Addition of Points on a Cubic Curve

April 11, 2008

Scrolling Slides

Weierstrass form

$$y^2 + a_1xy + a_3y \;=\; a_0x^3 + a_2x^2 + a_4x + a_6 \quad a_0 \neq 0$$

Rationale for coefficient subscripts

1. Assign weight 2 to x
2. Assign weight 3 to y
3. Every monomial x^jy^k has a weight
4. Weight of a monomial product = sum of weights of factors
5. x^jy^k has weight $w \;=\; 2j + 3k$
6. Coefficient of x^jy^k has subscript $6 - w$
7. In every term

$$\text{coefficient subscript} + \text{weight of monomial} \;=\; 6$$

Projective or homogeneous form of the equation

Multiply each monomial by a power of z so that every term then has degree 3.

$$y^2z + a_1xyz + a_3yz^2 \;=\; a_0x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

From projective to affine

Recover the affine form of a Weierstrass equation from the projective form by setting

$$z \;=\; 1$$

Equivalence of projective and affine forms

(x, y) is a solution of the affine Weierstrass equation if and only if $(x, y, 1)$ is a solution of the projective equation.

These are "affine points" of the cubic curve.

When $z \neq 0$, (x, y, z) is a solution of the projective equation if and only if

$$(\frac{x}{z}, \frac{y}{z}, 1)$$

is a solution of the affine equation.

An affine solution (x, y) corresponds to the line of points (X, Y, Z) in space given parametrically, with parameter t, by

$$\begin{aligned} X &= tx \\ Y &= ty \\ Z &= t \end{aligned}$$

The projective plane

The *projective plane* is the set of all lines in space passing through the origin.

The affine plane as a subset of the projective plane

The *lines* through the origin of space meeting the plane with equation $z = 0$ only at the origin correspond to the *points* of the affine plane.

These are the affine points in the projective plane.

The points at infinity in the projective plane

The **lines** through the origin of space that lie in the plane with equation $z = 0$ are the "points at infinity" in the projective plane.

The projective plane is the union of the set of affine "points" and the set of "points" at infinity.

"Lines in the projective plane"

The projective plane is the set of lines through the origin of space.

Just as "points" of the projective plane are lines in space through the origin, a "line" in the projective plane is a plane in space through the origin.

Because $z = 0$ is the equation of a plane through the origin in space, one views the set of "points at infinity" as a "line" in the projective plane: the "line at infinity".

With a suitable change of coordinates any "line" in the projective plane may be made to serve as the "line at infinity".

The single point at infinity on a Weierstrass cubic

A cubic curve in Weierstrass form has a single "point" at infinity.

Obtain it by solving the homogeneous equation simultaneously with the equation $z = 0$.

The "point" at infinity on each cubic in Weierstrass form is $(0 : 1 : 0)$

It corresponds to the line in space given parametrically by

$$\begin{aligned} x &= 0 \\ y &= t \\ z &= 0 \end{aligned}$$

Addition of Points on a Weierstrass cubic

Characterized by two rules:

- The "point" at infinity is "zero"
- $$P + Q + R = \text{zero} \quad \Leftrightarrow \quad P,\ Q,\ R \text{ are collinear}$$

"Zero" for a Weierstrass cubic

The "point" at infinity is a triple point on a Weierstrass cubic.

So three copies of it may be regarded as collinear.

$$0 + 0 + 0 = 0$$

Why work in the projective plane?

- In the projective plane a cubic curve **without exception** intersects a line in 3 points, counting multiplicities.
- The point serving as "zero" for addition of points on a Weierstrass cubic is not an affine point.

Another fact about the projective plane

Without exception two different lines meet in a single point. Lines that are parallel in the affine plane share a single point on the "line" at infinity, which is the "line" of all "points" of the form $(x : y : z)$ with $z = 0$.

To find the "negative" of a point

To find the "negative" P' or $-P$ (but not the vector negative) of a point P on a Weierstrass cubic one seeks the third point on the "line" in the projective plane through P and "zero" (the point at infinity).

First example

Curve $y^2 = x^3 + 1$

Point $P = (2, 3)$

Projective equation: $y^2 z = x^3 + z^3$
Homogeneous coordinates of P: $(2 : 3 : 1)$

The "line" through P and "zero" corresponds to the plane through the origin of space containing $(2, 3, 1)$ and $(0, 1, 0)$.

This plane in space is the set of (vector) linear combinations of those points:

$$\begin{aligned} x &= 2u \\ y &= 3u + v \\ z &= u \end{aligned}$$

The affine points on this "line" in the projective plane are given by setting $z = 1$. Then necessarily $u = 1$ and

$$\begin{aligned} x &= 2 \\ y &= 3 + v \end{aligned}$$

This is a parameterization of the vertical line $x = 2$ in the affine plane.

The negative of P is the second affine point of the curve on the line $x = 2$, which is $-P = (2, -3)$.

Finding the third point of a Weierstrass cubic on the line through two given points of the cubic

- Represent the line parametrically
- Substitute the parametric equations into the Weierstrass equation
- Obtain a cubic equation in the parameter.

- Two of the three roots of this cubic equation correspond to the first two points on the line.
- The third point may be found by polynomial long division.

How to find the "sum" of two points on a Weierstrass cubic

P and Q denote two different given points on a cubic.

- Find the third point R on the line through P and Q.
- This point R is the "negative" of $P + Q$.
- Find the negative of R (as above).

Finding the "negative" of an affine point

Find the line through the given point and the point at infinity

---

The line through the point at infinity and an affine point is vertical

Affine point $(r, s) = (r : s : 1)$

Point at infinity $(0 : 1 : 0)$

The "line" is the plane in space through these points and the origin.

Normal vector to the plane: $(r, s, 1) \times (0, 1, 0) = (-1, 0, r)$

Equation of the plane: $-1 \cdot x + 0 \cdot y + r \cdot z = 0$

Simplified: $x = r$ (the vertical line through the affine point)

The "negative" is the other point of the curve on the same vertical line

If (r', s') denotes the "negative" of (r, s), then $r' = r$, and r' satisifes:

$$s'^2 + a_1 r s' + a_3 s' = s^2 + a_1 r s + a_3 s$$

or s' is a root of the quadratic equation

$$z^2 + (a_1 r + a_3) z - (s^2 + a_1 r s + a_3 s) = 0$$

The sum of the two roots is the negative of the coefficient of z.

$$s' = -a_1 r - a_3 - s$$

Formula for the "negative" of a point

$$\begin{aligned} r' &= r \\ s' &= -a_1 r - a_3 - s \end{aligned}$$

Example of Addition

Curve $y^2 = x^3 - 7x + 10$

Points $A = (2, 2)$ and $B = (1, -2)$

General

The "sum" is the "negative" of the third point of the curve on the line through the given points.

Both points must be points on the curve.

Finding the Line

The projective versions of the given points are $\tilde{\mathrm{A}} = (2 : 2 : 1)$ and $\tilde{\mathrm{B}} = (1 : -2 : 1)$. The "line" through them in the projective plane is the plane in space through the origin, $(2, 2, 1)$ and $(1, -2, 1)$.

This plane is the linear span of the vectors $(2, 2, 1)$ and $(1, -2, 1)$.

Two parameters for the plane:

$$P(u, v) = (2u + v, 2u - 2v, u + v)$$

Affine points: $u + v = 1$

One parameter for the affine form of the line:

$$p(u) = (2u + (1 - u), 2u - 2(1 - u)) = (u + 1, 4u - 2)$$

Note: $p(0) = (1, -2) = B$ and $p(1) = (2, 2) = A$

Equivalent affine form

This can be used directly as a general method for finding a parametric representation of the line between two affine points:

$$p(u) \;=\; uA + (1-u)B$$

Either way, for this example, the parametric form of the line is

$$p(u) \;=\; uA + (1-u)B \;=\; u(2,2) + (1-u)(1,-2) \;=\; (u+1, 4u-2)$$

Finding the third point on the line

The equation $f(x,y) \;=\; x^3 - 7x + 10 - y^2 \;=\; 0$

The line $p(u) \;=\; (u+1, 4u-2)$

Intersecting the curve with the parameterized line

Substitute (in *Maple* use `subs`):

$$\varphi(u) \;=\; f(p(u)) \;=\; (u+1)^3 - 7(u+1) + 10 - (4u-2)^2 \;=\; 0$$

Simplified:

$$\varphi(u) \;=\; u^3 - 13u^2 + 12u$$

The parameter values $u = 0$ and $u = 1$ must be roots if A and B are points on the cubic curve. So $\varphi(u)$ must be divisible by u and by $u-1$, hence, by $u^2 - u$.

$$\frac{\varphi(u)}{u^2 - u} \;=\; u - 12$$

The third point on the curve is $p(12) \;=\; (13, 46)$.

The "Sum"

The "sum" is the "negative" of the third point of the curve on the line through A and B. The third point is $(13, 46)$.

$$A + B \;\;=\;\; (2,2) \;+\; (1,-2) \;\;=\;\; (13,-46)$$

The "double" of a point

Curve $y^2 = x^3 - 7x + 10$

Point $B = (1, -2)$

For finding $2B = B + B$ the tangent line serves as the line through the two given points.

Finding the tangent line

Use implicit differentiation to find its slope:

$$2yy' = 3x^2 - 7$$

Evaluate when $(x, y) = (1, -2)$:

$$y' = 1$$

The tangent line at $(1, -2)$ is parallel to any vector with slope 1, e.g., $V = (1, 1)$.

Parametric equation:

$$p(t) = B + tV = (1, -2) + t(1, 1) = (1 + t, -2 + t)$$

Intersecting the curve with the tangent line

Substitute (in *Maple* use `subs`):

$$\varphi(t) = f(p(t)) = (1 + t)^3 - 7(1 + t) + 10 - (-2 + t)^2 = t^3 + 2t^2$$

Since the tangent line at B intersects the curve at B with multiplicity 2 and B corresponds to parameter value $t = 0$, it is guaranteed that t^2 divides $\varphi(t)$.

$$\frac{\varphi(t)}{t^2} = t + 2$$

The "third" point of the curve on the line tangent at B is the point $p(-2) = (-1, -4)$.

The "Double"

The "sum" is the "negative" of the third point of the curve on the line tangent to the curve at B. The third point is $(-1, -4)$.

$$2B = B + B = (-1, 4)$$

Watch out for points of finite order

In the arithmetic on the curve $y^2 = x^3 + 1$ the point $P = (2, 3)$ has the following multiples:

$$2P = (0, 1) \quad 3P = (-1, 0) \quad 4P = (0, -1) \quad 5P = (2, -3) \quad 6P = (0 : 1 : 0) \text{ i.e., zero}$$

Thus, P is what we call a point of order 6.

Definition: In the arithmetic on a cubic curve a point P has finite *order* $m > 0$ if some positive multiple of P is "zero" and m is the smallest positive integer for which $mP = 0$. If no positive multiple of m is "zero", then P may be said to have *infinite order*.

Watch out for denominators

Even for a cubic curve with integer coefficients and points on that curve with integer coordinates computations in the arithmetic on the curve more often than not lead to points having denominators in their coordinates.

Example

Curve $y^2 = x^3 - 7x + 10$

Point $B = (1, -2)$

Here one has

$$3B = (9, 26) \quad 4B = (\frac{9}{4}, -\frac{19}{8}) \quad 5B = (-\frac{79}{25}, \frac{94}{125}) \quad 6B = (\frac{439}{169}, \frac{6716}{2197}) \quad \ldots$$
