Arithmétique – Partie 2 – Corrigé de la séance du 28 janvier

I. Congruence

Définition I.1 : Soient m, n deux entiers relatifs et d un entier naturel supérieur ou égal à 2. On dit que m et n sont congrus modulo d si $n - m$ est divisible par d. On note alors $n \equiv m\ [d]$

Exemple I.2 : $8 \equiv 2\ [3]$ car $8 - 2 = 6$ est divisible par 3.

Remarque I.3 : Soit a un entier relatif et b un entier relatif non nul. Il existe (division euclidienne de a par b) un unique couple $(q\,;r) \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$.
Donc $a - r = bq$ et donc $a \equiv r\ [b]$.

Remarque I.4 : Attention !
Si $a \equiv r\ [b]$,alors r n'est pas forcément le reste de la division euclidienne de a par b.

Contre-exemple I.5 :
$65 - (-5) = 70 = 7 \times 10$ donc $65 \equiv -5[7]$ mais $65 = 7 \times 10 - 5$ n'est pas la division euclidienne de 65 par 7, celle-ci étant $65 = 7 \times 9 + 2$.

Remarque I.6 : Soient m, n deux entiers relatifs et d un entier naturel supérieur ou égal à 2. Alors par définition :
$n \equiv m\ [d]$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = m + kd$.

Propriété I.7 :
Soient m, n, m', n' quatre entiers relatifs et d un entier naturel supérieur ou égal à 2.
Si $n \equiv m\ [d]$ et $n' \equiv m'\ [d]$ alors :

1) $n + n' \equiv m + m'\ [d]$
2) $nn' \equiv mm'\ [d]$
3) $\forall\, p \in \mathbb{N},\ n^p \equiv m^p\ [d]$
4) $\forall\, a \in \mathbb{Z}, an \equiv am\ [d]$

Démonstration :
Si $n \equiv m\ [d]$ et $n' \equiv m'\ [d]$ alors il existe $(k; k') \in \mathbb{Z}^2$ tels que : $\begin{cases} n = m + kd \\ n' = m' + k'd \end{cases}$.
Donc :

1) $n + n' = m + m' + (k + k')d$
   Or $k + k' \in \mathbb{Z}$ donc $n + n' \equiv m + m'\ [d]$.
2) $n \times n' = (m + kd) \times (m' + k'd) = m \times m' + (km' + k'm + kk')d$.
   Or $km' + k'm + kk' \in \mathbb{Z}$ donc $n \times n' \equiv m \times m'\ [d]$.
3) $n^p - m^p = (n - m)(n^{p-1} + n^{p-2}m + \ldots + m^{p-1})$ (Égalité de Bernouilli, voir ci-après)
   Or $n - m \equiv 0\ [d]$ et $n^{p-1} + n^{p-2}m + \ldots + m^{p-1} \in \mathbb{Z}$ donc $n^p - m^p \equiv 0\ [d]$ ie $n^p \equiv m^p\ [d]$.
4) $an = a(m + kd) = am + akd$.
   Or $ak \in \mathbb{Z}$ donc $an \equiv am\ [d]$

Remarque I.8 : Attention !
Les réciproques sont fausses.

Propriété I.9 : (égalité de Bernouilli)
Soient a, b deux nombres réels et n un entier naturel supérieur ou égal à 1.

Alors : $a^n - b^n = (a - b)\sum_{k=0}^{n-1} a^{n-k-1}b^k = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

Démonstration :

$$(a - b)\sum_{k=0}^{n-1} a^{n-k-1}b^k = a\sum_{k=0}^{n-1} a^{n-k-1}b^k - b\sum_{k=0}^{n-1} a^{n-k-1}b^k$$
$$= \sum_{k=0}^{n-1} a^{n-k}b^k - \sum_{k=0}^{n-1} a^{n-k-1}b^{k+1}$$

$$= \sum_{k=0}^{n-1} a^{n-k}b^k - \sum_{l=1}^{n} a^{n-l}b^l$$
$$= a^n + \sum_{k=1}^{n-1} a^{n-k}b^k - \sum_{l=1}^{n-1} a^{n-l}b^l - b^n$$
$$= a^n - b^n$$

Application I.10 : Puissances d'un entier
Déterminer les restes de la division par 5 des puissances de 2^n pour $n \in \mathbb{N}$.

Solution :

$$2^0 = 1 \equiv 1\,[5]$$
$$2^1 = 2 \equiv 2\,[5]$$
$$2^2 = 4 \equiv 4\,[5]$$
$$2^3 = 8 \equiv 3\,[5]$$
$$2^4 = 16 \equiv 1\,[5]$$
$$2^5 = 32 \equiv 2\,[5]$$
$$2^6 = 64 \equiv 4\,[5]$$
$$\dots$$

On constate une périodicité.
Soit $n \in \mathbb{N}$. Ce qui précède donne l'idée d'effectuer la division euclidienne de n par 4.
Il existe $q \in \mathbb{N}$ *et* $r \in \mathbb{N}$ tels que $n = 4q + r$ et $0 \leq r < 4$.
Alors :

$$2^n = 2^{4q+r} = (2^4)^q \times 2^r \equiv 1^q \times 2^r\,[5] \equiv 2^r[5]$$

On obtient synthétiquement :

r	0	1	2	3
Reste de la division de 2^{4q+r} par 5	1	2	4	3

II. Algorithme d'Euclide et PGCD de deux entiers

1. Algorithme d'Euclide

Soient a et b deux entiers. On note $D(a)$ l'ensemble des diviseurs de a et $D(a,b)$ l'ensemble des diviseurs communs de a et b.

Lemme II.1 : Si a et b sont deux entiers, alors $D(a,b) = D(|a|,|b|)$

Démonstration : Il s'agit de prouver une égalité ensembliste. Nous allons procéder par double inclusion.

⊂ Soit $d \in D(a,b)$.
En particulier, d divise a donc d divise $\pm a$ et donc d divise $|a|$
De même, d divise $|b|$.
Donc $d \in D(|a|,|b|)$.

⊃ Raisonnement similaire, laissé au lecteur.

Remarque II.2 : ce lemme permet de limiter la recherche des diviseurs communs de deux nombres entiers à ceux de leurs valeurs absolues, c'est-à-dire de deux nombres entiers naturels.

Lemme II.3 : Si a et b sont deux entiers naturels avec $b > 0$ et si r désigne le reste de la division euclidienne de a par b, alors $D(a,b) = D(b,r)$.

Démonstration : Également par double inclusion.
Notons q le quotient de la division euclidienne de a par b, de sorte que $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$.

⊂ Soit $d \in D(a,b)$.
Alors d divise a et b.
De plus $r = a - bq$ donc d divise r.
Donc $d \in D(b,r)$.

⊃ Raisonnement similaire, laissé au lecteur.

Remarque II.4 : ce lemme permet de remplacer la recherche des diviseurs communs de a et b à ceux de b et r, avec $0 \leq r < |b|$.

Lemme II.5 : Si a est entier, alors $D(a,0) = D(a)$

Démonstration : Également par double inclusion, laissée au lecteur.

Remarque II.6 : ce lemme permet de conclure si un des deux entiers est nul.

Application II.7 : algorithme d'Euclide
Soient a et b deux entiers.
Notons $r_0 = |a|$ et $r_1 = |b|$. D'après le lemme II.1 : $D(a,b) = D(r_0, r_1)$.

- Étape 1 :
  - Si $r_1 = 0$, alors $D(r_0, r_1) = D(r_0)$ d'après le lemme II.5.
  - Sinon, on effectue la division de r_0 par r_1 : $\exists!\ (q_1\ ;r_2)\ \in \mathbb{N}^2$ tel que $\begin{cases} r_0 = r_1 q_1 + r_2 \\ 0 \leq r_2 < r_1 \end{cases}$.
    On a alors d'après le lemme II.3 : $D(r_0, r_1) = D(r_1, r_2)$.

- Étape 2 :
  - Si $r_2 = 0$, alors $D(r_1, r_2) = D(r_1)$ d'après le lemme II.5.
  - Sinon, on effectue la division de r_1 par r_2 : $\exists!\ (q_2\ ;r_3)\ \in \mathbb{N}^2$ tel que $\begin{cases} r_1 = r_2 q_2 + r_3 \\ 0 \leq r_3 < r_2 \end{cases}$.
    On a alors d'après le lemme II.3 : $D(r_1, r_2) = D(r_2, r_3)$.

…
On obtient une suite d'entiers naturels $(r_k)_{k\geq 0}$ strictement décroissante, donc $\exists N \geq 0$ tel que $r_N \neq 0$ et $r_{N+1} = 0$.
De plus $D(r_0, r_1) = D(r_1, r_2) = D(r_2, r_3) = \cdots = D(r_N, r_{N+1}) = D(r_N)$.

Exemple II.8 : Chercher avec l'algorithme d'Euclide les diviseurs communs de 56 et 12.

Solution :
- $56 = 4 \times 12 + 8$, donc $D(56,12) = D(12,8)$.
- $12 = 1 \times 8 + 4$, donc $D(12,8) = D(8,4)$.
- $8 = 2 \times 4 + 0$, donc $D(8,4) = D(4,0)$.
- D'après le lemme II.5, $D(4,0) = D(4)$.

Conclusion : les diviseurs communs de 56 et 12 sont ceux de 4, c'est-à-dire $\pm 1, \pm 2, \pm 4$.

2. PGCD de deux entiers

Propriété II.9 :
Soient a et b deux entiers.
Alors il existe un unique entier naturel, noté $a \wedge b$ (ou $PGCD(a\ ;b)$) appelé plus grand commun diviseur de a et b tel que :
1) $a \wedge b$ divise a et b
2) Tout diviseur de a et b divise $a \wedge b$
De plus, ce PGCD, nul si a et b sont nuls, est, dans tous les autres cas, égal au dernier reste non nul dans l'algorithme d'Euclide appliqué à $|a|$et $|b|$.

Démonstration : On suppose a et b non nuls.
- Unicité : Soient d et d' deux entiers naturels vérifiant 1) et 2).
D'après 1), d est un diviseur commun de a et b, donc d'après 2), d divise d'.
De même d' divise d.
Comme d et d' sont positifs, alors $d = d'$.
- Existence : Notons r_N le dernier reste non nul dans l'algorithme d'Euclide appliqué à $|a|$et $|b|$.
C'est un entier naturel et d'après les lemmes précédents : $D(a,b) = D(|a|,|b|) = D(r_N)$. Donc :
  - r_N divise a et b
  - Tout diviseur de a et b divise r_N

  Par unicité $r_N = a \wedge b$.

Exemple II.10 : Déterminer le PGCD de 2952 et 516.

Solution :

$$2952 = 516 \times 5 + 372$$
$$516 = 372 \times 1 + 144$$

$$372 = 144 \times 2 + 84$$
$$144 = 84 \times 1 + 60$$
$$84 = 60 \times 1 + 24$$
$$60 = 24 \times 2 + 12$$
$$24 = 12 \times 2 + 0$$

Donc $2952 \wedge 516 = 12$.

3. Égalité de Bézout

Propriété II.11 : Soient a et b deux entiers.
Alors il existe deux entiers u et v (mais pas nécessairement uniques) tels que : $au + bv = a \wedge b$

Démonstration : on reprend les notations utilisées pour l'algorithme d'Euclide avec $r_0 = |a|$ et $r_1 = |b|$. On a :

(0) $u_0 a + v_0 b = r_0$, avec $u_0 = \pm 1$ et $v_0 = 0$
(1) $u_1 a + v_1 b = r_1$, avec $u_1 = 0$ et $v_1 = \pm 1$

On écrit $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 < r_1$, puis l'égalité $(2) = (0) - q_1 \times (1)$:

(2) $u_0 a + v_0 b - q_1 \times (u_1 a + v_1 b) = r_0 - q_1 r_1$
Soit : $(u_0 - q_1 u_1)a + (v_0 - q_1 v_1)b = r_0 - q_1 r_1$
On obtient : $u_2 a + v_2 b = r_2$, avec : $u_2 = u_0 - q_1 u_1$ et $v_2 = v_0 - q_1 v_1$

On écrit $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 < r_1$, puis l'égalité $(3) = (1) - q_2 \times (2)$:

(3) $u_1 a + v_1 b - q_2 \times (u_2 a + v_2 b) = r_1 - q_2 r_2$
Soit : $(u_1 - q_2 u_2)a + (v_1 - q_2 v_2)b = r_1 - q_2 r_2$
On obtient : $u_3 a + v_3 b = r_3$, avec : $u_3 = u_1 - q_2 u_2$ et $v_3 = v_1 - q_2 v_2$

On poursuit le processus jusqu'au premier reste nul : $r_{N-1} = q_N r_N + 0$
On a alors $r_N = a \wedge b$ et l'égalité (N) :

(N) $u_N a + v_N b = r_N$, avec : $u_N = u_{N-2} - q_{N-1} u_{N-1}$ et $v_N = v_{N-2} - q_{N-1} v_{N-1}$.

Remarque II.13 : La démonstration peut paraître ardue, en raison des notations, mais le principe est très simple : il s'agit simplement de « remonter l'algorithme d'Euclide » à partir du dernier reste non nul, comme nous allons l'illustrer avec l'exemple ci-dessous.

Exemple II.14 : Chercher une solution particulière de $2952 \times u + 516 \times v = 12$.

Solution :

$$2952 = 516 \times 5 + 372 \quad (1)$$
$$516 = 372 \times 1 + 144 \quad (2)$$
$$372 = 144 \times 2 + 84 \quad (3)$$
$$144 = 84 \times 1 + 60 \quad (4)$$
$$84 = 60 \times 1 + 24 \quad (5)$$
$$60 = 24 \times 2 + 12 \quad (6)$$
$$24 = 12 \times 2 + 0 \quad \text{STOP}$$

Donc, comme déjà vu, $2952 \wedge 516 = 12$. De plus :

$12 = 60 - 24 \times 2$ — 12 est exprimé par (6)
$= 60 - (84 - 60 \times 1) \times 2$ — 24 est exprimé par (5)
$= 60 \times 3 - 84 \times 2$ — Réduction
$= (144 - 84 \times 1) \times 3 - 84 \times 2$ — 60 est exprimé par (4)
$= 144 \times 3 - 84 \times 5$ — Réduction
$= 144 \times 3 - (372 - 144 \times 2) \times 5$ — 84 est exprimé par (3)
$= 144 \times 13 - 372 \times 5$ — Réduction
$= (516 - 372 \times 1) \times 13 - 372 \times 5$ — 144 est exprimé par (2)
$= 516 \times 13 - 372 \times 18$ — Réduction
$= 516 \times 13 - (2952 - 516 \times 5) \times 18$ — 372 est exprimé par (1)
$= 516 \times 103 - 2952 \times 18$ — Réduction

Conclusion : $12 = 2952 \times u + 516 \times v$ avec $u = -18$ et $v = 103$.

4. Propriétés de base

Propriété II.15 : (homogénéité du PGCD)
Soient a, b et p trois entiers.
Alors $(pa) \wedge (pb) = |p| a \wedge b$

Démonstration : Si $p = 0$, le résultat est trivial. On suppose donc p non nul.

- $a \wedge b$ divise a et b, donc $|p| a \wedge b$ divise pa et pb.

Donc $|p| a \wedge b$ divise $(pa) \wedge (pb)$.

- p divise pa et pb, donc p divise $(pa) \wedge (pb)$

Ainsi $\frac{(pa)\wedge(pb)}{|p|}$ est entier.
Comme $(pa) \wedge (pb)$ divise pa et pb, $\frac{(pa)\wedge(pb)}{|p|}$ divise par conséquent a et b, donc aussi $a \wedge b$.
Donc $(pa) \wedge (pb)$ divise $|p| a \wedge b$.

Comme $(pa) \wedge (pb)$ et $|p| a \wedge b$ sont positifs, on en déduit que $(pa) \wedge (pb) = |p| a \wedge b$.

Propriété II.16 : (associativité du PGCD)
Soient a, b et c trois entiers.
Alors $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
De plus, c'est l'unique nombre entier naturel, noté $a \wedge b \wedge c$, appelé PGCD de a, b et c, tel que :
1) $a \wedge b \wedge c$ divise a, b et c
2) tout diviseur de a, b et c divise $a \wedge b \wedge c$

Démonstration :

- $(a \wedge b) \wedge c$ divise $a \wedge b$ et c, donc divise a, b et c, et donc divise a et $b \wedge c$.
  Donc $(a \wedge b) \wedge c$ divise $a \wedge (b \wedge c)$.
  De même $a \wedge (b \wedge c)$ divise $(a \wedge b) \wedge c$.
  Ces deux nombres étant des entiers naturels, on a donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
- Le point précédent a déjà établi que $a \wedge b \wedge c$ divise a, b et c.
- Soit maintenant d un diviseur de a, b et c.
  Alors il divise $a \wedge b$ et c, donc divise $a \wedge b \wedge c$.
- Si d et d' sont deux PGCD de a, b et c, alors comme d divise a, b et c, donc divise leur PGCD d'.
  De même, d' divise d.
  Ces deux nombres étant des entiers naturels, on en déduit que $d = d'$.

Exemple II.17 :
La propriété fournit la méthode pour déterminer le PGCD de trois nombres, par exemple avec l'égalité $a \wedge b \wedge c = (a \wedge b) \wedge c$. On a déjà vu que $2952 \wedge 516 = 12$, donc $2952 \wedge 516 \wedge 8 = (2952 \wedge 516) \wedge 8 = 12 \wedge 8 = 4$.

Propriété II.18 : Soient a et b deux entiers.
1) $a \wedge a = a$
2) $a \wedge b = b \wedge a$
3) Soit k un entier naturel non nul. Si k divise a et b, alors $\frac{a}{k} \wedge \frac{b}{k} = \frac{1}{k} a \wedge b$.
4) Soit q un entier relatif, alors $a \wedge b = (a - bq) \wedge b$

Démonstration : (dernier point uniquement, les trois autres sont laissées au lecteur)
Soit $d = a \wedge b$ et $d' = (a - bq) \wedge b$

- d divise a et d divise b donc d divise $a - bq$ (combinaison linéaire de a et b)

Donc d est un diviseur commun à $a - bq$ et à b.
Ainsi d divise d'.

- d' divise $a - bq$ et d' divise b donc d' divise $a - bq + bq = a$.

Donc d' est un diviseur commun à a et b.
Ainsi d' divise d.
Comme d et d' sont positifs, $d = d'$.

III. Nombres premiers entre eux

1. Généralités

Définition III.1 :
Deux nombres entiers a et b sont dits premiers entre eux si et seulement si $a \wedge b = 1$

Propriété III.4 : Soient a et b deux entiers.
Si $a \wedge b = d$, alors les nombres $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

Démonstration :
C'est quasiment immédiat : $\frac{a}{d} \wedge \frac{b}{d} = \frac{1}{d} a \wedge b = \frac{1}{d} \times d = 1$.

2. Théorème de Bézout (1730-1783)

Théorème III.5 :
$a \wedge b = 1 \Leftrightarrow \exists (u; v) \in \mathbb{Z}^2$ tels que $au + bv = 1$

Démonstration :
$\Rightarrow$ Si $a \wedge b = 1$, on a déjà vu qu'il existe une égalité de Bézout en remontant l'algorithme d'Euclide, c'est-à-dire :
$\exists (u; v) \in \mathbb{Z}^2$ tels que $au + bv = 1$

$\Leftarrow$ Si $\exists (u; v) \in \mathbb{Z}^2$ tels que $au + bv = 1$, notons $d = a \wedge b$.
Alors d divise a, donc divise au.
De même, d divise b, donc divise bv.
Ainsi, d divise $au + bv = 1$.
Comme d est positif, alors $d = 1$.

Corollaire III.6 :
a est premier avec b et avec c si et seulement si a est premier avec le produit bc.

Démonstration :
- Supposons que $a \wedge b = 1$ et que $a \wedge c = 1$.

Alors $\exists (u; v) \in \mathbb{Z}^2$ tels que $au + bv = 1$
Et $\exists (w; x) \in \mathbb{Z}^2$ tels que $aw + cx = 1$
Ainsi, en multipliant : $(au + bv)(aw + cx) = 1$
On développe et on factorise ainsi : $a(auw + ucx + bvw) + bc(vx) = 1$.
Or $auw + ucx + bvw$ et vx sont entiers, donc d'après le théorème de Bézout : a est premier avec le produit bc.
- Réciproquement, si a est premier avec le produit bc, alors $\exists (u; v) \in \mathbb{Z}^2$ tels que $au + bcv = 1$

En écrivant $au + b(cv) = 1$ et comme u et cv sont entiers, a et b sont premiers entre eux d'après le théorème de Bézout. De même, en écrivant $au + c(bv) = 1$, on obtient que a et c sont premiers entre eux.

3. Théorème de Gauss

Théorème III.7 :
Soit a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration 1 :
$a \wedge b = 1$ donc $(ac) \wedge (bc) = |c| a \wedge b = |c|$.
Or, a divise ac et a divise bc, a divise $(ac) \wedge (bc) = |c|$
Donc a divise c.

Démonstration 2 :
$a \wedge b = 1$ donc d'après le théorème de Bézout : $\exists (u; v) \in \mathbb{Z}^2$ tels que $au + bv = 1$
Donc $auc + bvc = c$.
Or a divise bc donc divise bvc.
Comme a divise aussi auc, alors a divise $auc + bvc = c$.

Corollaire III.8 :
Soient a, b, c, d quatre entiers non nuls, avec $d \geq 2$.
Si $ac \equiv bc\ [d]$ et si c et d sont premiers entre eux, alors $a \equiv b\ [d]$.

Démonstration :
$ac \equiv bc\ [d]$ donc il existe $k \in \mathbb{Z}$ tel que $(a - b)c = kd$.
Or d divise $(a - b)c$ et d est premier avec c donc d'après le théorème de Gauss, d divise $a - b$.
Autrement dit, $a \equiv b\ [d]$.

Exercice III.9 : (lemme chinois)

Soit p et q deux nombres premiers entre eux et soient $(a; b) \in \mathbb{N}^2$ tels que $0 \leq a < p$ et $0 \leq b < q$.

1. Montrer qu'il existe $n_0 \in \mathbb{Z}$ tel que $\begin{cases} n_0 \equiv a[p] \\ n_0 \equiv b[q] \end{cases}$. On pourra raisonner par analyse/synthèse.
2. Exprimer en fonction de n_0 l'ensemble des solutions $n \in \mathbb{Z}$ du système $\begin{cases} n \equiv a[p] \\ n \equiv b[q] \end{cases}$. On pourra raisonner par analyse/synthèse.
3. Déterminer l'ensemble des solutions entières du système $\begin{cases} n \equiv 9[17] \\ n \equiv 3[5] \end{cases}$

Solution :

1. Analyse : supposons qu'il existe $n_0 \in \mathbb{Z}$ tel que $\begin{cases} n_0 \equiv a[p] \\ n_0 \equiv b[q] \end{cases}$.
   Alors $\exists u_0 \in \mathbb{Z}$ tel que $n_0 = u_0 p + a$ et $\exists v_0 \in \mathbb{Z}$ tel que $n_0 = v_0 q + b$.
   Donc $u_0 p - v_0 q = b - a$.
   Or, p et q sont premiers entre eux donc $\exists (u_1; v_1) \in \mathbb{Z}^2$ tels que $pu_1 + qv_1 = 1$.
   Donc $pu_1(b - a) + qv_1(b - a) = b - a$, c'est-à-dire $u_1(b - a)p + a = v_1(a - b)q + b$.

   Synthèse : posons $u_0 = u_1(b - a)$, $v_0 = v_1(a - b)$ et $n_0 = u_0 p + a$.
   Ces trois nombres sont entiers et on a bien $n_0 \equiv a[p]$.
   De plus :
   $v_0 q + b = v_1(a - b)q + b = v_1 q(a - b) + b = (1 - pu_1)(a - b) + b = a - b + pu_1(b - a) + b = u_0 p + a = n_0$.

   Donc $n_0 \equiv b[q]$.

2. Analyse : soit $n \in \mathbb{Z}$ une solution du système $\begin{cases} n \equiv a[p] \\ n \equiv b[q] \end{cases}$.

   Alors $\exists (u; v) \in \mathbb{Z}^2$ tel que $n = up + a = vq + b$.
   Or $n_0 = u_0 p + a = v_0 q + b$ donc $n - n_0 = (u - u_0)p = (v - v_0)q$.
   Donc p divise $(v - v_0)q$ et comme p et q sont premiers entre eux, alors p divise $v - v_0$ d'après le théorème de Gauss.
   Ainsi, il existe $k \in \mathbb{Z}$ tel que $v - v_0 = kp$ donc $(u - u_0)p = kpq$ d'où $u - u_0 = kq$
   On obtient donc $n - n_0 = kpq$, ou encore $n = n_0 + kqp$.

   Synthèse : réciproquement, s'il existe $k \in \mathbb{Z}$ tel que $n = n_0 + kqp$, alors $\begin{cases} n \equiv n_0[p] \equiv a[p] \\ n \equiv n_0[q] \equiv b[q] \end{cases}$.

3. On applique la méthode utilisée pour les questions précédentes en cherchant une solution particulière n_0 du système.
   On vérifie d'abord que 17 et 5 sont premiers entre eux (ici, c'est trivial car 17 et 5 sont deux nombres premiers distincts) puis on cherche $(u_1; v_1) \in \mathbb{Z}^2$ tels que $17u_1 + 5v_1 = 1$. Pour cela, on applique l'algorithme d'Euclide :

   $17 = 5 \times 3 + 2$ *(1)*
   $5 = 2 \times 2 + 1$ *(2)*
   $2 = 2 \times 1 + 0$ *STOP*

   On le remonte pour trouver l'égalité de Bézout :

   $1 = 5 - 2 \times 2$ *1 est exprimé par (2)*
   $= 5 - (17 - 5 \times 3) \times 2$ *24 est exprimé par (1)*
   $= 17 \times (-2) + 5 \times 7$ *Réduction*

   Posons alors $n_0 = v_0 q + b = v_1(a - b)q + b = 7 \times (9 - 3) \times 5 + 3 = 213$.

   On a bien : $\begin{cases} 213 = 12 \times 17 + 9 \equiv 9[17] \\ 213 = 42 \times 5 + 3 \equiv 3[5] \end{cases}$.

   De plus, $n \in \mathbb{Z}$ vérifie le système si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = n_0 + kqp = 213 + 85k$.

Exercice III.10 (Théorème de Wilson)

L'objectif de cet exercice est de démontrer le théorème de Wilson :

Soit p un entier naturel strictement supérieur à 1. Alors :

$$p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1\ [p]$$

1. Prouver le sens indirect.
2. Pour le sens direct :
   a. Vérifier que la propriété est vraie pour $p = 2$ et $p = 3$.
   b. Soit p un nombre premier supérieur ou égal à 5 et soit q un entier naturel compris entre 2 et $p-2$. Justifier qu'il existe des entiers α et β tels que $\alpha q + \beta p = 1$.
   c. Soit r le reste de la division de α par p.
      i. Montrer que $rq \equiv 1\ [p]$.
      ii. Vérifier que $2 \leq r \leq p-2$.
      iii. Montrer qu'à chaque entier q compris 2 et $(p-2)$, on peut associer de manière unique un entier r compris entre 2 et $(p-2)$ tel que $rq \equiv 1\ [p]$. On pourra raisonner par l'absurde.
   d. Conclure.

Solution :

1. Si $(p-1)! \equiv -1\ [p]$ alors $\exists\, k \in \mathbb{Z}$ tel que $(p-1)! + 1 = kp$ donc $kp - (p-1)! = 1$

D'après le théorème de Bézout, $(p-1)!$ et p sont premiers entre eux.
Ainsi p est premier avec tous les entiers naturels non nuls qui lui sont inférieurs.
Donc p est premier.

2. Soit p un nombre premier.
   a. Si $p = 2$ ou $p = 3$, le résultat est trivial.
   b. Soit p un nombre premier supérieur ou égal à 5 et soit q un entier naturel compris entre 2 et $p-2$.

p est premier donc p et q sont premiers entre eux.
D'après le théorème de Bézout, il existe α et β entiers relatifs tels que $\alpha q + \beta p = 1$.

   c. Soit r le reste de la division de α par p.
      i. $\alpha q + \beta p = 1 \Rightarrow \alpha q \equiv 1[p] \Rightarrow rq \equiv 1[p]$
      ii. r le reste de la division de α par p, donc $0 \leq r \leq p-1$.

- Si $r = 0$, alors $rq \equiv 1[p] \Rightarrow 0 \equiv 1[p]$, impossible.
- Si $r = 1$, alors $rq \equiv 1[p] \Rightarrow q \equiv 1[p]$, donc p divise $q - 1 \leq p - 3$, impossible.
- Si $r = p-1$, alors $(p-1)q \equiv 1[p] \Rightarrow -q \equiv 1[p]$, donc p divise $q + 1 \leq p - 1$, impossible.

Donc $2 \leq r \leq p-2$.

      iii. Soit q et q' deux entiers distincts compris 2 et $(p-2)$.

Raisonnons par l'absurde en supposant qu'il existe un entier r tel que $2 \leq r \leq p-2$ et $\begin{cases} rq \equiv 1\ [p] \\ rq' \equiv 1\ [p] \end{cases}$.

Alors $r(q-q') \equiv 0\ [p]$.
Or $-p + 2 < q - q' < p - 2$ et $p \in \mathbb{P}$ donc p et $(q-q')$ sont premiers entre eux.
D'après le théorème de Gauss, p divise r, absurde.

Donc, à chaque entier q compris 2 et $(p-2)$, on peut associer de manière unique un entier r compris entre 2 et $(p-2)$ tel que $rq \equiv 1\ [p]$.

   d. Les entiers de 2 à $p-2$ peuvent être regroupés en couples de produit congru à 1 modulo p (un nombre ne peut être associé à lui-même).

Ainsi $(p-1)! = (p-2)! \times (p-1) \equiv 1 \times (p-1)\ [p] \equiv -1\ [p]$.