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

FEUILLE D'EXERCICES n° 2

Exercice 1 – En représentant les polynômes de $\mathbb{Z}[X]$ des tableaux d'entiers, programmer la multiplication $a \times b$ (algorithme naïf).

Exercice 2 – En représentant les entiers $a, b > 0$ par des tableaux de bits, programmer la multiplication $a \times b$ (algorithme naïf). Tester la complexité pratique.

Exercice 3 – Programmer l'algorithme de multiplication de Karatsuba, appliqué à deux entiers $0 \leqslant a, b < B^n$, où $B = 2^{32}$. Pour le découpage $a = a_1 B^{n/2} + a_0$, on pourra utiliser

```
a1 = a >> (16*n);
a0 = a - a1 << (16*n);
```

1) Tester la complexité pratique de votre implantation.

2) Que se passe-t'il si on remplace les expressions ci-dessus par les définitions plus naturelle

```
N = 2^(16*n); a1 = a \ N; a0 = a % N;
```

Exercice 4 – `Mod(a,N)` est un constructeur pour la classe de congruence $a \in \mathbb{Z}/N\mathbb{Z}$.

1) Évaluer la complexité pratique des opérations $+, -, \times, /$ dans $\mathbb{Z}/N\mathbb{Z}$ (en fonction de la taille de N).

2) La fonction `gcd` calcule un pgcd et `gcdext` une relation de Bezout.

a) Comparer leurs complexité pratique.

b) Estimer expérimentalement la probabilité que deux entiers dans $[0, X]^2$ soient premiers entre eux (quand $X \to \infty$).

3) Écrire un programme retournant un vecteur contenant les éléments inversibles de $\mathbb{Z}/N\mathbb{Z}$.

4) [*Réduction paresseuse*]. Écrire une fonction calculant le produit scalaire de deux vecteurs de $(\mathbb{F}_p)^n$; tester là avec des vecteurs de `t_INTMOD`s, puis avec des vecteurs d'entiers en réduisant le résultat *final* modulo p.

Exercice 5 –

1) Programmer les tests de non-primalité de Miller-Rabin et Solovay-Strassen. La fonction `kronecker(a,b)` calcule le symbole de Jacobi $\left(\frac{a}{b}\right)$.

2) Pour un entier impair N non premier, calculer le nombre de faux-témoins pour l'un et l'autre test. Essayer plusieurs valeurs de N, en particulier $N = 561$. (On doit atteindre sans problême des valeurs de l'ordre de 10^6.)