بِسمِ اللهِ الرَّحمٰنِ الرَّحِيمِ

Devoir Libre $N°$ 4

Travel in arithmetics

À rendre le

Objectif

✍ On démontre dans la premiere partie un théorème de **Lagrange** dont on utilise le résultat pour démontrer le théorème de **Wilson** dans la deuxième partie.
✍ Dans la suite du problème on s'intéresse à **l'indicatrice d'Euler** : la troisième partie donne une formule de $\varphi(n)$. La quatrième partie présente le théorème **d'Euler** qui généralise le **petit théorème de Fermat**.

PROBLÈME

Première partie :
Théorème de Lagrange

1. Monter que pour tout entier $n \geq 1$ et tout $k \in [\![1, n]\!]$ $kC_n^k = nC_{n-1}^{k-1}$.
2. Montrer que pour tout entier premier p et tout entier $k \in [\![1, p-1]\!]$, p divise C_p^k.
3. Soit p un entier premier ≥ 3. On considère la fonction f définie sur $\mathbb{R}$ par :

$$f(x) = \prod_{k=1}^{p-1} (x+k)$$

3.1 Montrer que pour tout réel x on a $pf(x) = (x+1)f(x+1) - xf(x)$.

3.2 justifier l'existence des entiers $a_0, a_1, \ldots, a_{p-1}$ tels que, pour tout $x \in \mathbb{R}$;
$f(x) = \sum_{k=0}^{p-1} a_k x^{p-1-k}$.

3.3 Montrer que $a_0 = 1$ et $a_{p-1} = (p-1)!$.

3.4 À l'aide de la question 3.a et en faisant intervenir le binôme de Newton, montrer que pour tout entier $k \in [\![0, p-1]\!]$ $pa_k = \sum_{i=0}^{k} C_{p-i}^{k+1-i} a_i$.

3.5 En déduire que $a_1 = C_p^2$ et que pour tout $k \in [\![2, p-1]\!]$ on a :

$$ka_k = C_p^{k+1} + \sum_{i=1}^{k-1} C_{p-i}^{k+1-i} a_i$$

3.6 En déduire le théorème de **Lagrange** :

Si p est un entier premier ≥ 3 et $f(x) = \prod_{k=1}^{p-1}(x+k) = \sum_{i=0}^{p-1} a_i x^{p-1-i}$ alors les coefficients $a_1, \ldots, a_{p-2}$ sont divisibles par p.

Deuxième partie :
Théorème de Wilson

On se propose dans cette partie de démontrer le théorème de **Wilson** :
Si p est un entier premier alors $(p-1)! = -1\ [p]$.

1. Vérifier que la propriété est vraie pour $p = 2$.
2. p est maintenant un entier premier ≥ 3.
   - 2.1 Montrer que $p! = 1 + \sum_{k=1}^{p-2} a_k + (p-1)!$.
     Les entiers $(a_i)_i$ sont ceux définis à la question 3.b
   - 2.2 En déduire que $(p-1)! = -1\ [p]$
3. Montrer que la réciproque du théorème de **Wilson** est vraie.
4. On se propose d'étudier ce que devient le théorème de **Wilson** pour les entiers non premiers supérieurs strictement à 4.
5. On suppose que $n > 4$ et que la décomposition en produit de facteurs premiers de n comprend au moins deux facteurs premiers distincts. Montrer que $(n-1)! = 0\ [n]$.
6. On suppose que $n > 4$ et que $n = p^\alpha$ où p est un entier premier et α un entier strictement supérieur à 2. Montrer que $(n-1)! = 0\ [n]$.
7. 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 $(n-1)! = 0\ [n]$.

Troisième partie :
Indicatrice d'Euler

Soit $n \in \mathbb{N}^*$, on définit **l'indicatrice d'Euler** par :

$$\varphi(n) = \text{card}(P(n))$$

où

$$P(n) = \{k \in [[1,n]] /\ k \wedge n = 1\}$$

Autrement dit $\varphi(n)$ est le nombre d'entiers naturels premiers avec n inférieurs à n.

1. Calculer $\varphi(n)$, pour $n = 1, 2, 7, 16$.
2. Soit $p \in \mathbb{N}^*$. Montrer que p est premier si, et seulement si, $\varphi(p) = p - 1$.
3. Soit p premier et $\alpha \in \mathbb{N}^*$.
   - 3.1 Soit $k \in \mathbb{N}^*$, montrer que k et p^α ne sont pas premiers eux si, et seulement si, p divise k.
   - 3.2 Qu'il est le nombre des multiples de p compris entre 1 et p^α.
   - 3.3 En déduire que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
4. Soit $m, n \in \mathbb{N}^*$ deux entiers premiers entre eux , on définit l'application $h : P(nm) \to P(n) \times P(m)$ par $h(x) = (r(x), s(x))$ où $r(x)$ est le reste dans la division euclidienne de x par n et $s(x)$ le reste dans la division euclidienne de x par m.

4.1 Montrer que h est bien définie.

4.2 Soit $(r,s) \in P(n) \times P(m)$

4.2.1 Justifier l'existence de deux entiers relatifs u et v tels que $nu + mv = 1$.

4.2.2 On pose $z = sum + rvn$. Montrer que $z = r\,[n]$ et $z = s\,[m]$.

4.2.3 En déduire que h est surjective.

4.3 Montrer que h est bijective.

4.4 En déduire que $\varphi(nm) = \varphi(n)\varphi(m)$.

5. Soit $n \geq 2$, dont la décomposition en facteurs premiers s'écrit : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Démontrer que $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

Quatrième partie :
Théorème d'Euler

Le bute de cette partie est de démontrer le théorème d'**Euler** qui s'énonce ainsi :
Soit $n \geq 2$ et a un entier tel que $a \wedge n = 1$ alors $a^{\varphi(n)} = 1\,[n]$.
Soit $n \in \mathbb{N}^*$, $a \in P(n)$ et $r : P(n) \to P(n)$ où pour $x \in P(n)$, $r(x)$ désigne le reste de la division euclidienne de ax par n.

1. Montrer que r est bien définie.

2. Justifier que, pour tout $x \in P(n)$, il existe $y \in P(n)$ tel que $xy = 1\,[n]$.

3. Montrer que r est bijective.

4. Justifier que, pour tout $x \in P(n)$; $r(x) = ax\,[n]$.

5. En déduire que $a^{\varphi(n)} = 1\,[n]$.
Indication : Calculer modulo n ; de deux façons le produit des éléments de $P(n)$.

6. Retrouver **le petit théorème de Fermat**.