Des triangles, des quadrilatères et des courbes elliptiques

Matilde Lalín

Université de Montréal

mlalin@dms.umontreal.ca
http://www.dms.umontreal.ca/~mlalin

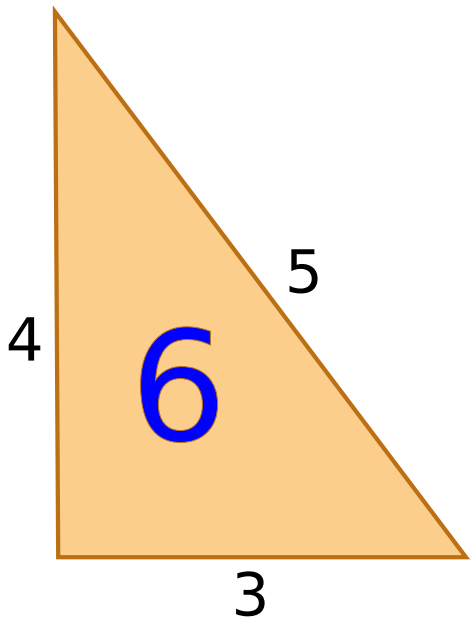
Club mathématique
20 mars 2019

Université de Montréal

Les nombres congruents

Définition

n entier positif est dit congruent s'il existe un triangle rectangle dont les trois côtés sont des nombres rationnels et dont l'aire est n.



n	a	b	c
5	$\frac{3}{2}$	$\frac{20}{3}$	$\frac{41}{6}$
6	3	4	5
7	$\frac{35}{12}$	$\frac{24}{5}$	$\frac{337}{60}$
13	$\frac{780}{323}$	$\frac{323}{30}$	$\frac{106921}{9690}$
14	$\frac{8}{3}$	$\frac{21}{2}$	$\frac{65}{6}$
15	4	$\frac{15}{2}$	$\frac{17}{2}$
20	3	$\frac{40}{3}$	$\frac{41}{3}$

Université de Montréal

Le problème des nombres congruents

Question

Quels sont les nombres entiers positifs n congruents ?

- Comment trouver des nombres congruents ?
- Comment trouver des nombres non-congruents ?
- Comment trouver un nombre infini des nombres congruents ?

Université de Montréal

Un peu d'histoire

- Ben Alhocain ($\sim$ 972) : Le problème est mentionné dans un manuscrit arabe. 5 et 6 sont congruents.
- Fibonacci (1225) : 7 est congruent, conjecture: 1 n'est pas congruent.
- Fermat (1659) : 1,2,3 ne sont pas congruents (avec la technique du descent infini).

Université de Montréal

Quelques méthodes

Prendre une solution et la multiplier par un entier positif plus grand que 1.

$$\begin{array}{rcl} 3-4-5 & \xrightarrow{\times 10} & 30-40-50 \\ 6 & \longrightarrow & 600 \end{array}$$

Pas très intéréssant...

On cherche des solutions n entier sans facteur carré.

Université de Montréal

La parametrisation des triplets pythagoriciens

Un triplet (a, b, c) d'entiers positifs est un triplet pythagoricien s'il vérifie la relation de Pythagore

$$a^2 + b^2 = c^2.$$

Il est primitif si a, b, c sont premiers entre eux.

Théorème

(a, b, c) est un triplet pythagoricien primitif avec a impair.

$$\Updownarrow$$

Il existe $(p, q) \in \mathbb{Z}^2_{>0}$ avec $p > q$, p et q premiers entre eux et de parités différentes, tels que

$$a = p^2 - q^2, \quad b = 2pq \quad \text{et} \quad c = p^2 + q^2.$$

Dans ce cas, l'aire est $pq(p^2 - q^2)$.

Université de Montréal

Quelques cas

p	q	(a, b, c)	aire	sans facteur carré
2	1	(3,4,5)	6	6
3	2	(5,12,13)	30	30
4	1	(15,8,17)	60	15
4	3	(7,24,25)	84	21
5	2	(21,20,29)	210	210
5	4	(9,40,41)	180	5
6	1	(35,12,27)	210	210
6	5	(11,60, 61)	330	330
7	2	(45,28,53)	630	70
7	4	(33,56,65)	616	154
7	6	(13,84,85)	546	546
8	1	(63,16,65)	504	126
⋮	⋮	⋮	⋮	⋮

Université de Montréal

157 est congruent!

L'algorithme précedente n'est pas très bon.
(Zagier, 1989)

$$a = \frac{6,803,298,487,826,435,051,217,540}{411,340,519,227,716,149,383,203}$$
$$b = \frac{411,340,519,227,716,149,383,203}{21,666,555,693,714,761,309,610}$$
$$c = \frac{224,403,517,704,336,969,924,557,513,090,674,863,160,948,472,041}{8,912,332,268,928,859,588,025,535,178,967,163,570,016,480,830}$$

avec

$$p = 443,624,018,997,429,899,709,925$$
$$q = 166,136,231,668,185,267,540,804$$

est la plus petite solution (avec $p + q$ minimal) pour montrer que 157 est congruent!

Université de Montréal

Les théorèmes de Tunnel

Théorème (Tunnel, 1983)

Soit $n \in \mathbb{Z}_{>0}$ impair sans facteur carré. Si le nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$2x^2 + y^2 + 8z^2 = n$$

n'est pas le double du nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$2x^2 + y^2 + 32z^2 = n$$

alors, n n'est pas congruent.

Exemple

$$2(0)^2 + (\pm 1)^2 + 8(0)^2 = 1$$
$$2(0)^2 + (\pm 1)^2 + 32(0)^2 = 1$$

2 solutions chaque, 1 n'est pas congruent!

Les théorèmes de Tunnel

Théorème (Tunnel, 1983)

Soit $n \in \mathbb{Z}_{>0}$ pair sans facteur carré. Si le nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$8x^2 + 2y^2 + 64z^2 = n$$

n'est pas le double du nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$8x^2 + 2y^2 + 16z^2 = n$$

alors, n n'est pas congruent.

Université de Montréal

Une équation spéciale

Théorème

$n \in \mathbb{Z}_{>0}$ est congruent si et seulement si l'équation

$$y^2 = x^3 - n^2 x = x(x^2 - n^2)$$

a une solution $(x_0, y_0) \in \mathbb{Q}$ avec $y_0 \neq 0$.

$(0,0), (\pm n, 0)$ sont toujours des solutions

Preuve.

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{ab}{2} = n \end{cases} \quad \Rightarrow \quad x_0 = \frac{nb}{c-a}, \qquad y_0 = \frac{2n^2}{c-a}$$

$$a = \left| \frac{x_0^2 - n^2}{y_0} \right|, b = \left| \frac{2nx_0}{y_0} \right|, c = \left| \frac{x_0^2 + n^2}{y_0} \right| \quad \Leftarrow \quad y_0^2 = x_0^3 - n^2 x_0$$

Les congrua

$$y^2 = x(x+n)(x-n)$$

Fibonacci: Un nombre entier n est un congruum ssi il y a $x \in \mathbb{Z}$ tel que

$$x^2 - n, x^2, x^2 + n$$

sont des carrés (suite arithmétique de carrés).

$$24, 96, 120, 216, 240, 336, 384, 480, 600, 720, \ldots$$

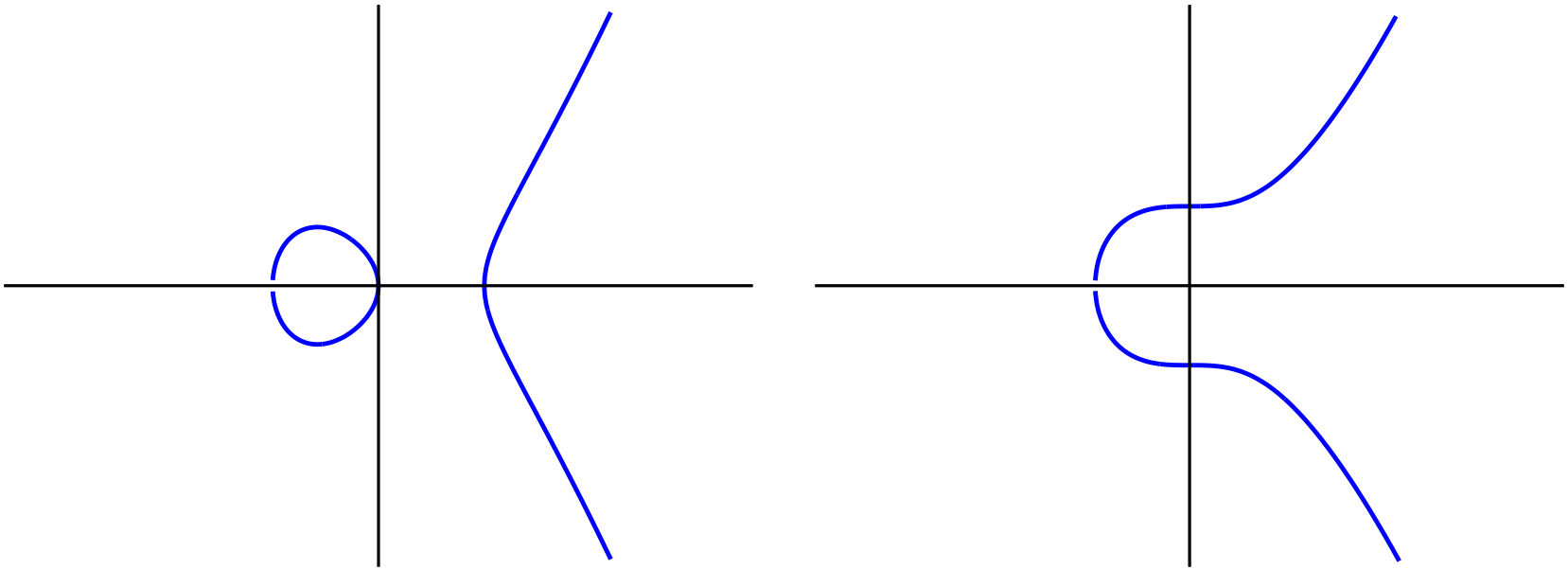
Les congrua sont des nombres congruents, et chaque nombre congruent est un congruum multiplié par le carré d'un nombre rationnel.

Université de Montréal

Les courbes elliptiques

Une courbe elliptique est donnée par une équation cubique à deux variables. On peut supposer

$$E : y^2 = x^3 + Ax + B$$



On peut penser aux solutions réeles, complexes, rationnelles, entières, etc.
On écrit $E(\mathbb{R})$, $E(\mathbb{C})$, $E(\mathbb{Q})$, $E(\mathbb{Z})$, etc.

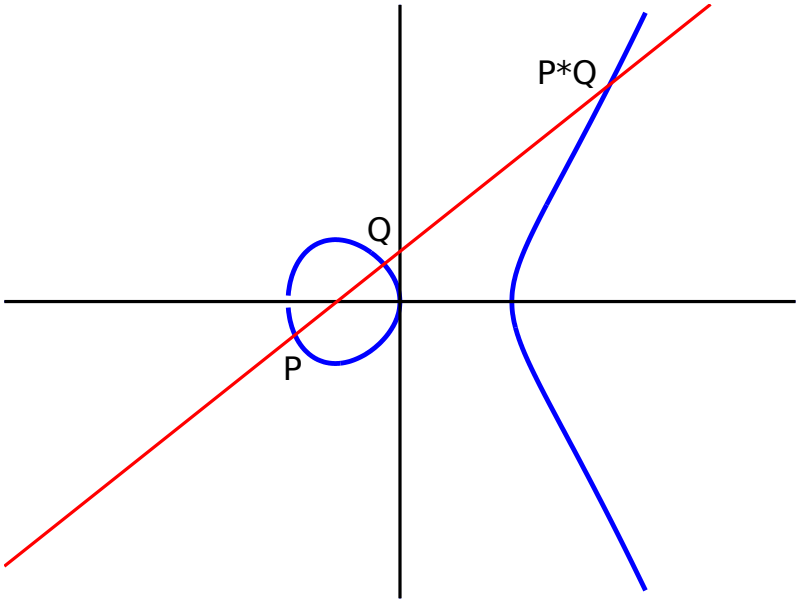
Université de Montréal

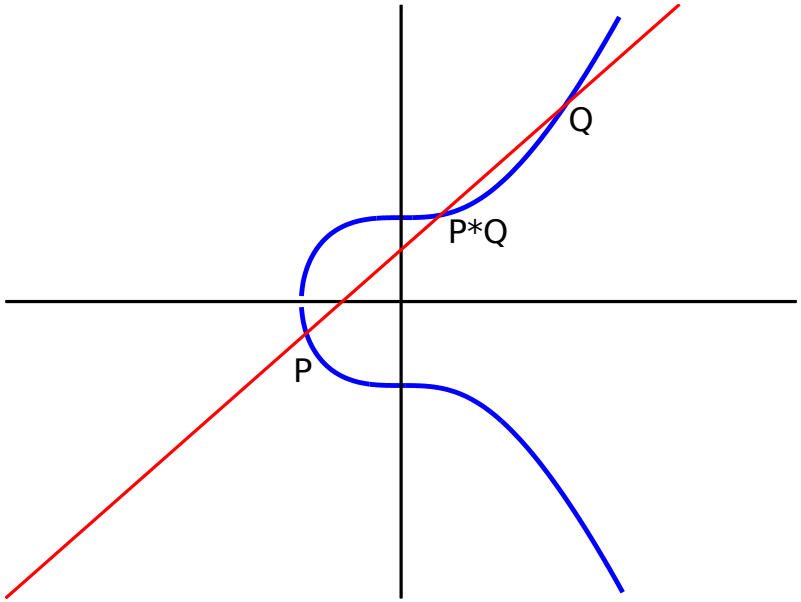
L'opération étoile

Soient $P, Q \in E$. Considérons la droite qui passe par P et par Q, $D : y = ax + b$.

$$D \cap E : (ax + b)^2 = x^3 + Ax + b.$$

Nous avons, en général, trois solutions[1]: P, Q, et $P * Q$.

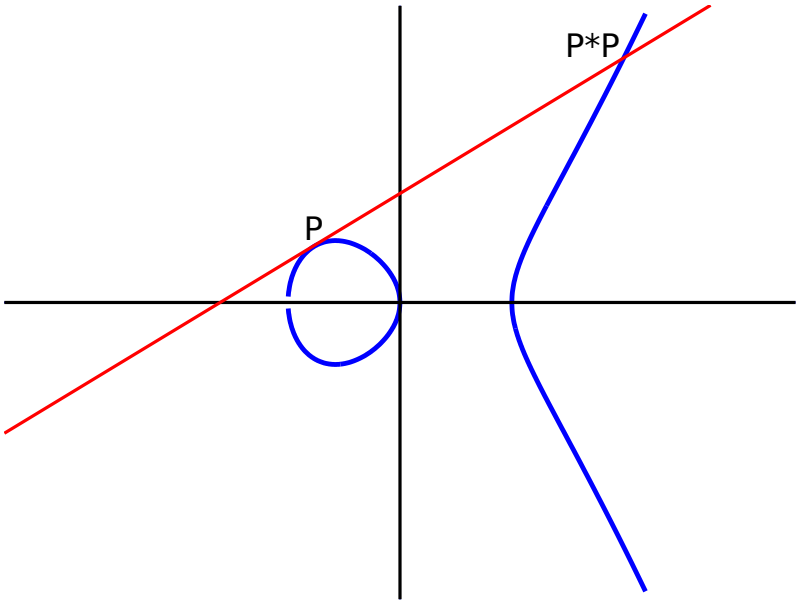


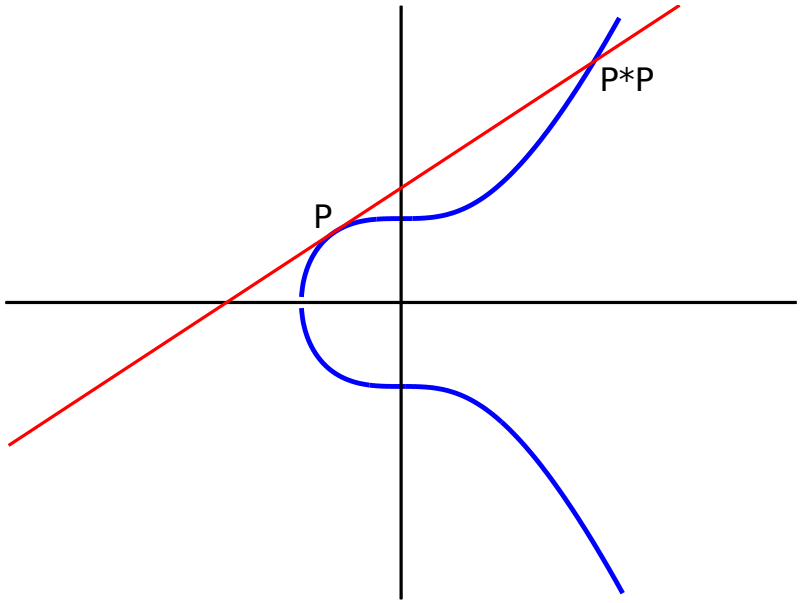


[1] Sur les complexes!

L'opération étoile, $P = Q$

Soit $P \in E$. Alors $P * P$ est défini en considérant la droite tangente à P.

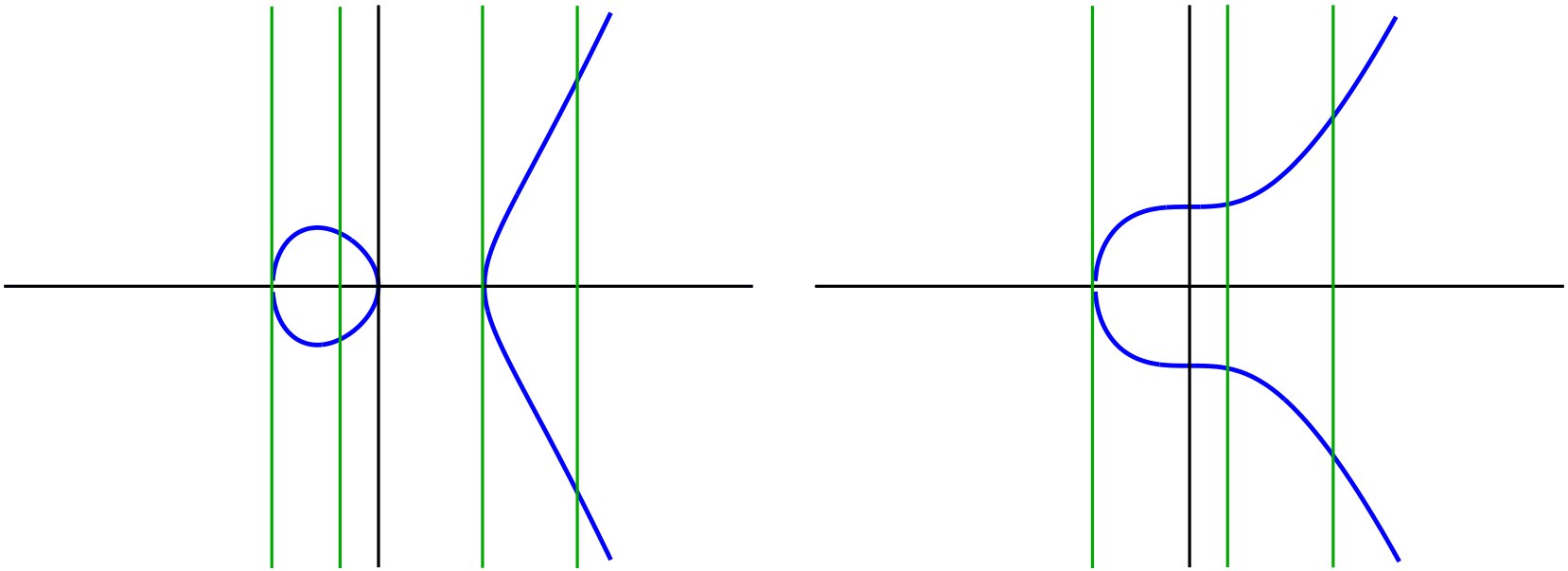




Université de Montréal

Le point à l'infini de E

Imaginons un point à l'infini O (hors du plan). Les droites qui passent par O sont les droites verticales.



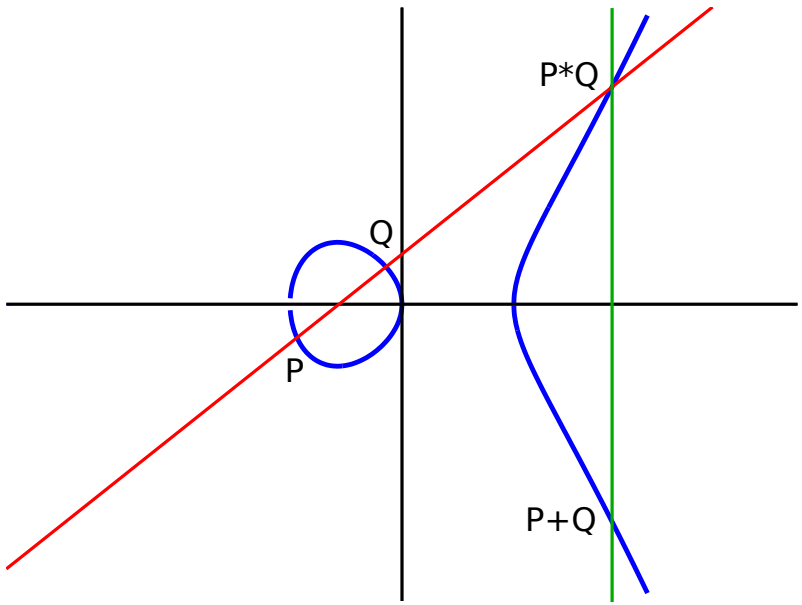
Université de Montréal

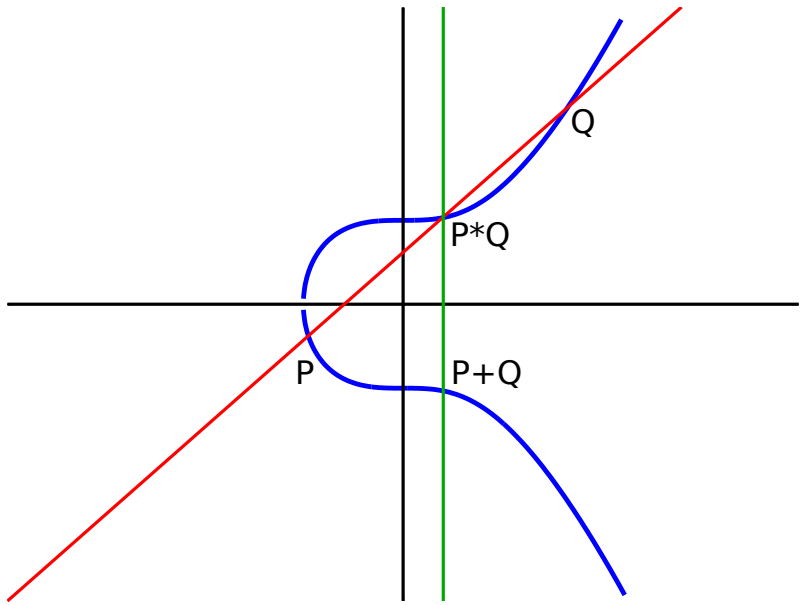
L'opération somme sur E

L'opération somme sur E est définie par

$$P + Q = (P * Q) * O.$$

En d'autres mots, on prend le point symétrique de $P * Q$ par rapport a l'axe x.





Université de Montréal

Le groupe de E

- Associativité : $(P+Q)+S = P+(Q+S)$
- Identité : $P+O = P = O+P$.
- Inverse : $-P$ est le point symétrique de P par rapport à l'axe x. $P+(-P) = (-P)+P = O$.
- Commutativité : $P+Q = Q+P$.

E avec la somme est un groupe (abélien)!

Université de Montréal

Des exemples

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

$$E(\mathbb{Q}) = \{(-2,0),(2,0),(0,0),O\}$$

$$2(\pm 2,0) = O,\ 2(0,0) = O$$

$$E : y^2 = x^3 - 7^2 x$$

$$\{(-7,0),(7,0),(0,0),O\}$$

et, en plus

$$P = (25,120) \rightsquigarrow \left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$$

$$2P = \left(\frac{113,569}{14,400}, \frac{17,631,503}{1,728,000}\right) \rightsquigarrow \left(\frac{52,319}{40,440}, \frac{566,160}{52,319}, \frac{23,058,557,761}{2,115,780,360}\right)$$

$$\ldots$$

Université de Montréal

Le théorème de Mordell

Théorème (Mordell, 1922)

Le groupe $E(\mathbb{Q})$ est finiment engendré.

$E(\mathbb{Q})$ a deux types de points :

- Un ensemble fini de points d'ordre fini (points de torsion). O est toujours un point de torsion.
- Un ensemble finitement engendré de points d'ordre infini comme $\mathbb{Z}^r$. Cet ensemble peut étre vide ($r = 0$).

Lorsque les points de torsion sont faciles à trouver, il est bien difficile de déterminer $\mathbb{Z}^r$.
Idéalement, étant donné $E(\mathbb{Q})$ on voudrait donner r générateurs de $\mathbb{Z}^r$.
Mais, même la valeur de r est difficile à trouver!

Université de Montréal

La conjecture de Birch–Swinnerton-Dyer

Étant donné E, on peut construire sa fonction L, une fonction analytique.

Conjecture (Birch et Swinnerton-Dyer, 1965)

- $r = 0$ *si et seulement si* $L(E, 1) \neq 0$.
- *Si* $r > 0$, *alors* r *est l'ordre d'annulation en* $s = 1$ *de* $L(E, s)$.

Université de Montréal

Conséquences de la conjecture de Birch–Swinnerton-Dyer

Pourquoi est-elle importante?

- On peut dire si $E(\mathbb{Q})$ a un nombre infini ou fini de points en faisant un calcul numérique facile avec un ordinateur.

- Elle peut être étendue dans des plusieurs directions, et forme parte d'une théorie très riche donnant une compréhension globale des structures géometriques et algébriques très générales.

  Même l'hypothèse de Riemann peut être associée à BSD dans ce contexte...

Université de Montréal

Les théorèmes de Tunnel

Théorème (Tunnel, 1983)

Soit $n \in \mathbb{Z}_{>0}$ impair sans facteur carré. Supposons que BSD est vraie. Si le nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$2x^2 + y^2 + 8z^2 = n$$

est égal au double du nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$2x^2 + y^2 + 32z^2 = n$$

alors, n est congruent.

Exemple

$$2x^2 + y^2 + 8z^2 = n$$
$$2x^2 + y^2 + 32z^2 = n$$

n'ont pas de solution si $n = 5, 7$, donc, ils sont des nombres congruents.

Les théorèmes de Tunnel

Théorème (Tunnel, 1983)

Soit $n \in \mathbb{Z}_{>0}$ pair sans facteur carré. Supposons que BSD est vraie. Si le nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$8x^2 + 2y^2 + 64z^2 = n$$

est égal au double du nombre de triplets $x, y, z \in \mathbb{Z}$ tels que

$$8x^2 + 2y^2 + 16z^2 = n$$

alors, n est congruent.

Université de Montréal

La conjecture de Birch–Swinnerton-Dyer

- En 2000, la conjecture de Birch–Swinnerton-Dyer a été incluse parmi les sept problèmes du prix du millénaire. (Un autre problème dans la liste est l'hypothèse de Riemann.)

  La résolution de chacun des problèmes est dotée d'un prix d'un million de dollars américains offert par le Clay Mathematics Institute.

- Jusqu'à maintenant, c'est connu que

$$\mathrm{ord}_{s=1} L(E,s) = 0,1 \Rightarrow r = 0,1$$

  (Coates, Wiles, Gross, Zagier, Kolyvagin, Breuil,...)

- En 2015 Bhargava and Shankar ont prouvé que la moyenne de r est bornée par 0.885. Cela donne un proportion positive des courbes elliptiques avec $L(E,1) \neq 0$ et qui satisfont BSD.

Université de Montréal

Quelques familles infinies de nombres congruents (ou pas)

p premier.

- Genocchi (1882) :
  - $p \equiv 3 \pmod 8$, p n'est pas congruent.
  - $p \equiv 5 \pmod 8$, $2p$ n'est pas congruent.
- Heegner (1952) : $p \equiv 3 \pmod 4$, $2p$ est congruent.
- Monsky (1984) : $p \equiv 5, 7 \pmod 8$, p est congruent.
- $p \equiv 1 \pmod 8$??? On ne sait pas: 41 est congruent mais 17 ne l'est pas!
- Stephens (1995) : BSD implique $n \equiv 5, 6, 7 \pmod 8$ sont congruents.
- Feng, Li–Tian, Zhao (1996-2001): un nombre infini de $n \equiv 1, 2, 3 \pmod 8$ avec un nombre arbitraire de facteurs premiers ne sont pas congruents.
- Gross, Monsky, Tian (1985-2012): un nombre infini de $n \equiv 5, 6, 7 \pmod 8$ avec un nombre arbitraire de facteurs premiers sont congruents.

Université de Montréal

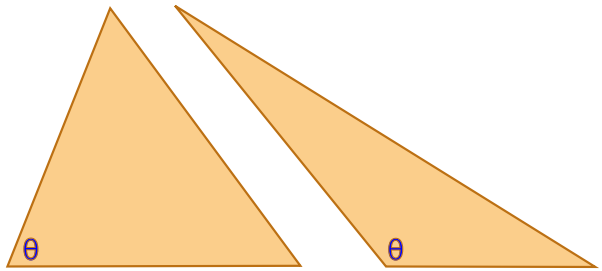
Les nombres θ-congruents

Définition

Soit $0 < \theta < 2\pi$ *tel que*

$$\cos\theta = \frac{s}{r}, \quad r, s \in \mathbb{Z}, \quad |s| \leq r, \quad \operatorname{pgcd}(r, s) = 1.$$

Un n *entier positif est dit* θ*-congruent s'il existe un triangle avec angle* θ *dont les trois côtés sont des nombres rationnels et dont l'aire est* $n\sqrt{r^2 - s^2}$.



Fujiwara (1998): On peu associer la courbe elliptique

$$y^2 = x(x - n(r - s))(x + n(r + s)).$$

Université de Montréal

Nombres $\pi/3$ et $2\pi/3$-congruents

- Fujiwara (1998) : $p \equiv 5, 7, 19 \pmod{24}$, p n'est pas $\pi/3$-congruent.
- Kan (2000) : $p \equiv 7, 11, 13 \pmod{24}$, p n'est pas $2\pi/3$-congruent.
- Girard, L, Nair (2018) : des familles specifiques avec un nombre arbitraire de facteurs premiers non-$\pi/3$-congruents ou non-$2\pi/3$-congruents.
- Mokrani (2018+) : adaptation de la méthode de Monsky pour engendrer un nombre arbitraire des familles non-$\pi/3$ ou non-$2\pi/3$-congruentes.

Université de Montréal

Les triangles d'Heron

Définition

Un triangle est dit un triangle d'Heron si ses trois côtés et son aire sont des nombres rationnels.

Les lois des cosinus et des sinus $\Rightarrow \cos\theta,\ \sin\theta \in \mathbb{Q}$.

$n \in \mathbb{Z}_{>0}$ est l'aire d'un triangle d'Heron ssi il y a un nombre $\tau \in \mathbb{Q}^*$ tel que la courbe elliptique

$$y^2 = x(x - n\tau)(x + n\tau^{-1})$$

a un point (x_0, y_0) avec $y_0 \neq 0$.
Le paramètre τ fait de l'équation une surface elliptique.

Théorème (Goins–Maddox, 2006)

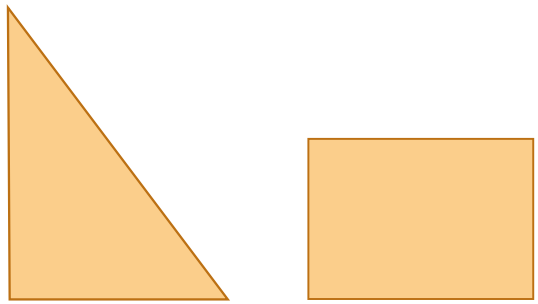
Soit $n \in \mathbb{Z}_{>0}$. Il y a un nombre infini de triangles d'Heron avec aire n.

Université de Montréal

Un triangle rectangle et un rectable

Question (Sands)

Existe-t-il un triangle rectangle de côtes entiers avec la même aire et le même perimètre qu'un rectangle de côtes entiers ?



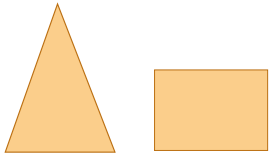
Théorème (Guy, 1995)

Non.

$$y^2 = x^3 + x^2 - 8x + 16$$

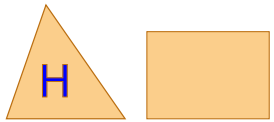
n'a que des points de torsion.

Université de Montréal



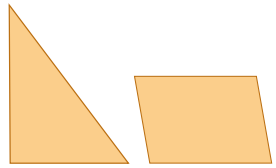
∞

Guy 1995



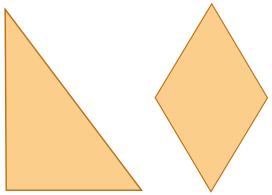
∞

Brenmer–Guy 2006



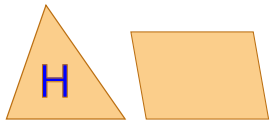
∞

Zhang 2016



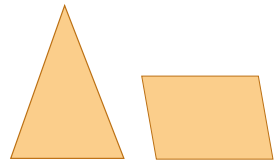
∞

Cheng 2016



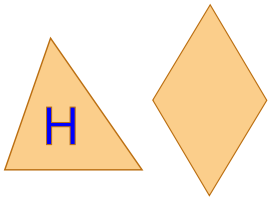
∞

Zhang–Peng 2017



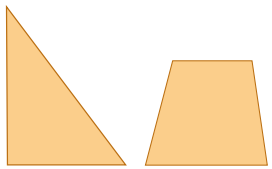
∞

Das, Juyal, Moody 2017



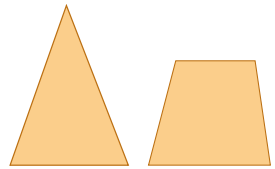
∞

Das, Juyal, Moody 2017



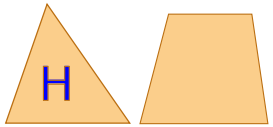
∞

Zhang, Peng, Wang 2018



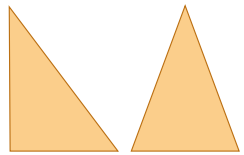
∞

Zhang, Peng, Wang 2018



∞

Zhang, Peng, Wang 2018



$(377, 135, 352)$ et $(366, 366, 132)$

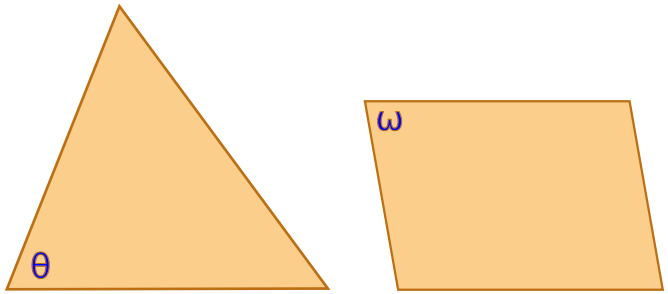
Hirakawa, Matsumura 2019

Université de Montréal

Triangle et parallelogramme en choissisant des angles

Théorème (L–Ma, 2018+)

Soit θ *tel que* $\cos\theta = a \in \mathbb{Q}$, *pour presque tout* $t \in \mathbb{Q}$ *avec* $0 < t \leq \frac{1}{\sqrt{1-a^2}}$, *il y a un nombre infini de couples de* θ*-triangle à côtés entiers et de* ω*-parallelogramme à côtés entiers tels que* $\sin\omega/\sin\theta = t$ *avec même aire et même perimètre.*



$$y^2 = x^3 + t((1+a)^2 t + 4(a-3))x^2 + 32(1-a)t^2 x$$

a presque toujours un nombre infini de solutions ($r = 1$).

Les paramètres t et a font de l'équation un "threefold" elliptique.

Université de Montréal

Merci de votre attention!!!

et merci aussi à mes étudiant.e.s d'été
Vincent Girard, Xinchun Ma, Youcef Mokrani et Sivasankar Nair.

Université de Montréal