# TP2 : Théorie des Nombres et algorithmes élémentaires

Pierre-Alain Fouque

4 février 2013

## 1 Algorithmes élémentaires

On testera nos algorithmes avec des entiers de 30 bits.

1. Programmer l'algorithme d'Euclide
2. Programmer l'algorithme d'Euclide étendu
3. Programmer le calcul de l'inverse modulaire
4. Programmer une multiplication modulaire
5. Programmer une exponentiation modulaire
6. Programmer un crible d'Eratosthène.
7. Programmer un algorithme qui chiffre et déchiffre avec RSA.
   La connaissance de la clé secrète RSA permet de factoriser le module $N = pq$. Étant donné $d$, calculer $k = de - 1$. D'après la définition de $d$ et $e$, on sait que $k$ est un multiple de $\varphi(N)$. Comme $\varphi(N)$ est pair, $k = 2^t \cdot r$ avec $r$ un entier impair et $t > 1$. On a $g^k = 1$ pour tout $g \in \mathbb{Z}_N^*$ et par conséquent, $g^{k/2}$ est une racine carrée de l'unité modulo $N$. D'après le théorème des restes chinois, 1 a 4 racines carrées modulo $N = pq$. Deux de ces racines carrées sont $\pm 1$. Les deux autres valent $\pm x$ tel que $x = 1 \bmod p$ et $x = -1 \bmod q$. En utilisant l'une de ces deux racines carrées, la factorisation de $N$ peut être calculées en calculant $\gcd(x-1, N)$. En déduire un algorithme pour factoriser $N$ si on connaît une multiple de $\varphi(N)$.
8. Programmer l'algorithme qui factorise $N = pq$ si on connaît un multiple de $\varphi(N)$

## 2 Algorithmes avancés – Application d'Euclide étendu

L'algorithme d'Euclide étendu permet de calculer des approximations linéaires petites de deux entiers $a$ et $b$. On consultera le livre en ligne `http://shoup.net/ntb/ntb-v2.pdf`.

1. Programmer l'algorithme qui calcule une version effective du théorème des 2 carrés de Fermat ($p = r^2 + s^2$ si $p = 1 \bmod 4$) (page 87-88)
2. Programmer l'attaque de Wiener (exercice 4.27 page 102)