SÉRIE 6 DISTRIBUÉE LE 26 MARS 2009

(1) Montrer le critère suivant permettant de déterminer si un nombre donné est premier ou non :

Proposition. Le nombre entier $n > 1$ est premier ssi pour tout $1 < d \leq \sqrt{n}$, n n'est pas divisible par d.

(2) Pour tout entier $n \geq 0$ on définit le n-ième *nombre de Fermat*

$$F_n = 2^{2^n} + 1.$$

(a) Montrer par récurrence que $\prod_{k=0}^{n-1} F_k = F_n - 2$.
(b) Pour des indices m, n distincts, montrer que F_m et F_n sont premiers entre eux.
(c) En déduire une démonstration de l'infinitude des nombres premiers.

Digression historique. Fermat a cru que F_n est premier pour tout n. En 1732, Euler a découvert que F_5 ne l'est pas, et plus précisément que c'est un multiple de 641. En effet, comme

$$2^{2^5} = (641 - 625)2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 = 641 \cdot 2^{28} - (641 - 1)^4$$

on voit que $641 \mid 2^{2^5} + 1$. Aujourd'hui, on ne connaît aucun nombre de Fermat qui soit premier, hormis les cinq connus de Fermat et Euler. On connaît plusieurs nombres de Fermat composés (= non premiers), par exemple celui d'indice 23471 (!). Mais on ne sait s'il y a une infinité de nombres de Fermat premiers, ni s'il y en a une infinité de composés.

(3) (a) Pour les entiers $a, m \geq 2$, montrer que si $n = a^m - 1$ est premier, alors $a = 2$ et m est premier.

Pour p premier, le nombre $2^p - 1$ s'appelle le nombre M_p de Mersenne. Trouver les deux premières valeurs p_1 et p_2 telles que le nombre de Mersenne M_{p_1} est premier et le nombre de Mersenne M_{p_2} est composé.

Remarque. Actuellement, 46 nombres premiers de Mersenne sont connus, le plus grand étant $M_{43112609} = 2^{43112609} - 1$. On ne sait pas s'il y a des nombres de Mersenne non encore découverts entre $M_{13466917}$ et $M_{43112609}$.

(b) Un nombre entier n est *parfait* s'il est égal à la somme de ses diviseurs d tels que $1 \leq d < n$. Vérifier que 6 et 28 sont parfaits. Montrer que si p est un nombre premier tel que le nombre de Mersenne $M_p = 2^p - 1$ est aussi premier, alors $n = 2^{p-1}(2^p - 1)$ est parfait.

Remarque. Euclide connaissait une preuve de ce fait. Dix-huit à vingt siècles plus tard, Euler a montré que, réciproquement, tout nombre parfait *pair* est de cette forme.

(4) Un groupe G est dit *cyclique* s'il existe un $g \in G$ tel que tout élément de G est une puissance de g.

Soit m un nombre entier, $m \geq 2$. On peut montrer que le groupe $U(\mathbb{Z}/m\mathbb{Z})$ des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$ est cyclique si et seulement si m est ou bien une puissance d'un nombre premier impair, ou bien le double d'une puissance d'un nombre premier impair, ou bien l'un des nombres 2, 4.

Vérifier cet énoncé pour les nombres composés $m \leq 14$.

(5) Prouver le théorème de Wilson : Pour tout nombre premier p on a

$$(p-1)! \equiv -1 \mod p.$$

Indication:

(i) Vérifier le théorème pour $p = 2$ et $p = 3$; ceci fait, on suppose $p \geq 5$.

(ii) Soient $x, y \in \{1, \ldots, p-1\}$ tels que $xy \equiv 1 \mod p$; alors $x = y$ si et seulement si $x = 1$ ou $x = p - 1$.

(iii) Montrer que $2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \mod p$. [Grouper les facteurs par paires.]

(iv) Constater l'égalité $1 \cdot (p-1) \equiv -1 \mod p$.

(6) (a) Pour un entier $n \geq 2$, montrer que $(n-1)! \equiv -1 \mod n$ si et *seulement si* n est premier.

Indication: Supposons que $n = qd$ avec $1 < q < n$. Alors q est un facteur qui intervient dans $(n-1)!$, de sorte que $(n-1)! \equiv 0 \mod q$. Si on avait $(n-1)! \equiv -1 \mod n$, on aurait a fortiori $(n-1)! + 1 \equiv 0 \mod q$, exclu par ce qui précède.

Remarque : Vu de (a), le théorème de Wilson fournit un test pour la primalité d'un nombre entier, mais aucune indication pour les facteurs d'un nombre non premier!

(b) Soit $n > 1$ un nombre qui n'est pas premier. Si $n \neq 4$, préciser l'affirmation de (a) en montrant que $(n-1)! \equiv 0 \mod n$.