

Algorithmique et programmation en Maple
Travaux pratiques : corrigé
9 décembre 2005
Marc Mezzarobba

Exercice 1. Écrire une fonction `ordre(k,n)` qui renvoie l'ordre d'un élément k dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$. (On supposera que k est bien inversible modulo n .)

```
ordre := proc(k::integer, n::integer)::integer;
  local r::integer, j::integer;
  r := k mod n; j := 1;
  while r <> 1 do
    r := (r * k) mod n;
    j := j + 1;
  od;
  RETURN(j);
end proc;
```

Exercice 2. On représente un polynôme $P \in \mathbb{Z}[X]$ de degré n par le tableau $a[i], i \in \llbracket 1, n \rrbracket$ de ses coefficients ($a[i]$ contenant le coefficient de X^i). Écrire une fonction `evaluate(a,x)`, ou `evaluate(a,n,x)`, qui calcule la valeur de P en un point $x \in \mathbb{Z}$, en temps $O(n)$.

```
evaluate := proc(a::array, x::integer)::integer;
  local n::integer, i::integer, v::integer;
  n := op(op(2,eval(a))[1])[2];
  v := 0;
  for i from n to 0 by -1 do
    v := v * x + a[i];
  od;
  RETURN(v);
end proc;
```