in an isogeny class there are at most eight elliptic curves. From his proof it even follows that in an isogeny class there can only be 1, 2, 3, 4, 6 or 8 curves. Consequently, the number of elliptic curves with a given conductor does not exceed eight times the number of isogeny classes.

We shall use the following shorthand notation:

$$\mathcal{E}(N)=1^{r_1}2^{r_2}3^{r_3}4^{r_4}6^{r_6}8^{r_8},$$

which means that in $\mathcal{E}(N)$ there are $r_j$ isogeny classes of cardinality $j$ for $j\in J:=\{1,2,3,4,6,8\}$.

Hence

$$\#\mathcal{E}(N)=r_1+2r_2+3r_3+4r_4+6r_6+8r_8=\sum_{j\in J} jr_j.$$

First, we consider the case $p=2$. From Theorem 2.1 we get

THEOREM 7.2. *For every odd $m$ we have*

$$\mathcal{E}(2^4 m) * (-1) = \bigcup_{k=0}^{3} \mathcal{E}(2^k m), \tag{7.2}$$

*and on the r.h.s. there is a union of pairwise disjoint sets.*

*Proof.* From Theorem 2.1 it follows that the twist by $-1$ maps the set on the l.h.s. of (7.2) onto the set on the r.h.s. ∎

Similarly, from Theorem 3.1 we get

THEOREM 7.3. *For every odd $m$ we have*

$$\mathcal{E}(2^6 m) * 2 = \bigcup_{k=0}^{5} \mathcal{E}(2^k m) \ (\textit{disjoint union}). \tag{7.3}$$

*Proof.* From Theorem 3.1 it follows that the twist by 2 maps the set on the l.h.s. of (7.3) onto the set on the r.h.s. ∎

From Theorems 7.2 and 7.3 it follows that for every odd $m$,

$$\#\mathcal{E}(2^4 m) = \sum_{k=0}^{3} \#\mathcal{E}(2^k m), \tag{7.4}$$

$$\#\mathcal{E}(2^6 m) = \sum_{k=0}^{5} \#\mathcal{E}(2^k m). \tag{7.5}$$

Let $r_{k,m}(j)$ be the number of isogeny classes of cardinality $j$ in the set $\mathcal{E}(2^k m)$ of elliptic curves of conductor $2^k m$, where $m$ is odd. Then from (7.4) and (7.5) we get, for $j \in J$,

$$r_{4,m}(j) = \sum_{k=0}^{3} r_{k,m}(j), \tag{7.6}$$

$$r_{6,m}(j) = \sum_{k=0}^{5} r_{k,m}(j) = 2\sum_{k=0}^{3} r_{k,m}(j) + r_{5,m}(j). \tag{7.7}$$

It follows that for fixed odd $m$, there are in general much more elliptic curves with conductors $2^4 m$ and $2^6 m$ than those with conductors $2^k m$ for $k = 0, 1, 2, 3, 5$.

The corresponding data for $1 \le m \le 51$ and $451 \le m \le 501$ are given in Tables 7.2 and 7.3. To distinguish the prime values of $m$ we use the bold font.

To save space, the columns corresponding to the conductors $2^4 m$ and $2^6 m$ are omitted, since, in view of (7.4) and (7.5), these columns are sums of all earlier ones. The empty set symbol Ø signifies that there are no curves belonging to the specified set.

Let us observe that for some values of $m$ there are no elliptic curves with conductors $2^k m$ for all $0 \le k \le 8$. For example, it is the case for $m = 191, 317$ and 479. Moreover, we have verified that for every prime $m < 659$ at least one of the classes $\mathcal{E}(2^k m)$, $0 \le k \le 8$, is empty, with two exceptions $m = 19$ and $m = 101$.

Looking at the tables we can make the following observation concerning the cardinalities $j$ of isogeny classes appearing in the columns $\mathcal{E}(2^k m)$:

| $j$ | $k$ |
|---|---|
| 1 | all |
| 2 | all |
| 3 | 0, 1, 4, 6 |
| 4 | all $\neq 7$ |
| 6 | 0, 1, 3, 4, 6 |
| 8 | 0, 1, 4, 6 |

Moreover, if $m$ is a prime number, then the cardinalities of isogeny classes are very small. They do not exceed 2, with some exceptions.

These observations make us suspect that the following statements may be true:

(i) For $N = 2^7 m$, where $m$ is odd, every isogeny class contains at most two curves.

(ii) For $N = 2^k m$, where $k \in \{2, 5, 8\}$ and $m$ is odd, every isogeny class contains 1, 2 or 4 curves.

(iii) If $m > 37$ is a prime number, then every isogeny class of curves with conductor $N = 2^k m,\ 0 \leq k \leq 8$, contains at most two curves.

Moreover, it can be observed that in general for $m$ prime there are very few elliptic curves with conductor $m$.

Now let $p = 3$. Denote by $\mathcal{E}(N)_{\mathrm{III}}$ the set of elliptic curves of conductor $N$ with Kodaira symbols III or III*. Then from Theorem 4.1 we get immediately

Theorem 7.4. *For every $m$ not divisible by* 3 *we have*

$$\mathcal{E}(3^2 m) * (-3) = \mathcal{E}(m) \cup \mathcal{E}(3m) \cup \mathcal{E}(3^2 m)_{\mathrm{III}} \quad (\textit{disjoint union}). \tag{7.6}$$

*Hence*

$$\#\mathcal{E}(3^2 m) = \#\mathcal{E}(m) + \#\mathcal{E}(3m) + \#\mathcal{E}(3^2 m)_{\mathrm{III}}. \tag{7.9}$$

Let $r_{k,m}(j)$ be the number of isogeny classes of cardinality $j$ in the set $\mathcal{E}(3^k m)$, where $3 \nmid m$. We define $r_{k,m}(j)_{\mathrm{III}}$ analogously, replacing $\mathcal{E}(3^k m)$ by $\mathcal{E}(3^k m)_{\mathrm{III}}$. Then (7.9) implies that

$$r_{2,m}(j) = r_{0,m}(j) + r_{1,m}(j) + r_{2,m}(j)_{\mathrm{III}}.$$

It follows that for a fixed $m$ not divisible by 3, there are, in general, more elliptic curves with conductor $3^2 m$ than those with conductors $m$ and $3m$. This is confirmed by the numerical data in Table 7.4.

Similarly, for $p > 3$ we can easily deduce from Table 5.1 that for fixed $m$ not divisible by $p$ there are, in general, more elliptic curves with conductor $p^2 m$ than those with conductors $m$ and $pm$.

**8. Estimates of $\#\mathcal{E}(N)$ and $\#\,\mathrm{Cond}(X)$.** We have the following obvious estimate from below:

Theorem 7.5. *There is an absolute constant $c_1 > 0$ such that*

$$\#\,\mathrm{Cond}(X) \geq c_1 X^{1/2}.$$

*Proof.* There is a curve $\mathcal{E}$ of conductor $N = 11$. Let a positive integer $d$ satisfy:

$$(d, 22) = 1, \qquad d \quad \text{is squarefree.} \tag{7.10}$$

Define $d^* := (-1)^{(d-1)/2} \cdot d$. Then the twisted curve $\mathcal{E} * d^*$ has conductor $11d^2$. Thus every number of the form $11d^2$, where $d$ satisfies (7.10), is a conductor.

Now, $11d^2 \le X$ iff $d \le \sqrt{11}X^{1/2}$, and the number of numbers $d \le X_1$ satisfying (7.10) is $\ge c_2X_1$, where $c_2 > 0$ is an effective constant. Consequently, $\#\operatorname{Cond}(X) \ge \sqrt{11}c_2X^{1/2}$. ∎

One can improve Theorem 7.5 as follows. E. Fouvry, M. Nair and G. Tenenbaum [FNT] proved the following estimate from below:

$$\sum_{N \le X} \#\mathcal{E}(N) \ge c_3X^{5/6}, \tag{7.11}$$

with an absolute constant $c_3 > 0$.

On the other hand, H. A. Helfgott and A. Venkatesh [HV] recently proved an estimate from above: $\#\mathcal{E}(N) \le c_4N^{0.22377}$, which has been improved to

$$\#\mathcal{E}(N) \le c_5N^{0.169} \tag{7.12}$$

by J. S. Ellenberg and A. Venkatesh [EV]. Here $c_4$ and $c_5$ are absolute constants. This considerably improves earlier estimates proved by L. B. Pierce [P], A. Brumer and J. H. Silverman [BS], and S. Wong [W].

The estimates (7.11) and (7.12) give:

Theorem 7.6. *There is an absolute constant* $c_6 > 0$ *such that*

$$\#\operatorname{Cond}(X) \ge c_6X^{0.664}.$$

*Proof.* In view of (7.11) and (7.12) we have

$$c_3X^{5/6} \le \sum_{N \le X} \#\mathcal{E}(N) \le c_5 \sum_{N \in \operatorname{Cond}(X)} N^{0.169} \le c_5X^{0.169} \cdot \#\operatorname{Cond}(X).$$

Since $5/6 = 0.833 = 0.169 + 0.664$, the result follows. ∎

All the recent upper bound estimates of $\#\mathcal{E}(N)$ follow directly from improved estimates of the 3-part $h_3(D)$ of class numbers corresponding to quadratic fields with discriminant $D$. Conjecturally, $h_3(D) \ll |D|^{\varepsilon}$, where $\varepsilon > 0$, from which it would follow that $\#\operatorname{Cond}(X)$ is bounded from below by $cX^{5/6-\varepsilon}$, where $c > 0$ is a constant depending on $\varepsilon$.

Of course, even such a conjecturally optimal estimate would still not lead to a density result for $\#\operatorname{Cond}(X)$, assuming that such density approaches are meaningful in the first place.

## References

[BS] A. Brumer and J. H. Silverman, *The number of elliptic curves over* $\mathbb{Q}$ *with conductor* $N$, Manuscripta Math. 91 (1996), 95–102.

[Co] S. Comalada, *Twists and reduction of an elliptic curve*, J. Number Theory 49 (1994), 45–62.

[Cr1] J. E. Cremona, private communication (June 2006).

[Cr2] —, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997, http://www.warwick.ac.uk/staff/J.E.Cremona/.

[EV] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Notices 2007, art. ID rnm002, 18 pp.

[FNT] E. Fouvry, M. Nair et G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France 120 (1992), 485–506.

[Ha] T. Hadano, *On the conductor of an elliptic curve with a rational point of order* 2, Nagoya Math. J. 53 (1974), 199–210.

[HV] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and* 3*-torsion in class groups*, J. Amer. Math. Soc. 19 (2006). 527–550.

[Ke] M. A. Kenku, *On the number of* $\mathbb{Q}$*-isomorphism classes of elliptic curves in each* $\mathbb{Q}$*-isogeny class*, J. Number Theory 15 (1982), 199–202.

[Kr] A. Kraus, *Quelques remarques à propos des invariants* $c_4, c_6$ *et* $\Delta$ *d'une courbe elliptique*, Acta Arith. 54 (1989), 75–80.

[LRS] P. Lockhart, M. Rosen, J. H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geom. 2 (1993), 569–601.

[Pa] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152.

[P] L. B. Pierce, *The* 3*-part of class numbers of quadratic fields*, J. London Math. Soc. 71 (2005), 579–598.

[Ser] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[Set] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. 10 (1975), 367–378.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[Si2] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[Ta] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable, IV (Antwerp, 1972), Lecture Notes in Math. 476, Springer, 1975, 33–52.

[W] S. Wong, *Exponents of class groups and elliptic curves*, J. Number Theory 89 (2001), 114–120; Corrigendum, ibid. 90 (2001), 376–377.

**Table 2.1**
$(p = 2)$

| No. | Kodaira class | Add. cond. | $v(N)$ | $v(j)$ | $\nu$ | Tate case |
|---|---|---|---|---|---|---|
| 1 | $\mathrm{I}_0(4,6,12)'$ | (0) | 0 | 0 | | 1 |
| 2 | $\mathrm{I}_0(\nu,9,12)'$ | (0) | 0 | $3\nu-12$ | $\nu \geq 8$ | |
| 3 | $\mathrm{I}_\nu(4,6,12+\nu)'$ | (0) | 1 | $-\nu$ | $\nu \geq 1$ | 2 |
| 4 | $\mathrm{II}(4,5,4)$ | (1) | 4 | 8 | | 3 |
| 5 | $\mathrm{II}(5,5,4)$ | (1) | 4 | 11 | | |
| 6 | $\mathrm{II}(\nu,5,4)$ | (1) | 4 | $3\nu-4$ | $\nu \geq 6$ | |
| 7 | $\mathrm{II}(4,\nu,6)$ | (1) | 6 | 6 | $\nu \geq 7$ | |
| 8 | $\mathrm{II}(\nu,6,6)$ | – | 6 | $3\nu-6$ | $\nu \geq 5$ | |
| 9 | $\mathrm{II}(4,6,7)$ | – | 7 | 5 | | |
| 10 | $\mathrm{III}(4,5,4)$ | $(1)'\,\&(2)$ | 3 | 8 | | 4 |
| 11 | $\mathrm{III}(5,5,4)$ | $(1)'$ | 3 | 11 | | |
| 12 | $\mathrm{III}(4,\ \nu,6)$ | $(1)'$ | 5 | 6 | $\nu \geq 7$ | |
| 13 | $\mathrm{III}(5,7,8)$ | – | 7 | 7 | | |
| 14 | $\mathrm{III}(5,\ \nu,9)$ | – | 8 | 6 | $\nu \geq 8$ | |
| 15 | $\mathrm{IV}(4,5,4)$ | $(1)'\,\&(2)'$ | 2 | 8 | | 5 |
| 16 | $\mathrm{IV}(\nu,5,4)$ | $(1)'$ | 2 | $3\nu-4$ | $\nu \geq 6$ | |
| 17 | $\mathrm{I}_0^*(4,6,8)$ | (3) | 4 | 4 | | 6 |
| 18 | $\mathrm{I}_0^*(6,7,8)$ | (3) | 4 | 10 | | |
| 19 | $\mathrm{I}_0^*(\nu,7,8)$ | (3) | 4 | $3\nu-8$ | $\nu \geq 7$ | |
| 20 | $\mathrm{I}_0^*(4,6,9)$ | – | 5 | 3 | | |
| 21 | $\mathrm{I}_0^*(\nu,8,10)$ | – | 6 | $3\nu-10$ | $\nu \geq 6$ | |
| 22 | $\mathrm{I}_1^*(4,6,8)$ | $(3)'\,\&(4)$ | 3 | 4 | | 7 |
| 23 | $\mathrm{I}_1^*(6,7,8)$ | $(3)'$ | 3 | 10 | | |
| 24 | $\mathrm{I}_2^*(4,6,10)$ | (4) | 4 | 2 | | |
| 25 | $\mathrm{I}_2^*(6,\nu,12)$ | (5) | 6 | 6 | $\nu \geq 10$ | |
| 26 | $\mathrm{I}_2^*(6,9,13)$ | – | 7 | 5 | | |
| 27 | $\mathrm{I}_3^*(4,6,11)$ | (4) | 4 | 1 | | |
| 28 | $\mathrm{I}_3^*(6,\nu,12)$ | $(5)'$ | 5 | 6 | $\nu \geq 10$ | |
| 29 | $\mathrm{I}_{4+\nu}^*(4,6,12+\nu)$ | $(0)'$ | 4 | $-\nu$ | $\nu \geq 0$ | |
| 30 | $\mathrm{I}_{4+\nu}^*(6,9,14+\nu)$ | – | 6 | $4-\nu$ | $\nu \geq 0$ | |
| 31 | $\mathrm{IV}^*(4,6,8)$ | $(3)'\,\&(4)'$ | 2 | 4 | | 8 |
| 32 | $\mathrm{IV}^*(\nu,7,8)$ | $(3)'$ | 2 | $3\nu-8$ | $\nu \geq 7$ | |
| 33 | $\mathrm{III}^*(4,6,10)$ | $(4)'$ | 3 | 2 | | 9 |
| 34 | $\mathrm{III}^*(7,9,12)$ | – | 5 | 9 | | |
| 35 | $\mathrm{III}^*(7,10,14)$ | – | 7 | 7 | | |
| 36 | $\mathrm{III}^*(7,\nu,15)$ | – | 8 | 6 | $\nu \geq 11$ | |
| 37 | $\mathrm{II}^*(4,6,11)$ | $(4)'$ | 3 | 1 | | 10 |
| 38 | $\mathrm{II}^*(\nu,9,12)$ | $(0)'$ | 4 | $3\nu-12$ | $\nu \geq 8$ | |
| 39 | $\mathrm{II}^*(\nu,10,14)$ | – | 6 | $3\nu-14$ | $\nu \geq 8$ | |

**Table 2.2**
($p = 2,\ d = -1$)

| $v(N) = 0$ | $v(N) = 1$ | $v(N) = 2$ | $v(N) = 3$ | $v(N) = 4$ | $\nu$ | Add. cond. |
|---|---|---|---|---|---|---|
| $\mathrm{I}_0(4,6,12)'$ | | | | $\mathrm{I}_4^*(4,6,12)$ | | |
| | $\mathrm{I}_\nu^*(4,6,12+\nu)'$ | | | $\mathrm{I}_{4+\nu}^*(4,6,12+\nu)$ | $\nu \geq 1$ | |
| $\mathrm{I}_0(\nu,9,12)'$ | | | | $\mathrm{II}^*(\nu,9,12)$ | $\nu \geq 8$ | |
| | | | $\mathrm{III}(4,5,4)$ | $\mathrm{II}(4,5,4)a$ | | (2) |
| | | $\mathrm{IV}(4,5,4)$ | | $\mathrm{II}(4,5,4)b$ | | (2)$'$ |
| | | | $\mathrm{III}(5,5,4)$ | $\mathrm{II}(5,5,4)$ | | |
| | | $\mathrm{IV}(\nu,5,4)$ | | $\mathrm{II}(\nu,5,4)$ | $\nu \geq 6$ | |
| | | | $\mathrm{I}_1^*(4,6,8)$ | $\mathrm{I}_0^*(4,6,8)a$ | | (4) |
| | | $\mathrm{IV}^*(4,6,8)$ | | $\mathrm{I}_0^*(4,6,8)\,b$ | | (4)$'$ |
| | | | $\mathrm{I}_1^*(6,7,8)$ | $\mathrm{I}_0^*(6,7,8)$ | | |
| | | $\mathrm{IV}^*(\nu,7,8)$ | | $\mathrm{I}_0^*(\nu,7,8)$ | $\nu \geq 7$ | |
| | | | $\mathrm{III}^*(4,6,10)$ | $\mathrm{I}_2^*(4,6,10)$ | | |
| | | | $\mathrm{II}^*(4,6,11)$ | $\mathrm{I}_3^*(4,6,11)$ | | |

**Table 3.1**
($p = 2,\ d = 2$)

| No. | $E$ | Add. cond. | $f$ | $E' := E * 2$ | Add. cond. | $f'$ | $\nu$ | See |
|---|---|---|---|---|---|---|---|---|
| 1 | $\mathrm{I}_0(4,6,12)'$ | (0) | 0 | $\mathrm{I}_8^*(6,9,18)$ | – | 6 | | |
| 2 | $\mathrm{I}_0(\nu,9,12)'$ | (0) | 0 | $\mathrm{II}(\nu-2,6,6)$ | – | 6 | $\nu \geq 8$ | |
| 3 | $\mathrm{I}_\nu(4,6,12+\nu)'$ | (0) | 1 | $\mathrm{I}_{\nu+8}^*(6,9,\nu+18)$ | – | 6 | $\nu \geq 1$ | |
| 4 | $\mathrm{II}(\nu,5,4)$ | (1) | 4 | $\mathrm{I}_0^*(\nu+2,8,10)$ | – | 6 | $\nu \geq 4$ | |
| 5 | $\mathrm{II}(4,\nu,6)$ | (1) | 6 | $\mathrm{I}_3^*(6,\nu+3,12)$ | (5)$'$ | 5 | $\nu \geq 7$ | Lem. 3.1 |
| 6 | $\mathrm{II}(5,6,6)$ | – | 6 | $\mathrm{III}^*(7,9,12)$ | – | 5 | | |
| 7 | $\mathrm{II}(\nu,6,6)$ | – | 6 | $\mathrm{I}_0$ or $\mathrm{II}^*$ | | | $\nu \geq 6$ | Lem. 3.2 |
| 8 | $\mathrm{II}(4,6,7)$ | – | 7 | $\mathrm{I}_2^*(6,9,13)$ | – | 7 | | |
| 9 | $\mathrm{III}(4,5,4)$ | (1)$'$ &(2) | 3 | $\mathrm{I}_0^*(6,8,10)$ | – | 6 | | |
| 10 | $\mathrm{III}(5,5,4)$ | (1)$'$ | 3 | $\mathrm{I}_0^*(7,8,10)$ | – | 6 | | |
| 11 | $\mathrm{III}(4,\nu,6)$ | (1)$'$ | 5 | $\mathrm{I}_2^*(6,\nu+3,12)$ | (5) | 6 | $\nu \geq 7$ | Lem. 3.1 |
| 12 | $\mathrm{III}(5,7,8)$ | – | 7 | $\mathrm{III}^*(7,10,14)$ | – | 7 | | |
| 13 | $\mathrm{III}(5,\nu,8)$ | – | 8 | $\mathrm{III}^*(7,\nu+3,15)$ | – | 8 | $\nu \geq 8$ | |
| 14 | $\mathrm{IV}(4,5,4)$ | (1)$'$ &(2)$'$ | 2 | $\mathrm{I}_0^*(6,8,10)$ | – | 6 | | |
| 15 | $\mathrm{IV}(\nu,5,4)$ | (1)$'$ | 2 | $\mathrm{I}_0^*(\nu+2,8,10)$ | – | 6 | $\nu \geq 6$ | |
| 16 | $\mathrm{I}_0^*(4,6,8)$ | (3) | 4 | $\mathrm{I}_4^*(6,9,14)$ | – | 6 | | |
| 17 | $\mathrm{I}_0^*(\nu,7,8)$ | (3) | 4 | $\mathrm{II}^*(\nu+2,10,14)$ | – | 6 | $\nu \geq 6$ | |
| 18 | $\mathrm{I}_0^*(4,6,9)$ | – | 5 | $\mathrm{I}_5^*(6,9,15)$ | – | 6 | | |
| 19 | $\mathrm{I}_0^*(6,8,10)$ | – | 6 | II, III or IV | | | | Lem. 3.4 |
| 20 | $\mathrm{I}_0^*(7,8,10)$ | – | 6 | II or III | | | | Lem. 3.5 |
| 21 | $\mathrm{I}_0^*(\nu,8,10)$ | – | 6 | II or IV | | | $\nu \geq 8$ | Lem. 3.6 |
| 22 | $\mathrm{I}_1^*(4,6,8)$ | (3)$'$&(4) | 3 | $\mathrm{I}_4^*(6,9,14)$ | – | 6 | | |
| 23 | $\mathrm{I}_1^*(6,7,8)$ | (3)$'$ | 3 | $\mathrm{II}^*(8,10,14)$ | – | 6 | | |
| 24 | $\mathrm{I}_2^*(4,6,10)$ | (4) | 4 | $\mathrm{I}_6^*(6,9,16)$ | – | 6 | | |
| 25 | $\mathrm{I}_2^*(6,\nu,12)$ | (5) | 6 | $\mathrm{I}_6^*(4,\nu-3,6)$ | (1)$'$ | 5 | $\nu \geq 10$ | Lem. 3.1 |
| 26 | $\mathrm{I}_2^*(6,9,13)$ | – | 7 | $\mathrm{II}(4,6,7)$ | – | 7 | | |
| 27 | $\mathrm{I}_3^*(4,6,11)$ | (4) | 4 | $\mathrm{I}_7^*(6,9,17)$ | – | 6 | | |
| 28 | $\mathrm{I}_3^*(6,\nu,12)$ | (5)$'$ | 5 | $\mathrm{II}(4,\nu-3,6)$ | (1) | 6 | $\nu \geq 10$ | Lem. 3.1 |
| 29 | $\mathrm{I}_4^*(6,9,14)$ | – | 6 | $\mathrm{I}_0^*$, $\mathrm{I}_1^*$ or $\mathrm{IV}^*$ | | | | Lem. 3.8 |

**Table 3.1**
(continued)

| No. | $E$ | Add. cond. | $f$ | $E' := E * 2$ | Add. cond. | $f'$ | $\nu$ | See |
|---|---|---|---|---|---|---|---|---|
| 30 | $\mathrm{I}_{4+\nu}^*(4,6,12+\nu)$ | $(0)'$ | 4 | $\mathrm{I}_{8+\nu}^*(6,9,18+\nu)$ | – | 6 | $\nu \geq 0$ | |
| 31 | $\mathrm{I}_5^*(6,9,15)$ | – | 6 | $\mathrm{I}_0^*(4,6,9)$ | – | 5 | | |
| 32 | $\mathrm{I}_6^*(6,9,16)$ | – | 6 | $\mathrm{I}_2^*$ or $\mathrm{III}^*$ | | | | Lem. 3.11 |
| 33 | $\mathrm{I}_7^*(6,9,17)$ | – | 6 | $\mathrm{I}_3^*$ or $\mathrm{II}^*$ | | | | Lem. 3.12 |
| 34 | $\mathrm{I}_{4+\nu}^*(6,9,14+\nu)$ | – | 6 | $\mathrm{I}_{\nu-4}$ or $\mathrm{I}_\nu^*$ | | | $\nu \geq 4$ | Lem. 3.13 |
| 35 | $\mathrm{IV}^*(4,6,8)$ | $(3)'\&(4)'$ | 2 | $\mathrm{I}_4^*(6,9,14)$ | – | 6 | | |
| 36 | $\mathrm{IV}^*(\nu,7,8)$ | $(3)'$ | 2 | $\mathrm{II}^*(\nu+2,10,14)$ | – | 6 | $\nu \geq 7$ | |
| 37 | $\mathrm{III}^*(4,6,10)$ | $(4)'$ | 3 | $\mathrm{I}_6^*(6,9,16)$ | – | 6 | | |
| 38 | $\mathrm{III}^*(7,9,12)$ | – | 5 | $\mathrm{II}(5,6,6)$ | – | 6 | | |
| 39 | $\mathrm{III}^*(7,10,14)$ | – | 7 | $\mathrm{III}(5,7,8)$ | – | 7 | | |
| 40 | $\mathrm{III}^*(7,\nu,15)$ | – | 8 | $\mathrm{III}(5,\nu-3,9)$ | – | 8 | $\nu \geq 11$ | |
| 41 | $\mathrm{II}^*(4,6,11)$ | $(4)'$ | 3 | $\mathrm{I}_7^*(6,9,17)$ | – | 6 | | |
| 42 | $\mathrm{II}^*(\nu,9,12)$ | $(0)'$ | 4 | $\mathrm{II}(\nu-2,6,6)$ | – | 6 | $\nu \geq 8$ | |
| 43 | $\mathrm{II}^*(8,10,14)$ | – | 6 | $\mathrm{I}_0^*$ or $\mathrm{I}_1^*$ | | | | Lem. 3.14 |
| 44 | $\mathrm{II}^*(\nu,10,14)$ | – | 6 | $\mathrm{I}_0^*$ or $\mathrm{IV}^*$ | | | $\nu \geq 9$ | Lem. 3.15 |

**Table 4.1**
($p = 3,\ d = -3$)

| No. | $E$ | Add. cond. | $f_3$ | $E' := E * (-3)$ | Add. cond. | $f_3'$ | $\nu$ |
|---|---|---|---|---|---|---|---|
| 1 | $\mathrm{I}_0(0,0,0)$ | | 0 | $\mathrm{I}_0^*(2,3,6)$ | | 2 | |
| 2 | $\mathrm{I}_0(1,\nu,0)$ | | 0 | $\mathrm{I}_0^*(3,3+\nu,6)$ | | 2 | $\nu \geq 3$ |
| 3 | $\mathrm{I}_\nu(0,0,\nu)$ | | 1 | $\mathrm{I}_\nu^*(2,3,6+\nu)$ | | 2 | $\nu \geq 1$ |
| 4 | $\mathrm{II}(\nu,3,3)$ | $\mathrm{P}_2'$ | 3 | $\mathrm{IV}^*(\nu+2,6,9)$ | $\mathrm{P}_5'$ | 3 | $\nu \geq 2$ |
| 5 | $\mathrm{II}(2,4,3)$ | | 3 | $\mathrm{IV}^*(4,7,9)$ | | 3 | |
| 6 | $\mathrm{II}(2,3,4)$ | | 4 | $\mathrm{IV}^*(4,6,10)$ | | 4 | |
| 7 | $\mathrm{II}(\nu,4,5)$ | | 5 | $\mathrm{IV}^*(\nu+2,7,11)$ | | 5 | $\nu \geq 3$ |
| 8 | $\mathrm{III}(\nu,3,3)$ | $\mathrm{P}_2$ | 2 | $\mathrm{III}^*(\nu+2,6,9)$ | $\mathrm{P}_5$ | 2 | $\nu \geq 2$ |
| 9 | $\mathrm{III}(2,\nu,3)$ | | 2 | $\mathrm{III}^*(4,\nu+3,9)$ | | 2 | $\nu \geq 5$ |
| 10 | $\mathrm{IV}(2,3,5)$ | | 3 | $\mathrm{II}^*(4,6,11)$ | | 3 | |
| 11 | $\mathrm{IV}(3,5,6)$ | | 4 | $\mathrm{II}^*(5,8,12)$ | | 4 | |
| 12 | $\mathrm{IV}(\nu,5,7)$ | | 5 | $\mathrm{II}^*(\nu+2,8,13)$ | | 5 | $\nu \geq 4$ |

**Table 5.1**
($p > 3,\ d = p$)

| No. | $E$ | $f_p$ | $E' := E * p$ | $f_p'$ | $\nu$ |
|---|---|---|---|---|---|
| 1 | $\mathrm{I}_0(0,\nu,0)$ | 0 | $\mathrm{I}_0^*(2,\nu+3,6)$ | 2 | $\nu \geq 0$ |
| 2 | $\mathrm{I}_0(\nu,0,0)$ | 0 | $\mathrm{I}_0^*(\nu+2,3,6)$ | 2 | $\nu \geq 1$ |
| 3 | $\mathrm{I}_\nu(0,0,\nu)$ | 1 | $\mathrm{I}_\nu^*(2,3,6+\nu)$ | 2 | $\nu \geq 1$ |
| 4 | $\mathrm{II}(\nu,1,2)$ | 2 | $\mathrm{IV}^*(\nu+2,4,8)$ | 2 | $\nu \geq 1$ |
| 5 | $\mathrm{III}(1,\nu,3)$ | 2 | $\mathrm{III}^*(3,3+\nu,9)$ | 2 | $\nu \geq 2$ |
| 6 | $\mathrm{IV}(\nu,2,4)$ | 2 | $\mathrm{II}^*(\nu+2,5,10)$ | 2 | $\nu \geq 2$ |

**Table 7.1**

| Interval | # of conductors | # of prime conductors | # of primes | $\frac{\#\text{ prime cond.}}{\#\text{ all primes}}$ | $\frac{\#\text{ prime cond.}}{\#\text{ all cond.}}$ |
|---|---|---|---|---|---|
| 0–1000 | 707 | 52 | 168 | 0.309 | 0.0735 |
| 1001–2000 | 689 | 32 | 135 | 0.237 | 0.0464 |
| 2001–3000 | 689 | 28 | 127 | 0.220 | 0.0406 |
| 3001–4000 | 690 | 29 | 120 | 0.241 | 0.0420 |
| 4001–5000 | 662 | 20 | 119 | 0.168 | 0.0302 |
| 125001–126000 | 608 | 9 | 84 | 0.107 | 0.0148 |
| 126001–127000 | 593 | 10 | 83 | 0.120 | 0.0168 |
| 127001–128000 | 614 | 9 | 86 | 0.104 | 0.0146 |
| 128001–129000 | 608 | 8 | 89 | 0.089 | 0.0131 |
| 129001–130000 | 620 | 14 | 83 | 0.168 | 0.0225 |

**Table 7.2**

| $m$ | $\mathcal{E}(m)$ | $\mathcal{E}(2m)$ | $\mathcal{E}(2^2m)$ | $\mathcal{E}(2^3m)$ | $\mathcal{E}(2^5m)$ | $\mathcal{E}(2^7m)$ | $\mathcal{E}(2^8m)$ |
|---|---|---|---|---|---|---|---|
| 1 | $\emptyset$ | $\emptyset$ | $\emptyset$ | $\emptyset$ | $4^{1}$ | $2^{4}$ | $2^{4}$ |
| **3** | $\emptyset$ | $\emptyset$ | $\emptyset$ | $6^{1}$ | $4^{2}$ | $2^{8}$ | $2^{4}4^{4}$ |
| **5** | $\emptyset$ | $\emptyset$ | $4^{1}$ | $4^{1}$ | $2^{2}$ | $2^{8}$ | $\emptyset$ |
| **7** | $\emptyset$ | $6^{1}$ | $\emptyset$ | $2^{1}4^{1}$ | $2^{2}$ | $2^{4}$ | $2^{8}$ |
| 9 | $\emptyset$ | $\emptyset$ | $4^{1}$ | $6^{1}$ | $2^{2}4^{3}$ | $2^{20}$ | $2^{12}4^{4}$ |
| **11** | $3^{1}$ | $\emptyset$ | $2^{1}$ | $1^{1}$ | $1^{6}$ | $2^{4}$ | $\emptyset$ |
| **13** | $\emptyset$ | $2^{1}3^{1}$ | $2^{1}$ | $1^{1}$ | $1^{2}$ | $1^{12}2^{8}$ | $1^{8}2^{4}$ |
| 15 | $8^{1}$ | $8^{1}$ | $\emptyset$ | $4^{1}6^{1}$ | $4^{8}$ | $2^{24}$ | $2^{28}$ |
| **17** | $4^{1}$ | $4^{1}$ | $\emptyset$ | $2^{2}$ | $2^{6}$ | $\emptyset$ | $2^{8}$ |
| **19** | $3^{1}$ | $2^{1}3^{1}$ | $1^{1}$ | $1^{2}$ | $1^{6}$ | $1^{8}$ | $1^{12}2^{4}$ |
| 21 | $6^{1}$ | $6^{1}$ | $2^{1}4^{1}$ | $4^{2}$ | $2^{4}4^{4}$ | $2^{24}$ | $2^{12}$ |
| **23** | $\emptyset$ | $2^{1}$ | $1^{1}2^{1}$ | $1^{3}2^{1}$ | $\emptyset$ | $2^{4}$ | $2^{4}$ |
| 25 | $\emptyset$ | $4^{2}$ | $4^{1}$ | $1^{2}2^{2}4^{1}$ | $1^{4}2^{2}4^{1}$ | $1^{16}2^{12}$ | $1^{8}2^{16}$ |
| 27 | $4^{1}$ | $3^{2}$ | $2^{1}$ | $1^{4}$ | $1^{12}$ | $1^{16}$ | $1^{24}$ |
| **29** | $\emptyset$ | $1^{1}2^{1}$ | $1^{1}2^{2}$ | $1^{2}$ | $1^{2}$ | $1^{12}2^{4}$ | $\emptyset$ |
| **31** | $\emptyset$ | $4^{1}$ | $1^{1}2^{1}$ | $1^{2}2^{1}$ | $\emptyset$ | $\emptyset$ | $2^{4}$ |
| 33 | $4^{1}$ | $4^{3}$ | $2^{2}$ | $2^{2}4^{2}$ | $2^{6}4^{4}$ | $2^{20}$ | $2^{24}$ |
| 35 | $3^{1}$ | $4^{1}$ | $1^{1}2^{1}$ | $1^{2}$ | $1^{12}4^{4}$ | $2^{12}$ | $2^{20}$ |
| **37** | $1^{1}3^{1}$ | $\emptyset$ | $1^{1}$ | $1^{2}$ | $1^{6}2^{2}$ | $\emptyset$ | $\emptyset$ |
| 39 | $4^{1}$ | $4^{1}$ | $2^{1}4^{1}$ | $2^{4}4^{2}$ | $2^{8}4^{2}$ | $2^{8}$ | $\emptyset$ |
| **41** | $\emptyset$ | $2^{1}$ | $\emptyset$ | $2^{2}$ | $2^{2}$ | $2^{4}$ | $2^{4}$ |
| **43** | $1^{1}$ | $\emptyset$ | $2^{1}$ | $1^{1}$ | $\emptyset$ | $\emptyset$ | $\emptyset$ |
| 45 | $8^{1}$ | $4^{2}8^{1}$ | $4^{1}$ | $2^{2}4^{2}6^{1}$ | $2^{6}4^{8}$ | $2^{48}$ | $2^{44}$ |
| **47** | $\emptyset$ | $2^{1}$ | $\emptyset$ | $\emptyset$ | $\emptyset$ | $2^{4}$ | $\emptyset$ |
| 49 | $4^{1}$ | $6^{1}$ | $2^{2}$ | $1^{4}2^{1}4^{1}$ | $2^{8}4^{1}$ | $2^{8}$ | $2^{16}$ |
| 51 | $2^{1}$ | $2^{1}4^{1}6^{1}$ | $1^{2}$ | $1^{2}2^{1}4^{1}$ | $1^{8}2^{2}4^{2}$ | $2^{16}$ | $2^{16}$ |

**Table 7.3**

| $m$ | $\mathcal{E}(m)$ | $\mathcal{E}(2m)$ | $\mathcal{E}(2^2m)$ | $\mathcal{E}(2^3m)$ | $\mathcal{E}(2^5m)$ | $\mathcal{E}(2^7m)$ | $\mathcal{E}(2^8m)$ |
|---|---|---|---|---|---|---|---|
| 451 | $1^1$ | $1^1 2^1$ | $1^1 2^2$ | $1^4$ | $1^6$ | $2^7$ | $2^8$ |
| 453 | Ø | $1^6 2^1 3^1$ | $1^1 2^1$ | $1^2$ | $1^6$ | $1^{32} 2^4$ | $1^8 2^4$ |
| 455 | $4^2$ | $1^2 2^5 3^1 4^2 6^1$ | Ø | $1^2 2^7 4^1$ | $1^4 2^{14} 4^2$ | $1^{12} 2^{28}$ | $1^{20} 2^{36}$ |
| **457** | Ø | $1^1 2^1$ | Ø | $1^1 2^1$ | Ø | $1^4$ | $1^4$ |
| 459 | $1^6 2^2$ | $1^6 2^6$ | $1^2$ | $1^{16}$ | $1^{48}$ | Ø | $1^{32}$ |
| **461** | Ø | $1^1$ | $1^1$ | Ø | $1^2$ | Ø | $1^4$ |
| **463** | Ø | $2^1$ | Ø | Ø | Ø | Ø | Ø |
| 465 | $2^1 4^1$ | $1^4 2^7 4^3 6^1$ | $2^3$ | $1^2 2^3 4^3$ | $1^6 2^8 4^6$ | $1^{20} 2^{56}$ | $1^{20} 2^{40}$ |
| **467** | $1^1$ | $1^2 2^1$ | Ø | $1^1$ | $1^4$ | $1^4$ | $1^8 2^4$ |
| 469 | $1^2$ | $1^2 2^1 3^1$ | $1^1 2^1$ | $1^{11} 2^2$ | $1^{12} 2^2$ | $2^4$ | $2^4$ |
| 471 | $1^1$ | $1^4$ | $2^2$ | $1^3 2^2$ | $1^4 2^2$ | $1^{20}$ | $1^4$ |
| 473 | $1^1$ | $1^1 2^1 4^1$ | $1^3 2^2$ | $1^5 2^1 4^1$ | $1^4$ | $1^{12}$ | $2^8$ |
| 475 | $2^2 3^1$ | $1^2 2^2 3^1$ | $1^1 2^2$ | $1^3 2^5 4^1$ | $1^8 2^6$ | $1^{16} 2^4$ | $1^{32} 2^{12}$ |
| 477 | $1^1$ | $1^8 2^5$ | $1^1 2^1$ | $1^2$ | $1^{14} 4^2$ | $1^{56} 2^{12}$ | $1^{28} 2^{12}$ |
| **479** | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| 481 | $2^1$ | $2^1$ | $1^1$ | $1^2$ | $1^6$ | $2^8$ | $2^4$ |
| 483 | $1^2$ | $1^3 2^5 4^2 6^1$ | $1^1 2^1$ | $1^3 2^2 4^1$ | $1^{10} 2^4 4^8$ | $1^{16} 2^{26}$ | $1^{28} 2^{32}$ |
| 485 | $1^1 3^1$ | $1^2$ | $1^1$ | $1^2$ | $1^{12} 2^2$ | $2^4$ | $1^8 2^8$ |
| **487** | Ø | $1^7 2^1$ | Ø | Ø | $1^{10}$ | $1^4$ | $1^{24}$ |
| 489 | Ø | $1^6 2^2$ | $1^1 2^1$ | $1^3$ | $1^8 2^2 4^2$ | $1^{20} 2^8$ | $1^{24} 2^4$ |
| **491** | Ø | $1^1$ | $1^1$ | $1^2$ | Ø | Ø | Ø |
| 493 | $1^2$ | $1^4 2^2$ | Ø | $1^2$ | $1^2$ | $1^{16}$ | Ø |
| 495 | $4^1$ | $2^5 4^5 6^2$ | $2^3 4^3$ | $1^1 2^{11} 4^6 6^2$ | $1^6 2^{16} 4^{12}$ | $1^{16} 2^{80}$ | $1^{24} 2^{60}$ |
| 497 | $1^1$ | $1^1 2^4 4^2$ | $1^1$ | $2^1$ | $1^4 2^4$ | $1^{12} 2^8$ | $2^4$ |
| **499** | Ø | Ø | $1^1$ | $1^2$ | $1^2$ | Ø | Ø |
| 501 | $2^1$ | $1^3 2^2$ | Ø | $1^2 2^2$ | $1^2 2^2$ | $2^4$ | $1^8 2^4$ |

**Table 7.4**

| $m$ | $\mathcal{E}(m)$ | $\mathcal{E}(3m)$ | $\mathcal{E}(3^2m)$ | $\mathcal{E}(3^3m)$ | $\mathcal{E}(3^4m)$ | $\mathcal{E}(3^5m)$ |
|---|---|---|---|---|---|---|
| 1 | Ø | Ø | Ø | $4^1$ | Ø | $2^2$ |
| **2** | Ø | Ø | Ø | $3^2$ | $2^2 4^2$ | $2^6$ |
| 4 | Ø | Ø | $4^1$ | $2^1$ | $2^4$ | $2^4$ |
| **5** | Ø | $8^1$ | $8^1$ | $1^2$ | $1^2 2^4$ | $1^8 2^2$ |
| **7** | Ø | $6^1$ | $6^1$ | $1^2 3^2$ | $1^2$ | $1^{10}$ |
| 8 | Ø | $6^1$ | $6^1$ | $1^4$ | $1^4$ | $1^{10}$ |
| 10 | Ø | $8^1$ | $4^2 8^1$ | $2^4$ | $2^8$ | $2^{16}$ |
| **11** | $3^1$ | $4^1$ | $2^2 3^1 4^1$ | $1^4$ | $1^4 2^4$ | Ø |
| **13** | Ø | $4^1$ | $4^1$ | Ø | $1^4$ | $1^6$ |
| 14 | $6^1$ | $6^1$ | $6^2$ | $1^4 3^4$ | $1^4 2^4$ | $1^{10} 2^{10}$ |
| 16 | Ø | $6^1$ | $4^1 6^1$ | $1^4 2^1 3^2 4^1$ | $1^4 2^6 4^2$ | $1^{10} 2^{12}$ |
| **17** | $4^1$ | $2^1$ | $1^2 2^1 4^1$ | $1^6 2^2$ | Ø | Ø |
| **19** | $3^1$ | $1^1 2^1 4^1$ | $1^1 2^1 3^1 4^1$ | $1^2$ | $1^6$ | $1^8$ |
| 20 | $4^1$ | Ø | $4^1$ | $2^6$ | $2^6$ | $2^2$ |
| 22 | Ø | $4^3$ | $4^5$ | $1^6 2^2$ | $1^6 2^6$ | $1^{12} 2^6$ |
| **23** | Ø | $2^1$ | $2^1$ | $1^2$ | Ø | $1^4 2^2$ |
| 25 | Ø | $2^2 8^1$ | $2^4 8^1$ | $1^6 2^2 4^1$ | $1^2 2^4$ | $1^{30} 2^{12}$ |
| 26 | $2^1 3^1$ | $4^1$ | $2^3 3^1 4^1$ | $1^{10} 2^2 3^4$ | $1^4 2^2$ | $1^6 2^6$ |
| 28 | Ø | $2^1 4^1$ | $2^1 4^1$ | $1^2 2^4$ | $1^2 2^2$ | $1^4 2^4$ |
| **29** | Ø | Ø | Ø | Ø | Ø | Ø |
| **31** | Ø | Ø | Ø | Ø | Ø | Ø |
| 32 | $4^1$ | $4^2$ | $2^2 4^3$ | $1^{12}$ | $1^8$ | $1^{16}$ |
| 34 | $4^1$ | $2^1 4^1 6^1$ | $2^1 4^2 6^1$ | $1^6 2^6$ | $1^6$ | $1^{10} 2^4$ |
| 35 | $3^1$ | $4^1$ | $3^1 4^1$ | Ø | $1^4 2^4$ | $1^6 2^4$ |
| **37** | $1^1 3^1$ | Ø | $1^1 2^2 3^1$ | $1^2$ | Ø | Ø |
| 38 | $2^1 3^1$ | $2^1 4^2$ | $2^4 3^1 4^2$ | $1^8 2^6 3^2$ | $1^6$ | $1^4 2^2$ |