EXERCICES – CHAPITRE 4

CONGRUENCES

Calculs de congruences

EXERCICE 1 ⋆

Pour chaque valeur de a, trouver un entier relatif $x \in [-4; 4]$ tel que : $a \equiv x\ [9]$:

1. $a = 11$ 2. $a = 24$ 3. $a = 62$ 4. $a = 85$ 5. $a = -12$ 6. $a = 32$

EXERCICE 2 ⋆

Soient a, b deux entiers relatifs et $n \geqslant 2$ un entier. Dire si chacune des affirmations suivantes est **Vraie** ou **Fausse**, en justifiant par une démonstration ou un contre-exemple.

1. Si $a \equiv b\ [n]$, alors $a^2 \equiv b^2\ [n]$.
2. Si $a^2 \equiv b^2\ [n]$, alors $a \equiv b\ [n]$ ou $a \equiv -b\ [n]$.
3. Si $2a \equiv 2b\ [n]$, alors $a \equiv b\ [n]$.
4. Si $ab \equiv 0\ [n]$, alors $a \equiv 0\ [n]$ ou $b \equiv 0\ [n]$.
5. Si $a \equiv b\ [12]$, alors $a \equiv b\ [4]$.
6. Si $a \equiv b\ [6]$, alors $a \equiv b\ [12]$.

EXERCICE 3 ⋆

En utilisant les congruences, déterminer le reste de la division par :

a) 11, des nombres 12^{15}, 10^7, 78^{15}, 13^{12} et $(-2)^{19}$.

b) 7, des nombres $351^{12} \times 85^{15}$ et $16^{12} - 23^{12}$.

EXERCICE 4 ⋆

1. Déterminer le reste de la division euclidienne de 2^{100} par 3, par 5, par 7 et par 9.
2. Déterminer le reste de la division euclidienne de 2026^{2026} par 7, puis celui de 17^{2026} par 5.

Divisibilité et chiffres

EXERCICE 5 ⋆

Démontrer que :

1. Pour tout $k \in \mathbb{N}$, $5^{4k} - 1$ est divisible par 13.
2. Pour tout $n \in \mathbb{N}$, $5^{2n} - 14^n$ est divisible par 11.

EXERCICE 6 ⋆⋆

1. À l'aide des congruences, montrer que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrer par récurrence que pour tout $n \in \mathbb{N}$, $4^n + 15n - 1$ est divisible par 9.
3. Retrouver le résultat de la question 2 à l'aide des congruences, en distinguant trois cas selon le reste de la division euclidienne de n par 3.

EXERCICE 7 ⋆⋆

Déterminer le chiffre des unités de :

a) 3^{2025} b) 7^{2025} c) 13^{2025}

Puis du nombre suivant :

$$7^{7^{7^{7^{7^{7}}}}}$$

EXERCICE 8 : CRITÈRES DE DIVISIBILITÉ ⋆⋆

Soit $N = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$ un entier naturel écrit en base 10.

1. En remarquant que $10 \equiv 1\ [9]$ et $10 \equiv -1\ [11]$, retrouver les critères de divisibilité par 9 et par 11 démontrés au chapitre 1 (exercice 28).
2. Montrer que N est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres l'est.
3. Vérifier que $1001 = 7 \times 11 \times 13$, puis que $1000 \equiv -1\ [7]$. En déduire un critère de divisibilité par 7 portant sur les tranches de trois chiffres de N, et l'appliquer à $N = 3\,214\,987\,608$.

Tableaux de congruences et équations

EXERCICE 9 ⋆

On veut montrer que l'équation suivante n'a pas de solutions entières :

$$11x^2 - 7y^2 = 5$$

1. On suppose qu'il existe une solution $(x; y)$. Montrer en raisonnant modulo 5 que l'équation peut s'écrire sous la forme :
$$x^2 \equiv 2y^2\ [5]$$
2. Recopier puis compléter les tableaux de congruence suivants :

$x \equiv \cdots\ [5]$	0	1	2	3	4
$x^2 \equiv \cdots\ [5]$					

et

$y \equiv \cdots\ [5]$	0	1	2	3	4
$2y^2 \equiv \cdots\ [5]$					

3. En déduire que x et y sont des multiples de 5.
4. Conclure.

EXERCICE 10 ⋆

1. Soit n un entier quelconque, dresser le tableau de congruence pour n et n^2 modulo 8.
2. Avec l'aide de la question précédente, résoudre dans $\mathbb{Z}$ l'équation suivante :
$$(x+3)^2 - 1 \equiv 0\ [8]$$
3. Utiliser une méthode analogue pour résoudre dans $\mathbb{Z}$ l'équation :
$$4x \equiv 5\ [9]$$

EXERCICE 11 ⋆⋆

Soient x et k deux entiers relatifs, et $n = x^2 + x - 2$.

1. Déterminer l'ensemble E_7 des entiers x tels que n est divisible par 7.
2. Déterminer l'ensemble E_3 des entiers x tels que n est divisible par 3.
3. En déduire que si $x = 1 + 21k$ ou $x = -2 + 21k$, alors n est divisible par 42.

EXERCICE 12 ⋆

Soit n un entier naturel quelconque, on considère l'équation suivante :

$$(E) \qquad : \qquad 3x^2 + 7y^2 = 10^{2n} \qquad \text{où } x,\, y \in \mathbb{Z}$$

1. Montrer que $100 \equiv 2\ [7]$ et en déduire que si $(x; y)$ est solution de l'équation (E), alors :

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

2. Reproduire et compléter le tableau suivant :

$x \equiv \cdots\ [7]$	0	1	2	3	4	5	6
$3x^2 \equiv \cdots\ [7]$							

3. Démontrer que 2^n congrue à 1, 2 ou 4 modulo 7, et en déduire que l'équation (E) n'admet pas de solutions.

EXERCICE 13 ⋆⋆

À l'aide de tableaux de congruences, résoudre dans $\mathbb{Z}$ les équations suivantes :

a) $3x \equiv 4\ [7]$
b) $5x \equiv 2\ [12]$
c) $6x \equiv 3\ [9]$
d) $4x \equiv 3\ [10]$
e) $x^2 \equiv 2\ [7]$
f) $x^2 + x \equiv 0\ [6]$

EXERCICE 14 : LE PROBLÈME DE SUNZI ⋆⋆

On reprend le problème évoqué dans l'introduction du cours : déterminer un nombre d'objets x tel que, comptés 3 par 3, il en reste 2, comptés 5 par 5, il en reste 3, et comptés 7 par 7, il en reste 2.

1. Traduire ce problème par un système de trois congruences.
2. Déterminer les entiers de $[\![0; 14]\!]$ vérifiant les deux premières congruences. En déduire que les deux premières congruences équivalent à $x \equiv 8\ [15]$.
3. Résoudre alors le système complet, et montrer que ses solutions sont les entiers $x \equiv 23\ [105]$.
4. Combien d'objets y a-t-il si l'on sait qu'il y en a entre 100 et 200 ?

Petit théorème de Fermat

EXERCICE 15 ⋆

1. Montrer que pour tout $n \in \mathbb{N}$, $3^{6n} - 1$ est divisible par 7.
2. Soit p un nombre premier différent de 3. Montrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

EXERCICE 16 ⋆

1. Montrer que $4^{28} - 1$ est divisible par 29.
2. Montrer que pour tout $n \in \mathbb{N}$, $4^n - 1$ est divisible par 3.
3. Montrer que pour tout $k \in \mathbb{N}$, $4^{4k} - 1$ est divisible par 5 et par 17.
4. En déduire quatre diviseurs premiers de $4^{28} - 1$.

EXERCICE 17 ⋆

À l'aide du petit théorème de Fermat :

1. déterminer le reste de la division euclidienne de 3^{100} par 13 ;
2. déterminer le reste de la division euclidienne de 2^{2026} par 17 ;
3. montrer que $2^{70} + 3^{70}$ est divisible par 13.

EXERCICE 18 ⋆

Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

1. Montrer que a est divisible par 5.
2. Montrer que $a = n(n^2 - 1)(n^2 + 1)$ puis que a est divisible par 2 et 3. En déduire que a est divisible par 30.

EXERCICE 19 ⋆

1. Soit $n \in \mathbb{N}$ et $A = n^7 - n$.
   (a) Montrer que A est divisible par 7.
   (b) Vérifier que $A = n(n^3 + 1)(n^3 - 1)$ et en déduire que A est divisible par 2 et par 3.
   (c) Montrer que A est divisible par 42.
2. Soit $n \in \mathbb{N}$ et $B = n^2(n^2 + 1)(n^2 - 1)$.
   (a) Montrer que B est divisible par 3 et par 5.
   (b) En utilisant un tableau de congruence, montrer que B est divisible par 4.
   (c) En déduire que B est divisible par 60.

Exercices d'approfondissement

EXERCICE 20 ⋆⋆

On considère la suite (u_n) définie sur $\mathbb{N}$ par $\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6 \end{cases}$

1. Calculer u_1, u_2, u_3 et u_4. Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?
2. Montrer que pour tout entier naturel n, $u_{n+2} \equiv u_n$ [4].
   En déduire que pour tout entier naturel k, $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4].
3. (a) Montrer par récurrence que pour tout entier naturel n, $2u_n = 5^{n+2} + 3$.
   (b) En déduire que, pour tout entier naturel n, $2u_n \equiv 28$ [100].
4. Déterminer les deux derniers chiffres de u_n en fonction de n.

EXERCICE 21 ⋆⋆

Le but de cet exercice est de montrer qu'il existe un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009\ [10000]$.

Partie A

1. Quel est le reste de la division euclidienne de 2009^2 par 16 ?
2. En déduire que $2009^{8001} \equiv 2009\ [16]$.

Partie B

Soit la suite (u_n) définie sur $\mathbb{N}$ par $\begin{cases} u_0 = 2009^2 - 1 \\ u_{n+1} = (u_n + 1)^5 - 1 \end{cases}$

1. (a) Démontrer que u_0 est divisible par 5.

   (b) Démontrer que pour tout $n \in \mathbb{N}$:

   $$u_{n+1} = u_n[u_n^4 + 5(u_n^3 + 2u_n^2 + 2u_n + 1)]$$

   (c) Démontrer par récurrence que :

   $$\forall n \in \mathbb{N},\ u_n \text{ est divisible par } 5$$

2. (a) Vérifier que $u_3 = 2009^{250} - 1$ puis en déduire que $2009^{250} \equiv 1\ [625]$.

   (b) Démontrer alors que $2009^{8001} \equiv 2009\ [625]$.

Partie C

Déterminer un entier dont l'écriture décimale du cube se termine par 2 009.

EXERCICE 22 ⋆⋆

On considère la suite (u_n) définie sur $\mathbb{N}^*$ par :

$$u_n = 2^n + 3^n + 6^n - 1$$

1. Calculer les six premiers termes de la suite.
2. Montrer que pour tout $n \in \mathbb{N}^*$, u_n est pair.
3. Montrer que pour tout $n \in \mathbb{N}^*$ pair, u_n est divisible par 4.
   On note désormais E l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).
4. Les entiers 2, 3, 5 et 7 appartiennent-ils à l'ensemble E ?
5. Soit p un nombre premier strictement supérieur à 3.

   (a) Montrer que :

   $$6 \times 2^{p-2} \equiv 3\ [p] \qquad \text{et} \qquad 6 \times 3^{p-2} \equiv 2\ [p]$$

   (b) En déduire que $6u_{p-2} \equiv 0\ [p]$.
6. Le nombre p appartient-il à l'ensemble E ? Qu'en déduire sur E ?

EXERCICE 23 : NOMBRES DE POULET ⋆⋆⋆

Soit $n \in \mathbb{N}^*$ impair, tel que : $2^{n-1} \not\equiv 1\ [n]$.

1. Montrer que n n'est pas premier.
2. Quel est le reste de la division de 2^{340} par 341 ?
   Que cela signifie-t-il par rapport au petit théorème de Fermat ? Un nombre comme 341 est appelé nombre de Poulet.
3. Parmi les nombres entiers inférieurs à 25 milliards, 1091987405 sont premiers et seulement 21853 sont des nombres de Poulet (donc non premier).
   On prend un nombre n au hasard parmi les entiers inférieurs à 25 milliards et l'on décide de déclarer, après avoir calculé 2^{n-1} modulo n :
   - Si $2^{n-1} \not\equiv 1\ [n]$: « n n'est pas premier »
   - Si $2^{n-1} \equiv 1\ [n]$: « n est premier »

   (a) Quelle est la probabilité d'énoncer un résultat faux ?

   (b) Quelle est la probabilité que le nombre soit premier sachant qu'il a été annoncé comme tel ?

EXERCICE 24 : NOMBRES DE CARMICHAËL ⋆⋆

Un nombre de Carmichaël est un entier n non premier qui vérifie la propriété :

« Pour tout entier a premier avec n, l'entier n est un diviseur de $(a^n - a)$. »

1. (a) Soit $n = 561$. Décomposer n en produit de facteurs premiers.

   (b) Vérifier que pour tout facteur premier p de n, $(p-1)$ divise $(n-1)$.

   (c) En déduire que pour tout entier a premier avec n, on a : $a^{n-1} \equiv 1\ [n]$ et que n est un nombre de Carmichaël.
2. Reprendre les mêmes questions avec $n = 1105$.
3. En quoi ces deux exemples montrent que la réciproque du petit théorème de Fermat n'est pas vérifiée ?

EXERCICE 25 : CLÉ DE CONTRÔLE ISBN ⋆⋆⋆

Jusqu'en 2007, les livres étaient identifiés par un numéro ISBN de dix chiffres $a_1 a_2 \dots a_{10}$, le dernier, appelé clé, étant choisi dans $[\![0; 10]\!]$ (la valeur 10 s'écrivant X) de sorte que :

$$S = 10a_1 + 9a_2 + 8a_3 + \cdots + 2a_9 + a_{10} \equiv 0\ [11].$$

1. Vérifier que le numéro fictif 2-7654-3210-4 est valide.
2. Déterminer la clé du numéro 2-1234-5678-a_{10}.
3. On commet une erreur sur un seul chiffre : a_i est remplacé par $b_i \neq a_i$. Montrer, à l'aide du lemme d'Euclide, que la nouvelle somme n'est plus divisible par 11, donc que l'erreur est détectée.
4. Montrer de même que l'échange de deux chiffres consécutifs distincts est toujours détecté.

EXERCICE 26 : CHIFFREMENT AFFINE ⋆⋆⋆

On numérote les lettres de l'alphabet de $A = 0$ à $Z = 25$. Pour chiffrer une lettre de numéro x, on calcule le reste y de la division euclidienne de $5x + 3$ par 26, et on la remplace par la lettre de numéro y.

1. Chiffrer le mot MATHS.
2. Vérifier que $5 \times 21 \equiv 1\ [26]$. En déduire que $y \equiv 5x + 3\ [26]$ équivaut à $x \equiv 21(y - 3)\ [26]$.
3. Déchiffrer le mot XOAXKU.
4. Expliquer pourquoi la clé $y \equiv 4x + 3\ [26]$ ne permettrait pas de déchiffrer les messages.

Pour aller plus loin

EXERCICE 27 ⋆⋆

1. Quel est le reste de la division de 5^{2022} par 8 ?
2. a) Vérifier que, si $n \in \mathbb{N}$, $(n+3)^3 \equiv n^3$ [9] et $7^{n+3} \equiv 7^n$ [9].
   b) Quel est le reste de la division euclidienne de $7^n + n^3$ par 9 ?

EXERCICE 28 ⋆⋆

1. Montrer que, si $x \in \mathbb{Z}$, $11 \mid 2x+3 \iff 11 \mid 5x+2$.
2. Quels sont les $x \in \mathbb{Z}$ tels que 12 divise x^2-1 ? tels que 12 divise x^2-2 ?

EXERCICE 29 ⋆⋆

a) Déterminer les $n \in \mathbb{N}$ tels que 5 divise $2^n - 3$.

b) Déterminer les $n \in \mathbb{N}$ tels que 13 divise $2^n - 3$.

c) Déterminer les $n \in \mathbb{N}$ tels que 65 divise $2^n - 3$.

EXERCICE 30 ⋆⋆

1. Quels sont les nombres premiers p tels que p divise $7^p + 8^p$?
2. Montrer que, pour tout $x \in \mathbb{Z}$, $x^{11} \equiv x$ [33].

EXERCICE 31 ⋆⋆⋆

Soit $(F_n)_{n\geqslant 0}$ la suite de Fibonacci, définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \in \mathbb{N}$. Pour $n \in \mathbb{N}$, calculer le reste de la division euclidienne de F_n par 8.

EXERCICE 32 ⋆⋆⋆

a) Décomposer 2730 en facteurs premiers.

b) Montrer que, pour tout nombre premier p divisant 2730, $p-1$ divise 12.

c) Montrer que, pour tout $x \in \mathbb{Z}$, on a $x^{13} \equiv x$ [2730].

EXERCICE 33 ⋆⋆⋆

En utilisant éventuellement le fait que p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$ (démonstration du petit théorème de Fermat), montrer que, si p est un nombre premier et $k \in \{0, \dots, p-1\}$, $\binom{p-1}{k} \equiv (-1)^k$ [p].

EXERCICE 34 ⋆⋆⋆⋆

Montrer que l'équation $x^2 + y^2 = 3z^2$ n'a pas de solution dans $\mathbb{Z}^3$ autre que $(0,0,0)$. On commencera par montrer que, si (x,y,z) est une solution, alors x, y, z sont divisibles par 3.

EXERCICE 35 : CARRÉS MODULO UN NOMBRE PREMIER ⋆⋆⋆⋆

Soit p un nombre premier. Si $x \in \mathbb{Z}$, on dit que x est un carré modulo p s'il existe $y \in \mathbb{Z}$ tel que $x \equiv y^2$ [p].

a) Vérifier que tout $x \in \mathbb{Z}$ est un carré modulo 2.

b) Quels sont les $x \in \mathbb{Z}$ qui sont des carrés modulo 3 ? 5 ? 7 ?

c) On suppose que p est impair et que $x \in \mathbb{Z}$, non divisible par p, est un carré modulo p. Montrer que $x^{\frac{p-1}{2}} \equiv 1$ [p].

d) On suppose que $p \equiv 3\ [4]$. Montrer que -1 n'est pas un carré modulo p.

Il existe une infinité de nombres premiers congrus à 1 modulo 4. Soient $n \geqslant 2$ un entier, p un diviseur premier de $(n!)^2 + 1$.

e) Montrer, en utilisant la question d), que $p \equiv 1\ [4]$.

f) Montrer que $p > n$.

g) Conclure que l'ensemble des nombres premiers congrus à 1 modulo 4 est infini.

EXERCICE 36 : LE PETIT THÉORÈME DE FERMAT PAR LA MÉTHODE D'EULER ⋆⋆⋆⋆

Soient p un nombre premier, $x \in \mathbb{Z}$ non divisible par p.

a) Montrer que l'application qui à $a \in \{1, \dots, p-1\}$ associe le reste $r(a)$ de la division euclidienne de ax par p est une bijection de $\{1, \dots, p-1\}$ sur lui-même.

b) En faisant le produit des congruences $ax \equiv r(a)\ [p]$ pour $a \in \{1, \dots, p-1\}$, retrouver le petit théorème de Fermat.

EXERCICE 37 : THÉORÈME DE WILSON ⋆⋆⋆⋆

Soit p un nombre premier. On dit que b est un inverse de a modulo p si $ab \equiv 1\ [p]$.

a) Justifier que tout $a \in \{1, \dots, p-1\}$ admet un unique inverse modulo p dans $\{1, \dots, p-1\}$, que l'on note $i(a)$.

b) Montrer que les seuls $a \in \{1, \dots, p-1\}$ tels que $i(a) = a$ sont 1 et $p-1$ (qui sont égaux si $p = 2$, distincts sinon).

c) En regroupant judicieusement les facteurs du produit $\prod_{a=1}^{p-1} a$, établir le théorème de Wilson :

$$(p-1)! \equiv -1\ [p].$$

d) On suppose que $n \geqslant 2$ est un entier tel que $(n-1)! \equiv -1\ [n]$. Montrer que tout élément de $\{1, \dots, n-1\}$ admet un inverse modulo n et en déduire que n est premier.