Travaux Dirigés de MT10

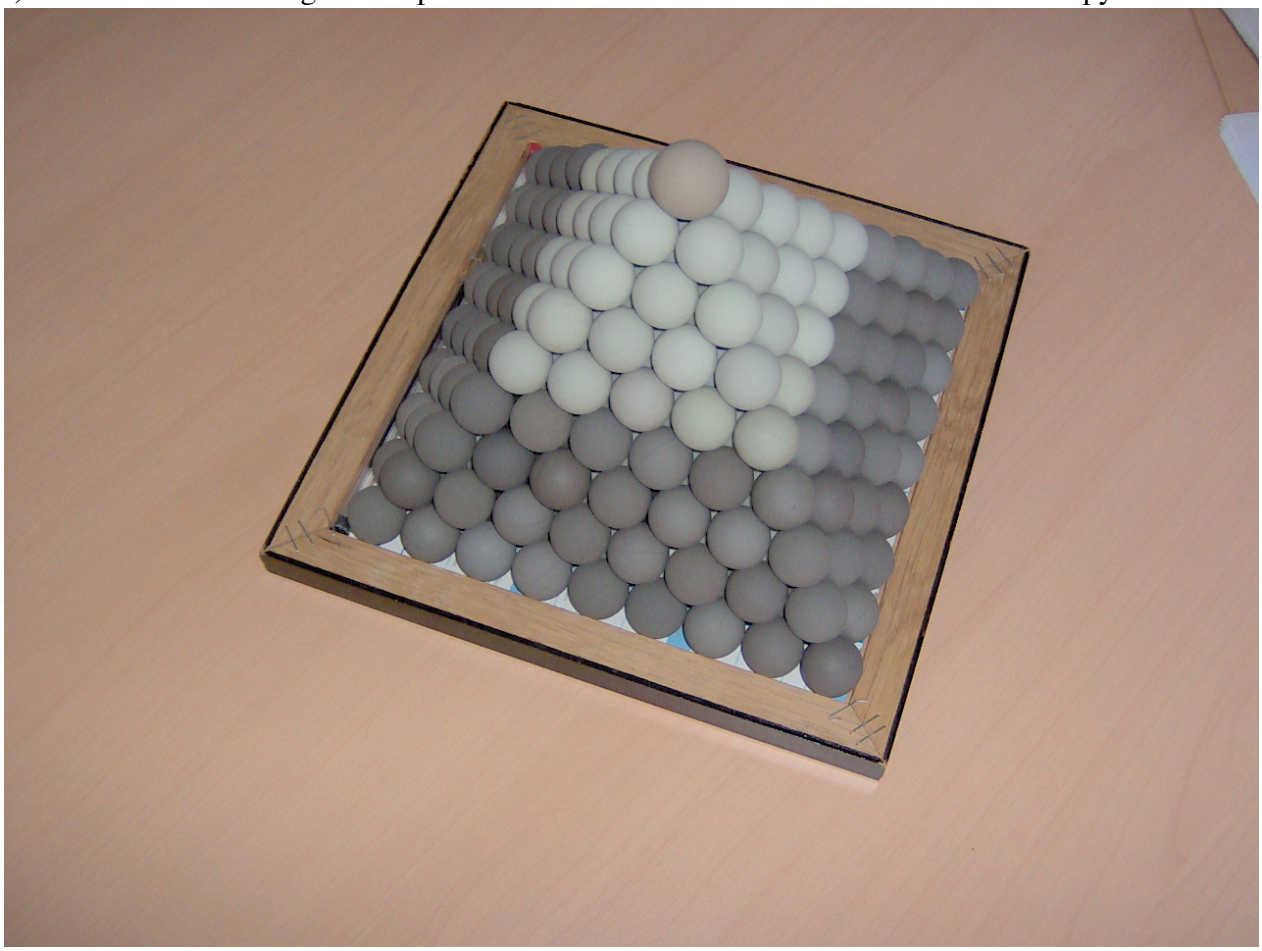
Calcul sur courbes elliptiques

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



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
- Ecrire l'équation donnant l'abscisse des points d'intersection de cette droite et de la courbe elliptique
- 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
- 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).

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)
4) Calculer (0,0)+(1,1)+(1,1)
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
6) Calculer 2P puis 3P
7) Déterminer tous les éléments du groupe et étudier sa structure (demande un peu de patience ou un outil dans ce cas).
8) Étudier (éléments du groupe, structure, générateurs éventuels, table d'addition) la courbe elliptique $y^2=x^3+3x+2$ définie sur Z/5Z
9) Mêmes questions pour $y^2=x^3+x+2$ définie sur Z/5Z
10) Mêmes questions pour $y^2=x^3+x$ définie sur Z/5Z