Local Arithmetic of Curves and Applications

Céline Maistret
University of Bristol

ANTS XVI

p-adic theories of curves

- Types of curves: Elliptic, hyperelliptic and general curves.
  - Algorithmic, families and global (rational points) applications.
    - L-function computation, Modular method, Parity conjecture.
  - Odd/even residue characteristic.
    - Odd residue characteristic.

L-functions of Elliptic Curves and local invariants

Let $E/\mathbb{Q}$ be an elliptic curve.

- $L(E,s) = \prod_p L_p(E, p^{-s})^{-1}$
- $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$
  - $\Lambda(E,s) = w \cdot \Lambda(E, 2-s)$
- Birch and Swinnerton-Dyer conjecture
  - $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = rk(E/\mathbb{Q})$
- (Strong) Birch and Swinnerton-Dyer conjecture
  - $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{rk_E}} = \frac{\Omega |Ш(E/\mathbb{Q})| R(E/\mathbb{Q}) \prod_p c_p}{|E_{tor}(\mathbb{Q})|^2}$

- $N = \prod p^{f_p}$
- $w = \prod_p w_p$
- $\prod_p c_p$

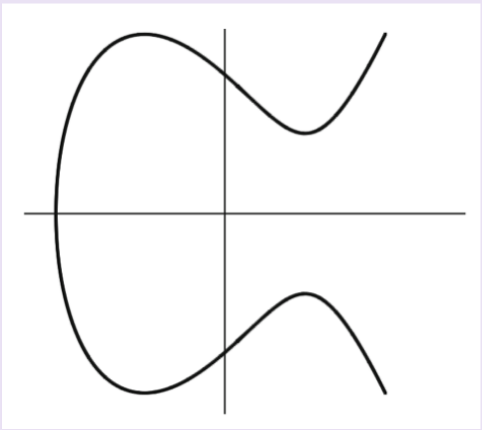
- $L_p(E, p^{-s})$
- f_p
- w_p
- c_p

Euler factors

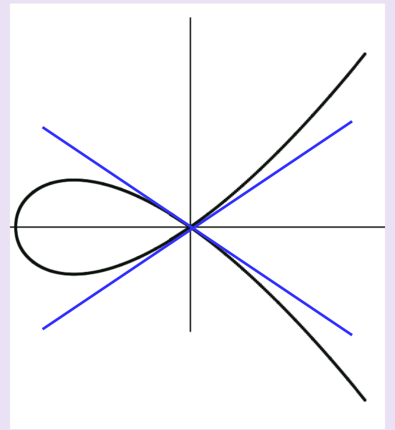
Let $E/\mathbb{Q}$ be an elliptic curve. Then $L(E,s) = \prod_p L_p(E, p^{-s})^{-1}$, where

$$L_p(E,T) = \begin{cases} 1 - a_pT + pT^2 & \text{if } E \text{ has good red. at } p, \text{ with } a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p), \\ 1 - T & \text{if } E \text{ has split mult. red. at } p, \\ 1 + T & \text{if } E \text{ has non-split mult. red. at } p, \\ 1 & \text{if } E \text{ has additive red. at } p\,. \end{cases}$$

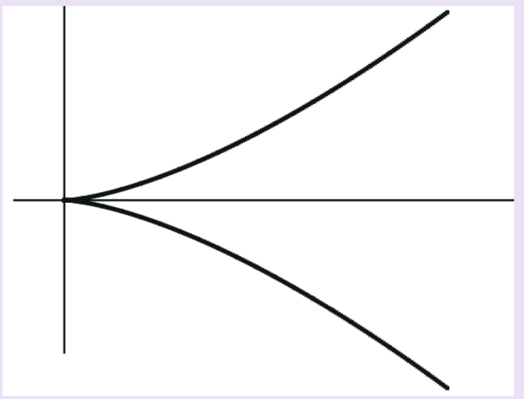
Consider $E/\mathbb{Z}_p : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$.



$\tilde{E} : \tilde{y}^2 = (\tilde{x}-\tilde{\alpha}_1)(\tilde{x}-\tilde{\alpha}_2)(\tilde{x}-\tilde{\alpha}_3)$



$\tilde{E} : \tilde{y}^2 = (\tilde{x}-\tilde{\alpha}_1)(\tilde{x}-\tilde{\alpha}_2)^2$



$\tilde{E} : \tilde{y}^2 = (\tilde{x}-\tilde{\alpha}_1)^3$

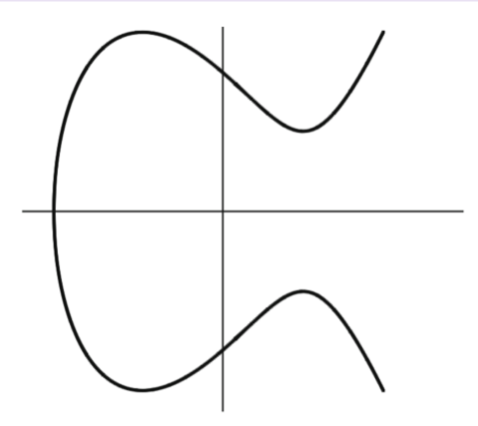
Euler factors: minimal data

Let $E/\mathbb{Q}$ be an elliptic curve. Then $L(E,s) = \prod_p L_p(E, p^{-s})^{-1}$, where

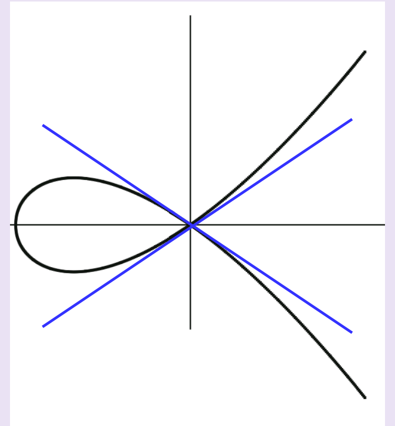
$$L_p(E,T) = \begin{cases} 1 - a_pT + pT^2 & \text{if } E \text{ has good red. at } p, \text{ with } a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p), \\ 1 - T & \text{if } E \text{ has split mult. red. at } p, \\ 1 + T & \text{if } E \text{ has non-split mult. red. at } p, \\ 1 & \text{if } E \text{ has additive red. at } p\,. \end{cases}$$

Consider $E/\mathbb{Z}_p : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

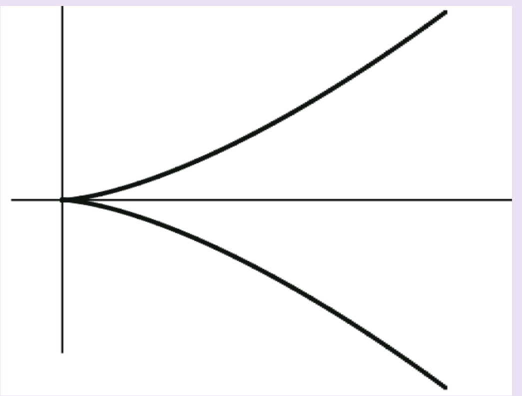
$\Delta_E = 2^4 \prod_{i<j} (\alpha_i - \alpha_j)^2$ ✗



$p \nmid \Delta_E$



$p \mid \Delta_E$



$p \mid \Delta_E$

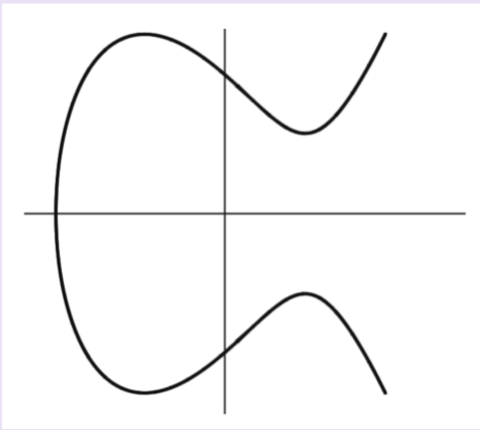
Euler factors: minimal data

Let $E/\mathbb{Q}$ be an elliptic curve. Then $L(E,s) = \prod_p L_p(E, p^{-s})^{-1}$, where

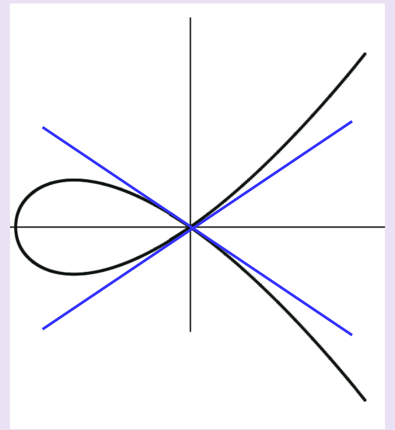
$$L_p(E,T) = \begin{cases} 1 - a_pT + pT^2 & \text{if } E \text{ has good red. at } p, \text{ with } a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p), \\ 1 - T & \text{if } E \text{ has split mult. red. at } p, \\ 1 + T & \text{if } E \text{ has non-split mult. red. at } p, \\ 1 & \text{if } E \text{ has additive red. at } p\,. \end{cases}$$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$ ✓

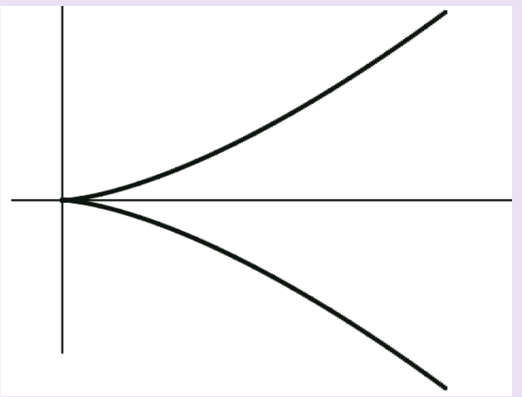
Consider $E/\mathbb{Z}_p : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.



$\tilde{E} : \tilde{y}^2 = (\tilde{x} - \tilde{\alpha}_1)(\tilde{x} - \tilde{\alpha}_2)(\tilde{x} - \tilde{\alpha}_3)$



$\tilde{E} : \tilde{y}^2 = (\tilde{x} - \tilde{\alpha}_1)(\tilde{x} - \tilde{\alpha}_2)^2$



$\tilde{E} : \tilde{y}^2 = (\tilde{x} - \tilde{\alpha}_1)^3$

Conductor exponents: minimal data

- $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$

- $N = \prod_p p^{f_p}$, where $f_p = \begin{cases} 0 & \text{if good,} \\ 1 & \text{if mult.,} \\ 2 & \text{if add. } (p \geq 5), \\ 2 + \delta_p, 0 \leq \delta_p \leq 6 & \text{if add. } (p = 2,3) \,. \end{cases}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$ ✗

Conductor exponents: minimal data

- $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$

- $N = \prod_p p^{f_p}$, where $f_p = \begin{cases} 0 & \text{if good,} \\ 1 & \text{if mult.,} \\ 2 & \text{if add. } (p \geq 5), \\ 2+\delta_p, 0 \leq \delta_p \leq 6 & \text{if add. } (p = 2,3)\,. \end{cases}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$

✓

Local root number: minimal data

- $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$
  - $N = \prod_p p^{f_p}$, where $f_p = \begin{cases} 0 & \text{if good,} \\ 1 & \text{if mult.,} \\ 2 & \text{if add. } (p \geq 5), \\ 2+\delta_p, 0 \leq \delta_p \leq 6 & \text{if add. } (p = 2,3). \end{cases}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$

✓

  - $w = -\prod_v w_v$, where $w_v = \begin{cases} 1 & \text{if good,} \\ -1 & \text{if split mult.,} \\ 1 & \text{if non-split mult.} \\ \{\pm 1\}, & \text{if add.,} \end{cases}$

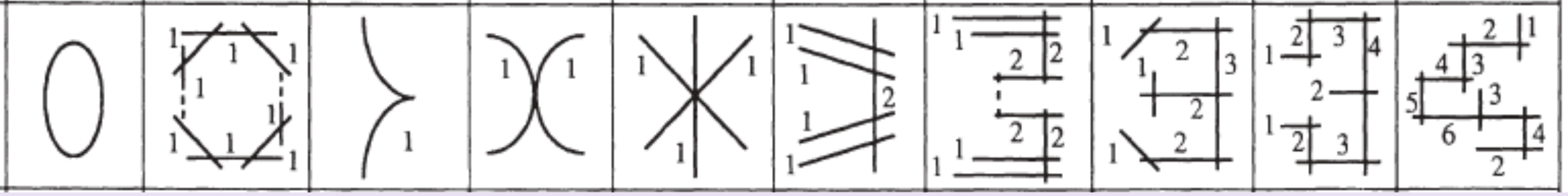
- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$
- p-adic distances

✓

Tamagawa numbers

- $$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^{rk_E}} = \frac{\Omega\ Ш(E/\mathbb{Q})\ (E/\mathbb{Q})\prod_p c_p}{|E_{tor}(\mathbb{Q})|^2}$$

Kodaira symbol	I_0	I_n $(n \geq 1)$	II	III	IV	I_0^*	I_n^* $(n \geq 1)$	IV*	III*	II*
Special fiber $\tilde{C}$ (The numbers indicate multiplicities)										

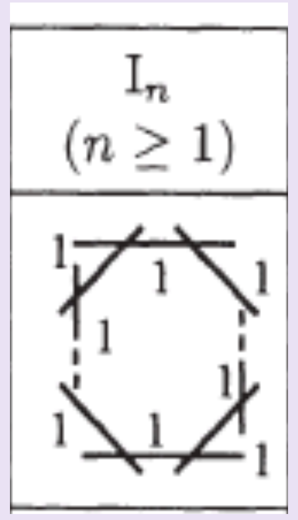


I_0	I_n	II	III
$c_p = 1$	$c_p = 1$	$c_p = 1$	$c_p = 1$
	$c_p = 2$		$c_p = 2$
	$c_p = n$		

Ref: The Arithmetic of Elliptic Curves, J.H. Silverman

Tamagawa numbers: minimal data

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{rk_E}} = \frac{\Omega\,\left|\text{Ш}(E/\mathbb{Q})\right|(E/\mathbb{Q})\prod_p c_p}{|E_{tor}(\mathbb{Q})|^2}$$



$c_p = 1$

$c_p = 2$

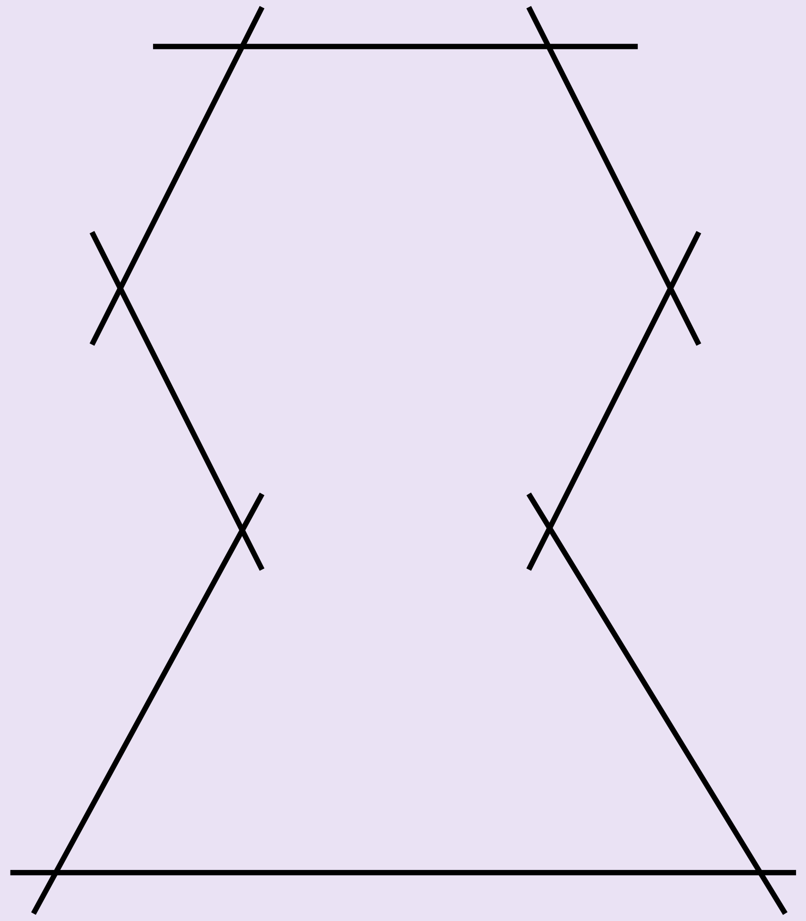
$c_p = n$

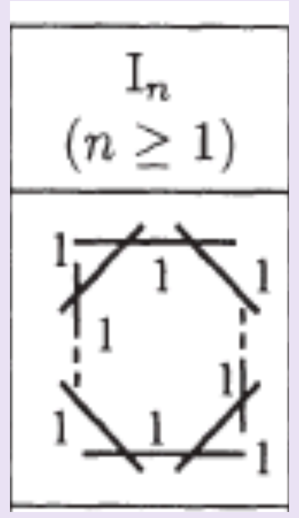
Ref: The Arithmetic of Elliptic Curves, J.H. Silverman

Tamagawa numbers: minimal data

- $E : y^2 = x(x-p^4)(x-1)$

- $y^2 = x(x-p^4)(x-1) \quad \Rightarrow \tilde{y}^2 = \tilde{x}^2(\tilde{x}-1) \quad \Rightarrow \tilde{y}^2 = (\tilde{x}-1)$
- $\begin{matrix} y_1 = yp \\ x_1 = xp \end{matrix} \quad \Rightarrow y_1^2 = x_1(x_1-p^3)(x_1p-1) \quad \Rightarrow \tilde{y}_1^2 = -\tilde{x}_1^2$
- $\begin{matrix} y_2 = y_1p \\ x_2 = x_1p \end{matrix} \quad \Rightarrow y_2^2 = x_2(x_2-p^2)(x_2p^2-1) \quad \Rightarrow \tilde{y}_2^2 = -\tilde{x}_2^2$
- $\begin{matrix} y_3 = y_2p \\ x_3 = x_2p \end{matrix} \quad \Rightarrow y_3^2 = x_3(x_3-p)(x_3p^3-1) \quad \Rightarrow \tilde{y}_3^2 = -\tilde{x}_1^3$
- $\begin{matrix} y_4 = y_3p \\ x_4 = x_3p \end{matrix} \quad \Rightarrow y_4^2 = x_4(x_4-1)(x_4p^4-1) \quad \Rightarrow \tilde{y}_4^2 = -\tilde{x}_4(\tilde{x}_4-1)$





- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- $v_p(\alpha_1 - \alpha_2)$

✓

$c_p = 8$

$c_p = 2$

L-functions of Elliptic Curves and local invariants

Let $E/\mathbb{Q}$ be an elliptic curve.

- $L(E,s) = \prod_p L_p(E,p^{-s})^{-1}$
- $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$
  - $\Lambda(E,s) = w \cdot \Lambda(E,2-s)$
- Birch and Swinnerton-Dyer conjecture
  - $\text{ord}_{s=1} L(E/\mathbb{Q},s) = rk(E/\mathbb{Q})$
- (Strong) Birch and Swinnerton-Dyer conjecture
  - $\lim_{s\to1} \frac{L(E,s)}{(s-1)^{rk_E}} = \frac{\Omega |Ш(E/\mathbb{Q})| R(E/\mathbb{Q}) \prod_p c_p}{|E_{tor}(\mathbb{Q})|^2}$

- $N = \prod p^{f_p}$
- $w = \prod_p w_p$
- $\prod_p c_p$

- $L_p(E,p^{-s})$
- f_p
- w_p
- c_p

L-functions of Elliptic Curves and local invariants

Let $E/\mathbb{Q}$ be an elliptic curve.

- $L_p(E, p^{-s})$
- f_p
- w_p
- c_p (semistable)

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$
- $v_p(\alpha_1 - \alpha_2)$

Extending to Hyperelliptic curves

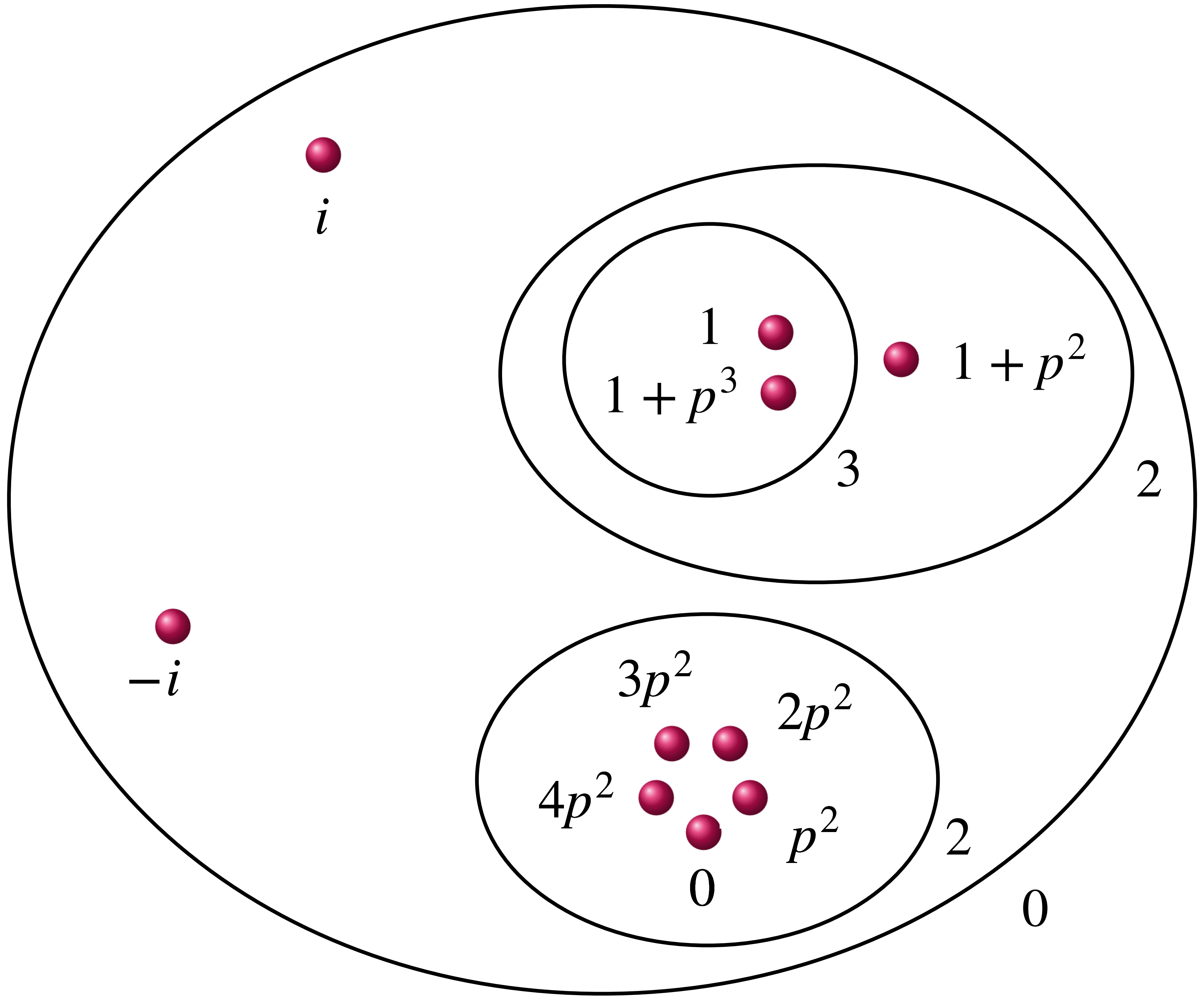
$$y^2 = x(x-p^2)(x-2p^2)(x-3p^2)(x-4p^2)(x^2+1)(x-1)(x-1-p^2)(x-1-p^3)$$

- $L_p(E, p^{-s})$
- f_p
- w_p
- c_p (semistable)

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$
- $v_p(\alpha_1 - \alpha_2)$



L-functions of Elliptic Curves and local invariants

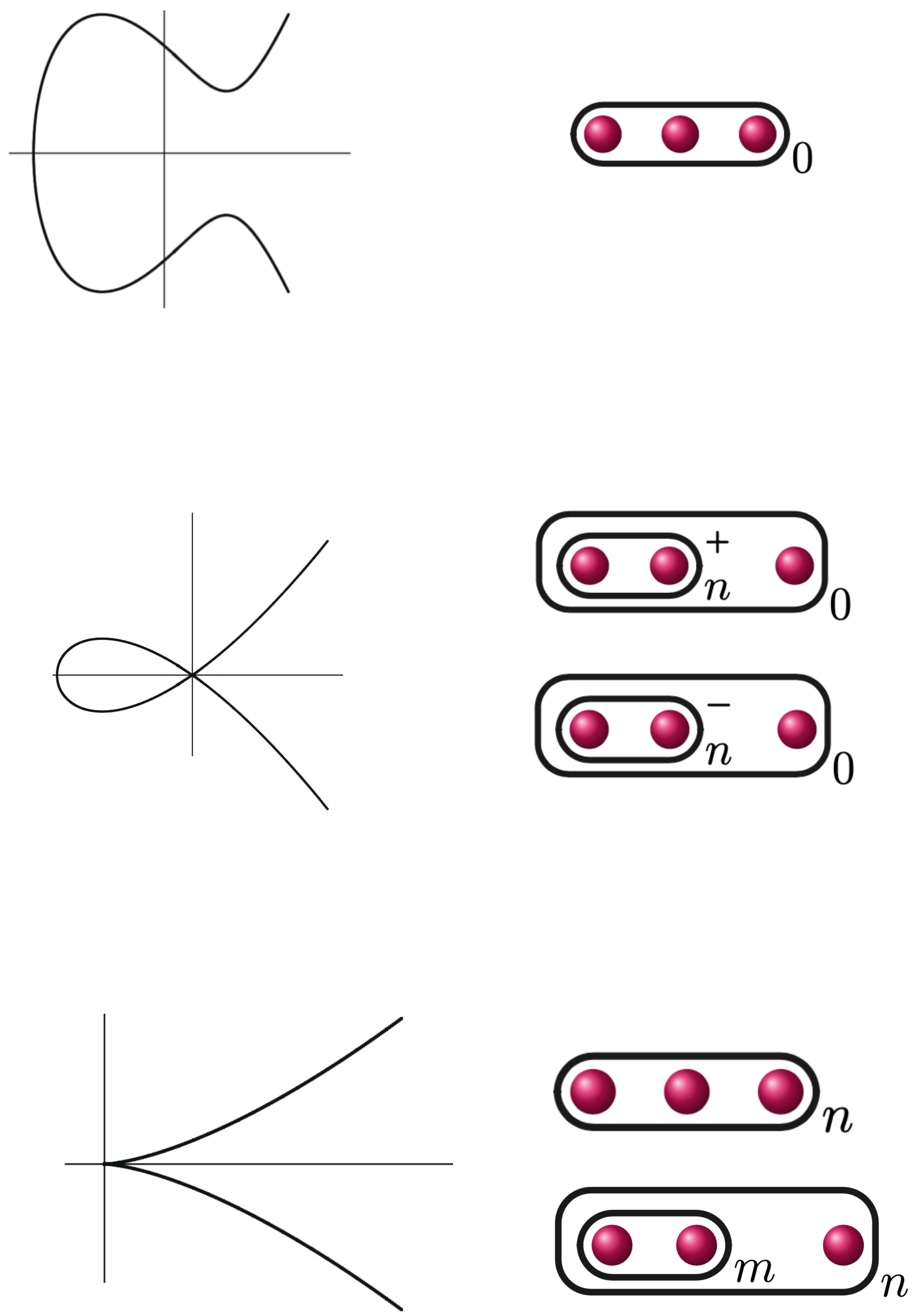
Let $E/\mathbb{Q}$ be an elliptic curve.

- $L_p(E, p^{-s})$
- f_p
- w_p
- c_p (semistable)

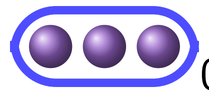
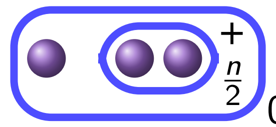
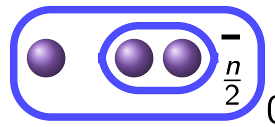
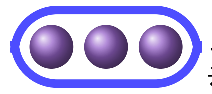
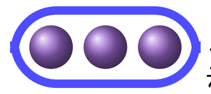
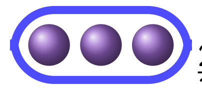
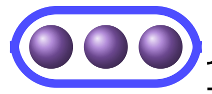
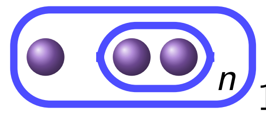
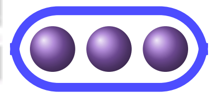
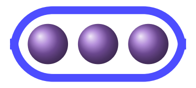
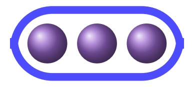
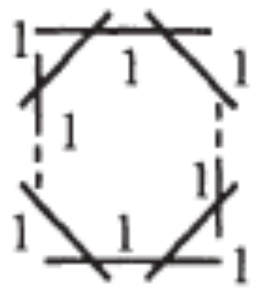
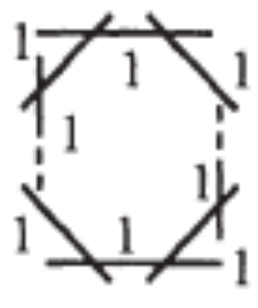
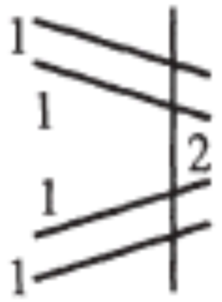
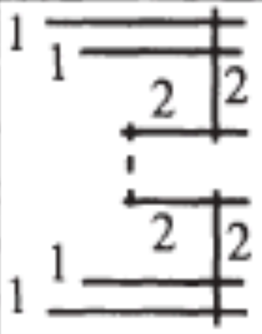
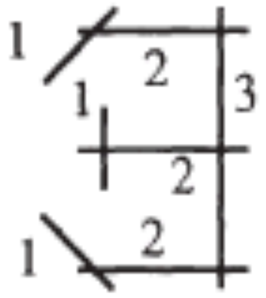
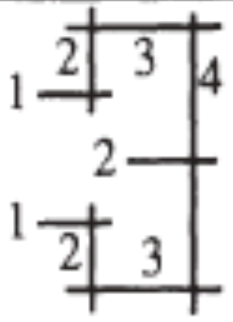
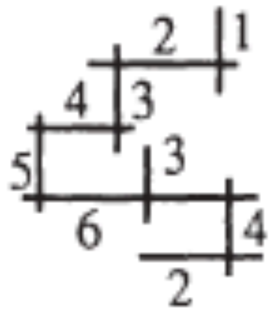
- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$

- $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$
- Galois action on $\{\alpha_1, \alpha_2, \alpha_3\}$
- $v_p(\alpha_1 - \alpha_2)$



Cluster pictures + Galois action on roots

Cluster Picture	 0	 $\frac{n}{2}^{+}$, 0	 $\frac{n}{2}^{-}$, 0	 $\frac{1}{3}$	 $\frac{1}{2}$	 $\frac{2}{3}$	 1	 n, 1	 $\frac{4}{3}$	 $\frac{3}{2}$	 $\frac{5}{3}$
Special fiber $\tilde{C}$ (The numbers indicate multiplicities)											
▷ $L_p(E, p^{-s})$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
▷ f_p	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
▷ w_p	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
▷ c_p	✓	✓	✓	✓	?	?	?	?	?	?	?

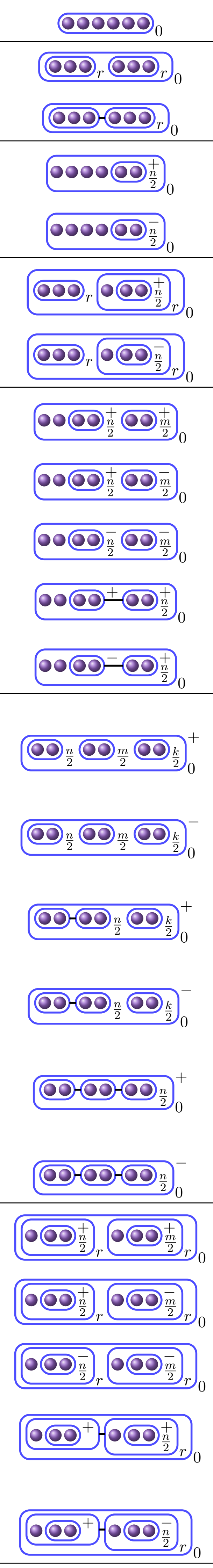
Ref: The Arithmetic of Elliptic Curves, J.H. Silverman

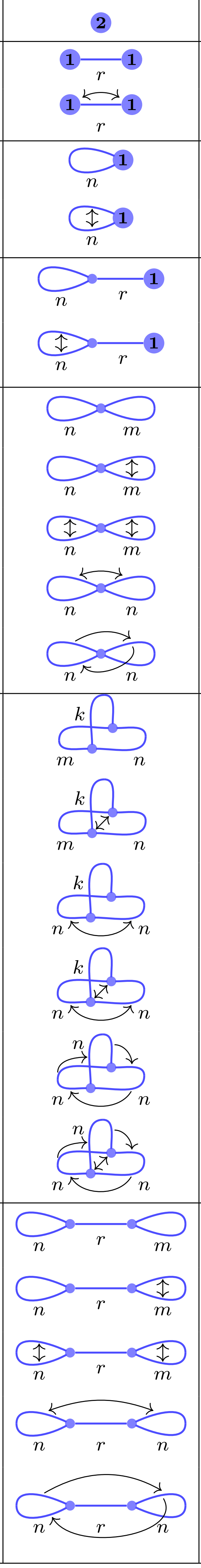
Hyperelliptic Curves over local fields ($p \neq 2$).

(Dokchitser-Dokchitser-M.-Morgan, 2022)

- Reduction type of curve and Jacobian + semistability criterion
- Regular model (semistable)
- Tamagawa Numbers (semistable) (Betts)
- Differentials (semistable) (Kunzweiler)
- Root numbers (tame) (Bisatt)
- SNC model (tame) (Faraggi-Nowell)
- Conductor exponent
- Galois representation ($\ell \neq p$)
- LMFDB (Best-van Bommel)

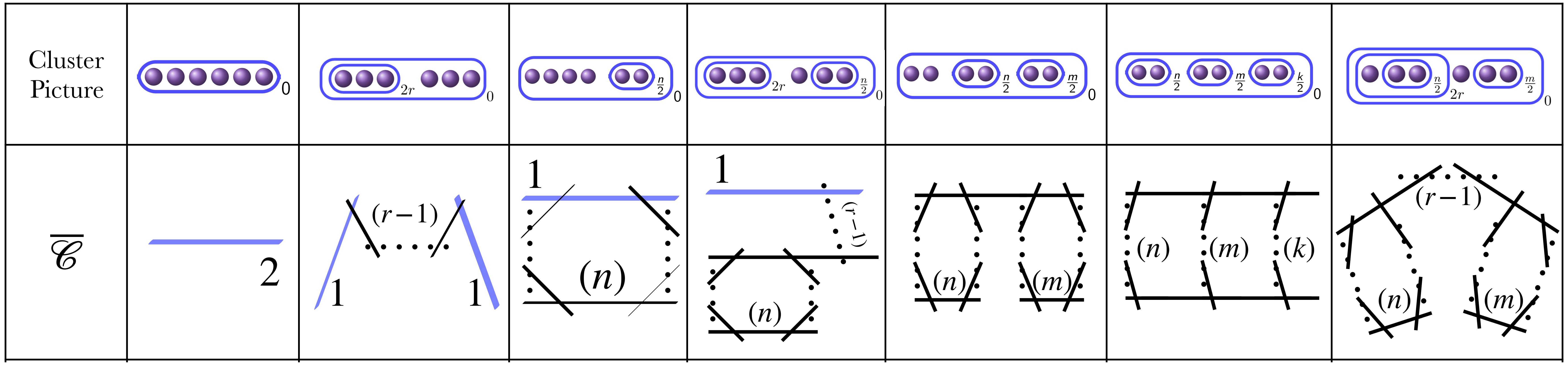
Semistable Hyperelliptic Curves, genus 2.





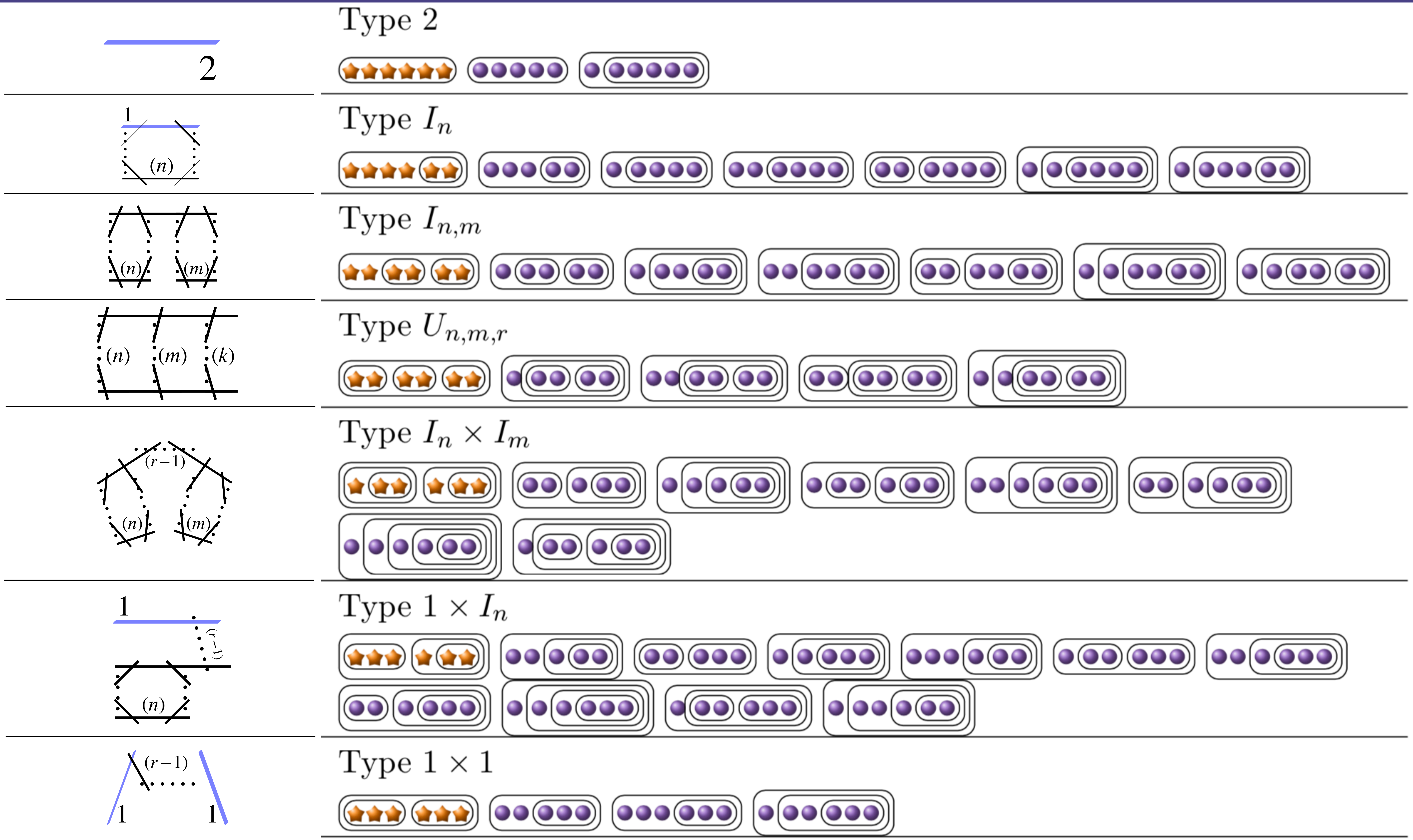
Type	Σ_C	$v(c_f)$	Υ_C	m_C	$H_1(\Upsilon_C,\mathbb{Z})$	n	w	c	Def	$v(\Delta_{min})$
2		0		1	–	0	+	1	+	0
$1\times_r 1$		$\bar r$		$r+1$	–	0	+	1	+	$12r$
$1\tilde\times_r 1$		$\bar r$		$r+1$	–	0	+	1	$(-)^r$	$12r+10\bar r$
I_n^+		0		n	$[1:n]$	1	−	n	+	n
I_n^-		0		n	$[2:n]$	1	+	$\tilde n$	+	n
$1\times_r \mathrm{I}_n^+$		$\bar r$		$n+r$	$[1:n]$	1	−	n	+	$12r+n$
$1\times_r \mathrm{I}_n^-$		$\bar r$		$n+r$	$[2:n]$	1	+	$\tilde n$	+	$12r+n$
$\mathrm{I}_{n,m}^{+,+}$		0		$n+m-1$	$[1.1:n,m]$	2	+	nm	+	$n+m$
$\mathrm{I}_{n,m}^{+,-}$		0		$n+m-1$	$[1.2_A:n,m]$	2	−	$n\tilde m$	+	$n+m$
$\mathrm{I}_{n,m}^{-,-}$		0		$n+m-1$	$[2.2:n,m]$	2	+	$\tilde n\tilde m$	+	$n+m$
$\mathrm{I}_{n\text{-}n}^{+}$		0		$2n-1$	$[1.2_B:n,n]$	2	−	n	+	$2n$
$\mathrm{I}_{n\text{-}n}^{-}$		0		$2n-1$	$[4:n]$	2	+	$\tilde n$	+	$2n$
$\mathrm{U}_{n,m,k}^{+}$		0		$n{+}m{+}k{-}1$	$[1.1:d,t/d]$	2	+	t	+	$n+m+k$
$\mathrm{U}_{n,m,k}^{-}$		0		$n{+}m{+}k{-}1$	$[2.2:d,t/d]$	2	+	$\widetilde{t/d}\cdot\tilde d$	$(-)^{nmk}$	$n+m+k$
$\mathrm{U}_{n\text{-}n,k}^{+}$		0		$2n+k-1$	$[1.2_B:n{+}2k,n]$	2	−	$n{+}2k$	+	$2n+k$
$\mathrm{U}_{n\text{-}n,k}^{-}$		0		$2n+k-1$	$[1.2_B:n,n{+}2k]$	2	−	n	$(-)^k$	$2n+k$
$\mathrm{U}_{n\text{-}n\text{-}n}^{+}$		0		$3n-1$	$[3:n]$	2	+	3	+	$3n$
$\mathrm{U}_{n\text{-}n\text{-}n}^{-}$		0		$3n-1$	$[6:n]$	2	+	1	$(-)^n$	$3n$
$\mathrm{I}_n^+\times_r \mathrm{I}_m^+$		$\bar r$		$n{+}m{+}r{-}1$	$[1.1:n,m]$	2	+	nm	+	$12r{+}n{+}m$
$\mathrm{I}_n^+\times_r \mathrm{I}_m^-$		$\bar r$		$n{+}m{+}r{-}1$	$[1.2_A:n,m]$	2	−	$n\tilde m$	+	$12r{+}n{+}m$
$\mathrm{I}_n^-\times_r \mathrm{I}_m^-$		$\bar r$		$n{+}m{+}r{-}1$	$[2.2:n,m]$	2	+	$\tilde n\tilde m$	+	$12r{+}n{+}m$
$\mathrm{I}_n^+\tilde\times_r \mathrm{I}_n$		$\bar r$		$2n+r-1$	$[1.2_B:n,n]$	2	−	n	$(-)^r$	$12r{+}2n{+}10\bar r$
$\mathrm{I}_n^-\tilde\times_r \mathrm{I}_n$		$\bar r$		$2n+r-1$	$[4:n]$	2	+	$\tilde n$	$(-)^r$	$12r{+}2n{+}10\bar r$

Semistable genus 2 curves



- Different special fibres correspond to different cluster pictures
- Several cluster picture correspond to same special fibre (change of variables, non-minimal)
  - Equivalent classes of cluster pictures (same special fibre)

Semistable genus 2 curves

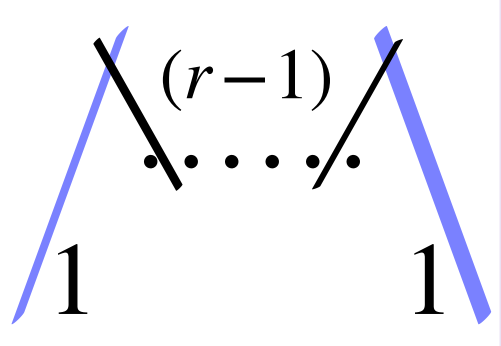


p-adic theories of curves

- Types of curves: Elliptic, hyperelliptic and general curves.
  - Algorithmic

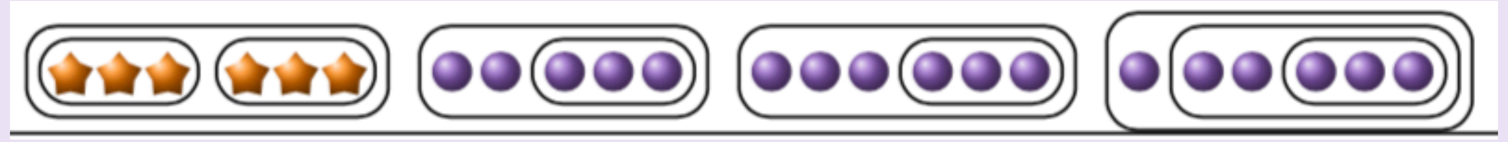
- Euler factors at primes of almost good reduction for genus 2 curves.
  - Joint with A. Sutherland.

- Let $C/\mathbb{Q}$ be a genus 2 curve.
  - p an odd prime of bad reduction for C and good reduction for $\mathrm{Jac}(C)$.
    - Almost good reduction

- 

- $L_p(C,T) = L_p(E_1,T)L_p(E_2,T)$

- $1 - a_{1,p}T + pT^2, \quad 1 - a_{2,p}T + pT^2$

- 

p-adic theories of curves

- Types of curves: Elliptic, hyperelliptic and general curves.
  - Computations in families

Conductor exponents for the Modular method.

- Joint with M. Azon, M. Curco Iranzo, M. Khawaja, D. Mocanu.

- Generalised Fermat equations: $x^r + y^q = z^p$.
- Conjecture: There are no non-trivial primitive solutions if $r, q, p \geq 3$.
- When $r = q = p$, it is Fermat's Last Theorem, proved using the "Modular Method".
- Darmon's Program: to each putative solution (a, b, c), attach a Frey variety.
  - One of the steps: compute the conductor exponents
- Signature (r, r, p). (Billerey-Chen-Dieulefait-Freitas)
  - $C_r(a,b) : y^2 = (ab)^{\frac{r-1}{2}} x \prod_{j=1}^{\frac{r-1}{2}} (x - \zeta_r^j - \zeta_r^{-j}) + b^r - a^r$

- Conductor exponents for the Modular method.
  - Joint with M. Azon, M. Curco Iranzo, M. Khawaja, D. Mocanu.

- Generalised Fermat equations: $x^r + y^q = z^p$.
- Conjecture: There are no non-trivial primitive solutions if $r, q, p \geq 3$.
- When $r = q = p$, it is Fermat's Last Theorem, proved using the "Modular Method".
- Darmon's Program: to each putative solution (a, b, c), attach a Frey variety.
  - One of the steps: compute the conductor exponents
- Signature (p, p, r). (Chen-Koutsianas)
  - $C_r^-(a,b,c) : y^2 = c^r \prod_{j=1}^{\frac{r-1}{2}} \left(\frac{x}{c}\right)^2 + \zeta_r^j - \zeta_r^{-j} - 2) - 2(a^p - b^p)$

Conductor exponents for the Modular method.

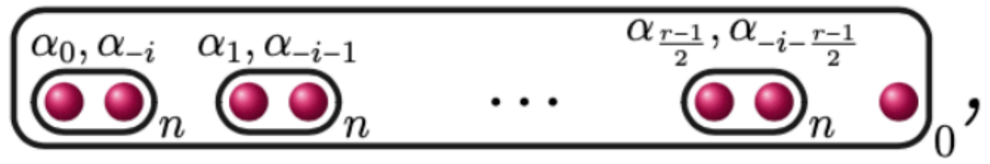
- Joint with M. Azon, M. Curco Iranzo, M. Khawaja, D. Mocanu.

- Generalised Fermat equations: $x^r + y^q = z^p$.
- Conjecture: There are no non-trivial primitive solutions if $r, q, p \geq 3$.
- When $r = q = p$, it is Fermat's Last Theorem, proved using the "Modular Method".
- Darmon's Program: to each putative solution (a, b, c), attach a Frey variety.
  - One of the steps: compute the conductor exponents
- Signature (p, p, r). (Chen-Koutsianas)
  - $C_r^+(a,b,c) : y^2 = (x+2c)\left(c^r \prod_{j=1}^{\frac{r-1}{2}} \left(\frac{x}{c}\right)^2 + \zeta_r^j - \zeta_r^{-j} - 2) - 2(a^p - b^p)\right)$

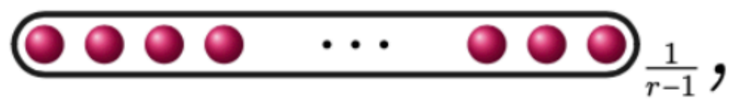
- Conductor exponents for the Modular method.
  - Joint with M. Azon, M. Curco Iranzo, M. Khawaja, D. Mocanu.

- Signature (r, r, p). (Billerey-Chen-Dieulefait-Freitas)
  - $C_r(a,b) : y^2 = (ab)^{\frac{r-1}{2}} x \prod_{j=1}^{\frac{r-1}{2}} (x - \zeta_r^j - \zeta_r^{-j}) + b^r - a^r$
    - Set of roots: $\{\zeta_r^i a + \zeta_r^{-i} b, \quad 0 \leq i \leq r-1\}$ + Galois action

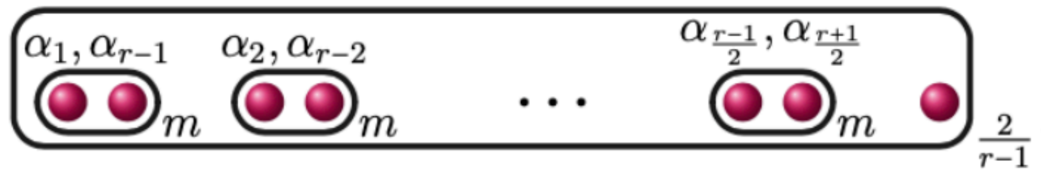
Theorem 3.4. *Let $q \in \mathbb{Z}$ be an odd prime such that $q \mid \Delta_{f_r(a,b)}$. Then the cluster pictures of $C_r(a,b)$ at q are as follows:*

(1) 

, if $q \neq r$ and $q \mid a^r + b^r$, where $n := v_q(a^r + b^r) \in \mathbb{Z}$,

(2) 

, if $q = r$ and $q \nmid a^r + b^r$,

(3) 

, if $q = r$ and $q \mid a^r + b^r$, where $m := v_r(a+b) - \frac{1}{r-1}$.

(1) If $q \neq r$, $q \mid a^r + b^r$, then $n_{C,q} = \frac{r-1}{2}$;
(2) If $q = r$, $q \nmid a^r + b^r$, then $n_{C,q} = r - 1$;
(3) If $q = r$, $q \mid a^r + b^r$, then $n_{C,q} = r - 1$.

p-adic theories of curves

- Types of curves: Elliptic, hyperelliptic and general curves.
  - Global application

p-Parity Conjecture for Elliptic curves over totally real fields.

Joint with H. Green

- Birch and Swinnerton-Dyer Conjecture: $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = rk(E/\mathbb{Q})$.
- $\Lambda(E/\mathbb{Q}, s) = w(E/\mathbb{Q}) \cdot \Lambda(E/\mathbb{Q}, 2-s)$.
- Parity conjecture: $(-1)^{rk(E/\mathbb{Q})} = w(E/\mathbb{Q})$.
  - For any prime p, p-Parity conjecture: $(-1)^{rk_p(E/\mathbb{Q})} = w(E/\mathbb{Q})$.
- Theorem

Let $E_1, E_2/K$ be elliptic curves over a number field. If $E_1[2] \simeq E_2[2]$ as Galois modules, then the 2-Parity conjecture holds for E_1/K if and only if it holds for E_2/K.

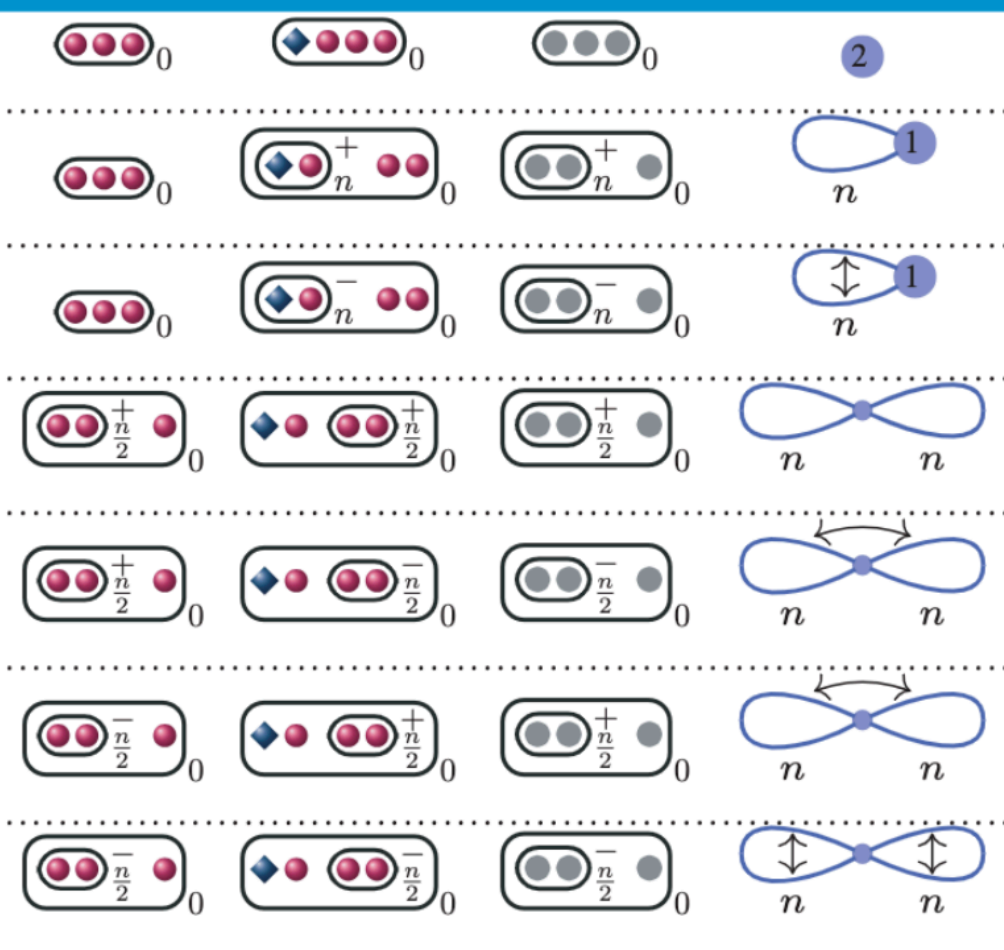
- Corollary

Let p be a prime and K be a totally real number field. Then the p-Parity conjecture holds for E/K.
(Dokchitser-Dokchitser, Nekovář: odd primes + $p = 2$ without CM).

p-Parity Conjecture for Elliptic curves over totally real fields.

Joint with H. Green

- Let K be a number field and $f(x) \in K[x]$ be a separable monic cubic polynomial.
  - $E: y^2 = f(x), \quad E': y^2 = xf(x), \quad C: y^2 = f(x^2).$
  - $(-1)^{rk_2(E/K)+rk_2(\mathrm{Jac}(E'/K))} = \prod_v \frac{c_v(E)c_v(E')}{c_v(C)} \overset{?}{=} \prod_v w_v(E/K)w_v(\mathrm{Jac}(E'/K)).$



types	$\Sigma_{E/\mathcal{K}}$	$\Sigma_{E'/\mathcal{K}}$	$\Sigma_{\mathrm{Jac}\,E'/\mathcal{K}}$	$\Upsilon_{C/\mathcal{K}}$	$c_{E/\mathcal{K}}$	$c_{\mathrm{Jac}\,E'/\mathcal{K}}$	$c_{\mathrm{Jac}\,C/\mathcal{K}}$	$\mu_{C/\mathcal{K}}$	$\lambda_{f,\mathcal{K}}$	$w_{E/\mathcal{K}}w_{\mathrm{Jac}\,E'/\mathcal{K}}$	$H_{f,\mathcal{K}}$
2					1	1	1	1	$+1$	$+1$	$+1$
1_n^+					1	$2n$	n	1	-1	-1	$+1$
1_n^-					1	2	$\tilde{n}$	1	$(-1)^n$	$+1$	$(-1)^n$
$\mathrm{I}_{n,n}^{+,+}$					n	n	n^2	1	$+1$	$+1$	$+1$
$\mathrm{I}_{n\sim n}^{+}(a)$					n	$\tilde{n}$	n	1	$(-1)^{n+1}$	-1	$(-1)^n$
$\mathrm{I}_{n\sim n}^{+}(b)$					$\tilde{n}$	n	n	1	$(-1)^{n+1}$	-1	$(-1)^n$
$\mathrm{I}_{n,n}^{-,-}$					$\tilde{n}$	$\tilde{n}$	$\tilde{n}^2$	1	$+1$	$+1$	$+1$

Notation: $\tilde{x} = 2$ if $2|x$ and $\tilde{x} = 1$ if $2 \nmid x$.

p-adic theories of curves

- Types of curves: Elliptic, hyperelliptic and general curves.
  - Global application
    - Local height on hyperelliptic curves and quadratic Chabauty (Betts, Duque-Rosero, Hashimoto, Spelier)

General curves and $p = 2$

- $p = 2$.
  - Dokchitser V.-Morgan (clusters at ordinary good red),
  - Yelton-Fiore,
  - Gehrunger-pink,
  - Wewers-Ossen,
  - …
- General curves.
  - algorithms
    - Dokchitser T., Dokchitser T.-Muselli,
    - …
  - Genus 3: Cayley Octads (van Bommel, Docking, Dokchitser V., Lercier, Lorenzo-Garcia)

Thank you!