MPRI – cours 2.12.2

F. Morain

Feuille d'exercices, 2014/09/29

1. Trouver une famille d'entiers N composés vérifiant $F(N) = \varphi(N)/4$.

2. Trouver tous les entiers $0 \leq k \leq 100$ tels que $2 \cdot k! + 1$ soit premier et en donner des certificats de primalité.

3. Programmer le crible d'Eratosthènes. Énumérer tous les nombres premiers $\leq 2^{32}$ et expliquer comment les stocker à l'aide d'un caractère (8 bits) dans un fichier.

4. Démontrer le théorème de Pocklington.

5. (Fonction de Möbius et formule d'inversion de Möbius) La fonction de Möbius est la fonction définie sur $\mathbb{N} - \{0\}$ par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 p_2 \ldots p_k \text{ est un produit de } k \text{ nombres premiers distincts.} \\ 0 & \text{sinon.} \end{cases}$$

(a) Montrer que la fonction de Möbius possède la propriété suivante :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon.} \end{cases}$$

(b) (Première formule d'inversion de Möbius) Soit $f\ : \mathbb{N}^* \to \mathbb{C}$, et $g\ : \mathbb{N}^* \to \mathbb{C}$ définie par

$$g(n) = \sum_{d|n} f(d).$$

Alors

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

6. Utiliser l'exercice 5 pour prouver que pour tout p et n, il existe un polynme irrductible de degr n.