Arithmétique – Partie 2 – Corrigé de la séance du 22 janvier

Ce cours fait suite à celui du 20 novembre 2024, dispensé par Johan Monteillet, voir les documents relatifs à cette première séance pour les prérequis (divisibilité dans $\mathbb{Z}$, nombres premiers et division euclidienne).

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 :

$$\begin{aligned} 2952 &= 516 \times 5 + 372 \\ 516 &= 372 \times 1 + 144 \\ 372 &= 144 \times 2 + 84 \\ 144 &= 84 \times 1 + 60 \\ 84 &= 60 \times 1 + 24 \\ 60 &= 24 \times 2 + 12 \\ 24 &= 12 \times 2 + 0 \end{aligned}$$

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 :

$2952 = 516 \times 5 + 372$	*(1)*
$516 = 372 \times 1 + 144$	*(2)*
$372 = 144 \times 2 + 84$	*(3)*
$144 = 84 \times 1 + 60$	*(4)*
$84 = 60 \times 1 + 24$	*(5)*
$60 = 24 \times 2 + 12$	*(6)*
$24 = 12 \times 2 + 0$	*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. Prochaine séance (5 mars).

4. Résolution dans $\mathbb{Z}$ de l'équation diophantienne $au + bv = c$ (a, b, c donnés)

Dans ce paragraphe, on considère trois entiers a, b, c avec $a \neq 0$ et $b \neq 0$.

Existence de solutions éventuelles :

- Supposons que l'équation ait au moins une solution $(u; v) \in \mathbb{Z}^2$.

$a \wedge b$ divise a et b, donc $a \wedge b$ divise $au + bv = c$.
Donc $a \wedge b$ divise c.

- Réciproquement, si $a \wedge b$ divise c, alors il existe $k \in \mathbb{Z}$ tel que $c = k(a \wedge b)$.

De plus : $\exists (u_0; v_0) \in \mathbb{Z}^2$ tels que $au_0 + bv_0 = a \wedge b$.
Donc $c = k(au_0 + bv_0) = a(ku_0) + b(kv_0)$.
Ainsi, puisque ku_0 et kv_0 sont entiers, $(ku_0; kv_0)$ est une solution particulière de l'équation.

On a obtenu le résultat suivant :

Il existe $(u; v) \in \mathbb{Z}^2$ tel que $au + bv = c$ si et seulement si $a \wedge b$ divise c.

Recherche de l'ensemble des solutions :

S'il existe des solutions, alors $d = a \wedge b$ divise a, b et c, donc il existe trois entiers a', b' et c' tels que $a = da'$, $b = db'$ et $c = dc'$ et on peut diviser l'équation par d : $\frac{a}{d}u + \frac{b}{d}v = \frac{c}{d}$ ie $a'u + b'v = c'$.

De plus, on a déjà vu dans les généralités de cette partie que $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont premiers entre eux.

Autrement dit, en divisant l'équation initiale par $a \wedge b$, on se ramène à l'équation $a'u + b'v = c'$ avec $a' \wedge b' = 1$.

Soit alors $(u_0\,; v_0)$ une solution particulière de cette équation, de sorte que $a'u_0 + b'v_0 = c'$.
Considérons maintenant une autre solution $(u\,; v)$: $a'u + b'v = c'$.
Par différence, on obtient : $a'(u - u_0) + b'(v - v_0) = 0$, ce qui équivaut à $a'(u - u_0) = b'(v_0 - v)$.
Donc a' divise $b'(v_0 - v)$. Comme $a' \wedge b' = 1$, a' divise $v_0 - v$ d'après le théorème de Gauss.
Ainsi il existe $k \in \mathbb{Z}$ tel que $ka' = v_0 - v$.
Donc en reportant dans l'équation : $a'(u - u_0) = b'ka'$.
Comme $a' \neq 0$, cette dernière égalité équivaut à $u - u_0 = b'k$.
En résumé, il existe $k \in \mathbb{Z}$ tel que $ka' = v_0 - v$ et $u - u_0 = b'k$, c'est-à-dire $v = v_0 - ka'$ et $u = u_0 + kb'$.
Réciproquement, tout couple $(u\,; v)$ de cette forme vérifie l'équation $a'u + b'v = c'$.

En résumé :

Les solutions $(u; v) \in \mathbb{Z}^2$ de l'équation diophantienne $a'u + b'v = c'$avec $a' \wedge b' = 1$ sont de la forme $u = u_0 + kb'$ et $v = v_0 - ka'$, où $(u_0\,; v_0)$ est une solution particulière l'équation et $k \in \mathbb{Z}$.

Exemples :

- $2x + 8y = 5$ n'admet pas de solution dans $\mathbb{Z}^2$ car $2 \wedge 8 = 2$ ne divise pas 5.
- Résoudre l'équation diophantienne $6x + 4y = 10$.

Solution :
On remarque que : $6x + 4y = 10 \Leftrightarrow 3x + 2y = 5$

Solution particulière évidente (si on en voit pas, on utilise l'algorithme d'Euclide, comme dans la partie II) : $(1;1)$.

On a : $\left.\begin{matrix} 3x + 2y = 5 \\ 3 \times 1 + 2 \times 1 = 5 \end{matrix}\right\}$ donc $3x + 2y = 3 \times 1 + 2 \times 1$.
Ainsi $3(x-1) = 2(1-y)$ (*)
Donc 3 divise $2(1-y)$.
De plus $3 \wedge 2 = 1$.
D'après le théorème de Gauss, 3 divise $(1-y)$.
Il existe donc $k \in \mathbb{Z}$ tel que $1 - y = 3k$ soit $y = 1 - 3k$.
On reporte dans (*) : $3(x-1) = 2(1-y) \Leftrightarrow 3(x-1) = 2 \times 3k \Leftrightarrow x - 1 = 2k \Leftrightarrow x = 2k + 1$

Réciproquement, les couples de la forme $(2k+1; 1-3k)$ vérifient l'équation.

Les solutions de $6x + 4y = 10$ sont donc de la forme $(2k+1; 1-3k)$ avec $k \in \mathbb{Z}$.

IV. Petit théorème de Fermat

Théorème IV-1 :
Soit a un entier relatif et p un nombre premier.
Si p ne divise pas a, alors $a^{p-1} \equiv 1\ [p]$

Démonstration : Prochaine séance (5 mars).

Remarque IV.2 : Attention !
La réciproque du petit théorème de Fermat est fausse, c'est-à-dire que si $a^{p-1} \equiv 1\ [p]$, avec p ne divisant pas, alors p n'est pas nécessairement premier

Contre-exemple : $a = 7$ et $p = 6$.
On a bien $7^5 = 16807 = 2801 \times 6 + 1 \equiv 1[6]$ et 6 n'est pas premier.

Corollaire IV.3 :
Si p est un nombre premier, alors pour tout entier a : $a^p \equiv a\ [p]$

Démonstration : Prochaine séance (5 mars).

V. Quelques extraits du concours général

Exercice V.1 : (logarithme discret)
Si m_1 et m_2 sont deux entiers tels que $m_1 \leq m_2$, on désigne par $[\![m1\ , m2]\!]$ l'ensemble des entiers k tels que $m_1 \leq k \leq m_2$.

Si a ,b et n sont trois entiers, on note $a \equiv b\ [n]$ lorsque a et b sont congrus modulo n, c'est-à-dire lorsque $b - a$ est multiple de n.

Dans tout cet exercice, p désigne un nombre premier.

Pour tout $A \in \mathbb{N}$, on note $(A\ mod\ p)$ le reste de la division euclidienne de A par p. C'est l'unique entier de $[\![0\ , p-1]\!]$ congru à A modulo p.

Un entier $x \in [\![1\ , p-1]\!]$ est appelé racine primitive modulo p lorsque l'ensemble des $(x^k\ mod\ p)$, pour $k \in \mathbb{N}$ est l'ensemble $[\![1\ , p-1]\!]$, c'est-à-dire lorsque les puissances de x, calculées modulo p, décrivent $[\![1\ , p-1]\!]$ tout entier.

Ainsi, pour $p = 5$:

- 1 n'est pas une racine primitive modulo 5 puisque toutes ses puissances valent 1.
- 2 est une racine primitive modulo 5 puisque : $(2^0 \ mod \ 5) = 1$; $(2^1 \ mod \ 5) = 2$; $(2^2 \ mod \ 5) = 4$ et $(2^3 \ mod \ 5) = 3$
- De même 3 est une racine primitive modulo 5 et 4 n'en est pas une.

1. On prend dans cette question $p = 7$. Déterminer les racines primitives modulo 7.

On admet désormais que, quel que soit le nombre premier p, il existe au moins une racine primitive modulo p. Dans la suite, on désigne par g une racine primitive modulo p.

2. a. Montrer que l'ensemble des $(g^k \ mod \ p)$ pour $k \in [\![0\,, p-2]\!]$ est $[\![1\,, p-1]\!]$.
   b. Soit $A \in [\![1\,, p-1]\!]$. Justifier l'existence et l'unicité d'un entier $a \in [\![0\,, p-2]\!]$ tel que $A = (g^a \ mod \ p)$.
   On dit que a est le logarithme de base g modulo p de A.
   c. Soit b un entier naturel congru à a modulo $p-1$. Calculer $(g^b \ mod \ p)$.

Solution : **à chercher pour la prochaine séance (5 mars). Indice pour la question 2a : utiliser le petit théorème de Fermat (théorème IV-1).**

Exercice V.2 : (nombres pointus, session 2020)

1 Problème 1 : Nombres pointus

Soit n un entier naturel non nul. On dit que n est pointu si n admet au plus un facteur premier ou bien si, en notant p et q les deux plus grands facteurs premiers de n, avec $p > q$, l'inégalité $p \geqslant 2q$ est vérifiée.
Par exemple, 1 est pointu, car il n'a aucun facteur premier. De même, 25 est pointu, car il n'a qu'un seul facteur premier, et 147 est pointu, car $147 = 3 \times 7^2$ et $7 \geqslant 2 \times 3$. Au contraire, 105 n'est pas pointu, puisque $105 = 3 \times 5 \times 7$ et $7 < 2 \times 5$.
Dans ce problème, on cherche à démontrer qu'il existe des suites arbitrairement longues d'entiers consécutifs pointus. Plus précisément, on souhaite démontrer la propriété $\mathscr{P}$ suivante :

Pour tout entier $m \geqslant 1$, il existe un entier $n \geqslant 0$ tel que les nombres $n+1, n+2, \ldots, n+m$ soient tous pointus.

1.1 Quelques exemples

1. Le nombre 2020 est-il pointu ?
2. Quel est le plus petit entier naturel non nul qui ne soit pas pointu ?
3. Quel est le plus petit nombre pointu possédant au moins quatre facteurs premiers distincts ?
4. Démontrer qu'il existe une infinité de nombres pointus.
5. Démontrer qu'il existe une infinité d'entiers naturels non nuls qui ne sont pas pointus.
6. Établir la liste des nombres pointus entre 1 et 20 inclus. Quelle est la longueur maximale d'une suite de nombres pointus consécutifs entre 1 et 20 ?

1.2 Peu de grands nombres premiers

On pose $0! = 1$, et $\ell! = 1 \times 2 \times \cdots \times \ell = \ell(\ell-1)!$ pour tout entier $\ell \geqslant 1$. Soient alors k et n deux entiers naturels tels que $k \leqslant n$. On s'intéresse à la fraction

$$\frac{n!}{k!(n-k)!}$$

que l'on note $F_{n,k}$.

7. a. Calculer les valeurs des nombres $F_{3,1}$ et $F_{9,4}$.

b. Démontrer que, si $k = 0$ ou $k = n$, alors $F_{n,k} = 1$.

c. Démontrer que, si $1 \leqslant k \leqslant n-1$, alors $F_{n,k} = F_{n-1,k} + F_{n-1,k-1}$

d. En déduire que, pour tout entier naturel n et pour tout entier naturel $k \leqslant n$, $F_{n,k}$ est un entier naturel non nul inférieur ou égal à 2^n.

Dans cette question et dans les parties qui suivent, pour tout entier naturel n, on note $\mathbb{P}_n$ l'ensemble des nombres premiers p tels que $n+1 \leqslant p \leqslant 2n$, et on note π_n le nombre d'éléments de $\mathbb{P}_n$.

8. a. Démontrer que, pour tout nombre premier p appartenant à l'ensemble $\mathbb{P}_n$, l'entier $F_{2n,n}$ est divisible par p.

b. Démontrer que, si a, b et c sont des entiers naturels non nuls tels que b et c sont premiers entre eux et divisent a, alors l'entier bc divise a lui aussi.

c. Soit d le produit de tous les éléments de $\mathbb{P}_n$. Démontrer que l'entier $F_{2n,n}$ est divisible par d.

d. En déduire que $n^{\pi_n} \leqslant 2^{2n}$.