Exercices : Arithmétique

1 pgcd et ppcm

1.1 Calculs des coefficients de Bézout

Résoudre dans $\mathbb{Z}$ les équations suivantes :

$$95x + 71y = 1 \qquad 24x - 15y = 3 \qquad 12x + 15y + 20z = 1$$

1.2 Divers calculs de pgcd et ppcm

Soit a, b deux entiers. Calculer :

$$(15a^2 + 8a + 6) \wedge (30a^2 + 21a + 13) \qquad (a^3 + a) \wedge (2a + 1)$$

$$(a - b)^3 \wedge (a^3 - b^3) \qquad (a + b) \vee (a \wedge b)$$

1.3 Autour du pgcd

1. Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge c = 1$. Montrer que :
$$(ab) \wedge c = b \wedge c$$
2. Trouver l'ensemble des couples $(a, b) \in \mathbb{Z}^2$ tels que :
$$a \wedge b = a + b - 1$$

1.4 Autour de la suite de Fibonacci

On définit la suite de Fibonacci par :

$$F_0 = 0 \quad F_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N} \quad F_{n+2} = F_{n+1} + F_n$$

1. Démontrer que :
$$\forall n \in \mathbb{N}^* \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$
En déduire que F_n et F_{n+1} sont premiers entre eux.
2. Démontrer que :
$$\forall n \in \mathbb{N} \quad \forall p \in \mathbb{N}^* \quad F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$$
En déduire que $F_n \wedge F_p = F_{n+p} \wedge F_p$.
3. Montrer que :
$$\forall n, p \in \mathbb{N} \quad F_n \wedge F_p = F_{n \wedge p}$$

1.5 Reste de la division euclidienne d'une puissance

Soit n un entier supérieur à 2 et a un entier premier avec n. Pour tout entier k on note r_k le reste de la division euclidienne de a^k par n.

1. Montrer que la suite r est périodique. Pour cela on montrera dans l'ordre :
   (a) qu'il existe $k_1 > k_2$ tels que $a^{k_1} \equiv a^{k_2}\ [n]$
   (b) puis, qu'il existe $T \in \mathbb{N}^*$ tel que $a^T \equiv 1\ [n]$
   (c) et enfin conclure
2. Quel est le reste de la division euclidienne de 3^{1998} par 5 ?
3. Montrer que 13 divise $3^{126} + 5^{126}$.

2 Théorèmes classiques

2.1 Le théorème chinois

On se donne p_1 et $p_2 \in \mathbb{Z}$ premiers entre eux, et a_1 et $a_2 \in \mathbb{Z}$.

1. On souhaite montrer qu'il existe $n \in \mathbb{Z}$ tel que :
$$n \equiv a_1 \quad [p_1] \qquad \text{et} \qquad n \equiv a_2 \quad [p_2]$$
   (a) Montrer que le problème admet une solution lorsque $a_1 = 1$ et $a_2 = 0$ ainsi que lorsque $a_1 = 0$ et $a_2 = 1$.
   (b) En déduire le cas général.
2. En déduire l'ensemble des solutions du système :
$$n \equiv a_1 \quad [p_1] \qquad \text{et} \qquad n \equiv a_2 \quad [p_2]$$
3. **Application :** Résoudre le système
$$n \equiv 3 \quad [21] \qquad \text{et} \qquad n \equiv 1 \quad [5]$$

2.2 Les pirates

Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui-ci reçoit 3 pièces.
Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précedemment ; le cuisinier reçoit alors 4 pièces.
Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.
Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

2.3 Petit théorème de Fermat, système de chiffrementRSA

1. Soit p un nombre premier.
   (a) Soit $k \in [\![1, p-1]\!]$. Montrer que p divise $\binom{p}{k}$.
   (b) Soit $a, b \in \mathbb{Z}$. Montrer que :
   $$(a+b)^p \equiv a^p + b^p \quad [p]$$
   (c) En déduire que pour tout $m \in \mathbb{Z}$:
   $$m^p \equiv m \quad [p]$$
   (d) En déduire que si $m \in \mathbb{Z}$ et p sont premiers entre eux :
   $$m^{p-1} \equiv 1 \quad [p]$$
2. On se donne deux nombres premiers p et q distincts et on pose $n = pq$. Soit c, d deux entiers tels que
   $$cd \equiv 1 \quad [\varphi(n)]$$
   où $\varphi(n) = \text{Card}\{k \in [\![0, n-1]\!] : k \wedge n = 1\}$
   (a) Montrer que $\varphi(n) = (p-1)(q-1)$.
   (b) Montrer que si $t \in \mathbb{Z}$, alors $t^{cd} \equiv t \quad [n]$.

3 Sur les nombres premiers

3.1 Rarefication des nombres premiers

Montrer qu'il existe des intervalles de $\mathbb{N}$ de longueur aussi grande que l'on veut qui ne contiennent aucun nombre premier.

3.2 Encadrement du n-ième nombre premier

Pour tout $n \in \mathbb{N}^*$, on note p_n le n-ième nombre premier.

1. Montrer que :
   $$\forall n \in \mathbb{N} \quad p_{n+1} \leqslant p_1 \dots p_n + 1$$
2. En déduire que :
   $$\forall n \in \mathbb{N} \quad p_n \leqslant 2^{2^n}$$
3. Soit $x \in \mathbb{R}_+$. On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Montrer que pour x assez grand :
   $$\ln(\ln x) \leqslant \pi(x) \leqslant x$$
   On démontrera le fait que pour $n \geqslant 3$, $e^{e^{n-1}} \geqslant 2^{2^n}$.

3.3 Cas particuliers du théorème de Dirichlet

1. Montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$.
2. Montrer qu'il existe une infinité de nombres premiers de la forme $6k+5$.

Le théorème de Dirichlet *affirme que si a et b sont premiers entre eux, il existe une infinité de nombres premiers de la forme $ak+b$.*