COURS 1 (17 janvier 2024)

Chapitre 1 : Les nombres premiers

* Un nombre entier $n \geq 2$ est premier si les seuls diviseurs de n sont 1 et n. Autrement, on note p les nbs premiers et $\mathcal{P}$ l'ensemble qu'ils forment.

* Si n n'est pas premier, alors n est divisible par un nbre premier $p \leq \sqrt{n}$.

* Crible d'Eratosthène :

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

$\Longrightarrow \mathcal{P} \cap \{1, \dots, 19\} = \{2, 3, 5, 7, 11, 13, 17, 19\}$

(en fait pour calculer $\mathcal{P} \cap \{1, \dots, N\}$, il suffit de rayer les multiples de $p \leq \sqrt{N}$).

* Lemme d'Euclide :

Lemme : Soient a et b des nbres entiers et soit p un nbre premier qui divise ab. Alors p divise a ou p divise b.

Démonstration : Supposons que p ne divise pas a.
Soit $n = \min\{m > 1 \mid p \text{ divise } am\}$. On a

$$1 < n \leq p.$$

Soit $p = nq + r$ la division euclidienne. $0 \leq r < n$
On a alors

$$ar = ap - anq = ap - (an)q \Rightarrow p \mid ar$$

d'où $r = 0$ par minimalité de n. Donc,
$p = nq \Rightarrow \boxed{n = p}$ car p est premier.
D'un autre côté, p divise ab par hypothèse,
d'où $p = n \leq b$. Soit $b = pn + s$ la
division euclidienne. Alors :

$$as = ab - apn = (ab) - (an)p \Rightarrow p \mid as$$

s est multiple de p, d'où $s = 0$ comme avant

$\Rightarrow p$ divise b ∎

(Avec un peu plus de théorie)

$$G = \{n \in \mathbb{Z} \mid p \text{ divise } an\} \subseteq \mathbb{Z}$$

est un sous-groupe, on revient à la
car il contient p, donc $G = n\mathbb{Z}$ pour
le même n qu'avant.

Si p ne divise pas a, alors $n > 1$. Comme $p \in n\mathbb{Z}$, $p = n$. Par hypothèse, $b \in G$, donc $n = p$ divise b

* Variante : Soient a, b des entiers pas tous deux nuls. Alors

$$\langle a, b \rangle = \{ an + bm \mid n, m \in \mathbb{Z} \} \subset \mathbb{Z}$$

$$= \underbrace{pgcd(a,b)}_{\text{le plus petit élément } \geq 1 \text{ de } \langle a,b \rangle} \cdot \mathbb{Z}$$

$a, b \in \langle a, b \rangle$
$\Rightarrow pgcd(a,b) \mid a$
$pgcd(a,b) \mid b$
et c'est le plus grand avec cette propriété

En particulier, pour $d = pgcd(a,b)$, on a une relation

$$d = au + bv \qquad \text{(Bézout)}$$

Si $d = 1$, on dit que a et b sont premiers entre eux.

Proposition : Soit n un entier ≥ 2.

① Soit a un nombre entier. Alors :

a et n sont premiers entre eux

$\Leftrightarrow$ a mod n est inversible dans $\mathbb{Z}/n\mathbb{Z}$

② n est un nbre premier

$\Leftrightarrow$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps

$\Leftrightarrow$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre

(c'est-à-dire, ne contient pas de diviseur de zéro)

$\boxed{\Rightarrow}$

Démonstration : ① Si a et n sont premiers entre eux, alors $1 = au + nv$, (Bézout) d'où

$1 = \bar{1} \equiv \bar{a}\bar{u} \pmod{n}$,

c'est-à-dire $\bar{a}$ est inversible.

$\boxed{\Leftarrow}$ Si $\bar{a}$ est inversible, alors il existe $b \in \mathbb{Z}$ tel que $1 \equiv \bar{a}.\bar{b} \pmod{n}$. On a donc $1 = ab + nv$, ce qui entraîne que a et n sont premiers entre eux

② Si n est premier, n est premier avec tout $1 \leq a < n$, donc tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible par ①.

On a toujours corps $\Rightarrow$ intègre.

Si n n'est pas premier, alors $n = ab$ pour $1 < a, b < n$, donc $0 \equiv \bar{a}.\bar{b} \pmod{n}$ ($\bar{a} \neq 0$, $\bar{b} \neq 0$)

donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. ∎

Notation :

$$\varphi(n) = \left| \{ a \mid 1 \leq a \leq n \text{ premiers avec } n \} \right|$$

$$= \left| (\mathbb{Z}/n\mathbb{Z})^\times \right|$$

indicatrice d'Euler

Lemme chinois : Soient m et n des entiers premiers entre eux. Alors

$$f : \mathbb{Z}/mn \xrightarrow{\sim} \mathbb{Z}/m \times \mathbb{Z}/n$$

$$a \longmapsto (a \bmod m,\ a \bmod n)$$

f : surjective d'ensemble

d'où : $(\mathbb{Z}/mn)^\times \simeq (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$

et en particulier $\varphi(mn) = \varphi(m)\varphi(n)$

(c'est une fonction multiplicative).

Démonstration : * Il suffit de montrer que f est surjective. Soient $x \bmod m$, $y \bmod n$.

Comme n et m sont premiers entre eux, $1 = nu + mv$ et on pose

$$z = nxu + myv$$

Alors : $z \bmod m = nxu = x(1-mv) \equiv x \bmod m$

$z \bmod n = myv = y(1-nu) \equiv y \bmod n$

* Si $f : A \to B$ est un isomorphisme d'anneaux, alors $f_{|A^\times} : A^\times \to B^\times$ est un isomorphisme de groupes et $(B \times C)^\times \simeq B^\times \times C^\times$ □

Généralisation à plusieurs entiers

$$\mathbb{Z}/m_1 \dots m_\ell \mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_\ell \mathbb{Z}$$

Si $m_1, \dots, m_\ell$ deux à deux premiers entre eux.
et de même pour les inversibles

* Factorisation

Théorème : Pour tout entier $n \geq 1$, il existe des nombres premiers p_i et des exposants $q_i \geq 1$ tels que

$$n = p_1^{q_1} \dots p_2^{q_2}$$

et cette "factorisation" est unique à l'ordre des facteurs près.

Démonstration : par récurrence sur n.

Pour $n=1$, produit vide / supposons le résultat vrai pour les entiers $< n$. On écrit :

$$n = p\,n' \qquad 1 \leq n' < n$$

$$= p\,p_1^{a_1} \cdots p_2^{a_2} \quad \text{par récurrence}$$

Unicité de la factorisation :

$$n = p_1^{a_1} \cdots p_2^{a_2} = q_1^{b_1} \cdots q_s^{b_s}$$

Chaque p_i divise le produit $q_1^{b_1} \cdots q_s^{b_s}$, donc par le lemme d'Euclide divise un des facteurs, donc $p_i = q_j$ pour un certain j. De même, $q_i = p_j$ pour un certain j. Donc $r = s$ et $\{p_1, \ldots, p_2\} = \{q_1, \ldots, q_s\}$, puis $a_i = b_i$ en appliquant encore Euclide. □

Plus généralement, n'importe quel $x \in \mathbb{Q}^\times$ s'écrit de manière unique comme

$$x = \varepsilon \prod_{p \in \mathcal{P}} p^{a_p} \qquad \varepsilon \in \{\pm 1\}$$

$(a_p)_{p \in \mathcal{P}}$ presque tous nuls $a_i \in \mathbb{Z}$

Définition : $a_p = \mathrm{ord}_p(x)$ valuation p-adique

$\mathrm{ord}_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ $\quad \mathrm{ord}_p(0) = \infty$

satisfait à

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$$

$$\mathrm{ord}_p(x+y) \geq \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))$$

avec égalité si $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$.

* $x \in \mathbb{Q}$ est dans $\mathbb{Z} \iff \mathrm{ord}_p(x) \geq 0$ pour tout p

* L'ensemble des nbs premiers est infini.

En effet, autrement $\mathcal{P} = \{p_1, \dots, p_m\}$. Alors $N = p_1 \cdots p_m + 1 > 1$ est multiple d'un nbre premier, mais aucun des p_i divise N $\lightning$

Buts de la première moitié du cours

- Théorème des nbs premiers (Hadamard, de la Vallée-Poussin, 1896)

Pour $X > 0$ réel, posons

$$\pi(X) = \{p \leq X \mid p \text{ premier}\}$$

Alors, $\pi(X) \sim \dfrac{X}{\log X}$ lorsque $X \to \infty$.

(i.e. $\lim\limits_{X \to \infty} \pi(X) \dfrac{\log X}{X} = 1$)

• Théorème de la progression arithétique (Dirichlet) 1837

Soient a et n des entiers premiers entre eux. Alors il existe une infinité de nbs premiers de la forme $a + kn$ (c'est-à-dire congrus à a modulo n)

② Critères de primalité et de non-primalité

Comment savoir si un nbre donné n est premier ou pas ? La méthode de essayer tous les premiers $\leq \sqrt{n}$ est en pratique impraticable.

→ Critère de Fermat. Soit p un nbre premier. Pour tout entier a qui n'est pas multiple de p, on a $a^{p-1} \equiv 1 \mod p$. (« petit théorème de Fermat »)

Démonstration : Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe de cardinal $p-1$. Donc $a^{p-1} = 1$ pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ □

Application : S'il existe $a \in \{1, \dots, n-1\}$ tel que $a^{n-1} \not\equiv 1 \mod n$, alors n n'est pas premier.

⚠ ce n'est pas un critère de primalité :
il existe des nbres, tels que $561 = 3 \times 11 \times 17$,
avec la propriété $a^{n-1} \equiv 1 \pmod n$ pour
tout $1 \leq a < n$ premier à n.
(nbres de Carmichael)

→ Test de Miller-Rabin

Proposition : Soit $p \geq 3$ premier. Écrivons
$p-1 = 2^s m$. Soit a un nbre entier non
multiple de p. Soit $s \geq 0$ le plus petit
tel que $a^{2^s m} \equiv 1 \pmod p$. Si $s > 0$,
alors $a^{m 2^{s-1}} \equiv -1 \pmod p$.

Démonstration : Si $s > 0$, $a^{2^s m} = \left(a^{2^{s-1} m}\right)^2$.
Si p est premier et $b^2 \equiv 1 \pmod p$, alors
$p \mid b^2 - 1 = (b-1)(b+1)$, donc par le
lemme d'Euclide $p \mid b-1 \iff b \equiv 1 \pmod p$
ou $p \mid b+1 \iff b \equiv -1 \pmod p$

Comme $a^{2^{s-1} m} \equiv 1 \pmod p$ contredit la minimalité
de s, on a $a^{2^{s-1} m} \equiv -1 \pmod p$ □

(test de non-primalité)

→ Critère de Lucas :

Quelques propriétés des groupes finis :

Lemme : G groupe abélien fini

$g, h \in G$ d'ordres m, n

Si m et n sont premiers entre eux, alors gh est d'ordre mn.

Démonstration : $\langle g \rangle \cap \langle h \rangle = \{e\}$ dans G car si $x \in \langle g \rangle \cap \langle h \rangle$, l'ordre de x divise m et divise n, donc est égal à 1

Si $(gh)^N = 1$, alors $g^N = h^{-N}$ car G est commutatif. On a donc $g^N = h^{-N} = 1$, ce qui entraîne $n \mid N$, $m \mid N$, donc $mn \mid N$. D'autre part,

$$(gh)^{mn} = g^{mn} h^{mn} = (g^n)^m (h^m)^n = 1$$

□

Proposition : G groupe abélien fini, $S \subset G$ sous ensemble. Il existe un élément de G d'ordre le ppcm(ordres des éléments de S)

Démonstration : Il suffit de voir que si G possède g d'ordre m et h d'ordre n, alors il possède un élément d'ordre $\mathrm{ppcm}(m,n)$. On écrit :

$m = m' m''$ si $\mathrm{ord}_p(m) \geq \mathrm{ord}_p(n)$ $\Rightarrow$
$n = n' n''$

si $\mathrm{ord}_p(m) < \mathrm{ord}_p(n)$

m et p dans m'', n''

$g^{m''}$ d'ordre m' ⟵ premiers entre eux
$h^{n'}$ d'ordre n'' ⟵

$m' n'' = \mathrm{ppcm}(m,n)$

$\Longrightarrow$ l'ordre de $g^{m''} h^{n'}$ est $\mathrm{ppcm}(m,n)$ □

Lemme

Théorème : Soit $n \geq 2$ un entier. Supposons que pour tout $p \mid n-1$, il existe un entier a tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$. Alors n est un nombre premier.

Démonstration : Si $a^{n-1} \equiv 1 \bmod n$, alors a et n sont premiers entre eux. (a est inversible) Pour tout $p \mid n-1$, il existe $a_p \in (\mathbb{Z}/n\mathbb{Z})^\times$ dont l'ordre divise $n-1$ mais pas $\frac{n-1}{p}$. Le ppcm de ces ordres est égale à $n-1$. Par la proposition, il existe un élément d'ordre $n-1$. Donc

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = n-1 \Rightarrow n \text{ est premier} \quad \square$$

Remarque : Nous avons donc démontré que, sous les hypothèses du théorème, $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. C'est toujours le cas pour n premier, ce qui montre que le théorème est mieux si et seulement si.

Théorème : Soit F un corps et soit $G \subset F^\times$ un sous-groupe fini. Alors G est cyclique.

Démonstration 1 : Soit $g \in G$ un élément d'ordre multiple de tous les éléments de G (autrement dit avec $S = G$). Posons $n = \mathrm{ord}(g)$. Alors

$$x^n = 1 \quad \text{pour tout } x \in G$$

L'équation $x^n = 1$ a au plus n solutions (car F est un corps). Comme

$$1, g, g^2, \dots, g^{n-1}$$

sont solutions, on a $G = \langle g \rangle$ □

Démonstration 2 : Soit $n = |G|$. D'après le lemme, il suffit de trouver $g_p \in G$ d'ordre $p^{\mathrm{val}_p(n)}$ (= 2) pour tout $p \mid n$.

L'équation $x^{n/p} = 1$ a au plus $\frac{n}{p} < n$ solutions, donc il existe $x \in G$ tel que $x^{n/p} \neq 1$.

Posons $y = x^{n/p^2}$. On a $y^{p^2} = 1$, $y^{p^{2-1}} = x^{n/p} \neq 1$.

Donc l'ordre de y divise p^2 mais pas p^{2-1},

donc $g_p = y$ convient □

Exemple : calcul d'un générateur de $(\mathbb{Z}/71\mathbb{Z})^\times$

$71 - 1 = 70 = 2 \times 5 \times 7$

on cherche des éléments d'ordre 2, 5, 7

ordre 2 : $-1 = g_2$

ordre 5 : on cherche $x^{14} \neq 1 \mod 71$

$2^{14} \equiv 4^7 \equiv 4 \cdot (16)^3 \equiv 4 \cdot 16 \cdot 256$

$\equiv \underbrace{4 \cdot 16}_{64} \cdot 43 \equiv (-7) \cdot 43 \equiv -301 \equiv -17$

$\Rightarrow g_5 = -17$

ordre 7 : on cherche $x^{10} \neq 1 \mod 71$

$2^{10} \equiv 16 \cdot 64 \equiv 16 \cdot (-7) \equiv -112 \equiv 30$

$\Rightarrow g_7 = 30$

$g_2 g_5 g_7 = (-1) \cdot (-17) \cdot 30 \equiv 510 \equiv 13$

donc $(\mathbb{Z}/71\mathbb{Z})^\times = \langle 13 \rangle$.