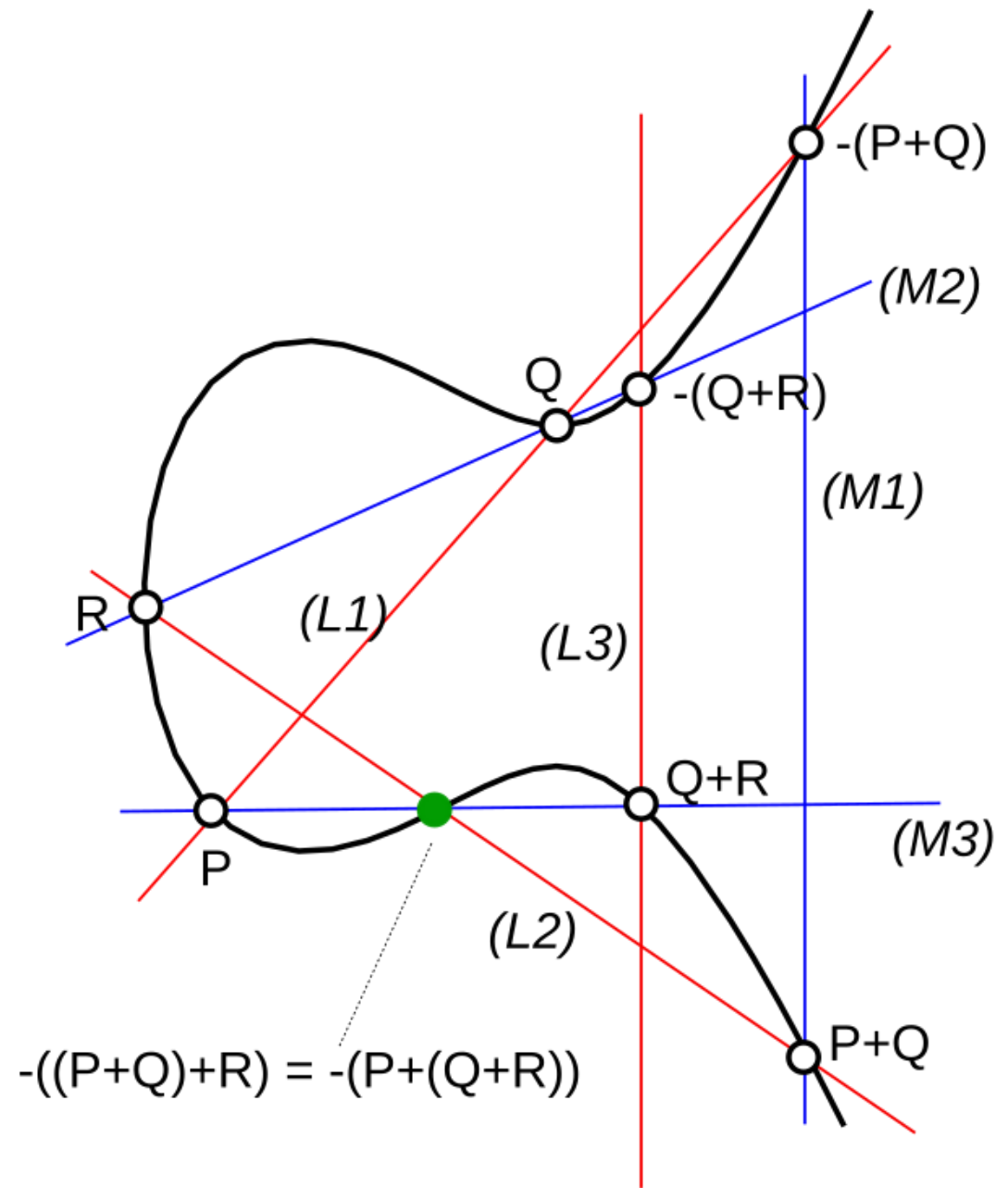


**Et si
on
additionnait
des
points?**





Jérôme Cardan
1501 - 1576

Retour sur l'équation du troisième degré

Au XVI^e siècle, pour les mathématiciens européens, les nombres négatifs sont systématiquement écartés. Les coefficients des équations sont positifs et les solutions attendues sont positives. On cherche à résoudre des équations du type $x^3 + ax = b$, où a et b sont positifs



Niccolo Tartaglia
1499 - 1557

Scipione Ferro of Bologna, almost thirty years ago, discovered the solution of the cube and things equal to a number, a really beautiful and admirable accomplishment. In distinction this discovery surpasses all mortal ingenuity, and all human subtlety.

Pourquoi n'y a-t-il pas de terme du second degré? Posons $x = y + u$, on obtient :

$$x^3 + ax^2 + bx + c = y^3 + (3u + b)y^2 + (3u^2 + 2au + b)y + u^3 + au^2 + bu + c$$

Ce qui montre qu'on peut s'en passer...

TERZA RISPOSTA

DATA DA NICOLO TARTALEA BRISCIANO
Al Eccellente M. Hieronimo Cardano Medico Milanese, &
Lettor Publico in Pavia.

Et al Eccellente messer Lodouico Ferraro delle Mathematiche
Lettor publico in Melano; Con la resolutione, ouer
Risposta de, 31. Quesiti, ouer questioni da
quelli allui proposti.

Eccellente m. Hieronimo, & voi messer Lodouico alli. 21. di Aprile
vi dedi risoluta risposta allo vostro secondo Cartello, Et con quella vi
indirizai Quesiti, ouer Questioni. 31. con offerta che se voi ambidui
insieme con che altro vi paresse, me li resolueate in termine de giorni. 15.
dapoi la presentatione di quelli, che mi contentaua di perdere ducatti. 25. de
danari, & la mita delli mei restanti libri che tanto ve infestano, (per narrar in
quelli la pura verita) liquali danari & libri ascendeuano alla somma de duc.
150. Et che se per sorte voi non me sapeuate resoluer li detti Quesiti nel det
to termine, io non voleua che voi fosti tenuti a perdere cosa alcuna. Et vi scrif
si anchora che se per sorte voi non li sapeuate risoluer cosi in giorni. 15. vi
concedeu a per manco vostra infamia che soluendoli anchor dapoi el detto
termine, vn mese, & anchor dui, o tutti, ouer parte de quelli, che potesti publi
car le dette vostre solutioni al mondo, Laqual mia risposta, & Quesiti furno
consignati alla S. de m. Ottauiano Scotto el primo di di maggio, Presente m.
Dominico del q. Dona Cantor. Et adi. 3. del detto mese trouai la Signoria di
m. Ottauiano Scotto, & lo adimandai se vi haueua mandata la detta mia ri
sposta, & quesiti, quel mi rispose (presente a dui homini da bene) che il gior
no auanti se era partito il portaror di quella, che faria stato adi. 2. di maggio,
talmente che tassando, 3. ouer. 4. giorni al detto latore per venire da Venetia
a Melano, faccio conto che alli. 5. ouer al piu alli. 6. di maggio voi douesti ri
ceuer la detta mia risposta, & quesiti. Et perche molti mei amici me represe
deuano grandamente ogni giorno digando che io era stato troppo largo, &
liberale a farue a d ambidui cosi largo partito, & massime con liberta di poter
ui far agiutare anchora ad altri, & conoscendo che me diceuano il vero, son
stato per fin alli. 6. di giugno alquanto suspeso dubitando che non mi manda
ssi la resolutione di quelli nel termine a voi assignato. Dico per fin alli. 6. di
giugno, perche io vi limitaua (come detto) giorni. 15. per resoluer li detti ca

Al Signor Gabrio da Caravaggio

Pas facile de reconstituer l'histoire de
la résolution d'équations du troisième
degré en Italie au XVIe siècle.
Ci-contre un fac-similé d'une lettre
adressée par Tartaglia à Cardan et
Ferrari.

Quando chel cubo con le cose appresso
 Se agguaglia à qualche numero discreto
 Trovan dui altri differenti in esso.
 Dapoi terrai questo per consueto
 Che'l lor prodotto sempre sia eguale
 Al terzo cubo delle cose neto,
 El residuo poi suo generale
 Delli lor lati cubi ben sottratti
 Varra la tua cosa principale.
 In el secondo de cotești atti
 Quando che'l cubo restasse lui solo
 Tu offeruarai quest' altri contratti,
 Del numer farai due tal part' à uolo
 Che l'una in l'altra si produca schietto
 El terzo cubo delle cose in stolo
 Delle qual poi, per commun precetto
 Torrai li lati cubi insieme giunti
 Et cotal somma sarà il tuo concetto.
 El terzo poi de questi nostri conti
 Se solue col secondo se ben guardi
 Che per natura son quasi congiunti.
 Questi trouai, & non con passi tardi
 Nel mille cinquecentè, quatro e trenta
 Con fondamenti ben sald'è gagliardi
 Nella città dal mar' intorno centa.

La recette de Tartaglia

Pas exactement L'équation est écrite : $x^3 + px = q$.

Posons $x = u + v$ il vient $u^3 + v^3 + (u + v)(3uv + p) = q$

On impose $uv = -\frac{p}{3}$ On doit alors résoudre le système

$$\begin{cases} u^3 + v^3 = q \\ u^3 v^3 = -\frac{p^3}{27} \end{cases} \quad u^3 \text{ et } v^3 \text{ sont solutions de l'équation}$$

$X^2 - qX - \frac{p^3}{27} = 0$. Le discriminant de cette équation est le célèbre $\Delta = \frac{4p^3 + 27q^2}{27}$. Par principe les coefficients p et q sont positifs, Δ est positif, il y a deux racines dont u et v sont les

racines cubiques : $u = \sqrt[3]{\frac{q + \sqrt{\Delta}}{2}}$ et $v = \sqrt[3]{\frac{q - \sqrt{\Delta}}{2}}$ et l'équation

possède une solution unique $x = \sqrt[3]{\frac{q + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{q - \sqrt{\Delta}}{2}}$

L'ALGEBRA
PARTE MAGGIORE
DELL'ARITMETICA
DIVISA IN TRE LIBRI
DI RAFAEL BOMBELLI
DA BOLOGNA.

Nouamente posta in luce.



IN BOLOGNA

Nella Stamperia di Giovanni Rossi

M D L X X I I

Con Licentia dell'RR. VV. del Vesc. & Inquis.

L'algebra (1572) de
Raphaël Bombelli

L'équation du troisième degré avec d'autres nombres

La méthode de Tartaglia n'envisage pas les données négatives, mais si on essaie : $x^3 - 15x = 4$ possède la solution 4 qui échappe à la formule de

résolution, qui donnerait $4 = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$

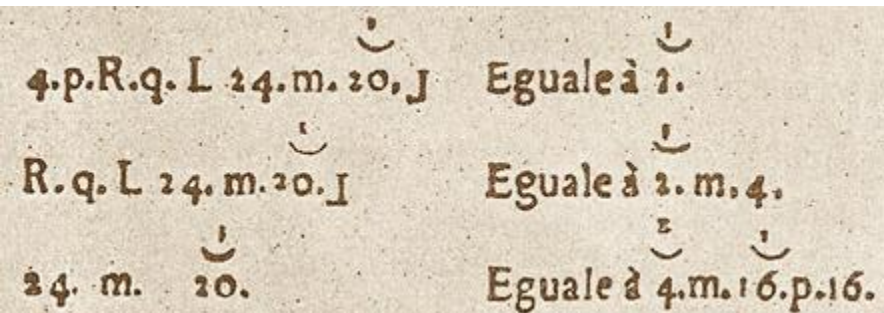
Une supposition de Raphaël Bombelli (1526 – 1572) : chercher une « racine cubique » de $2 + 11\sqrt{-1}$ de la forme $2 + a\sqrt{-1}$, ce qui donnerait

$$8 - 6a^2 + 12a\sqrt{-1} - a^3\sqrt{-1} = 2 + 11\sqrt{-1}$$

Par identification : $12a - a^3 = 11$ et $8 - 6a^2 = 2$

enfin $a = 1$ et $x = 2 + \sqrt{-1} + 2 - \sqrt{-1} = 4$

C'était le début pour les nombres
que Descartes appellera *imaginaires*



L'écriture mathématique de Bombelli
(selon Florian Cajori)

Courbes elliptiques (1)

La définition retenue par Weierstrass, une courbe elliptique (C) **sur le corps des nombres réels** possède une équation $y^2 = x^3 + ax + b$.

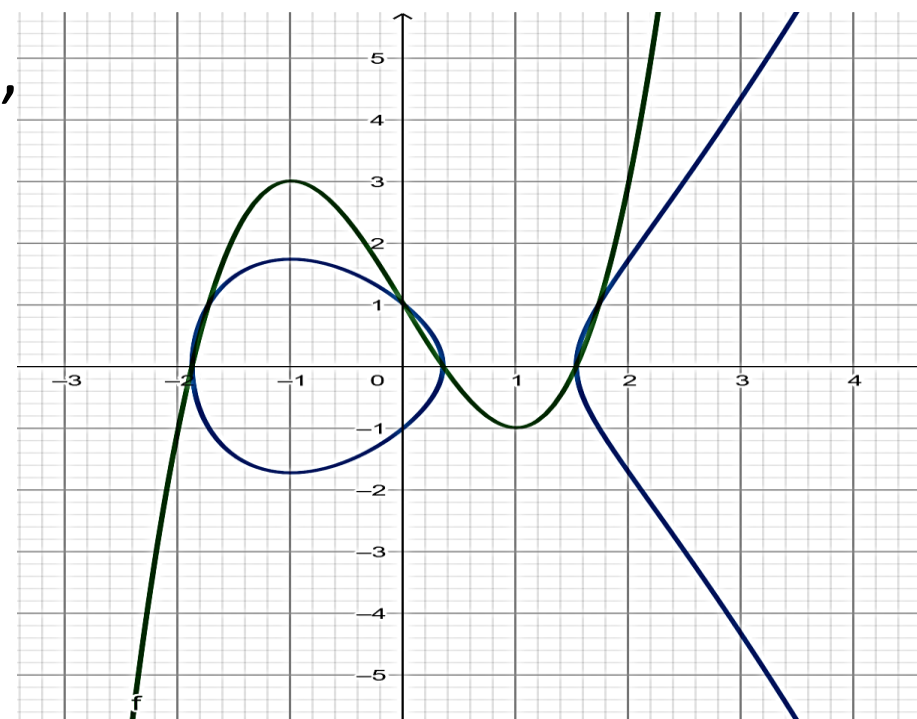
Étude du polynôme $f(x) = x^3 + ax + b$

Si $a \geq 0$, f est monotone croissante, il y a une seule racine (réelle);

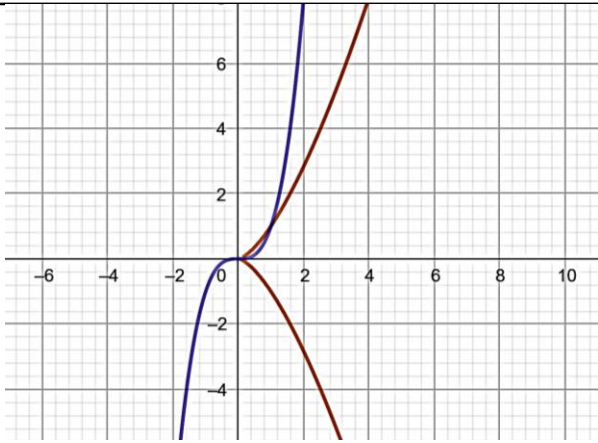
Si $a < 0$, la fonction dérivée f' possède deux zéros,

en $\sqrt{\frac{-a}{3}}$ et $-\sqrt{\frac{-a}{3}}$. Le maximum et le minimum relatifs sont de signe contraire si et seulement si $\Delta < 0$, où $\Delta = 4a^3 + 27b^2$

(en **vert**, la courbe de f , en **bleu** la courbe (C))

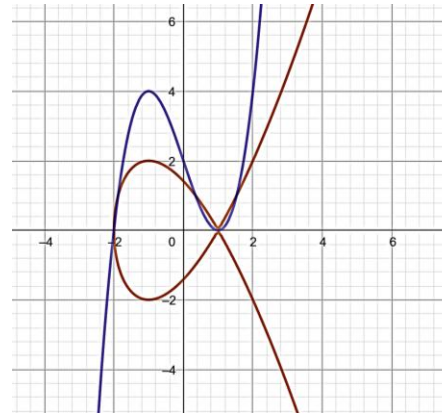


Courbes elliptiques (2)



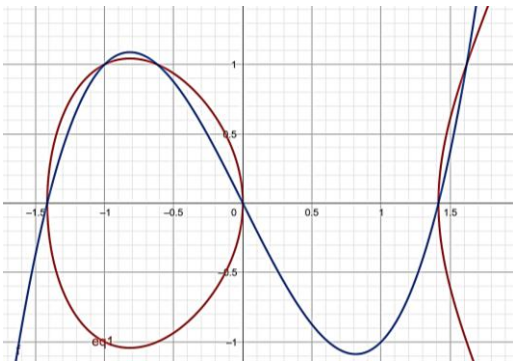
Le polynôme f possède une racine triple. La courbe (C) présente un point de rebroussement

$$\Delta = 0$$



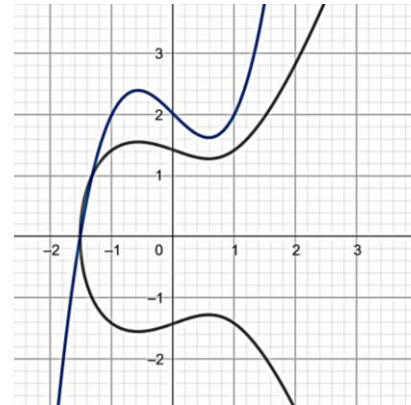
Le polynôme f possède une racine double positive. La courbe (C) présente un point double

$$\Delta = 0$$



Le polynôme f possède trois racines. La courbe (C) a deux composantes

$$\Delta > 0$$

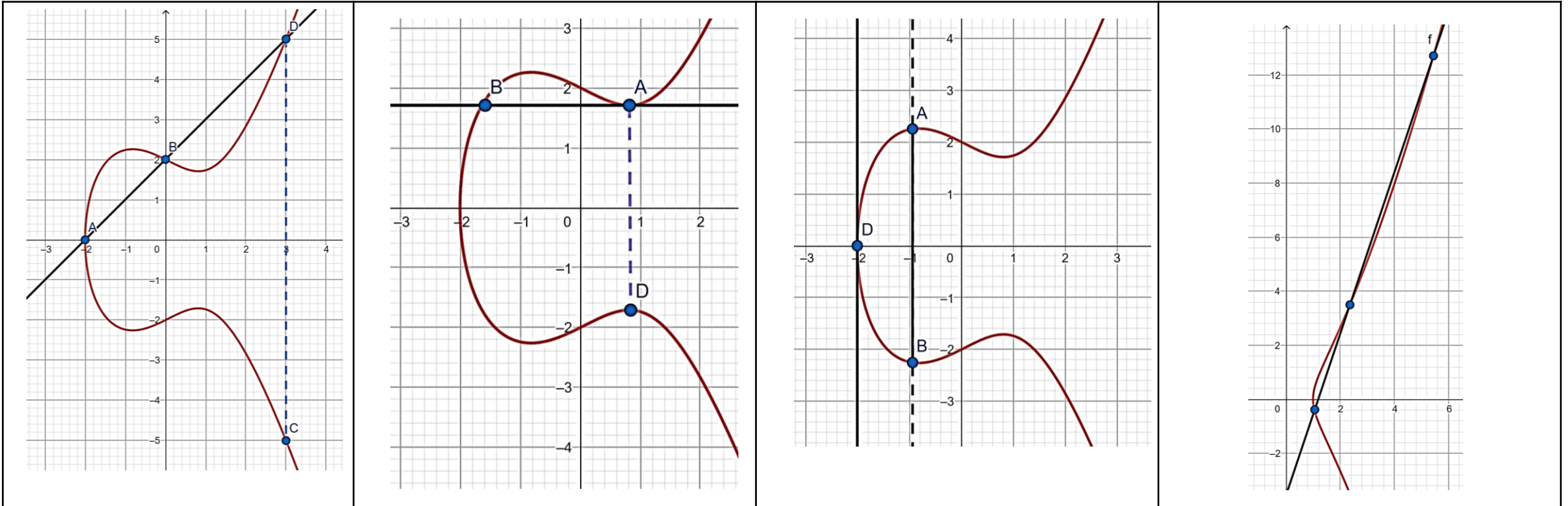


Le polynôme f possède une seule racine. La courbe (C) a une seule composante

$$\Delta < 0$$

Seule la deuxième ligne du tableau intéresse la suite. On n'a pas illustré le cas d'une racine double négative...

Une addition de points



Si la droite coupe la courbe en trois points, le symétrique du « troisième » par rapport à l'axe des abscisses est la somme des deux premiers. Si elle est tangente à la courbe, c'est le point de contact qui est le « troisième ». Si la droite est verticale la somme de A et B (troisième colonne) comme la somme de D et D sont le « point à l'infini », noté (maladroitement) O. **N'oublions pas que toute droite passant par un point de la courbe est ou bien une verticale, ou bien est tangente à la courbe, ou bien la coupe en trois points.**

Coordonnées de la somme

... dans le cas d'une sécante oblique de pente rationnelle...

La courbe (C) d'équation $y^2 = x^3 + Ax + B$ et la droite (d) d'équation $y = ax + b$ se coupent en deux points donnés de coordonnées (x_1, y_1) et (x_2, y_2) .

L'équation aux abscisses des points d'intersection s'écrit :

$$x^3 + Ax + B = (ax + b)^2$$

Ou encore $x^3 - a^2x^2 + (A - 2a)x + B - b^2 = 0$

Cette équation a trois solutions, x_1, x_2 et x_3 , on a donc $x_1 + x_2 + x_3 = a^2$,

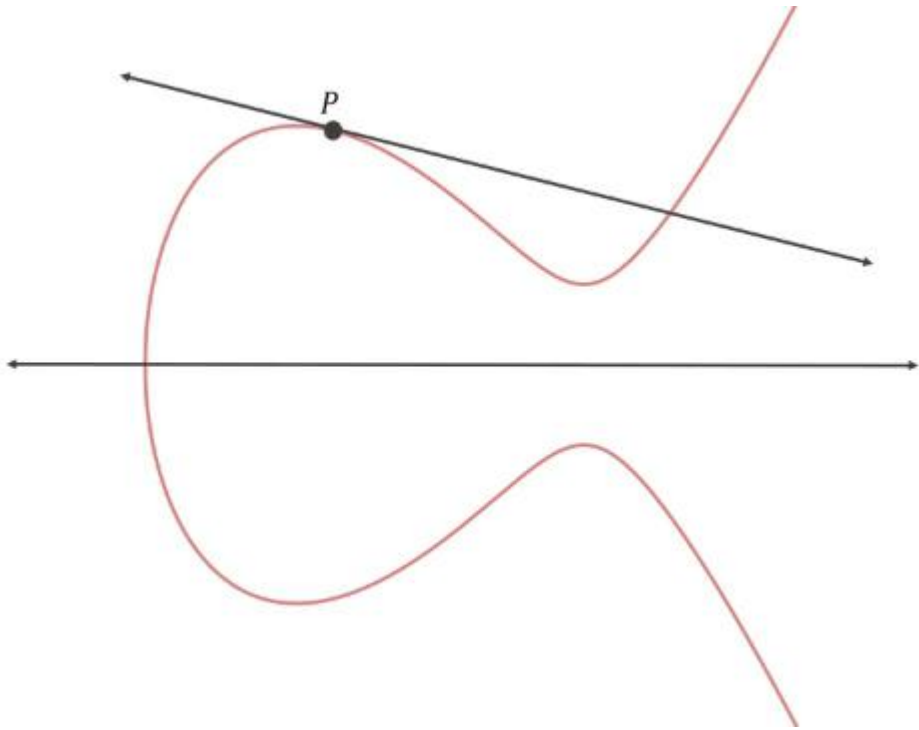
Ce qui fournit $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

Le point somme a pour coordonnées cet x_3 et $y_4 = -(ax_3 + b)$

Remarque fondamentale :

deux points « rationnels » ont une somme « rationnelle »

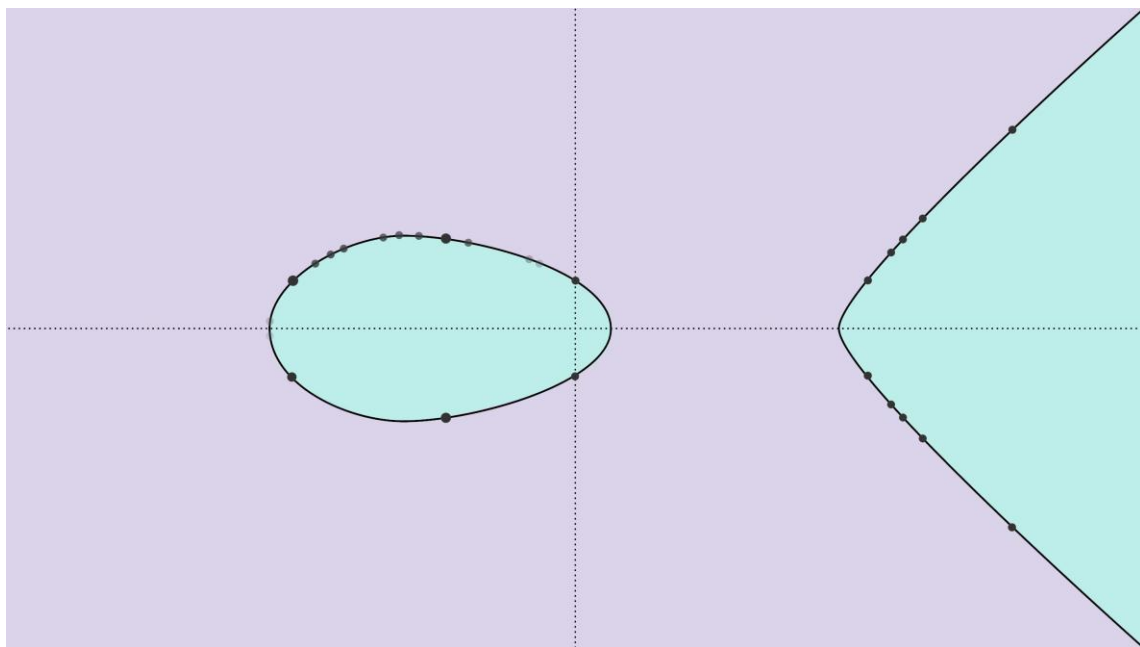
Multiplication par un entier



La tangente en un point P de la courbe recoupe celle-ci en un point disons Q dont le symétrique par rapport à l'axe des abscisses est $P+P$ (à ne pas confondre avec le point $Q+P$, qui est le symétrique de P par rapport à cet axe).

On peut poursuivre le procédé et construire le point $(P+P)+P$ qui est aussi $P+(P+P)$ – nous n'avons pas démontré l'*associativité* de l'opération $+$. On peut ainsi obtenir les points nP pour toutes les valeurs de n sauf si P est un point de *torsion*.

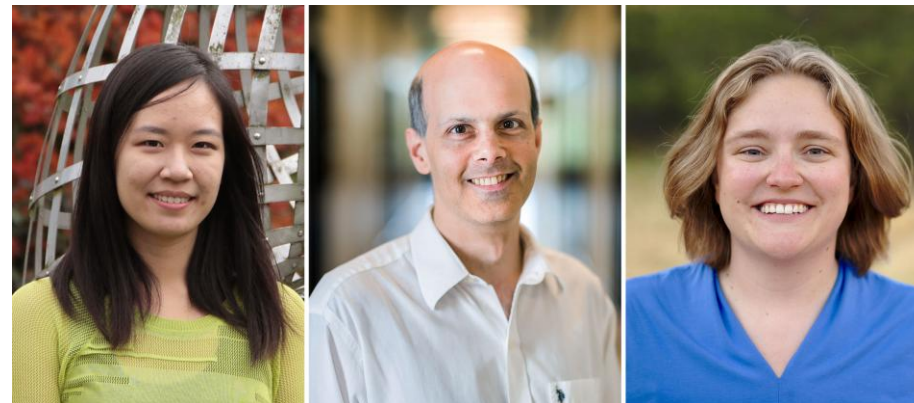
Les points « rationnels »



Points rationnels sur la courbe $y^2 = x^3 - 4x + 1$

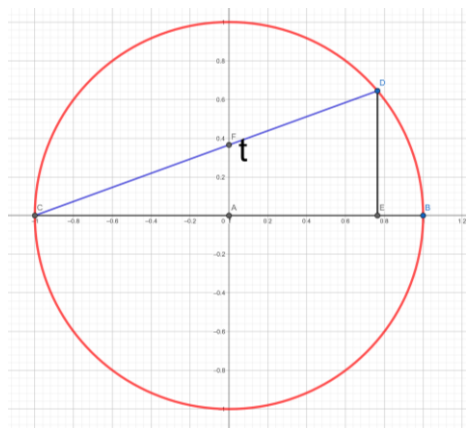
Le **rang** d'une courbe elliptique est le nombre minimum de points rationnels indépendants permettant de trouver **tous** les points rationnels de la courbe

À partir de deux points à coordonnées rationnelles, on en trouve un troisième et ainsi de suite. Peut-on, en partant de quelques points de la courbe, trouver **tous** les points à coordonnées rationnelles?

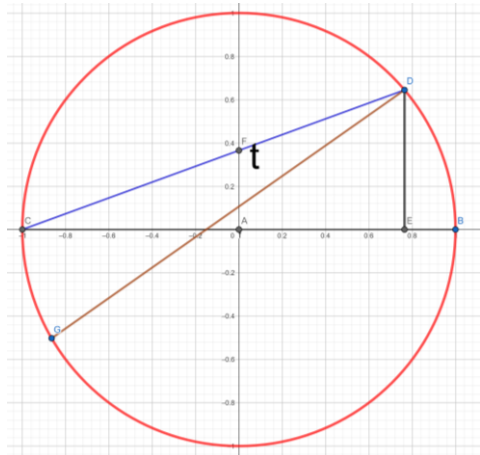


Jennifer Park, Bjorn Poonen et Melanie Wood, avec John Voight, en pointe dans les recherches sur le rang des courbes elliptiques (en 2018)

... déjà, le cercle lui-même...

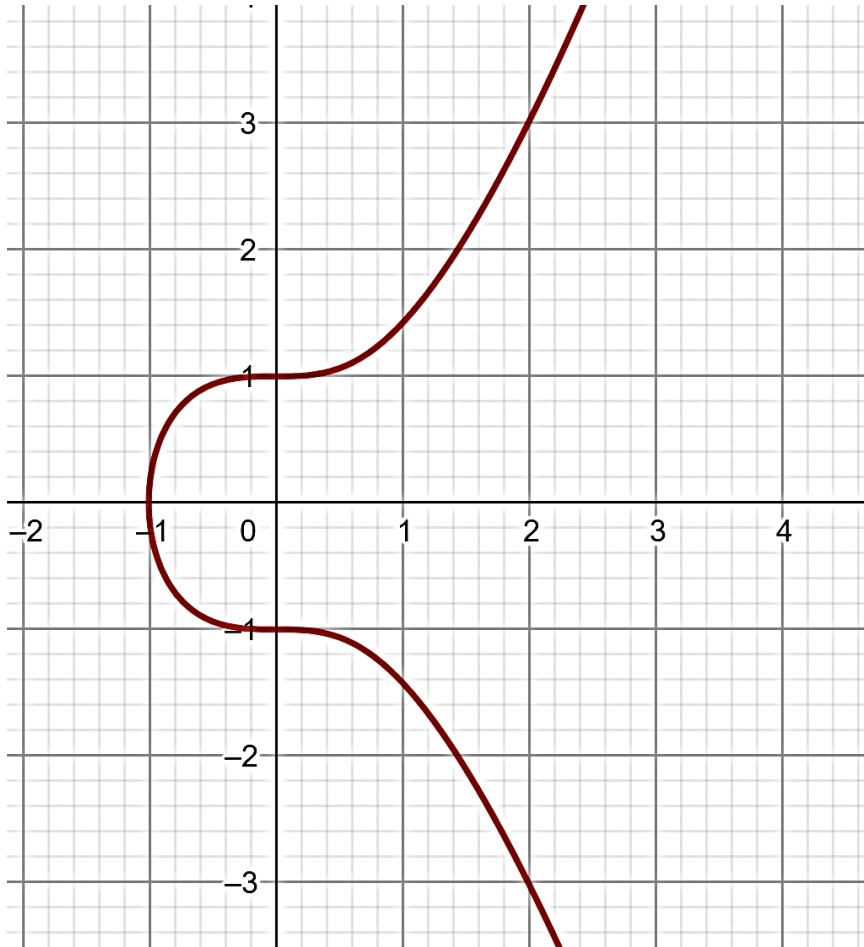


A partir du point de coordonnées $(-1, 0)$ du cercle (C) de centre O et de rayon 1, on trace la droite passant par le point de coordonnées $(0, t)$, droite d'équation $y = t(1 + x)$. t est un rationnel compris entre 0 et 1. Cette droite recoupe le cercle au point de coordonnées $(x, t(1 + x))$, où $x^2 + t^2(1 + x)^2 = 1$, égalité qui peut s'écrire $t^2(1 + x) = 1 - x$ pour tout $x \neq -1$. On obtient $x = \frac{1-t^2}{1+t^2}$ et $y = \frac{2t}{1+t^2}$.



On peut continuer en traçant une droite de pente rationnelle passant par le point obtenu. Tous les points du cercle à coordonnées rationnelles peuvent être obtenus, et donc tous les triplets pythagoriciens puisque $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ et $a^2 + b^2 = c^2$ sont identiques.

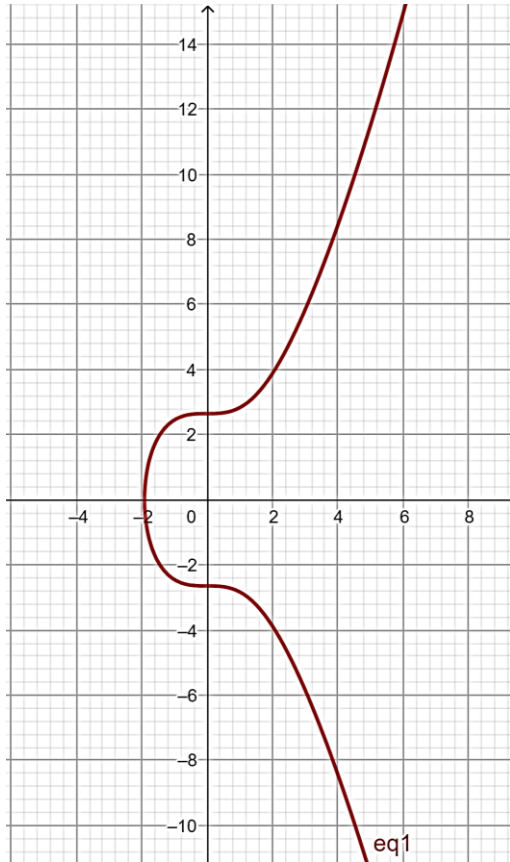
Quelques exemples (1)



Une équation de Mordell : $y^2 = x^3 + 1$
La courbe ne présente que cinq points à coordonnées entières et l'ensemble formé par ces cinq points et le point à l'infini est stable par addition. Ce sont les seuls points rationnels. La courbe est dite de rang 0.

Rappel arithmétique : en nombres entiers positifs $x^3 = (y - 1)(y + 1)$
 $y - 1$ et $y + 1$. Si y est pair, les deux facteurs sont impairs et premiers entre eux ... **DONC** ce sont des cubes et la différence de deux cubes d'entiers supérieurs à 1 est supérieure à 2 (exercice : écrire tout ça)

Quelques exemples (2)



« Secp256k1 » est le nom donné en cryptographie à cette courbe, dont l'équation est $y^2 = x^3 + 7$.

Si on se donne un point P et un point Q multiple de P, le nombre n tel que $Q = nP$ est caché et c'est dans ce nombre qu'on peut dissimuler des informations confidentielles.

Ça, c'est le point de départ. Quel genre de coordonnées?

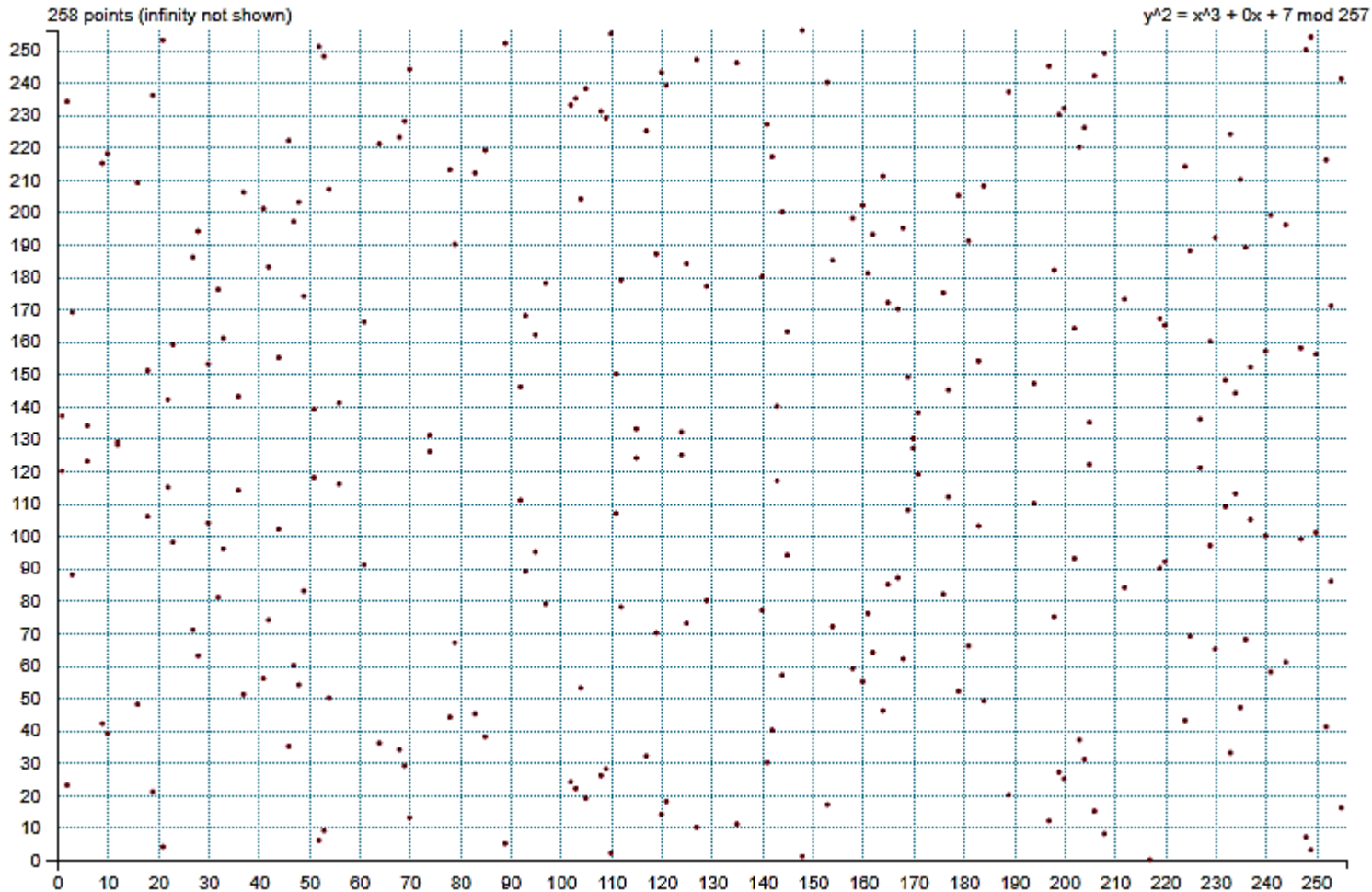
abscisse x :

5506626302227734366957871889516853432625060345377
75941755001873609396729240

ordonnée y :

3267051002075881697808308513050704318447127338065
9243275938904335757337482424

Il faudra d'autres outils



Avec de tels nombres, il faut des outils de calcul à la hauteur... La courbe ne sert à rien puisqu'on a les démarches du calcul. Ci-contre, un tableau donnant une suite de points (modulo 257 pour les coordonnées).