Exercices : Nombres premiers

Exercice 1

1. Vérifier que les entiers 2,3,5,7,11,13,17,19,23,31,37,41,47 sont premiers
2. Justifier que 2017 est premier

Exercice 2

Montrer que si p et q sont premiers alors ils sont premiers entre eux

Exercice 3

Soit $P(n) = n^2 - n + 41$

Calculer $P(n)$ pour n de -39 à 40 et vérifier que $P(n)$ est premier

Exercice 4 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 5 *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 $\mathbb{N}^*$?

Exercice 6

1. Vérifier que $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$
2. Quels sont les valeurs de a pour lesquelles $a^3 - 27$ est premier ?

Exercice 7

1. Vérifier que $x^4 + x^2 + 1 = (x^2 + 1 + x)(x^2 + 1 - x)$
2. Montrer que $f(n) = 2^{2^n} + 2^{2^{n-1}} + 1$ a au moins n facteurs premiers pour $n \geqslant 1$

Exercice 8 *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 9 *Petit Théorème de Fermat (congruences)*

1. Montrer que pour tout nombre premier p et pour tout k tel que $1 \leqslant k \leqslant p-1$ on a $p|\binom{p}{k}$
2. En déduire que pour tout a,b entiers et p premier $(a+b)^p \equiv a^p + b^p \ [n]$
3. Démontrer par récurrence pour tout a entier et p premier , que $a^p \equiv a \ [p]$

Exercice 10

1. Décomposer 1001 en facteurs premiers
2. Soit 3 chiffres non nuls a,b er c. Vérifier que le nombre $abcabc = abc \times 1001$
3. En déduire que $abcabc$ est composé
4. Que peut on dire de $abcabcabc$?

Exercice 11 *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 12 *Nombres a pseudo premier*

Montrer en utilisant les propriétés des congruences que

1. 341 est un nombre 2-pseudo premier
2. 15 est un nombre 4-pseudo premier

Exercice 13 *Nombres de Carmichael*

A l'aide d'un programme en Python vérifier que 561 est un nombre de Carmichaël

Exercice 14

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

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

Indications :

1. Traiter plusieurs cas particuliers : par exemple $5! = 120 = 2^3 \times 3 \times 5$ et d'autres et vérifier que la propriété est correcte

   Avoir compris que : Les nombres entre 2 et n multiples de p sont p,$2p$,....$[\frac{n}{p}]$, il y en a $[\frac{n}{p}]$

   puis, les nombres entre 2 et n multiples de p^2 sont p^2,$2p^2$,....$[\frac{n}{p^2}]$, il y en a $[\frac{n}{p^2}]$

   Ensuite on partitionne $n!$ ainsi on range les multiples de p mais pas de p^2 ensemble puis les multiples de p^2 mais pas de p^3, etc... et enfin le reste

   Pour obtenir p^α j'extrais p autant de fois qu'il y a d'éléments dans l'ensemble des multiples de p mais pas de p^2, puis j'extrais p^2 autant de fois qu'il y a d'éléments dans l'ensemble des multiples de p^2 mais pas de p^3 etc....

   Donc $\alpha = 1 \times (.....) + 2 \times (.....) + 3 \times (.....).....$

   La quantité qui multiplie 1 est le nombre d'éléments dans l'ensemble des multiples de p mais pas de p^2

   La quantité qui multiplie 2 est le nombre d'éléments dans l'ensemble des multiples de p^2 mais pas de p^3, etc...
2. Traduire "100 ! se termine par k zéros" par "dans la décomposition en facteurs premiers de 100 ! il y a ...."

Exercice 15

1. Démontrer par récurrence sur $n > 1$ que $\binom{2n}{n} > \dfrac{4^n}{2\sqrt{n}}$
2. En déduire par récurrence que pour tout n on a $P_n = \prod_{p_i \leqslant n} p_i < 4^n$
3. En déduire si p est un diviseur premier de $\binom{2n}{n}$ et si $p \geqslant \sqrt{2n}$ alors l'exposant de p dans la décomposition de $\binom{2n}{n}$ est 1

Indications :

1. Pour l'hérédité vérifier que $\binom{2(n+1)}{n+1} = \dfrac{2(2n+1)}{n+1}\binom{2n}{n}$

   puis montrer que $\dfrac{2(2n+1)}{n+1} > 2\sqrt{\dfrac{n}{n+1}}$ pour $n \geqslant 1$

2. Puisque $P_{2n} = P_{2n-1}$ pour l'hérédité le problème est le passage de $2n$ à $2n+1$ mais ici une récurrence "normale" serait maladroite il faut donc faire une récurrence forte et descendre de $2n+1$ à un rang k plus avant et

$$P_{2n+1} = \prod_{p_i \leqslant 2n+1} p_i = \prod_{p_i \leqslant k} p_i \prod_{k+1 \leqslant p_i \leqslant 2n+1} p_i$$

Si on applique l'hypothèse de récurence alors $\prod_{p_i \leqslant k} p_i < 4^k$ si on réussit à majorer $\prod_{k+1 \leqslant p_i \leqslant 2n+1} p_i$ par 4^{2n+1-k}, l'hérédité sera vérifiée
Quel k choisir ?
Prendre suffisamment de nombres premiers dans une suite de nombres entiers successifs qui ne va pas jusqu'à 2, nous fait penser au coefficient binomial
Vérifier que :

(a) Si p premier tel que $n+2 \leqslant p \leqslant 2n+1$ alors p divise $\binom{2n+1}{n}$

(b) En déduire $\prod_{n+2 \leqslant p_i \leqslant 2n+1} p_i$ divise $\binom{2n+1}{n}$

(c) En déduire $\prod_{n+2 \leqslant p_i \leqslant 2n+1} p_i \leqslant \binom{2n+1}{n}$

(d) Il reste à majorer $\binom{2n+1}{n}$ par une puissance de 4.
Retenir que les coefficients binomiaux interviennent dans la formule de Newton
donc $(1+1)^{2n+1} > \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}$ en déduire ce que l'on cherche et finir la démonstration de l'hérédité

3. On utilise le 1) de l'exercice 14 :
Si p est un diviseur premier de $\binom{2n}{n} = \dfrac{(2n)!}{n! \times n!}$ alors

(a) Justifier que l'exposant α de p dans $\binom{2n}{n}$ est égal à $([\frac{2n}{p}] - 2[\frac{n}{p}]) + ([\frac{2n}{p^2}] - 2[\frac{n}{p^2}]) + ...$

(b) Justifier que $\alpha = ([\frac{2n}{p}] - 2[\frac{n}{p}])$ (tenir compte de $p > \sqrt{2n}$) ($p = \sqrt{2n}$ que pour $n = 2$, donc on se place dans le cas $n > 2$)

(c) En déduire $\alpha = 1$

Exercice 16

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 17

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 18

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

Exercice 19 On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x

1. Que vaut $\pi(10)$?
2. On admet que $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10^6) = 78\ 498$ et $\pi(10^9) = 50\ 847\ 534$. Comparer $\dfrac{x}{\pi(x)}$ à $\ln(x)$
3. Gauss (1777-1855) conjectura que $\lim\limits_{x\to+\infty} \dfrac{\frac{\pi(x)}{x}}{\frac{1}{\ln(x)}} = 1$. Ce résultat ne fut démontré qu'un siècle plus tard en 1896 indépendamment par un mathématicien français Hadamard et un mathématicien belge De la Vallée Poussin. On regarde $\dfrac{\pi(x)}{x}$ comme **la densité de nombres premiers aux environs de** x Que vaut-elle aux environs de 10^{12} ? que vaut-elle aux environs de 10^{20} ?

Exercice 20

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 21

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 22

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