MT10/P11 - TP Factorisation d'entiers

Table des matières

1 La force brute

Soit N l'entier à factoriser.

1. **le plus petit diviseur** > 1
   On effectue la division euclidienne de N par les entiers $d \in [\![2, \sqrt{N}]\!]$ successivement. On s'arrête au premier reste nul. Dire pourquoi le plus petit diviseur $d_1 > 1$ de N est forcément un nombre premier. Si aucun reste nul n'est obtenu, alors N est un nombre premier.
2. On pose $N_1 = N/d_1$, et on recommence.

Programmation :
Ecrire d'abord une fonction qui retourne le plus petit facteur (premier) d'un entier. Ecrire ensuite une fonction qui renvoie la factorisation en facteurs premiers d'un entier N.

Expérience :
A partir de quelle taille de clé RSA, cette méthode de brute échoue-t-elle ? Quand est-il de la fonction `factor` de `MuPAD`.

2 L'algorithme $p-1$ de Pollard

Une utilisation astucieuse du petit théorème de Fermat, due à John M. Pollard, permet, dans certains cas, d'obtenir un diviseur non trivial d'un (grand) entier N. Cette méthode est efficace si N possède un diviseur premier p tel que $p-1$ n'admette que des petits diviseurs. On dira que $p-1$ est friable. Avant de présenter l'astuce de Pollard, précisons cette notion de friabilité.

2.1 Friabilité

Définition 1 (B-friable) *Soit $B \in \mathbb{N}$. On dit que l'entier K est B-friable si tous ses facteurs premiers sont $\leq B$:*

$$(\forall p \in \mathbb{P}) \qquad p|K \Longrightarrow p \leq B$$

Evidemment tout entier K est K-friable, donc la B-friabilité n'a d'intérêt que si B est (très) petit devant N. Voici une notion plus forte de friabilité :

Définition 2 (B-superfriable) *Soit $B \in \mathbb{N}$. On dit que l'entier K est B-superfriable si toutes les puissances de nombre premier qui le divisent sont $\leq B$:*

$$(\forall p \in \mathbb{P})(\forall \alpha \in \mathbb{N}) \qquad p^\alpha|K \Longrightarrow p^\alpha \leq B$$

Un entier B-superfriable est *a fortiori* B-friable.

Lemme 3 *Soit $B \in \mathbb{N}$. Pour tout $K \in \mathbb{N}$, on a :*

1. *K est B-superfriable $\implies K|B!$*
2. *K est B-superfriable $\implies K|ppcm(2,3,\ldots,B)$*

Démonstration. On écrit $K = \prod_{p\in\mathbb{P}} p^{v_p(K)}$. Si K est B-superfriable, on doit avoir $\forall p \in \mathbb{P}, \quad p^{v_p(K)} \leq B$. Comme ces termes sont premiers deux à deux, les résultats s'ensuivent. □

2.2 Principe de l'algorithme $p-1$ de Pollard

Soit N un entier non premier dont on veut trouver un facteur non trivial.

1. Choisir $B \in \mathbb{N}$, compatible avec les capacités de calcul.
   Cas favorable : N possède un facteur premier p tel que $p-1$ soit B-superfriable.
2. Choisir $a \in [\![2, \sqrt{N}]\!]$ au hasard.
   • Si $d = \text{pgcd}(a, N) \neq 1$, champagne ! on vient de trouver un facteur non trivial de N.
   • Sinon, $\text{pgcd}(a, N) = 1$. On a donc aussi $\text{pgcd}(a, p) = 1$, et le petit théorème de Fermat s'applique :
   $$a^{p-1} = 1 \qquad [p]$$
   Dans le cas favorable, le lemme fournit aussi :
   $$a^{B!} = 1 \qquad [p] \quad \text{et} \quad a^{\text{ppcm}(2,3,\ldots,B)} = 1 \qquad [p]$$
3. Calcul de $t = a^{B!} - 1 \ \ [N]$, ou de $t = a^{\text{ppcm}(2,3,\ldots,B)} - 1 \ \ [N]$.
   Dans les deux cas, on a $p|t$ (dire pourquoi).
   • Si $t \neq 0 \ \ [N]$, champagne ! $\text{pgcd}(t, N)$ est un facteur non trivial de N.
   • Sinon, on recommence à l'étape 2.

Programmation :
Ecrire une fonction qui prend comme entrée deux entiers N et B, et qui, si N possède un facteur premier p tel que $p-1$ soit B-superfriable, renvoie un facteur non trivial de N, selon la méthode de Pollard.
Attention à ce que la fonction s'arrête en temps raisonnable, même sur un échec (si on est dans un cas défavorable, B trop petit, N trop grand ...)

Exercice : Il se peut que même si N possède un facteur premier p tel que $p-1$ soit B-superfriable, l'étape 3 donne toujours $t = 0 \ \ [N]$, auquel cas la méthode de Pollard est sans intérêt. Expliquer cela, donner un exemple.

Expériences :
• Tester la friabilité de $p-1$ pour des (grands) nombres premiers. Commentaires sur le choix des modules RSA ?
• Factoriser les modules RSA donnés dans le notebook "Nombre_a_factoriser.mn". Utiliser la méthode de Pollard, et la fonction `factor` de `MuPAD`. Commenter les échecs et succès éventuels.