بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
وَ قُلِ إِعمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُم وَ رَسُولُهُ وَ المُؤ مِنُون
صَدَقَ اللَّهُ العَظِيم

CPGE My Youssef, Rabat

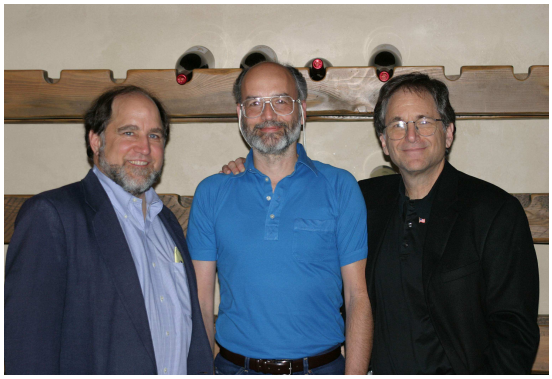
Corrigé Contrôle (08-09): *Arithmétique*

Jeudi le 19 Mars 2009

Durée : 1heure

Blague du jour :
• Quelle différence y a-t-il entre Windows et un clou ?
- Aucune : tous deux sont destinés à se planter.
• Quelle est la différence entre Windows XP et un virus ?
- Le virus il fonctionne !

Mathématiciens du jour ***RSA***
RSA est un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman (voir photo prise en 2003 de gauche à droite), d'où le sigle RSA. En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux, ...).



1) Classes inversible dans $\mathbb{Z}/n\mathbb{Z}$.

a) $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \iff \exists \overline{u}$ tel que $\overline{au} = \overline{1} \iff \exists u \in \mathbb{Z}$ tel que $ua \equiv 1\ [n] \iff \exists u, v \in \mathbb{Z}$ tel que $ua - 1 = vn \iff \exists u, v \in \mathbb{Z}$ tel que $ua + vn = 1 \iff a \wedge n = 1$.

b) Le nombre de classes inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est celui d'entier $1 \leq k \leq n$ tel que $k \wedge n = 1$, donc exactement $\varphi(n)$.

c) Les classes inversibles dans $\mathbb{Z}/8\mathbb{Z}$ sont celles de 1,3,5 et 7.

2) Fonction indicatrice d'Euler.

a) Tous les entiers $1 \leq k \leq p-1$ sont premiers avec p, donc $\varphi(p) = p - 1$.

b) Soit p premier et $\alpha \in \mathbb{N}^*$.
Les multiples de p inferieurs à p^α, sont de la forme kp avec $1 \leq k \leq p^{\alpha-1}$, il y en a exactement $p^{\alpha-1}$, ce sont ces entiers qui ne sont pas premiers avec p, donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

c) Les entiers inférieurs à pq qui ne sont pas premiers avec pq sont ceux qui ne sont pas premiers ni avec p ni avec q, c'est à dire les multiples de p ou de q inférieurs à pq. Les multiples de p inférieurs à pq sont de la forme kp avec $1 \leq k \leq q$, donc il y en a q exactement. De même il y a p multiples de q inférieurs à pq. D'autre part pq est l'unique multiple commun de p et q inférieurs à pq, donc $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

3) Théorème d'Euler.

a) **D'après la question 1b, on a :** $\text{card}U = \varphi(n)$.

b) **On a** a **est premier avec** n**, donc** $\overline{a}$ **est inversible dans** $\mathbb{Z}/n\mathbb{Z}$**, donc régulier, d'où l'application** $f : \overline{k} \mapsto \overline{ak}$ **est injective, entre deux ensembles finis de même cardinaux donc bijective.**

c) **L'application** f **étant bijective, donc** $U = \text{Im}f = \overline{a}U$**, donc** $\overline{k} \in U \Longleftrightarrow \overline{k} = \overline{ap}$ **où** $\overline{p} \in U$**, d'où** $\displaystyle\prod_{\overline{k}\in U} \overline{k} = \prod_{\overline{p}\in U} \overline{pa}$.

d) **Comme** $\text{card}U = \varphi(n)$**, d'où** $\displaystyle\prod_{\overline{k}\in U} \overline{a} = \prod_{\overline{k}\in U} \overline{ka} = a^{\varphi(n)} \prod_{\overline{k}\in U} \overline{k}$**, on peut simplifier par** $\displaystyle\prod_{\overline{k}\in U} \overline{k}$ **car inversible en tant que produit de classes inversibles. D'où** $\overline{a^{\varphi(n)}} = \overline{1}$**, donc** $a^{\varphi(n)} \equiv 1\ [n]$.

4) Principe du RSA.

a) **Résultat immédiat de la question 1a.**

b) **On a** $ed = 1 + k\varphi(n)$**, donc** $D \equiv C^d\ [n] \equiv M^{ed}\ [n] \equiv M^{1+k\varphi(n)}\ [n] \equiv M.\left(M^{\varphi(n)}\right)^k\ [n] \equiv M\ [n]$.

c) $\varphi(n) = (p-1)(q-1) = 8$**, prenons** $e = 3$ **et** $d = 3$. $C = M^e = 12^3 \equiv (-3)^3 = -27 \equiv 3\ [15]$ **et** $D = C^d = 3^3 = 27 \equiv 12 = M\ [15]$.

Fin
Bonne chance