# Congruence dans $\mathbb{Z}$.



## 1 Congruence.

**Définition 1.**
Soit $a, a' \in \mathbb{Z}$ et $n \in \mathbb{N}$

On dit que $a \equiv a' \, mod[n]$ Ssi il existe $k \in \mathbb{Z}$ tel que $a = a' + kn$

**Théorème 2. Division euclidienne.**
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$.

Il existe un unique couple d'entiers $(q, r)$ tel que : $a = bq + r$ et $0 \leqslant r < b$

Vocabulaire :

> L'entier $q \in \mathbb{Z}$ est appelé le quotient de la division euclidienne de $a$ par $b$.

> l'entier naturel $r \in \{0, 1, ...., b-1\}$ est le reste de la division euclidienne de $a$ par $b$.

**Théorème 3. Formulaire, Division euclidienne, le petit théorème de Fermat**

> **Formulaire.** Soit $a, a', b, b', c, c' \in \mathbb{Z}$, truc $\in \mathbb{N}$ et $n \in \mathbb{N}$. On a

$$\left.\begin{array}{l} a \equiv a' \mod [n] \\ \text{et} \\ b \equiv b' \mod [n] \end{array}\right\} \Longrightarrow \begin{array}{l} (2a-3b) \equiv \left(2a'-3b'\right) \mod [n] \\ (ab) \equiv \left(a'b'\right) \mod [n] \\ a^{truc} \equiv \left(a'\right)^{truc} \mod [n] \end{array}$$

> **Transformation** :

$$(a+b) \equiv c \mod [n] \Longrightarrow a \equiv (b-c) \mod [n]$$

$$a \equiv a' \mod [n] \Longrightarrow 2a \equiv 2a' \mod [2n] \Longrightarrow 2a \equiv 2a' \mod [n]$$

$$2a \equiv 2a' \mod [n] \Longrightarrow a \equiv a' \mod \left[n/2\right] \not\Longrightarrow a \equiv a' \mod [n]$$

> **Congruence,div Euclidienne et divise (difficile).** Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$.

$$a = bq + r \Longleftrightarrow a \equiv r \mod [b]$$

Application : $n$ divise $a \Longleftrightarrow a \equiv 0 \, mod[n]$

> **Le petit théorème de Fermat** Soit $p$ un nombre premier et $a \in \{1, 2, ..., p-1\}$

On a alors $a^{p-1} \equiv 1 \mod [p]$

Démonstration : La démonstration du petit théorème de Fermat en sup se fait par récurrence sur $a$.
elle utilise des propriétés des nombres premiers ainsi que le théorème de Gauss sur la divisibilité.
On la fera en fin de cours.

## 2 Critère de divisibilité en base 10.

Rappel : en base 10, on a : $1492 = 2.10^0 + 9.10^1 + 4.10^2 + 1.10^3$

> Un entier $n \in \mathbb{N}$ est divisible par 2 Ssi ....

> Un entier $n \in \mathbb{N}$ est divisible par 5 Ssi ....

> Un entier $n \in \mathbb{N}$ est divisible par 3 ou par 9.

Montrer que : $1492 \equiv (1+4+9+2) \mod [9]$. Généraliser.
En déduire un critère pour savoir si une entier $n$ est divisible par 3 ou par 9

> Un nombre $n \in \mathbb{N}$ est divisible par 11.

Montrer que : $1492 \equiv (1-4+9-2) \mod [11]$. Généraliser.
En déduire un critère pour savoir si une entier $n$ est divisible par 11.

# 3 Exercices

## — Congruence classiques et/ou célèbres —

**Exercice 1.** [Correction]

1. Calculer $4444^{4444}$ modulo 7
2. Montrer que $2^{123}+3^{121}$ est divisible par 11
3. Montrer avec des congruences que, pour tout $n\in\mathbb{N}$, 11 divise $\left(9^{5n+2}-4\right)$
4. Montrer que : Pour tout $n\in\mathbb{N}$, $n(n+2)(7n-5)$ est divisible par 6

**Exercice 2.** [Correction]

1. Calculer $2^{29}$ modulo 9.
2. On admet que le nombre $2^{29}$ possède neuf chiffres, tous distincts (parmi $0,1,2,3,4,5,6,7,8,9$).
   Quel est le chiffre manquant ?

**Exercice 3.** [Correction] *Euler et les nombre de Fermat*

Justifier que 641 est un nombre premier.
En remarquant que $641=2^7.5+1$, CàD $2^7.5\equiv(-1) \mod 641$, montrer que :

$$2^{32}+1=2^{2^5}+1\equiv 0 \mod [641].$$

**Exercice 4.** [Correction] **Les nombres de Mersenne.**

Soit $\in\mathbb{N}$. On considère le nombre $M_n=2^n-1$

1. On suppose que $n$ est composée, ainsi on peut écrire $n=ab$ avec $2\leqslant a\leqslant\sqrt{n}\leqslant b$.

   Montrer que : $M_n\equiv 0 \mod [M_a]$

   *Indication :* $2^a-1=M_a\equiv 0 \mod [M_a] \Longrightarrow 2^a\equiv 1 \mod [M_a]$

   `Interprétation : le nombre` $M_a$ `divise` $M_n$ `donc le nombre` $M_n$ `est composée.`

   **Conclusion** : Lorsque le nombre $n$ est composée,
   Alors le nombre $M_n$ est composée

   `Remarque : la réciproque est fausse car 11 est premier, CàD non-composée,`
   `et pourtant` $M_{11}=2^{11}-1=2047=23\times 89$ `est un nombre composé.`

2. Écrire la contraposée.

**Exercice 5.** [Correction] **Les nombres de Fermat.**

Soit $\in\mathbb{N}$. On considère le nombre $f_n=2^n+1$

1. On suppose que $n=a\,b$ avec $b$ un nombre impair
   Montrer que : $f_n\equiv 0 \mod [f_a]$

   En déduire que : Si $f_n$ est un nombre premier alors $n$ n'a pas de diviseur impair donc $n=2^\alpha$
   Les nombres $F_n=2^{2^n}+1$ sont appelés les nombres de Fermat.

2. la réciproque est fausse.
   En remarquant que $641=2^7.5+1$, montrer que : $F_5\equiv 0 \mod [641]$.

   `On a la factorisation :` $F_5=4294967297=641\times 6700417$.

## Plus difficile ou plus originale.

**Exercice 6.** Pour $n \in \mathbb{N}$, on note $u_n = \underbrace{11\ldots1}_{n \text{ chiffres}}$

1. Pour tout $k \in \mathbb{N}$, on note $r_k$ le reste de la division euclidienne de $u_k$ par 23.
   Justifier qu'il existe deux entiers distincts $k > k' \geqslant 1$ tel que $r_k = r_{k'}$
2. Simplifier $u_k - u'_k$. En déduire que $u_{k-k'} \equiv 0 \mod [23]$

   Conclusion : On a trouver un nombre de la forme $11\ldots1$ divisible par 23.
3. Peut-on remplacer 23 par un autre entier.

**Exercice 7.** Soit $a, b$ des nombres premiers entre eux.

1. Pour tout $k \in \mathbb{N}^*$, on note $r_k$ le reste de la division euclidienne de $a^k$ par $b$.
   Justifier qu'il existe deux entiers distincts $k, k'$ tel que $r_k = r_{k'}$
2. En déduire qu'il existe $n \in \mathbb{N}^*$ tel que $a^n \equiv 1 \mod [b]$.

**Exercice 8.** Soit $n \in \mathbb{N}$ et $A_n = n^2 + n + 1$.

1. On suppose que $p$ est un diviseur premier de $p$ et que $p > 3$
   (a) Montrer que : $n \not\equiv 1 \mod [p]$ puis que $n^2 \not\equiv 1 \mod [p]$.
   (b) Montrer que : $n^3 \equiv 1 \mod [p]$.
   (c) En utilisant le petit théorème de Fermat, montrer que $p \equiv 1 \mod [3]$.
2. Montrer qu'il existe une infinité de nombre premier congrus à 1 modulo 3.

# Correction.

**Solution de l'exercice 1 (Énoncé)**

1. Calculer $4444^{4445}$ modulo 7

   $>$ Comme $4444 = 7\times 634+6$, on a $4444^{4445} \equiv 6^{4445} \mod [7]$

   $>$ De plus on a $6 \rightsquigarrow 6^2 = 36 \equiv 1 \mod [7]$

   Ainsi $6^{4445} = 6^{4444}.6 = \left(6^2\right)^{2222}.6 \equiv 1.6 \mod [7]$

   Conclusion : $4444^{4445} \equiv 6^{4445} \mod [7] \equiv 6 \mod [7]$

2. Montrer que $2^{123}+3^{121}$ est divisible par 11

   On a modulo 11

   $2 \rightsquigarrow 2^2 = 4 \rightsquigarrow 2^3 = 8 \rightsquigarrow 2^4 = 16 \equiv 5 \mod [11] \rightsquigarrow 2^5 = 2.2^4 \equiv 2.5 \equiv 10 \equiv -1 \mod [11] \rightsquigarrow\rightsquigarrow\rightsquigarrow 2^{10} \equiv 1 \mod [11]$

   Ainsi $2^{123} = 2^{120+3} = 2^{120}.2^3 \equiv 1.8 \mod [11]$

   $3 \rightsquigarrow 3^2 = 9 \rightsquigarrow 3^3 = 27 \equiv 5 \mod [11] \rightsquigarrow 2^4 = 16 \equiv 5 \rightsquigarrow\rightsquigarrow\rightsquigarrow\rightsquigarrow 3^{10} \equiv 1 \mod [11]$

   Ainsi $3^{121} = 3^{120+1} = 2^{120}.3 \equiv 3 \mod [11]$

   Conclusion : $(2^{123}+3^{121}-1) \equiv (8+3) \equiv 0 \mod [11]$

3. Montrer avec des congruences que, pour tout $n \in \mathbb{N}$, 11 divise $\left(9^{5n+2}-4\right)$

   On sait que : $9^{5n+2}-4 = \left(9^5\right)^n.9^2-4$

   De plus $9^2 = 81 = 4+77 \equiv 4 \mod [11]$ et $9^5 = 9^2.9^2.9 \equiv 4.4.(-2) \mod [11]$

   $\equiv 16.(-2) \mod [11]$

   $\equiv 5.(-2) \mod [11]$

   $\equiv (-10) \mod [11]$

   $\equiv 1 \mod [11]$

   Ainsi $9^{5n+2}-4 \equiv \left[(1)^n.4-4\right] \mod [11]$

   $\equiv 0 \mod [11]$

   Conclusion : 11 divise $\left(9^{5n+2}-4\right)$

4. Montrer que : Pour tout $n \in \mathbb{N}$, $n(n+2)(7n-5)$ est divisible par 6

   On sait que $7 \equiv 1 \mod [6]$ et $-5 \equiv 1 \mod [6]$

   ainsi $n(n+2)(7n-5) \equiv n(n+2)(n+1) \mod [6]$

   Lorsque l'on choisit 3 entiers consécutifs forcément il y en a 1 pair et un divisible par 3

   Conclusion : Pour tout $n \in \mathbb{N}$, 6 divise $n(n+2)(7n-5)$.

**Solution de l'exercice 2 (Énoncé)**

1. Calculer $2^{29}$ modulo 9.

   On a $2^1 = 2$

   $2^2 = 4$

   $2^3 = 8$

   $2^4 = 16 \equiv 7 \mod [9]$

   $2^5 = 2^4.2 \equiv 7.2 \mod [9] \equiv 14 \mod [9] \equiv 5 \mod [9]$

   $2^6 = 2^5.2 \equiv 5.2 \mod [9] \equiv 10 \mod [9] \equiv 1 \mod [9]$

   Ainsi on a $2^{29} = 2^{6.4+5} = \left(2^6\right)^4.2^5 \equiv 1^4.5 \mod [9]$

   $\equiv 5 \mod [9]$

2. On admet que le nombre $2^{29}$ possède neuf chiffres, tous distincts (parmi $0,1,2,3,4,5,6,7,8,9$).
   Quel est le chiffre manquant ?

   On sait que : n modulo [9] est est égale à la somme des chiffres (en base 10), ainsi

   $2^{29} \equiv (\textit{somme des chiffes}) \mod [9]$

   $\equiv (0+1+2+3+4+5+6+7+8+9-a) \mod [9]$ *avec $a$ le chiffre manquant*

   $\equiv (O-a) \mod [9]$

   $\equiv -a \mod [9]$

   Ainsi : $2^{29} \equiv -a \mod [9]$ et $2^{29} \equiv 5 \mod [9]$

Conclusion : $-a \equiv 5 \mod [9]$ et $a \in \{0,1,2,3,4,5,6,7,8,9\}$
Donc $a = 4$

Confirmation : On sait grâce à Python que : $2^{29} = 536870912$. Donc Yes ! ! !

**Solution de l'exercice 3 (Énoncé)** En remarquant que $641 = 2^7.5+1$, montrer que : $F_5 \equiv 0 \mod [641]$.

Comme $641 = 2^7.5+1$, on a

$$\begin{aligned} 5.2^7 &\equiv -1 \mod [641] \\ &\Longrightarrow \left(5.2^7\right)^4 \equiv (-1)^4 \mod [641] \\ &\Longrightarrow \underbrace{625}_{\equiv -16 \mod [641]}.2^{28} \equiv 1 \mod [641] \\ &\Longrightarrow -\underbrace{16}_{=2^4}.2^{28} \equiv 1 \mod [641] \\ &\Longrightarrow -2^{32} \equiv 1 \mod [641] \\ &\Longrightarrow \underbrace{2^{32}+1}_{=F_5} \equiv 0 \mod [641] \end{aligned}$$

Conclusion : 641 divise $F_5$ Donc $F_5$ n'est pas premier ! ! ! !

**Solution de l'exercice 4 (Énoncé)**

1. Montrer que : $M_n \equiv 0 \mod [M_a]$

   On sait que : $2^a - 1 = M_a \equiv 0 \mod [M_a]$ ainsi $2^a \equiv 1 \mod [M_a]$, d'où le calcul

$$\begin{aligned} 2^a &\equiv 1 \mod [M_a] \\ &\Longrightarrow \left(2^a\right)^b \equiv 1^b \mod [M_a] \\ &\Longrightarrow 2^{ab} \equiv 1 \mod [M_a] \\ &\Longrightarrow \underbrace{2^{ab}-1}_{=M_n} \equiv 0 \mod [M_a] \\ &\quad \textit{Conclusion : } M_n \equiv 0 \mod [M_a] \end{aligned}$$

   Comme $n$ est composée, on a $2 \leqslant a \leqslant \sqrt{n} \leqslant b$
   Ainsi $M_a = 2^a - 1 \geqslant 2^2 - 1 = 3$ Donc $M_a$ est bien un diviseur "intermédiaire" de $M_n$,
   Donc $M_n$ est composée.

2. En déduire que : Si $M_n$ est premier alors n est premier.

   Par contraposée, Si $M_n$ est premier alors n est premier.

**Solution de l'exercice 5 (Énoncé)**

1. Montrer que : $f_n \equiv 0 \mod [f_a]$

   On sait que : $2^a + 1 = f_a \equiv 0 \mod [f_a]$ ainsi $2^a \equiv (-1) \mod [f_a]$, d'où le calcul

$$\begin{aligned} 2^a &\equiv (-1) \mod [f_a] \\ &\Longrightarrow \left(2^a\right)^b \equiv (-1)^b \mod [f_a] \\ &\quad \textit{Or } b \textit{ est impair et } (-1)^{impair} = (-1) \\ &\Longrightarrow 2^{ab} \equiv (-1) \mod [f_a] \\ &\Longrightarrow \underbrace{2^{ab}+1}_{=f_n} \equiv 0 \mod [f_a] \\ &\quad \textit{Conclusion : } f_n \equiv 0 \mod [f_a] \end{aligned}$$

   Si $b \neq 1$ alors $3 \leqslant f_a < f_n$, donc $f_a$ est bien un diviseur "intermédiaire" de $f_n$,
   alors $f_n$ est composée.

   Par contraposée : Si $f_n$ est premier alors $n$ n'a pas de diviseur impair
   Ainsi dans sa factorisation en facteur premier, il n'y a pas de facteur premier impair
   Ainsi $n = 2^\alpha$.

2. En remarquant que $641 = 2^7.5+1$, montrer que : $F_5 \equiv 0 \mod [641]$.

Comme $641 = 2^7.5+1$, on a

$$\begin{aligned}
5.2^7 \equiv -1 \mod [641] \\
\implies \left(5.2^7\right)^4 \equiv (-1)^4 \mod [641] \\
\implies \underbrace{625}_{\equiv -16 \mod [641]}.2^{28} \equiv 1 \mod [641] \\
\implies -\underbrace{16}_{=2^4}.2^{28} \equiv 1 \mod [641] \\
\implies -2^{32} \equiv 1 \mod [641] \\
\implies \underbrace{2^{32}+1}_{=F_5} \equiv 0 \mod [641]
\end{aligned}$$

Conclusion : 641 divise $F_5$ Donc $F_5$ n'est pas premier ! ! ! !