Exercice 1

Soit N un entier composé, produit de k nombres premiers distincts. On suppose qu'on dispose de s congruences uniformément aléatoires de la forme $x^2 \equiv y^2 \mod N$. Donner une borne inférieure sur la probabilité que l'une de ces congruences permette de factoriser N.

Exercice 2

À partir de quelle taille de nombres N un hyptothétique algorithme de complexité exactement $L_N[1/2, 1]$ est-il plus rapide qu'un algorithme de complexité exactement $N^{1/4}$.

Exercice 3

Soit $G = \langle g \rangle$ un groupe cyclique. On suppose qu'on doit calculer le logarithme discret de r éléments $(a_i)_{1 \leq i \leq r}$ dans la base g. Comment modifier l'algorithme des pas de bébé et des pas de géant pour optimiser le calcul de ces logarithmes, avec quel coût final ?

Exercice 4

Soit M une matrice définie sur un corps fini K. On dispose d'un algorithme $\mathcal{A}$ qui, pour $b \in \Im(M)$, obtient une solution du système linéaire inhomogène $Mx = b$. Montrer qu'on peut utiliser $\mathcal{A}$ pour obtenir un vecteur alatoire x du noyau de M (c'est-à-dire tel que $Mx = 0$). On veillera à montrer qu'on peut obtenir une solution x uniformément distribuée dans le noyau de M.

Exercice 5

Soit $p = 4m + 3$ un nombre premier tel que $q = 2p + 1$ est premier. Montrer que -2 est un générateur multiplicatif de $(\mathbb{Z}/q\mathbb{Z})^*$.

Exercice 6

On considère l'algorithme de calcul de logarithme discret d'Adleman dans le corps fini premier $\mathbb{F}_q$ de générateur g. Dans la première phase, on cherche des nombres B-friables satisfaisant

$$g^b \equiv \prod_{p \leq B} p^{e_p}.$$

On suppose qu'on teste cette B-friabilité avec un algorithme sensible non pas à la taille des nombres factorisés, mais à la taille de leur plus petit facteur, c'est-à-dire qu'on dispose d'un algorithme $\mathcal{A}(n)$ qui en un temps $T(B)$ renvoie soit un facteur $p \leq B$ de n, soit échoue. Un tel algorithme est souvent probabiliste, mais on fait le choix d'ignorer cet aspect.
Dans le cas où le temps $T(B)$ s'écrit $L_B[1/2, c]$, donner la complexité de l'algorithme d'Adleman (complexité optimale de la phase de recherche, de la phase d'algèbre linéaire, etc). Il faut aussi donner la complexité optimale de la seconde phase, dans laquelle on doit chercher une instance $g^b h$qui est B-friable pour trouver le logarithme discret de h en base g.

Exercice 7

On considère encore l'algorithme d'Adleman, cette fois-ci dans le cors $\mathbb{F}_p$. On souhaite calculer les logarithmes discrets dans un sous-groupe de cardinal r^2 de $\mathbb{F}_p^*$, où on a $r^2 \mid (p-1)$. Montrer comment il est possible de résoudre ce problème en ne résolvant qu'un seul système linéaire défini modulo r.