Éléments primitifs de $\mathbb{F}_p$

Exercice. Soit p un nombre premier.

(1) Montrez que la classe modulo p de l'entier

$$1+\sum_{i=1}^{p-1}\prod_{j=1}^{i}\left(1-\prod_{k=1}^{\lfloor\frac{p-1}{2}\rfloor}(j^k-1)^{p-1}\right)$$

est un générateur du groupe multiplicatif $\mathbb{F}_p^\times$.

En général, si q est une puissance de p et k est un corps à q éléments [1], on appelle *élément primitif* de k un générateur du groupe (cyclique) multiplicatif $k^\times$.

(2) *Essayez* d'utiliser cette formule pour $p = 7, 19, 43$ et comparez avec la « méthode bête » consistant à tester si $2, 3, \ldots$ est un générateur.

1. Lire le paragraphe 9.3.3 dans le *Cours d'algèbre* de Demazure à propos de la notation $\mathbb{F}_q$ et ses dangers.