

Une introduction aux courbes elliptiques

Riccardo Brasca

Math en mouvement 2025 : théorie des nombres

15 novembre 2025

On trouve sur internet beaucoup de questions mathématiques pas très intéressantes

Only genius can do this!

$$45 - 15 \div 5 \times 3$$

facebook.com/Thinkmath.kenyousee

Mais il y a des exceptions !

95% of people cannot solve this!

$$\frac{\text{apple}}{\text{banana} + \text{pineapple}} + \frac{\text{banana}}{\text{apple} + \text{pineapple}} + \frac{\text{pineapple}}{\text{apple} + \text{banana}} = 4$$

Can you find positive whole values

for apple, banana, and pineapple?

Les fruits c'est bien mais...

On cherche $x, y, z \in \mathbb{N}_{>0}$ tels que

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$$

C'est plus raisonnable de travailler dans $\mathbb{Z}$ et chercher à la fin des solutions positives

En se débarrassant des dénominateurs (attentions aux nouvelles solutions!) on a

$$x(x+y)(x+z) + y(x+y)(y+z) + z(z+x)(z+y) = 4(x+y)(x+z)(y+z)$$

Il s'agit d'une équation de degré 3 en trois variables (difficile!), mais elle est *homogène*

Si (x, y, z) est une solution alors $(\lambda x, \lambda y, \lambda z)$ l'est aussi, pour tout $\lambda \in \mathbb{Q}^*$

Si $z = 0$ on obtient

$$(x + y)(x^2 + y^2) = 4xy(x + y)$$

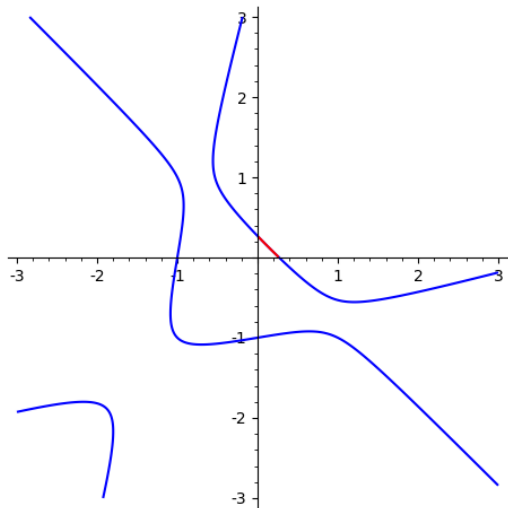
Donc $x = -y$ ou $(2x - y)^2 = 3x^2$ ce qui est impossible car $\sqrt{3} \notin \mathbb{Q}$
À partir d'ici on suppose $z \neq 0$.

Quitte à multiplier par z^{-1} , on peut supposer $z = 1$ et on cherche les solutions *rationnelles* de

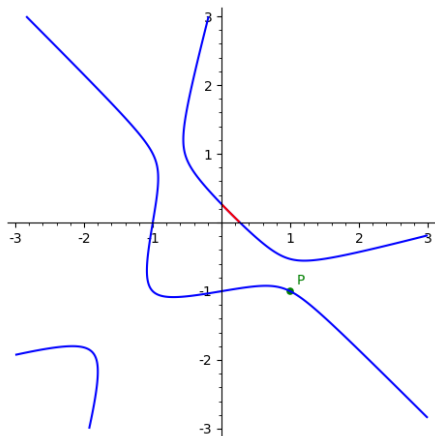
$$x^3 + y^3 - 3(x + y + x^2 + y^2 + xy^2 + x^2y) + 1 = 5xy$$

Il s'agit d'une courbe, et on peut dessiner les solutions réelles

On cherche donc les points avec *les deux coordonnées rationnelles* dans la région rouge de la courbe

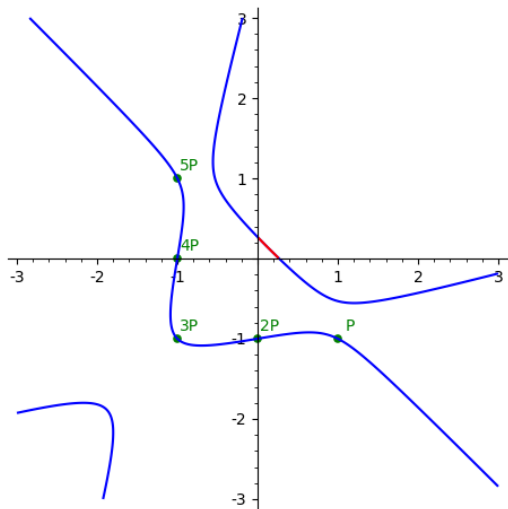


C'est facile de trouver sur la courbe des points avec les deux coordonnées rationnelles : $P = (1, -1)$

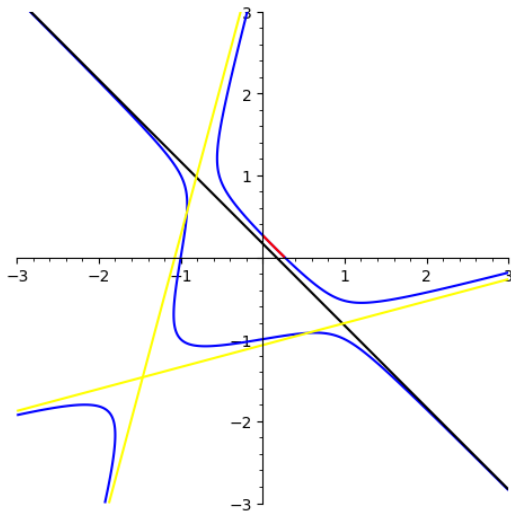


Mais ça ne donne pas une solution à l'équation de départ à cause des dénominateurs

Et pareil pour $(0, -1)$, $(-1, -1)$, $(-1, 0)$ et $(-1, 1)$



Notre courbe a trois asymptotes : $y + x = 1/6$, $x - (2 + \sqrt{3})y = 4$
et $y - (2 + \sqrt{3})x = 4$



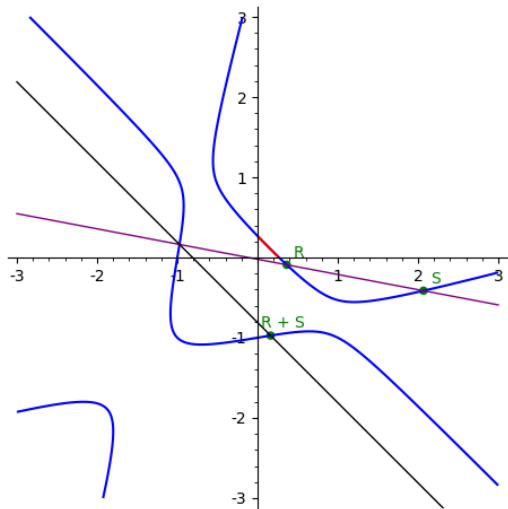
Il faut penser que A , le premier asymptote intersect la courbe en un point (à coordonnées rationnelles!) « très loin », à *l'infini*

Cela peut être rendu précis en utilisant la géométrie projective, et ça correspond aux points de l'équation initiale avec $z = 0$

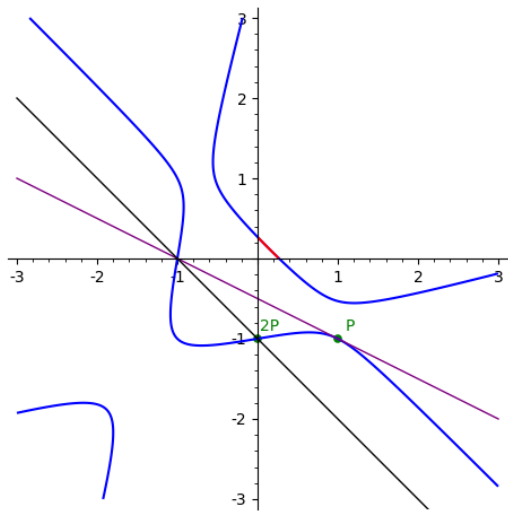
Si R et S sont deux points sur la courbe on peut faire la procédure suivante pour trouver un troisième point sur la courbe

- On trace la droite L qui passe par R et S
- Étant l'équation de degré 3, on a que L intersecte la courbe en un troisième point T
- On regarde la droite A' parallèle à A qui passe par T
- A' intersecte la courbe en seulement deux point (plus le point « très loin », donc au total c'est trois!) : T et un point qu'on appelle $R + S$

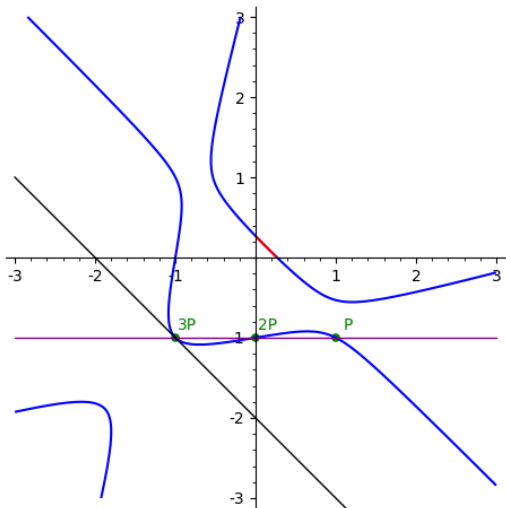
Ça peut paraître un peu délirant, mais voici un dessin



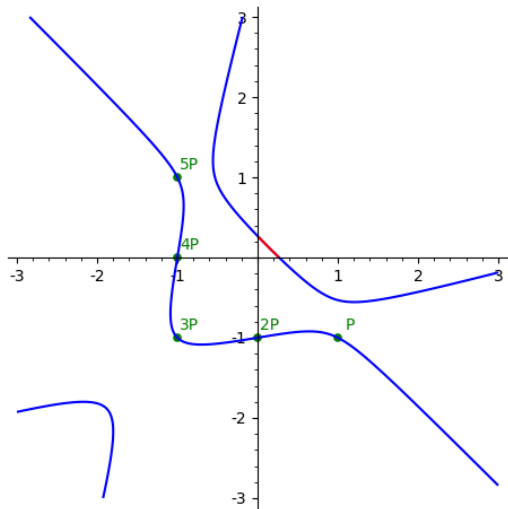
Si on prend deux fois le même point P c'est la même procédure, mais on commence avec la droite tangente à la courbe en P .



Voici le calcul de $3P = P + 2P$.



Cela explique les noms ci-dessus



Pour calculer $6P = P + 5P$ il faut considérer la droite qui passe par $(1, -1)$ et $(-1, 1)$, ce qui est $Y = -X$, donc il n'y a pas de troisième point d'intersection !

La solution est d'introduire un point, noté 0 , qui est l'intersection de la courbe et de la droite $Y = -X$ à l'infini

Il s'agit du point à l'infini déjà mentionné

La droite A' est en général la droite qui passe par T et par 0

Calculons $6P$:

- La droite qui passe par P et $5P$, qui est $Y = -X$, intersecte la courbe en P , $5P$ et le point « fictif » $T = 0$.
- La droite A' est la droite qui passe par 0 deux fois : elle est la *tangente à la courbe en 0*
- Cette droite doit être parallèle à A . De plus, elle ne peut pas intersecter la courbe en aucun autre point
- On peut démontrer qu'il s'agit de A , qui a donc une intersection *triple* en 0 avec la courbe
- En particulier on a

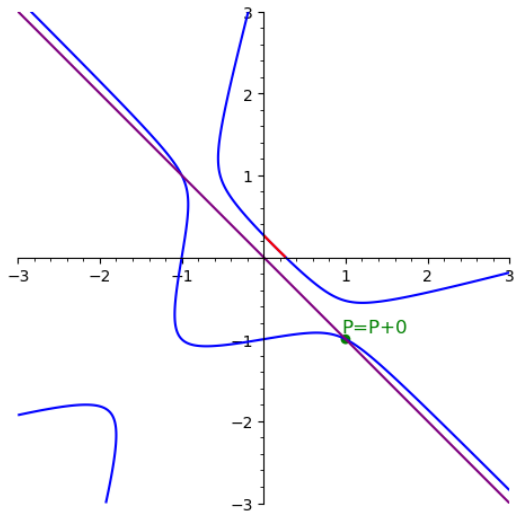
$$6P = P + 5P = 0$$

Il nous reste à calculer $R + 0$

- On trace la droite L qui passe par R et 0 : c'est la parallèle à A qui passe par R
- On note T le troisième point d'intersection
- On a que A' et L sont parallèles
- A' intersecte la courbe en T et R (plus le point 0 à l'infini)
- Finalement on a

$$R + 0 = R$$

Voici le dessin de $P + 0 = P$



- La procédure marche pour tout R et S , et on obtient un point bien défini $R + S$ qui est sur la courbe
- On a $R + S = S + R$
- On a $R + 0 = R$
- Pour tout R il existe un point S tel que $R + S = 0$
- Si R et S sont à coordonnées rationnelles alors $R + S$ est aussi à coordonnées rationnelles
- Le calcul de $R + S$ est facile à faire en pratique
- L'opération $+$ est *associative*

On a donc que l'ensemble de points à coordonnées rationnelles de la courbe, plus le point à l'infini 0 , est un *group abélien*

On a que $6P = 0$ et donc P est un point d'ordre fini

On ne peut pas l'utiliser pour fabriquer d'autre points, on a

$$15P = 3P$$

Avec un peu d'effort on trouve un autre point sur la courbe

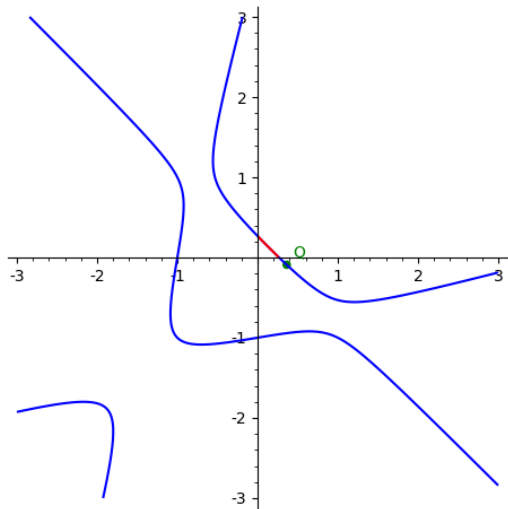
$$Q = (4/11, -1/11)$$

Ça correspond à la solution de l'équation initiale

$$x = 4 \quad y = -1 \quad z = 11$$

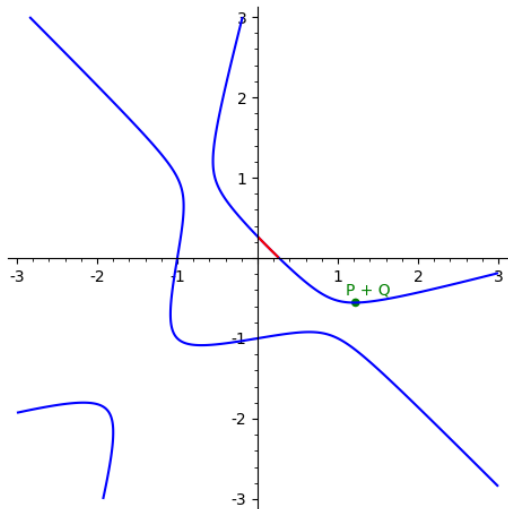
qui est dans $\mathbb{Z}$ (mais malheureusement pas dans $\mathbb{N}_{>0}$)

Le point Q

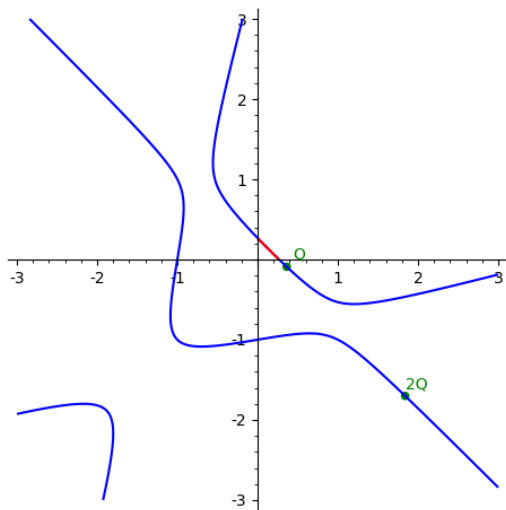


On peut maintenant utiliser P et Q pour fabriquer d'autres points, en espérant d'en trouver un dans la zone rouge.

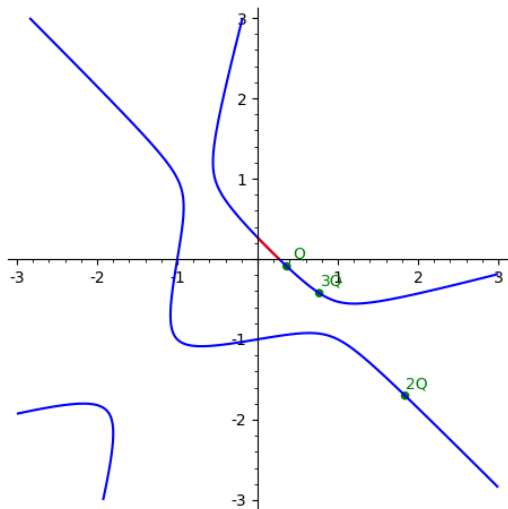
Voici $P + Q$, qui ne marche pas



Et $2Q$, qui ne marche pas non plus



Pas de chance avec $3Q$



Additionner des multiples de P n'aide pas, mais on peut continuer avec les multiples de Q

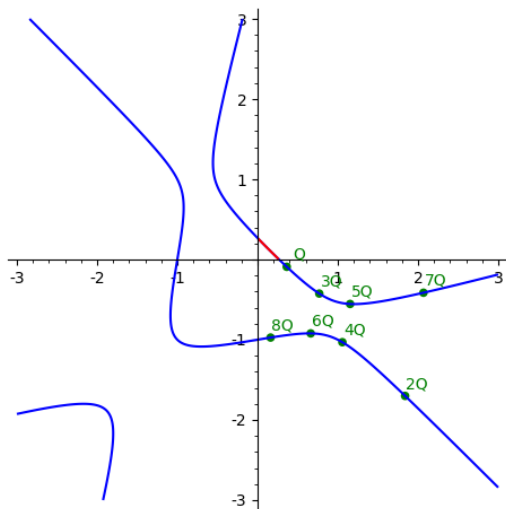
Le calcul des coordonnées est faisable en pratique, et il nous donne des solutions de l'équation initiale très difficiles à trouver à la main.

Par exemple

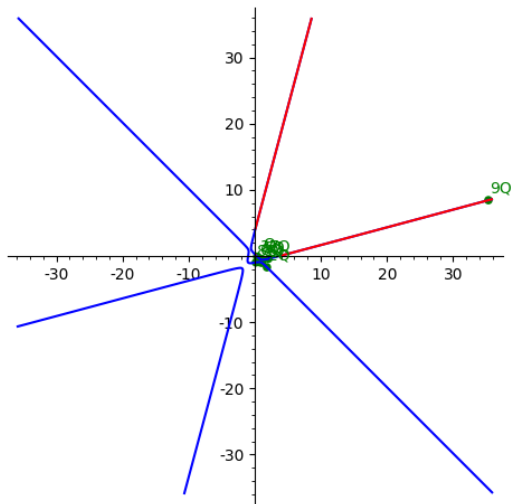
$$2Q = (9499/5165, -8784/5165)$$

$$3Q = (679733219/883659076, -375326521/883659076)$$

On insiste jusqu'à $8Q$ sans trouver une solution...



Mais 9Q marche !



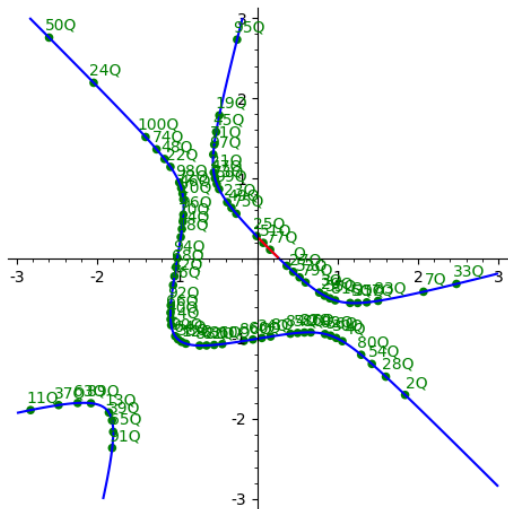
Ça donne la solution suivante au problème de départ

$$\text{🍎} = 15447680210874616644195131501991983748566432566956 \\ 5431700026634898253202035277999$$

$$\text{🍌} = 36875131794129999827197811565225474825492979968971 \\ 970996283137471637224634055579$$

$$\text{🍍} = 43736126779286972578612526023713901528165375581616 \\ 13618621437993378423467772036$$

77Q marche aussi (et il est de taille totalement délirante)



🍎 = 11959341396359824492755391126696226056463070002449
89101850698418095812680970498973126196730020281797
49202705773609200503501488219418940009605226693902
64744571129945173834146077216359168456696449641296
94731390515202154006630483626281172626888213104889
85516652158900076978130874984745247664301477580310
27162196107160849577574695128812304920482885888296
42254886681446505156823304242449572651129712184041
09290170484552622203203370684149051339419305222267
74081850346178682085862839178001085443776219503810
56617156036349529666302951997789329042250244787873
93203157052750219871472257987786254894772038548907
98413603972289560901811605495933347162263530072050
17717260154220419837608518168870140076676944326510
75315798611024818628995320084831222661818983629529
01347106614451933346869142419025766413862067477...

a 5816 chiffres

Un courbe (projective et lisse) E qui est aussi un groupe s'appelle
une courbe elliptique

Notre equation donne un exemple d'une telle courbe

$E(\mathbb{Q})$ est donc un groupe, qui est toujours *finiment engendré*

Dans notre cas on a

$$E(\mathbb{Q}) \cong \mathbb{Z}/6 \oplus \mathbb{Z}$$

Et on a trouvé tous les points de torsions !

Vu que l'équation est à coefficient dans $\mathbb{Z}$ on peut aussi compter les solutions modulo p pour un premier p ... mais c'est une autre histoire