UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

**FLMA607 Calcul Formel – 2010–2011**

**Feuille de TD n°1 : Algorithmes élémentaires.**

# Les quatre opérations

**Exercice 1**

En vous inspirant de l'algorithme vu en cours pour l'addition, donner un algorithme permettant de calculer la soustraction $a - b$ de deux entiers longs $a \geq b \geq 0$ écrits en base $\beta$. Compter le nombre d'opérations effectuées.

**Exercice 2**

Calculer à la main les divisions euclidiennes de :
a) 514 par 6
b) 1246 par 27
c) $X^5 + 2X^3 + 7X^2 + 4$ par $X^3 + X + 1$
d) $X^7 - 1$ par $X^2 - 1$.

**Exercice 3**

Démontrer que dans $\mathbb{Z}[X]$, la division euclidienne de $X^2$ par $2X + 1$ n'existe pas. Donner une « pseudo-division euclidienne » de la forme

$$2^n X^2 = Q.(2X + 1) + R.$$

(Expliciter $n$, $Q$ et $R$.)

**Exercice 4**

Si deux entiers naturels $a$ et $b$ s'écrivent respectivement avec $n$ et $m$ chiffres en base $\beta$, combien faudra-t-il de chiffres pour écrire leur produit $ab$ ? Et pour écrire le quotient $q$ et le reste $r$ dans la division euclidienne $a = bq + r$ (avec $b \neq 0$) ?

**Exercice 5 (Conversions)**

1) Combien valent les nombres $(342)_5$, $(1001101)_2$ et $(A6F)_{16}$ ?
2) Écrire 1027 en base 2, 3 puis 7.
3) Convertir $(10101101)_2$ en base 16, $(D58)_{16}$ en base 2 et 12345678 en base $10^3$ le tout sans calculs (ou presque).
4) Convertir $(123)_5$ en base 4 et $(123)_4$ en base 5 en passant par la base 10.
5) Imaginez que vous êtes un ordinateur et essayez d'écrire le nombre $(110100101)_2$ en base 5 (ou plutôt devrais-je dire en base $(101)_2$) *sans utiliser la base 10.* Il faut donc faire toutes les divisions euclidiennes directement en base 2. On pourra tout de même utiliser les symboles usuels 0, 1, 2, 3, 4 pour écrire le résultat.

**Exercice 6**

En utilisant la base $10^4$ et une calculatrice « huit chiffres » (du moins en faisant comme si votre calculatrice ne pouvait afficher que huit chiffres), effectuer la multiplication

$$567843573828 \times 76543214562$$

par l'algorithme naïf. Combien avez-vous fait de multiplications ? D'additions ?

# Multiplication rapide

**Exercice 7**

Calculer le produit des polynômes $7X^3 + 5X^2 + 3X - 1$ et $2X^3 + 4X^2 - X + 1$ avec l'algorithme de Karatsuba. Calculer de même le produit $1247 \times 3982$ (à la main, en base 10). Combien avez-vous fait de multiplications élémentaires dans chaque cas ?

**Exercice 8**

Reprendre l'exercice 6, mais en utilisant cette fois-ci l'algorithme de Karatsuba.

**Exercice 9**

Étant donné les parties imaginaires et réelles $a, b, c, d$ de deux nombres complexes $z_1 = a + ib$ et $z_2 = c + id$ (avec $z_2 \neq 0$) montrer comment calculer les parties imaginaire et réelle du quotient $z_1/z_2 \in \mathbb{C}$ en utilisant au plus sept multiplications et divisions dans $\mathbb{R}$. Est-il possible de le faire avec seulement six opérations ?

**Exercice 10**

Montrer que pour multiplier deux polynômes de degré $< n = 2^k$ sur un anneau $R$, l'algorithme naïf requiert $2n^2 - 2n + 1$ opérations dans $R$, et celui de Karatsuba $7.3^k - 8.2^k + 2$. Pour quelles valeurs de $k$ l'algorithme de Karatsuba est-il le plus rapide ?

# Exponentiation rapide

**Exercice 11**

1) Montrer qu'en partant d'une indéterminée $x$ et en utilisant $d$ multiplications ou additions, on ne peut calculer que des polynômes de degré au plus $2^d$. En déduire qu'il faut au moins $\lceil \log_2 n \rceil$ multiplications pour calculer $x^n$, donc que l'algorithme d'exponentiation rapide est essentiellement optimal [1].
2) Donner un entier $n$ pour lequel on peut calculer $x^n$ en faisant *moins* de multiplications que par l'algorithme d'exponentiation rapide. Expliquer votre méthode.

**Exercice 12**

1) Avec l'algorithme d'exponentiation rapide, quels produits intermédiaires va-t-on effectuer pour calculer $x^{375}$ ? Combien aura-t-on fait de multiplications au total ? Combien en aurait-on fait par l'algorithme naïf ?
2) Calculer $2^{375}$ dans $\mathbb{Z}/7\mathbb{Z}$ avec la méthode ci-dessus. Vérifier votre résultat à l'aide du petit théorème de Fermat.
3) Calculer $7^{160}$ modulo 641. [2]

**Exercice 13**

On considère la suite d'éléments de $\mathbb{F}_{11}$ définie par

$$\begin{cases} u_0 &= 0 \\ u_1 &= 1 \\ u_{n+2} &= u_{n+1} + 3u_n \end{cases}$$

1) Calculer $u_{100}$ à la main en utilisant l'algorithme d'exponentiation rapide. On introduira la matrice $A$ (à coefficients dans $\mathbb{F}_{11}$) telle que

$$\begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = A \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}.$$

2) Montrer que la suite $(u_n)$ est périodique et calculer sa période.

**Exercice 14**

Calculer $2^{32}$ modulo 641. Que peut-on en déduire pour le cinquième nombre de Fermat $F_5 = 2^{2^5} + 1$ ?

**Exercice 15**

En utilisant le petit théorème de Fermat et l'exponentiation rapide, proposer une méthode pour calculer l'inverse de la classe d'un entier $a$ dans $\mathbb{Z}/p\mathbb{Z}$ (où $p$ est un nombre premier ne divisant pas $a$). Évaluer le coût de votre méthode.

1. Cependant, lorsque $x$ n'est pas une indéterminée mais un élément d'un ensemble plus structuré, il peut arriver que l'on puisse exploiter cette structure pour obtenir des algorithmes d'exponentiation encore plus rapides. Par exemple, l'exponentiation rapide n'est pas le meilleur algorithme pour calculer les puissances d'une matrice diagonalisable...
2. Ce calcul a été fait par Euler en 1758.

# Interpolation

**Exercice 16**

Sentant son heure approcher, l'arrière-arrière. . .-arrière petit-fils d'Ali-Baba décide de confier le secret de l'ouverture de la grotte dont il a hérité à ses cinq enfants. Le code secret est un nombre à quatre chiffres compris entre 0 et 9.[3] Afin de s'assurer qu'aucun de ses enfants ne sera écarté par les autres, il procède ainsi. Il considère le nombre premier $p = 10007$ et il note $f_0$ la classe du code secret dans $\mathbb{F}_p$. Il choisit alors au hasard neuf éléments $f_1, \ldots, f_4, u_0, \ldots, u_4$ de $\mathbb{F}_p$ de telle sorte que les $u_i$ soient deux à deux distincts et non nuls, puis il pose

$$f(x) = f_4x^4 + \cdots + f_1x + f_0 \in \mathbb{F}_p[x]$$

et confie au $i^{\text{ème}}$ enfant les valeurs de $u_i$ et $f(u_i)$.
1) Expliquer comment, ensemble, les cinq enfants pourront retrouver le code secret.
2) Montrer que si seulement quatre d'entre eux se rassemblent, ils n'ont aucune information sur le code.

**Exercice 17**

1) Calculer un polynôme $f \in \mathbb{F}_5[X]$ de degré au plus 2 tel que

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 4.$$

2) Faites la liste de tous les polynômes de $\mathbb{F}_5[X]$ de degré au plus 3 qui vérifient les équations ci-dessus. Combien y en a-t-il de degré au plus 4 ? Au plus $n$ ?

**Exercice 18**

Soit $f(X) = 4X^5 + 5X + 1 \in \mathbb{F}_{13}[X]$. Combien y a-t-il de polynômes dans $\mathbb{F}_{13}[X]$ de degré exactement 13 qui définissent la même fonction polynomiale que $f$ sur $\mathbb{F}_{13}$ ? Combien y en a-t-il de degré exactement 2010 ? Et de degré exactement 12 ?

**Exercice 19**

Calculer le polynôme d'interpolation de Lagrange de la fonction $f(x) = \frac{1}{1+x^2}$ aux points $\{-1, 0, 1, 2\}$ par la méthode des différences divisées.

3. La formule « Sésame, ouvre-toi ! » étant connue de trop de monde, il a dû changer le mot de passe.