$\mathbb{Z}$

Divisibilité, congruences.

Exercice 1. *Des divisibilités par 7*

1. Montrer que, pour tout entier n, $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrer que, pour tout $n \in \mathbb{N}$, $2^n + 3^n + 5^n$ n'est pas divisible par 7.
3. Montrer que : $7 \mid x^2 + y^2 \Leftrightarrow (7 \mid x \text{ et } 7 \mid y)$.

Exercice 2. *Congruences*

1. Quel est le reste de 1234^{5678} modulo 11 ?
2. Quel est le dernier chiffre de $2021^{2022^{2023}}$? Et en base 11 (avec chiffres 0, ..., 9, A) ?

Nombres premiers et valuations p-adiques

Exercice 3. *DE01, méthode arithmétique.* On cherche à résoudre $\begin{cases} x^y = y^x \\ 0 < x < y \end{cases}$, d'inconnues $x, y \in \mathbb{N}$.

1. Soit (x, y) un couple solution.
   a. Montrer qu'on a $x \mid y$.
   b. En notant $y = kx$, montrer qu'on a $k \geqslant 2$ et $x^{k-1} = k$.
   c. Montrer que, pour $k \geqslant 3$ on a $2^{k-1} > k$.
   d. En déduire les valeurs possibles de k, x et y.
2. Conclure.

Exercice 4. *Python*

1. Écrire une fonction Python `premier(n)` prenant comme argument un entier `n` et retournant un booléen indiquant si l'entier `n` est ou pas premier.
2. Écrire une fonction Python `factor(n)` retournant la décomposition en facteurs premier d'un entier $n \geqslant 1$. La décomposition devra être la liste des $[p, v_p(n)]$ où p est un diviseur premier de n.

   Exemple : `factor(126)` doit retourner `[[2, 1], [3, 2], [7, 1]]` car $126 = 2 \times 3^2 \times 7$.

Bézout, Gauss

Exercice 5.

Montrer que pour tout $n \geqslant 1$, $n! + 1$ et $(n+1)! + 1$ sont premiers entre eux.

Exercice 6. *Puissances dans $\mathbb{Z}[\sqrt{2}]$*

1. Justifier que, pour $n \in \mathbb{N}$, il existe un couple unique $(a_n, b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$.
   Que dire alors de $(1-\sqrt{2})^n$?
2. Justifier que a_n et b_n sont premiers entre eux.

Exercice 7. *Lemme d'Euclide*

Soit p un entier naturel supérieur à 2. Montrer qu'on a $p \in \mathcal{P} \Leftrightarrow \Big(\forall (a,b) \in \mathbb{Z}^2,\ p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b\Big)$.

$\mathbb{Z}$, exos

1/1 On veut mtq $\forall n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2} \equiv 0\ [7]$

Par récurrence

(I) Pour $n=0$. $\quad 3^1 + 2^2 = 3+4 = 7 \equiv 0\ [7]$

(H) Soit $n \in \mathbb{N}$ et supp $3^{2n+1} + 2^{n+2} \equiv 0\ [7]$

$$\Rightarrow 3^{2n+1} \equiv -2^{n+2}\ [7] \quad \text{car} \begin{cases} 2 \equiv 3^2\ [7] \\ 3^2 \equiv 2\ [7] \end{cases}$$

$$\Rightarrow 3^2 3^{2n+1} \equiv 2 \cdot (-2^{n+2})\ [7]$$

$$\Leftrightarrow 3^{2n+3} + 2^{n+3}\ [7]$$

Meth 2

$3 \equiv 3\ [7]$ $\qquad$ $2 \equiv 2\ [7]$

$3^2 \equiv 2\ [7]$ $\qquad$ $2^n \equiv 2^n\ [7]$

$3^{2n} \equiv 2^n\ [7]$ $\qquad$ $2^{n+1} \equiv 4 \cdot 2^n\ [7]$

$3^{2n+1} \equiv 3 \cdot 2^n\ [7]$

Par stabilité de la somme

$$3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n\ [7]$$
$$\equiv 2^n (7)\ [7]$$
$$\equiv 0\ [7]$$

1/2

n	0	1	2	3	4	5	6
	jamais divisible par 7						
$2^n \equiv \cdot\ [7]$	1	2	4	1	2	4	1
$3^n \equiv \cdot\ [7]$	1	3	2	6	4	5	1
$5^n \equiv \cdot\ [7]$	1	5	4	6	2	3	1
$2^n + 3^n + 5^n$	3	10	10	13	8	12	

Mq $\forall n \in \mathbb{N},\ 2^{n+6}+3^{n+6}+5^{n+6} \equiv 2^n+3^n+5^n \ [7]$

$$\begin{aligned} 2^{n+6}+3^{n+6}+5^{n+6} &\equiv 2^n 2^6 + 3^n 3^6 + 5^n 5^6 \ [7] \\ &\equiv 2^n \cdot 1 + 3^n \cdot 1 + 5^n \cdot 1 \ [7] \\ &\equiv 2^n + 3^n + 5^n \ [7] \end{aligned}$$

Ccl la suite des restes mod 7 ne s'annule pas entre 0 et 6 et elle est 6-périodique donc elle ne s'annule jamais

Ainsi $n \in \mathbb{N},\ 2^n+3^n+5^n \notin 7\mathbb{Z}$

2/3

$\Leftarrow$: Mq $7|a \wedge 7|b \Rightarrow 7|a^2+b^2$

Soient $a, b \in \mathbb{N}$ Supp $7|a \wedge 7|b$.

On a

$$\begin{aligned} & a \equiv 0 \ [7] \quad \wedge \quad b \equiv 0 \ [7] \\ \Rightarrow\ & a^2 \equiv 0 \ [7] \quad \wedge \quad b^2 \equiv 0 \ [7] \\ \Rightarrow\ & a^2+b^2 \equiv 0 \ [7] \quad \text{par stabilité} \\ \Rightarrow\ & 7 \mid a^2+b^2 \end{aligned}$$

$\Rightarrow$: Mq $7|a^2+b^2 \Rightarrow 7|a \wedge 7|b$

Soit $q \in \mathbb{N}$

$q \equiv \cdot \ [7]$	0	1	2	3	4	5	6
$q^2 \equiv \cdot \ [7]$	0	1	4	2	2	4	7

On a $a^2 \equiv 0 \ [7] \vee a^2 \equiv 1 \ [7] \vee a^2 \equiv 2 \ [7] \vee a^2 \equiv 4 \ [7]$

Testons les couples

$b^2 \equiv \cdot [7]$ \ $a^2 \equiv \cdot [7]$	0	1	2	4
0	0	1	2	4
1	1	2	3	5
2	2	3	4	6
4	4	5	6	1

Ainsi $a^2+b^2 \equiv 0\ [7]$

$\Leftrightarrow a^2 \equiv 0\ [7] \ \wedge\ b^2 \equiv 0\ [7]$

$\Leftrightarrow a \equiv 0\ [7] \ \wedge\ b \equiv 0\ [7]$

$\Rightarrow 7 \mid a^2+b^2 \Leftrightarrow 7 \mid a \ \wedge\ 7 \mid b$

2/1

$1234 \equiv ?\ [11]$ pour avoir $1234^n \equiv ?^n\ [11]$

$1234 \mid 11$, 112, reste 2 $\Rightarrow$ $1234 = 112 \cdot 11 + 2$

$\Rightarrow 1234 \equiv 2\ [11]$

$\Rightarrow 1234^{5678} \equiv 2^{5678}\ [11]$

$2^1 \equiv 2\ [11]$

$2^2 \equiv 4\ [11]$

$2^3 \equiv 8 \equiv -3\ [11]$

$2^4 \equiv -6\ [11]$

$2^5 \equiv -12 \equiv -1\ [11]$

$2^{10} \equiv (-1)^2\ [11] \Rightarrow 2^{10} \equiv 1\ [11]$

donc $\forall q\ \forall r,\ 2^{10q+r} \equiv (2^{10})^q 2^r\ [11] \equiv 2^r\ [11]$

$5678 = 567 \cdot 10 + 8$

$\Rightarrow 5678 \equiv 8\ [10]$

$\Rightarrow 2^{5678} \equiv 2^{10q+8} \equiv 2^8\ [11]$

$1234^{5678} \equiv 2^{5678} \equiv 2^8 \equiv 3\ [11]$

2/2 Soit $a \in \mathbb{Z}$. Le dernier chiffre de a est $n \in \mathbb{N}$ tq $a \equiv n\ [10]$

$2021 \equiv 1\ [10]$

$2021^{2022^{2023}} \equiv 1^{2022^{2023}}\ [10]$

$\equiv 1\ [10]$

Le dernier chiffre de $2021^{2022^{2023}}$ est 1.

$2021 \equiv 8\ [11]$

$8^1 \equiv 8\ [11]$
$8^2 \equiv -2\ [11]$
$8^3 \equiv -5\ [11]$
$8^4 \equiv 4\ [11]$
$8^5 \equiv -1\ [11]$
$8^{10} \equiv 1\ [11]$

$2022 \equiv 2\ [10]$

$2022^{2023} \equiv 2^{2023}\ [10]$

$2 \equiv 2\ [10]$
$2^2 \equiv 4\ [10]$
$2^3 \equiv 8\ [10]$
$2^4 \equiv 6\ [10]$
$2^5 \equiv 2\ [10]$

$2023 \equiv 3\ [4]$

$2022^{2023} \equiv 2^{4q+3} \equiv 2^3 \equiv 8\ [10]$

$8^8 \equiv (8^4)^2 \equiv 4^2 \equiv 16 \equiv 5\ [11]$

Corrigé de quelques exercices.

Exercice 3. *DE01, méthode arithmétique.* On cherche à résoudre $\begin{cases} x^y = y^x \\ 0 < x < y \end{cases}$, d'inconnues $x, y \in \mathbb{N}$.

1. Soit (x, y) un couple solution.

   a. Montrer qu'on a $x \mid y$.

   Soit $p \in \mathbb{P}$. On a $x^y = y^x$ et donc $v_p(x^y) = v_p(y^x)$.
   Avec les propriétés des valuations p-adiques, on le réécrit $yv_p(x) = xv_p(y)$, et donc $v_p(x) = \frac{x}{y} v_p(y) \leqslant v_p(y)$ (avec égalité si et seulement si $v_p(x) = 0$). Ainsi, pour tout nombre premier p, on a $v_p(x) \leqslant v_p(y)$, ce qui implique d'après les propriétés des valuations p-adiques qu'on a $x \mid y$.

   b. En notant $y = kx$, montrer qu'on a $k \geqslant 2$ et $x^{k-1} = k$.

   On a $k = \frac{y}{x} > 1$ car $x < y$, et comme k est entier on a bien $k \geqslant 2$. On réinjecte dans l'équation : $x^y = y^x$

   $\Leftrightarrow \quad x^{kx} = (kx)^x$

   $\Leftrightarrow \quad \left(x^k\right)^x = (kx)^x$ d'après les propriétés des puissances

   $\Rightarrow \quad x^k = kx$ par injectivité de $m \mapsto m^x$ $(x > 0)$ sur $\mathbb{R}_+^*$

   $\Rightarrow \quad x^{k-1} = k$ puisqu'on a $x > 0$ et $k > 0$.

   c. Montrer que, pour $k \geqslant 3$ on a $2^{k-1} > k$.

   Montrons-le par récurrence.

   Initialisation : Pour $k = 3$ on a bien $2^{k-1} = 2^2 = 4 > 3 = k$.

   Hérédité : Soit $k \geqslant 3$ et supposons $2^{k-1} > k$.En multipliant par 2 qui est bien strictement positif on obtient $2^k > 2k$. De plus, comme on a $k \geqslant 3$, on a $2k = k + k \geqslant k + 3 > k + 1$ et enfin, par transitivité, $2^k > k + 1$. La propriété est donc bien héréditaire.

   Conclusion : La propriété est vraie au rang 3, elle est héréditaire, elle est donc vraie pour tout entier $k \geqslant 3$.
   Remarque : l'inégalité de Bernoulli $(1 + x)^n \geqslant 1 + nx$ donne, pour $x = 1$ et $n = k - 1$: $2^{k-1} \geqslant k$. Si on sait que le cas d'égalité de Bernoulli est atteint uniquement pour $n = 0$ et $n = 1$, on peut aussi conclure puisqu'ici $n = k - 1 \geqslant 2$.

   d. En déduire les valeurs possibles de k, x et y.

   On a $x \in \mathbb{N}$ donc $x \geqslant 0$. De plus :
   - si on avait $x = 0$ on aurait $y > 0$ donc $x^y = 0 \neq 1 = y^x$, ce cas est donc exclu ;
   - si on avait $x = 1$ on aurait $y > 1$ donc $x^y = 1 \neq y = y^1$, ce cas est donc exclu ;

   On a donc $x \geqslant 2$, et par croissance de $t \mapsto t^{k-1}$, on a donc $x^{k-1} \geqslant 2^{k-1}$.
   Si $k \geqslant 3$, alors en utilisant les deux questions précédentes, on obtient $k = x^{k-1} \geqslant 2^{k-1} > k + 1$ ce qui est exclu.
   C'est donc qu'on a $k \leqslant 2$, mais comme on a vu qu'on avait $k \geqslant 2$, on a $k = 2$, puis $x = x^{2-1} = x^{k-1} = k = 2$ et $y = kx = 4$.

2. Conclure.

   Comme d'habitude.

   Analyse : considérons un couple (x, y) solution, alors d'après toutes les questions précédentes on a $x = 2$ et $y = 4$.

   Synthèse : $2^4 = 16 = 4^2$, ok.

   Conclusion : $\boxed{S = \{(2, 4)\}}$.

Équations Diophantiennes

Exercice 8. *Comme dans le cours*

Résoudre les équations $16x + 26y = 4$ et $16x + 26y = 5$, d'inconnues x et y dans $\mathbb{Z}$.

Exercice 9. *Réduire l'équation modulo un entier bien choisi.*

1. Montrer que l'équation $x^2 + y^2 = 3z^2$ a pour unique solution $(x, y, z) = (0, 0, 0)$ dans $\mathbb{Z}^3$.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $x^2 - 10y^2 = 2$.
3. Résoudre dans $\mathbb{Z}^2$ l'équation $3^x - 2^y = 5$.

Exercice 10. *Un système*

Résoudre le système : $\begin{cases} x \equiv 2 & [10] \\ x \equiv 5 & [13] \end{cases}$.

$\mathbb{Z}/n\mathbb{Z}$.

Exercice 11. *Une preuve plus simple de Fermat.*

On suppose p premier et $\overline{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$.

Justifier que $\left\{ \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} & \to & \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} \\ \overline{x} & \mapsto & \overline{ax} \end{array} \right.$ a une fonction réciproque que l'on explicitera.

Puis, en calculant de deux façons le produit $\prod_{\overline{x} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}} \overline{x}$, retrouver le petit théorème de Fermat.

Exercice 12. *Le théorème de Wilson.*

On suppose $p \geqslant 2$. Montrer qu'on a $p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1\ [p]$.

Indication : comme dans l'exercice précédent, on pourra calculer $\prod_{\overline{x} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}} \overline{x}$.

Exercice 5.

Montrer que pour tout $n \geqslant 1$, $n!+1$ et $(n+1)!+1$ sont premiers entre eux.

Une façon de faire[1]. Soit $n \geqslant 1$. On note $a = n!+1$ et $b = (n+1)!+1$.
On procède par CL successives (pas nécessairement les divisions euclidiennes) comme dans l'algorithme d'Euclide :
• $b = (n+1)a - n$ donc $a \wedge b = b \wedge n$;
• $a = n(n-1)!+1$ donc $b \wedge n = n \wedge 1 = 1$;
et donc $a \wedge b = 1$.
On remarque que la deuxième ligne n'est possible que parce qu'on a $n \geqslant 1$ (et de fait si $n = 0$ on obtient $2 \wedge 2 = 2$).

Exercice 6. ©© ★ *Puissances dans* $\mathbb{Z}[\sqrt{2}]$

1. Justifier que, pour $n \in \mathbb{N}$, il existe un couple unique $(a_n, b_n) \in \mathbb{N}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$.
   Que dire alors de $(1-\sqrt{2})^n$?

   Unicité : si pour un $n \in \mathbb{N}$ on a deux solution (a_n, b_n) et (a'_n, b'_n) alors $(1+\sqrt{2})^n = a_n + b_n\sqrt{2} = a'_n + b'_n\sqrt{2}$ donc $a_n - a'_n = (b_n - b'_n)\sqrt{2}$. On a $a_n - a'_n \in \mathbb{Z} \subset \mathbb{Q}$ et $\sqrt{2} \notin \mathbb{Q}$ donc nécessairement $b_n - b'_n = 0$, puis en réinjectant $a_n - a'_n = 0$. D'où l'unicité.

   Existence : On a plusieurs façons de procéder. On peut faire par récurrence.
   On peut aussi écrire la formule du binôme de Newton :
   $$\begin{aligned}(1+\sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} \left(\sqrt{2}\right)^k \\ &= \sum_{\substack{0 \leqslant k \leqslant n \\ n \text{ pair}}} \binom{n}{k} \left(\sqrt{2}\right)^k + \sum_{\substack{0 \leqslant k \leqslant n \\ n \text{ impair}}} \binom{n}{k} \left(\sqrt{2}\right)^k \\ &= \left(\sum_{p=0}^{\lceil \frac{n}{2} \rceil} \binom{n}{2p} 2^p\right) + \left(\sum_{p=0}^{\lceil \frac{n-1}{2} \rceil} \binom{n}{2p+1} 2^p\right)\sqrt{2} \ ;\end{aligned}$$
   il suffit donc de poser
   $$a_n = \sum_{p=0}^{\lceil \frac{n}{2} \rceil} \binom{n}{2p} 2^p \text{ et } b_n = \sum_{p=0}^{\lceil \frac{n-1}{2} \rceil} \binom{n}{2p+1} 2^p.$$

   Remarque : la même méthode (ou une autre) donne aussi $(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$ pour ces mêmes valeurs a_n et b_n.

2. Justifier que a_n et b_n sont premiers entre eux.

   $(-1)^n = (1-2)^n = (1+\sqrt{2})^n(1-\sqrt{2})^n = (a_n + b_n\sqrt{2})(a_n - b_n\sqrt{2}) = a_n^2 - 2b_n^2$. Posons $u = (-1)^n a_n$ et $v = (-1)^{n+1}2b_n$, on a donc $a_n u + b_n v = 1$, et Bézout nous donne $a_n \wedge b_n = 1$.

Exercice 8. *Réduire l'équation modulo un entier bien choisi.*

1. Montrer que l'équation $x^2 + y^2 = 3z^2$ a pour unique solution $(x, y, z) = (0, 0, 0)$ dans $\mathbb{Z}^3$.
   On remarque que $(x, y, z) = (0, 0, 0)$ est solution. Montrons que c'est la seule.

   Supposons qu'il existe une solution $(x, y, z) \neq (0, 0, 0)$. Alors $d = x \wedge y \wedge z \neq 0$. On peut donc poser $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$, $z' = \dfrac{z}{d}$. On a alors $x'^2 + y'^2 = \dfrac{x^2+y^2}{d^2} = \dfrac{3z^2}{d^2} = 3z'^2$ et donc (x', y', z') est aussi solution. Et on a aussi $x' \wedge y' \wedge z' = \dfrac{x \wedge y \wedge z}{d} = 1$.

   Réduisons modulo 3 : on obtient $x'^2 + y'^2 \equiv 0\ [3]$. Or les restes possibles de x' modulo 3 sont 0, 1, 2, et donc les restes possibles de x'^2 modulo 3 sont 0 et 1. Même chose pour y'^2. En examinant tous les cas possibles (on peut faire un tableau) on observe que $x'^2 + y'^2 \equiv 0\ [3]$ implique $x' \equiv y' \equiv 0\ [3]$. Par conséquent il existe k_x et k_y tels que $x' = 3k_x$ et $y' = 3k_y$. En réinjectant on observe $z'^2 = 3(k_x^2 + k_y^2)$ donc $3 \mid z'^2$ donc $3 \mid z'$ d'après le lemme d'Euclide.
   Finalement $3 \mid x' \wedge y' \wedge z'$, contradiction.

1. Autres possibilités : utiliser les décompositions en facteurs premiers, ou encore exhiber directement une relation de Bézout égale à 1...

Remarque : on peut également présenter les choses ainsi : si (x_0, y_0, z_0) est une solution non nulle, alors le calcul modulo 3 précédent montre qu'il existe trois entiers x_1, y_1, z_1 tels que $x_0 = 3x_1$, $y_0 = 3y_1$, $z_0 = 3z_1$, et en réinjectant (x_1, y_1, z_1) est une solution. Une récurrence immédiate permet alors de construire trois suites $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$, $(z_n)_{n\in\mathbb{N}}$ telle que pour tout entier n, $(x_{n-1}, y_{n-1}, z_{n-1}) = (3x_n, 3y_n, 3z_n)$ et (x_n, y_n, z_n) est solution. Comme au départ on a $(x_0, y_0, z_0) \neq (0, 0, 0)$ l'un des trois nombres x_0, y_0, z_0 est non nul. Si c'est x_0, alors $(|x_n|)_{n\in\mathbb{N}}$ est une suite strictement décroissante d'entiers naturels, contradiction. Raisonnement analogue si c'est y_0 ou z_0.

2. Résoudre dans $\mathbb{Z}^2$ l'équation $x^2 - 10y^2 = 2$.
Modulo 5 : $x^2 \equiv 2$ [5]. On regarde les restes possibles d'un carré modulo 5, on trouve 0,1,−1. Y'a pas 2.
Pas de solution.

3. Résoudre dans $\mathbb{Z}^2$ l'équation $3^x - 2^y = 5$.
Traitons quatre cas.
   - Si $y = 0$ l'équation s'écrit $3^x = 5$. Par unicité des la décomposition en facteurs premiers, pas de solution.
   - Si $y = 1$ l'équation s'écrit $3^x = 7$. Par unicité des la décomposition en facteurs premiers, pas de solution.
   - Si $y = 2$ l'équation s'écrit $3^x = 9$. Par unicité des la décomposition en facteurs premiers, on a une unique valeur de x convenable : $x = 2$.
   - Si $y \geqslant 3$ réduisons l'équation modulo 8. On obtient $3^x \equiv 5$ [8]. Or on a $3^0 \equiv 1$ [8], $3^1 \equiv 3$ [8], $3^2 \equiv 1$ [8], puis, par une récurrence immédiate, 3^x ne peut valoir que 1 ou 3 modulo 8. Il n'y a donc pas de solution dans ce cas.

   Conclusion : $S = \{(2, 2)\}$.

Exercice 10. *Une preuve plus simple de Fermat.*

On suppose p premier et $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$. Justifier que $\left\{ \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ x & \mapsto & ax \end{array} \right.$ est une bijection.

Puis, en calculant de deux façon le produit $\prod_{x\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} x$, retrouver le petit théorème de Fermat.

L'entier p est premier donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. Rappelons que l'on peut montrer ceci facilement à l'aide du théorème de Bézout et que c'est fait en détail dans le corrigé de l'exercice CCINP $n°66$.

On a $\overline{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ donc $\overline{a}$ a un inverse $\overline{b} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ qui vérifie par définition $\overline{b}\overline{a} = \overline{1}$. Même si on n'a pas encore fait le cours sur les applications, on doit avoir compris qu'une application est une bijection lorsque tous les éléments de l'ensemble d'arrivée ont un unique antécédent. Notons $f = \overline{x} \mapsto \overline{ax}$ et montrons qu'elle un bijective. Un mot d'explication cependant : f est la multiplication par $\overline{a}$ qui a pour inverse $\overline{b}$. Il n'est pas difficile de se convaincre que f a une réciproque qui est la multiplication par $\overline{a}^{-1} = \overline{b}$! Il n'est pas non plus difficile de voir que l'existence de cette réciproque équivaut à la bijectivité de f. C'est cette idée qui guide la preuve suivante.

Soit $\overline{y} \in \mathbb{Z}/p\mathbb{Z}$. Montrons que $\overline{y}$ a un unique antécédent par f.

Existence : notons $\overline{x} = \overline{b}\overline{y}$. On a $f(\overline{x}) = \overline{a}\overline{b}\overline{y} = \overline{1}\overline{y} = \overline{y}$.

Unicité : soient $\overline{x_1}$, $\overline{x_2}$ deux antécédents de $\overline{y}$. On a alors $\overline{ax_1} = \overline{ax_2}$ et en multipliant à gauche par $\overline{b}$ on obtient $\overline{x_1} = \overline{x_2}$.

Ouf, f est bien une bijection. La preuve précédente montre d'ailleurs que c'est aussi bien une bijection de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$ que de $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$. Remarque : la preuve précédente peut s'écrire en une ligne, j'ai juste essayé de détailler autant que possible sur une question qui déborde un peu sur un futur chapitre. Bref, c'est une bijection, on peut donc utiliser le théorème de changement d'indice dans un produit qui donne :

$$\prod_{\overline{x}\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{x} = \prod_{\overline{x}\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{ax} = \overline{a}^{p-1} \prod_{\overline{x}\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{x}$$

Enfin $\prod_{\overline{x}\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{x}$ est inversible comme produit d'éléments inversibles, et en multipliant par son inverse on obtient $\overline{a}^{p-1} = \overline{1}$ ce qui est une reformulation de $a^{p-1} \equiv 1$ [p] par stabilité des congruences par produit.

Ceci est vrai pour tout a tel que $\overline{a}$ est non nul, *i. e.* pour tout $a \in \mathbb{Z} \setminus p\mathbb{Z}$.

EXMTL #7 Mq $\forall p \geqslant d,\ p \in \mathbb{P} \Leftrightarrow \forall a,b \in \mathbb{Z},\ p|ab \Rightarrow p|a \vee p|b$

Soit $p \geqslant 2$ et supp $p \in \mathbb{P}$. Soient $a, b \in \mathbb{Z}$.

$\Rightarrow$: Supp $p|ab$. Mq $p|a \vee p|b$

ie $p \nmid a \Rightarrow p|b$.

Supp $p \nmid a$, on a $p \wedge a = 1$ d'ap le lien $\mathbb{P}$-p.e.e.

D'après le lemme de Gauss, $p|b$.

$\Leftarrow$: Mt par contraposition. Supp $p \notin \mathbb{P}$.
Mq il existe $(a,b) \in \mathbb{Z}^2$ tels que $\begin{cases} p \notin \mathbb{P} \\ p \geqslant d \end{cases}$.

il est composé donc il existe $k, d \in [\![2, n[\![$ tq

$$p = kd$$

Posons $\begin{cases} a = k \\ b = d \end{cases} \Rightarrow p = ab \Rightarrow p|ab \Rightarrow p \nmid a \wedge p \nmid b$

car $a < p \wedge b < p$

Exercice 11. *Le théorème de Wilson.*

On suppose $p \geqslant 2$. Montrer qu'on a $p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1\ [p]$.

Indication : comme dans l'exercice précédent, on pourra calculer $\displaystyle\prod_{\overline{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\overline{0}\}} \overline{x}$.

On suppose $p \geqslant 3$. En effet, pour $p = 2$, l'équivalence est acquise (les deux sont vrais).

$\boxed{\Leftarrow}$ Le sens réciproque est très facile. Supposons $(p-1)! \equiv -1\ [p]$, il existe donc $u \in \mathbb{Z}$ tel que $(p-1)! = up - 1$, donc en posant $v = -1$ on a $up + v(p-1)! = 1$ et d'après Bézout on a donc $p \wedge (p-1)! = 1$. En particulier aucun entier $k \in \{2, \dots, p-1\}$ ne peut diviser p puisque tous ces entiers divisent $(p-1)!$, donc p est premier.

$\boxed{\Rightarrow}$ Supposons p premier, tous les éléments de $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ ont un inverse. Deux éléments sont leur propre inverse : $\overline{-1}$ et $\overline{1}$. Il ne peut y avoir d'autres éléments qui soient leur propre inverse car un tel élément $\overline{x}$ vérifie $\overline{x}^2 - \overline{1} = \overline{0}$ *i. e.* $(\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}$ et un des deux facteurs est nécessairement nul (sinon en multipliant par leurs inverses on trouverait $\overline{1} = \overline{0}$, ce qui n'est pas).
Ainsi, dans le produit $\displaystyle\prod_{\overline{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{x}$, on isole les facteurs $\overline{-1}$ et $\overline{1}$ avec Chasles, les autres facteurs vont par paire en les regroupant avec leur inverse, ce qui montre que le produit de ces autres facteurs est $\overline{1}$ et finalement qu'on a

$$\prod_{\overline{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{0\}} \overline{x} = \overline{-1} \times \overline{1} \times \overline{1} = \overline{-1}.$$

Mais par ailleurs ce produit est $\overline{1} \times \overline{2} \times \cdots \times \overline{p-1} = \overline{(p-1)!}$ et donc $\overline{(p-1)!} = \overline{-1}$, ce qui équivaut bien à $(p-1)! \equiv -1\ [p]$.