Exercices - Feuille F `À rendre le 9 Avril 2004`

Exercice F1. Soit p un nombre premier impair et f un entier ≥ 1.
a) Montrer par récurrence sur $k \geq 0$ la congruence

$$(p+1)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}.$$

b) En déduire que la classe de $p+1$ modulo p^f est d'ordre p^{f-1} dans $(\mathbf{Z}/p^f\mathbf{Z})^\times$.
c) Soit x un entier dont la classe modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^\times$ (autrement dit soit x une racine primitive modulo p). Montrer que l'ordre de la classe de x modulo p^f dans $(\mathbf{Z}/p^f\mathbf{Z})^\times$ est un multiple de $p-1$. En déduire qu'il existe un élément d'ordre $p-1$ dans $(\mathbf{Z}/p^f\mathbf{Z})^\times$.
d) En conclure que $(\mathbf{Z}/p^f\mathbf{Z})^\times$ est cyclique.
e) Soit y un entier dont la classe modulo p^2 engendre $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Montrer que la classe de y modulo p^f engendre $(\mathbf{Z}/p^f\mathbf{Z})^\times$.
f) Combien y a-t-il d'entiers modulo p^2 dont la classe modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^\times$ mais dont la classe modulo p^2 n'engendre pas $(\mathbf{Z}/p^2\mathbf{Z})^\times$?

Exercice F2. Soit f un entier ≥ 1.
a) Vérifier que le groupe multiplicatif $(\mathbf{Z}/2^f\mathbf{Z})^\times$ est cyclique pour $f=1$ et $f=2$.
On suppose désormais $f \geq 3$.
b) Montrer par récurrence sur $k \geq 0$ la congruence

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

c) En déduire que la classe de 5 modulo 2^f est d'ordre 2^{f-2} dans $(\mathbf{Z}/2^f\mathbf{Z})^\times$.
d) Montrer que la classe de -1 modulo 2^f n'appartient pas au sous-groupe de $(\mathbf{Z}/2^f\mathbf{Z})^\times$ engendré par la classe de 5.
e) En conclure que $(\mathbf{Z}/2^f\mathbf{Z})^\times$ est isomorphe au produit d'un groupe cyclique d'ordre 2 par un groupe cyclique d'ordre 2^{f-2}, donc n'est pas cyclique.

http://www.math.jussieu.fr/∼miw/enseignement.html