Leçon 7

Congruences dans $\mathbb{Z}$. Applications.

1 Mon esquisse de plan

Plan

1) Généralités

- **Relation de congruence modulo n.** Définition. CNS pour que a et b soit congru modulo p à l'aide de la division euclidienne. Opérations sur les congruences (somme, produit, puissance). Théorème chinois (version congruence).
- **Ensemble $\mathbb{Z}/n\mathbb{Z}$.** La relation de congruence est une relation d'équivalence. L'ensemble des classes d'équivalence de $\mathbb{Z}$ par cette relation est l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$ et $\mathrm{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

2) L'anneau $\mathbb{Z}/n\mathbb{Z}$

- **Structure d'anneau.** Définition de l'addition $+$ et de la multiplication $\times$ sur $\mathbb{Z}/n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est alors un anneau commutatif. Théorème chinois (version $\mathbb{Z}/n\mathbb{Z}$).
- **Éléments inversibles.** Caractérisation des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. CNS pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Expression de l'indicatrice d'Euler $\varphi(n)$ égale au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

3) Applications.

- Théorème d'Euler : Si a et n sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1[n]$.

  Petit théorème de Fermat (corollaire du précédent) : Si p est premier, alors pour tout entier a, $a^p \equiv a[p]$.

  Théorème de Wilson : p est premier si et seulement si $(p-1)! \equiv -1[p]$.
- Critère de divisibilité en base b. Et si $b = 10$, critères classiques de divisibilité par $2, 3, 5, 9, 10, 11$...

Développements possibles

Opérations sur les congruences (somme, produit, puissance).
Théorème chinois (version congruence ou $\mathbb{Z}/n\mathbb{Z}$).
Théorème d'Euler, de Fermat et de Wilson.

Exercices et programmes informatiques possibles

Chiffrement.
RSA.

Bibliographie

- B. Bajou, M. Saint-Lannes et X. Sorbe. Mathématiques, épreuve orale d'exposé.
- J. de Biasi. Mathématiques pour le CAPES et l'Agrégation Interne.
- G. Debeaumarché. Manuel de Mathématiques. Volume 2. Algèbre et géométrie.
- D. Delaunay. Exercices d'algèbre et de probabilités.
- X. Gourdon. Les maths en tête. Algèbre.

2 Questions

Niveau 1

1. Montrer que, pour tout entier naturel n, $5 \mid (2^{3n+5} + 3^{n+1})$.
2. Montrer que, pour tout entier naturel n, $30 \mid (n^5 - n)$.
3. Quel est le reste de la division par 7 de 59^{45} ? de 247^{349} ?
4. Déterminer les restes des divisions de 37^n par 11, avec n un entier naturel.
5. Trouver les deux derniers chiffres du nombre $7^{9^{9^9}}$.
6. Trouver le reste par 5 de $N = 2222^{3333} + 3333^{2222}$.
7. Montrer qu'un entier n est pair si et seulement si n^2 est pair.
8. Résoudre l'équation $x^2 - 7y^2 = 3$, où x et y sont deux entiers relatifs.

9. Montrer que, dans un triangle rectangle dont tous les cotés sont entiers, il y a au moins un coté qui est divisible par 5.

10. Montrer que, pour tous nombres premiers p et q, on a :

$$p^{q-1} + q^{p-1} \equiv 1[pq].$$

Niveau 2

1. On considère un nombre premier p.

   (a) Établir la relation $p\binom{p-1}{k-1} = k\binom{p}{k}$ et en déduire que p divise $\binom{p}{k}$ pour $0 < k < p$.

   (b) Établir par récurrence sur a la relation $a^p = a[p]$ pour $a \in \mathbb{N}$, puis $\mathbb{Z}$.

   (c) En déduire, si p ne divise pas a, que $a^{p-1} \equiv 1[p]$.

2. Déterminer le reste de la division de 2^{1997} par 3, par 23, par 69.

   Déterminer le reste de la division de 7^{102} par 65.

   Déterminer les deux derniers chiffres de l'entier 11^{121}.

3. 17 pirates s'emparent d'un navire. S'ils se partagent alors le butin, il reste 3 pièces d'or pour le cuisinier chinois. Mais les pirates se querellent et 6 d'entre eux sont tués. S'ils se partagent alors le butin, il resterait 4 pièces d'or pour le cuisinier. Le navire fait alors naufrage, et seuls 6 pirates survivent. Le partage laisserait 5 pièces d'or au cuisinier.

   Combien celui-ci aura-t-il au minimum lorsqu'il empoisonnera les pirates survivants ?

4. Pour tout couple d'entiers (a, b), le nombre $A = ab(a^{30} - b^{30})$ est divisible par 14322.

5. Quel est le reste de la division euclidienne de $16^{(2^{1000})}$ par 7 ?

6. Soit A la somme des chiffres de 4444^{4444} et B la somme des chiffres de A. Que vaut C, la somme des chiffres de B ?

7. Pour tout entier naturel n, on pose $F_n = 2^{2^n} + 1$ (nombre de Fermat).

   (a) Montrer que les nombres $(F_n)_{n\in\mathbb{N}}$ sont premiers entre eux deux à deux.

   (b) En déduire une démonstration du fait qu'il y une infinité de nombres premiers.

8. Soit p un nombre premier. Montrer que, pour tout entier a, il existe un couple (x, y) de $\mathbb{Z}^2$ tel que :

$$a \equiv x^2 + y^2[p].$$