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

I Constructions, généralités

Soit $n \in \mathbb{N}$, $n \geq 2$

Soient X et Y deux classes de $\mathbb{Z}/n\mathbb{Z}$ $X = \bar{k} = \overline{k'}$ $Y = \bar{\ell} = \overline{\ell'}$

- - - - $\overline{k'\ell'} = \overline{k\ell}$ on pose $XY = \overline{k\ell}$.

Th $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un a.c.u tel que l'application canonique

$(\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad k \mapsto \bar{k})$ soit un morphisme d'anneau

surjectif de noyau $n\mathbb{Z}$

D/ Exos

Th: Soit $a = \bar{k} \in \mathbb{Z}/n\mathbb{Z}$

1) a est inversible $\Leftrightarrow k \wedge n = 1$
2) Si a n'est pas inversible, c'est un diviseur de 0

D/ 1) s'il existe $b = \bar{\ell} \in \mathbb{Z}/n\mathbb{Z}$ tq $ab = \bar{1}$

il vient $\overline{k\ell} = \bar{1}$ càd $k\ell \equiv 1 (n)$ on a donc $\exists r \in \mathbb{Z}$ $k\ell - rn = 1$

$(\Leftarrow)$ Bezout

2) $a = \bar{k}$ - - -

Corollaire : si $n = p$ nbre premier $\mathbb{Z}/p\mathbb{Z}$ est un corps
tout $k \in \{1, \dots, p-1\}$ est premier avec p, [illegible]

Ex : Quels sont les nilpotents de $\mathbb{Z}/_{n}\mathbb{Z}$?

$\bar{k} \in \mathbb{Z}/_{n}\mathbb{Z}$ nil $\Leftrightarrow \exists l \ n / k^l$

Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ | p_i 2 à 2 ≠ ; $n / k^l \Rightarrow p_1 \dots p_r / k^l$
$\Rightarrow p_i / k \quad i = 1 \dots r$

Réciproquement ------

II Théorème chinois

A) Anneaux

Morphisme : $f : A \to B$ on impose tq $f(1_A) = 1_B$

Groupe des unités $U(A) = \{x \in A, \exists y \in A, xy = yx = 1_A\}$

$(U(A), \times)$ est un groupe

Ex $A = \mathbb{Z}[i]$ on pose $x = u + iv \in A$. $N(x) = u^2 + v^2 = |x|^2$
Si $x \in U(A)$, il existe $y \in A$ tq $xy = 1$, d'où $N(xy) = 1$

$N(x) N(y) = 1$ Ainsi $N(x) = N(y) = 1$ | $x \in \{-1, 1, i, -i\}$

Anneau produit $A \times B$ est muni de la loi + produit et de $(x, y)(x', y')$
$= (xx', yy'$

Unité $(1_A, 1_B)$, $A \times B$ n'est jamais intègre $(1_A, 0_B)(0_A, 1_B) = (0_A, 0_B)$

Groupe des unités $U(A \times B) = U(A) \times U(B)$ (vérifier !)

B) Le Théorème

Th Soit m et n deux entiers ≥ 2 et premiers entre eux
Alors $f \left(\begin{array}{l} \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{x} \mapsto (\bar{x}_m, \bar{x}_n) \end{array} \right)$ est bien défini

et est un isomorphisme d'anneaux

$n\alpha$ $m\beta$ $q\beta'$

1/ Si $x = x' [mn] \Rightarrow x = x' [m]$, $x = x' [n]$ j est bien déf

j est un morphisme d'anneaux par définition

* j est injectif et surjectif Ker j $j(\bar{x}) = 0 \Leftrightarrow m \mid x$ et $n \mid x$
$\Leftrightarrow mn \mid x$

* est surj par cardinalité

Calcul explicite Soit $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$\exists u, v : um + vn = 1$ | $um = 1 [n]$, $vn = 1 [m]$: $x = uma + vnb$

$x \equiv uma [n]$
$\equiv a [n]$

$x \equiv vnb [m] \equiv b [m]$ OK.

Conséquence : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

2) $m \wedge n = 1$: $U(\mathbb{Z}/mn\mathbb{Z}) \simeq U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$

Rq : On peut Mq si $p \geq 3$ $U(\mathbb{Z}/p^{\alpha}\mathbb{Z})$ est cyclique (ADS)

Ex. Mq $\forall n \geq 3$ $U(\mathbb{Z}/2^n\mathbb{Z})$ n'est pas cyclique (Mines) (Cen)

S/ $n=1$ $U(\mathbb{Z}/2\mathbb{Z}) = \{\bar{1}\}$ $n = 2$ $U(\mathbb{Z}/4\mathbb{Z}) = \{\bar{1}, \bar{3}\} = \langle \bar{3} \rangle$

$U(\mathbb{Z}/8\mathbb{Z}) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ $\forall a \in U(\mathbb{Z}/8\mathbb{Z})$ $a^2 = \bar{1}$

On Mq par récurrence : $\forall a \in U(\mathbb{Z}/2^n\mathbb{Z})$ $a^{2^{n-2}} = \bar{1}$

On suppose donc que $a^{2^{n-2}} = \bar{1}$ ie x impair $x^{2^{n-2}} \equiv 1 [2^n]$

$x^{2^{(n-2)}} = 1 + \lambda 2^n$ on regarde $x^{2^{n-1}} = (1+\lambda 2^n)^2$

$= 1 + \lambda 2^{n+1} + 2^{n+1}$

$\equiv 1 [2^{n+1}]$ OK

2) Indicatrice d'Euler

$\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$ $n \geq 2$ $(\varphi(1) = 1)$

$\forall m, n \in \mathbb{N}^{*2}$: 1) $\varphi(mn) = \varphi(m)\varphi(n)$ $m \wedge n = 1$

2) $\varphi(n) = \prod_{k=1}^{n} \varphi(p_i^{\alpha_i})$

relui de nml de beds [illegible]

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$

$\varphi(n) = n \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right)$

Ex

III Théorème d'Euler (de l'uni)

Th Soit a et n ds $\mathbb{N}^*$, a et n sont premiers entre eux ssi

$a^{\varphi(n)} \equiv 1 [n]$

D/ $(\Leftarrow)$ clair $(\Rightarrow)$ $n \geq 2$ alors $\bar{a}$ est dans $U(\mathbb{Z}/n\mathbb{Z})$ donc moyennant Lagrange $\bar{a}^{|U(\mathbb{Z}/n\mathbb{Z})|} = \bar{a}^{\varphi(n)} = \bar{1}$ $[n]$.

Ex (Mines) Soit $m \in \mathbb{N}^*$ $2 \nmid m$, $5 \nmid m$ Mq $\exists k, l \in \mathbb{N}^{*}$

$km = 3 \ldots 3$ $lm = 1 \ldots 1$

$10^k x - x \in \mathbb{Q}$ OK $\quad x \in \mathbb{Q}$
$\forall k\ 10^k x - x \in \mathbb{Q}$

S/ $10 \wedge m = 1 (m) \Rightarrow 10^{\varphi(m)} \equiv 1\ (m)$

$\Rightarrow k_m = 10^{\varphi(m)} - 1 = k m$

Dem $10^{\varphi(3m)} - 1 = \ell \cdot 3m \Rightarrow P_m = 1 \ldots 1$

Ex $\forall m, \exists\ \varphi(m)$ pair : $(-1)^{\varphi(m)} = 1$.

Ex Soit $x \in \mathbb{R}$, Alors $\Updownarrow$ $x \in \mathbb{Q}$
le dév décimal de x est périodique

D/ $\Uparrow$ $x = \lfloor x \rfloor + x'$ où $x' \in [0,1[$, $x' = 0{,}x_1 x_2 \ldots x_N \ldots x_{N+T-1}$

ie $x' = \sum_{k=1}^{N-1} x_k 10^{-k} + \underbrace{x_N 10^{-N} + \ldots + x_{N+T-1} 10^{-N-T+1}}_{y\,10^{-N}} + y\,10^{-T} + y\,10^{-2T} \ldots$

$= \sum_{1}^{N-1} x_k 10^{-k} + y\,10^{-N}\left(\frac{10^T}{10^T - 1}\right) \in \mathbb{Q}$

$\Downarrow$ SNG $x = \frac{p}{q} = \frac{p'}{10^d n}$ $\quad 10^d \wedge n = 1$

de là $\exists (u,v) \in \mathbb{Z}^2$ $u 10^d + v n = 1$

$10^T x - x \in \mathbb{N}$ | on écrit $x = \frac{p'(u 10^d + n v)}{10^d n} = \frac{m}{n} + \frac{p' u v}{10^d}$ décimal

$\frac{m}{n} \xrightarrow{} = p' u$

on est ramené à $\frac{m}{n}$, en sortant la partie entière

et en simplifiant $x = \frac{m}{n} \in]0,1[$ $10 \wedge n = 1$

Euler $10^{\varphi(n)}-1 \equiv 0 [n]$, on écrit $10^{\varphi(n)}-1 = kn$, $k \geq 1$

puis $x = \dfrac{km}{10^T - 1}$ où $0 < km < 10^T - 1$

$T = \varphi(n)$

Avec $km = y_0 + y_1 10 + \dots + y_{T-1} 10^{T-1}$

$$x = \frac{(y_0 + y_1 10 + \dots + y_{T-1} 10^{T-1})}{10^T} \left(\sum_{\ell=0}^{\infty} (10^{-T})^{\ell} \right)$$

ie $x = 0, y_{T-1} \dots y_0 \; y_{T-1} \dots y_0 \dots$

IV Théorème de fermat p est premier

Th $\forall m \in \mathbb{N}$, $p / m^p - m$

D/ 1) Rec : lemme : Si $1 \leq k \leq p$ p / C_p^k

Em effet : $k! \, C_p^k = p(p-1) \dots (p-k+1)$

??? $m \geq 0$ $m = 0, 1$ puis si $p / m^p - m$

il vient $(m+1)^p - (m+1) = m^p - m + \sum_{k=1}^{p-1} C_p^k m^k$

2) Avec $(\mathbb{Z}/p\mathbb{Z})^*$ Si p / n, il est clair que $p / n^p - n$

Sinon il vient $\bar{n} \neq \bar{0}$ ds $\mathbb{Z}/p\mathbb{Z}$ et donc $\bar{n}^{p-1} = \bar{1}$ (Lagrange)

donc $p / n^{p-1} - 1 \rightarrow p / n^p - n$

Conséquence Si $Q \in \mathbb{Z}/p\mathbb{Z}[X]$: $Q(X)^p = Q(X^p)$

$P /$

En effet Si R, S $\mathbb{Z}/p\mathbb{Z}[X]$ $(R+S)^p = R^p + \sum_{k=1}^{p-1} C_p^k R^k S^{p-k} + S^p$

De là $Q = a_0 + \dots + a_d X^d$

$Q^p = a_0^p + \dots + a_d^p X^{pd} = Q(X^p)$,

Compléments: résidus quadratiques

$a \in (\mathbb{Z}/p\mathbb{Z})^* \quad \exists b \in \mathbb{Z}/p\mathbb{Z} \;/\; a = b^2$

$a = \bar{x}$, $p \nmid x$ et $\exists y \in \mathbb{Z}, x = y^2 [p]$

Ex Soit p un nbre premier ≥ 3

On note $H = \{ b^2 \mid b \in (\mathbb{Z}/p\mathbb{Z})^* \}$

1) Mq $|H| = \frac{p-1}{2}$

2) Mq $a \in H \Leftrightarrow a^{\frac{p-1}{2}} = \bar{1}$

3) Mq -1 est un carré modulo $p \Leftrightarrow p \equiv 1 [4]$

($X^2 + \bar{1}$ est divisé ds $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p \equiv 1[4]$)

S/ 1) On note $\sim$ la rel d'eq déf par $b \sim b' \Leftrightarrow b^2 = b'^2$

$b^2 = b'^2 \Leftrightarrow (b-b')(b+b') = 0 \Leftrightarrow b' = b$ ou $b' = -b$

Les classes d'équivalence, la bijection, la bijection avec les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$

ont 2 élém distincts $|H| \times 2 = |(\mathbb{Z}/p\mathbb{Z})^*| = p-1$

2) $a \in H$, $a^{\frac{p-1}{2}} = b^{p-1} = \bar{1}$ Fermat

$X^{\frac{p-1}{2}} - \bar{1}$ possède au plus $\frac{p-1}{2}$ racines [illegible] dans

or $H \subset Z(X^{\frac{p-1}{2}} - 1)$ donc $H = Z(X^{\frac{p-1}{2}} - 1)$

par [illegible] : on a la réciproque.

3) On écrit $p = 4q + r$ $r \in \{1, 3\}$

d'où $\frac{p-1}{2} = \frac{4q}{2} + \frac{r-1}{2}$

$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{r-1}{2}} \Rightarrow \begin{cases} r = 3 \Rightarrow -\bar{1} \\ r = 1 \to \bar{1} \end{cases}$

trait $p \equiv 1 \, [4] \Leftrightarrow \exists n \in \mathbb{N} \; p / n^2 + 1$

151