Chapitre 8

TDs, TPs Projets

TP/TD 1

L'objectif de se TP est d'expérimenter quelques notions d'arithmétique, d'arithmétique modulaire et de découvrir la classe BigInteger *de Java. Tous les (grands) entiers manipulés dans ce TP seront des objets de cette classe.*

Il vous sera demandé de mesurer des temps d'exécution moyens de certaines *tâches* (en utilisant par exemple *System.currentTimeMillis()* en java). Il sera parfois nécessaire de répéter la tâche un grand nombre de fois t, e.g. $t = 10000$, pour obtenir un temps significatif (de plusieurs secondes) et de diviser le temps total par t.

Exercice 73. *Importer la classe BigInteger et lisez sa javadoc ! On prêtera notamment attention aux constructeurs.*

Exercice 74.

1. *Générer aléatoirement 2 entiers a et b de 2048 bits. Afficher-les.*
2. *Quelle est la taille (en nombres de bits) de $a + b$ et $a \times b$.*
3. *Quels sont les temps d'exécution pour obtenir $a + b$, $a \times b$, a/b et $a \mod b$ (avec les méthodes* sum, multiply, divide *et* mod*).*

Exercice 75.

1. *Générer aléatoirement 2 entiers a et b de 2048 bits.*
2. *Approximer (expérimentalement) la probabilité que a soit premier.*
3. *Approximer (expérimentalement) la probabilité que a et b soient premiers entre eux, i.e. $\mathsf{pgcd}(a, b) = 1$.*

Exercice 76.

1. *Générer aléatoirement un entier p* ***non-premier*** *de 2048 bits.*
2. *Proposer et implémenter une méthode $\mathsf{AleaInf}(p)$ pour générer aléatoirement un entier a dans l'ensemble $\{1, 2, \ldots, p-1\}$.*

3. *Soit* $a = \mathsf{AleaInf}(p)$. *Calculer* $a^{p-1} \mod p$ *de 2 manières différentes :*
   (a) *En calculant* $c = a^{p-1}$ *puis* $c \mod p$
   (b) *En utilisant la méthode* modPow

   Quelle est la plus efficace ?
4. *Mesurer (expérimentalement) la probabilité que* $a^{p-1} \mod p = 1$ *(en échantillonnant a,p comme décrit ci-dessus).*

Exercice 77.

1. *Générer aléatoirement un entier premier p de 2048 bits.*
2. *Quel est le temps (moyen) de génération de p ?*
3. *Soit* $a = \mathsf{AleaInf}(p)$. *Vérifier (expérimentalement) que* $a^{p-1} \mod p = 1$.
4. *En déduire un test de primalité efficace.*

Exercice 78. *L'inverse modulaire de a modulo n est un entier* $b \in \{1, \ldots, n-1\}$ *tel que* $a \times b \mod n = 1$.

1. *Générer deux nombres premiers p et q de 1024 et les multiplier, i.e.* $n = pq$.
2. *Soit* $a = \mathsf{AleaInf}(p)$. *Calculer l'inverse b de a modulo n avec la fonction* modInverse.
3. *Vérifier que* $(a \times b) \mod n = 1$.
4. *Quel est l'inverse de p modulo n. Justifier.*