D13 - ARITHMETIQUE
14:00–15:00, salle W'210

14 décembre 2015

1 exercice

Soit A un anneau fini non commutatif. Pour un élément x de A, on considère les assertions :

1. Il existe un élément $y \in A$ tel que $xy = 1$.
2. Il existe un élément **non nul** $z \in A$ tel que $zx = 0$.

(a) Que dit-on quand x satisfait (1).
(b) Que dit-on quand x satisfait (2).
(c) Montrer que x ne peut pas vérifier à la fois (1) et (2).

```
exam> p=83
exam> factor $p
83: 83
exam> let s=(p-1)/2
exam> factor $s
41: 41
exam> bc <<< "2^$s % $p"
82
exam> bc <<< "3^$s % $p"
1
exam> bc <<< "2^27  % $p"
5
exam> bc <<< " 5^9 % $p"
52
```

2 exercice

On considère le nombre $p = 83$.

1. Quelle la nature de p ?
2. Quel est l'ordre multiplicatif de 2 modulo p.
3. Quel est l'ordre multiplicatif de 3 modulo p.
4. Donner un générateur de $\mathbf{F}_p{}^\star$.
5. Détailler les étapes du calcul de l'inverse de 52 modulo p.
6. Utiliser l'algorithme "pas de bébé", "pas de géant" pour déterminer le logarithme de 7 en base 5 modulo p.