# TP 2 : Euclide étendu et applications

**Exercice 1.** (*Euclide étendu*) [Passer cet exercice s'il a été traité lors du TP1]

1. Écrire l'algorithme d'Euclide étendu pour les entiers sous forme d'une fonction `euclideEtendu(a,b)`.
2. Vérifier que la procédure ci-dessus fonctionne toujours dans $\mathbf{Q}[X]$.
   [La commande `X=polygen(QQ,'X')` permet de travailler dans l'anneau de polynômes $\mathbf{Q}[X]$.]
3. Comparer `euclideEtendu` avec `xgcd` pour les entiers et les polynômes.

**Exercice 2.**

On considère le pseudocode suivant :

Entrée : $a, b$ des entiers naturels non nuls.

1. $r = a$, $r' = b$, $e = 0$.
2. Tant que $2 \mid r$ et $2 \mid r'$ faire $r = r/2$, $r' = r'/2$, $e = e + 1$.
3. Tant que $r' \neq 0$ :
   — Tant que $2 \mid r$ faire $r = r/2$
   — Tant que $2 \mid r'$ faire $r' = r'/2$
   — Si $r' < r$ alors $(r, r') = (r', r)$
   — $r' = r' - r$

Sortie : $2^e \cdot r$.

1. Implanter le pseudocode ci-dessus (utiliser les commandes `//` et `%`). Le tester sur $(a, b) = (126, 35)$, $(a, b) = (124, 186)$ et quelques autres couples d'entiers. Que calcule ce code ?
2. Donner la preuve de la correction de l'algorithme ci-dessus.
3. Quel avantage présente cet algorithme sur celui vu en cours et renvoyant le même résultat en sortie ?

**Exercice 3.** (*premiers dans les progressions arithmétiques, nombres de Carmichael*)

1. Écrire une fonction `listeDirichlet(a, b, N)` prenant en argument 2 entiers *premiers entre eux* $a$ et $b$ avec $b \geqslant 1$ ainsi qu'un entier positif $N$ et renvoyant en sortie la liste des $N$ premiers nombres premiers $p$ vérifiant $p \equiv a \pmod{b}$. Que peut-on conjecturer ?
2. Écrire une fonction `fermat(p)` qui teste le *petit théorème de Fermat* pour $p$ : "si $p$ est premier alors $a^p \equiv a \pmod{p}$ pour tout entier $a$". Vérifier le théorème pour les premiers $p \leqslant 11$. Le nombre 561 est-il premier ? A-t-on $a^{561} \equiv a \pmod{561}$ pour tout entier $a$ ? Que peut-on en conclure ?

**Exercice 4.** (*restes chinois*)

1. Écrire une fonction `systemeChinois(nu, m)` qui, à partir de listes d'entiers `nu` et `m`, renvoie une solution $x$ du système de congruences

$$x \equiv \nu_i \pmod{m_i}\,,\ 1 \leqslant i \leqslant r\,.$$

   en supposant que les $m_i$ sont des entiers naturels 2 à 2 premiers entre eux. Tester la procédure en résolvant le système $(x \equiv 28 \bmod 41, x \equiv 37 \bmod 75, x \equiv 62 \bmod 101)$. Comparer avec la commande `crt`.

2. On considère le pseudocode suivant :

   Entrée : $a_1, a_2, n_1, n_2$ des entiers satisfaisant : $\text{pgcd}(n_1, n_2) = 1$ et $0 \leq a_i < n_i$, pour $i = 1, 2$.

   (a) $b = n_1 \bmod n_2$, $t = b^{-1} \bmod n_2$, $h = (a_2 - a_1)t \bmod n_2$.

   (b) $a = a_1 + n_1 h$

   Sortie : $a \bmod n_1 n_2$.

   (a) Que fait cet algorithme ? Implanter cet algorithme et le tester sur quelques exemples.

   (b) Utiliser cet algorithme pour retrouver la solution au système de congruences considéré à la question 1.

**Exercice 5.** (*Test de primalité de Miller-Rabin*)

Soit $p$ un nombre premier impair.

1. Justifier que si $a^2 \equiv 1 \,(\text{mod}\, p)$ alors $a \equiv 1 \,(\text{mod}\, p)$ ou $a \equiv -1 \,(\text{mod}\, p)$.
2. On écrit $p - 1 = 2^s t$ où $s, t$ sont des entiers et $t$ est impair. Soit $a$ un entier qui n'est pas multiple de $p$ et soit $A = a^t$. Justifier que $A$ est inversible modulo $p$.
   On note $\alpha$ l'ordre de $A$ en tant qu'élément de $(\mathbf{Z}/p\mathbf{Z})^\times$.
3. Montrer que $\alpha$ divise $2^s$. Dans la suite on notera $\alpha = 2^j$.
4. Montrer que si $j = 0$ alors $a^t \equiv 1 (\bmod p)$.
5. Montrer que si $j \geqslant 1$ alors $a^{t2^{j-1}} \equiv -1 (\bmod p)$.
6. On considère le pseudo code suivant qui décrit le test de Miller-Rabin
   Entrée : un nombre impair $n$ et un nombre entier $a$ premier à $n$.
   (1) Calculer $s$ et $t$ tels que $n - 1 = 2^s \times t$, avec $t$ impair.
   (2) Si $a^t \equiv 1 (\bmod n)$, la procédure s'arrête et l'on renvoie « vrai ».
   (3) Pour $i$ de 0 à $s - 1$ :
   si $a^{t2^i} \equiv -1 (\bmod n)$ alors la procédure s'arrête et l'on renvoie « vrai ».
   (4) On renvoie « faux ».

   Que conclure si l'algorithme renvoie « vrai » ? Et s'il renvoie « faux » ?
7. Implanter le pseudo code ci-dessus en une fonction `MillerRabin(n, a)` et le tester sur quelques valeurs de $a$ et $n$.

**Exercice 6.** (*Cryptosystème de Rabin*)

On présente un système de cryptographie proche de RSA mais basé cette fois ci sur le fait qu'il est d'une part « facile »de calculer des racines carrées modulo $p$, pour $p$ premier, mais d'autre part « difficile »de calculer des racines carrées modulo $n = pq$, où $p$ et $q$ sont des nombres premiers distincts « grands », si l'on ne connait que le produit $n$ et pas ses facteurs $p$ et $q$.

On fixe $p$ et $q$ deux nombres premiers congrus à 3 modulo 4.

1. Justifier que si $\ell$ est un nombre premier impair quelconque et si $y$ n'est pas multiple de $\ell$ alors $y^{(\ell-1)/2} \equiv \pm 1 (\text{mod}\ell)$.
2. Soient $m$ et $x$ des entiers vérifiant $m^2 \equiv x (\text{mod} p)$. Quelle est la classe de congruence de $x^{(p+1)/4}$ modulo $p$ ?
3. Alice veut envoyer à Bob un message clair $m \in \mathbf{Z}/n\mathbf{Z}$ via le système de Rabin : $n$ est la clé publique de Bob (et le couple $(p, q)$ est sa clé privée, connue de lui seul). Alice envoie alors le message chiffré $x \equiv m^2 (\text{mod} n)$ à Bob. En utilisant la question précédente, expliquer comment Bob peut facilement déduire un ensemble $\mathcal{M}$ de 4 valeurs possibles pour le message initial $m$.
4. Écrire une procédure `ValPossibles(x,p,q)` prenant en entrée le triplet $(x, p, q)$ où $x$ est un carré modulo $pq$ et renvoyant un ensemble $\mathcal{M}$ de 4 valeurs possibles pour un $m$ vérifiant $m^2 \equiv x (\bmod pq)$.