Semistable models of hyperelliptic curves over residue characteristic 2

Jeff Yelton (Emory University)
joint work with
Leonardo Fiore

University of Connecticut (virtual)
June 13th, 2020

Hyperelliptic curves over local fields

Hyperelliptic curves over local fields

In this talk, R is a discretely-valued local ring of characteristic 0 with fraction field K, maximal prime ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p}$ of characteristic $p \geq 0$.

Hyperelliptic curves over local fields

In this talk, R is a discretely-valued local ring of characteristic 0 with fraction field K, maximal prime ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p}$ of characteristic $p \geq 0$.

We define a **hyperelliptic curve** C over K to be a smooth curve which can be given by an affine model of the form

$$y^2 = f(x) = \prod_{i=1}^{d}(x - a_i),$$

where $f(x) \in K[x]$ is a polynomial of degree $d \geq 3$ and roots $a_1, ..., a_d \in \bar{K}$. (If $d = 3$ then it is also an **elliptic curve**.)

Hyperelliptic curves over local fields

In this talk, R is a discretely-valued local ring of characteristic 0 with fraction field K, maximal prime ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p}$ of characteristic $p \geq 0$.

We define a **hyperelliptic curve** C over K to be a smooth curve which can be given by an affine model of the form

$$y^2 = f(x) = \prod_{i=1}^{d} (x - a_i),$$

where $f(x) \in K[x]$ is a polynomial of degree $d \geq 3$ and roots $a_1, \ldots, a_d \in \bar{K}$. (If $d = 3$ then it is also an **elliptic curve**.)
For simplicity, let's assume that $a_1, \ldots, a_d \in R$**.**

Hyperelliptic curves over local fields

In this talk, R is a discretely-valued local ring of characteristic 0 with fraction field K, maximal prime ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p}$ of characteristic $p \geq 0$.

We define a **hyperelliptic curve** C over K to be a smooth curve which can be given by an affine model of the form

$$y^2 = f(x) = \prod_{i=1}^{d}(x - a_i),$$

where $f(x) \in K[x]$ is a polynomial of degree $d \geq 3$ and roots $a_1, \ldots, a_d \in \bar{K}$. (If $d = 3$ then it is also an **elliptic curve**.)
For simplicity, let's assume that $a_1, \ldots, a_d \in R$**.**
Since the characteristic $\neq 2$ the singular points on C are of the form $(a, 0)$ where $f(a) = f'(a) = 0$. Therefore, the *smoothness* property means that the roots a_i of f are all distinct.

Reductions of hyperelliptic curves

Reductions of hyperelliptic curves

We are interested in the *reduction* of our hyperelliptic curve $C : y^2 = f(x) = \prod_{i=1}^{d}(x - a_i)$, that is, the curve $\bar{C}$ over the residue field $R/\mathfrak{p}$ given by $y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$, where each $\bar{a}_i$ is the reduction of a_i mod $\mathfrak{p}$. *Although we have assumed C is smooth, its reduction $\bar{C}$ might not be (*“bad reduction”*)!*

Reductions of hyperelliptic curves

We are interested in the *reduction* of our hyperelliptic curve $C : y^2 = f(x) = \prod_{i=1}^{d}(x - a_i)$, that is, the curve $\bar{C}$ over the residue field $R/\mathfrak{p}$ given by $y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$, where each $\bar{a}_i$ is the reduction of a_i mod $\mathfrak{p}$. *Although we have assumed C is smooth, its reduction $\bar{C}$ might not be (*"bad reduction"*)!*

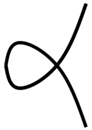
When $p \neq 2$, there will be a singular point on $\bar{C}$ corresponding to each subset (a **cluster**) of a_i's which are equivalent mod $\mathfrak{p}$.

Reductions of hyperelliptic curves

We are interested in the *reduction* of our hyperelliptic curve $C : y^2 = f(x) = \prod_{i=1}^{d}(x - a_i)$, that is, the curve $\bar{C}$ over the residue field $R/\mathfrak{p}$ given by $y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$, where each $\bar{a}_i$ is the reduction of a_i mod $\mathfrak{p}$. *Although we have assumed C is smooth, its reduction $\bar{C}$ might not be (*"bad reduction"*)!*

When $p \neq 2$, there will be a singular point on $\bar{C}$ corresponding to each subset (a **cluster**) of a_i's which are equivalent mod $\mathfrak{p}$.

If $p \neq 2$, a cluster of 2 roots
yields a **node** on $\bar{C}$.

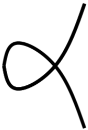


Reductions of hyperelliptic curves

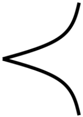
We are interested in the *reduction* of our hyperelliptic curve $C : y^2 = f(x) = \prod_{i=1}^{d}(x - a_i)$, that is, the curve $\bar{C}$ over the residue field $R/\mathfrak{p}$ given by $y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$, where each $\bar{a}_i$ is the reduction of a_i mod $\mathfrak{p}$. *Although we have assumed C is smooth, its reduction $\bar{C}$ might not be (*"bad reduction"*)!*

When $p \neq 2$, there will be a singular point on $\bar{C}$ corresponding to each subset (a **cluster**) of a_i's which are equivalent mod $\mathfrak{p}$.

If $p \neq 2$, a cluster of 2 roots yields a **node** on $\bar{C}$.



If $p \neq 2$, a cluster of ≥ 3 roots yields a **cusp** on $\bar{C}$.

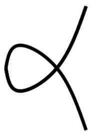


Reductions of hyperelliptic curves

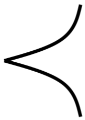
We are interested in the *reduction* of our hyperelliptic curve $C : y^2 = f(x) = \prod_{i=1}^{d}(x - a_i)$, that is, the curve $\bar{C}$ over the residue field $R/\mathfrak{p}$ given by $y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$, where each $\bar{a}_i$ is the reduction of a_i mod $\mathfrak{p}$. *Although we have assumed C is smooth, its reduction $\bar{C}$ might not be (*"bad reduction"*)!*

When $p \neq 2$, there will be a singular point on $\bar{C}$ corresponding to each subset (a **cluster**) of a_i's which are equivalent mod $\mathfrak{p}$.

If $p \neq 2$, a cluster of 2 roots yields a **node** on $\bar{C}$.



If $p \neq 2$, a cluster of ≥ 3 roots yields a **cusp** on $\bar{C}$.



On the other hand, if $p = 2$, the reduced curve $\bar{C} : y^2 = \prod_{i=1}^{d}(x - \bar{a}_i)$ *always* has a singular point and every singular point is a cusp!

Semistable reduction

Semistable reduction

Definition

A curve over K is said to have semistable reduction *if its reduction over $R/\mathfrak{p}$ has (at worst) nodes as singularities.*

Semistable reduction

Definition

A curve over K is said to have semistable reduction *if its reduction over $R/\mathfrak{p}$ has (at worst) nodes as singularities.*

Theorem (Deligne-Mumford, Artin-Winters)

For any curve C over a discrete valuation field K, there is a curve C^{ss} over a finite algebraic extension K'/K which is isomorphic to C over K' and which has semistable reduction.

Semistable reduction

Definition

A curve over K is said to have semistable reduction *if its reduction over $R/\mathfrak{p}$ has (at worst) nodes as singularities.*

Theorem (Deligne-Mumford, Artin-Winters)

For any curve C over a discrete valuation field K, there is a curve C^{ss} over a finite algebraic extension K'/K which is isomorphic to C over K' and which has semistable reduction.

(It is easy to see this for an elliptic curve when $p \neq 2$: if all three roots are equivalent modulo $\mathfrak{p}$ (additive reduction), this can be "fixed" by translating and scaling x.)

Semistable reduction

Definition

A curve over K is said to have semistable reduction *if its reduction over $R/\mathfrak{p}$ has (at worst) nodes as singularities.*

Theorem (Deligne-Mumford, Artin-Winters)

For any curve C over a discrete valuation field K, there is a curve C^{ss} over a finite algebraic extension K'/K which is isomorphic to C over K' and which has semistable reduction.

(It is easy to see this for an elliptic curve when $p \neq 2$: if all three roots are equivalent modulo $\mathfrak{p}$ (additive reduction), this can be "fixed" by translating and scaling x.)

Theorem (Dokchitser-Dokchitser-Maistret-Morgan)

When $p \neq 2$, the reduction type of C^{ss} is determined entirely by how the roots "cluster".

Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}

Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		

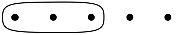
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		

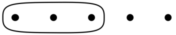
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		

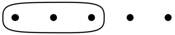
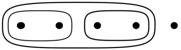
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		

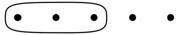
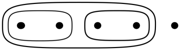
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

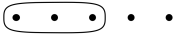
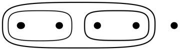
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

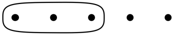
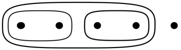
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

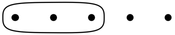
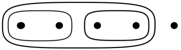
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

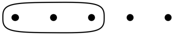
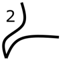
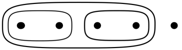
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

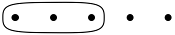
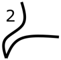
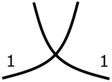
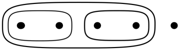
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

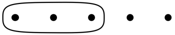
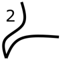
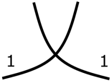
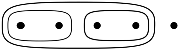
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

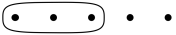
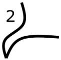
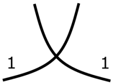
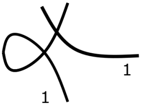
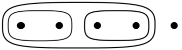
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

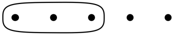
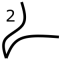
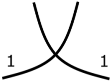
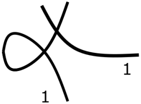
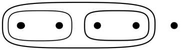
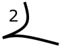
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

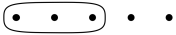
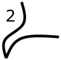
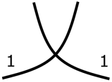
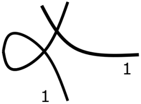
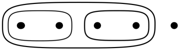
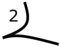
Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

Reductions of genus-2 curves when $p \neq 2$

For genus 2, $d = 5$, and $p \neq 2$, here are the main possibilities:

cluster picture	reduction type of C	reduction type of C^{ss}
pair 		
two pairs 		
three of a kind 		
full house 		
two pairs & four of a kind 		

Approach to finding semistable models when $p = 2$

Approach to finding semistable models when $p = 2$

1) We first make one or more substitutions of the form $x = \beta x_1 + \alpha$, $y = \beta^t y_1$, with $0 \leq t \leq \frac{d}{2}$ and $\beta \in \mathfrak{p}$. For each such substitution we get an equation

$$y_1^2 = f_1(x_1) \in K[x].$$

Approach to finding semistable models when $p = 2$

1) We first make one or more substitutions of the form $x = \beta x_1 + \alpha$, $y = \beta^t y_1$, with $0 \leq t \leq \frac{d}{2}$ and $\beta \in \mathfrak{p}$. For each such substitution we get an equation

$$y_1^2 = f_1(x_1) \in K[x].$$

2) Find some $G_1(x), H_1(x) \in R[x]$ such that

$$f_1(x) = \frac{1}{4} H_1(x_1)^2 + G_1(x_1).$$

Approach to finding semistable models when $p = 2$

1) We first make one or more substitutions of the form $x = \beta x_1 + \alpha$, $y = \beta^t y_1$, with $0 \leq t \leq \frac{d}{2}$ and $\beta \in \mathfrak{p}$. For each such substitution we get an equation

$$y_1^2 = f_1(x_1) \in K[x].$$

2) Find some $G_1(x), H_1(x) \in R[x]$ such that

$$f_1(x) = \frac{1}{4} H_1(x_1)^2 + G_1(x_1).$$

3) Perform the variable change $y_1 = y_1' + \frac{1}{2} H_1(x_1)$ to get the equation

$$(y_1')^2 + H_1(x_1) y_1' = G_1(x_1).$$

Approach to finding semistable models when $p = 2$

1) We first make one or more substitutions of the form $x = \beta x_1 + \alpha$, $y = \beta^t y_1$, with $0 \leq t \leq \frac{d}{2}$ and $\beta \in \mathfrak{p}$. For each such substitution we get an equation

$$y_1^2 = f_1(x_1) \in K[x].$$

2) Find some $G_1(x), H_1(x) \in R[x]$ such that

$$f_1(x) = \frac{1}{4}H_1(x_1)^2 + G_1(x_1).$$

3) Perform the variable change $y_1 = y_1' + \frac{1}{2}H_1(x_1)$ to get the equation

$$(y_1')^2 + H_1(x_1)y_1' = G_1(x_1).$$

With clever enough choices of α, β for each such substitution, the above equation(s) together reduce to a semistable curve.

Semistable reduction types for elliptic curves ($p = 2$)

Semistable reduction types for elliptic curves ($p = 2$)

As seen above, we can convert any elliptic curve to one with (at most) one cluster $\{a_1, a_2\}$. Let $v : K^\times \to \mathbb{Q}$ be the valuation on K normalized so that $v(2) = 1$ and let $m = v(a_2 - a_1) \geq 0$. There are two cases:

Semistable reduction types for elliptic curves ($p = 2$)

As seen above, we can convert any elliptic curve to one with (at most) one cluster $\{a_1, a_2\}$. Let $v : K^\times \to \mathbb{Q}$ be the valuation on K normalized so that $v(2) = 1$ and let $m = v(a_2 - a_1) \geq 0$. There are two cases:

- $0 \leq m \leq 4$: then we may perform a substitution using α and β as above, with $v(\beta) = \frac{m+2}{3}$ and $v(\alpha) = \frac{m}{2}$, and we get a smooth elliptic curve for the reduction

Semistable reduction types for elliptic curves ($p = 2$)

As seen above, we can convert any elliptic curve to one with (at most) one cluster $\{a_1, a_2\}$. Let $v : K^\times \to \mathbb{Q}$ be the valuation on K normalized so that $v(2) = 1$ and let $m = v(a_2 - a_1) \geq 0$. There are two cases:

- $0 \leq m \leq 4$: then we may perform a substitution using α and β as above, with $v(\beta) = \frac{m+2}{3}$ and $v(\alpha) = \frac{m}{2}$, and we get a smooth elliptic curve for the reduction
- $m > 4$: then we may perform a substitution with α and β as above, with $2 \leq v(\alpha) \leq m - 2$ and $v(\beta) = 2$ and get a nodal curve for the reduction

Semistable reduction types for elliptic curves ($p = 2$)

As seen above, we can convert any elliptic curve to one with (at most) one cluster $\{a_1, a_2\}$. Let $v : K^\times \to \mathbb{Q}$ be the valuation on K normalized so that $v(2) = 1$ and let $m = v(a_2 - a_1) \geq 0$. There are two cases:

- $0 \leq m \leq 4$: then we may perform a substitution using α and β as above, with $v(\beta) = \frac{m+2}{3}$ and $v(\alpha) = \frac{m}{2}$, and we get a smooth elliptic curve for the reduction
- $m > 4$: then we may perform a substitution with α and β as above, with $2 \leq v(\alpha) \leq m - 2$ and $v(\beta) = 2$ and get a nodal curve for the reduction

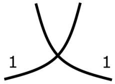
Corollary

In this setting, an elliptic curve has potentially good reduction iff $0 \leq m \leq 4$.

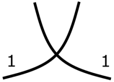
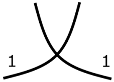
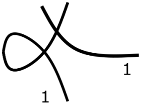
Semistable reduction types for genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
no cluster 	
pair 	
two pairs 	

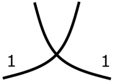
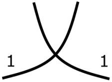
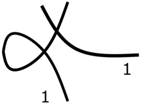
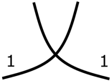
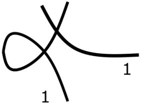
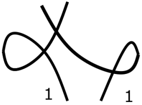
Semistable reduction types for genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
no cluster 	(two cases)  or 
pair 	
two pairs 	

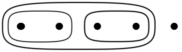
Semistable reduction types for genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
no cluster • • • • •	(two cases)  or 
pair (• •) • • • ($m :=$ valuation of difference between roots in pair)	$0 \le m \le \frac{8}{3}$  or  $\frac{8}{3} < m \le 4$ $m > 4$  or 
two pairs (• •) (• •) •	

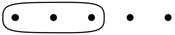
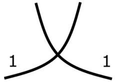
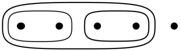
Semistable reduction types for genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
no cluster • • • • •	(two cases)  or 
pair (• •) • • • ($m :=$ valuation of difference between roots in pair)	$0 \leq m \leq \frac{8}{3}$  or  $\frac{8}{3} < m \leq 4$ $m > 4$  or 
two pairs (• •) (• •) • ($m_1, m_2 :=$ valuations of differences between roots in each pair)	two curves C_1, C_2, each with a node iff $m_i > 4$  or  or 

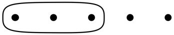
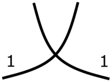
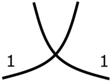
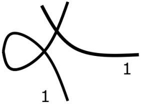
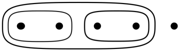
Semistable reduction types of hyperelliptic curves of genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
three of a kind 	
full house 	
two pairs and four of a kind 	

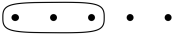
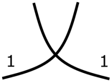
Semistable reduction types of hyperelliptic curves of genus 2 ($p = 2$)

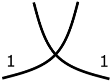
cluster picture	reduction type of C^{ss}
three of a kind 	
full house 	
two pairs and four of a kind 	

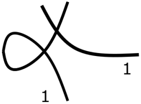
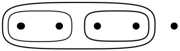
Semistable reduction types of hyperelliptic curves of genus 2 ($p = 2$)

cluster picture	reduction type of C^{ss}
three of a kind 	
full house  ($m :=$ valuation of difference between roots in pair)	$0 \leq m \leq 4$  $m > 4$ 
two pairs and four of a kind 	

Semistable reduction types of hyperelliptic curves of genus 2 ($p = 2$)

<table>
<tr><th>cluster picture</th><th>reduction type of C^{ss}</th></tr>
<tr><td>three of a kind
</td><td>
</td></tr>
<tr><td>full house

($m :=$ valuation of difference between roots in pair)</td><td>$0 \leq m \leq 4$ 

$m > 4$ 
</td></tr>
<tr><td>two pairs and four of a kind
</td><td>if evaluations of differences are $\gg 0$

</td></tr>
</table>