Singular Cubic Curves

Sarah Michele Rajtmajer

June 11, 2008

Let F be a projective plane curve over a field k, $F \neq 0$.
Fix $(x_0, y_0, w_0) \in F(k)$, and choose affine local coordinates about (x_0, y_0, w_0) given by some Φ with $\Phi(x_0, y_0, w_0) = (0,0,1)$.

Let:

$$f(x,y) = F\left(\Phi^{-1}(x,y,1)\right) \in k[x,y].$$

Generally, f is the sum of homogeneous terms of degree 1 through d, say $f = f_1 + f_2 + \ldots + f_d$, with $f_1, \ldots, f_d$ depending on (x_0, y_0, w_0) and Φ.

We say (x_0, y_0, w_0) is a nonsingular point if f_1 is not the zero polynomial in $k[x,y]$.
Otherwise, (x_0, y_0, w_0) is a singular point.

We say that the plane curve F is nonsingular if F is nonsingular at every point of $F(\bar{k})$.
Otherwise, F is singular.

In the affine sense,

If $(0,0)$ is a point on the affine curve $f(x,y)=0$ over k, then $(0,0)$ is a singular point if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ both vanish at $(0,0)$.
Equivalently, $(0,0)$ is singular if $f = f_1 + f_2 + ... + f_d$ where each $f_i \in k[x,y]$ is a homogeneous polynomial of degree i.

For instance, $(0,0)$ is singular on $y^2 = x^3$ and on $y^2 = x^3 + x^2$, but not on $y^2 = x^3 - x^2$.

Nonsingularity at all points in $F(k)$ does not imply F is nonsingular.

As a counterexample, consider the curve

$$F(x, y, w) = x^3 - 6xw^2 + 6yw^2 - y^3$$

F is defined over $k = \mathbb{Q}$, is nonsingular at every point of $F(\mathbb{Q})$, and has a singular point at $(x, y, w) = (\sqrt{2}, \sqrt{2}, 1)$. So the curve is singular.

In affine form, we have

$$f(x, y) = x^3 - 6x + 6y - y^3$$

It is easy to see that the conditions $\frac{\partial}{\partial x} = 0$ and $\frac{\partial}{\partial y} = 0$ imply $x = \sqrt{2}$ and $y = \sqrt{2}$.

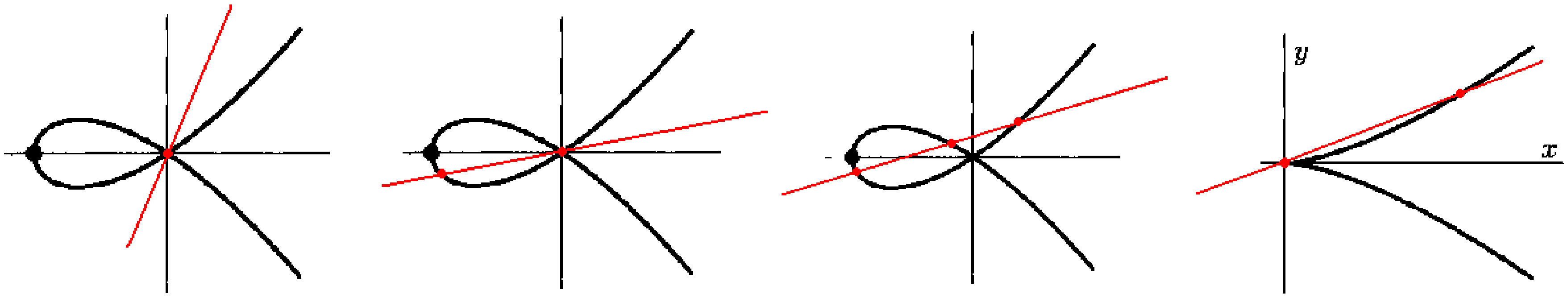
A cubic curve can have at most one singular point.

Let C be a cubic curve with a singular point $S \in C$.

Any line through S will intersect C at S with multiplicity at least two.

If there were a second singular point $S' \in C$, then the line L connecting S and S' would intersect C at least twice at S and at least twice at S', so L would intersect C at least four times.

However, a line and a cubic intersect in only three points counting multiplicities.



A cubic over a field k in Weierstrass form is given projectively by

$$y^2w+a_1xyw+a_3yw^2=x^3+a_2x^2w+a_4xw^2+a_6w^3$$

with coefficients in k.

Since behavior of the curve at $w=0$ $\left(\left(x,y,w\right)=\left(0,1,0\right)\right)$ is so well understood, we can work with the affine form

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

Let E be a singular Weierstrass curve over k, with singularity at $\left(x_0, y_0\right)$. Translating $\left(x_0, y_0\right)$ to the origin (an admissible change of variables), we are led to:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad \text{with } a_6 = 0.$$

Furthermore, the conditions that $\frac{\partial}{\partial x} = 0$ and $\frac{\partial}{\partial y} = 0$ at $(0,0)$ imply that a_4=0 and a_3=0, respectively.

Thus E is given by

$$y^2 + a_1xy = x^3 + a_2x^2.$$

From here we can see there are two distinct types of singularities.

We can factor

$$y^2 + a_1xy - a_2x^2 = x^3$$

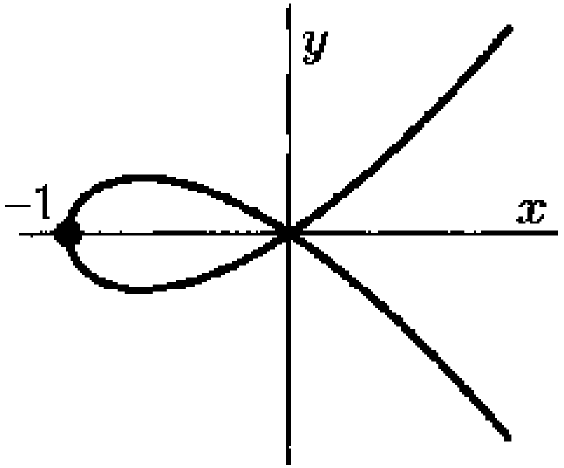
over k, obtaining

$$(y - \alpha x)(y - \beta x) = x^3 \qquad \text{with } \alpha, \beta \in \overline{k}.$$

We say that the singular point $(0,0)$ is

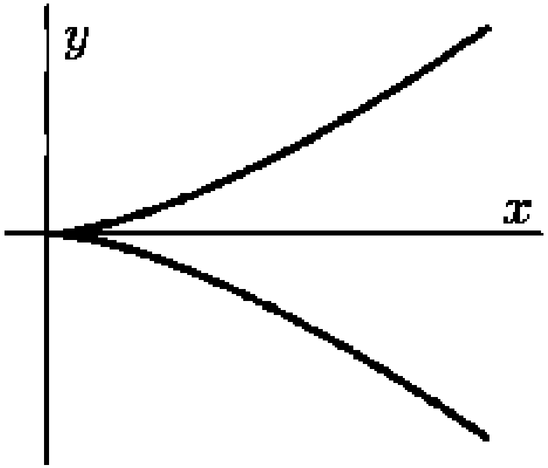
a cusp if $\alpha = \beta$, or

a node if $\alpha \neq \beta$.



A Singular Cubic with Distinct Tangent Directions

$$C : y^2 = x^3 + x^2$$



A Singular Cubic with A Cusp

$$C' : y^2 = x^3$$

Generally, a singular cubic curve can take three forms:

$y^2 = x^3,\ y^2 = x^3 + x^2,$ or $y^2 = x^3 + ax^2$ for $a \in \mathbb{Z}$ square-free.

We'd like to make the points of C into a group, as we did for non-singular cubics.

$$C_{ns} = \{P \in C : P \text{ is not a singular point}\}$$

Let $C_{ns}(\mathbb{Q})$ denote the subset of C_{ns} consisting of points with rational coordinates.

Fix $O \in C_{ns}$ to be the origin.

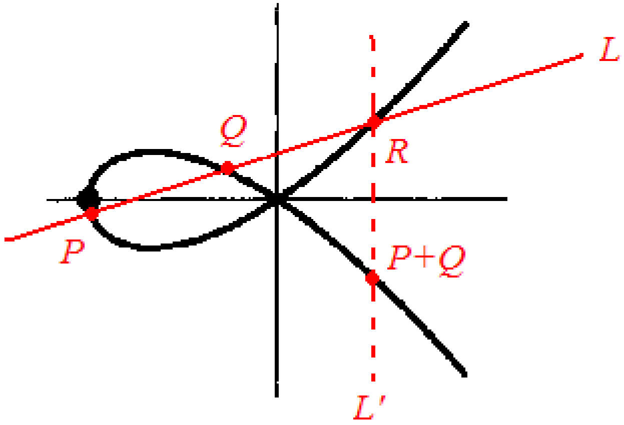
To add two points $P, Q \in C_{ns}$, we use the same geometric procedure that worked for nonsingular curves:

Draw a line L connecting P and Q, and let R be the other intersection point of $L \cap C$.

Draw a line L' through R and O.

The third intersection point of $L' \cap C$ is

defined to be the sum $P + Q$.



C_{ns} is an abelian group.

And if $O \in C_{ns}(\mathbb{Q})$, then $C_{ns}(\mathbb{Q})$ is a subgroup of C_{ns}.

$$C_{ns}$$

More explicitly, we can make a change of variables so the singular cubic curve is given by

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

and then all of the formulas for the addition law for the nonsingular case are still true.

For example, on the singular cubic curve

$$y^2 = x^3$$

with singular point $S = (0,0)$, the addition law becomes

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{\upsilon^2}{x_1 x_2}, \frac{-\upsilon^2}{y_1 y_2} \right), \quad \text{where } \upsilon = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}.$$

The Mordell-Weil theorem says that if C is nonsingular, $C(\mathbb{Q})$ is a finitely generated group.

But what does $C_{ns}(\mathbb{Q})$ look like for C singular?

There are two different answers depending on the type of singularity.

Theorem. (a) Let C be the singular cubic curve $y^2 = x^3 + x^2$. Then the map

$$\phi\colon C_{ns}(\mathbb{Q}) \to \mathbb{Q}^*, \qquad \phi(P) = \begin{cases} \dfrac{y-x}{y+x}, & \text{if } P = (x, y) \\ 1, & \text{if } P = O \end{cases}$$

is a group isomorphism from $C_{ns}(\mathbb{Q})$ to the multiplicative group of non-zero rational numbers.

(b) Let C be the singular cubic curve $y^2 = x^3$. Then the map

$$\phi\colon C_{ns}(\mathbb{Q}) \to \mathbb{Q}, \qquad \phi(P) = \begin{cases} \dfrac{x}{y}, & \text{if } P = (x, y) \\ 0, & \text{if } P = O \end{cases}$$

is a group isomorphism from $C_{ns}(\mathbb{Q})$ to the additive group of all rational numbers.

PROOF of (a).

Observe that ϕ is well defined.

The only possible problem would be if we had a point $(x, y) \in C_{ns}(\mathbb{Q})$ with $y + x = 0$.
But then the equation of C would imply that $x^3 = y^2 - x^2 = (y+x)(y-x) = 0$, so $x = 0$, and then also $y = 0$.
Since $(0,0)$ is the singular point on C, we see that $y + x \neq 0$ for all points $(x, y) \in C_{ns}$.

Next, set $t = \dfrac{y-x}{y+x}$ and solve for $y = \left(\dfrac{1+t}{1-t}\right)x$. Then substitute into $y^2 = x^3 + x^2$ and solve for x:

$$x = \frac{4t}{(1-t)^2}.$$

We get a map

$$\psi\colon \mathbb{Q}^* \to C_{ns}(\mathbb{Q}), \qquad \psi(t) = \begin{cases} \left(\dfrac{4t}{(1-t)^2}, \dfrac{4t(1+t)}{(1-t)^3} \right) & \text{if } t \neq 1, \\ O & \text{if } t = 1. \end{cases}$$

$\phi(\psi(t)) = t$ and $\psi(\phi(P)) = P$, so ϕ and ψ are inverse maps. Hence ϕ and ψ are one-to-one and onto as maps of sets.

Show that ϕ and ψ are homomorphisms:

Check that ψ sends inverses to inverses.

$$\begin{aligned}\psi\left(\frac{1}{t}\right) &= \left(\frac{4t^{-1}}{(1-t^{-1})^2}, \frac{4t^{-1}(1+t^{-1})}{(1-t^{-1})^3}\right) \\ &= \left(\frac{4t}{(1-t)^2}, -\frac{4t(1+t)}{(1-t)^3}\right) \\ &= -\psi(t).\end{aligned}$$

Next let $P_1, P_2, P_3 \in C_{ns}$ be any three points on C_{ns}. We know that their sum is zero if and only if they are collinear. If we use coordinates $P_i = (x_i, y_i)$, then the line through P_1 and P_2 has the equation

$$(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1).$$

Substitute $(x, y) = (x_3, y_3)$ and multiplying out both sides, we find that P_1, P_2, P_3 are collinear if and only if their coordinates satisfy the condition

$$x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_1 - x_1 y_3 = 0. \qquad (*)$$

Verify that if three elements $t_1, t_2, t_3 \in \mathbb{Q}^*$ multiply to 1, then their images $\psi(t_1), \psi(t_2), \psi(t_3) \in C_{ns}(\mathbb{Q}^*)$ sum to O:

Recall we have the formula for ψ:

$$\psi(t) = \left(\frac{4t}{(1-t)^2}, \frac{4t(1+t)}{(1-t)^3} \right)$$

Letting $P_1 = \psi(t_1), P_2 = \psi(t_2), P_3 = \psi(t_3),$ substituting into the left hand side of (*) and manipulating, we have:

$$x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_1 - x_1 y_3 = \frac{32(t_1 - t_2)(t_1 - t_3)(t_2 - t_3)(t_1 t_2 t_3 - 1)}{(1-t_1)^3 (1-t_2)^3 (1-t_3)^3}.$$

This proves that

$$\begin{aligned} t_1 t_2 t_3 = 1 \quad &\Rightarrow \psi(t_1), \psi(t_2), \text{ and } \psi(t_3) \text{ are collinear} \\ &\Rightarrow \psi(t_1) + \psi(t_2) + \psi(t_3) = O, \end{aligned}$$

provided that t_1, t_2, t_3 are distinct and not equal to 1.

The remaining cases can be dealt with similarly, or we can define the group law on all of the real points in C_{ns} and argue that because $\psi: \mathbb{R}^* \to C_{ns}(\mathbb{R})$ is a homomorphism for distinct points, it is a homomorphism for all points by continuity.

(b) follows similarly to (a):

However, in this case we set $t = \dfrac{x}{y}$ and solve for $y = \left(\dfrac{1}{t}\right)x.$

Then substitute into $y^2 = x^3$ and solve for x:

$$x = \frac{1}{t^2}.$$

And we get a map

$$\psi\colon \mathbb{Q} \to C_{ns}(\mathbb{Q}), \qquad \psi(t) = \begin{cases} \left(\dfrac{1}{t^2}, \dfrac{1}{t^3}\right) & \text{if } t \neq 0, \\ O & \text{if } t = 0. \end{cases}$$

As in (a), we then show that ϕ and ψ are inverse maps, hence one-to-one and onto as maps of sets. Furthermore, we can show ϕ and ψ are homomorphisms.

The groups $\left(\mathbb{Q}^{*},*\right)$ and $\left(\mathbb{Q},+\right)$ are not finitely generated.

So our theorem implies that the group of rational points $C_{ns}\left(\mathbb{Q}\right)$
on a singular cubic curve is not finitely generated, at least for the two curves covered in the theorem.

This is of course very different from the case of non-singular cubic curves, whose groups of rational points are finitely generated, as we know by the Mordell-Weil theorem.

Exercise 3.10.

(a) Let C be the singular cubic curve $y^2 = x^3$. Prove that the group law on C_{ns} is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{\upsilon^2}{x_1 x_2}, \frac{-\upsilon^2}{y_1 y_2} \right), \quad \text{where } \upsilon = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}.$$

Given nonsingular points $P = (x_1, y_1), Q = (x_2, y_2) \in \Gamma_{ns}$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ is the slope of the line through } P, Q$$

and the equation of the line is $y = \lambda x + \upsilon$, where υ has the formula given in the problem:

$$\upsilon = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}.$$

If $P + Q = (x_3, y_3)$, then $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = -\lambda x_3 - \upsilon$.

It is straightforward to verify that using the additional relations $\mathrm{x}_1^3 = y_1^2$ and $\mathrm{x}_2^3 = y_2^2$, we have

$$(x_3, y_3) = \left(\frac{\upsilon^2}{x_1 x_2}, \frac{\upsilon^3}{y_1 y_2} \right).$$

Exercise 3.11.

Let C be the singular cubic curve $y^2 = x^3$. Prove that the map

$$\phi : C_{ns}(\mathbb{Q}) \to \mathbb{Q}, \qquad \phi(P) = \begin{cases} \dfrac{x}{y} & \text{if } P = (x, y) \\ 0 & \text{if } P = O \end{cases}$$

is a group isomorphism from $C_{ns}(\mathbb{Q})$ to the additive group of all rational numbers.

Given distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ not equal to O, we can compute $(x_3, y_3) = P + Q$ as in Exercise 3.10, and from that formula get $\frac{\mathrm{x}_3}{\mathrm{y}_3} = \frac{y_1 y_2}{x_1 x_2 \upsilon}$.

Thus to prove ϕ is a homomorphism we must show that $\frac{y_1 y_2}{x_1 x_2 \upsilon} = \frac{\mathrm{x}_1}{\mathrm{y}_1} + \frac{\mathrm{x}_2}{\mathrm{y}_2}$.

Once again, using the relations $\mathrm{x}_1^3 = y_1^2$ and $\mathrm{x}_2^3 = y_2^2$, this is a straightforward calculation.

We can deal with the case $P = Q$ by arguing continuity.

Once we know ϕ is a homomorphism, to prove it is bijective it is enough to demonstrate an inverse map.
Define $\psi : \mathbb{Q} \to C_{ns}(\mathbb{Q})$ by

$$\psi(q) = \begin{cases} (q^{-2}, q^{-3}) & \text{if } q \neq 0 \\ O & \text{if } q = 0 \end{cases}.$$

It is easy to check that ϕ and ψ are inverses as maps of sets.

Conclusion

Singular cubic curves are those of the form:

$y^2 = x^3$, $y^2 = x^3 + x^2$, or $y^2 = x^3 + ax^2$ for $a \in \mathbb{Z}$ square-free.

Their corresponding groups of rational points on the curve are $\left(\mathbb{Q}^*, *\right)$ or $\left(\mathbb{Q}, +\right)$.

Elliptic curves over finite fields can be used for cryptography, using the group operator as its basic arithmetic operation.

In application, singular elliptic curves are unsuitable for cryptography.
Since their corresponding groups are isomorphic to either the multiplicative or the additive group over the underlying field (depending on the type of singularity), they are easy to crack.