**Département d’informatique 11/02/2020**

**3ème année licence**

**Module : Cryptographie**

**Série 2 (Concepts *mathématiques)***

**Cours :**

1. Que représente l’expression 31 mod 26 ? Quelle est sa valeur ?

2. Que vaut −3 mod 26 ?

3. Rappeler la définition d’un nombre premier, du pgcd de deux entiers.

**Exercice 1 :** Calculez

* 2256 mod 128 = 0
* 529436 mod 66 = 1
* 10234064 mod 1024 = 1
* 100325 mod 391 = 36
* 15362 mod 26 = 17
* Le reste de la division de 10351255642 par 17 = 9
* 5555555555 mod 7 = 16
* 10100 mod 247 = 237

**Exercice 2 :**

* Montrer que pour tout n ∈ N∗ , **n5 − n** est divisible par **30**
* Montrer que **236 + 518** est divisible par **41**
* Déterminer, suivant les puissances de n∈N, le reste de la division euclidienne de **2n  par 5**.
* Quel est le reste de la division par **5 de 13572013** ?

**Exercice 3 :** Algorithme *d'Euclide Etendu*

On demande de trouver les coefficients de Bézout pour les nombres entiers suivants:

* (a, b)= (19, 60) = PGCD(19,60)= 1= au + bv = 19 \* 19 + 60\*(-6)
* (a, b)= (11,280) = 1 = 11\*51 + 280\*(-2)
* (a, b)= (38, 26) = 2 = 38\*(-2)+ 26\*3
* (a,b) = (99,78) = 3= 99\*(-11) + 78\*14

**Exercice 4:** *inverse modulaire*

Calculer l'inverse de : 4-1 mod 53 = 22

317-1 mod 521 = 166

 8-1 mod 40 = Pas de solution PGCD(8,40) différent de 1

**Exercice 5:** *Calcul modulaire*

Résoudre les équations suivantes:

* 19x ≡10 mod 60
* 18x ≡9 mod 27
* 8y ≡ 17 mod 32

**Remarque :** Les solutions seront détaillées prochainement.