MATHEMATICS OF COMPUTATION
VOLUME 38, NUMBER 157
JANUARY 1982

An Algorithm for Finding a Minimal Weierstrass Equation for an Elliptic Curve

By Michael Laska

Dedicated to Professor Jens Mennicke on his 50th birthday

Abstract. Let E be an elliptic curve defined over an algebraic number field K and assume that some Weierstrass equation for E over K is given. Then an algorithm is described which yields a global minimal Weierstrass equation for E over K provided such a global minimal Weierstrass equation does exist.

1. General Remarks. Tate's algorithm in [2], which is actually intended to give the conductor and Kodaira reduction type of an elliptic curve E_K defined over K, where K is an algebraic number field, can be used to calculate a minimal (with respect to some discrete valuation of K) Weierstrass equation for E_K, once some Weierstrass equation for E_K is given. In the following we describe an algorithm which does the same. It is quite easy to write a computer program for the present algorithm, whereas Tate's algorithm needs greater effort and requires iteration. Moreover, the present algorithm may be useful in conjunction with Tate's algorithm for calculating the conductor, because implementing Tate's algorithm on a computer is much easier if one knows ahead of time that the Weierstrass equation for E_K is minimal.

In the following let K be an algebraic number field of degree n, let $\mathfrak{O} = \mathfrak{O}_K$ be the ring of integers of K, and let $\{\omega_1, \ldots, \omega_n\}$ be any integral basis for $\mathfrak{O}$. Let $E = E_K$ be an elliptic curve defined over K. We assume that E admits a global minimal Weierstrass equation over K; this is always the case for example if the class number of K is prime to 6. Details on elliptic curves may be found in [1]; we recall here only the following facts.

Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be any Weierstrass equation for E over K. Then $y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$ is also a Weierstrass equation for E over K if and only if there is transformation of type

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

with $r, s, t \in K$ and $u \in K^*$. In this case the coefficients of the two equations and their quantities c_4, c_6, Δ and c_4', c_6', Δ', respectively, are related by the following formulas:

$$ua_1' = a_1 + 2s,$$
$$u^2a_2' = a_2 - sa_1 + 3r - s^2,$$

Received March 1, 1980; revised February 27, 1981.
1980 *Mathematics Subject Classification.* Primary 14K07.

$$u^3a_3' = a_3 + ra_1 + 2t,$$
$$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$
$$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2,$$
$$u^4c_4' = c_4,$$
$$u^6c_6' = c_6,$$
$$u^{12}\Delta' = \Delta.$$

The coefficients a_1, a_2, a_3 of any integral Weierstrass equation for E over K satisfy the following congruences in terms of the quantities c_4 and c_6:

$$a_1^4 \equiv c_4 \bmod 8, \qquad a_2^3 \equiv -a_1^6 - c_6 \bmod 3,$$

$$a_1a_3 \equiv a_1^2a_2 + \frac{c_4 - a_1^4}{8} \bmod 2,$$

and moreover, if $a_1 \equiv 0 \bmod 2$, then $c_6 \equiv 0 \bmod 8$ and

$$a_3^2 \equiv \frac{c_6}{8} \bmod 4.$$

We call an integral Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for E over K of *restricted type*, if

$$a_1, a_3 \in \left\{ \sum_{i=1}^{n} \alpha_i\omega_i \mid \alpha_i = 0 \text{ or } 1 \right\}, \qquad a_2 \in \left\{ \sum_{i=1}^{n} \alpha_i\omega_i \mid \alpha_i = -1, 0 \text{ or } 1 \right\}.$$

Let $\mathfrak{M}$ be the set of all global minimal equations of restricted type for E over K. Then $\mathfrak{M} \neq \emptyset$, and we have an action of $\mathfrak{O}^*$ on $\mathfrak{M}$, where $\mathfrak{O}^*$ denotes the group of units in $\mathfrak{O}$. Indeed, take any global minimal equation for E over K and make a transformation with $u = 1$ and suitable choice of $r, s, t \in \mathfrak{O}$, successively; this yields $\mathfrak{M} \neq \emptyset$. The action of $\mathfrak{O}^*$ is defined as follows. For $u \in \mathfrak{O}^*$ and an equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in $\mathfrak{M}$ we define an equation $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ in the following way: Let

$$a_1', a_3' \in \left\{ \sum_{i=1}^{n} \alpha_i\omega_i \mid \alpha_i = 0 \text{ or } 1 \right\}, \qquad a_2' \in \left\{ \sum_{i=1}^{n} \alpha_i\omega_i \mid \alpha_i = -1, 0 \text{ or } 1 \right\}$$

be such that

$$ua_1 = a_1' + 2s, \quad u^2a_2 = a_2' - sa_1' + 3r - s^2, \quad u^3a_3 = a_3' + ra_1' + 2t,$$

with $s, r, t \in \mathfrak{O}$. Finally define a_4' and a_6' by the equations

$$a_4' = u^4a_4 + sa_3' - 2ra_2' + (t + rs)a_1' - 3r^2 + 2st,$$
$$a_6' = u^6a_6 - ra_4' - r^2a_2' - r^3 + ta_3' + rta_1' + t^2.$$

Then $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ is an equation in $\mathfrak{M}$ and moreover, an action of $\mathfrak{O}^*$ on $\mathfrak{M}$ is defined in this way. If $K = \mathbf{Q}$, then $\mathfrak{M}$ contains exactly one element. It follows from the action of $\mathfrak{O}^*$ on $\mathfrak{M}$ that if $x, y \in \mathfrak{O}$ are the quantities c_4, c_6, respectively, of an equation in $\mathfrak{M}$, then the same holds for u^4x, u^6y, where $u \in \mathfrak{O}^*$ is arbitrary.

Now let

$$(*) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be any given Weierstrass equation for E over K with $a_i \in \mathfrak{O}$ and with discriminant Δ. In the second chapter we describe an algorithm which leads from equation (*) to a global minimal equation of restricted type for E. The correctness of the algorithm follows from well-known general principles and the facts mentioned above. In particular concerning step (2) of the algorithm it is sufficient to consider the numbers $u \in \mathfrak{O}$ up to associates. In the third section we describe an optimized algorithm for the case $K = \mathbf{Q}$. This variation of the general algorithm was suggested by Joe Silverman, who saw a preprint of the original version of this paper. I am grateful to Silverman for his careful reading of the original version and for his suggested modifications.

2. The Algorithm.

(1) Compute the quantities c_4 and c_6 for the given equation (*):

$$c_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4),$$
$$c_6 = -(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(a_1a_3 + 2a_4) - 216(a_3^2 + 4a_6).$$

(2) Determine a complete set S of pairwise nonassociated numbers $u \in \mathfrak{O}$ satisfying the following conditions: There exists $x_u, y_u \in \mathfrak{O}$ such that

$$u^4x_u = c_4, \qquad u^6y_u = c_6.$$

(S is clearly finite.)

(3) Choose $u \in S$.

(4) Choose $a_1', a_3' \in \{\sum_{i=1}^n \alpha_i\omega_i \mid \alpha_i = 0 \text{ or } 1\}$, $a_2' \in \{\sum_{i=1}^n \alpha_i\omega_i \mid \alpha_i = -1, 0 \text{ or } 1\}$ subject to the following conditions:

$$a_1'^4 \equiv x_u \bmod 8, \qquad a_2'^3 \equiv -a_1'^6 - y_u \bmod 3,$$

and additionally in the case $a_1' = 0$:

$$y_u \equiv 0 \bmod 8 \quad \text{and} \quad a_3'^2 \equiv \frac{y_u}{8} \bmod 4,$$

in the case $a_1' = 1$:

$$a_3' \equiv a_2' + \frac{x_u - 1}{8} \bmod 2.$$

(5) Solve the following equations for a_4' and a_6' successively:

$$x_u = (a_1'^2 + 4a_2')^2 - 24(a_1'a_3' + 2a_4'),$$
$$y_u = -(a_1'^2 + 4a_2')^3 + 36(a_1'^2 + 4a_2')(a_1'a_3' + 2a_4') - 216(a_3'^2 + 4a_6').$$

If a_4' or a_6' is not in $\mathfrak{O}$, then continue with (8); otherwise continue with (6). (We have $x_u = c_4'$ and $y_u = c_6'$, where c_4' and c_6' come from the integral Weierstrass equation, denoted by $\Gamma_{u,a_1',a_2',a_3'}$, given by the coefficients $a_1', a_2', a_3', a_4', a_6'$. $\Gamma_{u,a_1',a_2',a_3'}$ has discriminant $u^{-12}\Delta$. We test now whether $\Gamma_{u,a_1',a_2',a_3'}$ is an equation for E.)

(6) Solve the following equations for s, r, t successively:

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2, \quad u^3a_3' = a_3 + ra_1 + 2t.$$

If the values for s, r, t are not in $\mathfrak{O}$, then continue with (8); otherwise continue as follows.

If the values for s, r, t are not related by the equations

$$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$

$$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,$$

then continue with (8); otherwise continue with (7). ($\Gamma_{u,a_1',a_2',a_3'}$ is an equation for E.)

(7) Store the equation $\Gamma_{u,a_1',a_2',a_3'}$ and its discriminant, provided the store is empty. Then continue with (9). If the store is not empty, then continue as follows.

Compare the discriminant of the equation in the store with the discriminant of $\Gamma_{u,a_1',a_2',a_3'}$: If the discriminant of the equation in the store divides the discriminant of $\Gamma_{u,a_1',a_2',a_3'}$, then continue with (9); otherwise continue as follows.

Store the equation $\Gamma_{u,a_1',a_2',a_3'}$ and its discriminant, and cancel the old equation and its discriminant. Then continue with (9).

(8) If all possible a_1', $a_3' \in \{\sum_{i=1}^n \alpha_i\omega_i \mid \alpha_i = 0 \text{ or } 1\}$, $a_2' \in \{\sum_{i=1}^n \alpha_i\omega_i \mid \alpha_i = -1, 0 \text{ or } 1\}$ subject to the conditions have already been chosen, then continue with (9); otherwise choose new a_1', a_2', a_3' and return to (5).

(9) If all possible $u \in S$ have already been chosen, then continue with (10); otherwise choose a new $u \in S$ and return to (4).

(10) Look at the store. (It is not empty and contains a global minimal equation of restricted type for E.)

3. The Optimized Algorithm for $K = \mathbf{Q}$.

(2′) Determine $u_{\max}$, the largest integer u satisfying the conditions of step (2).

Factor $u_{\max} = 2^{e_2}3^{e_3}v$ with v prime to 6.

(From general principles we know that

(i) if we choose $u = v$ in step (3), then we will get a successful test in step (6) for some choice of a_1', a_2', a_3' in step (4);

(ii) if $u = u_1$ and $u = u_2$ in step (3) both give a successful test in step (6) and u_1, u_2 are relatively prime, then $u = u_1u_2$ will also test successfully in step (6).

Thus the general procedure is as follows.)

(3′) Determine the largest integer f_2 satisfying $0 \leqslant f_2 \leqslant e_2$ so that $u = 2^{f_2}$ in step (3) tests successfully in step (6) for some choice of a_1', a_2', a_3' in step (4).

(3″) Determine the largest integer f_3 satisfying $0 \leqslant f_3 \leqslant e_3$ so that $u = 3^{f_3}$ in step (3) tests successfully in step (6) for some choice of a_1', a_2', a_3' in step (4).

(3‴) Choose $u = 2^{f_2}3^{f_3}v$ in step (3). (The test in step (6) is guaranteed to be successful, and the a_1', a_2', a_3', a_4', a_6' found will be the desired global minimal equation of restricted type for E.)

Sonderforschungsbereich
"Theoretische Mathematik"
Beringstrasse 4
5300 Bonn, West Germany

1. J. T. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 179–206.

2. J. T. TATE, "Algorithm for determining the type of singular fiber in an elliptic pencil," *Modular Functions of One Variable*. IV, Lecture Notes in Math., Vol. 476, Springer-Verlag, Berlin and New York, 1975.