1 Arithmétique et Cryptographie

1.1 PROGRAMME AGREG

A reviser pour la planche :
Entiers relatifs. Division euclidienne. Nombres premiers et decomposition en produit de nombres premiers. PGCD, PPCM.Théorème de Bachet-Bezout et relation de Bezout. Congruences et anneaux Z/nZ. Groupe des inversibles de Z/nZ et indicatrice d'euler. Théorème Chinois.
partie du programme d'agrégation abordée en plus
Problèmes de calendrier , codages et cryptages. Equations diophantiennes du type $ax + by = c$.

1.2 exercices

.

Exercice ($ax + by = c$)
On cherche les solutions entières de l'équation $17x + 25y = 13$
1) Ecrire une relation de bezout pour 17 et 25 et en déduire une solution de l'équation précédente.
2) Déduire toutes les solutions de l'équation.
3) Décrire la méthode de résolution générale des equations diophantiennes de type $ax + by = c$.

Exercice (résolution systématique de congruences simultannées) : On considère a et b des entiers premiers entre eux et l'isomorphisme d'anneaux f de $\mathbb{Z}/ab\mathbb{Z}$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ donné par le théorème chinois.
1) ici a=8 et b=21.
a) Ecrire une relation de bezout pour a et b.
b)Déterminer alors un multiple de a congru à 1 modulo 21 et un multiple de b congru à 1 modulo 8
c) En déduire un entier congru à 7 modulo a et à 14 modulo b.
2) Déduire du 1) une méthode pour trouver rapidement l'antécédent par f d'un élément quelconque de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Exercice d'application (un problème de calendrier) :
en 2011 le 3 septembre tombait un samedi alors qu'en 2012 le 3 septembre tombait un lundi. D'une année sur l'autre les jours de la semaine ne tombent donc pas aux même dates.
En fait en observant les différents les calendriers sur plusieurs dizaines d'années on remarque que toutes les 28 années les jours de la semaine reviennent à la même date. D'autre part on observe d'une année sur l'autre un décalage similaire pour les lunaisons (pleine lune, nouvelle lune) ainsi les pleines lunes de 2012 ne sont pas tombé aux même dates que celle des 2011.
Là encore l'observation des calendrier montre que tous les 19 ans les lunaisons retombent aux mêmes dates du mois.
Trouver la prochaine année pour laquelle simultanément :
- les jours de la semaines tomberont aux même dates qu'en 2017.
- les lunaisons tomberont aux même dates qu'en 2006.

Exercice (indicatrice d'euler)
Soit n un entier naturel supérieur ou égal à 2, on note $\varphi(n)$ le nombre d'éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$(c'est à dire l'ordre du groupe des inversibles).
0) Montrer que les inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont aussi les générateurs de de $(\mathbb{Z}/n\mathbb{Z}, +)$ et les classes des entiers premiers avec n.
1) Calculer $\varphi(n)$ dans le cas où n est premier.
2) A l'aide du lemme chinois, dans le cas où $n = pq$ avec p, q des nombres premiers montrer que $\varphi(n) = (p-1)(q-1)$.
3) Dans le cas où $n = p^k$ avec p premier et k entier montrer que $\varphi(n) = (p-1)p^{k-1}$.
4) En s'isprirant du 2) et du 3) calculer $\varphi(p^k q^r)$ avec p, q premiers et k, r entiers naturels non nuls.

Exercice(puissances dans $\mathbb{Z}/n\mathbb{Z}$)
1) (méthode fine)Calculer le chiffre des unité de $7^{(3^{10})}$ et exploitant l'egalité $\varphi(10) = 4$.
2) (Méthode calculatoire : Exponentiation rapide) Calculer à la main le chiffre des unités de 8^{1040} (calculer dans $\mathbb{Z}/10\mathbb{Z}$ $8^2, 8^4, 8^{16}, 8^{32}$ etc...). La methode fine s'adapte t'elle ?
3) Proposer une méthode fine pour le 2) exploitant l'isomorphisme d'anneau entre $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice (RSA)
Alice veut pouvoir recevoir un message crypté à bob. Elle choisit deux nombres premiers p et q et deux entiers c et d vérifant $cd = 1[\varphi(n)]$ avec $n = pq$.
On suppose que le message m de bob est un élément de $\mathbb{Z}/n\mathbb{Z}$, qu'alice est seule à connaitre p, q et d(clé de dechiffrage) et que c(clé de chiffrage) et n sont connus de tous.
1) Bob envoit à Alice $x = m^c$, alice calcule alors x^d. Justifier à l'aide du lemme chinois que $x^d = m$.
2) Dans le cas où $p = 7$,$q = 11$ et $c = 13$ déterminer une valeur de d qui conviendrait.
3) (Mauvaise utilisation de RSA) Supposons que bob envoi le même message m élément de $\mathbb{Z}/n\mathbb{Z}$ à alice et à charlie avec des clés de chiffrement respectivement égales à c_1 et c_2 supposés premiers entre eux.
On considère deux entiers a, b tels que $ac_1 + bc_2 = 1$.
Expliquer comment David qui a intercepté m^{c_1} et m^{c_2} peut retrouver m sans connaitre les clés de dechiffrement.

Exercice(chiffrement de Rabin)
1)Soit p un nombre premier congru à 3 modulo 4, montrer que si a est un carré dans $\mathbb{Z}/p\mathbb{Z}$ alors les solutions de $x^2 = a$ sont $\pm a^{\frac{p+1}{4}}$
2) Soit p, q des nombres premiers distincts congru à 3 modulo 4 , soit a un carré de $\mathbb{Z}/n\mathbb{Z}$ et $n = pq$. Expliquer comment à l'aide du lemme chinois on peut trouver les solutions de $x^2 = a$. Faire le calcul avec $p = 11, q = 23, a = 169$.
On suppose qu'Alice seule connait p et q, qu'elle a choisi $B \in \mathbb{Z}/n\mathbb{Z}$ et a publié n et B. Bob veut lui transmettre un message $x \in \mathbb{Z}/n\mathbb{Z}$.
Il calcule $C = x(x + B)$ et transmet C à Alice qui n'a plus qu'à résoudre l'équation du second degré pour trouver x.
3) Justifier que 2 et 4 sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ et montrer que l'équation précédente est équivalente à $(x + \frac{1}{2}B)^2 = C + \frac{1}{4}B^2$
4) Expliquer la méthodes qu'alice pourra mettre en oeuvre pour résoudre cette dernière équation. Combien de solutions trouvera elle ?