Université de Bordeaux — **MHT911 – Master CSI**
Mathématiques — 2015–2016

FEUILLE D'EXERCICES n° 3

Exercice 1 – Programmer le test de non-primalité de Rabin-Miller

Exercice 2 –

1) Programmer la preuve de primalité Pocklington-Lehmer, qui prend en entrée un entier N et retourne un certificat de primalité.

2) Écrire un programme de vérification du certificat produit par la question précédente.

Exercice 3 – Programmer la méthode ρ de factorisation dans $\mathbb{Z}$ de Pollard.

Exercice 4 – Programmer l'algorithme de factorisation dans $\mathbb{Z}$ de Dixon.