Travaux Dirigés de MT10

Calcul sur courbes elliptiques

Ce TD a pour objectif de se familiariser avec les calculs sur courbes elliptiques.

On considère la pyramide de boules représentée par les figures ci-dessous.

Par conséquent : à 1 étage, il y a une boule, à deux étages 1+4, à 3 étages 1+4+9, à 4 étages 1+4+9+16…

1) Donner une formule générale permettant de calculer le nombre de boules de cette pyramide

Solution : $\sum_{i=1}^{N} i^2$ où N est le nombre d'étages.

*Solution Cette comme vaut N(N+1)(2N+1)/6 , démonstration par récurrence (il existe des démonstrations plus élégantes) : vrai pour N=1, si on la suppose vraie pour N-1 (il y a donc (N-1)N(2N-1)/6 pour N-1 etages donc pour N étages (N-1)N(2N-1)/6+N*N = (N/6)[(N-1)(2N-1)+6N] qui vaut bien N(N+1)(2N+1)/6*

2) On souhaite résoudre le problème suivant : existe-t-il des pyramides de ce type où il est possible de réarranger les boules en un carré, autrement dit étant donné x le nombre de couches existe-t-il des cas où l'on sait trouver un entier y tel que $y^2= x(x+1)(2x+1)/6$?
x=1, y=1 est une solution évidente du problème, ainsi que x=0, y=0 en existe-t-il d'autres ? Le problème est équivalent à la recherche de points sur une courbe elliptique, sachant que l'on connaît déjà deux de ces points. On peut donc imaginer en trouver d'autres en utilisant la loi de groupe (additionner les deux points connus en donne un troisième etc.). On note que l'équation $6y^2=2x^3+3x^2+x$ n'est pas sous la forme de Weierstrass mais des changements de variable permettraient de s'y ramener (ici comme on pourra s'en convaincre à titre d'exercice subsidiaire en posant $X=\frac{1}{\sqrt[3]{3}}\left(x+\frac{1}{2}\right)$ ramène l'équation à $y^2 = X^3 - \frac{\sqrt[3]{3}}{12}X$, ce qui permettrait d'utiliser la loi de groupe sous la forme présentée en cours, mais ici il est plus simple de ré-établir les équations de la loi de groupe dans les variables initiales (ce qui vous rafraichira la mémoire sur la manière dont sont établies ces équations) :
   - Ecrire l'équation d'une droite passant par les points $P_1(x_1,y_1)$ et $P_3(x_2,y_2)$ appartenant à la courbe
     Solution $y=m(x-x_1)+y_1$, ou m est la pente de la droite soit m=(y2-y1)/(x2-x1))
   - Ecrire l'équation donnant l'abscisse des points d'intersection de cette droite et de la courbe elliptique
     Solution $6[m(x-x_1)+y_1]^2= 2x^3+3x^2+x$ ou encore $[m(x-x_1)+y_1]^2=x^3/3+x^2/2+x/6$
   - Etant donné un polynôme en x de degré 3 ayant trois racines x_1, x_2 et x_3 établir le coefficient du terme en x^2 sachant que le coefficient du terme en x^3 vaut 1
     Solution : $(x-x_1)(x-x_2)(x-x_3)=x^3-(x_1+x_2+x_3)x^2+\ldots)$, le coefficient du terme en x^2 est donc l'opposé de la somme des racines si l'on s'est ramené au cas où le coefficient du terme en x^3 vaut 1.
   - Dans notre cas particulier donc chercher ce coefficient du terme en x^2 et en déduire les équations de la loi de groupe (retreinte au cas où les points sont distincts et d'abscisse différente).
     Solution : si le coefficient de x^3 vaut 1/3 celui de x^2 vaut $(1/2 -m^2)$, la somme des racines de l'équation en x donnant l'abscisse des points d'intersection de la droite et de la courbe elliptique vaut donc $3(m^2-1/2)$ d'où
     $x_3=3(m^2-1/2)-x_1-x_2$ et $y_3=m(x_1-x_3)-y_1$
3) Sous cette forme on voit aisément que la courbe peut être définie sur les nombres réels ou complexes bien sûr, mais aussi sur les rationnels. Utilisant le résultat précédent, calculer (0,0)+(1,1), puis l'opposé de ce point (inverse de l'opération d'addition)

Solution : m=1 d'où x3=3(1-1/2)-0-1=3/2-1=1/2, y3=1(0-1/2)-0=-1/2 par conséquent (0,0)+(1,1)=(1/2,-1/2). Dans les coordonnées utilisées, bien que l'équation ne soit pas sous la forme de Weirstrass, il reste vrai que –(x,y)=(x,-y), le point (x,-y) appartenant également à la courbe pour des raisons évidentes de symétrie de l'équation, le troisième point d'intersection de la droite verticale et la courbe étant le point à l'infini. Par conséquent le point (1/2,1/2), comme d'ailleurs le point (1,-1) sont sur la courbe. Pour l'instant cela ne nous apprend pas grand-chose sur les pyramides de boules.

4) Calculer (0,0)+(1,1)+(1,1)

*Solution : le point cherché est donc (1/2,-1/2)+(1,1) m vaut donc m=3 et x_3=3(9-1/2)-1/2-1=24, y3=3(1-24)-1=-70 c'est donc le point (24,-70). Par symétrie le point (24,70) appartient aussi à la courbe (en effet 70*70= 24*25*49/6) ce qui signifie que si l'on a 4900 boules on peut les disposer en une pyramide de 24 étages, ou en un carré de 70x70). C'est la seule solution en nombres entiers autres que les deux triviales… mais ceci est une autre histoire. On peut par contre trouver une infinité de points à coordonnées rationnelles en continuant nos additions…Sur la photo ci-dessous, il n'y a « que » 16 étages..*

5) Courbes elliptiques sur les corps finis : en cryptographie, on utilise des courbes elliptiques définies non pas sur les rationnels mais sur les corps finis, prenons un exemple simple : on considère la courbe suivante définie sur Z/11Z sur l'exemple de $y^2=x^3+x+2$. Vérifier que le point P(4,2) est sur la courbe.

   Solution $y^2=4$, $x^2=16=5$, $x^3=20=9$, $x^3+x+2=9+4+2=15=4$)

6) Calculer 2P puis 3P :

Solution 2P=P+P, dans ce cas il faut prendre la tangente en P:

Rappels d'une manière générale $x_3=m^2-x_1-x_2$ et $y_3=m(x_1-x_3)-y_1$
avec pour lorsque les deux points sont distincts $m=(y_2-y_1)/(x_2-x_1)$
et lorsqu'ils ne le sont pas la pente de la tangente : $m=(3x_1^2+A)/2y_1$ où A est le coefficient de x dans l'équation de la courbe sous la forme de Weierstrass (ici A=1) et l'équation en x_3 devenant $x_3=m^2-2x_1$

*Donc ici m=(3*5+1)/4 =5/4 il faut donc déterminer l'inverse de 4 ce qu'on pourrait faire par Euclide mais il est ici évident que 4*3=1 donc m=5*3=4 et m^2=5 donc x_3=5-2*4=-3=8 et y_3=4(4-8)-2=-16-2=-18=4 par conséquent P+P=(8,4), le fait que cela corresponde à l'addition des entiers dans chaque composante étant purement fortuit.*
*On vérifie à toutes fins utiles que ce point est bien sur la courbe : 8*8=64=9, donc 8^3=9*8=72=6 donc 8^3+8+2=6+8+2=16=5, 4*4=16=5*

*Pour calculer 3P on prend la pente entre les points P et 2P soit m=(4-2)/(8-4)=2/4=2*3=6 et m^2=36=3 d'où x_3=3-8-4=-9 = 2 et y_3=6(4-2)-2=12-2=10 (on aurait pu faire aussi 6(8-2)-4=36-4=32=10 qui donne le même résultat en inversant les rôles de P et de 2P). Donc le point 3P vaut (2,10)*
*On vérifie de même que le point est bien sur la courbe : 2*2*2+2+2=8+2+2=12=1, 10*10=100=1*

7) Déterminer tous les éléments du groupe et étudier sa structure (demande un peu de patience ou un outil dans ce cas)

Solution : par la méthode exposée en cours, on calcule toutes les valeurs possibles de y^2 (quand y prend les 11 valeurs possibles) et de x^3+x+2 (quand x prend toutes les valeurs possibles) et on détermine les valeurs communes qui donnent les points de la courbe, on n'oublie pas le point à l'infini. On trouve que c'est un groupe d'ordre 16 dont les points sont :
∞
(2,1), (2,10) : valeur de y^2 et x^3+x+2 : 1
(1,2), (1,9), (4,2), (4, 9), (6,2), (6, 9) : valeur de y^2 et x^3+x+2 : 4
(5,0), (7,0), (10,0) : valeur de y^2 et x^3+x+2 : 0
(8,4), (8,7) : valeur de y^2 et x^3+x+2 : 5
(9,5), (9,7) : valeur de y^2 et x^3+x+2 : 3
On peut ensuite trouver la structure complète en recherchant les groupes cycliques engendrés par les éléments, on se souvient du théorème de Lagrange qui permettra de détecter de possibles erreurs de calcul dans la détermination des sous-groupes cycliques.
Les tables ci-dessous sont générées par les web-outils MT10 disponibles sur mes pages web.
Liste des groupes cycliques :
(1,2) -> (10,0) -> (1,9) -> ∞
(1,9) -> (10,0) -> (1,2) -> ∞
(2,1) -> (8,4) -> (4,9) -> (10,0) -> (4,2) -> (8,7) -> (2,10) -> ∞
(2,10) -> (8,7) -> (4,2) -> (10,0) -> (4,9) -> (8,4) -> (2,1) -> ∞
(4,2) -> (8,4) -> (2,10) -> (10,0) -> (2,1) -> (8,7) -> (4,9) -> ∞
(4,9) -> (8,7) -> (2,1) -> (10,0) -> (2,10) -> (8,4) -> (4,2) -> ∞
(5,0) -> ∞
(6,2) -> (8,4) -> (9,6) -> (10,0) -> (9,5) -> (8,7) -> (6,9) -> ∞

(6,9) -> (8,7) -> (9,5) -> (10,0) -> (9,6) -> (8,4) -> (6,2) -> ∞
(7,0) -> ∞
(8,4) -> (10,0) -> (8,7) -> ∞
(8,7) -> (10,0) -> (8,4) -> ∞
(9,5) -> (8,4) -> (6,9) -> (10,0) -> (6,2) -> (8,7) -> (9,6) -> ∞
(9,6) -> (8,7) -> (6,2) -> (10,0) -> (6,9) -> (8,4) -> (9,5) -> ∞
(10,0) -> ∞
∞

Table d'addition

	(1,2)	(1,9)	(2,1)	(2,10)	(4,2)	(4,9)	(5,0)	(6,2)	(6,9)	(7,0)	(8,4)	(8,7)	(9,5)	(9,6)	(10,0)	∞
(1,2)	(10,0)	∞	(9,6)	(6,2)	(6,9)	(9,5)	(8,7)	(4,9)	(2,1)	(8,4)	(5,0)	(7,0)	(2,10)	(4,2)	(1,9)	(1,2)
(1,9)	∞	(10,0)	(6,9)	(9,5)	(9,6)	(6,2)	(8,4)	(2,10)	(4,2)	(8,7)	(7,0)	(5,0)	(4,9)	(2,1)	(1,2)	(1,9)
(2,1)	(9,6)	(6,9)	(8,4)	∞	(8,7)	(10,0)	(9,5)	(1,2)	(7,0)	(6,2)	(4,9)	(2,10)	(1,9)	(5,0)	(4,2)	(2,1)
(2,10)	(6,2)	(9,5)	∞	(8,7)	(10,0)	(8,4)	(9,6)	(7,0)	(1,9)	(6,9)	(2,1)	(4,2)	(5,0)	(1,2)	(4,9)	(2,10)
(4,2)	(6,9)	(9,6)	(8,7)	(10,0)	(8,4)	∞	(6,2)	(1,9)	(5,0)	(9,5)	(2,10)	(4,9)	(1,2)	(7,0)	(2,1)	(4,2)
(4,9)	(9,5)	(6,2)	(10,0)	(8,4)	∞	(8,7)	(6,9)	(5,0)	(1,2)	(9,6)	(4,2)	(2,1)	(7,0)	(1,9)	(2,10)	(4,9)
(5,0)	(8,7)	(8,4)	(9,5)	(9,6)	(6,2)	(6,9)	∞	(4,2)	(4,9)	(10,0)	(1,9)	(1,2)	(2,1)	(2,10)	(7,0)	(5,0)
(6,2)	(4,9)	(2,10)	(1,2)	(7,0)	(1,9)	(5,0)	(4,2)	(8,4)	∞	(2,1)	(9,6)	(6,9)	(8,7)	(10,0)	(9,5)	(6,2)
(6,9)	(2,1)	(4,2)	(7,0)	(1,9)	(5,0)	(1,2)	(4,9)	∞	(8,7)	(2,10)	(6,2)	(9,5)	(10,0)	(8,4)	(9,6)	(6,9)
(7,0)	(8,4)	(8,7)	(6,2)	(6,9)	(9,5)	(9,6)	(10,0)	(2,1)	(2,10)	∞	(1,2)	(1,9)	(4,2)	(4,9)	(5,0)	(7,0)
(8,4)	(5,0)	(7,0)	(4,9)	(2,1)	(2,10)	(4,2)	(1,9)	(9,6)	(6,2)	(1,2)	(10,0)	∞	(6,9)	(9,5)	(8,7)	(8,4)
(8,7)	(7,0)	(5,0)	(2,10)	(4,2)	(4,9)	(2,1)	(1,2)	(6,9)	(9,5)	(1,9)	∞	(10,0)	(9,6)	(6,2)	(8,4)	(8,7)
(9,5)	(2,10)	(4,9)	(1,9)	(5,0)	(1,2)	(7,0)	(2,1)	(8,7)	(10,0)	(4,2)	(6,9)	(9,6)	(8,4)	∞	(6,2)	(9,5)
(9,6)	(4,2)	(2,1)	(5,0)	(1,2)	(7,0)	(1,9)	(2,10)	(10,0)	(8,4)	(4,9)	(9,5)	(6,2)	∞	(8,7)	(6,9)	(9,6)
(10,0)	(1,9)	(1,2)	(4,2)	(4,9)	(2,1)	(2,10)	(7,0)	(9,5)	(9,6)	(5,0)	(8,7)	(8,4)	(6,2)	(6,9)	∞	(10,0)
∞	(1,2)	(1,9)	(2,1)	(2,10)	(4,2)	(4,9)	(5,0)	(6,2)	(6,9)	(7,0)	(8,4)	(8,7)	(9,5)	(9,6)	(10,0)	∞

Ce groupe n'est donc pas cyclique

8) Étudier (éléments du groupe, structure, générateurs éventuels, table d'addition) la courbe elliptique $y^2=x^3+3x+2$ définie sur Z/5Z
Solution : groupe d'ordre 5, tous les éléments en dehors de ∞ sont générateurs

	(1,1)	(1,4)	(2,1)	(2,4)	∞
(1,1)	(2,1)	∞	(2,4)	(1,4)	(1,1)
(1,4)	∞	(2,4)	(1,1)	(2,1)	(1,4)
(2,1)	(2,4)	(1,1)	(1,4)	∞	(2,1)
(2,4)	(1,4)	(2,1)	∞	(1,1)	(2,4)
∞	(1,1)	(1,4)	(2,1)	(2,4)	∞

9) Mêmes questions pour $y^2=x^3+x+2$ définie sur Z/5Z

Solution : C'est l'exemple du cours : groupe d'ordre 4, (1,2) et (1,3) sont générateurs (4,0) est son propre inverse. Ce groupe est donc isomorphe au groupe additif Z/4Z ou au groupe multiplicatif $(Z/5Z)^*$

	(1,2)	(1,3)	(4,0)	∞
(1,2)	(4,0)	∞	(1,3)	(1,2)
(1,3)	∞	(4,0)	(1,2)	(1,3)
(4,0)	(1,3)	(1,2)	∞	(4,0)
∞	(1,2)	(1,3)	(4,0)	∞

10) Mêmes questions pour $y^2=x^3+x$ définie sur Z/5Z

Solution : groupe d'ordre 4 également mais tous les éléments sont leur propre inverse (donc isomorphe au groupe (Z/2Z)x(Z/2Z) muni de l'addition composante par composante.

	(0,0)	(2,0)	(3,0)	∞
(0,0)	∞	(3,0)	(2,0)	(0,0)
(2,0)	(3,0)	∞	(0,0)	(2,0)
(3,0)	(2,0)	(0,0)	∞	(3,0)
∞	(0,0)	(2,0)	(3,0)	∞