Correction Fiche TD 12
Rudiment d'arithmétique

Partie A : Diviseurs et multiples

Exercice A1 : Démontrer que :

$$\sqrt{3} \notin \mathbb{Q}$$

On va faire cette démonstration par l'absurde de deux façons !

M1 : Sans les congruences

On suppose que $\sqrt{3} \in \mathbb{Q}$. On a alors :

$$\sqrt{3} \in \mathbb{Q} \Longrightarrow \exists (a,b) \in \mathbb{N} \times \mathbb{N}^*, \sqrt{3} = \frac{a}{b} \text{ et } a \wedge b = 1$$
$$\Longrightarrow a^2 = 3b^2$$
$$\Longrightarrow \exists k \in \mathbb{N}, a^2 = 3k^2$$

On va montrer le lemme suivant :

Lemme : Soit $a \in \mathbb{N}$. On a alors :

$$3|a^2 \Longrightarrow 3|a$$

Démo : On va prouver ce lemme par contraposée.

Soit $a \in \mathbb{N}$ tel que $3 \nmid a$.

1er cas : $\exists k \in \mathbb{N}, a = 3k + 1$

On a alors :

$$a^2 = 3(3k^2 + 2k) + 1 = 3k' + 1$$

Donc $3 \nmid a^2$

2ième cas : $\exists k \in \mathbb{N}, a = 3k + 2$

On a alors :

$$a^2 = 3(3k^2 + 4k + 1) + 1 = 3k' + 1$$

Donc $3 \nmid a^2$

Par contraposée on en déduit que :

$$3|a^2 \Longrightarrow 3|a$$

On en déduit donc que :

$$\exists k \in \mathbb{N}, a = 3k \Longrightarrow a^2 = 9k^2 \Longrightarrow 3b^2 = 9k^2 \Longrightarrow 3|b^2 \Longrightarrow 3|b$$

On a donc :

$$\begin{cases} a \wedge b = 1 \\ 3|a, 3|b \end{cases}$$

C'est impossible.

Donc $\sqrt{3} \notin \mathbb{Q}$.

M2 : Avec les congruences

On suppose que $\sqrt{3} \in \mathbb{Q}$. On a alors :

$$\sqrt{3} \in \mathbb{Q} \Longrightarrow \exists (a,b) \in \mathbb{N} \times \mathbb{N}^*, \sqrt{3} = \frac{a}{b} \text{ et } a \wedge b = 1$$
$$\Longrightarrow a^2 = 3b^2$$
$$\Longrightarrow a^2 \equiv 0[3]$$

Or on sait que :

$$a \equiv 1[3] \Longrightarrow a^2 \equiv 1[3] \text{ et } a \equiv (-1)[3] \Longrightarrow a^2 \equiv 1[3]$$

On en déduit donc par contraposée que :

$$a^2 \equiv 0[3] \Longrightarrow a \equiv 0[3]$$

On en déduit donc que :

$$\exists k \in \mathbb{N}, a = 3k$$

On a donc :

$$\exists k \in \mathbb{N}, a^2 = 9k^2$$

On a donc :

$$9k^2 = 3b^2 \Longrightarrow b^2 = 3k^2 \Longrightarrow b^2 \equiv 0[3] \Longrightarrow b \equiv 0[3] \Longrightarrow 3|b$$

On a donc :

$$\sqrt{3} \in \mathbb{Q} \Longrightarrow \exists (a,b) \in \mathbb{N} \times \mathbb{N}^*, \sqrt{3} = \frac{a}{b} \text{ et } a \wedge b = 1 \text{ et } 3|a, 3|b$$
$$\Longrightarrow \exists (a,b) \in \mathbb{N} \times \mathbb{N}^*, \sqrt{3} = \frac{a}{b} \text{ et } a \wedge b = 1 \text{ et } a \wedge b \geq 3$$

Contradiction.

Donc $\sqrt{3} \notin \mathbb{Q}$.

Exercice A2 : Soit $(a,b) \in \mathbb{Q}^2$ tels que $\sqrt{a} \notin \mathbb{Q}$ ou $\sqrt{b} \notin \mathbb{Q}$. Montrer que $\sqrt{a} + \sqrt{b} \notin \mathbb{Q}$

On raisonne par contraposée. On suppose que :

$$\sqrt{a} + \sqrt{b} \in \mathbb{Q}$$
$$\Longrightarrow \exists (p,q) \in \mathbb{Z}^* \times \mathbb{N}^*, \sqrt{a} + \sqrt{b} = \frac{p}{q} > 0$$
$$\Longrightarrow \frac{q}{p}(a-b) = \left(\sqrt{a} - \sqrt{b}\right)$$
$$\Longrightarrow \sqrt{a} - \sqrt{b} \in \mathbb{Q} \ (\text{car } (a,b) \in \mathbb{Q}^2)$$

On en déduit donc que :

$$\exists (p,p',q,q') \in \mathbb{Z}^2 \times (\mathbb{N}^*)^2, \begin{cases} \sqrt{a} + \sqrt{b} = \frac{p}{q} \\ \sqrt{a} - \sqrt{b} = \frac{p'}{q'} \end{cases}$$
$$\Longrightarrow \exists (p,p',q,q') \in \mathbb{Z}^2 \times (\mathbb{N}^*)^2, \sqrt{a} = \frac{1}{2}\left(\frac{p}{q} + \frac{p'}{q'}\right) = \frac{pq' + p'q}{2qq'}$$
$$\Longrightarrow \exists (p'',q'') \in \mathbb{Z}^2 \times (\mathbb{N}^*)^2, \sqrt{a} = \frac{p''}{q''}$$
$$\Longrightarrow \sqrt{a} \in \mathbb{Q}$$

Par contraposée on en déduit donc que :

$$\sqrt{a} \notin \mathbb{Q} \text{ et } \sqrt{b} \notin \mathbb{Q} \Longrightarrow \sqrt{a} + \sqrt{b} \notin \mathbb{Q}$$

Exercice A.3 : Soit n un entier naturel non nul. Déterminer la division euclidienne de 7n+16 par 2n+3.

On sait que :

$$\forall n \in \mathbb{N}^*, 7n + 16 = 3(2n+3) + n + 7$$

On sait que $n + 7$ est le reste de la division euclidienne de 7n+16 par 2n+3 si et seulement si $0 \leq n + 7 < 2n + 3$. On résout :

$$n + 7 < 2n + 3 \Leftrightarrow n > 4$$

On en déduit donc que :

$\forall n \geq 5$, le reste de la division euclidienne de 7n+16 par 2n+3 est n+7 et le quotient est 3.

Pour $n \leq 4$ on a :

$$7n + 16 = 4(2n+3) - n + 4$$

$\forall n \in [\![1;4]\!]$, le reste de la division euclidienne de 7n+16 par 2n+3 est $4 - n$ et le quotient est 4.

Exercice A.4 : La différence de deux entiers naturels est 538. Si l´on divise l´un par l´autre, le quotient est 13 est le reste est 34. Déterminer ces deux nombres.

On pose a et b les deux nombres recherchés. On suppose que $a > b$. On en déduit donc que a et b vérifient le système suivant :

$$\begin{cases} a - b = 538 \\ a = 13b + 34 \end{cases}$$

On a alors :

$$\begin{cases} a - b = 538 \\ a = 13b + 34 \end{cases} \Leftrightarrow a = 498 \text{ et } b = 42$$

Exercice A.5 : Soit $(a_0; a_1; \dots; a_n) \in [\![0; 9]\!]^{n+1}$. On pose :

$$\overline{a_n a_{n-1} \dots a_0} = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$$

Démontrer que :

$$3 | \overline{a_n a_{n-1} \dots a_0} \Leftrightarrow 3 | \sum_{k=0}^{n} a_k$$

On raisonne par récurrence. On pose :

$$\forall n \in \mathbb{N}, \mathcal{P}(n) = " \, 3 | (10^n - 1)"$$

Initialisation : n=0

On sait que $10^0 - 1 = 0$ et $3|0$ donc $\mathcal{P}(0)$ est vraie.

Hérédité : Soit n un entier naturel n fixé. On suppose vraie $\mathcal{P}(n)$. On a alors :

$$\exists k_n \in \mathbb{Z}, 10^n = 3k_n + 1$$

On en déduit donc que :

$$10^{n+1} = 10^n \times 10 = (3k_n + 1) \times 10 = 3(10k_n + 3) + 1$$

On en déduit donc que :

$$10^{n+1} = 3k_{n+1} + 1 \Longrightarrow 3 | (10^{n+1} - 1)$$

On en déduit donc que $\mathcal{P}(n)$ est héréditaire.

Conclusion : On conclut d'après le principe de récurrence.

De plus on sait que :

$$\overline{a_n a_{n-1} \dots a_0} = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$$
$$= \sum_{i=0}^{n} a_i \times 10^i = \sum_{k=0}^{n} a_k \times (3k_i + 1) = 3 \sum_{k=0}^{n} a_k \times k_i + \sum_{k=0}^{n} a_k$$

On en déduit donc que :

$$\sum_{k=0}^{n} a_k = \overline{a_n a_{n-1} \dots a_0} - 3 \sum_{k=0}^{n} a_k \times k_i$$

Comme $3 | 3 \sum_{k=0}^{n} a_k \times k_i$ on en déduit donc que :

$$3 | \overline{a_n a_{n-1} \dots a_0} \Leftrightarrow 3 | \sum_{k=0}^{n} a_k$$

Exercice A.6 : Montrer que :

$$a_n = \frac{21n - 3}{4} \text{ et } b_n = \frac{15n - 2}{4}$$

Ne sont pas simultanément dans $\mathbb{Z}$

On raisonne par l'absurde. On suppose que :

$$\exists n \in \mathbb{N}, \left(\frac{21n - 3}{4}, \frac{15n - 2}{4} \right) \in \mathbb{Z}^2$$

On en déduit donc que $4|(21n - 3)$ et $4|(15n - 2)$. On en déduit donc que 4 divise toutes combinaisons linéaire de $21n - 3$ et $15n - 2$.

On en déduit donc que :

$$4 | 7(15n - 2) - 5(21n - 3) \Longrightarrow 4 | 1$$

Cela est bien sur absurde. On en déduit donc que 4 ne divise pas simultanément $\frac{21n-3}{4}$ et $\frac{15n-2}{4}$.

Exercice A.7 : Montrer que :

$$\forall n \geq 2, 10 | \left(2^{2^n} - 6\right)$$

On raisonne par récurrence.
Initialisation : $n = 2$
On a :

$$2^{2^2} - 6 = 10$$

Hérédité : Soit n un entier naturel supérieur ou égale à 2. On suppose que $10 | \left(2^{2^n} - 6\right)$
Ainsi :

$$\exists k_n \in \mathbb{N} \; tel \; que \; 2^{2^n} - 6 = 10k_n$$

On a donc :

$$2^{2^{n+1}} - 6 = \left(2^{2^n}\right)^2 - 6 = (10k_n + 6)^2 - 6 =$$

Partie B : PPCM et PGCD

Exercice B.1 : Calculer $9100 \wedge 1848$ et $9100 \vee 1848$

On peut utiliser la décomposition en nombre premier de 9100 et de 1848.
On sait que :

$$9100 = 100 \times 91 = 2^2 \times 5^2 \times 91$$

Or on sait que $91 \in \mathcal{P}$. On peut le prouver.
Lemme : $91 \in \mathcal{P}$.
Démo :

$$\mathcal{P} \cap [\![2; \sqrt{91}]\!] = \{2; 3; 5; 7\}$$

Or on a :

$$91 = 2 \times 45 + 1, 91 = 3 \times 30 + 1, 91 = 5 \times 18 + 1, 91 = 7 \times 13$$

On en déduit donc que :

$$9100 = 2^2 \times 5^2 \times 7 \times 13$$

De même on a :

$$1848 = 2^3 \times 3 \times 7 \times 11$$

On en déduit donc que :

$$9100 \wedge 1848 = 2^2 \times 7 = 28$$

De même on a :

$$9100 \vee 1848 = 2^3 \times 3 \times 5^2 \times 7 \times 11 \times 13 = 600600$$

Exercice B.2 : Soit $n \in \mathbb{N}^*$. Calculer $(n^3 + 2n) \wedge (n^4 + 3n^2 + 1)$ et $(n^3 + 2n) \vee (n^4 + 3n^2 + 1)$

On effectue la division euclidienne de $n^4 + 3n^2 + 1$ par $n^3 + 2n$:

$$n^4 + 3n^2 + 1 = n(n^3 + 2n) + n^2 + 1$$
$$n^3 + 2n = n(n^2 + 1) + n$$
$$n^2 + 1 = n \times n + 1$$

On en déduit donc que :

$$\forall n \in \mathbb{N}^*, (n^3 + 2n) \wedge (n^4 + 3n^2 + 1) = 1$$

Or on sait que :

$$[(n^3 + 2n) \wedge (n^4 + 3n^2 + 1)] \times [(n^3 + 2n) \vee (n^4 + 3n^2 + 1)] = (n^3 + 2n) \times (n^4 + 3n^2 + 1)$$

On en déduit donc que :

$$(n^3 + 2n) \vee (n^4 + 3n^2 + 1) = (n^3 + 2n) \times (n^4 + 3n^2 + 1)$$

Exercice B.3 : a) Déterminer les entiers $n \in \mathbb{N}^*$ tels que s on divise 4373 et 826 par n, on obtient respectivement 8 et 7 pour restes.
b) Déterminer les entiers $n \in \mathbb{N}^*$ tels que s on divise 6381 et 3954 par n, on obtient respectivement 9 et 6 pour restes.

a) Il suffit de poser le système obtenu :

$$\begin{cases} 4373 = q_1 \times n + 8 \\ 826 = q_2 \times n + 7 \end{cases}$$

On en déduit donc que :

$$(q_1 - q_2)n + 1 = 3547 \Longrightarrow n|3546$$

Or on sait que :

$$3546 = 2 \times 3^2 \times 197$$

On en déduit que 3546 admet 12 diviseurs :

$$\mathcal{D}^+_{3546} = \{1,2,3,6,9,18,197,394,591,1182,1773,3546\}$$

On sait de plus que $n \geq 9$ car le reste de la division euclidienne de 4373 par n est 8.
De plus on sait que $n < 826$.
Il nous reste alors 5 choix.
On vérifie l'un après l'autre et on trouve que $n = 9$.

Remarque : On peut faire un programme Python pour résoudre cet exercice :

```
a=[]
for n in range(9,414):
    if (4373%n==8) and (826%n==7):
        a.append(n)
print(a)
```

```
DM 1 Toussaint.py × module1
Console Python
*** Python 3.4.5 |Continuum Analytics, Inc.| (default, Jul
 win32. ***
>>>
*** Console de processus distant Réinitialisée ***
>>>
[9]
```

b) On utilise le même principe et on trouve $n = 12$.

Remarque : On peut faire un programme Python pour résoudre cet exercice :

```
a=[]
for n in range(9,1978):
    if (6381%n==9) and (3954%n==6):
        a.append(n)
print(a)
```

```
DM 1 Toussaint.py × module1
Console Python
*** Python 3.4.5 |Continuum Analytics, Inc.| (default, Jul  5 2016,
 win32. ***
>>>
*** Console de processus distant Réinitialisée ***
>>>
[12]
```

Exercice B.4 : On considère trois entiers naturels n,p ,q avec $n \geq 2$ et $q > 0$.
1) On écrit la division euclidienne de p par q sous la forme $p = aq + r$. Montrer que la division euclidienne de $n^p - 1$ par $n^q - 1$ est :

$$n^p - 1 = \left(\sum_{k=0}^{a-1} n^{kq+r}\right)(n^q - 1) + (n^r - 1)$$

2) En déduire $(n^p - 1) \wedge (n^q - 1)$ en fonction de n et $p \wedge q$.

1) On sait que :

$$\sum_{k=0}^{a-1} n^{kq+r} = n^r \sum_{k=0}^{a-1} (n^q)^k = n^r \times \frac{(n^q)^a - 1}{n^q - 1} \text{ car } n^q \neq 1$$

On en déduit donc que :

$$\left(\sum_{k=0}^{a-1} n^{kq+r}\right)(n^q - 1) + (n^r - 1) = n^r(n^q)^a - n^r + n^r - 1 = n^{aq+r} - 1 = n^p - 1$$

De plus on sait que :

$$0 \leq r < q \Rightarrow 1 \leq n^r \leq n^q \Rightarrow 0 \leq n^r - 1 \leq n^q - 1$$

On en déduit donc que la division euclidienne de $n^p - 1$ par $n^q - 1$ est :

$$n^p - 1 = \left(\sum_{k=0}^{a-1} n^{kq+r}\right)(n^q - 1) + (n^r - 1)$$

b) On pose la succession de division euclidienne suivante, en exécutant l'algorithme d'Euclide :

$$\begin{cases} p = a_1 q + r_1 \\ q = a_2 r_1 + r_2 \\ r_1 = a_3 r_2 + r_3 \\ \vdots \\ r_{n-2} = a_n r_{n-1} + r_n \\ r_{n-1} = a_{n+1} r_n + 0 \end{cases}$$

D'après ce que l'on sait de l'algorithme d'Euclide on a :

$$p \wedge q = r_n$$

De plus on sait que :

$$\begin{cases} n^p - 1 = b_1(n^q - 1) + n^{r_1} - 1 \\ n^q - 1 = b_2(n^{r_1} - 1) + n^{r_2} - 1 \\ n^{r_1} - 1 = b_3(n^{r_2} - 1) + n^{r_3} - 1 \\ \vdots \\ n^{r_{n-2}} - 1 = b_n(n^{r_{n-1}} - 1) + n^{r_n} - 1 \\ n^{r_{n-1}} - 1 = b_{n+1}(n^{r_n} - 1) + 0 \end{cases}$$

On en déduit donc que :

$$(n^p - 1) \wedge (n^q - 1) = n^{r_n} - 1 = n^{p \wedge q} - 1$$

Exercice B.5 : 1) Montrer que pour tout $(a, b) \in \mathbb{N}^2$, pour tout $\lambda \in \mathbb{N}$, $(\lambda a) \wedge (\lambda b) = \lambda(a \wedge b)$.
2) En déduire que pour tout $(a, b) \in \mathbb{N}^2$, pour tout $\lambda \in \mathbb{N}$, $(\lambda a) \vee (\lambda b) = \lambda(a \vee b)$

1) On peut le voir de deux façons. Soit par l'algorithme d'Euclide, soit par la décomposition en nombre premier de a et b. La deuxième façon est plus rapide car cela nous donne aussi le PPCM :
On pose :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \quad \text{et} \quad b = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

On a alors :

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\alpha_p; \beta_p)}$$

De plus on sait que :

$$\lambda a = \prod_{p \in \mathcal{P}} p^{\lambda_p} \prod_{p \in \mathcal{P}} p^{\alpha_p} = \prod_{p \in \mathcal{P}} p^{(\alpha_p + \lambda_p)} \quad \text{et} \quad \lambda b = \prod_{p \in \mathcal{P}} p^{\lambda_p} \prod_{p \in \mathcal{P}} p^{\beta_p} = \prod_{p \in \mathcal{P}} p^{(\beta_p + \lambda_p)}$$

On en déduit donc que :

$$(\lambda a) \wedge (\lambda b) = \prod_{p \in \mathcal{P}} p^{\min(\alpha_p + \lambda_p; \beta_p + \lambda_p)} = \prod_{p \in \mathcal{P}} p^{\min(\alpha_p; \beta_p)} p^{\lambda_p} = \prod_{p \in \mathcal{P}} p^{\lambda_p} \prod_{p \in \mathcal{P}} p^{\min(\alpha_p; \beta_p)} = \lambda(a \wedge b)$$

2) On sait de plus que :

$$\big((\lambda a) \vee (\lambda b)\big) \times \big((\lambda a) \wedge (\lambda b)\big) = \lambda^2 ab$$
$$\Rightarrow \big((\lambda a) \vee (\lambda b)\big) \times \lambda(a \wedge b) = \lambda^2 (a \vee b) \times (a \wedge b)$$
$$\Rightarrow (\lambda a) \vee (\lambda b) = \lambda(a \vee b)$$

Exercice B.6 : Chercher les couples d'entiers (a, b) tels que :

$$\begin{cases} a \wedge b = 42 \\ a \vee b = 1680 \end{cases}$$

On sait que $42 = 2 \times 3 \times 7$ et $1680 = 2^4 \times 3 \times 5 \times 7$.
De plus on sait que :

$$a \wedge b = 42 \Leftrightarrow \exists (a', b') \in \mathbb{Z}^2 \begin{cases} a = 42a' \\ b = 42b' \\ a' \wedge b' = 1 \end{cases}$$

On en déduit donc que :

$$\begin{cases} a \wedge b = 42 \\ a \vee b = 1680 \end{cases} \Leftrightarrow \begin{cases} \begin{cases} a = 2 \times 3 \times 7 = 42 \\ b = 2 \times 3 \times 7 \times \mathbf{2^3} \times \mathbf{5} = 1680 \end{cases} \\ \text{ou} \\ \begin{cases} a = 2 \times 3 \times 7 \times \mathbf{5} = 210 \\ b = 2 \times 3 \times 7 \times \mathbf{2^3} = 336 \end{cases} \\ \text{ou} \\ \begin{cases} a = 2 \times 3 \times 7 \times \mathbf{2^3} = 336 \\ b = 2 \times 3 \times 7 \times \mathbf{5} = 210 \end{cases} \\ \text{ou} \\ \begin{cases} a = 2 \times 3 \times 7 \times \mathbf{2^3} \times \mathbf{5} = 1680 \\ b = a = 2 \times 3 \times 7 = 42 \end{cases} \end{cases}$$

Exercice B.7 : Déterminer les entiers b naturels non nuls tels que $28 \vee b = 140$

On sait que $140 = 28 \times 5$.
On sait de plus que $28 = 2^2 \times 7$.
On en déduit donc que :
$b = 5$ ou $b = 2 \times 5 = 10$ ou $b = 2^2 \times 5 = 20$ ou $b = 7 \times 5 = 35$ ou $b = 2 \times 7 \times 5 = 70$ ou $b = 2^2 \times 5 \times 7 = 140$
On a donc :

$$\{b \in \mathbb{N}, 28 \vee b = 140\} = \{5; 10; 20; 35; 70; 140\}$$

Partie C : Nombres premiers

Exercice C.1 : Soit $(a, n) \in (\mathbb{N}^*)^2$, soit p un nombre premier. Montrer que :

$$p | a^n \Longrightarrow p^n | a^n$$

Pour tout $a \in \mathbb{N}^*, a \geq 2$ on a :

$$a = \prod_{p \in \mathcal{P}} p^{a_p}, a_p \in \mathbb{N}, \forall p \in \mathcal{P}$$

On peut aussi écrire :

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \text{avec } \alpha_i \in \mathbb{N}^*$$

On a alors:

$$\forall n \in \mathbb{N}^*, a^n = \left(p_1^{\alpha_1} \dots p_k^{\alpha_k}\right)^n = p_1^{n\alpha_1} \dots p_k^{n\alpha_k} = (p_1^n)^{\alpha_1} \dots (p_k^n)^{\alpha_k}$$

On a donc :

$$p | a^n \Longrightarrow \exists i \in [\![1; k]\!], p_i = p \Longrightarrow p^n | a^n$$

Exercice C.2 : Soit $(a, b, c, k) \in (\mathbb{N}^*)^4$. Montrer que :

$$\begin{cases} ab = c^k \\ a \wedge b = 1 \end{cases} \Longrightarrow \exists (\alpha, \beta) \in (\mathbb{N}^*)^2, \text{tels que } \begin{cases} a = \alpha^k \\ b = \beta^k \end{cases}$$

On pose :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p}, b = \prod_{p \in \mathcal{P}} p^{\beta_p}, c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

On en déduit donc que :

$$ab = c^k = \left(\prod_{p\in\mathcal{P}} p^{\gamma_p}\right)^k = \prod_{p\in\mathcal{P}} p^{k\gamma_p}$$

De plus on sait que :

$$ab = \prod_{p\in\mathcal{P}} p^{(\alpha_p+\beta_p)}$$

Par unicité de la décomposition en nombre premier, on en déduit donc que :

$$\forall p \in \mathcal{P}, \alpha_p + \beta_p = k\gamma_p$$

De plus on sait que $a \wedge b = 1 \Longrightarrow \min(\alpha_p, \beta_p) = 0$

On en déduit donc que :

$$\forall p \in \mathcal{P}, \alpha_p + \beta_p = \begin{cases} \alpha_p \\ ou \\ \beta_p \end{cases}$$

On pose :

$$\mathcal{P}_1 = \{p \in \mathcal{P}, \alpha_p > 0\} \text{ et } \mathcal{P}_2 = \{p \in \mathcal{P}, \beta_p > 0\}$$

On a alors :

$$a = \prod_{p\in\mathcal{P}_1} p^{\alpha_p} \text{ et } b = \prod_{p\in\mathcal{P}_2} p^{\beta_p}$$

De plus comme $a \wedge b = 1$, on a $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$.

De plus on sait que :

$$\alpha_p + \beta_p = \begin{cases} \alpha_p \text{ si } p \in \mathcal{P}_1 \\ \beta_p \text{ si } p \in \mathcal{P}_2 \\ 0 \text{ sinon} \end{cases}$$

On en déduit donc que :

$$\forall p \in \mathcal{P}_1, \alpha_p = k\gamma_p$$
$$\forall p \in \mathcal{P}_2, \beta_p = k\gamma_p$$

On en déduit donc que :

$$a = \prod_{p\in\mathcal{P}_1} p^{k\gamma_p} = \left(\prod_{p\in\mathcal{P}_1} p^{\gamma_p}\right)^k = \alpha^k$$

De même on a :

$$b = \prod_{p\in\mathcal{P}_2} p^{k\gamma_p} = \left(\prod_{p\in\mathcal{P}_2} p^{\gamma_p}\right)^k = \beta^k$$

On a bien :

$$\begin{cases} ab = c^k \\ a \wedge b = 1 \end{cases} \Longrightarrow \exists(\alpha, \beta) \in (\mathbb{N}^*)^2, \text{tels que } \begin{cases} a = \alpha^k \\ b = \beta^k \end{cases}$$

Exercice C.3 (petit théorème de Fermat) : Soit p un nombre premier.

1) Montrer que :

$$\forall p \in \mathcal{P}, \forall k \in [\![1; p-1]\!], p \left|\binom{p}{k}\right.$$

2) En déduire que :

$$\forall n \in \mathbb{Z}, p|(n^p - n)$$

3) a) Montrer que :

$$\forall n \in \mathbb{Z}, 42|(n^7 - n)$$

b) Montrer que :

$$\forall n \in \mathbb{Z}, \frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$$

1) On sait que :

$$\forall p \in \mathcal{P}, \forall k \in [\![1; p-1]\!], \binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$
$$\Longrightarrow k! \times \binom{p}{k} = p \times (p-1) \times \ldots \times (p-k+1)$$
$$\Longrightarrow \exists k_p \in \mathbb{Z}, k! \times \binom{p}{k} = p \times k_p$$
$$\Longrightarrow p \mid k! \times \binom{p}{k}$$

De plus on écrit la décomposition en facteur premier de $k \in [\![1; p-1]\!]$:

$$\forall k \in [\![1; p-1]\!], k = \prod_{\substack{q \in \mathcal{P} \\ q<p}} q^{k_q}$$

On en déduit donc que :

$$\forall k \in [\![1; p-1]\!], k! = \prod_{i=1}^{k} i = \prod_{i=1}^{k} \prod_{\substack{q \in \mathcal{P} \\ q<p}} q^{i_q}$$

On en déduit que p n'apparait pas dans la décomposition en facteur premier de k!, car cette décomposition est unique.

Or p apparait dans la décomposition en facteur premier de $k! \times \binom{p}{k}$.

On en déduit donc que p apparait dans la décomposition en facteur premier de $\binom{p}{k}$.

On en déduit donc que $p \mid \binom{p}{k}$.

2) **1er cas : $n \in \mathbb{N}$**

On va démontrer cette propriété par récurrence. On pose :

$$\forall n \in \mathbb{N}, \mathcal{P}(n): "p \mid (n^p - n)"$$

Initialisation : n=0

On sait que $0^p - 0 = 0$ et $p \mid 0$

Donc $\mathcal{P}(0)$ est vraie.

Hérédité : Soit n un entier naturel n fixé. On suppose que $p \mid n^p - n$

On sait que :

$$(n+1)^p - (n+1) = \sum_{k=0}^{p} \binom{p}{k} n^k - n - 1 = n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^k$$

Or d'après ce que l'on a démontré au 1), on sait que $p \mid \binom{p}{k}$, pour tout $k \in [\![1, p-1]\!]$.De plus d'après l'hypothèse de récurrence, on sait que $p \mid (n^p - n)$. On en déduit donc que $p \mid \big((n+1)^p - (n+1)\big)$.

Conclusion : $\mathcal{P}(0)$ est vraie et $\mathcal{P}(n)$ est héréditaire donc d'après le principe de récurrence, $\mathcal{P}(n)$ est vraie pour tout entier naturel n.

2ième cas : $n \in \mathbb{Z}^-$

On sait que $-n \in \mathbb{Z}$. Si $p > 2$.

On a alors :

$$p \mid (-n)^p - (-n) \Longrightarrow p \mid -n^p + n \Longrightarrow p \mid n^p - n$$

Si $p = 2$. On a alors :

$$n^2 - n = n(n-1)$$

Or n et n-1 sont deux entiers consécutifs donc l'un des deux est pair. Donc 2 divise $n(n-1)$

3) a) Comme $7 \in \mathcal{P}$, on sait d'après la proposition précédente que :

$$\forall n \in \mathbb{Z}, 7 \mid (n^7 - n)$$

De plus on sait :

$$n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n-1)(n^2 + n + 1)(n+1)(n^2 - n + 1)$$

Or on sait que $n(n-1)(n+1)$ est divise par 2 et par 3 car n et n-1 sont deux entiers consécutifs donc l'un des deux est pair, et n, n-1 et n+1 sont trois entiers consécutifs donc l'un des trois est divisible par 3.

On en déduit donc que 2, 3 et 7 apparaissent dans la décomposition en facteur premier de $n^7 - n$. Comme cette décomposition est unique, on en déduit donc que :

$$2 \times 3 \times 7 = 42 | n^7 - n$$

b) On sait que 5 et 7 sont premiers, donc d'parès le petit théorème de fermat, on a :

$$7 | n^7 - n \text{ et } 5 | n^5 - n$$

On en déduit donc que :

$$7 | 5(n^7 - n) \text{ et } 5 | 5(n^7 - n)$$

Donc 7 et 5 apparaissent dans la décomposition en facteur premier de $n^7 - n$. Donc $35 | 5(n^7 - n)$.
De même on a $35 | 7(n^5 - n)$.
Ainsi 35 divise toute combinaison linéaire de $7(n^5 - n)$ et $5(n^7 - n)$. On en déduit donc que :

$$35 | 7(n^5 - n) + 5(n^7 - n) + 35n$$

On en déduit donc que $35 | 7n^5 + 5n^7 + 23n$.
On en déduit donc que :

$$\forall n \in \mathbb{Z}, \frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$$

Exercice C.4 : On suppose qu'il existe un nombre fini d'entiers premiers de la forme $4n - 1$ où $n \geq 1$. On les note $p_1, \dots, p_N$ et on forme le nombre $4p_1 \times \dots \times p_N - 1$. Montrer que ce nombre admet nécessairement un diviseur premier de la forme $4n - 1$, et en déduire une contradiction. Conclure.

Le nombre $A = 4p_1 \times \dots \times p_N - 1$ est impair. Ainsi ses diviseurs premiers sont tous impairs, donc de la forme $4n - 1$ ou $4n + 1$.
On va raisonner par l'absurde. On suppose que tous les diviseurs premiers de A sont de la forme $4n + 1$:

$$\forall p \in \mathcal{P} \cap \mathcal{D}_A, \exists n_p \in \mathbb{N}, p = 4n_p + 1$$

On a alors :

$$A = \prod_{p|A} p^{\alpha_p} = \prod_{p|A} (4n_p + 1)^{\alpha_p}$$

On va ensuite montrer par récurrence que :

$$\forall (k_1, \dots, k_n) \in \mathbb{Z}^n, \prod_{i=1}^{n} (4k_i + 1) = 4k + 1, k \in \mathbb{Z}$$

Initialisation : $n = 1$. C'est trivial.
Hérédité : Soit n un entier naturel n fixé non nul. On suppose que

$$\forall (k_1, \dots, k_n) \in \mathbb{Z}^n, \prod_{i=1}^{n} (4k_i + 1) = 4k + 1, k \in \mathbb{Z}$$

On a alors :

$$\forall (k_1, \dots, k_n, k_{n+1}) \in \mathbb{Z}^{n+1}, \prod_{i=1}^{n+1} (4k_i + 1) = (4k_{n+1} + 1) \prod_{i=1}^{n} (4k_i + 1)$$
$$= (4k_{n+1} + 1)(4k + 1)$$
$$= 4(4k \times k_{n+1} + k_{n+1} + k) + 1$$
$$= 4k' + 1, k' \in \mathbb{Z}$$

Donc la proposition est héréditaire.
Conclusion : On conclut avec le principe de récurrence.
On en déduit donc que si on a :

$$\forall p \in \mathcal{P} \cap \mathcal{D}_A, \exists n_p \in \mathbb{N}, p = 4n_p + 1$$

Alors A est de la forme $4k + 1$. Or on sait que $A = 4p_1 \times \dots \times p_N - 1$.
On a alors :

$$4p_1 \times \dots \times p_N - 1 = 4k + 1 \Longrightarrow 4(p_1 \times \dots \times p_N - k) = 2$$

ce qui conduit à une contradiction.
On en déduit donc que A admet un diviseur premier de la forme $4n - 1$.
On en déduit donc que :

$$\exists i \in [\![1; N]\!], p_i | A$$

On en déduit donc que :

$$p_i | p_1 \times ... \times p_N \text{ et } p_i | A$$

Donc $p_i | 1$. Ce qui est absurde. Ainsi il existe une infinité de diviseurs premiers de la forme $4n - 1$.

Remarque : Il existe aussi une infinité de diviseurs premiers de la forme $4n + 1$.

Exercice C.5 : Soit $n \in \mathbb{N}^*, n = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers.
1) Calculer le nombre de diviseurs positifs de n.
2) Calculer la somme $S(n)$ des diviseurs positifs de n.
3) Montrer que si m et n sont premiers entre eux, alors $S(mn) = S(m)S(n)$.

1) On a vu dans le cours que :

$$\#\mathcal{D}_n^+ = (\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_r + 1) = \prod_{i=1}^{r} (\alpha_i + 1)$$

2) Cette question est compliquée si on essaie de la faire directement. On va la fragmenter.

1er cas : Si $n = p^\alpha$

On a alors :

$$S(n) = \sum_{d|n} d = \sum_{k=0}^{\alpha} p^k = \frac{p^{\alpha+1} - 1}{p - 1}$$

2ième cas : Si $n = p_1^\alpha \times p_2^\beta$

On sait que :

$$\mathcal{D}_n^+ = \left\{ d = p_1^{k_1} \times p_2^{k_2}, (k_1, k_2) \times [\![0, \alpha]\!] \times [\![0; \beta]\!] \right\}$$

On en déduit donc que :

$$S(n) = \sum_{d|n} d = \sum_{i=0}^{\beta} \sum_{k=0}^{\alpha} p_1^k \times p_2^i = \sum_{i=0}^{\beta} p_2^i \sum_{k=0}^{\alpha} p_1^k = \sum_{i=0}^{\beta} p_2^i \left(\frac{p_1^{\alpha+1} - 1}{p - 1} \right) = \left(\frac{p_1^{\alpha+1} - 1}{p_1 - 1} \right) \times \left(\frac{p_2^{\beta+1} - 1}{p_2 - 1} \right)$$

En généralisant le procédé ou en utilisant une récurrence, on obtient que :

$$n = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r} \Longrightarrow S(n) = \sum_{d|n} d = \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

3) Si m et n sont premiers entre eux alors on a :

$$m = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r} \text{ et } n = q_1^{\alpha'_1} \times ... \times q_{r'}^{\alpha'_{r'}} \text{ avec } q_i \neq p_j, \forall (i, j) \in [\![1, r']\!] \times [\![1, r]\!]$$

On en déduit donc la décomposition en facteur premier de $m \times n$:

$$mn = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r} \times q_1^{\alpha'_1} \times ... \times q_{r'}^{\alpha'_{r'}}$$

$$\Longrightarrow S(mn) = \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right) \times \prod_{i=1}^{r'} \left(\frac{q_i^{\alpha'_i+1} - 1}{q_i - 1} \right) = S(m) \times S(n)$$