MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 174
APRIL 1986, PAGES 637-658

Explicit Determination of Nontrivial Torsion Structures of Elliptic Curves Over Quadratic Number Fields

By Markus A. Reichert

Abstract. We determine equations of the modular curves $X_1(N)$ for $N = 11, 13, 14, 15, 16, 17$ and 18. Except for $N = 17$, these are the only existing elliptic or hyperelliptic $X_1(N)$. Applying these $X_1(N)$, we calculate tables of elliptic curves E over quadratic fields K with torsion groups of one of the following isomorphism types:

$$E_{\text{tor}}(K) \cong \mathbf{Z}/m\mathbf{Z}, \qquad m = 11, 13, 14, 15, 16 \text{ and } 18.$$

1. Introduction. Let E denote an elliptic curve defined over an algebraic number field K of finite degree over the rationals $\mathbf{Q}$. We shall assume that the curve E is given in *Weierstrass normal form*:

$$(1)\quad E\colon Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6; \qquad a_1, a_2, a_3, a_4, a_6 \in K.$$

Designate by $E(K)$ the group of rational points of E over K. Mordell and Weil proved that $E(K)$ is finitely generated. Hence, $E(K)$ may be written as a direct sum,

$$E(K) = E_{\text{tor}}(K) \oplus E_{\text{fr}}(K),$$

of the torsion group $E_{\text{tor}}(K)$ and a free group $E_{\text{fr}}(K)$. The number of free generators of $E_{\text{fr}}(K)$ is called the *rank* of E over K. Of course, $E_{\text{tor}}(K)$ is finite, and it is conjectured that the order of $E_{\text{tor}}(K)$ is bounded by a constant $N(K)$ depending only on K.

Boundedness Conjecture:

$$|E_{\text{tor}}(K)| \leqslant N(K).$$

In 1969 Manin [7] proved this conjecture for the p-component of $E_{\text{tor}}(K)$, p being a prime. In 1979 Kenku [2] explicitly determined this Manin-bound for the case $p = 2$ and K a quadratic field over $\mathbf{Q}$. He proved that the maximal 2-power order of a K-rational torsion point of an elliptic curve over K is 16. This bound is sharp. We have computed elliptic curves over quadratic fields K over $\mathbf{Q}$ with K-rational points of order 16.

In 1977 Mazur [8] proved the boundedness conjecture in the case $K = \mathbf{Q}$. He determined that $N(\mathbf{Q})$ equals 16, and more precisely he obtained

$$E_{\text{tor}}(\mathbf{Q}) \cong \begin{cases} \mathbf{Z}/m\mathbf{Z}; & m = 1, 2, \ldots, 10 \text{ or } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}; & m = 1, 2, 3, 4. \end{cases}$$

Received January 5, 1984.
1980 *Mathematics Subject Classification*. Primary 14K07, 10B10, 10D12; Secondary 14K15, 14G25.

2. Determination of Nontrivial Torsion Structures. When speaking of nontrivial torsion structures, we think of structures which do not exist over $\mathbf{Q}$. We have calculated tables of elliptic curves E over quadratic fields K whose torsion group is isomorphic to one of the following groups:

$$E_{\mathrm{tor}}(K) \cong \mathbf{Z}/m\mathbf{Z}, \qquad m = 11, 13, 14, 15, 16 \text{ and } 18.$$

These tables were computed by a modification of a method of Kubert [4] which in turn is extending the method of Billing and Mahler [1] leading to the modular curves $X_1(N)$. Our first result is

THEOREM 1. *For $N = 11, 13, 14, 15, 16, 17$ and 18 the modular curves $X_1(N)$ are given by the following equations*:

(i) $X_1(11)$: $V^2 + V = U^3 - U^2$,

(ii) $X_1(13)$: $V^2 + (U^3 - U^2 - 1)V - U^2 + U = 0$,

(iii) $X_1(14)$: $V^2 + UV + V = U^3 - U$,

(iv) $X_1(15)$: $V^2 + UV + V = U^3 + U^2$,

(v) $X_1(16)$: $(U^2 + 3U + 2)V^2 + (U^3 + 4U^2 + 4U)V - U = 0$,

(vi) $X_1(17)$: $V^4 + (U + 2)V^3 + (U^3 + 1)V^2 + (-U^5 - 2U^4 - U^3 - U^2 - U)V - U^5 - 2U^4 - U^3 = 0$,

(vii) $X_1(18)$: $(U^2 - 2U + 1)V^2 + (-U^3 + U - 1)V + U^3 - U^2 = 0$.

Except for $N = 17$, these are the only existing elliptic or hyperelliptic $X_1(N)$ [9]. In the literature, these $X_1(N)$ are partially known, but nobody as yet seems to have used them for calculating examples of nontrivial torsion structures.

Proof. To prove Theorem 1, we start from a special form of the elliptic curve E over K:

$$E(b,c)\colon Y^2 + (1 - c)XY - bY = X^3 - bX^2; \qquad b, c \in K.$$

This is called the *$E(b,c)$-form*. We obtain it from the Weierstrass normal from (1) of E by imposing on E the following three conditions:

(i) $P = (0,0) \in E_{\mathrm{tor}}(K)$,

(ii) the straight line $X = 0$ is a tangent to E at P,

(iii) $\mathrm{ord}(P) \neq 2, 3$.

(i) implies that $a_6 = 0$, and from (ii) and (iii) one deduces that a_2, $a_3 \neq 0$, and $a_4 = 0$. Now the equation for E assumes the form

$$E\colon Y^2 + a_1XY + a_3Y = X^3 + a_2X^2; \qquad a_2,\ a_3 \neq 0.$$

Applying the birational transformation

$$X = \left(\frac{a_3}{a_2}\right)^2 X', \qquad Y = \left(\frac{a_3}{a_2}\right)^3 Y',$$

we get the equation

$$E\colon Y'^2 + \frac{a_1a_2}{a_3}X'Y' + \frac{a_2^3}{a_3^2}Y' = X'^3 + \frac{a_2^3}{a_3^2}X'^2.$$

On substituting

$$(2) \qquad 1 - c = \frac{a_1a_2}{a_3} \quad \text{and} \quad -b = \frac{a_2^3}{a_3^2} \neq 0,$$

we obtain the $E(b,c)$-form of the elliptic curve. We shall carry out in detail the necessary calculations relating to $X_1(N)$ in the most simple case $N = 11$ and outline the remaining cases of $N = 13$, 14, 15, 16, 17 and 18, which are treated in a similar manner. (See [11] for more details.)

The Case of $X_1(11)$. To calculate $X_1(11)$, we assume that $\mathrm{ord}(P) = 11$. Then $5P = -6P$, and

$$x_{5P} = x_{-6P} = x_{6P}. \tag{3}$$

In Eq. (3), x_{nP} means the x-coordinate of the n-multiple nP of P. Now we calculate the multiples of P on $E(b,c)$. They are:

$$\begin{aligned}
\underline{P} &= (0,0), && \\
\underline{2P} &= (b, bc), && \\
\underline{3P} &= (c, b-c), && \\
\underline{4P} &= \big(r(r-1), r^2(c+r-1)\big); && b = cr, \\
\underline{5P} &= \big(rs(s-1), rs^2(r-s)\big); && c = s(r-1), \\
\underline{6P} &= \big(-mt, m^2(m+2t-1)\big); && m(1-s) = s(1-r) \text{ and} \\
& && r - s = t(1-s).
\end{aligned}$$

Equation (3) implies that

$$rs(s-1) = -mt. \tag{4}$$

Without loss of generality, the cases $s = 1$ and $s = 0$ may be excluded. Reversing the substitutions made when calculating $6P$, we obtain from Eq. (4):

$$X_1(11)\colon r^2 - 4sr + 3s^2r - s^3r + s = 0. \tag{5}$$

This is one of the equations for $X_1(11)$, called the "raw form" of $X_1(11)$. This equation has to be transformed birationally into the equation of the $X_1(11)$ given in Theorem 1. The goal of this transformation is to get an equation of $X_1(11)$ with as few singularities as possible. This transformation is done in three steps. When computing the other $X_1(N)$ we can take roughly the same steps to get the desired transformations.

1. *Step*: *Translation*. We translate the point $Q = (1,1)$ on $X_1(11)$ according to Eq. (5) to obtain $Q' = (0,0)$ by the birational transformation:

$$s = U_1 + 1, \qquad r = V_1 + 1.$$

Equation (5) implies

$$V_1^2 - U_1V_1 - U_1^3V_1 - U_1^3 = 0. \tag{5.1}$$

2. *Step*: *Quadratic transformation*. By this transformation we remove the singularity at $(0,0)$. We put

$$U_1 = \frac{1}{U_2}, \qquad V_1 = \frac{1}{V_2},$$

to obtain from Eq. (5.1)

$$V_2^2 + U_2^2V_2 + V_2 - U_2^3 = 0. \tag{5.2}$$

3. *Step*: *Separation of variables*. We set

$$U_2 = \frac{U}{V}, \qquad V_2 = \frac{1}{V}.$$

From Eq. (5.2), one derives

$$X_1(11)\colon V^2 + V = U^3 - U^2. \tag{6}$$

Up until now, we made the calculations by hand. The subsequent calculations were performed by means of the computer algebra system SAC-2, which we implemented on a "Siemens 7.561" at the "Rechenzentrum der Universität des Saarlandes". First of all, we give a list of the multiples nP for $n = 7, \dots, 10$. We shall write $nP = (Nx/Dx, Ny/Dy)$ and exhibit Nx, Dx, Ny and Dy.

$\underline{7P}$:

$$\begin{aligned}
Nx &= 2mt^3 + (5m^2 - 3m)t^2 + (4m^3 - 5m^2 + m)t + m^4 - 2m^3 + m^2,\\
Dx &= -t^3 + t^2,\\
Ny &= -mt^6 + (-4m^2 + 4m)t^5 + (-6m^3 + 15m^2 - 6m)t^4\\
&\quad + (-4m^4 + 22m^3 - 20m^2 + 4m)t^3\\
&\quad + (-m^5 + 16m^4 - 25m^3 + 11m^2 - m)t^2\\
&\quad + (6m^5 - 14m^4 + 10m^3 - 2m^2)t\\
&\quad + m^6 - 3m^5 + 3m^4 - m^3,\\
Dy &= t^5 - 2t^4 + t^3.
\end{aligned}$$

$\underline{8P}$:

$$\begin{aligned}
Nx &= -t^5 + (-2m + 3)t^4 + (-m^2 + 6m - 3)t^3 + (4m^2 - 5m + 1)t^2\\
&\quad + (m^3 - 2m^2 + m)t,\\
Dx &= -4t^3 + (-4m + 8)t^2 + (-m^2 + 6m - 5)t + m^2 - 2m + 1,\\
Ny &= -t^7 + (-6m + 3)t^6 + (-13m^2 + 14m - 3)t^5\\
&\quad + (-13m^3 + 22m^2 - 10m + 1)t^4\\
&\quad + (-6m^4 + 14m^3 - 10m^2 + 2m)t^3 + (-m^5 + 3m^4 - 3m^3 + m^2)t^2,\\
Dy &= 8t^4 + (12m - 20)t^3 + (6m^2 - 24m + 18)t^2\\
&\quad + (m^3 - 9m^2 + 15m - 7)t - m^3 + 3m^2 - 3m + 1.
\end{aligned}$$

$\underline{9P}$:

$$\begin{aligned}
Nx &= 2mt^4 + (9m^2 - 5m)t^3 + (12m^3 - 16m^2 + 4m)t^2\\
&\quad + (6m^4 - 13m^3 + 18m^2 - m)t + m^5 - 3m^4 + 3m^3 - m^2,\\
Dx &= t^4 - 4t^3 + (-2m + 6)t^2 + (4m - 4)t + m^2 - 2m + 1,\\
Ny &= 4m^2t^7 + (12m^3 - 16m^2)t^6 + (13m^4 - 30m^3 + 25m^2)t^5\\
&\quad + (6m^5 - 3m^4 + 16m^3 - 19m^2)t^4\\
&\quad + (m^6 + 28m^5 - 52m^4 + 16m^3 + 7m^2)t^3\\
&\quad + (24m^6 - 71m^5 + 69m^4 - 21m^3 - m^2)t^2\\
&\quad + (8m^7 - 32m^6 + 48m^5 - 32m^4 + 8m^3)t\\
&\quad + m^8 - 5m^7 + 10m^6 - 10m^5 + 5m^4 - m^3,
\end{aligned}$$

$$\begin{aligned}Dy = {} & t^7 - 7t^6 + (-3m + 21)t^5 + (15m - 35)t^4 + (3m^2 - 30m + 35)t^3 \\ & + (-9m^2 + 30m - 21)t^2 + (-m^3 + 9m^2 - 15m + 7)t \\ & + m^3 - 3m^2 + 3m - 1.\end{aligned}$$

$\underline{10P}$:

$$\begin{aligned}Nx = {} & -mt^7 + (-2m^2 + 4m)t^6 + (-m^3 + 6m^2 - 6m)t^5 + (-4m^2 + 4m)t^4 \\ & + (-3m^4 + 11m^3 - 3m^2 - m)t^3 + (-m^5 + 14m^4 - 17m^3 + 4m^2)t^2 \\ & + (6m^5 - 13m^4 + 8m^3 - m^2)t + m^6 - 3m^5 + 3m^4 - m^3, \\ Dx = {} & t^6 + (6m - 4)t^5 + (11m^2 - 20m + 6)t^4 + (6m^3 - 30m^2 + 24m - 4)t^3 \\ & + (m^4 - 14m^3 + 28m^2 - 12m + 1)t^2 + (-2m^4 + 10m^3 - 10m^2 + 2m)t \\ & + m^4 - 2m^3 + m^2, \\ Ny = {} & 3m^2t^{10} + (13m^3 - 21m^2)t^9 + (22m^4 - 91m^3 + 64m^2)t^8 \\ & + (18m^5 - 160m^4 + 271m^3 - 111m^2)t^7 \\ & + (7m^6 - 146m^5 + 472m^4 - 449m^3 + 120m^2)t^6 \\ & + (m^7 - 73m^6 + 438m^5 - 744m^4 + 453m^3 - 83m^2)t^5 \\ & + (-19m^7 + 235m^6 - 654m^5 + 687m^4 - 285m^3 + 36m^2)t^4 \\ & + (-2m^8 + 74m^7 - 330m^6 + 537m^5 - 379m^4 + 109m^3 - 9m^2)t^3 \\ & + (13m^8 - 96m^7 + 230m^6 - 245m^5 + 120m^4 - 23m^3 + m^2)t^2 \\ & + (m^9 - 15m^8 + 52m^7 - 78m^6 + 57m^5 - 19m^4 + 2m^3)t \\ & - m^9 + 5m^8 - 10m^7 + 10m^6 - 5m^5 + m^4, \\ Dy = {} & t^9 + (9m - 6)t^8 + (30m^2 - 48m + 15)t^7 \\ & + (45m^3 - 141m^2 + 105m - 20)t^6 \\ & + (30m^4 - 186m^3 + 267m^2 - 120m + 15)t^5 \\ & + (9m^5 - 111m^4 + 303m^3 - 258m^2 \\ & + 75m - 6)t^4 + (m^6 - 30m^5 + 156m^4 - 244m^3 + 132m^2 - 24m + 1)t^3 \\ & + (-3m^6 + 36m^5 - 102m^4 + 99m^3 - 33m^2 + 3m)t^2 \\ & + (3m^6 - 18m^5 + 30m^4 - 18m^3 + 3m^2)t - m^6 + 3m^5 - 3m^4 + m^3.\end{aligned}$$

Next we calculate the equation of $X_1(13)$. On putting

$$6P = -7P,$$

we obtain

$$m\left(t^4 - 3t^3 + (-5m + 3)t^2 + (-4m^2 + 5m - 1)t - m^3 + 2m^2 - m\right) = 0.$$

Without loss of generality, the case $m = 0$ can be excluded. We get for $X_1(13)$ the "raw form":

$$t^4 - 3t^3 + (-5m + 3)t^2 + (-4m^2 + 5m - 1)t - m^3 + 2m^2 - m = 0.$$

By the birational transformation

$$m = \frac{V + U^3 - U}{V}, \qquad t = \frac{-U^2 + U}{V},$$

we arrive at the equation for $X_1(13)$ claimed in the theorem:

$$X_1(13)\colon V^2 + (U^3 - U^2 - 1)V - U^2 + U = 0.$$

The case of $X_1(14)$. For the calculation of $X_1(14)$, one must make sure that P is not a point of order 7. From the equation

$$6P = -8P,$$

one obtains

$$t^5 + (6m - 3)t^4 + (5m^2 - 14m + 3)t^3 + (m^3 - 10m^2 + 10m - 1)t^2 \\ + (-2m^3 + 4m^2 - 2m)t = 0.$$

The case $t = 0$ and $m \neq 0, 1$ implies that P has order 7. On the other hand, if $t = 0$ and $m = 0, 1$, one obtains $b = 0$. This is a contradiction to (2). Without loss of generality, t may be assumed different from zero. Then we get for $X_1(14)$ the "raw form":

$$t^4 + (6m - 3)t^3 + (5m^2 - 14m + 3)t^2 + (m^3 - 10m^2 + 10m - 1)t \\ -2m^3 + 4m^2 - 2m = 0.$$

By the substitution

$$m = \frac{8V - 24U + 32}{(2U - 8)V - U^3 + 6U^2 - 32}, \qquad t = \frac{2V - U^2 - 2U + 8}{2V - U^2 + 2U + 8},$$

we transform this equation birationally into

$$V^2 = U^3 + U^2 - 8U + 16.$$

Applying now the algorithm of Laska [6], we get the form of $X_1(14)$ given in the theorem:

$$X_1(14)\colon V^2 + UV + V = U^3 - U.$$

The case of $X_1(15)$. To calculate $X_1(15)$, we put

$$7P = -8P.$$

This implies the condition

$$\begin{aligned} &t^8 + (2m - 4)t^7 + (m^2 + 6)t^6 + (33m^2 - 17m - 4)t^5 \\ &\quad + (37m^3 - 78m^2 + 32m + 1)t^4 \\ &\quad + (25m^4 - 94m^3 + 93m^2 - 24m)t^3 + (8m^5 - 50m^4 + 84m^3 - 50m^2 + 8m)t^2 \\ &\quad + (m^6 - 12m^5 + 31m^4 - 31m^3 + 12m^2 - m)t - m^6 \\ &\quad + 4m^5 - 6m^4 + 4m^3 - m^2 = 0; \end{aligned}$$

or, equivalently,

$$\begin{aligned} &(m + t - 1)(t - 1)(m + t) \\ &\quad \big(t^5 - 2t^4 + (7m + 1)t^3 + (12m^2 - 12m)t^2 \\ &\qquad + (6m^3 - 12m^2 + 6m)t + m^4 - 3m^3 + 3m^2 - m\big) = 0. \end{aligned}$$

Without loss of generality, we can exclude the case that the first three factors are equal to zero. Then the "raw form" of $X_1(15)$ is given by

$$t^5 - 2t^4 + (7m + 1)t^3 + (12m^2 - 12m)t^2 + (6m^3 - 12m^2 + 6m)t \\ + m^4 - 3m^3 + 3m^2 - m = 0.$$

By the transformation

$$m = \frac{-V^2 + (U^2 - U)V + U^3}{-V^2 + (U^2 + U)V + U^3 + U^2}, \qquad t = \frac{UV}{-V^2 + (U^2 + U)V + U^3 + U^2},$$

we get the form of $X_1(15)$ required in the theorem:

$$X_1(15)\colon V^2 + UV + V = U^3 + U^2.$$

The case of $X_1(16)$. To calculate $X_1(16)$, we put

$$7P = -9P.$$

This implies the following condition:

$$\begin{aligned}
&4mt^7 + (14m^2 - 18m)t^6 + (16m^3 - 54m^2 + 34m)t^5 \\
&\quad + (7m^4 - 53m^3 + 89m^2 - 35m)t^4 \\
&\quad + (m^5 - 21m^4 + 80m^3 - 81m^2 + 21m)t^3 \\
&\quad + (-3m^5 + 34m^4 - 68m^3 + 42m^2 - 7m)t^2 \\
&\quad + (8m^5 - 25m^4 - 27m^3 - 11m^2 + m)t + m^6 - 4m^5 + 6m^4 - 4m^3 + m^2 = 0.
\end{aligned}$$

Equivalently,

$$\begin{aligned}
&m(m + t - 1)(m + 2t - 1) \\
&\quad \big(2t^5 + (4m - 6)t^4 + (m^2 - 10m + 7)t^3 + (-3m^2 + 11m - 4)t^2 \\
&\qquad\qquad + (5m^2 - 6m + 1)t + m^3 - 2m^2 + m\big) = 0.
\end{aligned}$$

Once more we can exclude that the first three factors are zero, and therefore the "raw form" of $X_1(16)$ is:

$$\begin{aligned}
&2t^5 + (4m - 6)t^4 + (m^2 - 10m + 7)t^3 + (-3m^2 + 11m - 4)t^2 \\
&\quad + (5m^2 - 6m + 1)t + m^3 - 2m^2 + m = 0.
\end{aligned}$$

By the following birational transformation

$$m = \frac{V^2 + (U - 1)V}{V^2 + (U - 1)V - U}, \qquad t = \frac{-1}{V - 1},$$

this form is equivalent to

$$X_1(16)\colon (U^2 + 3U + 2)V^2 + (U^3 + 4U^2 + 4U)V - U = 0.$$

The case of $X_1(17)$. We calculate the equation of $X_1(17)$ by setting

$$8P = -9P$$

and obtain the condition

$$\begin{aligned}
&-t^9 + (-2m + 7)t^8 + (-m^2 + 24m - 21)t^7 + (56m^2 - 87m + 35)t^6 \\
&\quad + (89m^3 - 213m^2 + 151m - 35)t^5 \\
&\quad + (81m^4 - 291m^3 + 332m^2 - 143m + 21)t^4 \\
&\quad + (40m^5 - 212m^4 + 365m^3 - 261m^2 + 75m - 7)t^3 \\
&\quad + (10m^6 - 81m^5 + 200m^4 - 215m^3 + 105m^2 - 20m + 1)t^2 \\
&\quad + (m^7 - 15m^6 + 52m^5 - 78m^4 + 57m^3 - 19m^2 + 2m)t \\
&\quad - m^7 + 5m^6 - 10m^5 + 10m^4 - 5m^3 + m^2 = 0.
\end{aligned}$$

This is equivalent to

$$\begin{aligned}&(m+t-1)^2\\&\quad\big(t^7-5t^6+(-12m+10)t^5+(-27m^2+33m-10)t^4\\&\qquad+(-23m^3+59m^2-33m+5)t^3+(-8m^4+40m^3-45m^2+14m-1)t^2\\&\qquad+(-m^5+11m^4-21m^3+13m^2-2m)t+m^5-3m^4+3m^3-m^2\big)=0.\end{aligned}$$

The case $m+t-1=0$ can be excluded without loss of generality, and the "raw form" of $X_1(17)$ is

$$\begin{aligned}&t^7-5t^6+(-12m+10)t^5+(-27m^2+33m-10)t^4\\&\quad+(-23m^3+59m^2-33m+5)t^3+(-8m^4+40m^3-45m^2+14m-1)t^2\\&\quad+(-m^5+11m^4-21m^3+13m^2-2m)t+m^5-3m^4+3m^3-m^2=0.\end{aligned}$$

By virtue of the transformation

$$m=\frac{V+1}{V+U^2},\qquad t=\frac{U^2+U}{V+U^2},$$

the above form of $X_1(17)$ is birationally equivalent to the form required in the theorem:

$$\begin{aligned}X_1(17)\colon\quad &V^4+(U+2)V^3+(U^3+1)V^2+(-U^5-2U^4-U^3-U^2-U)V\\&-U^5-2U^4-U^3=0.\end{aligned}$$

The case of $X_1(18)$. To calculate the equation of $X_1(18)$, we set

$$8P=-10P.$$

This equation implies the condition:

$$\begin{aligned}&-t^{11}+(-12m+7)t^{10}+(-36m^2+76m-21)t^9\\&\quad+(-47m^3+209m^2-204m+35)t^8\\&\quad+(-30m^4+251m^3-497m^2+300m-35)t^7\\&\quad+(-9m^5+151m^4-508m^3+617m^2-260m+21)t^6\\&\quad+(-m^6+44m^5-222m^4+462m^3-416m^2+132m-7)t^5\\&\quad+(5m^6-10m^5+44m^4-140m^3+136m^2-36m+1)t^4\\&\quad+(26m^6-120m^5+162m^4-64m^3-8m^2+4m)t^3\\&\quad+(9m^7-67m^6+153m^5-147m^4+58m^3-6m^2)t^2\\&\quad+(m^8-14m^7+47m^6-68m^5+47m^4-14m^3+m^2)t\\&\quad-m^8+5m^7-10m^6+10m^5-5m^4+m^3=0;\end{aligned}$$

or, equivalently,

$$\begin{aligned}&(m+t)(t-1)(m+t-1)^2(t^2-2t-m+1)\\&\quad\big(t^5+(9m-2)t^4+(6m^2-11m+1)t^3+(m^3+3m)t^2\\&\qquad\qquad+(4m^3-4m^2)t+m^4-2m^3+m^2\big)=0.\end{aligned}$$

Without loss of generality, the first four factors can be omitted, and we get for $X_1(18)$ the "raw form":

$$\begin{aligned}X_1(18)\colon\quad &t^5+(9m-2)t^4+(6m^2-11m+1)t^3+(m^3+3m)t^2\\&+(4m^3-4m^2)t+m^4-2m^3+m^2=0.\end{aligned}$$

Transforming now this equation birationally by means of the transformation

$$m = \frac{(-U+1)V+U^2}{-V^2+(U+1)V+U^2}, \qquad t = \frac{UV}{-V^2+(U+1)V+U^2},$$

we obtain the form of $X_1(18)$ asserted in the theorem:

$$X_1(18)\colon (U^2-2U+1)V^2+(-U^3+U-1)V+U^3-U^2=0.$$

The $X_1(N)$ are elliptic for $N = 11$, 14 and 15. The form of these $X_1(N)$ as given in the theorem is called an *equation of restricted type* for $X_1(N)$ [6].

In the following table, we compile the characteristics of these $X_1(N)$. In the first row we list the values of N, in the second the discriminant of $X_1(N)$, then the j-invariant, the conductor of $X_1(N)$, the torsion group of $X_1(N)$ over **Q**, and in the last row we display a generator of $X_1(N)_{\text{tor}}(\mathbf{Q})$.

N	11	14	15
Δ	-11	$-2 \cdot 14$	-15
j	$-\frac{2^{12}}{11}$	$-\frac{5^6}{2 \cdot 14}$	$-\frac{1}{15}$
$C_{X_1(N)}$	11	14	15
$X_1(N)_{\text{tor}}(\mathbf{Q})$	$\mathbf{Z}/5\mathbf{Z}$	$\mathbf{Z}/6\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$
Generator of $X_1(N)_{\text{tor}}(\mathbf{Q})$	(1, -1)	(1, -2)	(15, 108)

For calculating an elliptic curve with a point of order 11, we transform $X_1(11)$ into the form $Y^2 = f(X)$ for $f(X) \in \mathbf{Z}[X]$. The corresponding equation for $X_1(11)$ is

$$(7) \qquad Y^2 = X^3 - 4X^2 + 16.$$

Inserting, e.g., $X = 2$ yields

$$Y = \pm 2\sqrt{2}.$$

We now carry out our calculations over the ground field $\mathbf{Q}(\sqrt{2})$. If we set $X = 2$ and $Y = 2\sqrt{2}$ in the birational transformations, performed to obtain $X_1(11)$ in the form of Eq. (7), and reverse these transformations, we get the coefficients b and c as

$$b = -\frac{1}{16}\sqrt{2}, \qquad c = \frac{1}{4}(1-2\sqrt{2}),$$

giving the elliptic curve E in $E(b,c)$-form

$$E\colon Y^2 + \left(\frac{3}{4} + \frac{1}{4}\sqrt{2}\right)XY + \frac{1}{16}\sqrt{2}\,Y = X^3 + \frac{1}{16}\sqrt{2}\,X^2$$

with $P = (0,0)$ as a point of order 11.

Not much is known concerning the question: Over which quadratic fields K are there elliptic curves with a K-rational point of order 11 and over which are there none? With regard to this question, we have examined the fields $\mathbf{Q}(\sqrt{-1})$ and $\mathbf{Q}(\sqrt{-11})$ and have proved

THEOREM 2. *Over the quadratic fields $K = \mathbf{Q}(\sqrt{-1})$ and $K = \mathbf{Q}(\sqrt{-11})$, there are no elliptic curves having a K-rational point of order* 11.

Proof. One must find the rational points of $X_1(11)$ and the rational points of $X_1(11)$ twisted by -1 or -11. Then one proves Theorem 2 by means of theorems of Nagell [10] and Kramer [3]. (See [11] for details.)

We shall now establish tables of elliptic curves E with torsion groups of one of the following isomorphism types:

$$E_{\text{tor}}(K) \cong \mathbf{Z}/m\mathbf{Z}; \qquad m = 11, 13, 14, 15, 16 \text{ and } 18.$$

K is a proper quadratic number field over $\mathbf{Q}$. The only K-rational points which we have found on $X_1(17)$ over quadratic number fields K over $\mathbf{Q}$ are cusps. Therefore, we do not expect that there are examples of elliptic curves over K with K-rational points of order 17. This is also suggested by the fact that $X_1(17)$ has genus 5.* In our list of examples, the curve E will be given in *short Weierstrass normal form*:

$$E\colon Y^2 = X^3 + AX + B; \qquad A, B \in K,$$

which is *quasi-minimal*. This means that there are no rational primes p such that

$$p^4 | A \quad \text{and} \quad p^6 | B.$$

Each example in the tables is separated from the other by a row of stars. The examples are printed according to the following scheme:

X		D	
A			
B			
j			
p		$v_{\mathfrak{p}}(j)$	type of decomposition
	x		y
p		$\mu_{\mathfrak{p}}$	type of decomposition

Here: "X" is the X-value which we insert into the equation $Y^2 = f(X)$ of $X_1(N)$ for getting the desired elliptic curve E over K. "D" is, up to a factor 4, the discriminant of the quadratic ground field $K = \mathbf{Q}(\sqrt{D})$. "A" and "B" are the coefficients of the elliptic curve E given in short Weierstrass normal form. In addition, we have calculated the j-invariant and a prime decomposition of j. Here p denotes the rational prime that divides the prime divisor $\mathfrak{p}$, $v_{\mathfrak{p}}$ is the normalized $\mathfrak{p}$-adic exponential valuation and $v_{\mathfrak{p}}(j)$ is the $\mathfrak{p}$-value of j. The last column contains the type of decomposition of p in K. "D" denotes decomposed, "I" inert and "R" ramified. "x" and "y" are the x- and y-coordinates of a generator of $E_{\text{tor}}(K)$. Finally, we calculated the $\mu_{\mathfrak{p}}$-values of E and determined the coefficient divisor m (see [14]). The $\mu_{\mathfrak{p}}$-values are important with respect to the determination of the torsion structure of an elliptic curve over an algebraic number field [14] and with respect to height-calculations [5]. For each rational prime p, we display the $\mu_{\mathfrak{p}}$-value and the type of decomposition of p in K, if $\mu_{\mathfrak{p}}$ is different from zero. If the $\mu_{\mathfrak{p}}$-values are zero for all prime divisors $\mathfrak{p}$ of K, we leave the space empty.

The numbers $\alpha = a + b\sqrt{D} \in \mathbf{Q}(\sqrt{D})$, $a, b \in \mathbf{Q}$, are displayed as follows:

$$\alpha = (a, b).$$

*Recently Kamienny has proved, that there are no elliptic curves over quadratic number fields K over $\mathbf{Q}$ having a K-rational point of order 17. (Cf. S. Kamienny, "Torsion points on elliptic curves over all quadratic fields", to appear.)

Table I
$E_{\mathrm{tor}}(K) \cong \mathbf{Z}/11\mathbf{Z}$

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

-4       -7

( -2187 , -864 )
( 170694 , -87264 )

( 2994657/68608 , 4432109/137216 )

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
2             -11             D
67            -1              D
67            0               D
13729         3               D
13729         0               D

( 15 , -12 )                     ( 324 , -108 )

3             1               I
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

2        2

( -3483 , 1836 )
( 163890 , -108108 )

( -998961/184 , -4758131/1472 )

2             -11             R
23            -1              D
23            0               D
7393          3               D
7393          0               D

( 33 , 30 )                      ( 0 , 432 )

3             1               I
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

Table II
$E_{\mathrm{tor}}(K) \cong \mathbf{Z}/13\mathbf{Z}$

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

-2       193

( -17501728071870 , 125980162056 )
( 1262137402216304190 , -908506381637 19672 )

( -1966266751104504 73/326517350400 , 0 )

2             -13             D
3             -13             D
5             -2              I
7             3               D
83071         3               D

( 549447 , -39516 )              ( 34274664 , -2466936 )

3             1               D

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

TABLE II (*continued*)

```
************************************************************

-1        17

( -411864 , 99560 )
( 211240640 , -51226432 )

( -60698457/406960 , 0 )

2               -13             D
3               3               I
5               -1              I
131             3               I

( 358 , -74 )                       ( 6656 , -1536 )

************************************************************

2         17

( -4323 . -1048 )
( 227630 , 55208 )

( -60698457/40960 , 0 )

2               -13             D
3               3               I
5               -1              I
131             3               I

( -49 , -12 )                       ( -296 , -72 )

************************************************************

3         313

( 2327667525288 , 1315675463376 )
( 15514489700031254440 , 8769308056319 6352 )

( 68633948441807/65303470080 , 0 )

2               -13             D
3               -13             D
5               -1              I
7               3               I
5849            3               D

( -277962 , -15714 )                ( -292750848 , -16547328 )

3               1               D

************************************************************

4         2257

( -1794164929227099 , -37765616934240 )
( 409127309804631089 72790 , 86117753211312825 2448 )

( 4229962591466145 4417/534966026895360 , 0 )

2               -26             D
3               -13             D
5               -1              I
13              6               I
53              3               I
389             3               D

( 18897603 , 397776 )               ( -6952140576 , -146336544 )

3               1               D

************************************************************
```

Table III
$E_{\text{tor}}(K) \cong \mathbf{Z}/14\mathbf{Z}$

```
***********************************************************

-3        22

( -4399866430373381403 , -9380390912860 5216 )
( 7516285622934343121440566 , 1602474795479465435675232 )

( 19631310746169659224439/53197633242289815552 , 1262333629667
54013038293/434447338145366827008 )

2               -28             R
3               -14             D
7               -7              D
13              -2              D
13              0               D
239             -1              D
239             0               D
11113           0               D
11113           3               D
34651           0               D
34651           3               D
1718011         3               D
1718011         0               D

( -48820125 , -14300688 )         ( -5334018607008 , -1153680851232 )

3               1               D
***********************************************************

-2        7

( -51033138723 , -19289646936 )
( 6265927466034894 , 2368297291386600 )

( 3265635553/11664 , 29548593817/279936 )

2               -14             R
3               -7              D
19              3               D
19              0               D
165059          0               D
165059          3               D

( 92463 , 27300 )                 ( -5429592 , -3143448 )
***********************************************************
```

TABLE III (*continued*)

```
*************************************************************

-1          6

( -15417181441042073l , -6293487143767l616 )
( 32948988908969804432803542 , 13451360607076546447682112 )

( 251731528398115981471352 9/1498265856000000 , 368307445325827
41490l1931/5618496960000000 )

2                 -28              R
3                 -7               R
5                 -7               D
19                0                D
19                3                D
43                -1               D
43                0                D
71                -2               D
71                0                D
211               0                D
211               3                D
331               3                D
331               0                D
503               0                D
503               3                D
861293            0                D
861293            3                D

( 167199699 , 61992864 )        ( 5543964000 , -21639096000 )

*************************************************************


1          10

( -12054662356347 , 2794167678816 )
( 19484656563306373974 , -5460161248744831008 )

( 21795187981092955589 39/32626354176000 , -513654278948026651 2
563/244397656320000 )

2                 -28              R
3                 -7               D
5                 -7               R
13                0                D
13                -1               D
31                3                D
31                0                D
41                0                D
41                -2               D

*************************************************************

79                0                D
79                3                D
1721              3                D
1721              0                D
1180409           3                D
1180409           0                D

( -708717 , 591792 )            ( -4394878560 , 1320854688 )

3                 1                D

*************************************************************
```

TABLE III (*continued*)

```
************************************************************
2        3

( -2952963 , 1704888 )
( 1067436846 , -616284936 )

( 15792703/22464 , -103368947/134784 )

2               -14             R
3               -7              R
13              -1              D
13              0               D
37              0               D
37              3               D
2269            3               D
2269            0               D

( -1185 , 684 )                ( -26568 , 15336 )
************************************************************
```

TABLE IV
$E_{\text{tor}}(K) \cong \mathbf{Z}/15\mathbf{Z}$

```
************************************************************
-1       -7

( 539042262696 , -91517868792 )
( -158658192869698368 , -141784327118177856 )

( -19853211655423/61975789568 , 8327088487989/108457631744 )

2               -15             D
7               -5              R
11              0               D
11              -3              D
29              0               D
29              -1              D
179             0               D
179             3               D
259499          0               D
259499          3               D

( 4155606 , -54978 )           ( 8591837184 , -197793792 )

3               1               I
************************************************************
-1/2     -95

( -36843438820539915 , 9129754598177520 )
( 3933501427988825876471430 , -1526895018264725064674640 )

( -130339725162288764665/1531233206539812864 , 163416495031638
43652635/130920439159153999872 )

2               -15             D
3               -15             D
5               2               R
11              -3              D
11              0               D
19              -5              R
61              -1              D
61              0               D
2671            0               D
2671            3               D
23189           0               D
23189           3               D
223259          0               D
223259          3               D
************************************************************
```

TABLE IV (*continued*)

```
**********************************************************

( 964404375 , 2334036 )
( 29444742515700 , 232692977124 )

3                 1                 D
5                 2/3               R

**********************************************************

3/2       33

( 4943582901 , -860567328 )
( 100854159004422 , -17556455592864 )

( -189670366553O8187/8785723392 , -4955692963031933/13178585088 )

2                 -15               D
3                 -5                R
29                0                 D
29                3                 D
31                -3                D
31                0                 D
12281131          0                 D
12281131          3                 D

( -8889 , 1548 )                 ( -2251476 , 391932 )

**********************************************************

2         5

( -630315 , 281880 )
( 328392630 , -146861640 )

( -121945/32 , 0 )

2                 -5                I
5                 2                 R
29                3                 D

( -585 , 264 )                   ( -11340 , 5076 )

3                 1                 I
5                 2/3               R

**********************************************************
```

TABLE V
$E_{\text{tor}}(K) \cong \mathbf{Z}/16\mathbf{Z}$

```
**********************************************************

-4        10

( -4919326431372 , -540298585008 )
( 4389838223699367504 , 688123047823241184 )

( 3784994652202948 81/120530818800 , 0 )

2                 -8                R
3                 -16               D
5                 -4                R
7                 -1                I
723361            3                 D

( 84458 , 151140 )               ( -689692320 , 111484512 )

3                 1                 D

**********************************************************
```

TABLE V (*continued*)

```
*************************************************************

-3        -15

( 404692008 , 73778280 )
( -1931895059776 , -658051602240 )

( 1023887723039/928972800 , 0 )

2               -16             D
3               -8              R
5               -4              R
7               -1              I
10079           3               I

( 27238 , -2602 )               ( 5253120 , -497664 )

*************************************************************

-1/2      -15

( 272133 , 0 )
( 41173974 , 0 )

( 1023887723039/928972800 , 0 )
2               -16             D
3               -8              R
5               -4              R
7               -1              I
10079           3               I

( 3 , -144 )                    ( -6480 , -432 )

*************************************************************

1         105

( 319281675048 , 22722016968 )
( 63178738374096576 , 5446154665957824 )

( 1023887723039/928972800 , 0 )

2               -16             D
3               -8              R
5               -4              R
7               -2              R
10079           3               D

( 698502 , 58590 )              ( 934778880 , 78575616 )

*************************************************************

2         70

( -69908375342547 , -49190139939420 )
( 254857783665620184714 , 23370400912286838060 )

( 3784994652202948881/120530818800 , 0 )

2               -8              R
3               -16             D
5               -1              R
7               -2              R
723361          3               D

( 7270053 , 456582 )            ( 12615228360 , 1377258876 )

3               1               D

*************************************************************
```

TABLE VI
$E_{\text{tor}}(K) = \mathbf{Z}/18\mathbf{Z}$

```
************************************************************

-1        33

( -162675 , -28296 )
( 35441118 , 6168312 )

( 31701473569/524288 , 5519537297/524288 )

2            -9            D
2            -18           D
17           0             D
17           3             D
3329         3             D
3329         0             D

( -285 , -48 )                ( -4428 , -756 )

************************************************************

-1/4      8241

( -6681030592835O7 , -6973228583640 )
( 9041240256839470910O6 , 987144137879290246S0 )

( 56066410524761901395411477945777126615952l/17826086125568000
000000000000000 , -6176028936156912169249015730864995075351/17
826086125568000000000000000000 )

2            -18           D
2            -36           D
5            -18           D
5            -9            D
7            -6            D
7            -3            D
17           -2            D
17           -1            D
197          0             D
197          3             D
307          0             D
307          3             D
13358503     3             D
13358503     0             D
927720953    3             D
927720953    0             D

( 11499447 , 88980 )          ( -2890029240 , -31744440 )

************************************************************

1/2       33

( -162675 , 28296 )
( 35441118 , -6168312 )

( 31701473569/524288 , -5519537297/524288 )

2            -18           D
2            -9            D
17           3             D
17           0             D
3329         0             D
3329         3             D

( 147 , -24 )                 ( -540 , 108 )

************************************************************
```

For the sake of completeness, we mention that Stephens and Stroeker [12], by a different method, have found three elliptic curves with a point of order 11 and one elliptic curve with a point of order 15.

We now give an example of an elliptic curve with a point of order 18, where the coefficients are much bigger than before.

```
99/2        8691664833337

( -14768222079904599000226787421543491231849193473355 , -197
0467345153166758654514839049908324353312 )

( 2197129153421664762322899620769929522381139061084534394472
1343491235571462 , 43690982801166816298320513373853689518042
37918513251914616441002976 )


( 1820771879928064881129012745252230204273591164876834330993
955161082530792489104411320768821434152886994185291068594483
46574971204881791849038369/165171715810521209210213942419805
861455244043038594604419810218087221490524489372242729838653
659246889869907591168 , -19530081342348892804570498768647272
039415917364691634885610209665069114446730529340756778918126
0629305849739652435294219105604111310340811/1651717158105212
092102213942419805861455244043038594604419810218037221490524
489372242729839653659246889869907591168 )


( 2476188105984575611665015 , -1453439138376420 36 )

( 680494937500537833832958824599248388 , -764060714620524131
742929250396 )


3             1             D
```

Here we were unable to calculate the prime decomposition of the j-invariant, because to this end we had to factor the norm of the j-invariant over $\mathbf{Q}$, which is too large a number. Our calculations involved much bigger numbers, the biggest one being one of 5,000 digits.

We have added on microfiches (at the end of this issue) a rather comprehensive table of examples of elliptic curves with torsion points of order 11, 13, 14 15, 16 and 18. For lack of computer time, we have not calculated all the prime decompositions of j in our tables.

3. Algorithms. For finding the transformations needed for the calculation of the $X_1(N)$, no general algorithm exists. The number of steps necessary for carrying out the transformations varies greatly. For calculating an equation of $X_1(11)$, we used 3 steps. In other cases, sometimes more than 15 steps were required. To analyze the algebraic curves and to test the transformations, we wrote a program based on algorithms for the factorization of polynomials, for birational transformations and for computing resultants and singularities [11]. The program works interactively. There are many ways to deduce from the raw form the form of the $X_1(N)$ given in Theorem 1. The user of our program is in the position to interactively test many birational transformations before fixing the next step. The algorithm for the birational transformation is as follows:

(1) Input an algebraic curve $P(X,Y)=0$, $P(X,Y)\in \mathbf{Z}[X,Y]$,

$$P(X,Y)=\sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}X^iY^j.$$

Input the transformation

$$X=\frac{f_1(X_1,Y_1)}{f_2(X_1,Y_1)},\qquad Y=\frac{g_1(X_1,Y_1)}{g_2(X_1,Y_1)},$$

$f_i(X_1,Y_i)$, $g_i(X_1,Y_1)\in \mathbf{Z}[X_1,Y_1]$; $i=1,2$, and
$f_2(X_1,Y_1)\cdot g_2(X_1,Y_1)\not\equiv 0$.

(2) Determine $P_1(X_1,Y_1)$ in accordance with the equation

$$\begin{aligned}P(X,Y)&=\left(\sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij}f_1(X_1,Y_1)^i f_2(X_1,Y_1)^{k-i}g_1(X_1,Y_1)^j g_2(X_1,Y_1)^{l-j}\right)\\&\quad\cdot f_2(X_1,Y_1)^{-k}\cdot g_2(X_1,Y_1)^{-l}\\&=:P_1(X_1,Y_1)\cdot f_2(X_1,Y_1)^{-k}\cdot g_2(X_1,Y_1)^{-l},\\&\qquad\qquad P_1(X_1,Y_1)\in\mathbf{Z}[X_1,Y_1].\end{aligned}$$

(3) Print out the polynomial $P_1(X_1,Y_1)$.
By the above transformation, $P_1(X_1,Y_1)=0$ is the curve equivalent to $P(X,Y)=0$.
END.

We now state the algorithm used for the calculation of the tables.

(1) Input: – $X_1(N)$ given in the form $Y^2=f(X)$; $f(X)\in\mathbf{Z}[X]$
– the birational transformation to obtain this form of the $X_1(N)$ from the raw form, and the substitution made during the calculation of $6P$.
– the x-value which we wish to substitute into the equation of $X_1(N)$.

(2) If $f(x)=0$ then go to (7).
Determine the discriminant D of the ground field.

(3) Determine the coefficients b and c.
Calculate the discriminant Δ of a curve E in $E(b,c)$-form.
If $\Delta=0$ then go to (7).
If $\Delta\neq 0$ then E is an elliptic curve with the point $P=(0,0)$ as a point of order N.

(4) Transform E in short and quasi-minimal Weierstrass normal form such that the coefficients A and B are elements of $\mathbf{Z}[\sqrt{D}]$.

(5) Determine $E_{\mathrm{tor}}(\mathbf{Q}(\sqrt{D}))$ by the reduction method.
Calculate j and the $v_{\mathfrak{p}}(j)$-values.
Compute the $\mu_{\mathfrak{p}}$-values.

(6) Print the results in the form described above.
Go to (8).

(7) Print that the point $(x,f(x))$ on $X_1(N)$ is a cusp.

(8) END.

There is no difficulty in determining the $v_{\mathfrak{p}}$-values in a quadratic field $K=\mathbf{Q}(\sqrt{d})$, if $\mathfrak{p}$ lies over a rational prime p which is inert or ramifies in K. In case p is decomposed, we can prove the following lemma [11].

LEMMA. *Let $K = \mathbf{Q}(\sqrt{d})$, $d \in \mathbf{Z}$, be a quadratic field and let p be a rational prime which decomposes in K:*

$$p \cong \mathfrak{p}_1 \cdot \mathfrak{p}_2,$$

where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime divisors of K. Let $A = a_1 + a_2\sqrt{d} \in \mathbf{Z}(\sqrt{d})$, $a \in \mathbf{Z}$ be such that

$$a = \begin{Bmatrix} \gcd(a_1, a_2);\ \textit{if } d \equiv 2, 3 \bmod 4 \\ 2\gcd(a_1, a_2);\ \textit{if } d \equiv 1 \bmod 4 \end{Bmatrix}.$$

Let a_1', $a_2' \in \frac{1}{2}\mathbf{Z}$ be such that

$$A = a\left(a_1' + a_2'\sqrt{d}\right) =: aA'.$$

Then we have

(i) $p \mid \mathfrak{p}_2 \cdot A'$ *implies*

$$v_{\mathfrak{p}_1}(A) = v_p\big(N_{K/\mathbf{Q}}(A)\big) - v_p(a), \qquad v_{\mathfrak{p}_2}(A) = v_p(a).$$

(ii) $p \nmid \mathfrak{p}_2 \cdot A'$ implies

$$v_{\mathfrak{p}_1}(A) = v_p(a), \qquad v_{\mathfrak{p}_2}(A) = v_p\big(N_{K/\mathbf{Q}}(A)\big) - v_p(a).$$

$N_{K/\mathbf{Q}}$ denotes the norm function of $K/\mathbf{Q}$, and v_p is the normalized p-adic exponential valuation of $\mathbf{Q}$. The lemma yields the following algorithm for determining $v_{\mathfrak{p}_1}(A)$ and $v_{\mathfrak{p}_2}(A)$.

```
(1) Input $d$, $a_1$, $a_2$ and $p$.
(2) Determine $a$, $a_1'$, $a_2'$ as in the above lemma.
    If $p = 2$ then set $p_2 = (1 - \sqrt{d})/2$
            else determine $a \in \{1, 2, \ldots, (p-1)/2\}$ such that
            $a^2 \equiv 1 \bmod d$ and set $p_2 = a - \sqrt{d}$.
(3) Calculate $c = p_2 \cdot (a_1' + a_2'\sqrt{d})$.
    If $p \mid c$ then go to (4)
            else go to (5).
(4) Calculate $v_{\mathfrak{p}_1}(A) = v_p(N_{K/\mathbf{Q}}(A)) - v_p(a)$,
              $v_{\mathfrak{p}_2}(A) = v_p(a)$.
    END
(5) Calculate $v_{\mathfrak{p}_i}(A) = v_p(a)$,
              $v_{\mathfrak{p}_2}(A) = v_p(N_{K/\mathbf{Q}}(A)) - v_p(a)$.
    END
```

The cpu-time used to compute the tables varies greatly because the results are often very large numbers. We experienced cpu-times ranging from 15 seconds to half an hour for one single example.

4. Concluding Remarks. (1) The j-invariants of those elliptic curves with a point of order 13 or 16 appearing in our tables turn out to be defined already over $\mathbf{Q}$. This is probably due to the fact that we obtain our elliptic curves by choosing as x-values rational numbers in the equation of $X_1(N)$ for $N = 13$, respectively 16. Also, we encountered the phenomenon that different x-values in $X_1(N)$, $N = 11, 13, 14, 15, 16$ and 18, yield elliptic curves with the same j-invariant. It would be desirable to have some more information about the relationship between the x-values and the j-invariants.

(2) It is, of course, interesting to ask the question as to whether the order N ($N = 11, 13, 14, 15, 16$ and 18) of a torsion point of an elliptic curve over a quadratic field K depends on the type of decomposition in K of the rational primes p dividing N. This does not seem to be the case for $N = 11$, 13, 14 and 15 though, in the case of $N = 14$, we have only checked this for the prime $p = 7$. In the case of $N = 16$, we could not get any result of the desired type. In the case of $N = 18$, however, the prime $p = 2$ turned out to decompose, and the prime $p = 3$ either decomposed or ramified [11].

(3) On the basis of our tables, we could, for the first time, test many important theorems and results of the theory of elliptic curves. We could, e.g., verify the theorem of Nagell [10] already applied for proving Theorem 2. The $\mu_{\mathfrak{p}}$-values of the examples coincide with the generalized Nagell-Lutz-Cassels theorem (see [14]).

(4) Almost all the prime divisors dividing the j-invariants come from prime numbers which are decomposed in the corresponding quadratic field. In addition, we point out that the exponents of the prime divisors, which occur in the denominators of the j-invariants, are as they should be according to the theory of Tate-curves [13].

Acknowledgment. I would like to thank Professor H. G. Zimmer for calling my attention to this subject matter and making some valuable suggestions.

Fachbereich Mathematik
Universität des Saarlandes
D-6600 Saarbrücken
West Germany

1. G. Billing & K. Mahler, "On exceptional points on cubic curves," *J. London Math. Soc.*, v. 15, 1940, pp. 32–43.

2. M. A. Kenku, "Certain torsion points on elliptic curves defined over quadratic fields," *J. London Math. Soc.* (2), v. 19, 1979, pp. 233–240.

3. K. Kramer, "Arithmetic of elliptic curves upon quadratic extension," *Trans. Amer. Math. Soc.*, v. 264, 1981, pp. 121–135.

4. D. S. Kubert, "Universal bounds on the torsion of elliptic curves," *Proc. London Math. Soc.* (3), v. 33, 1976, pp. 193–237.

5. S. Lang, *Conjectured Diophantine Estimates on Elliptic Curves*, Progress in Mathematics, vol. 35, Birkhäuser, Basel, 1983.

6. M. Laska, "An algorithm for finding a minimal Weierstrass equation for an elliptic curve," *Math. Comp.*, v. 38, 1982, pp. 257–260.

7. Ju. I. Manin, "The p-torsion of elliptic curves is uniformly bounded," *Math. USSR-Izv.*, v. 3, 1969, pp. 433–438. (transl.)

8. B. Mazur, "Rational points of modular curves," in *Modular Functions of One Variable* V, Lecture Notes in Math., vol. 601, 1977, pp. 107–148.

9. J.-F. Mestre, "Corps euclidiens, unités exceptionnelles et courbes elliptiques," *J. Number Theory*, v. 13, 1981, pp. 123–137.

10. T. Nagell, "Les points exceptionnels sur les cubiques planes du premier genre. I, II," *Nova Acta Reg. Soc. Sci. Upsaliensis* (4), v. 14, nos. 1, 3, 1946–1947.

11. M. A. Reichert, *Explizite Bestimmung nichttrivialer Torsionsstrukturen elliptischer Kurven über quadratischen Zahlkörpern*, Diploma thesis, Saarbrücken, 1983.

12. N. M. Stephens & R. J. Stroeker, *The Torsion Group of Elliptic Curves Over Quadratic Fields*, Report 8113/M, Econometric Institute, Erasmus University Rotterdam, 1981.

13. J. T. Tate, "Algorithm for finding the type of a singular fibre in an elliptic pencil," in *Modular Functions of One Variable* IV, Lecture Notes in Math., vol. 476, 1975, pp. 33–52.

14. H. G. Zimmer, "Torsion points on elliptic curves over a global field," *Manuscripta Math.*, v. 29, 1979, pp. 119–145.