planetmath.org

Math for the people, by the people.

bad reduction

Canonical name	BadReduction
Date of creation	2013-03-22 13:49:21
Last modified on	2013-03-22 13:49:21
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	12
Author	alozano (2414)
Entry type	Definition
Classification	msc 14H52
Related topic	EllipticCurve
Related topic	JInvariant
Related topic	HassesBoundForEllipticCurvesOverFiniteFields
Related topic	TorsionSubgroupOfAnEllipticCurveInjectsInTheReductionOfTheCurve
Related topic	ArithmeticOfEllipticCurves
Related topic	SingularPointsOfPlaneCurve
Defines	bad reduction
Defines	good reduction
Defines	cusp
Defines	node
Defines	multiplicative reduction
Defines	additive reduction

1 Singular Cubic Curves

Let E be a cubic curve over a field K with Weierstrass equation $f(x, y) = 0$, where:

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

which has a singular point $P = (x_0, y_0)$. This is equivalent to:

$$\partial f/\partial x(P) = \partial f/\partial y(P) = 0$$

and so we can write the Taylor expansion of $f(x, y)$ at (x_0, y_0) as follows:

$$\begin{aligned} f(x,y) - f(x_0,y_0) &= \lambda_1(x-x_0)^2 + \lambda_2(x-x_0)(y-y_0) + \lambda_3(y-y_0)^2 - (x-x_0)^3 \\ &= [(y-y_0) - \alpha(x-x_0)][(y-y_0) - \beta(x-x_0)] - (x-x_0)^3 \end{aligned}$$

for some $\lambda_i \in K$ and $\alpha, \beta \in \bar{K}$ (an algebraic closure of K).

Definition 1. *The singular point P is a* node *if $\alpha \neq \beta$. In this case there are two different tangent lines to E at P, namely:*

$$y - y_0 = \alpha(x - x_0), \quad y - y_0 = \beta(x - x_0)$$

If $\alpha = \beta$ then we say that P is a cusp*, and there is a unique tangent line at P.*

Note: See the entry for elliptic curve for examples of cusps and nodes.

There is a very simple criterion to know whether a cubic curve in Weierstrass form is singular and to differentiate nodes from cusps:

Proposition 1. *Let E/K be given by a Weierstrass equation, and let Δ be the discriminant and c_4 as in the definition of Δ. Then:*

1. *E is singular if and only if $\Delta = 0$,*

2. *E has a node if and only if $\Delta = 0$ and $c_4 \neq 0$,*

3. *E has a cusp if and only if $\Delta = 0 = c_4$.*

Proof. See [**?**], chapter III, Proposition 1.4, page 50. □

2 Reduction of Elliptic Curves

Let $E/\mathbb{Q}$ be an elliptic curve (we could work over any number field K, but we choose $\mathbb{Q}$ for simplicity in the exposition). Assume that E has a minimal model with Weierstrass equation:

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

with coefficients in $\mathbb{Z}$. Let p be a prime in $\mathbb{Z}$. By reducing each of the coefficients a_i modulo p we obtain the equation of a cubic curve $\widetilde{E}$ over the finite field $\mathbb{F}_p$ (the field with p elements).

Definition 2.

1. *If $\widetilde{E}$ is a non-singular curve then $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ and we say that E has* good reduction *at p. Otherwise, we say that E has* bad reduction *at p.*

2. *If $\widetilde{E}$ has a cusp then we say that E has* additive reduction *at p.*

3. *If $\widetilde{E}$ has a node then we say that E has* multiplicative reduction *at p. If the slopes of the tangent lines (α and β as above) are in $\mathbb{F}_p$ then the reduction is said to be* split *multiplicative (and* non-split *otherwise).*

From *Proposition 1* we deduce the following:

Corollary 1. *Let $E/\mathbb{Q}$ be an elliptic curve with coefficients in $\mathbb{Z}$. Let $p \in \mathbb{Z}$ be a prime. If E has bad reduction at p then $p \mid \Delta$.*

Examples:

1. $E_1\colon y^2 = x^3 + 35x + 5$ has good reduction at $p = 7$.

2. However E_1 has bad reduction at $p = 5$, and the reduction is additive (since modulo 5 we can write the equation as $[(y-0) - 0(x-0)]^2 - x^3$ and the slope is 0).

3. The elliptic curve $E_2\colon y^2 = x^3 - x^2 + 35$ has bad multiplicative reduction at 5 and 7. The reduction at 5 is split, while the reduction at 7 is non-split. Indeed, modulo 5 we could write the equation as $[(y-0) - 2(x-0)][(y-0) + 2(x-0)] - x^3$, being the slopes 2 and -2. However, for $p = 7$ the slopes are not in $\mathbb{F}_7$ ($\sqrt{-1}$ is not in $\mathbb{F}_7$).

References

[1] James Milne, *Elliptic Curves*, `http://www.jmilne.org/math/CourseNotes/math679.html`onli course notes.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[3] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[4] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.