Canonical Minimal Models of Elliptic Curves Over Number Fields

Alyson Deines and Andrew Ohana

Let K be a number field with ring of integers $\mathcal{O}_K$ and unit group U_K. Let U_K^{12} denote all twelfth powers of units. For $n \in \mathcal{O}_K^{\times}$ and $m \in \mathcal{O}_K$ let $A_n(m)$ denote fixed representation of m mod $n\mathcal{O}_K$. We say $m \in \mathcal{O}_K$ is **restricted mod** n if $A_n(m) = m$.

Now let E be an elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_1, \cdots, a_6 \in \mathcal{O}_K$. This form is known as Weierstrass form. If τ is an isomorphism $\tau : E \to E'$, we will refer to all invariants of E' as $a_1', \cdots, a_6'$, c_4', c_6', Δ', etc.

We say E is of **restricted type** if a_1, a_3 are restricted mod 2 and a_2 is restricted mod 3. From Connell's Handbook for Elliptic Curves, Proposition 5.2.4, there exists a unique $\mathcal{O}_K$-isomorphism of the form $\tau = [r, s, t, 1]$ such that $E' = \tau E$ is of restricted type.

What we will prove is that given a deterministic way to choose a residue class of U_K/U_K^{12} and given an isomorphism class of elliptic curves and an ideal (Δ) generated by the discriminant Δ of one of the curves in this isomorphism class, we can define and compute a unique representative of this isomorphism class that has discriminant generating the ideal (Δ). Further, $\mathcal{O}_K$ is a PID then we can choose a unique representative for any isomorphism class of elliptic curves.

For this it will be useful to introduce a function $f : \mathcal{O}_K\backslash\{0\} \to \mathcal{O}_K\backslash\{0\}$ such that $f(x)/x \in U_K^{12}$ and if $y/x \in U_K^{12}$ then $f(x) = f(y)$. This function represents our deterministic way to choose a residue class of U_K/U_K^{12} as there is no canonical way. For example, if $K = \mathbf{Q}(\sqrt{5})$ and $a = \frac{1+\sqrt{5}}{2}$, then $U_K = \langle -1\rangle \times \langle a\rangle$ and $U_K^{12} = \langle a^{12}\rangle$. So we can fix f to take units to their residue in U_K/U_K^{12} by the map

$$f((-1)^n a^m) = (-1)^n a^{\overline{m}}$$

where $\overline{m}$ is m reduced modulo 12. Notice that even with $\mathbf{Q}(\sqrt{5})$ we had to make a choice of basis. We could have easily worked with $a^{-1} = \overline{a} = \frac{1-\sqrt{5}}{2}$ instead as this also generates $\langle a \rangle$.

There are several ideas about how to choose f. One idea is to just use whatever basis Pari returns. (What algorithm does this use?) Another idea is possibly using heights in a clever way. Both need to be looked into further.

Lemma 1. *Let E be an elliptic curve in Weierstrass form as above. Then there exists an isomorphism $\tau : E \to E'$ such that $\Delta' = f(\Delta)$ and Δ' is a fixed point of f.*

Proof. As $f(\Delta)/\Delta \in U_K^{12}$ there is a unit u such that $u^{12} f(\Delta) = \Delta$, so if we apply the transformation $[0, 0, 0, u]$ we get a new Weierstrass equation $y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6'$ where $u^i a_i' = a_i$ with discriminant such that $\Delta = u^{12}\Delta'$. Additionally note that Δ' is a fixed point of f since $\Delta'/\Delta = f(\Delta)/\Delta \in U_K^{12}$, so $f(\Delta') = f(\Delta) = \Delta'$. □

Theorem 1. *Let K be a number field with only the trivial 12-th roots of unity. Let E be an elliptic curve over K with Weierstrass model as above. Then E has a unique restricted Weierstrass model depending only on Δ and f.*

Proof. By the previous lemma, we can assume E has discriminant $\Delta = f(\Delta)$.

To show uniqueness, suppose that E and E' are isomorphic elliptic curves with discriminants Δ, Δ' respectively, such that $f(\Delta) = \Delta = \Delta' = f(\Delta')$, and restricted models:

$$\begin{aligned} E &: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \\ E' &: y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \end{aligned}$$

Let $\tau = [r, s, t, u]$ be an isomorphism $\tau : E \to E'$.

Then:

$$u b_1 = a_1 + 2s \tag{1}$$
$$u^2 b_2 = a_2 - s a_1 + 3r - s^2 \tag{2}$$
$$u^3 b_3 = a_3 + r a_1 + 2t \tag{3}$$
$$u^4 b_4 = a_4 - s a_3 + 2r a_2 - (t + rs) a_1 + 3r^2 - 2st \tag{4}$$
$$u^6 b_6 = a_6 + r a_4 + r^2 a_2 + r^3 - t a_3 - t^2 - r t a_1 \tag{5}$$

Since τ is an isomorphism of E preserving Δ, $\Delta = u^{12}\Delta' = \Delta'$. As the only 12-th roots of unity are square roots of unity, $u = \pm 1$.

$u = 1$. Considering (1), $b_1 = A_2(b_1) = A_2(a_1) = a_1$, so $s = 0$. Similarly, $r = 0$ and $t = 0$ so $\tau = [0, 0, 0, 1]$ is the identity transformation. Thus E and E' are the same global minimal models.

$u = -1$. Rearranging (1), $a_1 + b_1 = -2s$. As $a_1 = A_2(a_1)$ and $b_1 = A_2(b_1)$, $a_1 = b_1$ and so $s = -a_1$. Plugging this into (2), $b_2 = a_2 + 3r$. As b_2 and a_2 are 3-restricted, we can use the same argument to show $r = 0$. Similarly, we have that $t = -a_3 = -b_3$. From here it is trivial to verify that this transformation gives $b_4 = a_4$ and $b_6 = a_6$ we know r, s, t and u.

□

Example: Let E be the elliptic curve

$$y^2+(2a-2)\,xy+(-88a+144)\,y = x^3+(-4a+8)\,x^2+(-800a+1296)\,x+(-31168a+50432)\,.$$

Then E has discriminant

$$1118330236928a-1809496334336 = (-28657a+46368)\cdot(-4a+3)\cdot 2^{12}\cdot(a-7)\cdot(25a+244),$$

and $-28657a + 46368 = (-1)a^{-23}$. Using the above transformation, E'

$$y^2 = x^3 + (-a-1)\,x^2 + (16a+40)\,x + (-32a+204)$$

is an isomorphic curve which is of restricted type and has discriminant

$$-4968448a - 27189248 = (-a)\cdot(-4a+3)\cdot 2^{12}\cdot(a-7)\cdot(25a+244).$$

Notice that restricted type does not make any statements about minimality.

In many cases, such as when K has class number 1, an isomorphism class of elliptic curves has global minimal models, i.e.,Weierstrass models with a smallest possible discriminant keeping integral coefficients. Any two curves in an isomorphism class in global minimal Weierstrass form have discriminants which generate the same ideal. Thus by choosing a function f which gives a deterministic way to pick representatives of U_K/U_K^{12}, we have fixed both f and Δ for the entire isomorphism class of curves. Since the isomorphism used for finding restricted models preserves integrality, we have the following theorem:

Theorem 2. *Let K be a number field with only the trivial 12-th roots of unity. If $\mathcal{E}$ is an isomorphism class of elliptic curves and has global minimal models, then by fixing representatives in the residue classes of U_K/U_K^{12} we can define and compute unique restricted global minimal models, i.e. we can define and compute a unique representative for $\mathcal{E}$.*

Example: Let E be as above. Then E has global minimal model E'':

$$y^2 + (a+1)\,xy = x^3 + (a-1)\,x^2 + (-39a+65)\,x + (-491a+795)$$

with discriminant

$$273029843a - 441771566 = (-28657a + 46368) \cdot (-4a + 3) \cdot (a - 7) \cdot (25a + 244).$$

If we then find the restricted model of E'', we will have the unique representative of this isomorphism class E_u:

$$y^2 + axy + ay = x^3 + (a + 1)\, x^2 + (2a + 3)\, x + (2a + 5)$$

with discriminant

$$-1213a - 6638 = (-a) \cdot (-4a + 3) \cdot (a - 7) \cdot (25a + 244).$$