How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form

Problem Overview:

We are given a cubic curve and we want to put a group structure to the set of points on the curve. In order to make the group operation as simple as possible, we will use a point at infinity (counted as a rational point on the curve in $\mathbb{A}^2 \cup \mathbb{P}^1$) as the zero element of the group. Thus, it is necessary that the curve contains exactly one point at infinity.

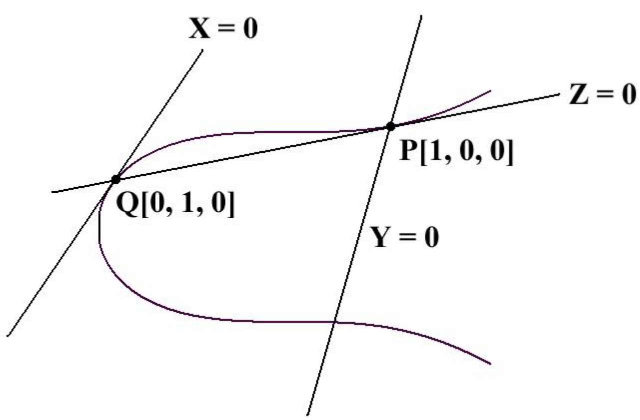
Viewing the curve in $\mathbb{P}^2$, what this means is that the line $Z = 0$ intersects the curve exactly once (as opposed to three times in the general case). In order to do this, we perform a change of coordinates in $\mathbb{P}^2$ that gives a one-to-one correspondence between the rational points of the curve in both coordinate systems.

Process:

Suppose we have a cubic curve $f(u, v) = 0$. Suppose further that we are given a rational point P on this curve, when viewed in the projective plane. We transform this curve to the desired form as follows.

1. Write it in homogeneous form $C : F(U, V, W) = 0$.

2. Find the tangent line to C at point P. This will be the axis $Z = 0$ in the new coordinate system.



3. Let point Q be the intersection of the curve C with the line $Z = 0$. Take the axis $X = 0$ to be the tangent line to C at point Q. Thus, in the new coordinate system, Q has coordinates $[0, 1, 0]$.

4. Finally, choose the axis $Y = 0$ to be any line (other than $Z = 0$) passing through point P. Thus, P has coordinates $[1, 0, 0]$ in this new coordinate system.

5. Upon this coordinate transformation in $\mathbb{P}^2$ (also called *projective transformation*), our curve has the form $C' : F'(X, Y, Z) = 0$. And C' contains the points $P[1, 0, 0]$ and $Q[0, 1, 0]$.

   Since F' is a homogeneous polynomial of degree 3, it has the form

   $$F'(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eZ \cdot G(X, Y, Z)$$

   where G is a homogeneous polynomial of degree 2. We will now show that a, b, and d must equal 0.

(a) Since $P[1,0,0] \in C'$, we see that $F'(1,0,0) = a = 0$.

(b) Since $Q[0,1,0] \in C'$, we see that $F'(0,1,0) = d = 0$.

(c) Consider the intersection of the curve C' with the line $Z = 0$. The intersection consists of point P (twice) and point Q, and is given by the roots of the equation $F'(X,Y,0) = 0$. Since we already know that $a = d = 0$, we get $bX^2Y + cXY^2 = 0$. Upon factoring, we get $XY(bX + cY) = 0$. Each linear factor corresponds to a point of intersection. Thus, point Q satisfies $X = 0$, and point P satisfies both $Y = 0$ and $bX + cY = 0$. So, it follows that $b = 0$.

6. Thus, the polynomial F' (in the new coordinate system) has the form

$$F'(X,Y,Z) = cXY^2 + eZ \cdot G(X,Y,Z)$$

When we dehomogenize the curve with respect to Z, the equation for C' takes the form

$$f(x,y) = xy^2 + ax^2 + bxy + cy^2 + dx + ey + g = 0 \qquad (*)$$

Note that the only term in f with degree 3 is xy^2.

7. Finally, rewrite equation $(*)$ as follows.

$$f(x,y) = (x+c)y^2 + ax^2 + bxy + dx + ey + g = 0$$

Replacing $x + c$ with x, we get the equation of the form

$$xy^2 + (ax+b)y = cx^2 + dx + e$$

Through further change of variables (see Silverman/Tate, p. 23, for details), we obtain an equation in *Weierstrass form*

$$y^2 = x^3 + ax^2 + bx + c$$

This curve (assuming it is non-singular) has exactly one point at infinity where vertical lines meet. Using this point as the zero element of the group is optimal because the elliptic curve is symmetric about the x-axis. So, to find $P + Q$, we simply take $P * Q$ and reflect it about the x-axis.

Example:

As an example, we will transform the cubic curve

$$f(u,v) = u^3 + uv^2 + v^3 + u + v - 2 = 0$$

into Weierstrass normal form.

1. We first homogenize the curve by writing

$$C : F(U,V,W) = U^3 + UV^2 + V^3 + UW^2 + VW^2 - 2W^3 = 0$$

Note that $P[1,0,1]$ is a rational point on the curve.

2. The tangent line to C at point P is given by the equation

$$\frac{\partial F}{\partial U}(P)(U-1) + \frac{\partial F}{\partial V}(P)(V-0) + \frac{\partial F}{\partial W}(P)(W-1) = 0$$

which simplifies to

$$4U + V - 4W = 0 \qquad (*)$$

It is *not* a coincidence that this tangent line is a homogeneous polynomial. We thus set

$$\boxed{Z = 4U + V - 4W}$$

3. Now we find the intersection of the curve C with the line given by $(*)$. Since $(*)$ implies $V = -4(U - W)$, we substitute this into $F(U, V, W) = 0$ to get

$$U^3 + 16U(U - W)^2 - 64(U - W)^3 + UW^2 - 4(U - W)W^2 - 2W^3 = 0 \qquad (**)$$

We know that the intersection consists of three points: point P (twice) and point Q. Therefore $(**)$ should factor into three linear terms two of which are $(U - W)^2$. It does, and $(**)$ can be rewritten as

$$(U - W)^2(-47U + 66W) = 0$$

Thus, point Q has coordinates $Q[66, -76, 47]$. The plane tangent to C at point Q has the equation

$$21053U + 9505V - 14194W = 0$$

Thus we set

$$\boxed{X = 21053U + 9505V - 14194W}$$

4. Since $P[1, 0, 1]$ is on the line $U + V - W = 0$, we let

$$\boxed{Y = U + V - W}$$

Note that the line $Y = 0$ is different from the line $Z = 0$.

5. Thus we have obtained the following (rational) transformation

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 21053 & 9505 & -14194 \\ 1 & 1 & -1 \\ 4 & 1 & -4 \end{bmatrix} \begin{bmatrix} U \\ V \\ W \end{bmatrix}$$

Inverting the transformation matrix, we get

$$\begin{bmatrix} U \\ V \\ W \end{bmatrix} = \begin{bmatrix} \frac{1}{6859} & -\frac{22}{19} & -\frac{1563}{6859} \\ 0 & \frac{4}{3} & -\frac{1}{3} \\ \frac{1}{6859} & -\frac{47}{57} & -\frac{1114}{1985} \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

Substituting these into the original curve $C : F(U, V, W) = 0$, we get a new curve C' with

$$C' : F(X, Y, Z) = XY^2 + aX^2Z + bXYZ + cY^2Z + dXZ^2 + eYZ^2 + gZ^3 = 0$$

where

$$\begin{aligned} a &= 122536011/1774335401915 \\ b &= -1492216408/983011303 \\ c &= -28388/40845345 \\ d &= -226218384460168/704411154560255 \\ e &= 45392975716595356/9756387182275 \\ g &= 6989284338276485910259/20973842127031592625 \end{aligned}$$

6. Finally, we dehomogenize the curve with respect to Z to get

$$f(x, y) = xy^2 + ax^2 + bxy + cy^2 + dx + ey + g = 0$$

Through further change of variables, we obtain a curve in Weierstrass form

$$\boxed{y^2 = x^3 - x^2 - 2x - 32}$$