Exercices - Nombres premiers

Exercice 1

On note $[x]$ la partie entière de x réel

1. Soit n un entier naturel tel que $n > p$ avec p premier
   Montrer que le nombre de multiples de p appartenant à $[\![p; n]\!]$ est $[\frac{n}{p}]$
2. Considérons l'ensemble E des termes 2, 3,...,n intervenant dans $n!$
   Soit p^k la plus grande puissance de p divisant n
   On note $M(p^i, \overline{p^{i+1}})$ les multiples de p^i mais pas de p^{i+1} pour $1 \leqslant i \leqslant k-1$

   On partitionne E par $E = \cup_i M(p^i, \overline{p^{i+1}}) \cup M(p^k)$

   En déduire que l'exposant α du facteur premier p dans $n!$
   est $\alpha = [\frac{n}{p}] + [\frac{n}{p^2}] + ...$
3. En déduire que l'exposant de 2 dans 100 ! est 97 et l'exposant de 5 dans 100 ! est 24
4. En déduire que 100 ! se termine par 24 zéros

Exercice 2

Soit q un nombre premier tel que $q > 5$ et $P = 5 \times 7 \times .... \times q$ le produit de tous les nombres premiers entre 5 et q.

On pose $N = 2^2P + 3$

1. Soit p un nombre premier divisant N.
   Montrer que $p > q$ et que p est de la forme $4n + 1$ ou $4n + 3$
2. Soit $N = \prod_i p_i^{\alpha_i}$ la décomposition de N en facteurs premiers. En raisonnant par l'absurde montrer qu'il existe un des facteurs premiers de la forme $4n + 3$
3. En déduire qu'il existe une infinité de nombres premiers de la forme $4n + 3$

Exercice 3

Adapter l'exercice précédent pour montrer qu'il existe une infinité de nombres premiers de la forme $6n + 5$

Exercice 4 *Identité de Sophie Germain et applications*

1. Vérifier que $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$
2. Est ce que $4^{545} + 545^4$ est premier ?
3. Montrer que si $n > 1$ alors $n^4 + 4^n$ est composé (il suffit de montrer pour n impair et utiliser 1))

Exercice 5

1. Soit $n \in \mathbb{N}^*$
   Montrer que la liste suivante comporte n entiers naturels composés

$$(n+1)! + 2,\ (n+1)! + 3,\ ....\ (n+1)! + n + 1$$

2. Ce qui a été prouvé précédemment est-il contradictoire avec le théorème suivant :
   Théorème de Tchebichev (1856) : Pour tout $n \geqslant 2$ il existe au moins un nombre premier entre n et $2n$

Exercice 6

1. Montrer par récurrence que pour tout $n \geqslant 1$ on a $10^n \equiv 4$ [6]
2. Justifier que $10^6 \equiv 1$[7]
3. En déduire que pour tout $n \geqslant 1$ on a $10^{10^n} \equiv 4$ [7]

Exercice 7
Soit p un nombre premier $\geqslant 3$. Pour $k \geqslant 1$ on pose $n = (p-1)(kp+1)$

1. Prouver que $n \equiv -1$ [p]
2. Prouver que $2^n \equiv 1$ [p]
3. En déduire que p divise $n.2^n + 1$

Exercice 8
Etant donnés deux entiers a et b tel que a et b plus grands que 2 et soit $N = ab(a^{60} - b^{60})$
Soit p un nombre premier tel que $p-1$ divise 60, montrer que p divise N
Exercice 9 *Théorème de Wilson*
Il s'agit de démontrer le théorème suivant :
p premier $\iff (p-1)! \equiv -1$ [p]

1. Vérifier la propriété pour $p = 3$, $p = 5$ et $p = 7$
2. Montrons que si p premier alors $(p-1)! \equiv -1$ [p] :
   (a) Montrer que $(p-1) \times (p-1) \equiv 1$ [p]
   On dit que $p-1$ est son propre inverse modulo p
   (b) Montrer que 1 aussi est son propre inverse modulo [p]
   (c) Soit a un nombre tel que $1 < a < p-1$. Montrer que a a un inverse modulo p différent de a . Montrer que cet inverse est unique on le note a^{-1}
   (d) Soit a et b deux nombres tel que $1 < a < p-1$ et $1 < b < p-1$. Montrer que si $a^{-1} = b^{-1}$ alors $a = b$
   (e) Montrer que l'on peut coupler les nombres de 2 à $(p-2)$ en mettant un nombre avec son inverse modulo p et en déduire que $(p-1)! \equiv p-1$ [p] $\equiv -1$ [p]
3. Montrons maintenant que si p composé alors $(p-1)! \not\equiv -1$ [p]
   (a) Tester pour $p = 4$
   (b) Supposons que $p = q^2 > 4$ dans ce cas montrer que $(p-1)! \equiv 0[p]$
   (c) Supposons que p ne soit pas un carré donc il existe deux entiers a et b tel que $1 < a < b < p$ et $p = ab$ en déduire $(p-1)! \equiv 0[p]$

Exercice 10 Vrai ou Faux ?

1. Si p est premier alors $p+1$ n'est pas premier
2. Si p est premier alors $p+2$ n'est pas premier
3. p est premier si et seulement si $p \equiv 1$ [6] ou $p \equiv -1$ [6]

4. $a^2 - b^2$ premier si et seulement si a et b consécutifs
5. Pour tout $n \geqslant 2$ et pour tout a,b entiers $(a+b)^n \equiv a^n + b^n \ [n]$

Exercice 11 *Crible de Mathyiasevitch*
Soit la parabole $\mathcal{P}$ d'équation $y = x^2$ relativement à un repère orthonormé
Soit m et n deux entiers naturels

1. Soit $N(n, n^2)$ et $M(-m, m^2)$ des points de la parabole. Quel est le point d'intersection de la droite (MN) et l'axe des ordonnées ?
2. Quels sont les points de l'axe des ordonnées qui n'appartiennent à aucune droite (MN) tracée lorsque m et n parcourent $\mathbb{N}^*$?