HX3 Mathématiques

Devoir en temps libre N^{o}3

À remettre le vendredi 4 novembre 2005

Les trois problèmes sont indépendants.

Il est demandé de ne pas recopier l'énoncé. On prendra bien soin de préciser toute notation non donnée dans l'énoncé. On laissera une marge à gauche.

Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie.

Problème 1 :

1) Soit $a \in \mathbb{N}$ et $n \in \mathbb{N}$, $a \geqslant 2$ et $n \geqslant 2$. Montrer que si $a^n - 1$ est un nombre premier, $a = 2$ et n est premier.

On note pour p premier, $M_p = 2^p - 1$: les M_p sont appelés *nombres de Mersenne.*

L'étude de la primalité de $a^n - 1$ se ramène à l'étude des M_p. En 1644, Mersenne affirma que M_p était premier pour $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ et composé pour les autres valeurs de p premier inférieur à 257. Mais en 1806, Pervasin et Seelhoff démontrèrent que M_{61} était premier. En 1876, Lucas établit un méthode pour tester la primalité des M_p (et prouva ainsi que M_{127} était premier). Durant l'été 1999, une équipe de trois mathématiciens japonais a prouvé que $M_{6972593}$ était premier : c'est le plus grand entier premier connu, il s'écrit avec 2098960 *chiffres.*

D'autre part, pour $n \geqslant 1$, on pose $\sigma(n) = \sum_{d|n} d$ la somme des diviseurs positifs de n.

2) Écrire un programme qui prend n en argument et renvoie $\sigma(n)$.

On dit que n est *parfait* si $\sigma(n) = 2n$: par exemple $n = 6$ est parfait.

3) a. Soit $n \geqslant 1$, $n' \geqslant 1$ deux entiers premiers entre eux. Si $k \in \mathbb{N}^*$, on note D_k l'ensemble des diviseurs positifs de k. Montrer que l'application :

$$\begin{array}{rccc} & D_n \times D_{n'} & \longrightarrow & D_{nn'} \\ \varphi : & (d, d') & \longmapsto & dd' \end{array}$$

est bijective.

b. En déduire que si n et n' sont des entiers naturels premiers entre eux, $\sigma(nn') = \sigma(n)\sigma(n')$.

4) a. Soit $p \geqslant 1$. Montrer que p est premier si, et seulement si $\sigma(p) = p + 1$.

b. Calculer pour $(q, r) \in \mathbb{N}^2$, $q, r \geqslant 2$, la somme $1 + q + q^2 + \ldots + q^r$.

c. Déterminer pour p premier et $r \geqslant 2$, $\sigma(p^r)$.

d. Exprimer $\sigma(n)$ où $n = p_1^{r_1} \ldots p_s^{r_s}$ avec $p_1 < \ldots < p_s$ premiers et chaque $r_i \geqslant 1$.

5) Montrer que si $M_{n+1} = 2^{n+1} - 1$ est premier, $2^n(2^{n+1} - 1)$ est parfait.

6) En utilisant la question **3)**, prouver que si a est parfait et pair, il existe $n \geqslant 1$ tel que $a = 2^n(2^{n+1} - 1)$ où $M_{n+1} = 2^{n+1} - 1$ est premier.

7) Montrer qu'un nombre $n \geqslant 3$ parfait et impair, alors n admet au moins trois facteurs premiers distincts.

A l'heure actuelle, on ne sait toujours pas s'il existe des nombres parfaits impairs.

Problème 2 :

Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers $k \in [\![1, n]\!]$ tel que $\text{pgcd}(k, n) = 1$ (c'est aussi le nombre de $k \in [\![0, n-1]\!]$ tel que $\text{pgcd}(k, n) = 1$).

I. Première partie.

Soit G un groupe dont la loi est notée multiplicativement. On suppose G cyclique d'ordre $n \geqslant 1$ engendré par a.

1) Soit $1 \leqslant k \leqslant n$. Montrer l'équivalence des deux conditions suivantes :

(i) a^k engendre G.

(ii) k et n sont premiers entre eux.

En déduire que tout groupe cyclique d'ordre n admet $\varphi(n)$ générateurs.

2) Soit d un diviseur de n. Montrer que $a^{\frac{n}{d}}$ est d'ordre d.

3) Soit $p \in \mathbb{Z}$. Montrer que l'ordre de a^p est $\dfrac{n}{\text{pgcd}(n, p)}$.

Si d est un diviseur de n, on note H_d le sous-groupe engendré par $a^{\frac{n}{d}}$.

4) Soit H' un sous-groupe de G d'ordre d. Montrer que $H' = H_d$. En déduire que pour tout diviseur d de n, G possède un unique sous-groupe d'ordre d.

5) Soit $b \in G$, $d \in \mathbb{N}$. Montrer que b engendre H_d si et seulement si b est d'ordre d. Combien H_d a t-il de générateurs?

6) Conclure que

$$n = \sum_{d|n} \varphi(d)$$

II. Deuxième partie.

1) Soit m et n deux entiers premiers entre eux. Soit $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ muni de la structure de groupe produit : si $(a, b, c, d) \in \mathbb{Z}^4$,

$$(\overline{a}, \dot{b}) + (\overline{c}, \dot{d}) = (\overline{a+b}, \dot{c+d}),$$

la classe de $x \in \mathbb{Z}$ modulo m (resp. n) étant noté $\overline{x}$ (resp. $\dot{x}$).

a. Quel est l'ordre de $a = (\overline{1}, \dot{1})$ dans le groupe $(G, +)$. En déduire que a engendre G. À quel groupe simple est isomorphe G ?

b. Soit $(k, l) \in \mathbb{Z}^2$. On suppose que k est premier avec m, l premier avec n. Montrer que $(\overline{k}, \dot{l})$ est d'ordre mn.

c. Soit $(k, l) \in \mathbb{Z}^2$. On suppose que k n'est pas premier avec m. Montrer que $(\overline{k}, \dot{l})$ a un ordre strictement inférieur à mn.

On montrerait qu'il en va de même si l n'est pas premier avec n.

d. Conclure que $\varphi(mn) = \varphi(m)\varphi(n)$.

2) Soit p un nombre premier.

a. Calculer $\varphi(p)$.

b. Soit $\alpha \in \mathbb{N}^*$. Dénombrer les multiples de p dans $[\![1, p^\alpha]\!]$. En déduire $\varphi(p^\alpha)$.

3) Soit $n \in \mathbb{N}^*$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers (les p_i sont premiers deux à deux distincts). Montrer que

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

Problème 3 :

Soient $f : [0,1] \longrightarrow [0,1]$ une fonction croissante et

$$F = \{x \in [0,1], \quad f(x) \leqslant x\}$$

1) Montrer que $F \neq \emptyset$.
2) Montrer que si $x \in F$, $f(x) \in F$.
3) Etablir l'existence de $a \in F$ tel que $f(a) = a$ (considérer $\inf F$).