Leçon 14: Congruences dans Z. Anneaux Z/nZ

quelques remarques sur les scans que je vous propose:

Exposé au tableau: pages 2 à 7

-les preuves apparaissant sur ces feuilles ont été faites au tableau (propo2, th6)

-les parties entre parenthèses n'ont pas été exposées au tableau pour tenir les 25mn

-la partie III a été traitée dans l'ordre 3), 1) et je n'ai pas eu le temps de parler de Fermat (2):

J'ai fait ce choix pour être certain d'avoir le temps de faire la preuve du th6 (théorème chinois) et il me semblait essentiel de parler de numération dans cette leçon (même en acceptant d'admettre sans l'écrire la définition d'un système de numération de position en base a). Honnêtement, je pense qu'il est également nécessaire de parler de Fermat le jour J... mais je suis pas un rapide et il me manquait pas grand chose, donc vous devriez y arriver, et dans ce cas autant traiter dans l'ordre 1), 2), 3).

1) → représentation des entiers dans la vie de tous les jours par des chiffres
2) → application à la cryptographie: test de primalité d'un entier
   parler si possible:
   - des nombre de Carmicael (qui font mentir la réciproque de Fermat)
   - du th de Wilson qui donne un critère de primalité apparemment génial mais finalement inapplicable à cause du calcul de la factorielle
3) → résolution d'équations intervenant notamment en astronomie mais pas que ! (périodicité des éclipses, comptage de l'armée impériale chinoise, problème d'Euler avec chevaux et bœufs, si vous le sentez on doit aussi pouvoir faire des histoires d'engrenages...)

Preuves complémentaires: pages 8 à 10

je n'avais pas écrit les preuves des résultats à partir du II.2) (qui me semblaient limpides)
n'hésitez pas à me demander si besoin

Commentaires et remarques de M. Dubois: pages 10 et 11

-énoncé du théorème chinois ainsi:
(n et p 1ers entre eux) → (Z/npZ est isomorphe à Z/nZ x Z/pZ)
sa preuve consiste à exhiber un tel isomorphisme (le plus naturel possible en plus !), mais bon, je trouve pas cet énoncé hyper naturel (en toit cas à mon niveau...)

-contre exemple: si n et p ne sont pas premiers entre eux,
ppcm(n,p) = m et l'application proposé l'envoie sur (0,0) (alors que m n'est pas élément neutre de npZ, donc l'appli n'est pas un isomorphisme dans ce cas.

-définition géométrique du nombre d'or et preuve de son irrationalité (plutôt joli... mais plutôt à mettre dans la leçon sur la division euclidienne ou le pgcd)

Résolution des exercices proposés: page 12

exp1

14. Congruences dans $\mathbb{Z}$
Anneaux $\mathbb{Z}/n\mathbb{Z}$

Prérequis : division euclidienne de $\mathbb{Z}$ (unicité (quotient, reste))
divisibilité, primalité (relative), Bézout, Gauss
relat° d'équivalence, classe, les classes forment 1 partition
$(\mathbb{Z}, +, \times)$ est 1 anneau comm unit., les ss gp de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$

$n \in \mathbb{N}$

I relation de congruence

1) définition

def 1 $a, b \in \mathbb{Z}$

On dit que "a est congru à b modulo n" ssi
$(a-b) \in n\mathbb{Z}$, et on note alors $a \equiv b \ [n]$

Rq $\forall (x, y) \in \mathbb{Z}^2$

$$\begin{cases} x \equiv y \ [1] \\ x \equiv y \ [0] \iff x = y \end{cases}$$

Th 1 la relation de congruence est une relat° d'équivalence

propo 1 : $a \equiv b \ [n] \iff$ a et b ont le même reste
dans la division euclidienne par n

2) opérations arithmétiques

Th 2 compatibilité avec l'addition et la soustraction de $\mathbb{Z}$

$$\left.\begin{array}{l} a \equiv b \ [n] \\ c \equiv d \ [n] \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a+c \equiv b+d \ [n] \\ ac \equiv bd \ [n] \end{array}\right.$$

propo 2 $p \in \mathbb{N}$

$$a \equiv b \ [n] \Longrightarrow \left\{\begin{array}{l} -a \equiv -b \ [n] \\ a^p \equiv b^p \ [n] \end{array}\right.$$

□ $p \geq 2$, $a^p - b^p = (a-b) \sum_{k=0}^{p-1} a^k b^{p-1-k}$

donc $n \mid (a-b) \Longrightarrow n \mid (a^p - b^p)$

d'où par définition $a^p \equiv b^p \ [n]$ ⊠

exo Mq a) $\left.\begin{array}{l} m \wedge n = 1 \\ ma \equiv mb \ [n] \end{array}\right\} \Longrightarrow a \equiv b \ [n]$

b) $\left.\begin{array}{l} a \equiv b \ [n] \\ n' \mid n \end{array}\right\} \Longrightarrow a \equiv b \ [n']$

exp 2

$n \geqslant 2$

II Anneau $\mathbb{Z}/n\mathbb{Z}$

1) ensemble quotient

notat° $\bar{a}$ la classe d'équivalence de a modulo n

(propo 3 : $\forall a \in \mathbb{Z}$
$\bar{a}$ contient un unique élément a' tel que :
$0 \leqslant a' < n$
(donc $\exists$ n classes et elles réalisent une partition de $\mathbb{Z}$))

Th 3 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est l'ensemble des classes modulo n (appelé ensemble des entiers modulo n)

le Th 2 permet de définir les deux lois de composition suivante sur $\mathbb{Z}/n\mathbb{Z}$:

$$\bar{x} + \bar{y} = \overline{x+y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{xy}$$

Propo 3 $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire d'élément nul $\bar{0}$ et d'élément unité $\bar{1}$

□ $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$ (surjection canonique) est 1 morphisme d'anneau ☒

exo a) Mq $a \wedge n = 1$
$\forall k \in \mathbb{N}$, $\begin{cases} a^k \equiv x_k \ [n] \\ 0 \leqslant x_k < n \end{cases}$ $\Rightarrow (x_k)$ est périodique

b) en déduire le reste de la division euclidienne de 100^{100} par 13

2) Éléments inversibles

Th 4 : $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

$\iff a \wedge n = 1$

Corollaire $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps commutatif

$\iff$ n est premier

III Applications

1) numération et critères de divisibilité

$a \in \mathbb{N}$, $a \geq 2$

def 2 la base a d'un système de numération de position est le nombre de symboles utilisés pour représenter tous les entiers naturels

propo 4 Tout entier n s'écrit de façon unique sous la forme :

$$n = \sum_{i=0}^{p} u_i a^i \quad \text{avec } \forall i \in \{0,..,p\} \quad 0 \leq u_i < a$$

on écrit alors $n = \overline{u_p u_{p-1} \dots u_0}^{a}$

propo 5 soit $n = \overline{u_p u_{p-1} \dots u_0}^{a}$, alors :

$a^k \mid n \iff$ l'écriture de n en base a se termine par k zéros

exp 3

$(a-1) \mid n \iff (a-1) \mid \sum_{i=0}^{p} u_i$

$(a+1) \mid n \iff (a+1) \mid \sum_{i=0}^{p} (-1)^i u_i$

ex: en base 10 on retrouve les critères de divisibilité par 9, 10 et 11

application : preuve par 9 et par 11

2) Théorème de Fermat

Lemme 1 : $p, k \in \mathbb{N}$

$\left.\begin{array}{l} p \text{ premier} \\ 0 < k < p \end{array}\right\} \Rightarrow \binom{p}{k} \equiv 0 \ [p]$

Th 5 : Petit Théorème de Fermat :

p premier $\Rightarrow \forall a \in \mathbb{Z}, \ a^p \equiv a \ [p]$

□ : $\forall (x,y) \in \mathbb{Z}^2 \quad (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^p y^{p-k} \equiv x^p + y^p \ [p]$

par récurrence, $(x_1 + \dots + x_m)^p \equiv \sum_{i=1}^{m} x_i^p \ [p]$

donc $a^p = (1 + \dots + 1)^p \equiv \sum_{i=1}^{a} 1^p \ [p]$

soit $a^p \equiv a \ [p]$ ⊠

3) Théorème Chinois

Th 6 : $n \wedge p = 1$, alors

$$\begin{cases} x \equiv a \ [n] \\ x \equiv b \ [p] \end{cases}$$ d'inconnue x

admet au moins une solution c dans $\mathbb{Z}$

l'ensemble des solutions est $\{c + knp \ ; \ k \in \mathbb{Z}\}$

□

$n \wedge p = 1 \xrightarrow{\text{Bézout}} \exists (u,v)$ tq $nu + pv = 1$

donc $c = bnu + apv$ est solution

en effet : $bnu + apv \equiv a \ [n]$

et $bnu + apv \equiv b \ [p]$

x est solution $\iff x \in \overline{c}$

$\iff x \in \{c + knp \mid k \in \mathbb{Z}\}$

■

Rq /

$$\begin{cases} x \equiv a \ [n] \\ x \equiv b \ [p] \\ x \equiv c \ [q] \end{cases}$$ avec n, p, q premiers 2 à 2

et d solution de $\begin{cases} x \equiv a \ [n] \\ x \equiv b \ [p] \end{cases}$

$$\iff \begin{cases} x \equiv d \ [np] \\ x \equiv c \ [q] \end{cases}$$

$$\begin{cases} x \equiv a \ [n] \\ x \equiv b \ [p] \end{cases} \text{ avec } \begin{cases} m \vee p = M \\ m \wedge p = d \\ d \mid (a-b) \end{cases} \longrightarrow \begin{cases} n = dn' \quad p = dp' \\ \exists (u',v') \text{ tq } n'u' - p'v' = 1 \end{cases}$$

$c = a + k_1 n = b + k_2 p \iff k_1 n - k_2 p = b - a$

$(k_1, k_2) = \big((b-a)u'd, \ (b-a)v'd\big)$ $\quad \{c + Mk, \ k \in \mathbb{Z}\}$

preuves 1

Th 1

symétrique $(a-b) \in n\mathbb{Z} \iff (b-a) \in n\mathbb{Z}$

$n\mathbb{Z}$ ss gp de $(\mathbb{Z}, +)$

réflexive $a - a = 0 \in n\mathbb{Z}$

transitive $\left.\begin{array}{l} a-b \in n\mathbb{Z} \\ b-c \in n\mathbb{Z} \end{array}\right\} \Rightarrow (a-b)+(b-c) \in n\mathbb{Z}$

$(n\mathbb{Z}, +)$ est 1 gp

propo 1 :

$a - b \in n\mathbb{Z} \iff n \mid a-b$

soit r_a tq $\begin{cases} a = k_a n + r_a \\ 0 \leq r_a < n \end{cases}$

r_b tq $\begin{cases} b = k_b n + r_b \\ 0 \leq r_b < n \end{cases}$

$a - b = (k_a - k_b) n + r_a - r_b$

donc $n \mid (a-b) \iff n \mid (r_a - r_b) \iff r_a - r_b = 0$

car $-n < -r_b \leq 0$

et donc $-n < r_a - r_b < n$

donc $r_a = r_b$

Th 2

$\left.\begin{array}{l} n \mid a-b \\ n \mid c-d \end{array}\right\} \Rightarrow n \mid (a-b)+(c-d) = (a+c)-(b+d)$

$\left.\begin{array}{l} a = nk_1 + b \\ c = nk_2 + d \end{array}\right\} \Rightarrow ac = n^2 k_1 k_2 + n(k_1 d + k_2 b) + bd$

donc $ac - bd = n^2 k_1 k_2 + n(k_1 d + k_2 b)$

et $n \mid (ac - bd)$

propo 2

$\left.\begin{array}{l} a \equiv b \ [n] \\ -1 \equiv -1 \ [n] \end{array}\right\} \Rightarrow (-1) \times a \equiv (-1)\, b \ [n]$

exo a) $\left.\begin{array}{l} n \mid m(a-b) \\ n \wedge m = 1 \end{array}\right\} \underset{\text{Gauss}}{\Rightarrow} n \mid (a-b)$

b) $\left.\begin{array}{l} n \mid a-b \\ n' \mid n \end{array}\right\} \Rightarrow n' \mid a-b$

(propo 3 $\quad \bar{a} = \{ x \in \mathbb{Z} \mid a \equiv x \ [n] \}$

$\left.\begin{array}{l} n \mid a-x \\ 0 \leqslant x < n \end{array}\right\} \Rightarrow x$ est <u>le</u> reste de a par n donc unique)

Th 3 $\quad \{ \bar{0}, \dots, \overline{n-1} \} \subset \mathbb{Z}/n\mathbb{Z}$ <u>immédiat</u>

$\forall\, p \in \mathbb{Z} \quad \left\{\begin{array}{l} p = nk_p + r_p \\ 0 \leqslant r_p < n \end{array}\right. \Rightarrow \overline{r_p} \in \{ \bar{0}, \dots, \overline{n-1} \}$

et $\bar{p} = \overline{r_p}$ donc $\bar{p} \in \{ \bar{0}, \dots, \overline{n-1} \}$

preuves 2

propo 3 $\forall x \in \overline{a}$
$\forall y \in \overline{b}$

$x+y \equiv a+b \ [n]$ donc $\overline{x+y} = \overline{a+b}$

et $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$(\overline{a}, \overline{b}) \longmapsto \overline{a+b}$

ne dépend pas des représentants a, b choisis

de même pour $\times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

donc $+$ et $\times$ sont des lois de compo int

Th Chinois $n \wedge p = 1$ alors $\mathbb{Z}/np\mathbb{Z} \xrightarrow{\text{isomorph}} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

□ $\mathbb{Z}/np\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$\overline{a} \longmapsto (\overline{\overline{a}}, \overline{\overline{a}})$

$n \wedge p = 1 \rightarrow \exists (u,v)$ tq $nu + pv = 1$

$c\,\overline{pu} \longmapsto (\overline{c}, \overline{\overline{0}})$

$b\,\overline{nu} \longmapsto (0, \overline{\overline{b}})$

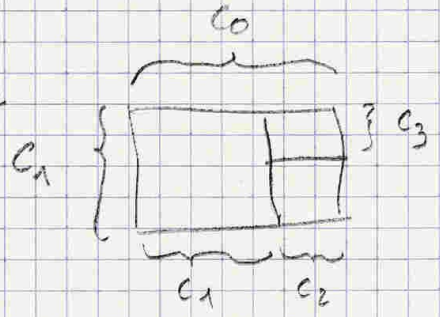
$\pi \longmapsto (\overline{\pi}, \overline{\overline{\pi}})$

$c\overline{pu} + b\overline{nu} \longmapsto (\overline{c}, \overline{\overline{b}})$

donc $n \wedge p = d$ $\quad n \vee p = m$

$$\mathbb{Z}/mp\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$
$$m \longmapsto (0,0)$$

appli Euclide



$$\frac{c_0}{c_1} = \frac{c_1}{c_2} = \frac{c_1}{c_0 - c_1}$$

Mq $\frac{c_0}{c_1} \notin \mathbb{Q}$ $\quad \left(\frac{c_0}{c_1} = \frac{\sqrt{5}-1}{2}\right)$

par algo Euclide

si $\frac{c_0}{c_1} \in \mathbb{Q}$ $\quad \exists$ unité de longueur r_q

$c_0, c_1 \in \mathbb{N}$

(ils sont commensurables)

$c_0 = c_1 + (c_0 - c_1) = c_1 + c_2$

$c_1 = c_2 + c_3$

$(c_0 - c_1) + (2c_1 - c_0)$

$c_1, c_2 \ldots \in \mathbb{N}$ de + $c_n \xrightarrow[n \to \infty]{} 0$

$\Rightarrow$ or $\forall n \; c_n \neq 0$ donc peut pas être infiniment strictement décroissante

d'où contradict°

(*)

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \end{cases}$$

$11 \wedge 17 = 1$

Euclide

$1 = 2 \times 17 - 3 \times 11$

donc $2 \times 17 \equiv 1\ [11]$

donc $8 \times 17 \equiv 4\ [11]$

et $(-3) \times 11 \equiv 1\ [17]$

donc $(-9) \times 11 \equiv 3\ [17]$

$8 \times 17 + (-9) \times 11 \equiv 3\ [17]$

$\equiv 4\ [11]$

donc $8 \times 17 + (-9) \times 11$ est solut°

exo

$$\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [p] \end{cases}$$

$n \wedge p = 1$

Bezout $\Rightarrow \exists (u,v)$ tq $nu + pv = 1$

donc $nu \equiv 1\ [p]$

$\Rightarrow bnu \equiv b\ [p]$

et $pv \equiv 1\ [n]$

$\Rightarrow apv \equiv a\ [n]$

$apv + bnu \equiv b\ [p]$

$\equiv a\ [n]$

donc $c = apv + bnu$ est solut°

(*) $100^{100} / 13$

$100 \equiv 9\ [13]$

$100^2 \equiv 81\ [13] \equiv 3\ [13]$

$100^3 \equiv 27\ [13] \equiv 1\ [13]$

donc
$$\begin{cases} 100^{3k} \equiv 1\ [13] \\ 100^{3k+1} \equiv 9\ [13] \\ 100^{3k+2} \equiv 3\ [13] \end{cases}$$

$100^{100} = 100^{99+1} \equiv 9\ [13]$

donc le reste de la div eucl de 100^{100} par 13 est 9