J. Normal forms, discriminant and j-invariant

Applications of elliptic curves that rely upon the difficulty of the discrete logarithm problem use equations with as little parameters as possible for the sake of efficiency when computing the group operation. The related cryptosystems have shorter keys than similar cryptosystems that are based on the difficulty of number factorization because the latter problem problem is easier to solve than the former problem. The reason is the existence of the number field sieve. No similar algorithm is known for elliptic curves. If the parameters of an elliptic curve are well chosen, then there seem to be no other attacks on mathematical principles of the problem but those that correspond to general (black box) attacks on the DLP. Of course, quantum computers may change the landscape completely, and dramatically, in particular if they will be widely available.

In the world of postquantum cryptography various concepts arise, and some of them use elliptic curves in a completely different way. This requires concepts that are different than the DLP.

As an example how the focus may change let us mention that in the advent of elliptic curve cryptography curves in characteristic two were considered as an attractive alternative to curves over primes since at that time no efficient methods solving the DLP in small characteristics were known.

Normal forms, discriminant and j-invariant are used in such discussions freely. They are considered as something that is well known and does not need an explanation. The purpose of this section is to provide such an explanation for the case of Weierstraß equations.

J.1. **Normal forms.** Recall that a Weierstraß curve is given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{J.1}$$

We assume that the coefficients a_i belong to a field K, and say that two Weierstraß equations are *linearly K-equivalent*, if there exists an invertible linear substitution over K that turns one such equation into a multiple of the other equation. For the sake of brevity the term "linearly K-equivalent" is shortened to "K-equivalent."

Let us first consider a somewhat weaker notion, in which only those substitutions are considered that turn an equation into an equation in a way that never allows for a possibility of a nontrivial multiple. Such substitutions necessarily have the form of $y \mapsto y + sx + t$ and $x \mapsto x + r$. Indeed, the substitution for x may not include y with a nonzero coefficient since in a Weierstraß equation the unknown y does not occur in the third power. Note that the substitution is invertible for any choice of $r, s, t \in K$.

These substitutions turn (J.1) into

$$(y+sx+t)^2+a_1(x+r)(y+sx+t)+a_3(y+sx+t) = (x+r)^3+a_2(x+r)^2+a_4(x+r)+a_6,$$

and that can be expressed as

$$\begin{aligned} y^2 + (2s+a_1)xy + (2t+a_1r+a_3)y = \\ x^3 + (3r+a_2-s^2-a_1s)x^2 + (3r^2+2a_2r+a_4-2st-a_1rs-a_1t-a_3s)x \\ + (r^3+a_2r^2+a_4r+a_6-t^2-a_1rt-a_3t). \end{aligned} \tag{J.2}$$

If $\mathrm{char}(K) \neq 2, 3$, then there exists exactly one triple $(r, s, t) \in K^3$ such that

$$\begin{aligned} 2s + a_1 = 0. \\ 3r + a_2 - s^2 - a_1s = 0, \text{ and} \\ 2t + a_1r + a_3 = 0. \end{aligned} \tag{J.3}$$

In other words, there exists exactly one triple $(r,s,t) \in K^3$ that transforms (J.1) into an equation $y^2 = x^3 + ax + b$.

If $\mathrm{char}(K) = 3$, then (J.2) takes the form

$$y^2 + (a_1{-}s)xy + (a_1r{+}a_3{-}t)y = \\ x^3 + (a_2{-}s^2{-}a_1s)x^2 + (a_4{-}a_2r{+}st{-}a_1rs{-}a_1t{-}a_3s)x \\ + (r^3{+}a_2r^2{+}a_4r{+}a_6{-}t^2{-}a_1rt{-}a_3t).$$

Setting $s = a_1$ yields $a_2 - s^2 - a_1s = a_2 + a_1^2$. The equations in which $a_2 + a_1^2 = 0$ are termed *supersingular*. By setting $s = a_1$ and $t = a_1r + a_3$ they are transformed into

$$y^2 = x^3 + (a_4 - a_3a_1)x + (r^3 + (a_4{-}a_3a_1)r + (a_3^2{+}a_6)).$$

A supersingular curve in characteristic three may thus attain the form $y^2 = x^3 + ax + b$, but with a much bigger degree of freedom in the choice of b. Obviously, if K is algebraically closed, then r may be chosen in such a way that b vanishes.

If $\mathrm{char}(K) = 3$ and $a_2 + a_1^2 \neq 0$, the choice of $s = a_1$ and $t = a_1r + a_3$ produces

$$y^2 = x^3 + (a_2{+}a_1^2)x^2 + (a_4{-}a_1a_3{-}(a_2{+}a_1^2)r)x \\ + (r^3{+}a_2r^2{+}a_4r{+}a_6{+}a_1^2r^2{+}a_3^2{-}a_1a_3r).$$

In the nonsupersingular case there is thus only one choice of $(r,s,t) \in K^3$ that transforms (J.1) into a form $y^2 = x^3 + ax^2 + b$, and in that case $a = a_2 + a_1^2$.

Suppose now that $\mathrm{char}(K) = 2$. Then (J.1) attains the form

$$y^2 + a_1xy + (a_1r{+}a_3)y = x^3 + (r{+}a_2{+}s^2{+}a_1s)x^2 \\ + (r^2{+}a_4{+}a_1rs{+}a_1t{+}a_3s)x + (r^3{+}a_2r^2{+}a_4r{+}a_6{+}t^2{+}a_1rt{+}a_3t).$$

A *supersingular* curve is obtained when $a_1 = 0$. In such a case the choice $r = a_2{+}s^2$ yields

$$y^2 + a_3y = x^3 + (s^4{+}a_3s{+}a_2^2{+}a_4)x + (s^6{+}(a_2^2{+}a_4)s^2{+}t^2{+}a_3t{+}a_4a_2{+}a_6).$$

If K is algebraically closed, then s and t may be chosen in such a way that the equation is K-equivalent to $y^2 + a_3y = x^3$.

If $a_1 \neq 0$, then t and r may be chosen in such a way that there exists a $c \in K$ such that the equation is K-equivalent to

$$y^2 + a_1xy = x^3 + (a_3a_1^{-1}{+}a_2{+}s^2{+}a_1s)x^2 + c.$$

If K is algebraically closed, then s may be chosen in such a way that the form $y^2 + a_1xy = x^3 + c$ is attained.

To sum up, for every Weierstraß equation there exist substitutions $x \mapsto x + r$ and $y \mapsto y + sx + t$ such that exactly one of the following forms is attained:

$$y^2 = x^3 + a_4x + a_6, \text{ if } \mathrm{char}(K) \neq 2, 3,$$
$$y^2 = x^3 + a_4x + a_6, \text{ where } \mathrm{char}(K) = 3,$$
$$y^2 = x^3 + a_2x^2 + a_6, \text{ where } \mathrm{char}(K) = 3 \text{ and } a_2 \neq 0,$$
$$y^2 + a_3y = x^3 + a_4x + a_6, \text{ where } \mathrm{char}(K) = 2, \text{ and}$$
$$y^2 + a_1xy = x^3 + a_2x^2 + a_6, \text{ where } \mathrm{char}(K) = 2 \text{ and } a \neq 0.$$

If $\mathrm{char}(K) = 2$, then in the nonsupersingular case the coefficients a_2 and a_6 are not determined uniquely and can be expressed by polynomials in one parameter, while in the supersingular case the coefficients a_4 and a_6 polynomially depend on two parameters. Similarly, the coefficient a_6 is polynomially dependent in the supersingular case of characteristic three.

To determine if two Weierstraß equations are K-equivalent it is possible to proceed in two stages, firstly applying the substitutions $x \mapsto x + r$ and $y \mapsto y + sx + t$ described above, and then substitutions $x \mapsto u^{-2}x$ and $y \mapsto u^{-3}y$. If the first stage produces an equation that is determined uniquely (as if $\mathrm{char}(K) \neq 2, 3$), then the second stage can be used straightforwardly to decide if the equations are K-equivalent or not. However, if the first stage produces equations with coefficients that may be parameterized, then all possible values of these parameters have to be taken into account when deciding the K-equivalence.

If the substitutions $x \mapsto u^{-2}x$ and $y \mapsto u^{-3}y$ are applied to $y^2 = x^3 + a_4x + a_6$, then we get $u^{-6}y^2 = u^{-6}x^3 + a_4u^{-2}x + a_6$, and that is

$$y^2 = x^3 + u^4a_4x + u^6a_6. \tag{J.4}$$

In the remaining three cases we obtain

$$\begin{aligned} y^2 &= x^3 + u^2a_2x^2 + u^6a_6, \text{ where } \mathrm{char}(K) = 3, \\ y^2 + a_3u^3y &= x^3 + u^4a_4x + u^6a_6, \text{ where } \mathrm{char}(K) = 2, \text{ and} \\ y^2 + a_1uxy &= x^3 + u^2a_2x^2 + u^6a_6, \text{ where } \mathrm{char}(K) = 2 \text{ as well.} \end{aligned}$$

If $\mathrm{char}(K) = 2$, then u is chosen so that $u^4a_4 = 1$ and $u = a_1^{-1}$, respectively. The former choice is possible if K is perfect, which is usually assumed.

Standardly there are considered five normal forms:

(SH1) $y^2 = x^3 + a_4x + a_6$ and $\mathrm{char}(K) \notin \{2, 3\}$;
(SH2a) $y^2 + xy = x^3 + a_2x^2 + a_6$ and $\mathrm{char}(K) = 2$;
(SH2b) $y^2 + a_3y = x^3 + a_4x + a_6$ and $\mathrm{char}(K) = 2$;
(SH3a) $y^2 = x^3 + a_2x^2 + a_6$, $a_2 \neq 0$ and $\mathrm{char}(K) = 3$; and
(SH3b) $y^2 = x^3 + a_4x + a_6$ and $\mathrm{char}(K) = 3$.

Only (SH2a) uses a nontrivial application of u, setting $u = a_1^{-1}$. If K is algebraically closed, then there exists a choice of u and of the other parameters such that the equation is transformed to one of the following forms:

(SH1) $y^2 = x^3 + x + a_6$ or $y^2 = x^3 + 1$ or $y^2 = x^3$;
(SH2a) $y^2 + xy = x^3 + x^2 + a_6$;
(SH2b) $y^2 + y = x^3$ or $y^2 = x^3$;
(SH3a) $y^2 = x^3 + x^2 + a_6$; and
(SH3b) $y^2 = x^3 + x$ or $y^2 = x^3$.

The above equations are determined uniquely, with the exception of varying the sign of a_6 in (SH1), and replacing a_6 by ηa_6, $\eta^3 = 1$, in (SH3a). Note that to get one of these forms only a finite degree extension of K is necessary since what we need is a split field for one or two polynomials over K.

There is another way how to decide whether two Weierstraß equations are $\bar{K}$-equivalent. If they are nonsingular (smooth), then this is true if and only if the have the same j-invariant. To define j-invariant we first need to define the discriminant.

J.2. **Discriminant.** The discriminant $D(a)$ of a polynomial $= \sum a_ix^i \in K[x]$ is often used just for the purpose of deciding whether a has or does not have multiple roots. Indeed, $D(a) = 0$ if and only if a posseses a multiple root, as implied by the following well known result:

Proposition J.1. *Assume that $a = \sum a_ix^i \in K[x]$, $n = \deg(a) \geq 1$. Then $D(a) = 0$ if and only if a possesses a multiple root. If $\alpha_1, \ldots, \alpha_n$ are the roots of a, then*

$$D(a) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

However, this formula should not be considered as the definition of $D(a)$ since it refers to roots, not coefficients. The definition is based upon the more general notion of resultant, and can be presented in this way:

The *discriminant* $D(a)$ of a polynomial $a = \sum a_i x^i \in K[x]$, $n = \deg(a) \geq 1$, is equal

$$(-1)^{\binom{n}{2}} a_n^{-1} \det(R(a, a'), \text{ where}$$

$$R(a,a') = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & na_n & (n-1)a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2a_2 & a_1 & 0 \\ 0 & 0 & 0 & \cdots & 3a_3 & 2a_2 & a_1 \end{pmatrix}$$

The discriminant of a cubic polynomial is thus given by

$$D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2 \qquad \text{(J.5)}$$

since

$$-a^{-1}\begin{vmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{vmatrix} = -a^{-1}\begin{vmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 0 & b & 2c & 3d & 0 \\ 0 & 0 & b & 2c & 3d \\ 0 & 0 & 3a & 2b & c \end{vmatrix}$$

$$= -a^{-1}\begin{vmatrix} a & b & c & d \\ ab & 2ca & 3da & 0 \\ 0 & b & 2c & 3d \\ 0 & 3a & 2b & c \end{vmatrix} = -\begin{vmatrix} 2ca - b^2 & 3da - cb & -db \\ b & 2c & 3d \\ 3a & 2b & c \end{vmatrix}$$

$$= -\begin{vmatrix} 2ca & 3da + cb & 2db \\ b & 2c & 3d \\ 3a & 2b & c \end{vmatrix} = \begin{array}{l} -4ac^3 - 27d^2a^2 - 9abcd - 4db^3 \\ \quad +12abcd + 3abcd + c^2b^2 + 12abcd. \end{array}$$

Suppose now that the Weierstraß equation is given by $y^2 = f(x)$, where $f(x) = x^3 + a_2x^2 + a_4x + a_6$. By (J.5),

$$D(f) = a_2^2a_4^2 - 4a_4^3 - 4a_2^3a_6 + 18a_2a_4a_6 - 27a_6^2.$$

For reasons that will become apparent later, define b_2, b_4 and b_6 so that $f(x) = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Thus $b_2 = 4a_2$, $b_4 = 2a_4$ and $b_6 = 4a_6$.

Obviously,

$$16D(f) = -8b_4^3 + 9b_2b_4b_6 - 27b_6^2 + b_2^2(b_4^2 - b_2b_6)/4. \qquad \text{(J.6)}$$

The transformation of (J.3) cannot be used when $\mathrm{char}(K) = 3$. However, the standard completion of a quadratic equation to square works for any characteristic different from two. This means to set $s = -a_1/2$, $t = -a_3/2$ and $r = 0$. With these values the equation (J.3) turns into

$$y^2 = x^3 + (a_2 + a_1^2/4)x^2 + (a_4 + a_1a_3/2)x + (a_6 + a_3^2/4).$$

Define now b_2, b_4 and b_6 for any Weierstraß equation given by (J.1) in such a way that the above equation gets the form $y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Thus

$$b_2 = 4a_2 + a_1^2, \quad b_4 = 2a_4 + a_1a_3 \quad \text{and} \quad b_6 = 4a_6 + a_3^2. \tag{J.7}$$

Define one more quantity, and that is b_8, by

$$b_8 = 4a_2a_6 + a_2a_3^2 + a_1^2a_6 - a_4^2 - a_1a_3a_4. \tag{J.8}$$

If $\operatorname{char}(K) \neq 2$, then

$$\frac{b_2b_6 - b_4^2}{4} = \frac{(4a_2 + a_1^2)(4a_6 + a_3^2) - (2a_4 + a_1a_3)^2}{4} = 4a_2a_6 + a_2a_3^2 + a_1^2a_6 - a_4^2 - a_1a_3a_4 = b_8.$$

For a Weierstraß curve C given by (J.1) define the *discriminant* by

$$\Delta(C) = -8b_4^3 + 9b_2b_4b_6 - 27b_6^2 - b_2^2b_8.$$

Comparing this definition with (J.6) shows that $\Delta(C) = 16D(f)$ if $\operatorname{char}(K) \neq 2$ and C is given by $y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$.

Theorem J.2. *Let C be a Weierstraß curve given by equation (J.1). Then $\Delta(C) = 0$ if and only if C is singular.*

If $\tilde{C}$ is given by an equation obtained via transformations $x \mapsto x + r$ and $y \mapsto y + sx + t$, then $\Delta(\tilde{C}) = \Delta(C)$.

If $\tilde{C}$ is given by an equation obtained via transformations $x \mapsto u^{-2}x$ and $y \mapsto u^{-3}y$, then $\Delta(\tilde{C}) = u^{12}\Delta(C)$.

This theorem may be proved by a direct verification. However, the polynomials that have to be compared are very long. There exists a short proof that relies upon the properties of the polynomial discriminants, upon the connection (J.6), and upon the fact that in both (J.7) and (J.8) there appears no fraction. The latter may be used for an argument that transfers the validity of the theorem in characteristic zero to a positive characteristic via factorization.

The definition of the discriminant together with (J.7) and (J.8) can be used to compute the discriminant value for the normal forms:

type	b_2	b_4	b_6	b_8	$\Delta(C)$
SH1	0	$2a_4$	$4a_6$	$-a_4^2$	$-64a_4^3 - 432a_6^2 = -8b_4^3 - 27b_6^2$
SH2a	1	0	0	a_6	$a_6 = b_8$
SH2b	0	0	a_3^2	a_4^2	$a_3^4 = b_6^2$
SH3a	a_2	0	a_6	a_2a_6	$-a_2^3a_6 = -b_2^2b_8$
SH3b	0	$-a_4$	a_6	$-a_4^2$	$-a_4^3 = -b_4^3$

J.3. **The j-invariant.** Substitutions $x \mapsto x + r$ and $y \mapsto y + sx + t$ do not change the value of b_{2i}, $1 \leq i \leq 4$. On the other hand the substitutions $x \mapsto u^{-2}x$ and $y \mapsto u^{-3}y$ change b_{2i} to $u^{2i}b_{2i}$. Because of that they also change c_4 to u^4c_4 and u_6 to u^6c_6 if

$$c_4 = b_2^2 - 24b_4 \text{ and } c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Let C be a Weierstraß curve given by (J.1). Suppose that C is nonsingular, i.e. that $\Delta(C) \neq 0$. The j-invariant of C is defined by

$$j(C) = \frac{c_4^3}{\Delta(C)}.$$

From Theorem J.2 it follows that it C and $\tilde{C}$ are K-equivalent, then $j(C) = j(\tilde{C})$. Furthermore,

$$j(C) = j(\tilde{C}) \quad \Longleftrightarrow \quad C \text{ and } \tilde{C} \text{ are } \bar{K}\text{-equivalent.}$$

The value of the j-invariant for the normal forms is as follows:

type	c_4	c_6	$j(C)$
SH1	$-48a_4$	$-864a_6$	$6912a_4^3/(4a_4^3+27a_6^2) = c_4^3/(c_4^3-c_6^2)$
SH2a	1	1	$1/a_6$
SH2b	0	0	0
SH3a	a_2^2	$-a_2^3$	$-a_2^3/a_6$
SH3b	0	0	0

Let the curve C be defined over a field of characteristic $p > 0$. The curve is said to be *supersingular* if $C[p] = \mathcal{O}$ (i.e., the group of C contains no element of order p). Note that supersingular curves are nonsingular, by definition. If $p \in \{2, 3\}$, then C is supersingular if and only if $j(C) = 0$.

Two smooth Weierstraß curves are birationally equivalent over K if and only if they are given by K-equivalent Weierstraß equations. Since any elliptic curve E is birationally equivalent to a Weierstraß curve, the j-invariant of E is well defined too. In fact, $j(E)$ is an invariant of the function field $\bar{K}(E)$.