Chap 11 : L'anneau $\mathbb{Z}/n\mathbb{Z}$

I. Construction

$a,b\in\mathbb{Z}$. On définit (correctement) le produit $\bar{a}\times\bar{b}=\overline{a\times b}$. $\left(\mathbb{Z}/n\mathbb{Z},+,\times\right)$ est un anneau commutatif et unitaire.

$s:\begin{cases}\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\\ a\mapsto\bar{a}\end{cases}$ est un morphisme d'anneaux surjectif, de noyau $n\mathbb{Z}$

$n\geq 2.\forall k\in\mathbb{Z}$ $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ *ssi* $k\wedge n=1$ || $\bar{k}$ engendre $\left(\mathbb{Z}/n\mathbb{Z},+\right)$ *ssi* $k\wedge n=1$

$\mathbb{Z}/n\mathbb{Z}$ est un corps *ssi* n est premier

Pour un anneau A, on note $U(A)$ le groupe des éléments inversibles de A.

$^{(I)}k\in\ \llbracket 1,n-1\rrbracket$. Si $d=n\wedge k>1$, $\bar{k}\dfrac{n}{d}=\overline{\left(\dfrac{k}{d}\right)}\bar{n}=\bar{0}$ || $\left|U\left(\mathbb{Z}/n\mathbb{Z}\right)\right|=\varphi(n)$

$P\in\mathbb{Z}/n\mathbb{Z}[X]$. Si n est premier, le nombre de racines de $P\leq\deg P$. (vrai $\forall$anneau intègre commutatif)

Si n non premier, il peut y avoir plus de racines

II. Indicatrice d'Euler, théorème chinois

A,B deux anneaux

$A\times B$ muni des lois : $\begin{cases}(a,b)+(a',b')=(a+a',b+b')\\ (a,b)\times(a',b')=(aa',bb')\end{cases}$ est un anneau d'élément neutre $(1_A,1_B)$

$U(A\times B)=U(A)\times U(B)$ Indicatrice d'Euler : $\varphi(n)=\operatorname{card}U(\mathbb{Z}/n\mathbb{Z})$

Cet anneau n'est jamais intègre || $[x/d]=|\{\text{multiples de } d\leq x\}|$

$m,n\geq 2, m\wedge n=1$ $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ sont isomorphes $\varphi(mn)=\varphi(m)\varphi(n)$

$^{(I)}(a,b)\in\mathbb{Z}$, on cherche $x\in\mathbb{Z}$ tq $x\equiv a[m], x\equiv b[n]\Rightarrow u,v$ tq $um+vn=1$, $x=umb+vna$

p premier $\Rightarrow(n\wedge p^r\neq 1\Leftrightarrow p\mid n)\Rightarrow\varphi(p^r)=p^r\left(1-\dfrac{1}{p}\right)$ $\Rightarrow\varphi\left(\prod_{i=1}^{r}p_i^{\alpha_i}\right)=\prod_{i=1}^{r}p_i^{\alpha_i}\times\prod_{i=1}^{r}\left(1-\dfrac{1}{p_i}\right)$

Fermat : p nombre premier, $\forall x\in\mathbb{Z}, x^p\equiv x[p]$, et si $x\notin p\mathbb{Z}, x^{p-1}\equiv 1[p]$

Théorème d'Euler : $n\geq 2, a\in\mathbb{Z}$. $a\wedge n=1\Leftrightarrow a^{\varphi(n)}\equiv 1[n]$

$^{//HP//}$ Wilson : $p\geq 2$ p premier $\Leftrightarrow(p-1)!\equiv -1[p]$ (racines de $X^{p-1}-\bar{1}$ avec *Fermat*)

$^{(I)}G=(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique ($c\in G$ tq $N=\omega(c)=ppcm\{\omega(a)\}_{a\in G}$,

$\forall a\in G, a^N=\bar{1}\Rightarrow N\leq p-1$ (nb racines ds 1 corps $\leq$ deg P), $c^{p-1}=\bar{1}\Rightarrow N\mid p-1$)

$^{(I)}$Résidus quadratiques : $p\geq 3$ premier. Le nb de carrés de $\mathbb{Z}/p\mathbb{Z}^*$ est $\dfrac{p-1}{2}$: c'est l'ens. des racines de $X^{\frac{p-1}{2}}-\bar{1}$

$\forall a\in\mathbb{Z}/p\mathbb{Z}^*, a^{\frac{p-1}{2}}\in\{-\bar{1};\bar{1}\}$ $\overline{-1}$ est carré dans $\mathbb{Z}/p\mathbb{Z}$ *ssi* $p\equiv 1[4]$