بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
رَبِّي إِشرَح لِي صَدرِي وَ يَسِّر لِي أَمرِي وَ أحلُل عُقدَة مِن لِسَانِي يَفقَهُوا قَولِي

صَدَقَ اللَّهُ العَظِيم
سورة طه

**CPGE My Youssef, Rabat**

# Contrôle (08-09): *Arithmétique*

**Jeudi le 19 Mars 2009**

**Durée : 1heure**

***Blague du jour :***
**Êtes-vous accro à l'Internet ? La réponse serait oui si :**
**• Votre dernière pensée avant de vous endormir est "shutdown completed".**
**• Vous double-cliquez sur les boutons d'ascenseur. Vous cherchez "Cancel" quand vous avez appuyé sur le mauvais bouton, et vous étonnez de la pauvreté de l'interface utilisateur.**
**• En train, vous admirez le scrolling du paysage.**
**• Quand vous fermez une fenêtre, vos doigts se mettent machinalement en position F4**

**Mathématiciens du jour** ***Théorème de Ibn Al Haytham-Wilson***

**John Wilson (1741-1793) est un mathématicien britannique qui redécouvre ce qu'il croyait être une conjecture et qui porte aujourd'hui son nom : le théorème de Wilson. Ce résultat était en fait connu de Alhassan Ibn Al Haytam (voir photo ci-contre) et Leibniz qui ne l'avaient pas publié.**
**Ibn al-Haytham (965-1039) est un mathématicien et un physicien perse. Il est l'un des pères de la physique quantitative et de l'optique physiologique.**
**Craignant de possible sanctions du calife d'Egypte, qui lui confie le projet d'arréter les innondations du Nil, il fait semblant de folie et fût assigné à résidence. Il profita de ce loisir forcé pour écrire plusieurs livres (environ 200)**
**Il a été le premier à expliquer pourquoi le soleil et la lune semblent plus gros (on a cru longtemps que c'était Ptolémée). C'est aussi lui qui a contredit Ptolémée sur le fait que l'oeil émettrait de la lumière. Selon lui, si l'oeil était conçu de cette façon on pourrait voir la nuit. Il a compris que la lumière du soleil se reflétait sur les objets et ensuite entrait dans l'oeil.**
**Il fut également le premier à illustrer l'anatomie de l'oeil avec un diagramme. Il dit qu'un objet en mouvement continue de bouger aussi longtemps qu'aucune force ne l'arrête : c'est le principe d'inertie que Galilée redécouvrira.**
**On lui doit l'invention de la chambre noire, instrument optique qui permet d'obtenir une projection en deux dimensions très proche de la vision humaine.**

**Le contrôle est noté sur 10 points, le barème total est 16 points dont 2 points sur la présentation et rédaction.**

***Conseils pour la rédaction et la présentation des copies.***

---

- **Chaque variable utilisée dans une démonstration doit être définie.**
- **L'énoncé ne doit pas être recopié sur les copies.**
- **Chaque résutat annoncé doit être justifié en citant précisément le théorème du cours avec ses hypothèses exactes utilisé ou en citant le numéro de la question précèdente utilisée.**
- **Les résultats importants doivent être simplifiés et encadrés.**
- **Les calculs doivent être détaillés et expliqués à l'aide de phrases simples.**
- **Laisser une marge à gauche de chaque feuille, en tirant un trait vertical, et un horizontal de la 1ère double feuille pour la note et les remarques du correcteur.**
- **Numéroter les double feuille de la façon suivante : 1/n,2/n,...,n/n où n est le nombre total de double feuille.**
- **Les questions doivent être traités dans l'ordre de l'énoncé.**
- **Tirer deux traits diagonaux pour rayer une partie du raisonnement que vous considérez fausse.**

---

**Mini-Problème : Système de cryptographie-RSA.**

---

**Pour tout $n \in \mathbb{N}^*$, on pose $\varphi(n) =$ card$\{k \in \{1,\dots,n\}$ tel que $k \wedge n = 1\}$, appelée fonction indicatrice d'Euler**

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

**a) (1 pt) Montrer que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \iff a \wedge n = 1$.**

**b) (0.5 pt) Combien y-a-il de classes inversibles dans $\mathbb{Z}/n\mathbb{Z}$.**

**c) (0.5 pt) Donner toutes les classes inversibles dans $\mathbb{Z}/8\mathbb{Z}$.**

**2) Fonction indicatrice d'Euler.**

**a) (0.5 pt) Soit $p$ premier. Montrer que $\varphi(p) = p - 1$.**

**b) Soit $p$ premier et $\alpha \in \mathbb{N}^*$.**
**(1 pt) Combien y a t-il de multiples de $p$ inferieurs à $p^\alpha$.**
**(1 pt) En déduire que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.**

**c) (2 pts) Soit $p$ et $q$ deux nombres premiers, montrer que $\varphi(n) = (p-1)(q-1)$.**

**3) Théorème d'Euler.**
**Soit $n \in \mathbb{N}^*$ et $a$ premier avec $n$, on note par $U$ l'ensemble des classes inversible dans $\mathbb{Z}/n\mathbb{Z}$.**

**a) (0.5 pt) Préciser card$U$.**

**b) (1 pt) Montrer que l'application $\overline{k} \mapsto \overline{ak}$ est bijective.**

**c) (1 pt) En déduire que $\displaystyle\prod_{\overline{k}\in U} \overline{k} = \prod_{\overline{k}\in U} \overline{ka}$.**

**d) (1 pt) En déduire que $a^{\varphi(n)} \equiv 1\ [n]$ (théorème d'Euler).**

**4) Principe du RSA.**
**Soit $p$ et $q$ deux nombres premiers, on pose $n = pq$. Soit $M$ un entier naturel premier avec $pq$, qui représente le message à décoder, $C$ le message codé envoyé et enfin $D$ le message décodé, on se propose de montrer que $D = M\ [n]$.**

**a) (0.5 pt) Soit $e$ premier avec $\varphi(n)$, justifier l'existence de $d \in \mathbb{Z}$ tel que $ed \equiv 1\ [\varphi(n)]$.**

**b) Le message $M$ est codé en $C$ tel que $C \equiv M^e\ [n]$, le recepteur le décode en $D$ tel que $D \equiv C^d\ [n]$.**
**(1.5 pt) Montrer que : $D \equiv M\ [n]$.**
***Indication :* On pourra penser à utiliser le théorème d'Euler.**

**c) (2 pts) Application : pour $p = 3, q = 5$ et $M = 12$, donner $C$ puis $D$.**

*Fin*
*Bonne chance*