Chapitre 3

Congruences

Sommaire

3.1 Activité

On sait que le 1er septembre 2016 est un jeudi. À partir de ce renseignement, on aimerait pouvoir déterminer le jour de la semaine de n'importe quelle date à venir de l'année 2016 ou des années suivantes.

1. On se propose de chercher quel jour de la semaine tombe le 31 décembre 2016.
   (a) Combien de jours n s'écoulent entre ces deux dates ?
   (b) En divisant ce nombre par 7, en déduire le nombre q de semaines complètes qui se sont écoulées entre ces deux dates.
   (c) Calculer alors le nombre de jours r restant après ces q semaines pour atteindre la date du 31 décembre 2016. Écrire n en fonction de 7, q et r.
   (d) En déduire quel jour de la semaine est le 31 décembre 2016.
2. Déterminer de la même façon quel est le jour de la semaine du 1er mai 2017.
3. Déterminer de la même façon quel est le jour de la semaine du 1er mai 2018.
4. Qu'ont en commun tous les lundis ? mardis ? Etc. ?

3.2 Bilan et compléments

3.2.1 Congruences modulo n

Définition 3.1. Soit $(a,b) \in \mathbb{Z}^2$, soit $n \in \mathbb{N}^*$.
Dire que a et b sont *congrus modulo n* signifie que a et b ont le même reste dans la division euclidienne par n.
On écrit $a \equiv b \pmod{n}$.

On écrit aussi parfois $a \equiv b\,[n]$ ou $a \equiv b\,(n)$.

Propriété 3.1. *La relation de congruence modulo n est une relation d'équivalence, c'est-à-dire qu'elle est :*

Réflexive : $\forall n \in \mathbb{N}^*, \forall a \in \mathbb{Z}, a \equiv a \pmod{n}$

Symétrique : $\forall n \in \mathbb{N}^*, \forall (a,b) \in \mathbb{Z}^2, a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

Transitive : $\forall n \in \mathbb{N}^*, \forall (a,b,c) \in \mathbb{Z}^3, a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

La preuve (assez triviale) sera faite en classe.
On a aussi les propriétés suivantes :

Propriété 3.2. $\forall n \in \mathbb{N}^*, \forall a \in \mathbb{Z}$ *:*
- *il existe un unique* $r \in [\![0; n-1]\!]$ *tel que* $a \equiv r \pmod{n}$ *et ce nombre r est le reste de la division euclidienne de a par n.*
- *Si* $n \mid a$ *alors* $a \equiv 0 \pmod{n}$.

Les preuves seront faites dans l'exercice 3.1.

Propriété 3.3. $\forall (a,b) \in \mathbb{Z}^2, a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$.

La preuve sera faite en classe.

3.2.2 Compatibilité avec les opérations algébriques

Propriété 3.4. $\forall n \in \mathbb{N}^*, \forall (a,b,a',b') \in \mathbb{Z}^4$ *:*
Si $a \equiv b \pmod{n}$ *et* $a' \equiv b' \pmod{n}$ *alors :*
- $a + a' \equiv b + b' \pmod{n}$
- $a - a' \equiv b - b' \pmod{n}$
- $aa' \equiv bb' \pmod{n}$

On dit que la relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

La preuve sera faite en classe.

Remarque. La relation de congruence n'est pas compatible avec la division en général. En effet, par exemple, $14 \equiv 6 \pmod{8}$ et $2 \equiv 2 \pmod{8}$ mais $7 \not\equiv 3 \pmod{8}$. Cependant la simplication est parfois possible dans certains cas : Si x et n sont premiers entre eux, alors $ax \equiv a'x \pmod{n} \Rightarrow a \equiv a' \pmod{n}$. Le preuve sera faite dans l'exercice 3.2.

Propriété 3.5. $\forall n \in \mathbb{N}^*, \forall (a,b) \in \mathbb{Z}^2$ *:*
Si $a \equiv b \pmod{n}$ *alors* $\forall p \in \mathbb{N}, a^p \equiv b^p \pmod{n}$.

La preuve sera faite dans l'exercice 3.3.

3.3 Exercices

3.3.1 Preuves

EXERCICE 3.1.
$\forall n \in \mathbb{N}^*, \forall a \in \mathbb{Z}$:

1. Montrer qu'il existe un unique $r \in [\![0\,;\, n-1]\!]$ tel que $a \equiv r \pmod{n}$ et ce nombre r est le reste de la division euclidienne de a par n.
2. En déduire que :

$$n \mid a \Rightarrow a \equiv 0 \pmod{n}$$

EXERCICE 3.2.
Montrer que si x et n sont premiers entre eux, alors $ax \equiv a'x \pmod{n} \Rightarrow a \equiv a' \pmod{n}$.

EXERCICE 3.3.
Montrer, à l'aide d'une récurrence sur p que $\forall n \in \mathbb{N}^*, \forall (a,b) \in \mathbb{Z}^2$:

$$a \equiv b \pmod{n} \Rightarrow \forall p \in \mathbb{N}, a^p \equiv b^p \pmod{n}$$

3.3.2 Technique

EXERCICE 3.4.
Déterminer :

- La valeur de $15 \pmod 7$ strictement inférieure à 7
- La valeur de $4 \pmod 2$ strictement inférieure à 2
- La valeur de $127 \pmod{25}$ strictement inférieure à 25

EXERCICE 3.5.
Vrai ou faux?

1. $132 \equiv 47 \pmod{15}$
2. $1214 \equiv -8 \pmod{44}$
3. $-209 \equiv 131 \pmod{28}$
4. $899 \equiv 1 \pmod{45}$

EXERCICE 3.6.
Les questions sont indépendantes.

1. Déterminer les entiers x tels que $2 + x \equiv 4 \pmod 6$.
2. Déterminer les entiers x tels que $2 \times x \equiv 4 \pmod 6$.
3. Déterminer les entiers x tels que $x^3 \equiv 4^3 \pmod 7$.

EXERCICE 3.7.
Déterminer, en utilisant la congruence modulo 7, le reste de la division euclidienne de 23^{41} par 7.

3.3.3 Technologie

EXERCICE 3.8.
Soit $n \in \mathbb{N}$. On pose $A = n(n^2+5)$.
Montrer, en utilisant la congruence modulo 3, que $3 \mid A$.

EXERCICE 3.9.
Soit $n \in \mathbb{N}$.
À l'aide de la congruence :

1. Déterminer le reste de la division de 2^n par 3 en fonction de l'entier naturel n.
2. En déduire le reste de la division de 2^{2013} par 3.
3. Déterminer le reste de la division euclidienne de $2^{3n} - 2^n$ par 3.

EXERCICE 3.10.
Soit $(n\,;\, p) \in \mathbb{N}^* \times \mathbb{N}^*$.

1. Montrer que $n(n^4-1)$ est multiple de 5.
2. En déduire que les nombres n^p et n^{p+4} ont même chiffre des unités.

EXERCICE 3.11.
Soit $n \in \mathbb{N}^*$.
Montrer que n a même reste dans le division euclidienne que la somme de ses chiffres.

EXERCICE 3.12.
Démontrer que, $\forall n \in \mathbb{N}$, $n^3 + 23n + 2016$ est multiple de 6.

EXERCICE 3.13.
Quel jour de la semaine était le 14 juillet 1789? *(voir la remarque ci-dessous).*

Remarque. Les années comptent 365 jours dont 28 en février, sauf les années bissextiles à 366 jours dont 29 en février.
Les années bissextiles sont :

- les années multiples de 4 mais pas de 100
- les années multiples de 2 000

EXERCICE 3.14.
On considère la suite (u_n) d'entiers naturels définie par :

$$(u_n)\begin{cases} u_0 = 2 \\ \forall n \in \mathbb{N}, u_{n+1} = 8u_n + 1 \end{cases}$$

1. Calculer les 5 premiers termes.
   Quelle conjecture peut-on émettre concernant le dernier chiffre de u_n pour $n \geqslant 1$?
2. Valider cette conjecture à l'aide d'une démonstration par récurrence.

EXERCICE 3.15.
1. (a) Déterminer le reste de la division euclidienne de 2013^4 par 16.
   (b) En déduire que $2013^{8001} \equiv 2013 \pmod{16}$
2. On considère la suite définie sur $\mathbb{N}$ par :

$$(u_n)\begin{cases} u_0 = 2013^2 - 1 \\ \forall n \in \mathbb{N}, u_{n+1} = (u_n + 1)^5 - 1 \end{cases}$$

   Démontrer par récurrence que, pour tout $n \in \mathbb{N}$, u_n est divisible par 4.

EXERCICE 3.16.
En étudiant les congruences modulo 5, démontrer que, si les entiers x, y et z sont tels que $x^2 + y^2 = z^2$, alors l'un au moins est divisible par 5.

EXERCICE 3.17.
1. Démontrer que, $\forall n \in \mathbb{N}$, $2^{3n} - 1$ est un multiple de 7.
   En déduire que $2^{3n+1} - 2$ est un multiple de 7 et que $2^{3n+2} - 4$ est un multiple de 7.
2. Déterminer les restes dans la division par 7 des puissances de 2.
3. Le nombre p étant un entier naturel, on considère le nombre entier $A_p = 2^p + 2^{2p} + 2^{3p}$.
   (a) Si $p = 3n$, quel est le reste de la division de A_p par 7 ?
   (b) Démontrer que si $p = 3n + 1$ alors A_p est divisible par 7.
   (c) Étudier le cas où $p = 3n + 2$.

EXERCICE 3.18.
Dans un Lycée, un code d'accès à la photocopieuse est attribué à chaque professeur.
Ce code est un nombre à quatre chiffres choisis dans $[\![0\,;9]\!]$, chaque chiffre pouvant être répété à l'intérieur d'un même code.
Ce code permet de définir un identifiant pour l'accès au réseau informatique. L'identifiant est constitué du code à quatre chiffres suivi d'une clé calculée à l'aide de l'algorithme suivant :

Entrée : N est le code à quatre chiffres.

Initialisation :
Affecter à P la valeur N ;
Affecter à S la valeur 0 ;
Affecter à K la valeur 1.

Traitement :
Tant que $K \leqslant 4$
Affecter à U le chiffe des unités de P ;
Affecter à K la valeur $K + 1$;
Affecter à S la valeur $S + K \times U$;
Affecter à P la valeur $\frac{P-U}{10}$;
Affecter à R le reste dans la division euclidienne de S par 7 ;
Affecter à C la valeur $7 - R$.
Fin du Tant que

Sortie : Afficher la clé C

1. Faire fonctionner l'algorithme avec $N = 2\,282$ et vérifier que la clé est alors 3.
2. Un professeur s'identifie sur le réseau informatique en entrant le code 4732 suivi de la clé 7. L'accès lui est refusé. Le professeur est sûr das trois derniers chiffres du code et de la clé, l'erreur porte sur le premier chiffre du code (qui n'est donc pas égal à 4). Quel est ce premier chiffre ?