Atelier PARI/GP 2022

Rank of certain elliptic surfaces over $\mathbb{Q}(T)$

Joint work with Francesco Battistoni and Sandro Bettin.

January 10, 2022

If you prefer an exercice

- Let $P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$.

$\rightsquigarrow$ Then $P(X) \in \mathbb{Q}[k, b_0, b_1][X]$ is irreducible.

Question

For all $k \in \mathbb{Z}^*$ and $b_0, b_1 \in \mathbb{Z}$, $P(X)$ is irreducible in $\mathbb{Q}[X]$?

Remark : false is we take

$$4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X + (b_0^2 - 20k^2).$$

If you prefer an exercice

- Let $P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$.

$\rightsquigarrow$ Then $P(X) \in \mathbb{Q}[k, b_0, b_1][X]$ is irreducible.

Question

For all $k \in \mathbb{Z}^*$ and $b_0, b_1 \in \mathbb{Z}$, $P(X)$ is irreducible in $\mathbb{Q}[X]$?

Remark : false is we take

$$4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X + (b_0^2 - 20k^2).$$

If you prefer an exercice

- Let $P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$.

$\rightsquigarrow$ Then $P(X) \in \mathbb{Q}[k, b_0, b_1][X]$ is irreducible.

Question

For all $k \in \mathbb{Z}^*$ and $b_0, b_1 \in \mathbb{Z}$, $P(X)$ is irreducible in $\mathbb{Q}[X]$?

Remark : false is we take

$$4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X + (b_0^2 - 20k^2).$$

If you prefer an exercice

- Let $P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$.

$\rightsquigarrow$ Then $P(X) \in \mathbb{Q}[k, b_0, b_1][X]$ is irreducible.

Question

For all $k \in \mathbb{Z}^*$ and $b_0, b_1 \in \mathbb{Z}$, $P(X)$ is irreducible in $\mathbb{Q}[X]$?

Remark : false is we take

$$4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X + (b_0^2 - 20k^2).$$

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $$\mathcal{F}: Y^2 = X^3 + a_2(T)X^2 + a_4(T)x + a_6(T), \text{ with } a_i(T) \in \mathbb{Z}[T],$$

  non-isotrivial.

  $\rightsquigarrow r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg a_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T)$, with $\alpha_i(T) \in \mathbb{Z}[T]$,

  non-isotrivial.

  $\rightsquigarrow r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T],$$

  non-isotrivial.

  $\rightsquigarrow r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T),$ with $\alpha_i(T) \in \mathbb{Z}[T]$,

  non-isotrivial.

  $\rightsquigarrow r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T)$, with $\alpha_i(T) \in \mathbb{Z}[T]$,

  non-isotrivial.

  $\rightsquigarrow r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T],$$

  non-isotrivial.

  $\rightsquigarrow$ $r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow$ $r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and Notations

- Family of elliptic curves: an elliptic curve over $\mathbb{Q}(T)$.

  $\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T)$, with $\alpha_i(T) \in \mathbb{Z}[T]$,

  non-isotrivial.

  $\rightsquigarrow$ $r \in \mathbb{N}$ the rank $\mathbb{Q}(T)$.

- Specialization: for all but finitely many $t \in \mathbb{Z}$, $\mathcal{F}(t)$ is an e. c. over $\mathbb{Q}$:

  $\rightsquigarrow$ $r(t)$ the rank of $\mathcal{F}(t)$ over $\mathbb{Q}$.

Goal: study $\mathcal{F}$ when $\deg \alpha_i(T) \leq 2$.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

- If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

- We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

- If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

- We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

• If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

• We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

- If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

- We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T),\ \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

- If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T),\ \text{ with } \deg \alpha_i(T) \leq 2.$$

- We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X),\ \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

- If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

- We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Motivations and notations

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \alpha_i(T) \in \mathbb{Z}[T].$$

• If $\deg \alpha_i(T) \leq 2$ then $\mathcal{F}$ is a rational elliptic surface.

Shioda-Tate's formula gives:

$$r_{\mathcal{F}/\overline{\mathbb{Q}}(T)} = 8 - \sum_v (m_v - 1),$$

where m_v is the number of irreducible components in v.

Here, we consider

$$\mathcal{F}\colon Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)x + \alpha_6(T), \text{ with } \deg \alpha_i(T) \leq 2.$$

• We write

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with } A, B, C \in \mathbb{Z}[X],$$

et $\deg A, B \leq 2$ et $\deg C - X^3 \leq 2$.

$\rightsquigarrow$ Using Nagao's formula, we obtain a close formula for r in function of A, B and C. And we find r points naturally.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \quad \text{with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \quad \text{with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \quad \text{with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \text{ with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \quad \text{with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral result

$$\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X), \quad \text{with} A, B, C \in \mathbb{Z}[X].$$

This gives

$$Y^2 = A(X)\left(T + \frac{B(X)}{2A(X)}\right)^2 - \frac{B^2(X) - 4A(X)C(X)}{4A(X)}$$

Observation

If $\rho \in \overline{\mathbb{Q}}$ is such that:

(i) ρ is a root of $\Delta := B^2(X) - 4A(X)C(X)$;

(ii) $A(\rho) = L^2(\rho) \in (\mathbb{Q}(\rho)^*)^2$;

Then

$$P(\rho) = \left(\rho, L(\rho)\left(T + \frac{B(\rho)}{2A(\rho)}\right)\right) \in \mathcal{F}(\mathbb{Q}(\rho)(T)).$$

$\rightsquigarrow$ Trace of $P(\rho)$ on $\mathcal{F}$ gives $P_{[\rho]} \in \mathcal{F}(\mathbb{Q}(T))$.

If $A(\rho) = B(\rho) = 0$ and $C(\rho) = L(\rho)^2$, consider $P(\rho) = (\rho, L(\rho))$.

Moral (but false) result

If $\gcd(A, B) = 1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho) = 0$ et $A(\rho) \in (\mathbb{Q}(\rho)^*)^2\}$.

False: if $A = k^2 \in \mathbb{Q}^*$ then for $n_\rho = \mathrm{ord}_\rho(B^2 - 4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho [P(\rho)] - d[O]$ is a divisor of $Y - kT - \frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A} = \mathrm{res}_Y(\Delta(Y), X^2 - A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A, B) = 1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho) = 0 \text{ et } \square(A(\rho)) = 1\} = \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*)$$

If $P(A)$ divides Δ^* for a P of degree 2 .

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho=\mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_{\rho} n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y-kT-\frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A}=\mathrm{res}_Y(\Delta(Y),X^2-A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A})-\Omega(\Delta^*)$$

if $P(A)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho]\colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho = \mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y - kT - \frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A} = \mathrm{res}_Y(\Delta(Y), X^2 - A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho]\colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - 2$$

If $P(X)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho=\operatorname{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_{\rho} n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y-kT-\frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A}=\operatorname{res}_Y(\Delta(Y),X^2-A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A})-\Omega(\Delta^*)$$

If $P(A)$ divides Δ^* for a P of degree 2 .

Moral (but false) result

If $\gcd(A, B) = 1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho) = 0$ et $A(\rho) \in (\mathbb{Q}(\rho)^*)^2\}$.

False: if $A = k^2 \in \mathbb{Q}^*$ then for $n_\rho = \mathrm{ord}_\rho(B^2 - 4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_{\rho} n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho [P(\rho)] - d[O]$ is a divisor of $Y - kT - \frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A} = \mathrm{res}_Y(\Delta(Y), X^2 - A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A, B) = 1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho) = 0 \text{ et } \square(A(\rho)) = 1\} = \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - 2$$

If $P(A)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho)=0 \text{ et } A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho = \mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y - kT - \frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A} = \mathrm{res}_Y(\Delta(Y), X^2 - A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - 2$$

if $P(A)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho]\colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho=\mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y - kT - \frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A} = \mathrm{res}_Y(\Delta(Y), X^2 - A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho]\colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*)$$

If $P(X)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho] \colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho=\mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y-kT-\frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A}=\mathrm{res}_Y(\Delta(Y),X^2-A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho] \colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A})-\Omega(\Delta^*) - 2$$

If $P(A)$ divides Δ^* for a P of degree 2.

Moral (but false) result

If $\gcd(A,B)=1$ then $r \asymp \sharp\{[\rho]\colon \Delta(\rho)=0$ et $A(\rho)\in(\mathbb{Q}(\rho)^*)^2\}$.

False: if $A=k^2\in\mathbb{Q}^*$ then for $n_\rho=\mathrm{ord}_\rho(B^2-4k^2C)$ we have

$$\sum_{[\rho]} n_\rho P_{[\rho]} = \sum_\rho n_\rho P(\rho) = 0$$

indeed $\sum_\rho n_\rho[P(\rho)] - d[O]$ is a divisor of $Y-kT-\frac{B(X)}{2k}$.

Notations:

- Δ^* is the radical of Δ (so $\Delta^*$is squarefree) ;
- $\Omega(\Delta)$ is the number of irr. factors of Δ with multiplicities ;
- $M_{\Delta,A}=\mathrm{res}_Y(\Delta(Y),X^2-A(Y))$;
- $\square(\cdot)$ is the characteristic non-zeros squares where $\cdot$ naturally lives.

Proposition

If $\gcd(A,B)=1$ then

$$\sharp\{[\rho]\colon \Delta^*(\rho)=0 \text{ et } \square(A(\rho))=1\} = \Omega(M_{\Delta^*,A})-\Omega(\Delta^*)-2$$

If $P(A)$ divides Δ^* for a P of degree 2.

The theorem

• Nagao's conjecture, proven by Rosen and Silverman for rational elliptic surfaces, gives:

$$r = \lim_{Q\to\infty} \frac{\log Q}{Q} \sum_{p\leq Q} \frac{1}{p} \sum_{x \bmod p} \sum_{t \bmod p} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right).$$

Using

- $\rightsquigarrow$ Weil's bound;
- $\rightsquigarrow$ Arithmetic;
- $\rightsquigarrow$ Resultant;
- $\rightsquigarrow$ Calculation;

we generalize the work of Arms, Lozano-Robledo and Miller and we obtain

The theorem

• Nagao's conjecture, proven by Rosen and Silverman for rational elliptic surfaces, gives:

$$r = \lim_{Q\to\infty} \frac{\log Q}{Q} \sum_{p\le Q} \frac{1}{p} \sum_{x \bmod p} \sum_{t \bmod p} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p} \right).$$

Using

$\rightsquigarrow$ Weil's bound;

$\rightsquigarrow$ Arithmetic;

$\rightsquigarrow$ Resultant;

$\rightsquigarrow$ Calculation;

we generalize the work of Arms, Lozano-Robledo and Miller and we obtain

The theorem

• Nagao's conjecture, proven by Rosen and Silverman for rational elliptic surfaces, gives:

$$r = \lim_{Q\to\infty} \frac{\log Q}{Q} \sum_{p\leq Q} \frac{1}{p} \sum_{x \bmod p} \sum_{t \bmod p} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p} \right).$$

Using

- $\rightsquigarrow$ Weil's bound;
- $\rightsquigarrow$ Arithmetic;
- $\rightsquigarrow$ Resultant;
- $\rightsquigarrow$ Calculation;

we generalize the work of Arms, Lozano-Robledo and Miller and we obtain

Theorem

$$
\begin{aligned}
r &= \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - \square(A) - \Upsilon_{\Delta,A} \\
&- \left(2\deg(\gcd(A,B)^*) - \Omega(M_{\gcd(A,B)^*,C}) + \Upsilon_{\gcd(A,B),C}\right) \\
&- \left(2\deg(\gcd(A,B,C)^*) - \Omega(\gcd(A,B,C)^*)\right)
\end{aligned}
$$

where $\Upsilon_{P,Q}$ small, explicit and often 0.

$\rightsquigarrow$ Algorithmic and explicit result

Corollary

If $A = 0$ then
$r = \Omega(M_{B^*,C}) - \Omega(B^*) - 2\deg(\gcd(B,C)^*) + \Omega(\gcd(B,C)^*) - \Upsilon_{B,C}$.

If $A \in (\mathbb{Q}^*)^2$ then $r = \Omega(\Delta^*) - 1$.

We have $r \leq \deg(\Delta^*) \leq 5$ and all the rank are possible.

Theorem

$$
\begin{aligned}
r &= \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - \Box(A) - \Upsilon_{\Delta,A} \\
&- \left(2\deg(\gcd(A,B)^*) - \Omega(M_{\gcd(A,B)^*,C}) + \Upsilon_{\gcd(A,B),C}\right) \\
&- \left(2\deg(\gcd(A,B,C)^*) - \Omega(\gcd(A,B,C)^*)\right)
\end{aligned}
$$

where $\Upsilon_{P,Q}$ small, explicit and often 0.

$$
\Upsilon_{P_1,P_2} := \begin{cases}
\delta_t(1-\delta_u+\Box(u)-\Box(uD_{P_1})) & \text{si } \deg(P_1)=2 \text{ and } P_2(X)=Q(X)P_1(X)+(tX+u) \text{ with } t,u\in\mathbb{Q},\ 0\neq Q\in\mathbb{Q}[X]\ ; \\
\Upsilon_{U,W} + 2 - \Omega(M_{U,W}) + \Omega(U(x^2)) - \Omega\left(U\left(\frac{x^2-D_{P_2}}{4s}\right)\right) & \text{si } \deg(P_1)=4,\ \deg(P_2)=2 \text{ and } P_1(X)=U(P_2(X)) \text{ for a } U\in\mathbb{Q}[X] \text{ and where } W(X):=4sX^2+D_{P_2}X\ ; \\
0 & \text{otherwise.}
\end{cases}
$$

with D_P the discriminant of P and s leading coefficient of P_2.

$\rightsquigarrow$ Algorithmic and explicit result

Corollary

If $A = 0$ then

$r = \Omega(M_{B^*,C}) - \Omega(B^*) - 2\deg(\gcd(B,C)^*) + \Omega(\gcd(B,C)^*) - \Upsilon_{B,C}.$

Theorem

$$
\begin{aligned}
r &= \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - \square(A) - \Upsilon_{\Delta,A} \\
&- (2\deg(\gcd(A,B)^*) - \Omega(M_{\gcd(A,B)^*,C}) + \Upsilon_{\gcd(A,B),C}) \\
&- (2\deg(\gcd(A,B,C)^*) - \Omega(\gcd(A,B,C)^*))
\end{aligned}
$$

where $\Upsilon_{P,Q}$ small, explicit and often 0.

$\rightsquigarrow$ Algorithmic and explicit result

Corollary

If $A = 0$ then
$r = \Omega(M_{B^*,C}) - \Omega(B^*) - 2\deg(\gcd(B,C)^*) + \Omega(\gcd(B,C)^*) - \Upsilon_{B,C}$.

If $A \in (\mathbb{Q}^*)^2$ then $r = \Omega(\Delta^*) - 1$.

We have $r \leq \deg(\Delta^*) \leq 5$ and all the rank are possible.

Theorem

$$\begin{aligned} r &= \Omega(M_{\Delta^*,A}) - \Omega(\Delta^*) - \Box(A) - \Upsilon_{\Delta,A} \\ &- (2\deg(\gcd(A,B)^*) - \Omega(M_{\gcd(A,B)^*,C}) + \Upsilon_{\gcd(A,B),C}) \\ &- (2\deg(\gcd(A,B,C)^*) - \Omega(\gcd(A,B,C)^*)) \end{aligned}$$

where $\Upsilon_{P,Q}$ small, explicit and often 0.

$\rightsquigarrow$ Algorithmic and explicit result

Corollary

If $A = 0$ then
$r = \Omega(M_{B^*,C}) - \Omega(B^*) - 2\deg(\gcd(B,C)^*) + \Omega(\gcd(B,C)^*) - \Upsilon_{B,C}$.

If $A \in (\mathbb{Q}^*)^2$ then $r = \Omega(\Delta^*) - 1$.

We have $r \leq \deg(\Delta^*) \leq 5$ and all the rank are possible.

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$
\begin{aligned}
A(X) &= X(X-1) + k^2, \\
2(b_1+b_2)(m_3^2-1)^2 B(X) &= 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2\big)X^2 + \\
&\quad 2\big((m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)X + \\
&\quad -4(m_3^4 + 2m_3^2 + 1)k^4 - 8(m_3^3 + m_3)k^3 + \\
&\quad 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2 - 2m_3^2\big)k^2 + \\
&\quad -\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big) \\
C(X) &= \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},
\end{aligned}
$$

where $r_3 = \frac{2m_3k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$
\begin{aligned}
p &= 4(m_3^4 + 2m_3^2 + 1)k^4 + 8(m_3^3 + m_3)k^3 + 4m_3^2k^2 \\
q &= -2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)k + \\
&\quad + (m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2.
\end{aligned}
$$

We have $A(r_i) = \left(\dfrac{(1+m_i^2)k + m_i}{1 - m_i^2}\right)^2$.

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$A(X) = X(X-1) + k^2,$$

$$\begin{aligned} 2(b_1+b_2)(m_3^2-1)^2 B(X) = {} & 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2\big)X^2 + \\ & 2\big((m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)X + \\ & -4(m_3^4 + 2m_3^2 + 1)k^4 - 8(m_3^3 + m_3)k^3 + \\ & 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2 - 2m_3^2\big)k^2 + \\ & -\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big) \end{aligned}$$

$$C(X) = \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},$$

where $r_3 = \frac{2m_3k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$\begin{aligned} p &= 4(m_3^4 + 2m_3^2 + 1)k^4 + 8(m_3^3 + m_3)k^3 + 4m_3^2k^2 \\ q &= -2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)k + \\ &\quad + (m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2. \end{aligned}$$

We have $A(r_i) = \left(\dfrac{(1+m_i^2)k + m_i}{1-m_i^2}\right)^2.$

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$
\begin{aligned}
A(X) &= X(X-1) + k^2, \\
2(b_1+b_2)(m_3^2-1)^2 B(X) &= 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2\big)X^2 + \\
&\quad 2\big((m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)X + \\
&\quad -4(m_3^4+2m_3^2+1)k^4 - 8(m_3^3+m_3)k^3 + \\
&\quad 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2 - 2m_3^2\big)k^2 + \\
&\quad -\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)
\end{aligned}
$$

$$C(X) = \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},$$

where $r_3 = \frac{2m_3k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$
\begin{aligned}
p &= 4(m_3^4+2m_3^2+1)k^4 + 8(m_3^3+m_3)k^3 + 4m_3^2k^2 \\
q &= -2\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)k + \\
&\quad + (m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2.
\end{aligned}
$$

We have $A(r_i) = \left(\frac{(1+m_i^2)k+m_i}{1-m_i^2}\right)^2$.

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$
\begin{aligned}
A(X) &= X(X-1) + k^2,\\
2(b_1+b_2)(m_3^2-1)^2 B(X) &= 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2\big)X^2 +\\
&\quad 2\big((m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)X +\\
&\quad -4(m_3^4+2m_3^2+1)k^4 - 8(m_3^3+m_3)k^3 +\\
&\quad 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2 - 2m_3^2\big)k^2 +\\
&\quad -\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)\\
C(X) &= \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},
\end{aligned}
$$

where $r_3 = \frac{2m_3k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$
\begin{aligned}
p &= 4(m_3^4+2m_3^2+1)k^4 + 8(m_3^3+m_3)k^3 + 4m_3^2k^2\\
q &= -2\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)k +\\
&\quad + (m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2.
\end{aligned}
$$

We have $A(r_i) = \left(\frac{(1+m_i^2)k+m_i}{1-m_i^2}\right)^2$.

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$
\begin{aligned}
A(X) &= X(X-1) + k^2, \\
2(b_1+b_2)(m_3^2-1)^2 B(X) &= 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2\big)X^2 + \\
&\quad 2\big((m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)X + \\
&\quad -4(m_3^4+2m_3^2+1)k^4 - 8(m_3^3+m_3)k^3 + \\
&\quad 2\big((m_3^4-2m_3^2+1)b_2^2 + (m_3^4-2m_3^2+1)b_1b_2 - 2m_3^2\big)k^2 + \\
&\quad -\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big) \\
C(X) &= \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},
\end{aligned}
$$

where $r_3 = \frac{2m_3k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$
\begin{aligned}
p &= 4(m_3^4+2m_3^2+1)k^4 + 8(m_3^3+m_3)k^3 + 4m_3^2k^2 \\
q &= -2\big((m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2\big)k + \\
&\quad + (m_3^4-2m_3^2+1)b_2^2 + 2(m_3^4-2m_3^2+1)b_1b_2 + (m_3^4-2m_3^2+1)b_1^2.
\end{aligned}
$$

We have $A(r_i) = \left(\frac{(1+m_i^2)k + m_i}{1-m_i^2}\right)^2$.

Rank 5 example: $Y^2 = A(X)T^2 + B(X)T + C(X)$

$$A(X) = X(X-1) + k^2,$$

$$\begin{aligned} 2(b_1+b_2)(m_3^2-1)^2 B(X) = {} & 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2\big)X^2 + \\ & 2\big((m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)X + \\ & -4(m_3^4 + 2m_3^2 + 1)k^4 - 8(m_3^3 + m_3)k^3 + \\ & 2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + (m_3^4 - 2m_3^2 + 1)b_1 b_2 - 2m_3^2\big)k^2 + \\ & -\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big) \end{aligned}$$

$$C(X) = \frac{B(X)^2 + 4X(X-1)(X-r_3)(X-r_4)(X-r_5)}{4A(X)},$$

where $r_3 = \frac{2m_3 k+1}{1-m_3^2}$, $r_4 = 1 - r_3$ and $r_5 = \frac{2m_5 k+1}{1-m_5^2}$.

With $m_5 = \frac{q-p}{q+p}$ and

$$\begin{aligned} p &= 4(m_3^4 + 2m_3^2 + 1)k^4 + 8(m_3^3 + m_3)k^3 + 4m_3^2 k^2 \\ q &= -2\big((m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2\big)k + \\ &\quad + (m_3^4 - 2m_3^2 + 1)b_2^2 + 2(m_3^4 - 2m_3^2 + 1)b_1 b_2 + (m_3^4 - 2m_3^2 + 1)b_1^2. \end{aligned}$$

We have $A(r_i) = \left(\dfrac{(1+m_i^2)k + m_i}{1-m_i^2}\right)^2$.

Application: $A = k^2$, $\mathcal{F}: Y^2 = k^2T^2 + BT + C$

- $r = \Omega((B^2 - 4k^2C)^*) - 1$.

Corollary

Let $\mathcal{C}: Y^2 = C(X)$ an elliptic curve defined over $\mathbb{Q}$ such that $\mathcal{C}(\mathbb{Q}) = \{O\}$. Then, for all B of degree ≤ 2 and all $k \in \mathbb{Z}^*$, the polynomial $B^2 - 4k^2C$ is a power of an irreducible polynomial.

- $\mathcal{C}: Y^2 = X^3 + X + 5$ has rank 0 and no nonzero torsion point, so

$$P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$$

is irreducible for all $k \in \mathbb{Z}^*$ et $b_0, b_1 \in \mathbb{Z}$.

Application: $A = k^2$, $\mathcal{F}\colon Y^2 = k^2T^2 + BT + C$

- $r = \Omega((B^2 - 4k^2C)^*) - 1$.

Corollary

Let $\mathcal{C}\colon Y^2 = C(X)$ an elliptic curve defined over $\mathbb{Q}$ such that $C(\mathbb{Q}) = \{O\}$. Then, for all B of degree ≤ 2 and all $k \in \mathbb{Z}^*$, the polynomial $B^2 - 4k^2C$ is a power of an irreducible polynomial.

- $\mathcal{C}\colon Y^2 = X^3 + X + 5$ has rank 0 and no nonzero torsion point, so

$$P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$$

is irreducible for all $k \in \mathbb{Z}^*$ et $b_0, b_1 \in \mathbb{Z}$.

Application: $A = k^2$, $\mathcal{F}\colon Y^2 = k^2T^2 + BT + C$

- $r = \Omega((B^2 - 4k^2C)^*) - 1$.

Corollary

Let $\mathcal{C}\colon Y^2 = C(X)$ an elliptic curve defined over $\mathbb{Q}$ such that $C(\mathbb{Q}) = \{O\}$. Then, for all B of degree ≤ 2 and all $k \in \mathbb{Z}^*$, the polynomial $B^2 - 4k^2C$ is a power of an irreducible polynomial.

- $\mathcal{C}\colon Y^2 = X^3 + X + 5$ has rank 0 and no nonzero torsion point, so

$$P(X) = 4k^2X^3 - b_1^2X^2 - (2b_0b_1 - 4k^2)X - (b_0^2 - 20k^2)$$

is irreducible for all $k \in \mathbb{Z}^*$ et $b_0, b_1 \in \mathbb{Z}$.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E : Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F} : Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F} : Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E\colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E\colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E\colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E \colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F} \colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F} \colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E\colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.

Application: finding rank and rational points.

Fact

If $P \in \mathcal{F}(\mathbb{Q}(T))$, we can compute the trace P efficiently (Thanks to Nicolas Mascot).

Let

$$E\colon Y^2 = C(X) = X^3 + a_2X^2 + a_1X + a_0$$

an elliptic curve over $\mathbb{Q}$.

$\rightsquigarrow$ Search $A, B \in \mathbb{Q}[X]$ st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank $r \geq 1$ and compute a point P.

$\rightsquigarrow$ Take $T = 0$. Generalization of brute force search (take $A = 0$ and $B = b_1X + b_0$).

Variant: if we know $(x_0, y_0) \in E(\mathbb{Q})$, search $A, B \in \mathbb{Q}[X]$ on the form

$$\begin{aligned} A &= (a_1X + a_0)^2 \\ B &= (X - x_0)(b_1X + b_0) + 2(a_1x_0 + a_0)y_0 \end{aligned}$$

st $\mathcal{F}\colon Y^2 = A(X)T^2 + B(X)T + C(X)$ has rank ≥ 2.