MATh.en.JEANS 2010-2011

27 septembre 2010

Problème 1 et 2 : Introduction

Cryptage et décryptage : communiquer en toute sécurité

La cryptographie est l'art de chiffrer un message de façon qu'il soit inintelligible à toute autre personne que son destinataire.
La cryptographie moderne utilise des procédés dits à clefs publiques basés sur les fonctions trappes (ou fonctions à sens uniques) : on sait facilement calculer $f(x)$ mais on ne sait pas retrouver x même lorsqu'on connaît $f(x)$
Exemple : $f(x) = x^2$ se calcule facilement mais on ne sait pas calculer aussi facilement $\sqrt{x}$ sans machine ! (pas réaliste).

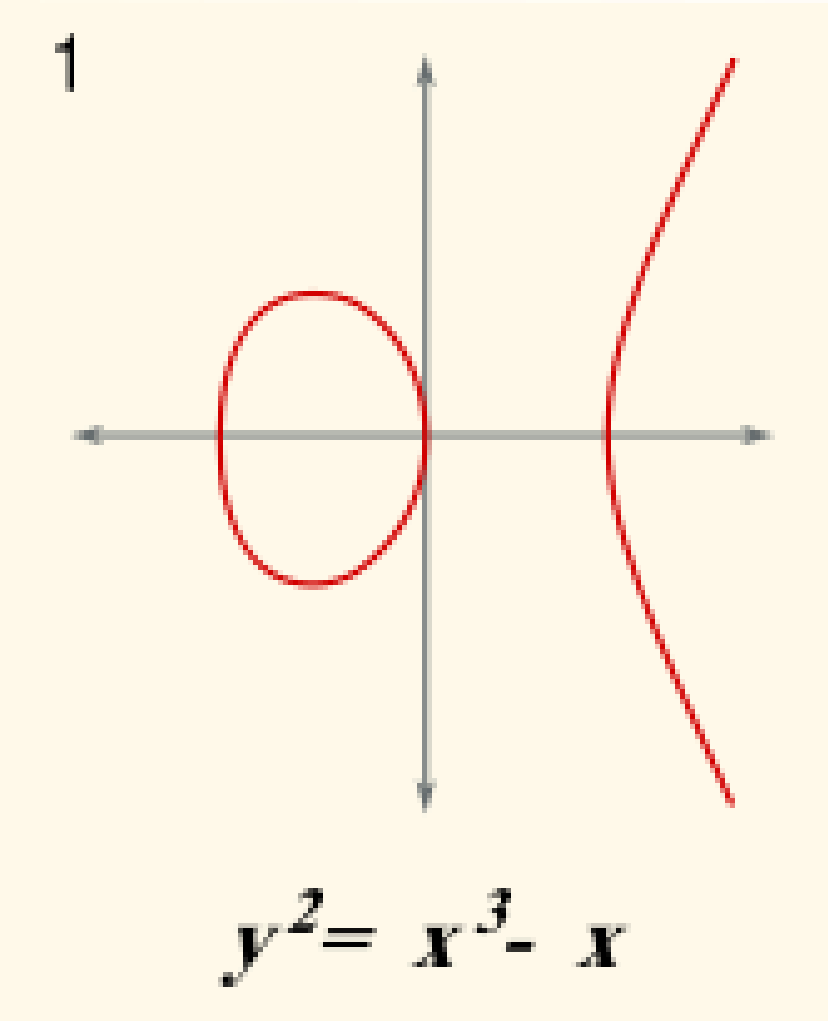
Courbes elliptiques : la géométrie algébrique au service des agents secrets !

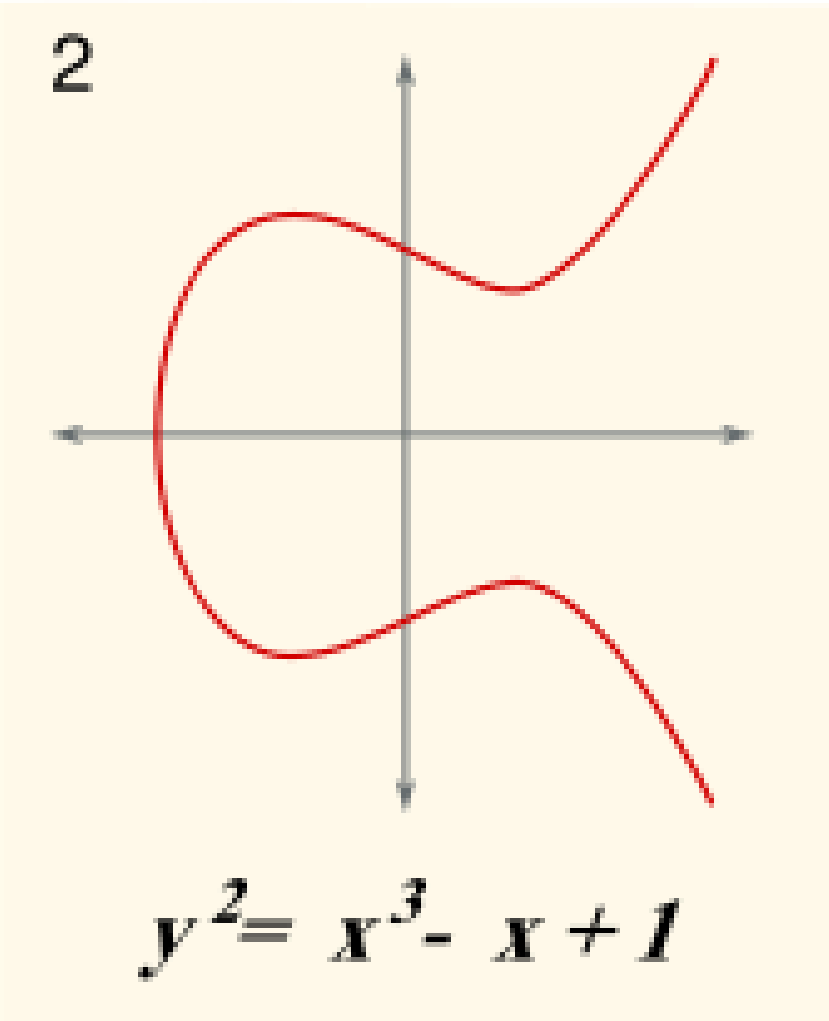
Il ne s'agit pas de courbes ayant la forme d'une ellipse, mais de courbes dont l'étude a débuté au XIXe siècle pour résoudre le problème difficile du calcul du périmètre d'une ellipse. Ces courbes, dont les propriétés sont particulièrement intéressantes, sont l'ensemble des points de coordonnées (x, y) qui vérifient une équation de la forme

$$y^2 = x^3 + ax + b,$$

avec a et b certains nombres réels. Pour des raisons techniques, on suppose que a et b ont été choisit de façon à ce que $4a^3 + 27b^2 \neq 0$.

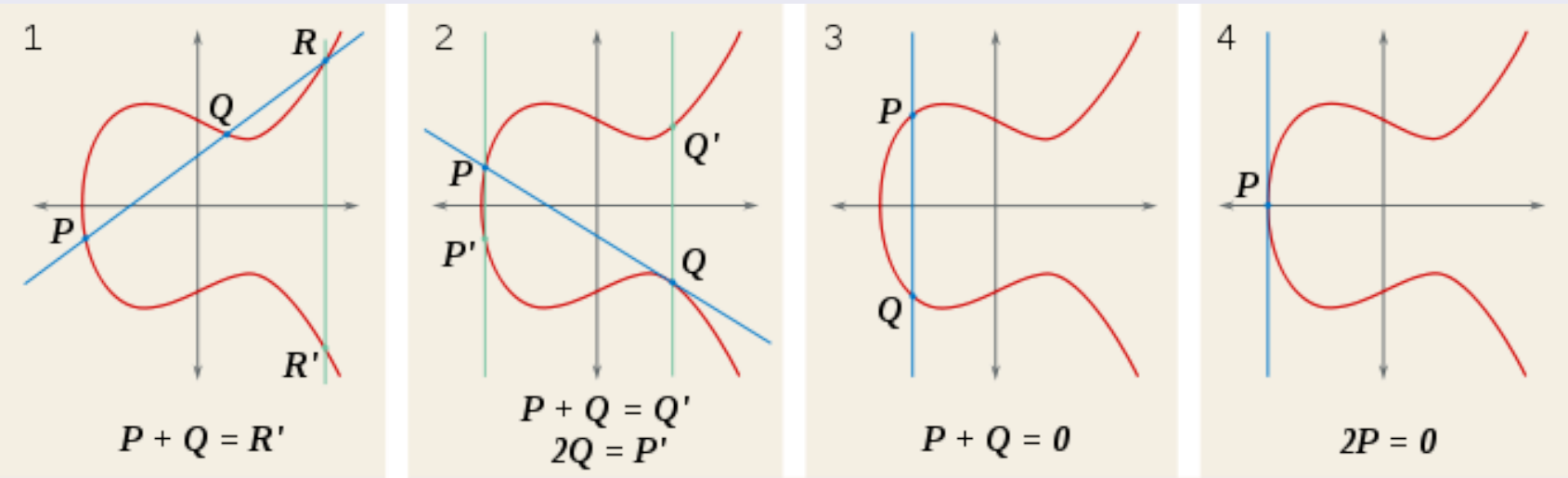
Problème 1





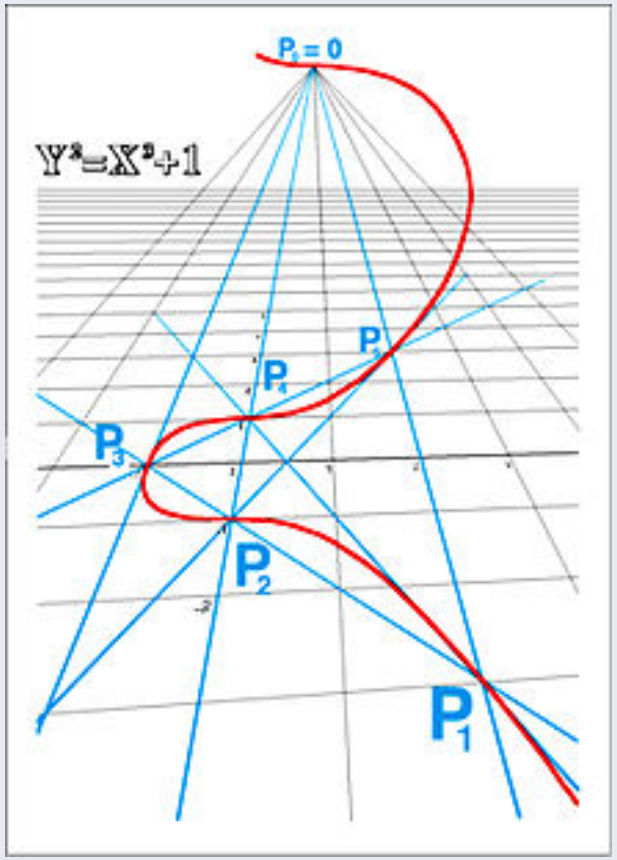
Un peu de folie...

On ajoute des points sur ces courbes comme vous vous ajoutez des entiers relatifs.



Encore plus fou !

On définit le « zéro » ou neutre comme le point à l'infini.



Problème 1

1) Définition de l'addition.

Prendre des points $P(x_1, y_1)$ et $Q(x_2, y_2)$ sur une courbe elliptique et distinguer les différents cas montrés ci-dessus pour définir l'addition sur une courbe elliptique c'est-à-dire retrouver les coordonnées (x_3, y_3) de $P + Q$.

2) Exemple.

Vérifier vos formules sur un exemple numérique.

3) Multiplication par un entier relatif.

Définir la multiplication d'un point d'une courbe elliptique par un entier relatif c'est-à-dire kP pour $k \in \mathbb{Z}$ et P un point d'une courbe elliptique.

Problème 2

Problème du sac à dos

L'énoncé de ce problème fameux est simple : « Étant donné plusieurs objets possédant chacun un poids et une valeur et étant donné un poids maximum pour le sac, quels objets faut-il mettre dans le sac de manière à maximiser la valeur totale sans dépasser le poids maximal autorisé pour le sac ? »

1) Etude d'un cas particulier

On suppose que l'on dispose des données suivantes :

Objets	1	2	3	4
Masse	13	12	8	10
Valeur	7	4	3	3

Donner plusieurs solutions et stratégies lorsque la masse du sac ne doit pas dépasser 30kg.

2) Quand le problème trouve une solution...

On oublie maintenant la valeur des objets, et on suppose que l'on dispose d'un sac dont la masse maximale est M et de n objets de masse respective $m_1, \ldots, m_n$. On souhaite remplir le sac en approchant le plus possible la masse limite M sans la dépasser, sous peine de casser le sac !

Réfléchir à une stratégie lorsque
$m_1 = 2, m_2 = 2^2 = 4, m_3 = 2^3 = 8, \ldots, m_n = 2^n$.

Plus généralement comment résoudre le problème si la suite $m_1, m_2, \ldots, m_n$ des masses des objets est supercroissante : pour tout i, tel que $2 \leq i \leq n$,

$$m_1 + m_2 + \cdots + m_{i-1} < m_i$$

Un peu de magie...

Voici une toile, intitulée la Mélancolie, réalisée par un artiste célèbre Albrecht Dürer :

Rapprochons-nous...

Si nous faisons un zoom sur le carré du haut voici ce que l'on voit :

C'est un carré magique. A une certaine époque on attribuait à ce genre de carré des pouvoirs magiques !

Problème 3

1) Qu'en est-il de la magie ?

Comprendre pourquoi ce carré est magique (indication : si vous trouvez vous n'aurez pas à payer l'addition !)

2) Application

Construire le carré magique d'ordre 3, à trois lignes et trois colonnes, dont les coefficients sont des entiers entre 1 et 9. Attention, j'ai bien dit le carré magique, cela mérite réflexion, et explication...

Problème 4

Où l'on apprend à compter...

On dit qu'un ensemble E est dénombrable (un ensemble dont on peut compter les éléments) s'il existe une bijection entre l'ensemble des entiers naturels $\mathbb{N}$ et E c'est–à-dire :
une application entre $\mathbb{N}$ et E qui a chaque élément de $\mathbb{N}$ fait correspondre un unique élément de E et tel que chaque élément de E correspond à un unique élément de $\mathbb{N}$

1) Avez-vous compris la notion de bijection ?

Prendre des ensembles ayant un nombre fini d'éléments et construire des exemples d'applications qui sont des bijections ?
Pouvez-vous donner une condition pour que deux ensembles finis soient en bijection ?

2) Plus « petit » mais dénombrable !

Montrer que $\mathbb{N}$ est dénombrable. Puis que $\mathbb{N}^*$, les entiers naturels sans zéro, et $\mathcal{P} = \{2k, k \in \mathbb{N}\}$, les entiers pairs sont dénombrables.

2) Plus « gros » mais ...

Que pouvez-dire de l'ensemble $\mathbb{Z}$ des entiers relatifs, et de $\mathbb{Q}$ l'ensemble des rationnels ?
Tous les ensembles sont-ils dénombrables ?