Maîtrise de Mathématiques
Logique et Complexité (Année 2003-2004)
TD 7

Exercice 1. (a) Calculer le probabilité p_i pour que, dans l'addition de deux entiers en base deux, il y ait une retenue à la i-me place (à partir de la droite) ; quelle est la limite quand i tend vers l'infini ?
(b) Même question en base dix, ou en base b.

Exercice 2. L'algorithme d'Euclide pour calculer le p.g.c.d. de deux entiers a_1 et a_2, où $a_1 > a_2 > 0$, consiste à calculer le reste a_3 de la division de a_1 par a_2, puis, si $a_3 > 0$, le reste a_4 de la division de a_2 par a_3, et ainsi de suite ; comme la suite décroit, on finit par tomber sur 0, et le p.g.c.d. est l'avant-dernier reste. Montrer que $a_{i+2} \leq a_i/2$. En déduire que l'algorithme d'Euclide, appliqué à deux nombres de longueur n écrits en base deux, s'effectue en un temps polynomial en n, qu'on évaluera.

Exercice 3. Calculer la probabilité pour que m vecteurs dans un espace vectoriel de dimension n sur le corps $\mathbb{F}_2$ forment un système libre. Soit p_n la probabilité pour qu'un déterminant $n \times n$ à coefficients dans $\mathbb{F}_2$ soit non nul ; montrer que p_n tend vers une limite p avec $1/4 < p < 1/e$ (on utilisera le développement du logarithme de p en série double).

Exercice 4. (a) Soient K un corps et k un sous-corps de K ; montrer que tout système d'équations linéaires à coefficients dans k qui a une solution dans K en a une dans k.
(b) Soient k un corps algébriquement clos et K une extension de k ; montrer que tout système d'équations et d'inéquations algébriques à coefficients dans k qui a une solution dans K en a une dans k.

Exercice 5. Combien de temps faut-il pour résoudre LIN2 (systèmes linéaires booléens de n équations à n inconnues, chaque équation ne faisant intervenir qu'une ou deux variables) ?

Exercice 6. Vérifier que $x \vee y = z$ équivaut au système $x \vee y \vee \neg z = 1$, $\neg x \vee z = 1$, $\neg y \vee z = 1$. Réduire SAT à SAT3.

Exercice 7. On appelle PROLOG le cas particulier de SAT pour lequel chaque équation ne contient au plus qu'une seule variable positive. Montrer que PROLOG est résoluble en temps polynomial (remarquer que, si chaque équation contient une variable négative, le système a une solution).