Weierstrass normal form

Dave Neary

May 2021

1 Weierstrass normal form for cubic equations

Given a general cubic equation

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

we can perform a set of substitutions to convert the equation to a form called Weierstrass normal form:

$$Y^2 = X^3 + AX^2 + BX + C$$

or, equivalently:

$$Y^2 = X^3 + \alpha X + \beta$$

In particular, for the cubic equation C:

$$u^3 + v^3 = \alpha$$

we can use the substitutions

$$x = \frac{12\alpha}{u+v}, y = 36\alpha\frac{u-v}{u+v}$$

to convert this equation to the form C':

$$y^2 = x^3 - 432\alpha$$

This process can be inverted, so from any point $(x, y) \in C'$ we can generate a point $(u, v) \in C$ by the transform:

$$u = \frac{36\alpha + y}{6x}, v = \frac{36\alpha - y}{6x}$$

By this means, if we find rational points on either curve, we can generate a rational point on the other by this bijection.

This transformation might seem like magic, but we can work through this process if we have a rational point on the homogeneous projective form of original curve. To get to this form, we replace $u = \frac{U}{W}, v = \frac{V}{W}$ and multiply across by W^3 to give:

$$U^3 + V^3 - \alpha W^3 = 0$$

The point in $\mathbb{P}^2$ $P = [-1;1;0]$ is on the curve C. Since $W = 0$ this corresponds to a point at infinity - a tangent point of the curve. The tangent at the point P is given by the line:

$$U\frac{\partial C}{\partial U}(P) + V\frac{\partial C}{\partial V}(P) + W\frac{\partial C}{\partial W}(P) = 0$$

$$\frac{\partial C}{\partial V} = 3V^2, \frac{\partial C}{\partial U} = 3U^2, \frac{\partial C}{\partial W} = 3\alpha W^2$$

So at the point $P = [-1;1;0]$ the tangent line in $\mathbb{P}^2$ is $3U + 3V = 0$ (and we can divide out the common factor of 3).

Examining the curve $u^3 + v^3 = \alpha$ we can see that this does not intersect at all in the real numbers, and has a triple root at the point at infinity. We will use this line as our $Z = 0$ axis after our transformation.

We will take $U - V = 0$ as our X axis, motivated by the fact that this is a line of symmetry of our curve, and finally we will take $U + V - W = 0$ as our Y axis, motivated by the fact that it intersects $Z = 0$ at P, and is helpfully orthogonal to the X axis, so we should avoid any pesky XY terms after transformation.

Putting this together, our transformation from (U, V, W) space to (X, Y, Z) space will be:

$$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} U \\ V \\ W \end{pmatrix} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

This matrix is, by design, invertible. Its inverse is:

$$A^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 0 & -2 & 2 \end{pmatrix}$$

This gives us an affine transformation which allows us to go from (X, Y, Z) space to (U, V, W) space as follows:

$$\begin{aligned} U &= \frac{1}{2}(X + Z) \\ V &= \frac{1}{2}(-X + Z) \\ W &= -Y + Z \end{aligned}$$

By substituting these equations back into our homogeneous version of C, we get:

$$\left(\frac{1}{2}(X + Z)\right)^3 + \left(\frac{1}{2}(-X + Z)\right)^3 - \alpha\left(-Y + Z\right)^3 = 0$$

Expanding and cancelling terms, we simplify our original equation to:

$$\begin{gathered} \frac{1}{8}(6X^2Z + 2Z^3) - \alpha(-Y^3 + 3Y^2Z - 3YZ^2 + Z^3) = 0 \\ 3X^2Z + Z^3 + 4\alpha Y^3 - 12\alpha Y^2 Z + 12\alpha YZ^2 - 4\alpha Z^3 = 0 \end{gathered}$$

Replacing $x = \frac{X}{Z}, y = \frac{Y}{Z}$ to dehomogenize, we get:

$$3x^2 + 1 + 4\alpha y^3 - 12\alpha y^2 + 12\alpha y - 4\alpha = 0$$

$$3x^2 = -4\alpha y^3 + 12\alpha y^2 - 12\alpha y + 4\alpha - 1$$

We want a perfect square term on the left, and a leading perfect cube on the right. We can achieve this by multiplying both sides by $3^3 \cdot 4^2 \cdot \alpha^2 = 432\alpha^2$:

$$3^4 4^2 \alpha^2 x^2 = -3^3 4^3 \alpha^3 y^3 + 3^3 4^3 \alpha^3 (3y^2) - 3^3 4^3 \alpha^3 (3y) + 3^3 4^3 \alpha^3 - 432\alpha^2$$

Substituting $a = 36\alpha x, b = -12\alpha(y-1)$ we get:

$$a^2 = b^3 - 432\alpha^2$$

The transforms from (a, b) to (u, v) are now straightforward to derive:

$$\begin{array}{rcll}
a & = & 36\alpha x & \text{\# Final substitution above} \\
 & = & 36\alpha \frac{X}{Z} & \text{\#}\ x = \frac{X}{Z} \\
 & = & 36\alpha \frac{U-V}{U+V} & \text{\#}\ X = U - V, Z = U + V \\
 & = & 36\alpha \frac{u-v}{u+v} & \text{\#}\ u = \frac{U}{W}, v = \frac{V}{W} \\
b & = & -12\alpha(y-1) & \text{\# Final substitution above} \\
 & = & -12\alpha\left(\frac{Y}{Z} - 1\right) & \text{\#}\ y = \frac{Y}{Z} \\
 & = & -12\alpha\left(\frac{U+V-W}{U+V} - 1\right) & \text{\#}\ Y = U + V - W, Z = U + V \\
 & = & -12\alpha\left(\frac{-W}{U+V}\right) & \text{\# Simplify}\ \frac{U+V}{U+V} = 1 \\
 & = & \frac{12\alpha}{u+v} & \text{\#}\ u = \frac{U}{W}, v = \frac{V}{W}
\end{array}$$

The transformation from (u, v) to (a, b) is similar:

$$\begin{array}{rcll}
u & = & \frac{U}{W} & \text{\# Homogenization of original cubic curve} \\
 & = & \frac{\frac{1}{2}(X+Z)}{-Y+Z} & \text{\#}\ U = \frac{1}{2}(X+Z), W = -Y + Z \\
 & = & \frac{\frac{X}{Z}+1}{-2\frac{Y}{Z}+2} & \text{\# Division by Z in numerator and denominator} \\
 & = & \frac{(x+1)}{-2(y-1)} & \text{\#}\ x = \frac{X}{Z}, y = \frac{Y}{Z} \\
 & = & \frac{(\frac{a}{36\alpha}+1)}{-2(\frac{-b}{12\alpha})} & \text{\#}\ a = 36\alpha x, b = -12\alpha(y-1) \\
 & = & \frac{a+36\alpha}{6b} & \text{\# Simplify fraction} \\
v & = & \frac{V}{W} & \text{\# Homogenization of original cubic curve} \\
 & = & \frac{\frac{1}{2}(-X+Z)}{-Y+Z} & \text{\#}\ V = \frac{1}{2}(-X+Z), W = -Y + Z \\
 & = & \frac{-X+Z}{-2Y+2Z} & \text{\# Simplify fraction} \\
 & = & \frac{-x+1}{-2(y-1)} & \text{\#}\ x = \frac{X}{Z}, y = \frac{Y}{Z} \\
 & = & \frac{-\frac{a}{36\alpha}+1}{-2(\frac{-b}{12\alpha})} & \text{\#}\ a = 36\alpha x, b = -12\alpha(y-1) \\
 & = & \frac{-a+36\alpha}{6b} & \text{\# Simplify fraction}
\end{array}$$