Maîtrise de mathématiques : M1/TD C

1. RSA, le retour

On rappelle les résultats qui sont à l'origine du test de Miller-Rabin :

Proposition. *Soit p un nombre premier avec $p-1=2^s t$ et t impair. Soit a un entier premier avec p. Alors l'une des deux assertions suivantes est vraie :*
- $a^t \equiv 1 \pmod p$;
- $\exists i,\ 0 \leq i < s,\ a^{2^i t} \equiv -1 \pmod p$.

Corollaire. *Soir n un entier impair avec $n-1=2^s t$ et t impair. S'il existe un entier a, $1<a<n$ tel que $a^t \not\equiv 1 \pmod n$ et tel que pour tout $i \in [0, s-1]$, $a^{2^i t} \not\equiv -1 \pmod n$, alors n est un entier composé (on dit dans ce cas que l'entier a est un* témoin de Miller-Rabin*).*

Théorème (Rabin)**.** *Soit n un entier impair composé et > 9 avec $n-1=2^s t$ et t impair. Les entiers a qui satisfont l'une des deux conditions de la proposition ci-dessus sont en nombre au plus $\phi(n)$.*

Exercice 1. Montrez que le premier nombre de Carmichael 561 n'est pas un nombre premier, en exhibant un témoin de Rabin-Miller. (nécessite un ordinateur).

Exercice 2. Démontrez le théorème suivant : soit n un nombre entier impair, si a est un élément de $\mathbf{Z}/n\mathbf{Z}$ d'ordre multiplicatif $n-1$, alors n est un nombre premier. Montrez tout d'abord que $(a,n)=1$. Montrez ensuite que si d désigne l'ordre multiplicatif de a modulo n, alors $d|\phi(n)$ puis concluez. En déduire que si $q_1, q_2, \ldots, q_r$ sont les r nombres premiers distincts de la décomposition de $n-1$ en produits de facteurs premiers, alors

$$[\forall i \in [1,r],\ a^{\frac{p-1}{q_i}} \not\equiv 1 \pmod n] \Rightarrow [n \text{ premier}].$$

Indication : montrez que d est un diviseur de $n-1$ tel que $x^d \equiv 1 \pmod n$ si et seulement s'il existe $i \in [1,r]$ tel que $d = \frac{p-1}{q_i}$.

Exercice 3. Considérez le système formel suivant :

axiomes : $(u,v,1),\ \forall (u,v) \in \mathbf{N} \times \mathbf{N}$

règle 1 : $(n,a,r) \vdash (n,a,rq)$ si q premier et $a^{\frac{n-1}{q}} \equiv 1 \pmod n$

règle 2 : $(n,a,n-1) \vdash n$ si $a^{p-1} \equiv 1 \pmod n$

Montrez que n est premier si et seulement si n est un théorème. Démontrez que 2 et 3 sont premiers dans ce système formel (ce sont les deux seuls entiers n tels que $n-1$ n'est pas composé).

Montrez à l'aide d'une récurrence que la preuve dans ce système demande l'application de $\lceil 4\log_2 n \rceil + 1$ règles (axiomes compris) au plus. Indication : montrez que la primalité d'un entier n peut être démontrée en $\lceil 4\log_2 n \rceil - 4$ règles au plus si l'on ne compte pas le nombre de règles nécessaires à prouver la primalité de 2 et 3.

Exercice 4. Montrez que l'on peut faire une exponentiation x^n en au plus $2\lfloor \log_2 n \rfloor$ produits. Donnez une majoration du coût d'un produit dans $\mathbf{Z}/m\mathbf{Z}$ et montrez que le temps nécessaire à validez la preuve de l'oracle est polynomiale. Concluez en montrant que le problème de la primalité est dans NP.