4.6 Quelques exercices corrigés

Comme à chaque fois, tous les exercices du chapitre ne sont pas corrigés. Seuls ceux qui nous ont paru moins simples ou moins répétitifs le sont.

4.6.1 Sur les entiers premiers

Exercice 2 :

Soit $a \in \mathbb{N}$, non premier. Montrer que son plus petit diviseur positif b est tel que $b \leqslant \sqrt{a}$

On appelle donc b le plus petit diviseur positif de a.
Il existe alors $d \in \mathbb{N}$, diviseur de a tel que $a = db$ avec $d \geqslant b$. Donc, $db \geqslant b^2$, c'est à dire $a \geqslant b^2$, et en passant à la racine, nous obtenons :

$$\sqrt{a} \geqslant b \Longleftrightarrow b \leqslant \sqrt{a}$$

Exercice 3 :

Soit $A = 315$. Trouver le plus petit entier naturel k tel que $k \times A$ soit le carré d'un nombre entier.

Mon dieu, rien de bien compliqué ici.
On décompose 315 en un produit de facteurs premiers : $315 = 3^2 \times 5 \times 7$
En prenant $k = 5 \times 7$, nous avons $k \times 315 = 3^2 \times 5^2 \times 7^2$. Et c'est tout ! !

Exercice 4 :

Montrer que les nombres suivants sont composés :

1. $n^4 - 20n^2 + 4$ *pour* $n \in \mathbb{Z}$

   Il suffit de factoriser $n^4 - 20n^2 + 4$. Nous avons :

   $$n^4 - 20n^2 + 4 = \left(n^2 - 2\right)^2 + 4n^2 - 20n^2 = \left(n^2 - 2\right)^2 - 16n^2 = \left(n^2 - 2 - 4n\right)\left(n^2 - 2 + 4n\right)$$

   Comme $n^4 - 20n^2 + 4 = \left(n^2 - 4n - 2\right)\left(n^2 + 4n - 2\right)$, $n^4 - 20n^2 + 4$ est bien un nombre composé
2. $a^4 + 4b^4$ *pour* $a \in \mathbb{N}$, $b \in \mathbb{N}$ *et* $a \geqslant 2$ *et* $b \geqslant 2$

   On procède, ici, de la même manière :

   $$a^4 + 4b^4 = \left(a^2 + 2b^2\right)^2 - 4a^2b^2 = \left(a^2 + 2b^2 - 2ab\right)\left(a^2 + 2b^2 + 2ab\right)$$

   C'est donc bien un nombre composé

Exercice 5 :

Soit n un entier naturel tel que $n \geqslant 2$

1. *On considère les $(n-1)$ nombres : $n!+2,\ n!+3,\ \cdots, n!+(n-1),\ n!+n$ Démontrer que ces nombres ne sont pas premiers*

   C'est assez facile, puisque, en écrivant, pour $k = 2, \cdots, n$

   $$n! + k = k \times \left(\prod_{\substack{j=2 \\ j \neq k}}^{n} j + 1\right)$$

   montre que $n! + k$ est divisible par $k \geqslant 2$ et n'est donc pas premier.
2. *En déduire que l'on peut trouver une suite de k nombres consécutifs non premiers*

   Soit $k \geqslant 2$ entier.
   Alors, en utilisant la construction vue dans la question précédente, les entiers

   $$(k+1)!+2,\ (k+1)!+3,\ \cdots, (k+1)!+k,\ (k+1)!+k+1$$

   sont k entiers consécutifs non premiers

Exercice 6 :

1. *Déterminer les couples* $(x, y) \in \mathbb{Z}^2$ *tels que* $x^2 - y^2 = 1969$

   Nous allons aller pas à pas
   - ▷ Tout d'abord, nous décomposons 1969 en un produit de facteurs premiers :
   $$1969 = 11 \times 179$$
   - ▷ D'autre part, $x^2 - y^2 = (x-y)(x+y)$, c'est à dire que $x+y$ et $x-y$ apparaissent conmme des diviseurs de 1969
   - ▷ Nous avons alors plusieurs systèmes d'équations :

   $\star \begin{cases} x+y = & 1 \\ x-y = & 1969 \end{cases}$ $\star \begin{cases} x+y = & 1969 \\ x-y = & 1 \end{cases}$ $\star \begin{cases} x+y = & 11 \\ x-y = & 179 \end{cases}$ $\star \begin{cases} x+y = & 179 \\ x-y = & 11 \end{cases}$

   - Résolution de $\begin{cases} x+y = & 1 \\ x-y = & 1969 \end{cases}$
     En additionnant, nous obtenons $2x = 1970$, d'où $x = 985$ et $y = -984$
   - Résolution de $\begin{cases} x+y = & 1969 \\ x-y = & 1 \end{cases}$
     Toujours en additionnant, $x = 985$ et $y = 984$
   - Résolution de $\begin{cases} x+y = & 11 \\ x-y = & 179 \end{cases}$
     Donc $2x = 190$ et donc $x = 95$ d'où $y = -84$
   - Résolution de $\begin{cases} x+y = & 179 \\ x-y = & 11 \end{cases}$
     Nous avons toujours $x = 95$ et, cette fois ci, $y = 84$

   Il y a donc 4 couples (x, y) solutions de ce système :
   $$(985, -984) \quad (985, 984) \quad (95, -84) \quad (95, 84)$$

2. *Déterminer les couples* $(x, y) \in \mathbb{Z}^2$ *tels que* $9y^2 - (x+1)^2 = 32$

   Nous allons procéder de la même manière que la question précédente. Si D_{32} est l'ensemble des diviseurs de 32, de $32 = 2^5$, nous tirons : $D_{32} = \{1, 2, 4, 8, 16, 32\}$
   D'autre part, comme tout à l'heure, $9y^2 - (x+1)^2 = (3y+x+1)(3y-x-1)$. Nous avons donc plusieurs systèmes à résoudre :
   - ▷ Les deux premiers : $\begin{cases} 3y+x+1 = & 1 \\ 3y-x-1 = & 32 \end{cases}$ et $\begin{cases} 3y+x+1 = & 32 \\ 3y-x-1 = & 1 \end{cases}$
     Dans les 2 systèmes, lorsque nous additionnons les deux lignes, nous obtenons $6y = 33$, qui est impossible puisque 33 est un nombre impair, alors que $6y$ est un nombre pair.
   - ▷ Deux autres systèmes semblables $\begin{cases} 3y+x+1 = & 2 \\ 3y-x-1 = & 16 \end{cases}$ et $\begin{cases} 3y+x+1 = & 16 \\ 3y-x-1 = & 2 \end{cases}$
     Dans les deux systèmes, lorsque nous additionnons, nous trouvons $6y = 18$, d'où $y = 3$.
     En remplaçant y par sa valeur dans la première équation du premier système, nous obtenons : $9 + x + 1 = 2$, c'est à dire $x = -8$
     En faisant la même opération dans la première équation du second système, nous obtenons : $9 + x + 1 = 16$ c'est à dire $x = 6$
     Nous obtenons, ici, deux couples solutions $(-8, 3)$ et $(6, 3)$
   - ▷ Nous allons étudier les deux derniers systèmes $\begin{cases} 3y+x+1 = & 4 \\ 3y-x-1 = & 8 \end{cases}$ et $\begin{cases} 3y+x+1 = & 8 \\ 3y-x-1 = & 4 \end{cases}$
     Dans les deux systèmes, lorsque nous additionnons, nous trouvons $6y = 12$, d'où $y = 2$.
     En remplaçant y par sa valeur dans la première équation du premier système, nous obtenons : $6 + x + 1 = 4$, c'est à dire $x = -3$
     En faisant la même opération dans la première équation du second système, nous obtenons : $6 + x + 1 = 8$ c'est à dire $x = 1$
     Nous obtenons, ici, deux couples solutions $(-3, 2)$ et $(1, 2)$

   Il y a donc 4 couples (x, y) solutions de ce système :
   $$(-8, 3) \quad (6, 3) \quad (-3, 2) \quad (1, 2)$$

Exercice 8 :

Montrer qu'il existe une infinité de nombres premiers de la forme $6p+5$

Supposons qu'il n'y en ait qu'un nombre fini de nombres premiers du type $6p+5$, et soit $6n+5$ le dernier. Les nombres premiers ne peuvent être que de la forme $6p+1$ ou $6p+5$, puisque les autres nombres qui sont tous de la forme $6p$, $6p+2$, $6p+3$ $6p+4$ admettent tous un diviseur propre et ne sont donc pas premiers.

Soient $A = \prod_{k=0}^{n}(6k+5)$ et $B = 6A+5$

Ce nombre B est congru à 5, modulo 6, et n'est en aucun cas divisible par un entier premier du type $6k+5$, donc B n'est divisible que par des entiers premiers du type $6k+1$, c'est à dire que B est congru à 1 modulo 6.

Contradiction. Donc, il existe une infinité de nombres premiers de la forme $6p+5$

Exercice 9 :

Montrer que si p est un nombre premier supérieur à 4, alors $p^2 \equiv 1\,[6]$

Cet exercice fait référence à l'exercice précédent. Modulo 6, les nombres premiers ne peuvent qu'être du type $6p+1$ ou $6p-1$. Donc, si $n \equiv 1\,[6] \Longleftrightarrow n = 6p+1$, alors $n^2 \equiv 1\,[6]$ ou si $n \equiv -1 \equiv 5\,[6] \Longleftrightarrow n = 6p+5$, alors $n^2 \equiv 1\,[6]$.

Ce que nous voulions.

Exercice 10 :

Soit $x = a^m b^n c^p$, où a, b et c sont 3 nombres premiers

1. *De quelle forme sont les diviseurs de x ?*

   Il est parfaitement clair qu'un diviseur de x est de la forme $x = a^i \times b^j \times c^k$ où $0 \leqslant i \leqslant m$, $0 \leqslant j \leqslant n$ et $0 \leqslant k \leqslant p$

2. *Soient $n_0 \leqslant n$ et $p_0 \leqslant p$ fixés ; calculez $\sum_{k=0}^{m} a^k b^{n_0} c^{p_0}$*

   Voilà qui n'est pas très difficile :

$$\begin{aligned}\sum_{k=0}^{m} a^k b^{n_0} c^{p_0} &= b^{n_0} c^{p_0} \sum_{k=0}^{m} a^k \\ &= b^{n_0} c^{p_0} \frac{1-a^{m+1}}{1-a}\end{aligned}$$

3. *En déduire la somme des diviseurs de x*

La somme des diviseurs est donnée par :

$$\begin{aligned}
\sum_{k=0}^{p}\left(\sum_{j=0}^{n}\left(\sum_{i=0}^{m}a^kb^jc^k\right)\right) &= \sum_{k=0}^{p}\left(\sum_{j=0}^{n}b^jc^k\left(\sum_{i=0}^{m}a^k\right)\right)\\
&= \sum_{k=0}^{p}\left(\sum_{j=0}^{n}b^jc^k\left(\frac{1-a^{m+1}}{1-a}\right)\right)\\
&= \left(\frac{1-a^{m+1}}{1-a}\right)\sum_{k=0}^{p}\left(\sum_{j=0}^{n}b^jc^k\right)\\
&= \left(\frac{1-a^{m+1}}{1-a}\right)\sum_{k=0}^{p}c^k\left(\sum_{j=0}^{n}b^j\right)\\
&= \left(\frac{1-a^{m+1}}{1-a}\right)\sum_{k=0}^{p}c^k\left(\frac{1-b^{m+1}}{1-b}\right)\\
&= \left(\frac{1-a^{m+1}}{1-a}\right)\left(\frac{1-b^{m+1}}{1-b}\right)\sum_{k=0}^{p}c^k\\
&= \left(\frac{1-a^{m+1}}{1-a}\right)\left(\frac{1-b^{n+1}}{1-b}\right)\left(\frac{1-c^{p+1}}{1-c}\right)
\end{aligned}$$

La somme des diviseurs de $x=a^mb^nc^p$, où a, b et c sont 3 nombres premiers est donc donnée par

$$\left(\frac{1-a^{m+1}}{1-a}\right)\left(\frac{1-b^{n+1}}{1-b}\right)\left(\frac{1-c^{p+1}}{1-c}\right)$$

Par exemple : $30=2\times3\times5$. La somme des diviseurs est donc donnée par :

$$\left(\frac{1-2^2}{1-2}\right)\left(\frac{1-3^2}{1-3}\right)\left(\frac{1-5^2}{1-5}\right)=\frac{-3}{-1}\times\frac{-8}{-2}\times\frac{-24}{-4}=3\times4\times6=72$$

Exercice 11 :

En étudiant les congruences modulo 3, montrer que si p et $2p-1$ sont premiers, alors, $2p+1$ est composé

C'est un exercice un peu....spécieux, plus ou moins intéressant.
Soit $p\in\mathbb{N}$ tel que p soit un nombre premier.
Alors, modulo 3, nous n'avons que 2 possibilités : $p\equiv1\,[3]$ ou $p\equiv2\,[3]$

- Si $p\equiv2\,[3]$, alors $2p-1\equiv0\,[3]$ et $2p-1$, n'est sûrement pas premier. Donc, ce cas ne nous intéresse pas.
- Si $p\equiv1\,[3]$, alors $2p-1\equiv1\,[3]$ et $2p-1$, est peut-être premier. Donc, $2p+1\equiv0\,[3]$ et $2p+1$ est sûrement un nombre composé.

Nous avons donc répondu à la question.

4.6.2 Exercices sur le pgcd

Exercice 13 :

a, b, c et d sont 4 entiers naturels non nuls tels que $ab-dc=1$

1. *Démontrer que cette relation est équivalente à $a(b+d)-d(c+a)=1$*

   Point très difficile : il suffit d'écrire :

   $$ab-dc=ab+ad-ad-dc=a(b+d)-d(c+a)$$

2. *En déduire que les fractions $\frac{a}{a+c}$, $\frac{d}{b+d}$ et $\frac{a+c}{b+d}$ sont irréductibles*

   En utilisant $a(b+d)-d(c+a)=1$ et le théorème de Bachet, nous voyons que :

- ⋆ Les nombres a et $b+d$ sont premiers entre eux, qu'ils n'ont pas de diviseurs commens et que donc la fraction $\dfrac{a}{a+c}$ n'est pas simplifiable et est donc irréductible.
- ⋆ Le même raisonnement vaut pour les fractions $\dfrac{d}{b+d}$ et $\dfrac{a+c}{b+d}$

Exercice 14 :

1. *Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, si $\operatorname{pgcd}(a,c)=1$, alors $\operatorname{pgcd}(a,b)=\operatorname{pgcd}(a,bc)$*

   Soient $D_{a,b}$ l'ensemble des diviseurs communs à a et b, $D_{a,bc}$ l'ensemble des diviseurs communs à a et bc. Nous allons montrer que si a et c sont premiers entre eux, alors $D_{a,b}=D_{a,bc}$
   — Premièrement, $D_{a,b} \subset D_{a,bc}$
   En effet, soit $x \in D_{a,b}$; alors, il existe k_1 et k_2 tels que $a=k_1x$ et $b=k_2x$.
   Donc $bc=k_2xc=(k_2c)x$, et x divise donc bc, donc $x \in D_{a,bc}$
   — Secondement, démontrons que $D_{a,bc} \subset D_{a,b}$
   Soit $x \in D_{a,bc}$; alors, il existe k_1 et k_2 tels que $a=k_1x$ et $bc=k_2x$.
   Or, a et c sont premiers entre eux, et d'après le théorème de Bachet, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au+cv=1$.
   Donc,

   - $a=k_1x \iff bua=buk_1x$
   - $bc=k_2x \iff bvc=vk_2x$

   En additionnant, nous obtenons :

   $$bua+bvc=vk_2x+buk_1x \iff b(ua+cv)=(vk_2+buk_1)x \iff b=(vk_2+buk_1)x$$

   C'est à dire que x divise b et donc $x \in D_{a,b}$
   Nous en déduisons que $D_{a,b}=D_{a,bc}$, et qu'en particulier, nous avons $\operatorname{pgcd}(a,b)=\operatorname{pgcd}(a,bc)$
2. *Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, nous avons :*

   $$\operatorname{pgcd}(a,c)=1 \text{ et } \operatorname{pgcd}(a,b)=1 \text{ équivalent à } \operatorname{pgcd}(a,bc)=1$$

   Nous allons utiliser l'identité de Bachet-Bezout de la proposition 4.2.7
   (a) Supposons que $\operatorname{pgcd}(a,c)=1$ et $\operatorname{pgcd}(a,b)=1$
   Alors, il existe $u \in \mathbb{Z}$, $v \in \mathbb{Z}$, $s \in \mathbb{Z}$ et $t \in \mathbb{Z}$ tels que $au+bv=1$ et $sa+tc=1$. En faisant le produit, nous obtenons :

   $$(au+bv)(sa+tc)=1 \iff a(sau+tcu+sbv)+(tv)bc=1$$

   Ce qui montre donc que $\operatorname{pgcd}(a,bc)=1$
   (b) Réciproquement, supposons que $\operatorname{pgcd}(a,bc)=1$
   Alors, il existe $u \in \mathbb{Z}$, $v \in \mathbb{Z}$ tels que $ua+v(bc)=1$. Or :
   — $ua+v(bc)=1 \Longrightarrow ua+(vb)c=1$, c'est à dire $\operatorname{pgcd}(a,c)=1$
   — $ua+v(bc)=1 \Longrightarrow ua+(vc)b=1$, c'est à dire $\operatorname{pgcd}(a,b)=1$
   Nous avons bien démontré l'équivalence.
3. *Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, nous avons l'équivalence suivante :*

   $$\operatorname{pgcd}(a,b)=1 \Leftrightarrow \operatorname{pgcd}(ab,a+b)=1$$

   Nous allons utiliser le théorème de Bachet-Bezout 4.2.7 qui est une équivalence ; nous avons :

   $$\operatorname{pgcd}(ab,a+b)=1 \iff \text{ il existe } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z} \text{ tels que } u(ab)+v(a+b)=1$$

   Or,

   $$u(ab)+v(a+b)=1 \iff a(ub+v)+bv=1 \iff aU_0+bV_0=1 \iff \operatorname{pgcd}(a,b)=1$$

   Ce que nous voulions

Exercice 15 :

Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, si $\text{pgcd}(a,b) = 1$ et si $a \mid c$ et $b \mid c$ alors $ab \mid c$

Ré-écrivons les hypothèses :

— Si $a \mid c$, il existe alors $k \in \mathbb{Z}$ tel que $c = ka$
— Si $b \mid c$, il existe alors $k_1 \in \mathbb{Z}$ tel que $c = k_1 b$
— Si $\text{pgcd}(a,b) = 1$, alors il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $ua + bv = 1$ *(cf 4.2.7)*

Clairement, nous avons :

$$ua + bv = 1 \Longleftrightarrow c(ua+bv) = c \Longleftrightarrow uac + bvc = c \Longleftrightarrow uak_1b + bvka = c \Longleftrightarrow ab(uk_1 + vk) = c$$

Ce qui montre bien que ab divise c

Exercice 16 :

Montrer que pour tout $n \in \mathbb{N}^*$ nous avons :

1. $(n^2 + n) \wedge (2n+1) = 1$
   — On montre d'abord que $(2n+1) \wedge (n+1) = 1$
   Rien de plus facile ; en utilisant Bachet-Bezout :
   $$2 \times (n+1) - (2n+1) = 1$$
   Et nous avons le résultat !
   — Il est tout aussi facile de montrer que $(2n+1) \wedge n = 1$
   — En utilisant le produit, nous avons :
   $$((2n+1) \wedge (n+1) = 1) \text{ et } ((2n+1) \wedge n = 1) \Longrightarrow (n(n+1) \wedge (2n+1) = 1)$$
2. $(3n^2 + 2n) \wedge (n+1) = 1$
   La démonstration est tout aussi simple :
   — On montre que $n \wedge (n+1) = 1$ par Bachet Bezout
   — Puis que $(3n+2) \wedge (n+1) = 1$, toujours par Bachet-Bezout
   — Et nous concluons en utilisant le produit
3. $(2^n + 3^n) \wedge (3^{n+1} + 2^{n+1}) = 1$
   Soit d un diviseur commun à $(2^n + 3^n)$ et $(3^{n+1} + 2^{n+1})$. Alors $(2^n + 3^n) = kd$ et $(3^{n+1} + 2^{n+1}) = k_1 d$
   ⋆ $(2^n + 3^n) - 3 \times (3^{n+1} + 2^{n+1}) = -2^n$ et donc $kd - 3k_1 d = -2^n \Longleftrightarrow d(k - 3k_1) = -2^n$, ce qui montre que $d \mid 2^n$
   ⋆ De même, $(3^{n+1} + 2^{n+1}) - 2 \times (2^n + 3^n) = 3^n$ et donc $k_1 d - 2kd = 3^n \Longleftrightarrow d(k_1 - 3k) = 3^n$, ce qui montre que $d \mid 3^n$

Or, $\text{pgcd}(2^n, 3^n) = 1$ et donc $d = 1$

Exercice 17 :

Trouver les nombres entiers naturels tels que :

$$\begin{cases} a + b = 182 \\ \text{pgcd}(a,b) = 13 \end{cases}$$

Remarquons tout d'abord que $182 = 2 \times 7 \times 13$ et que $a = 13a'$ et $b = 13b'$ avec $\text{pgcd}(a', b') = 1$.
Nous avons donc :

$$\begin{cases} 13a' + 13b' = 14 \times 13 \\ \text{pgcd}(a', b') = 1 \end{cases} \Longleftrightarrow \begin{cases} a' + b' = 14 \\ \text{pgcd}(a', b') = 1 \end{cases}$$

Nous trouvons donc comme couples :

— $a' = 1$ et $b' = 13$, c'est à dire $a = 13$ et $b = 169$
— $a' = 3$ et $b' = 11$, c'est à dire $a = 39$ et $b = 143$
— $a' = 5$ et $b' = 9$, c'est à dire $a = 65$ et $b = 117$

Exercice 18 :

1. *On considère deux entiers quelconques $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On considère 2 nombres A et B tels que :*

$$A = 5a + 4b \qquad \textit{et} \qquad B = 11a + 9b$$

Démontrer que $\text{pgcd}\,(a, b) = \text{pgcd}\,(A, B)$

On pose $D_{a,b}$ l'ensemble des diviseurs communs à a et b, ainsi que $D_{A,B}$ l'ensemble des diviseurs communs à A et B. Nous allons démontrer que $D_{a,b} = D_{A,B}$

— Montrons que $D_{a,b} \subset D_{A,B}$
Soit $x \in D_{a,b}$. Alors, il existe $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$ tels que $a = kx$ et $b = k'x$. Alors :

$$A = 5a + 4b = 5kx + 4k'x = x\,(5k + 4k')$$

Et donc x divise A. Nous démontrerions de même que $B = x\,(11k + 9k')$ et que x divise B, et donc $x \in D_{A,B}$
On vient de montrer que $D_{a,b} \subset D_{A,B}$

— Montrons que $D_{A,B} \subset D_{a,b}$
Soit $x \in D_{A,B}$. Alors, il existe $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$ tels que $A = kx$ et $B = k'x$. Alors :

$$A = 5a + 4b \qquad \text{et} \qquad B = 11a + 9b \iff kx = 5a + 4b \text{ et } \qquad k'x = 11a + 9b$$

Nous avons :

$$\left\{\begin{array}{rl} kx = & 5a + 4b \\ k'x = & 11a + 9b \end{array}\right. \iff \left\{\begin{array}{rl} 9 \times kx = & 45a + 36b \\ -4 \times k'x = & -44a - 36b \end{array}\right. \implies \text{en additionnant } x\,(9k - 4k') = a$$

Ce qui montre que x divise a
De même, nous avons :

$$\left\{\begin{array}{rl} kx = & 5a + 4b \\ k'x = & 11a + 9b \end{array}\right. \iff \left\{\begin{array}{rl} 11 \times kx = & 55a + 44b \\ -5 \times k'x = & -55a - 45b \end{array}\right. \implies \text{en additionnant } x\,(5k' - 11k) = b$$

Ce qui montre que x divise b et donc $x \in D_{a,b}$
On vient de montrer que $D_{A,B} \subset D_{a,b}$

Ainsi, $D_{A,B} = D_{a,b}$, ce qui signifie que a et b ont même diviseurs communs que A et B et donc même pgcd. Donc, $\text{pgcd}\,(a, b) = \text{pgcd}\,(A, B)$

2. *Généralisation*
On considère 2 nombres A' et B' tels que :

$$A' = pa + qb \qquad \textit{et} \qquad B' = ra + sb \qquad \textit{avec } ps - qr = 1$$

Démontrer que $\text{pgcd}\,(a, b) = \text{pgcd}\,(A', B')$

Bien entendu, la démonstration est semblable. Reprenant les même notations que pour la question 1, nous avons, de manière très évidente, $D_{a,b} \subset D_{A',B'}$

Démontrons maintenant que $D_{A',B'} \subset D_{a,b}$

Soit $x \in D_{A',B'}$. Alors, il existe $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$ tels que $A' = kx$ et $B' = k'x$. Alors :

$$(A' = pa + qb \text{ et } B' = ra + sb) \iff (kx = pa + qb \text{ et } k'x = ra + sb)$$

Nous avons :

$$\left\{\begin{array}{rl} kx = & pa + qb \\ k'x = & ra + sb \end{array}\right. \iff \left\{\begin{array}{rl} s \times kx = & spa + sqb \\ -q \times k'x = & -qra - sqb \end{array}\right. \implies \text{en additionnant } x\,(sk - qk') = a$$

en tenant compte de $ps - qr = 1$ Ce qui montre que x divise a
De même, nous avons :

$$\left\{\begin{array}{rl} kx = & pa + qb \\ k'x = & ra + sb \end{array}\right. \iff \left\{\begin{array}{rl} r \times kx = & rpa + rqb \\ -p \times k'x = & -pra - psb \end{array}\right. \implies \text{en additionnant } x\,(rk - pk') = b$$

en tenant compte de $ps - qr = 1$ Ce qui montre que x divise b et donc $x \in D_{a,b}$
On vient de montrer que $D_{A',B'} \subset D_{a,b}$
Ainsi, $D_{A',B'} = D_{a,b}$, ce qui signifie que a et b ont même diviseurs communs que A' et B' et donc même pgcd. Donc, $\text{pgcd}\,(a, b) = \text{pgcd}\,(A', B')$

Exercice 19 :

Montrer que pour tout entier $n \in \mathbb{N}^*$, $n+1 \mid \mathrm{C}_{2n}^{n} = \binom{2n}{n}$

Nous avons $\mathrm{C}_{2n+1}^{n+1} = \dfrac{(2n+1)!}{(n+1)! \times n!} = \dfrac{2n+1}{n+1} \times \mathrm{C}_{2n}^{n}$, c'est à dire :

$$(n+1)\,\mathrm{C}_{2n+1}^{n+1} = (2n+1)\,\mathrm{C}_{2n}^{n}$$

$n+1$ divise $(2n+1)\,\mathrm{C}_{2n}^{n}$, et comme $n+1$ et $2n+1$ sont premiers entre eux, d'après le lemme de Gauss, $n+1 \mid \mathrm{C}_{2n}^{n}$

Exercice 20 :

1. *Pour* $n \in \mathbb{N}$, *montrer qu'il existe un unique couple* $(a_n, b_n) \in \mathbb{N}^2$ *tel que :*

$$\left(1+\sqrt{2}\right)^n = a_n + b_n\sqrt{2} \text{ et } \left(1-\sqrt{2}\right)^n = a_n - b_n\sqrt{2}$$

C'est la question cruciale pour cet exercice !!

— **Démontrons l'unicité de** a_n **et** b_n

Supposons qu'il y ait une autre décomposition, c'est à dire que :

$$a_n + b_n\sqrt{2} = \alpha_n + \beta_n\sqrt{2}$$

Montrons que $a_n = \alpha_n$ et $b_n = \beta_n$

Supposons $a_n \neq \alpha_n$ et $b_n \neq \beta_n$[2] Alors, de l'égalité $a_n + b_n\sqrt{2} = \alpha_n + \beta_n\sqrt{2}$, on déduit que $\dfrac{a_n - \alpha_n}{\beta_n - b_n} = \sqrt{2}$. Or comme $\dfrac{a_n - \alpha_n}{\beta_n - b_n} \in \mathbb{Q}$, ceci sous entend que $\sqrt{2} \in \mathbb{Q}$, ce qui est faux.

Donc, $a_n = \alpha_n$ et $b_n = \beta_n$

— **Calculons explicitement** a_n **et** b_n

Nous commençons par calculer $\left(1+\sqrt{2}\right)^n$ en utilisant le binôme de Newton :

$$\left(1+\sqrt{2}\right)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \left(\sqrt{2}\right)^k$$

⋆ <u>Supposons n pair,c'est à dire $n = 2p$.</u>

Nous séparons la somme en deux : d'une part, les termes de rang pair, et d'autre part, les termes de rang impair :

$$\begin{aligned}\left(1+\sqrt{2}\right)^n &= \sum_{k=0}^{n} \mathrm{C}_n^k \left(\sqrt{2}\right)^k \\ &= \sum_{k=0}^{p} \mathrm{C}_n^{2k} \left(\sqrt{2}\right)^{2k} + \sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} \left(\sqrt{2}\right)^{2k+1}\end{aligned}$$

Or, $\displaystyle\sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} \left(\sqrt{2}\right)^{2k+1} = \sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} \left(\sqrt{2}\right)^{2k} \sqrt{2} = \sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} 2^k \sqrt{2} = \left(\sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} 2^k\right)\sqrt{2}$

De même, $\displaystyle\sum_{k=0}^{p} \mathrm{C}_n^{2k} \left(\sqrt{2}\right)^{2k} = \sum_{k=0}^{p} \mathrm{C}_n^{2k} 2^k$

⋆ Donc, si n est pair, avec $n = 2p$, $a_n = \displaystyle\sum_{k=0}^{p} \mathrm{C}_n^{2k} 2^k$ et $b_n = \displaystyle\sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} 2^k$

2. Démonstration un peu réductrice ; il faidrait supposer $a_n \neq \alpha_n$ **ou** $b_n \neq \beta_n$, puis envisager 3 cas : $a_n \neq \alpha_n$,$b_n \neq \beta_n$ et $a_n \neq \alpha_n$ **et** $b_n \neq \beta_n$; les deux premiers cas étant élémentaires ne sont donc pas traités ici.

◇ Supposons n impair,c'est à dire $n = 2p+1$.
Nous séparons une nouvelle fois la somme en deux, et de la même façon : d'une part, les termes de rang pair, et d'autre part, les termes de rang impair :

$$\begin{aligned}\left(1+\sqrt{2}\right)^n &= \sum_{k=0}^{n} \mathrm{C}_n^k \left(\sqrt{2}\right)^k \\ &= \sum_{k=0}^{p} \mathrm{C}_n^{2k} \left(\sqrt{2}\right)^{2k} + \sum_{k=0}^{p} \mathrm{C}_n^{2k+1} \left(\sqrt{2}\right)^{2k+1}\end{aligned}$$

Il n'y a donc pas grand chose de changé par rapport aux points ci-dessus

◇ Donc, si n est impair, avec $n = 2p+1$ $a_n = \sum_{k=0}^{p} \mathrm{C}_n^{2k} 2^k$ et $b_n = \sum_{k=0}^{p} \mathrm{C}_n^{2k+1} 2^k$

— **Intéressons nous maintenant à $\left(1-\sqrt{2}\right)^n$**

Nous réutilisons le binôme de Newton pour calculer $\left(1-\sqrt{2}\right)^n$:

$$\left(1-\sqrt{2}\right)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \left(-\sqrt{2}\right)^k$$

⋆ Supposons n pair,c'est à dire $n = 2p$.
Alors, en séparant d'une part, les termes de rang pair, et d'autre part, les termes de rang impair :

$$\begin{aligned}\left(1+\sqrt{2}\right)^n &= \sum_{k=0}^{n} \mathrm{C}_n^k \left(-\sqrt{2}\right)^k \\ &= \sum_{k=0}^{p} \mathrm{C}_n^{2k} (-1)^{2k} \left(\sqrt{2}\right)^{2k} + \sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} (-1)^{2k+1} \left(\sqrt{2}\right)^{2k+1} \\ &= \sum_{k=0}^{p} \mathrm{C}_n^{2k} \left(\sqrt{2}\right)^{2k} - \sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} \left(\sqrt{2}\right)^{2k+1} \\ &= \sum_{k=0}^{p} \mathrm{C}_n^{2k} 2^k - \left(\sum_{k=0}^{p-1} \mathrm{C}_n^{2k+1} 2^k\right)\sqrt{2}\end{aligned}$$

⋆ Donc, si n est pair, nous avons $\left(1-\sqrt{2}\right)^n = a_n - b_n\sqrt{2}$

◇ Supposons n impair,c'est à dire $n = 2p+1$.
Nous démontrions de la même manière que si n est impair, $\left(1-\sqrt{2}\right)^n = a_n - b_n\sqrt{2}$

2. *Calculer $a_n^2 - 2b_n^2$*

Nous avons :

$$\begin{aligned}a_n^2 - 2b_n^2 &= \left(a_n - b_n\sqrt{2}\right)\left(a_n + b_n\sqrt{2}\right) \\ &= \left(1-\sqrt{2}\right)^n \left(1+\sqrt{2}\right)^n \\ &= \left(\left(1-\sqrt{2}\right)\left(1+\sqrt{2}\right)\right)^n \\ &= (-1)^n\end{aligned}$$

3. *En déduire que a_n et b_n sont premiers entre eux*

La relation $a_n^2 - 2b_n^2 = (-1)^n$ permet d'écrire $a_n(a_n) - 2b_n(b_n) = (-1)^n$. Ce qui montre, d'après l'égalité de Bachet-Bezout que a_n et b_n sont premiers entre eux.

4.6.3 Equations diophantiennes

Exercice 21 :

Ecrire un algorithme de recherche du pgcd *de 2 nombres*

Nous proposons cet algorithme en Python. C'est un algorithme récursif, conforme au cours

```
def pgcd(a,b):
    r=a%b
    if r==0:
      return b
    else:
      return pgcd(b,r)
```

Exercice 23 :

1. *Calculer le pgcd de 5145, 4410, 3675*

   Nous avons $5145 = 5 \times 3 \times 7^3$, $4410 = 2 \times 3^2 \times 5 \times 7^2$ et $3675 = 3 \times 5^2 \times 7^2$ et donc

   $$\mathrm{pgcd}\,(5145, 4410, 3675) = 3 \times 5 \times 7^2 = 735$$

2. *Résoudre l'équation : $3675x - 5145y = 4410$*

   Il est possible de simplifier par $\mathrm{pgcd}\,(5145, 4410, 3675) = 735$, et nous avons

   $$3675x - 5145y = 4410 \Longleftrightarrow 5x - 7y = 6$$

   - ⋆ Recherche d'une solution particulière
     Les nombres 7 et 5 sont premiers entre eux, il existe donc $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ tels que $5x - 7y = 1$; il suffit de choisir $x' = 3$ et $y' = 2$.
     Les solutions particulières à l'équation $5x - 7y = 6$ sont donc $x_0 = 18$ et $y_0 = 12$
   - ⋆ Recherche de la solution générale
     Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ les solutions générales de l'équation $5x - 7y = 6$. Alors, nous avons :

     $$5x - 7y = 5x_0 - 7y_0 = 6 \Longleftrightarrow 5\,(x - x_0) = 7\,(y - y_0)$$

     Donc, par l'utilisation du lemme de Gauss
     - — 7 étant premier avec 5, divisant $5\,(x - x_0)$ divise forcément $x - x_0$. Donc $x - x_0 = 7k \Longleftrightarrow x = x_0 + 7k$ avec $k \in \mathbb{Z}$
     - — De même, $y - y_0 = 5k \Longleftrightarrow y = y_0 + 5k$ avec $k \in \mathbb{Z}$

     Les solutions de l'équation $3675x - 5145y = 4410$ sont donc données par : $\begin{cases} x = 18 + 7k \\ y = 12 + 5k \end{cases}$ avec $k \in \mathbb{Z}$

Exercice 24 :

Résoudre dans $\mathbb{Z}$, les équations

1. $65x = 16y$

   Tout d'abord, il est facile de remarquer que $\mathrm{pgcd}\,(65, 15) = 1$, c'est à dire que 65 et 16 sont premiers entre eux.
   16 divise $65x$, 16 est premier avec 65, donc, d'après le lemme de Gauss, 16 divise x et donc $x = 16k$ avec $k \in \mathbb{Z}$
   De même, pour 65, 65 divise y et donc $y = 65k_1$ avec $k_1 \in \mathbb{Z}$
   En remplaçant dans les équations, nous obtenons : $65 \times 16 \times k = 16 \times 65 \times k_1$; d'où $k = k =_1$ Les solutions sont donc :

   $$x = 16k \qquad y = 65k \text{ avec } k \in \mathbb{Z}$$

2. $65x - 16y = 1$

   65 et 16 étant premiers entre eux, d'après le théorème de Bachet, il existe bien $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ tels que $65x - 16y = 1$
   - ⋆ Une solution particulière est donnée par $x_0 = 1$ et $y_0 = 4$
   - ⋆ Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ la solution générale. Alors :

   $$65x_0 - 16y_0 = 1 = 65x - 16y \Longleftrightarrow 65\,(x - x_0) = 16\,(y - y_0)$$

- ⋆ Donc, d'après la question précédente :

$$x - x_0 = 16k \text{ et } y - y_0 = 65k \iff x = 1 + 16k \text{ et } y = 4 + 65k \text{ avec } k \in \mathbb{Z}$$

3. $65x - 16y = 7$

Comme tout à l'heure, 65 et 16 étant premiers entre eux, il existe bien $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ $65x - 16y = 7$

- ⋆ Une solution particulière est donnée par $x_0 = 7$ et $y_0 = 28$
- ⋆ Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ la solution générale. Alors :

$$65x_0 - 16y_0 = 7 = 65x - 16y \iff 65(x - x_0) = 16(y - y_0)$$

- ⋆ Donc, d'après la question 1 :

$$x - x_0 = 16k \text{ et } y - y_0 = 65k \iff x = 7 + 16k \text{ et } y = 28 + 65k \text{ avec } k \in \mathbb{Z}$$

Exercice 25 :

Un pays décide de ne mettre en circulation que des pièces de 3 et 5 euros.

1. *Combien de prix sont impraticables entre 1 et 20 euros, si le commerçant ne veut pas être obligé de rendre la monnaie ?*
2. *Tous les prix supérieurs à 20 euros sont-ils admissibles ?*
3. *Quels sont les prix admissibles si le commerçant accepte de rendre la monnaie ?*

- Soit S la somme *(positive)* que doit payer le client. Pour payer cette somme, il faut x pièces de 3 euros et y pièces de 5 euros pour obtenir la somme, c'est à dire pour que $3x + 5y = S$
- Comme 5 et 3 sont premiers entre eux, d'après le théorème de Bachet, il existe $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ tels que $3x + 5y = 1$

  Résolvons l'équation $3x + 5y = 1$
  - ⋆ Une solution particulière est $x_0 = 2$ et $y_0 = -1$
  - ⋆ Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ la slution générale. Alors :

$$3x + 5y = 3x_0 + 5y_0 \iff 3(x - x_0) = 5(y_0 - y)$$

D'où nous avons :

$$\begin{cases} x - x_0 = & 5k \\ y_0 - y = & 3k \end{cases} \text{ avec } k \in \mathbb{Z} \iff \begin{cases} x = & 2 + 5k \\ y = & -1 - 3k \end{cases} \text{ avec } k \in \mathbb{Z}$$

- Pour $S \in \mathbb{N}^*$, la solution à l'équation $3x + 5y = S$ est donnée par :

$$\begin{cases} x = & 2S + 5k \\ y = & -S - 3k \end{cases} \text{ avec } k \in \mathbb{Z}$$

- Ya-t-il des sommes impossibles à payer ?

  Regardons quelques cas particuliers :
  - ⋆ **Pour** $S = 1$

    Nous devons résoudre $3x + 5y = 1$ donc les solutions sont :

$$x = 2 + 5k \qquad y = -1 - 3k \text{ avec } k \in \mathbb{Z}$$

    Nous devons avoir $x \geqslant 0$ et $y \geqslant 0$, c'est à dire $2 + 5k \geqslant 0$ et $-1 - 3k \geqslant 0$ ce qui est équivalent à $\dfrac{-2}{5} \leqslant k \leqslant \dfrac{-1}{3}$; et il n'existe pas d'entiers tels que $\dfrac{-2}{5} \leqslant k \leqslant \dfrac{-1}{3}$

    Le client ne peut donc pas payer une somme de 1 euro.
  - ⋆ **Pour** $S = 2$**,** $S = 4$ **et** $S = 7$, c'est aussi impossible ; et la démonstration est la même.
  - ⋆ **Pour** $S = 3$, nous avons $x = 1$ et $y = 0$

$\star$ **Faisons la synthèse dans un tableau**

S	x	y
5	0	1
6	2	0
8	1	1
9	3	0
10	0	2
11	2	1
12	4	0
13	1	2

S	x	y
14	3	1
15	5	0
15	0	3
16	2	2
17	4	2
18	6	0
18	1	3
19	3	2
20	0	4

On peut remarquer que, pour $S = 15$ et $S = 18$, il y a 2 solutions.

- A partir de quelle somme pouvons nous payer ?
On peut payer si $x \geqslant 0$ et $y \geqslant 0$, c'est à dire si :
$$2S + 5k \geqslant 0 \text{ et } -S - 3k \geqslant 0 \Longleftrightarrow \frac{-2S}{5} \leqslant k \leqslant \frac{-S}{3}$$
Et k entier existe si et seulement si $\dfrac{-S}{3} - \left(\dfrac{-2S}{5}\right) \geqslant +1$
Or $\dfrac{-S}{3} - \left(\dfrac{-2S}{5}\right) = \dfrac{S}{15}$ et donc $\dfrac{S}{15} \geqslant 1 \Longleftrightarrow S \geqslant 15$
- Si le commerçant accepte de rendre la monnaie, ceci signifie que x ou y peuvent avoir des valeurs négatives, et à ce moment là, toutes les sommes S sont possibles.
Pour $S = 7$, les solutions à l'équation $3x + 5y = 7$ sont du type :
$$x = 14 + 5k \qquad y = -7 - 3k \text{ avec } k \in \mathbb{Z}$$
Une solution possible de cette équation est $x = 14$ et $y = -7$, ce qui veut dire que le client donne 14 pièces de 3 euros et que le commerçant rend 7 billet de 5 euros.
Une autre solution est $x = 9$ et $y = -4$ ou $x = 4$ et $y = -1$

Exercice 26 :

Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que :

▷ $5x + 7y = 1$

Comme 5 est premier avec 7, cette équation a des solutions.

$\star$ Une solution particulière est donnée par $x_0 = 3$ et $y_0 = -2$

$\star$ Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ la solution générale de l'équation ; alors, nous avons :
$$5x + 7y = 5x_0 + 7y_0 \Longleftrightarrow 5\,(x - x_0) = 7\,(y_0 - y)$$

$\star$ La solution générale est donc donnée par :
$$x = x_0 + 7k \quad y = y_0 - 5k \text{ avec } k \in \mathbb{Z} \Longleftrightarrow x = 3 + 7k \quad y = -2 - 5k \text{ avec } k \in \mathbb{Z}$$

▷ $48x + 60y = 30$

On peut simplifier par 6 ; nous avons donc :
$$48x + 60y = 30 \Longleftrightarrow 8x + 10y = 5$$
Or, pgcd $(8, 10) = 2$ et 2 ne divise pas 5 ; cette équiation est impossible.

▷ $20x + 25y = 1$

Comme pgcd $(20, 25) = 5$, cette équation est impossible

▷ $21x - 56y = 49$

On peut simplifier par 7 ; nous avons donc :

$$21x - 56y = 49 \Longleftrightarrow 3x - 8y = 7$$

Or, $\text{pgcd}\,(8, 3) = 1$, il existe donc des solutions

⋆ Une solution particulière est donnée par $x_0 = 21$ et $y_0 = 7$

⋆ Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ la solution générale de l'équation ; alors, nous avons :

$$3x - 8y = 3x_0 - 8y_0 \Longleftrightarrow 3\,(x - x_0) = 8\,(y - y_0)$$

⋆ La solution générale est donc donnée par :

$$x = x_0 + 8k \quad y = y_0 + 3k \text{ avec } k \in \mathbb{Z} \Longleftrightarrow x = 21 + 8k \quad y = 7 + 3k \text{ avec } k \in \mathbb{Z}$$

Exercice 27 :

Résoudre dans $\mathbb{Z}$ le système d'équation d'inconnue x $\left\{\begin{array}{l} x \equiv 4\,[7] \\ x \equiv 5\,[15] \end{array}\right.$

Nous avons :

$$\left\{\begin{array}{l} x \equiv 4\,[7] \\ x \equiv 5\,[15] \end{array}\right. \Longleftrightarrow \left\{\begin{array}{l} x = 4 + 7u \\ x = 5 + 15v \end{array}\right.$$

De $x = 4 + 7u$ et $x = 5 + 15v$, nous tirons :

$$4 + 7u = 5 + 15v \Longleftrightarrow 7u - 15v = 1$$

comme, $\text{pgcd}\,(7, 15) = 1$, il existe donc des solutions.

⋆ Une solution particulière est donnée par $u_0 = -2$ et $v_0 = -1$

⋆ Soient $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ la solution générale de l'équation ; alors, nous avons :

$$7u - 15v = 7u_0 - 15v_0 \Longleftrightarrow 7\,(u - u_0) = 15\,(v - v_0)$$

⋆ La solution générale est donc donnée par :

$$u = u_0 + 15k \quad v = v_0 + 7k \text{ avec } k \in \mathbb{Z} \Longleftrightarrow u = -2 + 15k \quad v = -1 + 7k \text{ avec } k \in \mathbb{Z}$$

D'où on trouve $x = -10 + 105k$ avec $k \in \mathbb{Z}$, c'est à dire $x \equiv 95\,[105]$

Exercice 28 :

Deux entiers naturels a et b s'écrivent dans le système de numération de base n :

$$a = \overline{(2310)}_n \qquad b = \overline{(252)}_n$$

On appelle $d = \text{pgcd}\,(a, b)$

1. (a) *Démontrer que $2n + 1$ divise a et b*

   Premièrement, il faut ré-écrire a et b :

   — $a = n + 3n^2 + 2n^3 = n\,(2n + 1)\,(n + 1)$ *(factorisation classique)*

   — $b = 2 + 5n + 2n^2 = (2n + 1)\,(n + 2)$

   D'après les factorisations ci-dessus, il est donc clair que $2n + 1$ divise a et b

   (b) *Démontrer que, si n est pair, alors $d = \text{pgcd}\,(a, b) = 2\,(2n + 1)$, et que, si n est impair, alors $d = \text{pgcd}\,(a, b) = 2n + 1$*

   Tout d'abord, $2n + 1$ divise d.

— Supposons n pair, c'est à dire que $\frac{n}{2}$ est un entier. Alors,

$$a = n(2n+1)(n+1) = 2 \times \frac{n}{2}(2n+1)(n+1) = [2(2n+1)]\frac{n}{2}(n+1)$$
$$b = (2n+1)(n+2) = (2n+1) \times 2 \times \left(\frac{n}{2}+1\right) = [2(2n+1)]\left(\frac{n}{2}+1\right)$$

Pour montrer que $d = \text{pgcd}(a,b) = 2(2n+1)$ il faut montrer que $\frac{n}{2}(n+1)$ et $\left(\frac{n}{2}+1\right)$ sont premiers entre eux, ou, d'après l'identité de Bezout, trouver A et B tels que

$$A \times \frac{n}{2}(n+1) + B \times \left(\frac{n}{2}+1\right) = 1$$

En choisissant $A = 1$ et $B = 1 - n$, nous avons :

$$\frac{n}{2}(n+1) + (1-n)\left(\frac{n}{2}+1\right) = \frac{n^2}{2} + \frac{n}{2} + \frac{n}{2} + 1 - \frac{n^2}{2} - n = 1$$

Nous avons donc bien $d = \text{pgcd}(a,b) = 2(2n+1)$

— Supposons n impair. Alors,

$$a = n(2n+1)(n+1) = [(2n+1)]\, n(n+1)$$
$$b = (2n+1)(n+2) = [(2n+1)](n+2)$$

Pour montrer que $d = \text{pgcd}(a,b) = (2n+1)$ il faut montrer que $n(n+1)$ et $(n+2)$ sont premiers entre eux.
Remarquons que si n est pair, $n(n+1)$ et $n+2$ sont pairs et ne sont pas premiers entre eux.
Nous avons $\text{pgcd}(n+1, n+2) = 1$. Si nous montrons que $\text{pgcd}(n, n+2) = 1$, par les résultats sur le produit, nous avons $\text{pgcd}(n(n+1), n+2) = 1$
Soit donc d un diviseur commun à $n+2$ et n . Alors, $n = kd$ et $n+2 = k'd$. n étant impair, $n+2$ l'est aussi, et donc k, k' et d sont aussi impair.
d, divisant n et $n+2$ divise aussi $n+2-n = 2$. La seule valeur possible est donc 1, et nous en déduisons que $\text{pgcd}(n, n+2) = 1$, et donc, que si n est impair, $\text{pgcd}(a,b) = 2n+1$

2. *On suppose que $n = 6$. Résoudre alors dans $\mathbb{Z} \times \mathbb{Z}$ l'équation diophantienne $ax + by = -26$*

Si $n = 6$, alors n est pair et donc le pgcd de a et b est $\text{pgcd}(a,b) = 26$.
Pour $n = 6$, l'équation $ax + by = -26$ devient : $21x + 4y = -1$ qui est une équation diophantienne classique dont une solution particulière est donnée par $x_0 = -1$ et $y_0 = 5$. La solution générale est donc donnée par :

$$\begin{cases} x = -1 + 4k \\ y = 5 + 21k \end{cases} \quad \text{avec } k \in \mathbb{Z}$$

Exercice 29 :

Un exercice d'arithmétique et de codage

1. (a) *Déterminer deux entiers relatifs u et v tels que $7u - 13v = 1$*

Premièrement, comme 7 et 13 sont premiers entre eux, d'après l'identité de Bachet-Bezout, cette équation admet des solutions. Une solution particulière de cette équation est bien entendue donnée par $(u_0, v_0) = (2, 1)$
Même si ceci n'est pas demandé, cherchons toutes les solutions de cette équation.
▷ Soit $(u, v) \in \mathbb{Z}^2$ la solution générale de l'équation ; alors, nous avons :

$$7u - 13v = 7u_0 - 13v_0 \iff 7(u - u_0) = 13(v - v_0)$$

Nous avons 7 qui divise le produit $13(v - v_0)$, et comme 7 est premier avec 13, d'après le lemme de Gauss, 7 divise $v - v_0$; donc $v - v_0 = 7k$

▷ En remplaçant $v - v_0$ par sa valeur trouvée, nous obtenons :

$$\left\{\begin{array}{rl} 7\,(u-u_0) = & 13\,(v-v_0) \\ = & 13\times 7k \end{array}\right. \iff u - u_0 = 13k$$

▷ La solution générale est donc donnée par :

$$\boxed{u = 2+13k \quad v = 1+7k \text{ avec } k\in\mathbb{Z}}$$

(b) *Déterminer tous les couples (a,k) d'entiers relatifs tels que $14a - 26k = 4$*

▷ Remarquons, sans perdre de généralité, que l'équation $14a - 26k = 4$ est équivalente à $7a - 13k = 2$. Donc, pour trouver des solutions particulières, il suffit de multiplier les solutions particulières de $7u - 13v = l$ trouvées juste auparavant par 2 pour les avoir. Donc, nous avons comme solutions pariculières :

$$a_0 = 4 \qquad k_0 = 2$$

▷ Pour trouver la solution générale, l'algorithme est le même que précédemment.
Soit $(a,k)\in\mathbb{Z}^2$ la solution générale de l'équation ; alors, nous avons :

$$7a - 13k = 7a_0 - 13k_0 \iff 7\,(a-a_0) = 13\,(k-k_0)$$

Nous avons 7 qui divise le produit $13\,(k-k_0)$, et comme 7 est premier avec 13, d'après le lemme de Gauss, 7 divise $k-k_0$; donc $k - k_0 = 7z$
En remplaçant $k-k_0$ par sa valeur trouvée, nous obtenons :

$$\left\{\begin{array}{rl} 7\,(a-a_0) = & 13\,(k-k_0) \\ = & 13\times 7z \end{array}\right. \iff a - a_0 = 13z$$

▷ La solution générale est donc donnée par :

$$\boxed{a = 4+13z \quad k = 2+7z \text{ avec } z\in\mathbb{Z}}$$

Il faut absolument remarquer l'analogie des solutions ; la différence se faisant uniquement sur les valeurs particulières

2. *On considère deux entiers naturels a et b. Pour tout entier n, on note $\rho\,(n)$ le reste 1e la division euclidienne de $an+b$ par 26.*
On décide de coder un message, en procédant comme suit :
— *À chaque lettre de l'alphabet on associe un entier compris entre 0 et 25 (A est numéroté 0, B numéroté 1. . . etc . . .)*
— *Pour chaque lettre α du message, on détermine l'entier n associé puis on calcule $\rho\,(n)$.*
— *La lettre α est alors codée par la lettre associée à $\rho\,(n)$.*
Dans cette question, on ne connaît pas les entiers a et b, mais on sait que la lettre F est codée par la lettre K et la lettre T est codée par la lettre O.

(a) *Montrer que les entiers a et b sont tels que $5a+b\equiv 10\,[26]$ et $19a+b\equiv 14\,[26]$*

En faisant un tableau de correspondances, si la lettre F est codée par la lettre K, au nombre 5 associé à F, correspond le nombre $\rho\,(5) = 10$ correspondant à K. Nous avons alors une première équation :

$$a\times 5 + b \equiv 10\,[26]$$

De même, si la lettre T est codée par la lettre 0, au nombre 19 associé à T, correspond le nombre $\rho\,(19) = 14$ correspondant à O. Nous avons donc le·système d'équation :

$$\begin{array}{l} 5a+b\equiv 10\,[26] \\ 19a+b\equiv 14\,[26] \end{array}$$

(b) *En déduire qu'il existe un entier $k \in \mathbb{Z}$ tel que $14a - 26k = 4$*

Par compatibilité de l'addition avec la relation de congruence, nous avons :

$$(19a + b) - (5a + b) \equiv 4\,[26]$$

C'est à dire $14a \equiv 4\,[26]$. Attention à ne pas faire l'erreur de simplifier, car 14, 4 et 26 ont pour pgcd 2

Il faut donc réécrire la congruence. Nous avons donc : $14a = 4 + 26k$ où $k \in \mathbb{Z}$

(c) *Déterminer tous les couples d'entiers (a, b), avec $0 \leqslant a \leqslant 25$ et $0 \leqslant b \leqslant 25$,tels que :*

$$\begin{array}{l} 5a + b \equiv 10\,[26] \\ 19a + b \equiv 14\,[26] \end{array}$$

D'après la question précédente, il faut donc commencer à résoudre $14a = 4+26k$ ou, $14a-26k = 4$ ou, ce qui est équivalent, $7a - 13k = 2$; dans des questions précédentes, nous avons trouvé :

$$a = 4 + 13z \qquad k = 2 + 7z \text{ avec } z \in \mathbb{Z}$$

C'est à dire $a \equiv 4\,[13]$. Les entiers a compris entre 0 et 25 vérifiant $a \equiv 4\,[13]$ sont donc 4 et 17

De $b \equiv 10 - 5a\,[26]$, nous tirons les couples d'entiers (a, b) où b compris entre 0 et 25 :

$$\boxed{(4, 16)\,(17, 3)}$$

3. *On suppose que $a = 17$ et $b = 3$.*

(a) *Coder le message « GAUSS »*

Il faut d'abord chercher les correspondance des lettres :

G	A	U	S
6	0	20	18

Puis rechercher les différents correspondances en fonction de la transformation proposée

$$\begin{array}{rcrcrcl} 6 & \longmapsto & 17 \times 6 + 3 = 105 & \equiv & 1\,[26] & \longmapsto & B \\ 0 & \longmapsto & 17 \times 0 + 3 = 3 & \equiv & 3\,[26] & \longmapsto & D \\ 20 & \longmapsto & 17 \times 20 + 3 = 343 & \equiv & 5\,[26] & \longmapsto & F \\ 18 & \longmapsto & 17 \times 18 + 3 = 309 & \equiv & 23\,[26] & \longmapsto & X \end{array}$$

Ainsi, « GAUSS »est noté « BDFXX »

(b) *Soient n et p deux entiers naturels quelconques. Montrer que, si $\rho(n) = \rho(p)$, alors $17(n - p) \equiv 0\,[26]$*

Par hypothèse, nous avons $\rho(n) = \rho(p)$, ce qui signifie donc que $17n + 3 \equiv 17p + 3\,[26]$, ce qui autrement traduit donne :

$$17n + 3 = 17p + 3 + 26k \Longleftrightarrow 17n - 17p \equiv 0\,[26] \Longleftrightarrow 17(n - p) == 0\,[26]$$

(c) *En déduire que deux lettres distinctes de l'alphabet sont codées par deux autres lettres distinctes*

Il faut en fait montrer que si $\rho(n) = \rho(p)$ alors, $n = p$ où, et c'est important, $0 \leqslant n \leqslant 25$ et $0 \leqslant p \leqslant 25$. Or, 17 est premier avec 26 et est donc inversible dans $\mathbb{Z}/26\mathbb{Z}$, et son inverse est un nombre u tel que $17u \equiv 1\,[26]$; par calcul, on trouve $3 \times 17 = 51 \equiv -1\,[26]$, et donc $(3 \times 17)^2 \equiv (-1)^2 \equiv 1\,[26]$, et donc l'inverse de 17 est donné par $u = 9 \times 17 = 153 \equiv 23\,[26]$

Je multiplie donc chaque membre de l'équation $17(n - p) \equiv 0\,[26]$ par 23, et j'obtiens :

$$\begin{aligned} 17(n - p) &\equiv 0\,[26] \\ 23 \times 17(n - p) &\equiv 0\,[26] \\ (n - p) &\equiv 0\,[26] \end{aligned}$$

D'où $n \equiv p\,[26]$

4. *On suppose toujours que $a = 17$ et $b = 3$*

(a) *Soit n un entier naturel. Calculer le reste de la division euclidienne de $23\rho(n) + 9 - n$ par 26*

D'après l'énoncé, nous avons $17n + 3 \equiv \rho(n)\,[26]$, et donc, en utilisant la question précédente,

$$23 \times (17n + 3) \equiv 23 \times \rho(n)\,[26]$$

Ce qui est équivalent à :

$$n + 69 \equiv 23 \times \rho(n)\,[26]$$

Comme $69 \equiv 17\,[26]$, nous avons : $n + 17 \equiv 23 \times \rho(n)\,[26]$, de telle sorte que :

$$23 \times \rho(n) - 17 - n \equiv 0\,[26] \Longleftrightarrow 23 \times \rho(n) + 9 - n \equiv 0\,[26]$$

(b) *En déduire un procédé de décodage*

L'objet de la question est de retrouver n connaissant $\rho(n)$. Or, dans la question précédente, nous avons trouvé que $23 \times \rho(n) + 9 - n \equiv 0\,[26]$, c'est à dire que $n \equiv 23 \times \rho(n) + 9\,[26]$; c'est le procédé de décodage !!

(c) *En déduire le décodage du message « KTGZDO »*

On recommence le même algorithme que dans la question 1 : Il faut d'abord chercher les correspondance des lettres :

K	T	G	Z	D	O
10	19	6	25	3	14

Puis on recherche les différents correspondances en fonction de la transformation proposée

$$\begin{array}{rclcll}
10 & \longmapsto & 23 \times 10 + 9 = 239 & \equiv & 5\,[26] & \longmapsto & F \\
19 & \longmapsto & 23 \times 19 + 9 = 446 & \equiv & 4\,[26] & \longmapsto & E \\
6 & \longmapsto & 23 \times 6 + 9 = 147 & \equiv & 17\,[26] & \longmapsto & R \\
25 & \longmapsto & 23 \times 25 + 9 = 584 & \equiv & 12\,[26] & \longmapsto & M \\
3 & \longmapsto & 23 \times 3 + 9 = 78 & \equiv & 0\,[26] & \longmapsto & A \\
14 & \longmapsto & 23 \times 14 + 9 = 331 & \equiv & 19\,[26] & \longmapsto & T
\end{array}$$

Ainsi, « KTGZDO »code le mot « FERMAT »

Allons plus loin

1. Pourquoi ne pas avoir pris $a = 4$ et $b = 16$. Très simplement parce qu'à 2 lettres différentes du message peu correspondre la même lettre du code ; par exemple :

$$\begin{array}{rclcll}
A = 0 & \longmapsto & 4 \times 0 + 16 = 16 & \equiv & 16\,[26] & \longmapsto & Q \\
N = 13 & \longmapsto & 4 \times 13 + 16 = 68 & \equiv & 16\,[26] & \longmapsto & Q \\
F = 5 & \longmapsto & 4 \times 5 + 16 = 36 & \equiv & 10\,[26] & \longmapsto & K \\
S = 18 & \longmapsto & 4 \times 18 + 16 = 88 & \equiv & 10\,[26] & \longmapsto & K
\end{array}$$

Ainsi, à un code correspond 2 lettres, ce qui rend impossible le décodage

2. La clef réside dans le fait que la fonction ρ doit être bijective :

$$\left\{\begin{array}{rcl} \rho : \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ n & \longmapsto & \rho(n) = an + b \end{array}\right.$$

3. Que faut-il pour que ρ soit bijective ?

Pour que ρ soit bijective, il faut que a soit premier avec 26, et donc inversible dans $\mathbb{Z}/26\mathbb{Z}$

▷ ρ est injective, puisque :

$$\rho(n) = \rho(p) \Longleftrightarrow an + b = ap + b \Longleftrightarrow an = ap \Longleftrightarrow a^{-1}(an) = a^{-1}(ap) \Longleftrightarrow n = p$$

▷ ρ est surjective, puisque si $p \in \mathbb{Z}/26\mathbb{Z}$, alors :

$$an + b = p \Longleftrightarrow an = p - b \Longleftrightarrow n = a^{-1}(p - b)$$

Et $\rho\left(a^{-1}(p - b)\right) = p$.

- ▷ Donc, si a est premier avec 26, $\rho(n) = an + b$ est bijective dans $\mathbb{Z}/26\mathbb{Z}$; et nous avons une fonction de décodage donnée par $\Delta(n) = a^{-1}(n - b)$
- ▷ C'est le problème plus général des fonctions ρ :

$$\left\{ \begin{array}{rcl} \rho : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \rho(x) = ax + b \end{array} \right.$$

  Pour que ρ soit bijective, il faut donc que $a \wedge n = 1$
- ▷ Si $a = 4$, alors $4 \wedge 26 = 2$; 4 et 26 ne sont pas premiers entre eux.

4. Historiquement, c'est le modèle de codage de Jules César. Jules n'utilisait qu'un seul code : $a = 1$ et $b = 3$. Il aurait dû, par prudence, modifier ses a et ses b en prenant simplement a tel que a soit premier avec 26.

4.6.4 Exercices sur le ppcm

Exercice 31 :

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

1. $\left\{ \begin{array}{l} x \equiv 3\,[11] \\ x \equiv 7\,[15] \end{array} \right.$

   Comme 11 et 15 sont premier entre eux, d'après le lemme chinois 4.4.5, il existe une unique solution modulo 165.

   Recherchons cette solution
   - Tout d'abord, nous avons $x = 3 + 11u$ et $x = 7 + 15v$, d'où nous tirons $3 + 11u = 7 + 15v \iff 11u - 15v = 4$
   - Les solutions particulières de cette équation sont : $u_0 = -16$ et $v_0 = -12$
   - Si u et v sont des solutions générales de l'équation, nous avons :

   $$11u - 15v = 11u_0 - 15v_0 \iff 11(u - u_0) = 15(v - v_0)$$

   D'où nous trouvons comme solutions :

   $$u - u_0 = 15k \text{ et } v - v_0 = 11k \iff u = -16 + 15k \text{ et } v = -12 + 11k \text{ avec } k \in \mathbb{Z}$$

   D'où nous obtenons $x = 3 + 11 \times (-16 + 15k) = 3 - 176 + 165k = -173 + 165k$, c'est à dire que $x \equiv -173\,[165] \iff x \equiv 157\,[165]$
2. $\left\{ \begin{array}{l} x \equiv 4\,[10] \\ x \equiv 8\,[14] \end{array} \right.$

Cette fois ci, c'est bien différent puisque 10 et 14 ne sont pas premiers entre eux.
- Tout d'abord, nous avons $x = 4 + 10u$ et $x = 8 + 14v$, d'où nous tirons $4 + 10u = 8 + 14v \iff 10u - 14v = 4 \iff 5u - 7v = 2$. Comme 5 et 7 sont premiers entre eux, cette équation a des solutions.
- Les solutions particulières de cette équation sont : $u_0 = 6$ et $v_0 = 4$
- Si u et v sont des solutions générales de l'équation, nous avons :

$$5u - 7v = 5u_0 - 7v_0 \iff 5(u - u_0) = 7(v - v_0)$$

D'où nous trouvons comme solutions :

$$u - u_0 = 7k \text{ et } v - v_0 = 7k \iff u = 6 + 7k \text{ et } v = 4 + 5k \text{ avec } k \in \mathbb{Z}$$

D'où nous obtenons $x = 4 + 10 \times (6 + 7k) = 64 + 70k$, c'est à dire que $x \equiv 64\,[70]$

Exercice 32 :

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Donner $\operatorname{pgcd}(a+b, \operatorname{ppcm}(a,b))$

On appelle $d = \operatorname{pgcd}(a,b)$
Alors, il existe $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$ et $\operatorname{pgcd}(a',b') = 1$
Donc, d'après 4.4.2 page 137, $\operatorname{ppcm}(a,b) = \operatorname{ppcm}(da', db') = d \times \operatorname{ppcm}(a',b') = da'b'$ puisque $a' \wedge b' = 1$.
Donc,

$$\begin{aligned} \operatorname{pgcd}(a+b, \operatorname{ppcm}(a,b)) &= \operatorname{pgcd}(da'+db', da'b') \\ &= d \times \operatorname{pgcd}(a'+b', a'b') \end{aligned}$$

D'après les résultats sur le pgcd vu en exercices, comme $\operatorname{pgcd}(a',b') = 1$, $\operatorname{pgcd}(a'+b', a'b') = 1$, et donc :

$$\operatorname{pgcd}(a+b, \operatorname{ppcm}(a,b)) = d$$

Exercice 33 :

Déterminer l'ensemble des couples (x,y) d'entiers naturels tels que :

$$\left\{ \begin{array}{l} \delta = 60 \\ \mu = 3600 \end{array} \right.$$

Où $\delta = \operatorname{pgcd}(x,y)$ et $\mu = \operatorname{pppcm}(x,y)$

Soient donc $x' \in \mathbb{N}$ et $y' \in \mathbb{N}$ tels que $x = \delta x'$ et $y = \delta y'$ avec $x' \wedge y' = 1$.
Nous avons aussi $\mu \times \delta = xy = \delta^2 x'y' \iff \mu = \delta x'y'$.
Nous avons donc :

$$\left\{ \begin{array}{l} \delta = 60 \\ \mu = 3600 \end{array} \right. \iff \left\{ \begin{array}{l} \delta = 60 \\ \delta x'y' = 3600 \end{array} \right. \iff \left\{ \begin{array}{l} \delta = 60 \\ x'y' = 60 \end{array} \right.$$

x' et y' apparaissent comme les diviseurs de 60. Les diviseurs de 60 sont : $\{1,2,3,4,5,6,10,12,15,20,30,60\}$.
Il faut maintenant choisir x' et y' tels que $x' \wedge y' = 1$.
Nous obtenons le tableau suivant :

x'	y'	x	y
1	60	60	3600
3	20	180	1200
4	15	240	900
5	12	300	720

4.6.5 Les théorèmes de Fermat et de Wilson

Exercice 34 :

Une autre démonstration du petit théorème de Fermat

1. *Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ tel que $0 < k < n$.*

   (a) *Montrer que si n est premier, alors n divise C_n^k*

   Par définition de l'analyse combinatoire :

   $$\mathrm{C}_n^k = \frac{n!}{k!\,(n-k)!} = \frac{n}{k} \times \frac{(n-1)!}{(k-1)!\,[(n-1)-(k-1)]!} = \frac{n}{k}\mathrm{C}_{n-1}^{k-1}$$

   En fait, nous avons donc : $k\mathrm{C}_n^k = n\mathrm{C}_{n-1}^{k-1}$, et donc n divise $k\mathrm{C}_n^k$. n étant un nombre premier, est premier avec k et, d'après le lemme de Gauss, divise C_n^k.
   Ainsi, si n est un nombre premier, pour tout k entier tel que $0 < k < n$, n divise C_n^k.

   (b) *Démontrer que si n est premier, alors n divise $2^n - 2$*

   Le résultat précédent peut aussi s'écrire :
   Si n est un nombre premier, pour tout k entier tel que $0 < k < n$, alors $\mathrm{C}_n^k \equiv 0\,[n]$

Nous avons :

$$\begin{aligned} 2^n &= (1+1)^n \\ &= \sum_{k=0}^{n} \mathrm{C}_n^k \\ &= \mathrm{C}_n^0 + \sum_{k=1}^{n-1} \mathrm{C}_n^k + \mathrm{C}_n^n \\ &= 2 + \sum_{k=1}^{n-1} \mathrm{C}_n^k \end{aligned}$$

Or, pour $0 < k < n$, nous avons $\mathrm{C}_n^k \equiv 0\,[n]$ et donc $\sum_{k=1}^{n-1} \mathrm{C}_n^k \equiv 0\,[n]$.

Nous en concluons donc que $2^n \equiv 2\,[n] \Longleftrightarrow 2^n - 2 \equiv 0\,[n]$, c'est à dire $2^n - 2$ divisible par n.

2. *Soit $n \in \mathbb{N}^*$, premier et $a \in \mathbb{N}$. Montrer que $a^n - a$ est divisible par n*

Nous allons faire cette démonstration par récurrence sur a

- ▷ C'est trivialement vrai pour $a = 0$
- ▷ Supposons que $a^n - a$ soit divisible par n
  C'est à dire que, écrit autrement, $a^n - a \equiv 0\,[n] \Longleftrightarrow a^n \equiv a\,[n]$
- ▷ Démontrons que $(a+1)^n - (a+1)$ est divisible par n

$$\begin{aligned} (a+1)^n &= \sum_{k=0}^{n} \mathrm{C}_n^k a^k \\ &= \mathrm{C}_n^0 a^0 + \sum_{k=1}^{n-1} \mathrm{C}_n^k a^k + \mathrm{C}_n^n a^n \\ &= 1 + a^n + \sum_{k=1}^{n-1} \mathrm{C}_n^k a^k \end{aligned}$$

n étant premier, pour $0 < k < n$, nous avons $\mathrm{C}_n^k \equiv 0\,[n]$ et donc $\sum_{k=1}^{n-1} \mathrm{C}_n^k a^k \equiv 0\,[n]$.

Nous en déduisons donc que $(a+1)^n \equiv 1 + a^n\,[n]$. Par hypothèse de récurrence, $a^n \equiv a\,[n]$, donc, par transitivité de la relation de congruence, $(a+1)^n \equiv 1 + a\,[n]$.

Ce que nous voulions.

Ainsi, pour $n \in \mathbb{N}^*$, premier et $a \in \mathbb{N}$, $a^n - a$ est divisible par n

Exercice 35 :

La fonction indicatrice d'Euler

1. *Calculer $\varphi(8)$ et $\varphi(78)$*
   - ▷ Calcul de $\varphi(8)$
     Nous avons $8 = 2^3$; les nombres premiers avec 8 sont donc $\{1, 3, 5, 7\}$ et donc $\varphi(8) = 4$
   - ▷ Calcul de $\varphi(78)$
     Ici, nous avons $78 = 2 \times 3 \times 13$ et les nombres qui sont premiers avec 78 sont ceux dont la décomposition en un produit de facteurs premiers ne comportent ni 2, ni 3 ni 13. Ce sont donc :

$$\{1, 5, 7, 11, 17, 19, 2325, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 67, 71, 73, 77\}$$

     et donc $\varphi(78) = 24$
2. *Démontrer que p est premier si et seulement si $\varphi(p) = p - 1$*
   - ▷ Supposons p premier
     Alors, pour tout k tel que $1 \leqslant k \leqslant p-1$, $p \wedge k = 1$ et donc $\varphi(p) = p - 1$

- $\triangleright$ Réciproquement, supposons $\varphi(p) = p - 1$
  Comme $\varphi(p) \geqslant 1$, nous avons $p \geqslant 2$
  Supposons p non premier ; alors, il existe k tel que $2 \leqslant k \leqslant p - 1$ tel que k divise p, c'est à dire que $p = kp'$ et donc $k = p \wedge k$, et donc $\varphi(p) < p - 1$.
  Nous aboutissons donc à une contradiction, et donc p est premier

3. *Soit p un nombre premier supérieur ou égal à 2*

   (a) *Montrer que $k \wedge p^\alpha \neq 1 \iff p \mid k$*

   - $\triangleright$ Supposons que p divise k
     Comme p divise p^α, p divise le pgcd de p^α et k et donc $k \wedge p^\alpha \neq 1$
   - $\triangleright$ Réciproquement, supposons que $k \wedge p^\alpha \neq 1$
     Soit $d = k \wedge p^\alpha$, ce qui veut dire que $d \mid p^\alpha$; p étant un nombre premier, d est du type p^β où $\beta \leqslant \alpha$.
     Nous avons $k = dk' = p^\beta k' = p \times \left(p^{\beta-1}k'\right)$, ce qui signifie que $p \mid k$

   (b) *Démontrer qu'il y a $p^{\alpha-1}$ multiples de p entre 0 et $p^\alpha - 1$*

   Soit u un multiple de p tel que $0 \leqslant u \leqslant p^\alpha - 1$; alors $u = kp$ avec $0 \leqslant k \leqslant p^{\alpha-1} - 1$
   En effet, si $k > p^{\alpha-1} - 1$, c'est à dire $k \geqslant p^{\alpha-1}$, alors $kp \geqslant p^\alpha > p^\alpha - 1$; il y a donc contradiction
   Il y a donc $p^{\alpha-1}$ multiples de p entre 0 et $p^\alpha - 1$

   (c) *En déduire $\varphi(p^\alpha)$*

   Une autre façon d'écrire la proposition $k \wedge p^\alpha \neq 1 \iff p \mid k$ est de l'écrire :

   $$k \wedge p^\alpha = 1 \iff k \text{ n'est pas multiple de } p$$

   Ainsi, $\varphi(p^\alpha)$ compte le nombre d'éléments qui ne sont pas multiples de p compris entre 1 et $p^\alpha - 1$; il y en a donc :

   $$(p^\alpha - 1) - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1}$$

   Donc, si p est premier, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

   Remarque :Retour à la question 1.
   Nous avons $\varphi(8) = \varphi\left(2^3\right) = 2^3 - 2^2 = 4$

4. *Soient $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. On appelle $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, les éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$, tout comme on appelle $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et $\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$, ceux de $\mathbb{Z}/m\mathbb{Z}$.*

   Nous confondons, volontairement, le nombre x et sa classe $\dot{x}$. Ceci ne pénalise en rien la généralité des démonstrations. Lorsque cela sera nécessaire, nous noterons $\hat{x}_{[n]}$ la classe de x modulo n

   (a) *Pour $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, on appelle r le reste de la division de x par m. Montrer que $r \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$.*

   Comme $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, nous avons $x \wedge mn = 1$. Effectuons la division euclidienne de x par m
   Nous avons alors : $x = am + r$ où $0 \leqslant r \leqslant m - 1$
   Nous allons montrer que r est premier avec m.
   Supposons le contraire, c'est à dire qu'il existe un entier $b \geqslant 2$ divisant à la fois m et r. Alors, b divise aussi x.
   b divisant x, divisant aussi m, divise aussi mn, ce qui contredit le fait que x est premier avec mn.
   Donc, r est premier, c'est à dire $r \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$
   Il faut faire remarquer que si r est le reste de la division de x par m, alors $x \equiv r\,[m]$

   (b) *Soit :*

   $$\begin{cases} f : \mathcal{U}(\mathbb{Z}/mn\mathbb{Z}) & \longrightarrow & \mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \\ \qquad x & \longmapsto & f(x) = (r, s) = \left(\hat{x}_{[m]}, \hat{x}_{[n]}\right) \end{cases}$$

   Montrer que f est un isomorphisme de groupe multiplicatif.

- ▷ Nous allons montrer que pour tout $x \in \mathbb{Z}/mn\mathbb{Z}$, $f(x)$ n'a qu'une seule valeur bien définie
  Soient $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ et $y \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ tels que $x \equiv y\,[mn]$ *(c'est à dire que $x = y$ dans $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$)*
  Alors, nous avons $x \equiv y\,[mn] \iff x - y = k \times mn$ avec $k \in \mathbb{Z}$, et nous avons alors $x \equiv y\,[n]$ et $x \equiv y\,[m]$, c'est à dire $f(x) = f(y)$
- ▷ f est un morphisme de groupe
  Soient $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ et $y \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$; alors :

$$f(xy) = \left(\widehat{xy}_{[m]}, \widehat{xy}_{[n]}\right) = \left(\hat{x}_{[m]}\hat{y}_{[m]}, \hat{x}_{[n]}\hat{y}_{[n]}\right) = \left(\hat{x}_{[m]}, \hat{x}_{[n]}\right) \times \left(\hat{y}_{[m]}, \hat{y}_{[n]}\right) = f(x)\,f(y)$$

  Et, pour finir, $f(1) = \left(\hat{1}, \dot{1}\right)$ qui est le neutre dans $\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$
- ▷ f est injective
  Soient $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ et $y \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ tels que $f(x) = f(y)$, ce qui sous-entend que $\left(\hat{x}_{[m]}, \hat{x}_{[n]}\right) = \left(\hat{y}_{[m]}, \hat{y}_{[n]}\right)$.
  Nous avons donc $x \equiv y\,[m]$ et $x \equiv y\,[n]$, ce qui est équivalent à $x - y = km$ et $x - y = k'n$.
  Nous en déduisons donc que $km = k'n$, et comme $n \wedge m = 1$ n divise k ; il existe donc $\lambda \in \mathbb{Z}$ tels que $k = \lambda n$, et donc $x - y = \lambda(nm)$, c'est à dire $x \equiv y\,[mn]$; autrement dit, $x = y$ dans $\mathbb{Z}/mn\mathbb{Z}$, et donc $x = y$ dans $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$
  f est donc injective
- ▷ f est surjective
  Soit $\left(\hat{x}_{[m]}, \hat{y}_{[n]}\right) \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$. Existe-t-il $\lambda \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ tel que $f(\lambda) = \left(\hat{x}_{[m]}, \hat{y}_{[n]}\right)$?
  Si ce λ existe, alors, nous avons le système d'équation :

$$\begin{aligned} \lambda &\equiv x\,[m] \\ \lambda &\equiv y\,[n] \end{aligned}$$

  Comme m et n sont premiers, d'après le théorème chinois 4.4.5, il existe une seule solution à ce système, modulo mn
  Il existe donc $\lambda \in \mathbb{Z}/mn\mathbb{Z}$ tel que $f(\lambda) = \left(\hat{x}_{[m]}, \hat{x}_{[n]}\right)$
  Il reste maintenant à montrer que $\lambda \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, c'est à dire que λ est premier avec mn
  Supposons le contraire, c'est à dire que λ ne soit pas premier avec mn, c'est à dire $\lambda \wedge mn = d$ avec $d \geqslant 2$
  Soit t un entier premier qui divise d *(on peut avoir $t = d$ ou t qui qui est un diviseur premier de d)* ; alors, t divise λ et mn.
  t étant premier et divisant mn alors t divise m ou t divise n
  Supposons que t divise m.
  Comme $\lambda \equiv x\,[m]$, nous avons $\lambda - x = km \iff x = \lambda - km \iff x = t\lambda' - ktm'$, c'est à dire que t divise x, donc t est un diviseur commun à x et m, et il y a contradiction avec le fait que $x \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$, c'est à dire que $x \wedge m = 1$
  Donc, λ est premier avec mn et $\lambda \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$

f est donc un isomorphisme de groupe

(c) *En déduire que si $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ sont tels que $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\,\varphi(n)$*

Nous venons de montrer que, si m et n étaient premiers entre eux, $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ étant en bijection avec $\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$; donc :

$$\text{Card}\,\mathcal{U}(\mathbb{Z}/mn\mathbb{Z}) = \text{Card}\,\left(\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z})\right)$$

D'après les propriétés des produits cartésiens, $\text{Card}\,\left(\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z})\right) = \text{Card}\,\mathcal{U}(\mathbb{Z}/m\mathbb{Z})\,\text{Card}\,\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.
Comme $\text{Card}\,\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) = \varphi(m)$, nous avons bien, si $m \wedge n = 1$, $\varphi(mn) = \varphi(m)\,\varphi(n)$

5. *Soit $n \in \mathbb{N}^*$. Exprimer $\varphi(n)$ en fonction de la décomposition de n en un produit de facteurs premiers.*

- ▷ Tout d'abord, si $m_1, \cdots, m_k$ sont des entiers premiers dans leur ensemble, nous avons, d'après la question précédente, bien évidemment :

$$\varphi\left(\prod_{j=1}^{k} m_j\right) = \prod_{j=1}^{k} \varphi(m_j)$$

▷ Soit $n \in \mathbb{N}^*$ dont la décomposition en un produits de facteurs premiers est donnée par :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Alors :

$$\begin{aligned}
\varphi(n) &= \varphi\left(\prod_{j=1}^{k} p_j^{\alpha_j}\right) \\
&= \prod_{j=1}^{k} \varphi\left(p_j^{\alpha_j}\right) \\
&= \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right) \\
&= \prod_{j=1}^{k} p_j^{\alpha_j}\left(1 - \frac{1}{p_j}\right) \\
&= \prod_{j=1}^{k} p_j^{\alpha_j} \prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right) \\
&= n \prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right)
\end{aligned}$$

Nous avons donc $\varphi(n) = n \prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right)$

6. *Montrer que, pour $n \geqslant 3$, nous avons $\varphi(n)$ est un nombre pair*

Tout d'abord, remarquons qu'il est licite de prendre $n \geqslant 3$, puisque $\varphi(2) = 1$ et $\varphi(3) = 2$

Nous aurons besoin, pour cette question, des résultats suivants :

— Pour tout entier impair $x \in \mathbb{N}^*$ et tout entier $n \in \mathbb{N}$, x^n est un nombre impair [3]

— La différence de deux nombres impairs est un nombre pair

Soit $n \geqslant 3$ de décomposition en un produit de facteurs premiers suivante :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \prod_{j=1}^{k} p_j^{\alpha_j}$$

Alors, $\varphi(n) = \prod_{j=1}^{k}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right)$

▷ Supposons que, pour $j = 1, \cdots, k$, p_j soit un nombre premier impair.
Alors $p_j^{\alpha_j}$ et $p_j^{\alpha_j - 1}$ sont des nombres impairs ; donc, la différence $p_j^{\alpha_j} - p_j^{\alpha_j - 1}$ est un nombre pair, et donc le produit $\prod_{j=1}^{k}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right)$ est un nombre pair.

On en conclue donc que, dans ce cas, $\varphi(n)$ est un nombre pair

▷ Supposons maintenant, qu'il existe j_0 entre 1 et k tel que p_{j_0} soit un entier premier pair. La seule possibilité que nous ayons est que $p_{j_0} = 2$. Nous avons alors, en réordonnant, $n = 2^{\alpha_1} \times p_2^{\alpha_2} \cdots p_k^{\alpha_k} = 2^{\alpha_1} \prod_{j=2}^{k} p_j^{\alpha_j}$

Alors, $\varphi(n) = \left(2^{\alpha_1} - 2^{\alpha_1 - 1}\right) \prod_{j=2}^{k}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right)$.

Nous venons de montrer que $\prod_{j=2}^{k}\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right)$ était un nombre pair.

Nous avons 2^{α_1} et $2^{\alpha_1 - 1}$ qui sont des nombres pairs, et donc $\varphi(n)$ est bien un nombre pair

On vient de montrer que, pour $n \geqslant 3$, nous avons $\varphi(n)$ est un nombre pair

Exercice 36 :

Démontrer que, pour $n \geqslant 3$, $\varphi(n) \geqslant \dfrac{n \ln 2}{\ln n + \ln 2}$

3. Facile à démontrer, par le binôme de Newton

L'objet de cet exercice est de donner une évaluation de $\varphi(n)$ en fonction de n. En fait, nous ne donnerons qu'une minoration très large de $\varphi(n)$, peu signicative.
La seule chose que nous pourrions conclure c'est que $\lim\limits_{n\to+\infty} \varphi(n) = +\infty$
Soit $n \geqslant 3$ que nous écrivons par sa décomposition en un produit de facteurs premiers : $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$
où nous avons $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_k$
Ici, k désigne le nombre de facteurs premiers distincts qui entrent dans la décomposition de n.
Nous avons que $\varphi(n) = n \prod\limits_{j=1}^{k} \left(1 - \dfrac{1}{p_j}\right)$

- ▷ <u>Etudions $\prod\limits_{j=1}^{k} \left(1 - \dfrac{1}{p_j}\right)$</u>

  Nous avons, pour tout j tel que $1 \leqslant j \leqslant k$, $p_j \geqslant j+1$, et donc, $\dfrac{1}{p_j} \leqslant \dfrac{1}{j+1}$, soit $1 - \dfrac{1}{p_j} \geqslant 1 - \dfrac{1}{j+1}$, et donc, en passant au produit :

$$\prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) \geqslant \prod_{j=1}^{k} \left(1 - \frac{1}{j+1}\right)$$

  Nous avons, $1 - \dfrac{1}{j+1} = \dfrac{j}{j+1}$ et donc $\prod\limits_{j=1}^{k} \left(1 - \dfrac{1}{j+1}\right) = \prod\limits_{j=1}^{k} \left(\dfrac{j}{j+1}\right)$
  Maintenant, $\prod\limits_{j=1}^{k} \left(\dfrac{j}{j+1}\right) = \dfrac{1}{2} \times \dfrac{2}{3} \times \dfrac{3}{4} \times \cdots \times \dfrac{k-1}{k} \times \dfrac{k}{k+1} = \dfrac{1}{k+1}$
  Donc, $\prod\limits_{j=1}^{k} \left(1 - \dfrac{1}{p_j}\right) \geqslant \dfrac{1}{k+1}$ et donc $\varphi(n) \geqslant \dfrac{n}{k+1}$
- ▷ <u>Majorons k en fonction de n</u>
  Les p_j pour $1 \leqslant j \leqslant k$ étant premiers, nous avons $p_j \geqslant 2$, et donc :

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \geqslant 2^{\alpha_1 + \cdots + \alpha_k}$$

  Comme pour chaque j, $\alpha_j \geqslant 1$, nous avons $\alpha_1 + \cdots + \alpha_k \geqslant k$ et donc $n \geqslant 2^k$ et donc, $k \leqslant \dfrac{\ln n}{\ln 2}$ [4]
  Donc, $k + 1 \leqslant \dfrac{\ln n}{\ln 2} + 1 = \dfrac{\ln n + \ln 2}{\ln 2}$; et donc $\dfrac{1}{k+1} \geqslant \dfrac{\ln 2}{\ln n + \ln 2}$

De $\varphi(n) \geqslant \dfrac{n}{k+1}$, on trouve bien $\varphi(n) \geqslant \dfrac{n \ln 2}{\ln n + \ln 2}$

Exercice 37 :

On appelle $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On sait que $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$ est un groupe commutatif de cardinal $\varphi(n)$. Montrer que pour tout $a \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, nous avons $a^{\varphi(n)} = 1$

Pour ce faire, nous allons utiliser une méthode classique.
Soit une application f définie par :

$$\left\{ \begin{array}{rcl} f : \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \\ x & \longmapsto & f(x) = ax \end{array} \right.$$

1. Nous allons montrer que f est bijective
   - ▷ <u>f est injective</u>
     Soient $x \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ et $y \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ tels que $f(x) = f(y)$.
     Nous avons alors $ax = ay$; en composannt à gauche par a^{-1}, nous avons $a^{-1}(ax) = a^{-1}(ay)$; en utilisant l'associativité, nous avons $\left(a^{-1}a\right)x = \left(a^{-1}a\right)y$, c'est à dire $x = y$
     f est donc injective.

4. Il faut se rappeler que k est le nombre de facteurs premiers apparaissant dans la décomposition de n. Cette inégalité donne donc une borne pour le nombre de facteurs premiers apparaisant dans la décomposion de n. Cette borne supérieure est donc $\dfrac{\ln n}{\ln 2}$

- f est surjective
  Soit $z \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$; montrons qu'il existe $x \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ tel que $f(x) = z$
  Si cet élément $x \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ existe, alors z est tel que $ax = z$, et en composant à gauche par a^{-1}, nous obtenons $x = a^{-1}z$
  f est donc surjective

2. f étant bijective, nous avons $f(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) = \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, et donc :

$$\prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} f(x) = \prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} x \iff \prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} ax = \prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} x$$

Or, $\displaystyle\prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} ax = a^{\varphi(n)}\left(\prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} x\right)$, ce qui nous donne :

$$a^{\varphi(n)}\left(\prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} x\right) = \prod_{x\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} x$$

Et donc, $a^{\varphi(n)} = 1$ par régularité dans un groupe.

Exercice 38 :

Soit $n \in \mathbb{N}^*$; en considérant les fractions $\left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{k}{n}, \cdots, \frac{n}{n}\right\}$, montrer que :

$$n = \sum_{d|n} \varphi(d)$$

Comme proposé, nous considérons les n fractions distinctes :

$$\left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{k}{n}, \cdots, \frac{n}{n}\right\}$$

On considère les fractions $\frac{a}{d}$ irréductibles associées aux fractions $\frac{k}{n}$ pour $1 \leqslant k \leqslant n$, c'est à dire $\frac{a}{d} = \frac{k}{n}$ et $a \wedge d = 1$.
Pour chaque d divisant n, il y a $\varphi(d)$ fractions du type $\frac{a}{d}$:

$$\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_{\varphi(d)}}{d} \text{ avec } a_i \wedge d = 1 \text{ pour } 1 \leqslant i \leqslant \varphi(d)$$

En appelant $A_d = \left\{\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_{\varphi(d)}}{d}\right\}$, les A_d où $d \mid n$ forment une partition de $\left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{k}{n}, \cdots, \frac{n}{n}\right\}$, et donc, comme Card $A_d = \varphi(d)$, nous avons donc : $n = \displaystyle\sum_{d|n} \varphi(d)$

Exercice 39 :

Soit $n \in \mathbb{N}^\star$ Montrer que si $(n-1)$! est un multiple de n, alors, n n'est pas un nombre premier ; la réciproque est-elle vraie ?

1. Le théorème de Wilson 4.5.8 nous assure que si l'entier n est premier, alors $(n-1)! \equiv n-1\,[n]$, c'est à dire que le nombre $(n-1)!$ n'est pas un multiple de n.
   L'énoncé proposé est donc la contraposée du théorème de Wilson 4.5.8
2. **Réciproquement**, si n n'est pas un nombre premier, alors, n possède des diseurs propres, c'est à dire qu'il existe k et j avec $1 < k < j < n$ tels que $n = k \times j$ Or,

$$\begin{aligned}(n-1)! &= 2\times 3\times\cdots\times k\times\cdots\times j\cdots\times(n-1)\\ &= (k\times j)(2\times\cdots\times(k-1)\times(k+1)\times\cdots\times(j-1)\times(j+1)\times\cdots\times(n-1))\\ &= n\times(2\times\cdots\times(k-1)\times(k+1)\times\cdots\times(j-1)\times(j+1)\times\cdots\times(n-1))\end{aligned}$$

   n divise donc $(n-1)!$, ou encore, $(n-1)!$ est un multiple de n