Du triangle rectangle à la courbe elliptique

Coline Wiatrowski

Colloque Inter'Actions 2019 - Bordeaux

20 mai 2019

Le problème des nombres congruents

Les courbes elliptiques

Les fonctions L et la conjecture de Birch et Swinnerton-Dyer

Retour aux nombres congruents

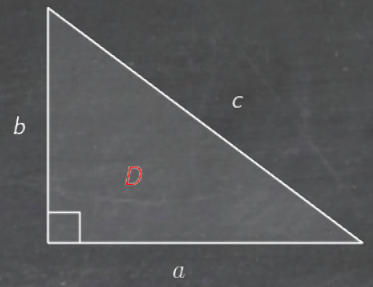
Le problème des nombres congruents

Soit D un entier sans facteur carré.

Définition

D est congruent s'il existe $a, b, c \in \mathbb{Q}$ tels que

- $a^2 + b^2 = c^2$,
- $D = \frac{ab}{2}$.

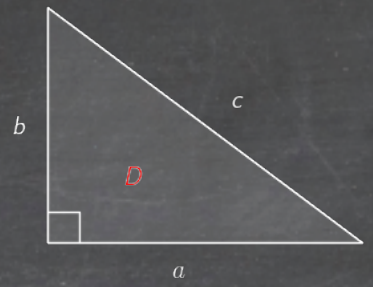


Soit D un entier sans facteur carré.

Définition

D est congruent s'il existe $a, b, c \in \mathbb{Q}$ tels que

- $a^2 + b^2 = c^2$,
- $D = \frac{ab}{2}$.



Exemple

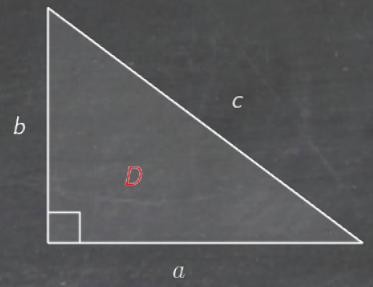
- 6 est congruent : $(a, b, c) = (3, 4, 5)$

Soit D un entier sans facteur carré.

Définition

D est congruent s'il existe $a, b, c \in \mathbb{Q}$ tels que

- $a^2 + b^2 = c^2$,
- $D = \frac{ab}{2}$.



Exemple

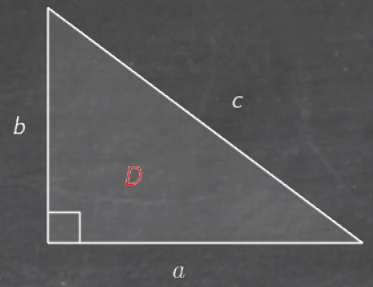
- 6 est congruent : $(a, b, c) = (3, 4, 5)$
- 5 est congruent : $(a, b, c) = (\frac{9}{6}, \frac{40}{6}, \frac{41}{6})$

Soit D un entier sans facteur carré.

Définition

D est congruent s'il existe $a, b, c \in \mathbb{Q}$ tels que

- $a^2 + b^2 = c^2$,
- $D = \frac{ab}{2}$.



Exemple

- 6 est congruent : $(a, b, c) = (3, 4, 5)$
- 5 est congruent : $(a, b, c) = (\frac{9}{6}, \frac{40}{6}, \frac{41}{6})$
- 157 est congruent :
  $a = \frac{6803298487826435051217540}{411340519227716149383203}$, $b = \frac{41134051922771614938320 3}{21666555693714761309610}$,
  $c = \frac{224403517704336969924557513090674863160948472041}{89123322689288595880255351789671635700164808 30}$

Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ a une solution dans $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.

Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ a une solution dans $(\mathbb{Q} \cap]-1; 0[) \times \mathbb{Q}^\times$.

Soit $a, b, c \in \mathbb{Q}$. Posons $u = \frac{a}{c}$ et $v = \frac{b}{c}$.

$$a^2 + b^2 = c^2 \quad \Leftrightarrow \quad u^2 + v^2 = 1$$

Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ a une solution dans $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.

Soit $a, b, c \in \mathbb{Q}$. Posons $u = \frac{a}{c}$ et $v = \frac{b}{c}$.

$$\begin{aligned} a^2 + b^2 = c^2 &\Leftrightarrow u^2 + v^2 = 1 \\ &\Leftrightarrow \exists t \in \mathbb{Q} \cap]0;1[\text{ tel que } u = \tfrac{1-t^2}{1+t^2} \text{ et } v = \tfrac{2t}{1+t^2} \\ &\Leftrightarrow \exists t \in \mathbb{Q} \cap]0;1[\text{ tel que } a = \tfrac{1-t^2}{1+t^2}c \text{ et } b = \tfrac{2t}{1+t^2}c \end{aligned}$$

($\Rightarrow$) On pose $x = -t$ et $y = \frac{1+t^2}{c}$.

($\Leftarrow$) On pose $a = \frac{1-x^2}{y}$, $b = \frac{-2x}{y}$, $c = \frac{1+x^2}{y}$.

Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ a une solution dans $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.

Soit $a, b, c \in \mathbb{Q}$. Posons $u = \frac{a}{c}$ et $v = \frac{b}{c}$.

$$\begin{aligned} a^2 + b^2 = c^2 &\Leftrightarrow u^2 + v^2 = 1 \\ &\Leftrightarrow \exists t \in \mathbb{Q} \cap]0;1[\text{ tel que } u = \tfrac{1-t^2}{1+t^2} \text{ et } v = \tfrac{2t}{1+t^2} \\ &\Leftrightarrow \exists t \in \mathbb{Q} \cap]0;1[\text{ tel que } a = \tfrac{1-t^2}{1+t^2}c \text{ et } b = \tfrac{2t}{1+t^2}c \end{aligned}$$

($\Rightarrow$) On pose $x = -t$ et $y = \frac{1+t^2}{c}$.

($\Leftarrow$) On pose $a = \frac{1-x^2}{y}$, $b = \frac{-2x}{y}$, $c = \frac{1+x^2}{y}$.

Exemple

Fermat : 1 n'est pas congruent.

Les courbes elliptiques

Définition

Soit K un corps.

Une courbe elliptique sur K est une courbe d'équation $y^2 = P(x)$ avec $P \in K[X]$ de degré 3 sans racine double.

On note $E(K) = \left\{(x; y) \in K^2, y^2 = P(x)\right\}$,

et $\overline{E}(K) = E(K) \cup \{\infty\}$.

$$E : y^2 = x^3 - x + 1$$

Définition

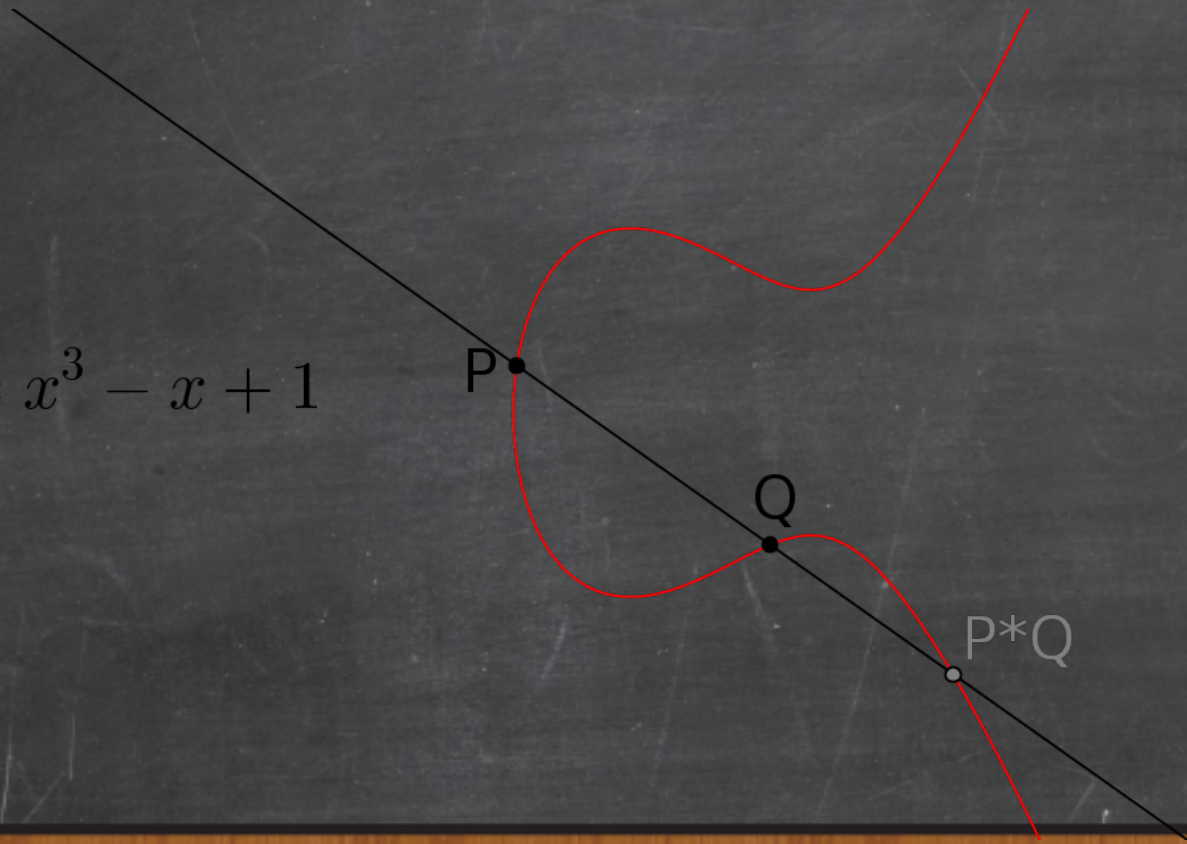
Soit K un corps.

Une courbe elliptique sur K est une courbe d'équation $y^2 = P(x)$ avec $P \in K[X]$ de degré 3 sans racine double.

On note $E(K) = \left\{(x; y) \in K^2, y^2 = P(x)\right\}$,

et $\overline{E}(K) = E(K) \cup \{\infty\}$.

$E : y^2 = x^3 - x + 1$



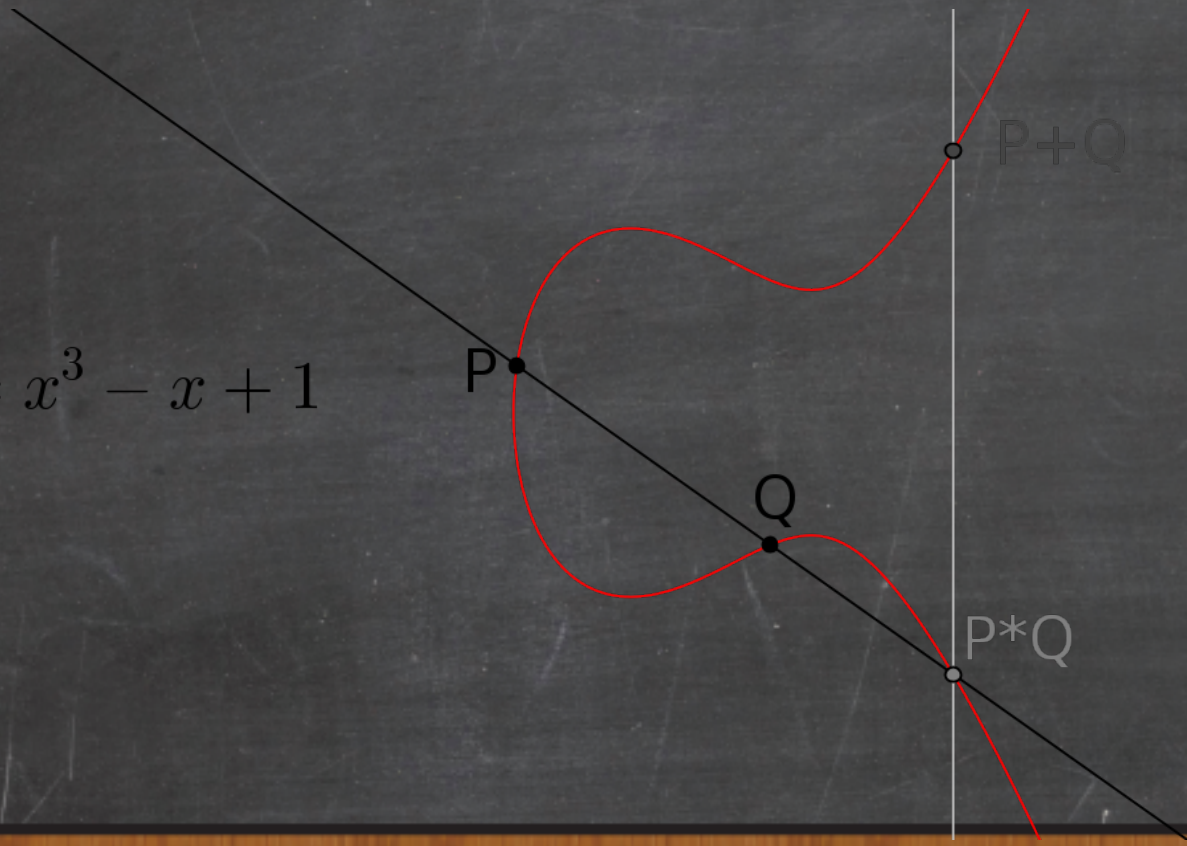
Définition

Soit K un corps.

Une courbe elliptique sur K est une courbe d'équation $y^2 = P(x)$ avec $P \in K[X]$ de degré 3 sans racine double.

On note $E(K) = \left\{(x; y) \in K^2, y^2 = P(x)\right\}$,

et $\overline{E}(K) = E(K) \cup \{\infty\}$.

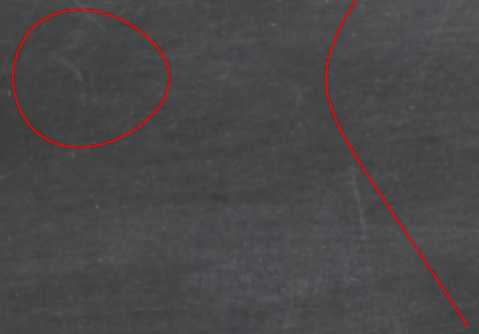


Proposition

$\overline{E}(K)$ est un groupe abélien pour la loi $+$.

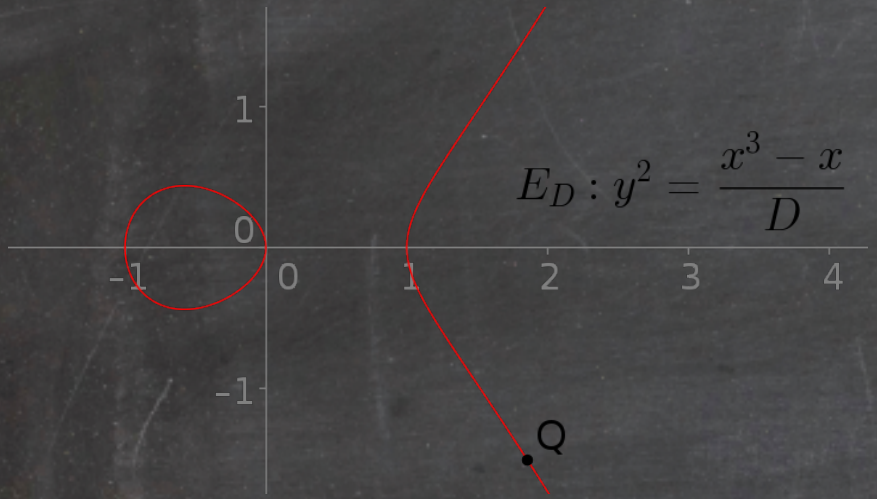
On s'intéresse à la courbe elliptique $E_D : y^2 = \frac{x^3-x}{D}$.

$$E_2 : y^2 = \frac{x^3 - x}{2}$$



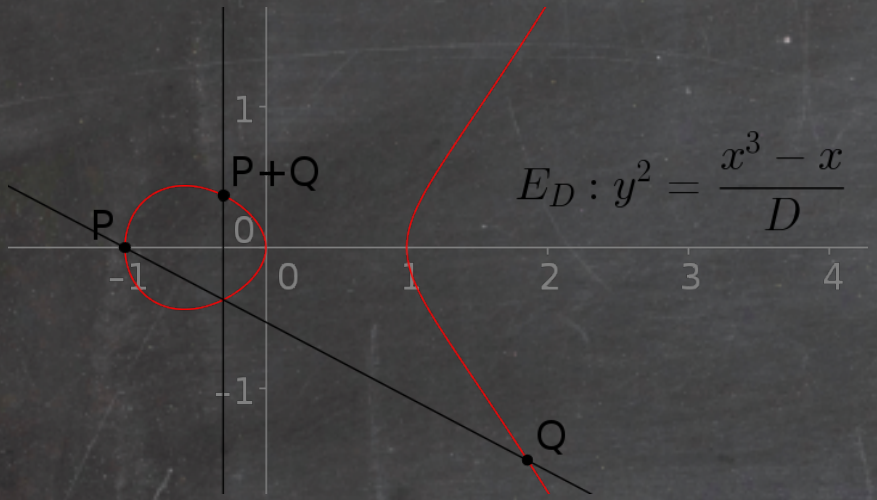
Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ *a une solution dans* $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.



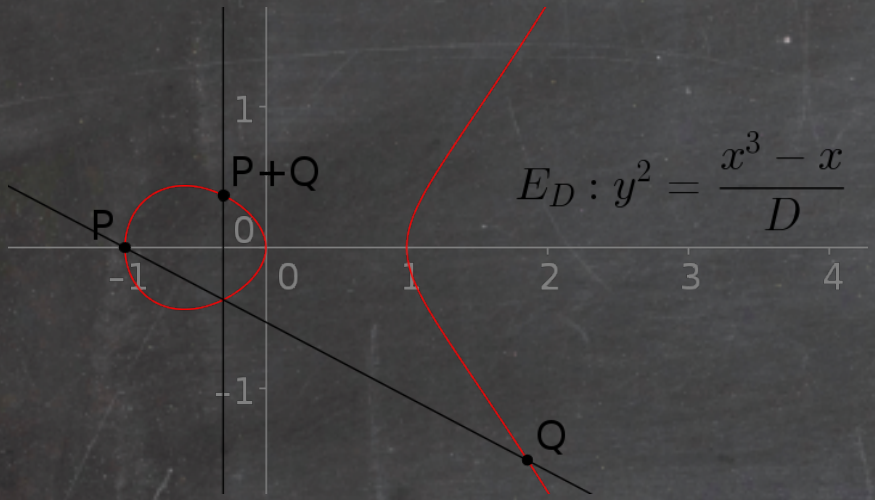
Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ a une solution dans $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.



Proposition

D est congruent si et seulement si $Dy^2 = x^3 - x$ *a une solution dans* $(\mathbb{Q} \cap]-1;0[) \times \mathbb{Q}^\times$.



Proposition

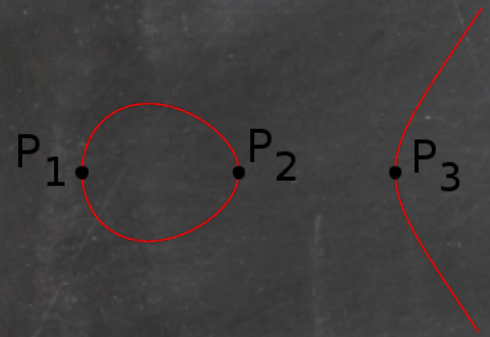
D est congruent si et seulement si E_D *a un point* $(x, y) \in \mathbb{Q} \times \mathbb{Q}^\times$.

Théorème (Mordell, 1922)

Soit E une courbe elliptique sur $\mathbb{Q}$.
Alors il existe $r \in \mathbb{N}$ tel que $\overline{E}(\mathbb{Q}) \simeq \overline{E}(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$.
r s'appelle le rang de E, on le note $r(E)$.

Théorème (Mordell, 1922)

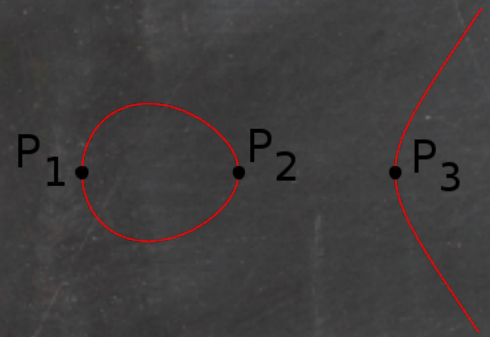
Soit E une courbe elliptique sur $\mathbb{Q}$.
Alors il existe $r \in \mathbb{N}$ tel que $\overline{E}(\mathbb{Q}) \simeq \overline{E}(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$.
r s'appelle le rang de E, on le note $r(E)$.



$$\overline{E_D}(\mathbb{Q})_{tors} = \{\infty; (-1,0); (0,0); (1,0)\}.$$

Théorème (Mordell, 1922)

Soit E une courbe elliptique sur $\mathbb{Q}$.
Alors il existe $r \in \mathbb{N}$ tel que $\overline{E}(\mathbb{Q}) \simeq \overline{E}(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$.
r s'appelle le rang de E, on le note $r(E)$.



$$\overline{E_D}(\mathbb{Q})_{tors} = \{\infty; (-1,0); (0,0); (1,0)\}.$$

Proposition

D est congruent si et seulement si $r(C_D) \geq 1$.

Soit E une courbe elliptique définie sur $\mathbb{Q}$, d'équation $y^2 = P(x) = ax^3 + bx^2 + cx + d$.

Définition

Soit p un nombre premier.

p est un bon premier s'il ne divise ni le dénominateur de a, b, c ou d, ni le numérateur du discriminant de P.

Proposition

Si p est un bon premier, E définit une courbe elliptique sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, notée $\overline{E}(\mathbb{F}_p)$.

Soit p un bon premier pour la courbe elliptique E.

Proposition

$\mathrm{Card}\overline{E}(\mathbb{F}_p) \leq 2p + 1$.

Définition

On définit $a_p = p + 1 - \mathrm{Card}\overline{E}(\mathbb{F}_p)$.

Soit p un bon premier pour la courbe elliptique E.

Proposition

$\mathrm{Card}\overline{E}(\mathbb{F}_p) \leq 2p + 1$.

Définition

On définit $a_p = p + 1 - \mathrm{Card}\overline{E}(\mathbb{F}_p)$.

Théorème (Hasse)

On a $|a_p| \leq 2\sqrt{p}$.

Les fonctions L et la conjecture de Birch et Swinnerton-Dyer

Soit E une courbe elliptique définie sur $\mathbb{Q}$ et p un bon premier pour E.

Définition

On définit une fonction L et des entiers $\alpha_n \in \mathbb{N}$ associé.e.s à la courbe elliptique E ainsi :
pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > \frac{3}{2}$,

$$L(E,s) = \prod_{p \text{ bon premier}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} \alpha_n n^{-s}$$

Théorème

L admet un prolongement analytique sur $\mathbb{C}$.

Conjecture (Birch et Swinnerton-Dyer faible)

$r(E) \geq 1$ si et seulement si $L(E, 1) = 0$.

Conjecture (Birch et Swinnerton-Dyer faible)

$r(E) \geq 1$ si et seulement si $L(E, 1) = 0$.

Conjecture (Birch et Swinnerton-Dyer)

En notant $r_{an}(E)$ l'ordre du zéro de $L(E, s)$ en $s = 1$, on a : $r(E) = r_{an}(E)$.

Conjecture (Birch et Swinnerton-Dyer faible)

$r(E) \geq 1$ si et seulement si $L(E,1) = 0$.

Conjecture (Birch et Swinnerton-Dyer)

En notant $r_{an}(E)$ l'ordre du zéro de $L(E,s)$ en $s = 1$, on a : $r(E) = r_{an}(E)$.

Théorème (Coates-Wiles)

Pour $E = E_D$, *si* $L(E,1) \neq 0$, *alors* $r(E) = 0$.

Retour aux nombres congruents

Définition

On définit la fonction $\theta : \begin{array}{ccc} \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\} & \to & \mathbb{C} \\ z & \mapsto & \sum_{n\in\mathbb{Z}} (e^{2i\pi z})^{n^2} \end{array}$

Théorème (Tunnel)

Soit $\Omega = \int_1^{+\infty} \frac{dx}{\sqrt{x^3-x}}$ *et*
$\sum_{n\in\mathbb{N}} b_n (e^{2i\pi z})^n = \theta(z)\theta(2z)(2\theta(32z) - \theta(8z))$.
Alors, si D est impair, $L(E_D, 1) = \frac{\Omega}{16\sqrt{D}} b_D^2$.

Définition

On définit la fonction $\begin{array}{rccc} \theta : & \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\} & \to & \mathbb{C} \\ & z & \mapsto & \sum_{n\in\mathbb{Z}} (e^{2i\pi z})^{n^2} \end{array}$

Théorème (Tunnel)

Soit $\Omega = \int_1^{+\infty} \frac{dx}{\sqrt{x^3-x}}$ *et*
$\sum_{n\in\mathbb{N}} b_n (e^{2i\pi z})^n = \theta(z)\theta(2z)(2\theta(32z) - \theta(8z))$.
Alors, si D est impair, $L(E_D, 1) = \frac{\Omega}{16\sqrt{D}} b_D^2$.

Théorème (Tunnel)

Soit D impair sans facteur carré.
Si D est congruent, alors

$$\mathrm{Card}\left\{(x,y,z) \in \mathbb{Z}^3, D = 2x^2 + y^2 + 32z^2\right\} = 1/2\ \mathrm{Card}\left\{(x,y,z) \in \mathbb{Z}^3, D = 2x^2 + y^2 + 8z^2\right\}$$

Si BSD faible est vérifiée pour E_D*, la réciproque est vraie.*