Université Paris 7
UFR de Mathématiques

Année 1998/99
MT 141

TP Maple n° 2

(J-Y Ducloux)

Résumé

Les deux thèmes de ce TP sont, d'une part la manipulation des racines de l'unité, et d'autre part l'étude des entiers modulo un produit de deux nombres premiers. Vous allez dans un premier temps valider les commandes MAPLE de cette feuille dont votre ordinateur a une copie et observer le résultat.

Ensuite, vous chercherez à comprendre les calculs faits par MAPLE. Les questions 1 à 3 auxquelles vous devez répondre sur une feuille annexe demandent une preuve (mathématique) de ce que les calculs de MAPLE vont aboutir. À la fin, s'il vous reste du temps, vous pourrez terminer le traitement d'un des deux thèmes en suivant les indications données dans les "études".

I. Expression de cos(Pi/17) par radicaux

On va poser `t := Pi/17` puis prouver qu'il est possible d'écrire `z1 := cos(t)` à l'aide de nombres entiers en utilisant +, -, *, /, et l'extraction de la racine carrée de nombres réels.

Pour se rendre compte de la difficulté de ce type de problème, on admet qu'aucune racine X de l'équation $X^5 - 6X + 3 = 0$ ne s'exprime à partir des nombres entiers en utilisant +, -, *, /, et l'extraction de racines carrée, cubique, ... de nombres complexes. Ce n'est bien sûr pas le cas pour l'équation $X^{34} - 1 = 0$.

```
> restart;   cos(Pi/5);   cos(Pi/17);      #on vérifie que Maple n'a pas la
>réponse

> t := Pi/17:
  x1 := cos(3*t) + cos(5*t) + cos(7*t) + cos(11*t):
  x2 := cos(t) + cos(9*t) + cos(13*t) + cos(15*t):
  y1 := cos(3*t) + cos(5*t):
  y2 := cos(7*t) + cos(11*t):
  y3 := cos(t) + cos(13*t):
  y4 := cos(9*t) + cos(15*t):
  z1 := cos(t):
  z2 := cos(13*t):

> combine(x1+x2,trig);
> evalf(");
> combine(x1*x2+2*x1+2*x2,trig);
> combine(y1*y2,trig);
> evalf(");
> combine(y3*y4,trig);
> evalf(");
> combine(z1*z2+1/2*y1,trig);
```

Question 1 Pourquoi l'évaluation de `x1+x2` (qui intervient au total 3 fois) est-elle correcte?

Pour prouver la nécessité de ne pas se contenter de calculs approchés, voici une *approximation* avec 7, 9, 13 chiffres après la virgule du nombre découvert par Ramanujan au début du siècle.

```
> restart; Ram := exp(Pi*sqrt(163)) - 262537412640768744;
  evalf(Ram,25); evalf(Ram,27); evalf(Ram,31);
```

Question 2 Quelle expression sous forme de produit de la somme des $cos(a+kb)$ lorsque k varie de 0 à $n-1$ (avec $n \in \mathbb{N} \setminus \{0\}$ et $a, b \in \mathbb{R}$ tels que $sin(b/2) \neq 0$) permet d'obtenir les inégalités suivantes: `x2<0<x1`, `y2<0<y1`, `y4<0<y3`, et `z2<0<z1`?

Étude Terminer le calcul de $cos(\pi/17)$. Pour cela, on utilisera la fonction "`solve`" de MAPLE.

La formule pour $cos(\pi/17)$ qui vient d'être obtenue permet de construire à la règle et au compas un polygône régulier à 17 (ou 34) cotés. Ce résultat a été obtenu par Gauss en 1796, à 18 ans. Par la suite, il a affirmé avoir la preuve (et il ne fait aucun doute qu'il l'ai eue) du résultat suivant : les polygônes réguliers dont la construction à la règle et au compas est possible sont ceux dont le nombre de cotés est de la forme $n = 2^k n_1 ... n_l$, où $k \in \mathbb{N}$ et les $n_i \in \mathbb{N}$ sont premiers distincts de la forme $n_i = 2^{(2^m)} + 1$ avec $m \in \mathbb{N}$. Peu de nombres premiers de la forme $2^{(2^m)} + 1$ sont connus. Celui qui suit 17 est 257.

Bibliographie :

Le chapitre 17 de la deuxième édition du livre "Galois Theory" de Ian Stewart. Voir aussi la page 39 du dossier hors série de janvier 1994 de la revue "Pour la science".

II. Cryptographie à clef publique (systèmeRSA)

On commence par construire un nombre n d'une centaine de chiffres. Il est produit de deux nombres premiers p et q qui seront tenus secrets. On choisit aussi un nombre $e \geq 2$ qui est premier avec $(p-1)(q-1)$.

La clef (n, e) qui va permettre à mes correspondants de m'envoyer des messages codés est dans l'annuaire à coté de mon nom. La clef d du décodage se calculera à partir de p et q.

Il faut savoir que la transmission de messages cryptés non déclarés a été longtemps *interdite* en France. J'ignore ce qu'il en est actuellement.

```
> restart; p := nextprime(rand(10^49..10^50)()):    #on choisit p et q avec
>50 chiffres
  q := nextprime(rand(10^49..10^50)()):  n := p*q;   #n est peu aléatoire!
(cf "rand")
> isprime(n);                                    #normalement "ifactor(n)"
>n'aboutit pas
> e := nextprime(rand(10^3..10^4)());     #on se donne e premier avec (p-1)(q-1)
```

Ensuite, on crypte une ligne de message (d'au plus 69 caractères) traduite par $m \in \mathbb{N}$ avec $m < n$, et l'envoie sous la forme d'une ligne de message crypté traduite par $c =$ `code` $\in \mathbb{N}$. Puis on décrypte.

```
> m := 4817021;
> code := m&^e mod n;                #pourquoi pas "m^e mod n"?
> x := 'x': d := op(1,op(Roots(e*x-1) mod (p-1)*(q-1)));
> decode := c&^d mod n;
   #normalement "Roots(x^e - c) mod n" n'aboutit pas
```

Question 3 Prouver que la méthode utilisée permet de décoder tous les messages.

Étude Réaliser le codage et le décodage automatique d'un texte d'une ligne d'au plus 69 caractères, écrit avec l'alphabet usuel de 26 lettres auquel on adjoint le symbole "_" pour représenter un espace. On utilisera les fonctions "`convert[base]`" et "`sum`" de MAPLE, et s'inspirera des exemples suivants :

```
> m27 := op(subs({ 'a'=1,'e'=5,'i'=9,'s'=19},
                         [seq( substring(essai,i) ,i=1..length(essai))]));
```

$$m27 := 5, 19, 19, 1, 9$$

```
> s := [m27]:    nops(s);    s[3];
```

$$5$$

$$19$$

```
> alpha := proc() subs( { 1='a',5='e',9='i',19='s'},[args] ): end:
  cat(op(alpha(m27)));
```

$$essai$$

Bibliographie :

Ce thème a été préparé à partir de l'encart page 90 du numéro de septembre 1998 de la revue "Pour la science". On peut aussi regarder l'encart page 764 du numéro spécial de la revue "La recherche" de juillet/août 1995. La cryptographie à clef publique a été inventée en 1976 par W. Diffie et M. Hellman. Le système RSA est dû à R. Rivest, A. Shamir et L. Adleman en 1978.