TD 1 de cryptographie

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. Calculer dans $\mathbb{Z}_7$: $[2]_7 + [6]_7$, $[2]_7.[5]_7$

3. Montrer que l'algorithme d'Euclide se termine et qu'il calcule le PGCD
Algorithme d'Euclide $R0 := |a|$;
$R1 := |b|$; $(b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;

4. Calculer $PGCD(79, 23)$

5. Calculer $18^{-1} \mod 23$, $25/8 \mod 11$, $7/4 \mod 10$, $8/3 \mod 10$.

6. On note $a\mathbb{Z} := \{\ldots, -a, 0, a, 2a, 3a, 4a, \ldots\}$ et on définit pour $a_1, \ldots, a_k$

$$a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} := \{a_1z_1 + \cdots + a_kz_k : z_1, \ldots, z_k \in \mathbb{Z}\}$$

   (a) Calculer $3\mathbb{Z} + 5\mathbb{Z}$, $6\mathbb{Z} + 9\mathbb{Z}$

   (b) Soit $a, b \in \mathbb{Z}$ et $d = PGCD(a, b)$, montrer que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

   (c) Que vaut $a\mathbb{Z} + b\mathbb{Z}$ si a et b sont premiers entre eux?

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

8. Si $PGCD(a_1, \ldots, a_k) = 1$, les entiers a_i sont-ils premiers deux à deux?
9. Montrer l'unicité de la factorisation d'un entier (théorème fondamental de l'arithmétique).
10. Résoudre $5x \equiv 20 \mod 25$ et $4x \equiv 3 \mod 29$
11. Calculer x tel que $\begin{cases} x = & 13 \mod 19 \\ x = & 6 \mod 23 \end{cases}$
12. Donner la définition de $\mathbb{Z}_n$ et celle de $\mathbb{Z}_n^*$.
13. Calculer $\#\mathbb{Z}_{24}^*$, $\#\mathbb{Z}_{11}^*$, $\#\mathbb{Z}_{1024}^*$, $\#\mathbb{Z}_{35}^*$.