Université de Limoges
Faculté des Sciences

Année Universitaire 2008-2009

Master de Mathématiques, Première Année
Calcul Formel
Feuille d'exercices n° 2 : Calcul modulaire et restes chinois

Exercice 1

1) On pose $P = (x^2 + x + 1)^2(x^2 + 3)(x^2 - x + 1)$.

a) Calculer le reste de la division euclidienne de P par $x^2 + 1$.

b) Calculer P(i) (où i désigne le nombre complexe de module 1 et d'argument $\pi/2$).

2) Manipulations arithmétiques :

a) Calculer $17.45.70$ modulo 11.

b) Calculer 2005^{2006} modulo 7.

c) Déterminer le reste modulo 11 de 102^{102}.

d) Déterminer le reste de la division euclidienne de $2222^{3333} + 3333^{2222}$ par 5.

Exercice 2

[Théorème de Wilson]

1) Soit $n \in \mathbb{N}$. Montrer que n divise $(n-1)!$.

2) Soit $p \in \mathbb{N}$ un nombre premier impair.

a) Montrer que 1 et $p-1$ sont les deux seules solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ (et sont incidemment leur propre inverse).

b) Montrer que $(p-2)!$ est congru à 1 modulo p. Indication : remarquer que $\{2, \ldots, p-2\}$ admet une partition par des couples $\{x, x^{-1}\}$.

3) En déduire le théorème de Wilson : p est premier si et seulement si p divise $(p-1)! + 1$.

Exercice 3

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?
On appliquera la méthode de Lagrange, puis la méthode de Garner.

Exercice 4

Soit k un corps et $p_0, \ldots, p_n, c_0, \ldots, c_n \in k$.

1) En utilisant le théorème des restes chinois, démontrer qu'il existe un unique polynôme $P \in k[X]$ de degré au plus n tel que $P(p_i) = c_i$ pour $i = 0, \ldots, n$. (indication : considérer P modulo $X - p_i$).

2) Comment pourrait-on prouver "directement" ce résultat (sans utiliser le théorème des restes chinois)

3) En adaptant la méthode de Lagrange vue pour les nombres, construire des polynômes $L_0, \ldots, L_n$ dépendant de $p_0, \ldots, p_n$ (le polynômes de Lagrange) tels que : $P = \sum_{i=0}^{n} c_i L_i$.

4) Construire un algorithme, utilisant la méthode de Garner, pour résoudre ce problème d'interpolation.

Exercice 5

Dans cet exercice, on montre la borne d'Hadamard sur les déterminants, et on l'applique à un calcul modulaire de déterminant.

1) Soit $M = (m_{i,j})_{i,j=1..n}$ une matrice réelle carrée.

a) On note $X_1, \ldots, X_n$ les vecteurs colonnes de M. Rappeler l'algorithme de Gram-Schmidt transformant cette famille en une base de vecteurs orthonormés $U_1, \ldots, U_n$.

b) On note U la matrice admettant les U_i pour colonnes. Montrer que U est orthogonale ($^tU = U^{-1}$) puis qu'il existe une matrice triangulaire $T = (t_{i,j})$ telle que $M = U.T$.

c) En déduire que $\det(M) = \prod_{i=1}^{n} t_{i,i}$.

d) Montrer que $|t_{i,i}| = | < U_i, X_i > | \leq ||X_i||_2$.

e) Démontrer la borne de Hadamard : $|\det(M)| \leq \prod_{j=1}^{n} \sqrt{\sum_{i=1}^{n} |m_{i,j}^2|}$.

2) Application au calcul modulaire de déterminant. On considère la matrice $M := \begin{pmatrix} 2 & 3 & 1 \\ 5 & 6 & 5 \\ 2 & 2 & 3 \end{pmatrix}$

a) Déterminer un entier positif b tel que $\det(M) \in [-b, b]$ (ex : $b = 200$, $b = 252$, etc).

b) Soit c un entier supérieur à $2b$. Montrer que si on connait $\det(M)$ modulo c, alors on peut en déduire $\det(M)$ (avec le signe correct).

c) On admet que $\det(M) \cong 4 \mod 23$. Calculer $\det(M)$ par une astucieuse méthode modulaire (on pourra noter que $2.3.5.23 = 690$).

Exercice 6

On définit $\Phi_n = \{a \in \{1, \ldots, n\} | \gcd(a, n) = 1\}$. La fonction d'Euler est définie par $\phi(n) = card(\Phi_n)$.

1) Démontrer que si $\gcd(m, n) = 1$, alors il existe une bijection entre $\Phi_n \times \Phi_m$ et Φ_{mn}. Idée : considérer $f : \Phi_n \times \Phi_m \to \Phi_{mn}, (a, b) \mapsto x$ où $x \cong a \mod m$ et $x \cong b \mod m$.

2) Montrer que si $\gcd(m, n) = 1$, alors $\phi(mn) = \phi(m)\phi(n)$.

3) Soit p, q des nombres premiers distincts ; on pose $n = pq$

a) Montrer que $\phi(n) = (p - 1)(q - 1)$.

b) Montrer que Φ_n peut être muni d'une structure de groupe multiplicatif.

c) En déduire que, pour tout $a \in \Phi_n$, $a^{(p-1)(d-1)} \cong 1 \mod n$

4) Montrer que si $n = p_1^{k_1} \cdots p_s^{k_s}$ est la décomposition de n en facteurs premiers, alors $\phi(n) = n.(1 - 1/p_1) \cdots (1 - 1/p_s)$.

Exercice 7

[RSA à la mode chinoise] Bob voudrait recevoir des messages chiffrés par le systèmes RSA. Il se donne donc deux nombres premiers p, q ("grands"). il choisit un entier e premier avec $(p-1)(q-1)$.

1) Comment calculer un nombre d tel que $ed-1$ soit un multiple de $(p-1)(q-1)$?

2) La clef publique de Bob est le couple (n, e), où $n = pq$. Sa clef privée est (n, d) (bien sur, p et q ne sont connus que de lui). Alice veut lui envoyer un message $M \in [0, \ldots, n-1]$. Elle calcule $C = M^e \mod n$ et envoie C à Bob. Pourquoi est-il difficile, pour l'espion Oscar, de retrouver M ?

3) Bob veut calculer $D = C^d \mod n$; vérifier que $M = D$.

4) Bill publie comme clef $(391, 3)$; sachant que $p = 17$ et $q = 23$, calculer $d_p := d \mod p$ et $d_q := d \mod q$. En déduire d.

5) Alphonsine envoie à Bill le message $C = 304$ chiffré avec sa clef privée. Retrouver le message d'Alphonsine en utilisant seulement n, d_p, d_q et les restes chinois.

Exercice 8

[Racines carrées et Chiffrement de Rabin] Soit p, q des grands nombres premiers congrus à 3 modulo 4 ; on pose $N = pq$.

1) Soit a un entier compris entre 1 et N.

a) Montrer que l'équation $x^2 \equiv a \mod p$ admet exactement zéro ou deux solutions $x \in \{1, \cdots p\}$. On dit que x est une racine carrée de a modulo p.

b) Application : pour $p = 7$ et tous les $i \in \{1, \cdots, p\}$, déterminer leur carré modulo 7 et en déduire lesquels admettent une racine carrée modulo 7.

c) Montrer qu'il existe des entiers $a \in \{1, \cdots p\}$ qui n'admettent pas de racine carrée modulo p (tester $p = 5, 7, 11, 13$). Combien d'éléments entre 1 et p admettent une racine carrée modulo p ?

2) On suppose maintenant que $p \equiv 3 \mod 4$.

a) Soit a un carré modulo p. Montrer qu'alors $\pm a^{\frac{p+1}{4}} \mod p$ est une racine carrée de a modulo p.

b) Montrer 3 est un carré modulo 11 et modulo 13, et déterminer sa racine carrée

c) On suppose que a admet deux racine carrées $\pm x$ modulo p et deux racines carrées $\pm y$ modulo q. Démontrer que a admet quatre racines carrées modulo N et indiquer un procédé pour les calculer (si x et y sont connus) ((penser chinois)).

d) On suppose maintenant qu'on ne connait pas p et q mais qu'on connait un entier a et deux racines carrées x et y de a modulo N tels que $x \not\equiv \pm y \mod N$. Montrer comment calculer p et q à partir de ces données. (Remarque : c'est essentiellement cette méthode là « en un peu plus sophistiqué » qui est utilisée par les meilleurs algorithmes de factorisation d'entiers).

3) Soit B compris entre 0 et $N-1$. On chiffre un message (nombre) x par $y = x(x+B) \mod N$. Vérifier que le nombre x se retrouve par la formule $x = \sqrt{B^2/4 + y} - B/2 \mod N$. Combien de solutions cette équation admet-elle ?

4) On prend $p = 7, q = 11$ clefs privés. $n = 77$ et $B = 9$ clefs publiques. Donner la formule de chiffrement et de déchiffrement.

5) Bob reçoit d'Alice le message $y = 22$. Montrer que le nombre clair correspondant est dans l'ensemble $\{2, 24, 44, 66\}$.

Exercice 9

Soit K un corps de caractéristique 0. Soit $e_1, \ldots, e_r$ des entiers positifs ou nuls et $u_1, \ldots, u_r$ des éléments de K. Pour tout i ($1 \leq i \leq r$), on se donne e_i éléments de K notés $(a_{i\,j})_{0 \leq j \leq e_i - 1}$. On cherche un polynôme $f \in K[X]$ tel que l'on ait :

$$f^{(j)}(u_i) = a_{i\,j} \quad \forall i, j \mid 1 \leq i \leq r, \quad 1 \leq j \leq e_i$$

La notation $f^{(j)}$ désigne la j-ième dérivée de f (la dérivée d'ordre 0 étant f).
Ce problème s'appelle le *problème d'interpolation de Hermite*.

1. On cherche dans cette question à résoudre le problème d'interpolation de Hermite suivant.
$$(H_1) : \qquad f(0) = 0,\ f'(0) = 1,\ f(1) = 1,\ f'(1) = 0$$

   a) Montrer, en utilisant la formule de Taylor aux points 0 et 1, que ce problème peut se reformuler comme un système (S_1) de *deux* congruences polynomiales (modulo des polynômes non-irréductibles).
   Montrer qu'il existe un unique polynôme de degré ≤ 3 solution de ce problème.

   b) Résoudre le système de congruence (S_1) associé au problème (H_1) par la méthode de Garner.

   c) Même question avec une méthode de Lagrange. Quelle méthode favoriseriez-vous ? (justifiez votre réponse).

2. On s'intéresse maintenant au problème général de l'interpolation de Hermite définie ci-dessus.

   a) En écrivant la formule de Taylor aux points u_i, montrer que ce problème peut se formuler comme un système de r congruences polynomiales.

   b) En utilisant le théorème des restes chinois, montrer que le problème admet une unique solution vérifiant $\deg f < e_0 + e_1 + \cdots + e_r$.

3. Étudions la complexité de la méthode de Lagrange, en *nombre d'opérations arithmétiques dans K* (addition, multiplication, inversion), pour résoudre le problème d'interpolation de Hermite.

   On suppose que :
   - Multiplier un polynôme de degré n avec un polynôme de degré m de $K[X]$ nécessite $O(n\,m)$ opérations dans K.
   - Diviser un polynôme de degré n par un polynôme de degré m de $K[X]$ (où $n > m$) nécessite $O((n-m)\,m)$ opérations dans K.
   - Additionner un polynôme de degré n avec un polynôme de degré m de $K[X]$ (où $n > m$) nécessite $O(m)$ opérations dans K.

   (a) Estimer la complexité de l'algorithme d'Euclide étendu appliqué à deux polynômes de degrés inférieur ou égaux à n.

   (b) On pose $n = e_0 + \cdots + e_r$. Estimer la complexité, en fonction de n, de la méthode de Lagrange pour résoudre le problème d'interpolation ci-dessus.