D0xd : arithmétique

29 juin 2015

Soit p un nombre premier impair. Si $2p+1$ est premier alors

$$\forall x, y, z \in \mathbf{Z},\ x^p + y^p = z^p \Rightarrow p^2 | xyz$$

1 exercice

Compléter la suite numérique :

$$3, 5, 11, 23, 29, 41, \ldots$$

2 exercice

Dans la suite, vous utiliserez librement le résultat des commandes suivantes concernant les nombres premiers $q = 83$ et $p = 41$.

```
mlc> p=41
mlc> let q=2p+1
mlc> bc <<< "(2^$p) % $q"
82
```

1. Que peut-on dire du nombre premier p ?
2. Quel est l'ordre multiplicatif de 2 modulo q ?

3 exercice

Calculer les paramètres du système de chiffrement RSA de module $n = pq$ correspondant à l'exposant de chiffrement $e = 3$.

4 exercice

Déterminer une paire d'entiers (u, v) tel que :

$$pu + qv = 1,$$

puis résoudre l'équation

$$x^2 = 1 \pmod{n}.$$

5 exercice

Utiliser la méthode dite "pas de bébé, pas de géant" pour calculer le logarithme discret de 3 en base 2 modulo 83. Prendre soin de détailler les principales étapes de l'algorithme.