

EXAMEN I31 DU 16 JUIN 2015, LICECNCE 2
D. Michelucci, M-N. Terrasse

Vous avez droit à tous vos documents personnels.

Les calculatrices, ordinateurs, téléphones, lunettes et montres connectées sont prohibés.

Pas de programme !

Ecrivez lisiblement, et répondez de façon claire et concise.

Question 1. Comme d'habitude, calculez x, y tels que $70x + 164y = \text{PGCD}(70, 164)$, soit avec l'algorithme d'Euclide généralisé, soit avec sa forme matricielle.

Question 2. Rappelez les règles pour le calcul rapide de la puissance n ième d'un nombre ou d'une matrice a . Ici n est un entier naturel ($0, 1, 2, \dots$). Quel est l'ordre de grandeur du nombre de multiplications ? Quelle est la condition sur la taille de la matrice a (nombre de lignes et de colonnes) pour que la question ait un sens ?

Question 3. Soit P un nombre entier naturel premier donné. Soit a un entier naturel donné, dans l'intervalle $[1, P-1]$. Il existe un entier b dans l'intervalle $[1, P-1]$ tel que le produit de a et b soit égal à 1 modulo P . On dit que b est l'inverse de a modulo P . Par exemple, pour $P=7$, si $a=3$, alors $b=5$; en effet, $3 \text{ fois } 5 = 15$ égale 1 modulo 7 . Donnez un algorithme (pas de programme JAVA!) pour calculer b , utilisant la méthode de la puissance rapide à la question 2.

Question 4 (suite de la question 3). Donnez un second algorithme, utilisant l'algorithme d'Euclide généralisé de la question 1.

Remarque : comme mentionné en cours, la cryptographie à clef publique RSA utilise ces algorithmes.

Question 5. Le graphe *orienté* G est infini. Les points (x, y) du plan, avec x et y des nombres entiers naturels, sont ses sommets. Chaque sommet (x, y) a 2 successeurs : $(x+1, y)$ et $(x, y+1)$. Le sommet $(0, 0)$ est appelé O . Dessinez le graphe pour x et y dans $[0, 4]$. Indiquez bien l'orientation des arcs.

Question 6. Donnez des formules (récursives) pour calculer le nombre de chemins entre O et un sommet donné (x, y) . N'oubliez pas les formules terminales (qui terminent la récursion). Cette fonction est notée $\text{Ch}(x, y)$. Indication : il y a au plus 2 sommets possibles juste avant (x, y) dans tout chemin de O à (x, y) .

Question 7 (suite). On note $C(a, b)$ le nombre de façons de choisir a éléments parmi b . Définir $Ch(x, y)$ en fonction de C . Justifier.

Question 8. Des arcs de (x, y) à $(x+1, y+1)$ sont ajoutés au graphe G . Donnez les formules récursives pour le nombre de chemins entre O et le sommet (x, y) .

Question 9. Dans les premiers ordinateurs, l'inverse d'un nombre flottant était calculé en utilisant la méthode de Newton. Soit $f(x) = -a + (1/x)$ où a est une constante. On rappelle que, sous certaines conditions, un point fixe de la fonction $N(x) = x - f(x) / f'(x)$ est une solution de l'équation $f(x) = 0$.

9.a. Donnez l'expression mathématique de $N(x)$ pour cette fonction. Indication : c'est un polynôme de degré 2.

9.b. Donnez l'expression mathématique de $N'(x)$. Quand $N'(x)$ vaut-il : 1, quand vaut-il : -1 ? Pourquoi est-ce important ?

9.c Pour $a=0.25$, dessinez la courbe de $N(x)$, pour x compris entre 0 et 6. Tracer la droite d'équation $x=y$. Dessinez la marche suivie par la méthode de Newton en partant de $x=6$.

Question 10. La fonction donnant le temps d'exécution $T(n)$ en fonction de n , la taille du problème, est parfois représentée par une courbe avec une échelle logarithmique : tout point $(n, T(n))$ de cette fonction est représenté par un point $(x, y) = (\log n, \log(T(n)))$. L'ensemble de ces points (x, y) donne la courbe en question. Vous utiliserez les log en base 2, 10, e , à votre convenance.

10.a. Supposons que la méthode est en temps polynomial ; autrement dit $T(n) = Cn^d$ où C est une constante (positive), et d un entier naturel est le degré. Quelle est l'équation (uniquement en fonction de x et y) de la courbe, et quelle est sa forme ? Dessinez la pour $d=1$, et pour $d=2$. Vous utiliserez des constantes $C > 0$ à votre convenance.

10.b. Si $T(n) = C^n$, où $C > 1$ est une constante, quelle est l'équation de la courbe (uniquement en fonction de x et y) ? Dessinez la.

10.c. Si $T(n) = C \log n$, quelle est l'équation (uniquement en fonction de x et y) de la courbe ? Quelle est sa forme ? Dessinez la.