Arithmétique

d'après Capes 2013

Partie A: Théorème de Lagrange

1. Montrer que, pour tout entier $n \geqslant 1$ et pour tout entier $k \in \{1, 2, \ldots, n\}$, on a $k\binom{n}{k} = n\binom{n-1}{k-1}$.
2. Montrer que, pour tout entier premier p et pour tout entier $k \in \{1, 2, \ldots, p-1\}$, p divise $\binom{p}{k}$.
3. Soit p un nombre premier impair. On considère la fonction f définie sur $\mathbb{R}$ par $f(x) = \prod_{k=1}^{p-1}(x+k)$.
   (a) Montrer que, pour tout réel x, nous avons $p \cdot f(x) = (x+1)f(x+1) - xf(x)$.
   (b) Justifier l'existence d'un p-uplet d'entiers $(a_0, a_1, \ldots, a_{p-1})$ tel que, pour tout réel x, nous ayons
   $$f(x) = \sum_{k=0}^{p-1} a_k x^{p-1-k}.$$
   (c) Montrer que $a_0 = 1$ et que $a_{p-1} = (p-1)!$.
   (d) A l'aide de la question **3.1** et en utilisant le binôme de Newton, montrer que pour tout entier $k \in \{1, 2, \ldots, p-1\}$, on a
   $$p \cdot a_k = \sum_{i=0}^{k} \binom{p-i}{k+1-i} a_i$$
   (e) En déduire que $a_1 = \binom{p}{2}$ et que, pour tout entier $k \in \{2, 3, \ldots, p-1\}$, on a
   $$k \cdot a_k = \binom{p}{k+1} + \sum_{i=1}^{k-1} \binom{p-i}{k+1-i} a_i$$
   (f) En déduire le théorème de Lagrange: si p est un entier premier impair et si $f(x) = \prod_{k=1}^{p-1}(x+k) = \sum_{k=0}^{p-1} a_k x^{p-1-k}$, alors les coefficients $a_1, a_2, \ldots, a_{p-2}$ sont divisibles par p.
   On pourra raisonner par récurrence

Partie B: Théorème de Wilson

On se propsoe de démontrer la propriété suivante, connue sur le nom de théorème de Wilson: si p est un entier premier, alors $(p-1)! \equiv -1 \mod p$.

1. Vérifier que la propriété est vraie pour $p = 2$.
2. On considère maintenant p un entier premier impair.
   (a) Montrer que $p! = 1 + \sum_{k=1}^{p-2} a_k + (p-1)!$ où les entiers $a_1, a_2, \ldots, a_{p-2}$ sont ceux définis à la question **A.3.2**
   (b) En déduire que $(p-1)! \equiv -1 \mod p$.
3. Montrer que la réciproque du théorème de Wilson est vraie.

4. On se propose d'étuder ce que devient le théorème de Wilson pour les entiers non premiers supérieur à 4.

   (a) On suppose que $n > 4$ et que la décomposition en produit de facteurs premiers de n comporte au moins deux facteurs premiers distincts. Montrer que $(n-1)! \equiv 0 \mod n$.

   (b) On suppose que $n > 4$ et que $n = p^\alpha$ où p est un entier premier et α est un entier strictement supérieur à 2.
   Montrer que $(n-1)! \equiv 0 \mod n$.

   (c) On suppose que $n > 4$ et que $n = p^2$, où p est un entier premier. Montrer que $1 < 2p < n$ et en déduire que $(n-1)! \equiv 0 \mod n$.

Partie C: Théorème de Wolstenholme

Pour tout entier naturel $n \geqslant 1$, on considère le rationnel $H_n = \sum_{k=1}^{n} \frac{1}{k}$. On désigne par s_n et t_n les deux entiers naturels tels que $H_n = \frac{s_n}{t_n}$ et $pgcd(s_n, t_n) = 1$.

1. Ecrire un algorithme permettant d'obtenir pour n allant de 2 à 10, les entiers s_n et t_n (on supposera que l'on dispose d'une instruction $pgcd(a, b)$ qui renvoir le plus grand commun diviseur des deux entiers a et b).

2. Calculer s_4, s_6 et s_{10}, et vérifier que ces entiers sont divisibles respectivement par 5^2, 7^2 et 11^2.

   Dans la suite, p désigne un nombre premier strictement supérieur à 3. On se propose de démontrer que l'entier s_{p-1} est divisible par p^2 (théorème de Wolstenholme).

3. Montrer que $H_{p-1} = \frac{a_{p-2}}{(p-1)!}$, où a_{p-2} est défini comme à la partie A. *On pourra utiliser une relation liant les racines d'un polynôme à l'un de ses coefficients*

4. Déduire de l'écriture de $f(-p)$ que $a_{p-2} = p^{p-2} - a_1 p^{p-3} + \ldots + a_{p-3} p$.

5. Conclure.