TD 1 de mathématiques

1. L'algorithme de division entière le plus simple consiste à soustraire autant de fois b de a qu'il est possible, jusqu'à obtenir un reste $< b$. Mais il existe un autre algorithme appelé algorithme de division binaire.

Division:=proc(a,b)
local r, q, u;

$r := a$;
$q := 0$;
while $(r >= b)$
. do
. $r := r - b$;
. $q := q + 1$;
. od;
$u := [q, r]$;
return(u);
end;

DivisionBinaire:=proc(a,b)
local r,q,aux,n,u;
. $r := a$; $q := 0$; $n := 0$; $aux := b$;
. while $(aux <= a)$
. $aux := 2 * aux$;
. $n := n + 1$;
. while $(n > 0)$
. $aux := aux/2$;
. $n := n - 1$;
. if $(r < aux)$
. then
. $q := 2 * q$;
. else
. $q := 2 * q + 1$;
. $r := r - aux$;
. fi; . $u := [q, r]$;
. return(u);
end;

   (a) Faire tourner les deux algorithmes pour calculer 123/23, puis 256/2.

   (b) Comparer les deux algorithmes en terme d'efficacité (nombre de boucles)

2. Soit $n \in \mathbb{N}$. Pour quelles valeurs de n le nombre $n^2 - 3n + 6$ est-il divisible par 5 ?

3. Montrer que pour tout idéal $I \subset \mathbb{Z}$, il existe un unique entier positif d tel que $I = d\mathbb{Z}$.

4. Montrer que pour tout $a, b \in \mathbb{Z}$, il existe un unique PGCD d de a et b et de plus $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

5. Montrer que l'algorithme d'Euclide se termine.
   Algorithme d'Euclide $R0 := |a|$;
   $R1 := |b|$; $\quad (b \neq 0)$
   Tantque $R1 > 0$ Faire
   $R := Reste\_Division(R0, R1)$;
   $R0 := R1$;
   $R1 := R$;

6. Calculer $PGCD(79, 23)$

7. Montrer que pour $a, b, c \in \mathbb{Z}$ tel que $c|ab$ et $PGCD(a, c) = 1$, on a $c|b$.

8. Calculer deux entiers s et t tels que $18.s + 23.t = 1$. En déduire l'inverse de 18 mod 23.

9. Calculer l'inverse de 23 mod 79.

10. Calculer l'inverse de 24 mod 99.

11. Montrer qu'il existe un nombre infini de nombres premiers.

12. Si $PGCD(a_1, \ldots, a_k) = 1$, les entiers a_i sont-ils premiers deux à deux?

13. Soit p un premier, $a, b \in \mathbb{Z}$. Montrer que $p|ab$ implique que $p|a$ ou $p|b$. Si p n'est pas premier, trouver un contre exemple.