Page 1 Christian PAULY
bureau 308 bât 9
pauly@math.univ-montp2.fr
feuilles de TD sur l'ENT.
Livre : Introduction à la cryptographie.
(Johannes Buchmann ; DUNOD ; §1 et 2)

Chapitre 1 : ensembles

$\mathbb{N} = \{0, 1, 2, \dots\}$ entiers naturels $= \mathbb{Z}_+$
$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$ entiers relatifs.
Lois de composition : $+, \cdot$
$\mathbb{Q} = \{\frac{a}{b} = x ;\ a \in \mathbb{Z}, b \in \mathbb{Z}^*\}$ nombres rationnels.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$
$$b \longmapsto \frac{b}{1}$$

Définition :

$x \in \mathbb{R}$. $\lfloor x \rfloor = E(x) =$ le plus gd des entiers $\leq x$.
$= \max\{b \in \mathbb{Z} / b \leq x\}$

Exemple :

$\lfloor \pi \rfloor = 3$; $e = 2,718 = \sum_{n \geq 0} \frac{1}{n!} \Rightarrow \lfloor e \rfloor = 2$
$\lfloor -\pi \rfloor = -4$

Une propriété de la partie entière : $\boxed{\lfloor x \rfloor \in \mathbb{Z}}$

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Chapitre 2 : Divisibilité :

Définition :

On dit que a divise n si $n = a.b$ pour un $b \in \mathbb{Z}$.
$a \in \mathbb{Z}$, $n \in \mathbb{Z}$

Notation :

a divise n, on écrit a/n.

Théorèmes :

1) Si $a|b$ et $b|c$, alors a/c.
2) Si $a|b$, alors $ac|bc$ pour tout entier c.
3) Si $c|a$ et $c|b$, alors $c|da+eb$ pour tous $d, e \in \mathbb{Z}$.
4) Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$.
5) Si $a|b$ et $b|a$, alors $|a| = |b|$.

Théorème (Division euclidienne) :

Soient $a, b \in \mathbb{N}$, alors il existe des entiers q et r ($q, r \in \mathbb{N}$) tq $a = bq + r$. q et r sont uniques. $0 \leq r < b$. q est le quotient de la division euclidienne de a par b et r on est le reste. $b \neq 0$

Démonstration :

$a = bq + r$. On divise par $b \neq 0$.

$$\underset{\mathbb{Q}}{\underset{\cap}{\frac{a}{b}}} = \underset{\mathbb{N}}{\underset{\cap}{q}} + \frac{r}{b}$$ on sait que $0 \leq \frac{r}{b} < 1$

$$\Rightarrow \left\lfloor \frac{a}{b} \right\rfloor = q$$

On prend $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r = a - b\left\lfloor \frac{a}{b} \right\rfloor$

Page 2 Notation :

r reste $= a \bmod b$, appelé le "reste de a modulo b".

Exemple :

$a = 133$, $b = 21$, $q = 6$, $r = 7$
$133 = 21 \cdot 6 + 7$.

Chapitre 3 : Le PGCD :

Soient $a, b \in \mathbb{N}$.

Définition :

Un diviseur commun à a et b est un entier d tel que $d|a$ et $d|b$.

$$1 \leq d \leq a \text{ et } 1 \leq d \leq b$$

Il n'y a qu'un nombre fini de diviseurs communs à a et b. On appelle le plus gd de ces diviseurs communs le PGCD (a,b).

Exemple :

PGCD $(18, 30)$:
$\text{div}(18) = \{1, 2, 3, \underline{6}, 9, 18\}$
$\text{div}(30) = \{1, 2, 3, 5, \underline{6}, 10, 15, 30\}$

Soient $a, b \in \mathbb{N}$:

$$a\mathbb{Z} + b\mathbb{Z} = \{\alpha_1 a + \alpha_2 b \mid \alpha_1, \alpha_2 \in \mathbb{Z}\} \subset \mathbb{Z}$$

ensemble des combinaisons linéaires de a et b. ss-ens ∞

Exemple :

$\underbrace{3\mathbb{Z}+4\mathbb{Z}}_{3\alpha_1+4\alpha_2} \subset \mathbb{Z}$

$1 = 3(-1) + 4\times 1$

$PGCD(4,3) = 1$

Définition :

On dit que a et b sont premiers entre eux sur leur PGCD vaut 1.

Théorème :

L'ensemble des combinaisons linéaires de a et b :

$$a\mathbb{Z}+b\mathbb{Z} = PGCD(a,b).\mathbb{Z}.$$

Démonstration :

*) On montre que l'ensemble $a\mathbb{Z}+b\mathbb{Z}$ est de la forme $g\mathbb{Z}$.

On prend le plus petit élément positif non nul de $a\mathbb{Z}+b\mathbb{Z}$ et on l'appelle g. Prenons $c \in a\mathbb{Z}+b\mathbb{Z}$ et considérons la divis° euclidienne de c par $g \geq 0$. On a :

$$c = gq + r \ , \ 0 \leq r < g$$

et on peut écrire $r = c - gq$

d'où $qg \in a\mathbb{Z}+b\mathbb{Z}$

$\hookrightarrow \in a\mathbb{Z}+b\mathbb{Z}$

$0 \leq r < g$, par minimalité de $g \Longrightarrow r = 0$

$\Longrightarrow c = qg$

$\Longrightarrow a\mathbb{Z}+b\mathbb{Z} = g\mathbb{Z}$

Page 3

*) Reste à montrer que $g = \mathrm{PGCD}(a,b)$

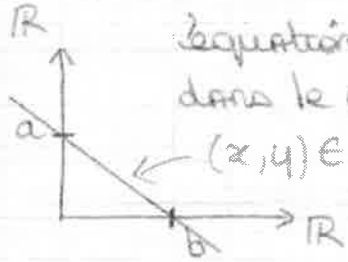
$$\underset{\substack{\cup\!\!\!\!\shortmid \\ g}}{g\mathbb{Z}} = \underset{\substack{\cup\!\!\!\!\shortmid \\ a = 1a + 0b \\ b = 0a + 1b}}{a\mathbb{Z}} + \mathbb{Z}b \Rightarrow g|a \text{ et } g|b$$

reste à montrer que g est le plus gd des diviseurs communs. Si $d|a$ et $d|b$, il faut montrer que $d|g$.

Comme $g \in a\mathbb{Z} + b\mathbb{Z}$, il existe des entiers $x, y \in \mathbb{Z}$ tels que : $g = xa + yb$.

Corollaire :

L'équation $ax + by = n$, avec $a, b, n \in \mathbb{Z}$ données et x, y indéterminées.



l'équation d'une droite affine $ax + by = n$ dans le plan $\mathbb{R}^2$.

$(x,y) \in \Delta \iff x + y = 3$

Il y a des solutions x, y <u>ssi</u> $\mathrm{PGCD}(a,b)$ divise n.

Démonstration :

$$a\mathbb{Z} + \mathbb{Z}b = \mathrm{PGCD}(a,b) \cdot \mathbb{Z}.$$

$$\gamma xa + yb\gamma = \underset{}{\overset{\cup\!\!\!\!\shortmid}{\mathrm{PGCD}}}(a,b)$$

d'après le théorème précédent.

1) Si l'éq° a une solut° (x,y) tel que $ax + by = n$ on sait que : $n \in a\mathbb{Z} + b\mathbb{Z} = \underset{\substack{\cup\!\!\!\!\shortmid \\ n}}{\mathrm{PGCD}(a,b)}$

2) Si $n = \underset{\substack{\cap \\ \mathbb{Z}}}{\gamma}\, \mathrm{PGCD}(a,b)$, on peut écrire

$$PGCD(a,b) = ax + by$$

je multiplie avec γ

$$n = \gamma PGCD(a,b) = (\gamma x)a + (\gamma y)b$$

Par récurrence, on définit le PGCD de n nombres $a_1, a_2, \ldots, a_n$:

$$PGCD(a_1, a_2, a_3) = PGCD(a_1, PGCD(a_2, a_3))$$

Autre descript° du PGCD (a, b) :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

p_i = nb premiers , α_i = puissances de $p_i \in \mathbb{N}^*$

$$\beta_i = \text{———} \; p_i$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$$

$$PGCD(a,b) = p_1^{\min(\alpha,\beta)} p_2^{\min(\alpha,\beta)} \ldots p_n^{\min(\alpha,\beta)}$$

Exemple :

$PGCD(18, 30) = 6$

On décompose en nb premiers (produit)

$$18 = 2^1 \times 3^2 \times 5^0$$
$$30 = 2^1 \times 3^1 \times 5^1$$
$$6 = 2^1 \times 3^1 \times 5^0$$

Arithmétique de $\mathbb{Z}$ et corps finis

Page 1 Contrôle continu le jeudi après les vacances de Pâques (23/04/09)

Prof absent la semaine avant les vacances de Pâques (du 4/04 au 11/04)

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

$d = PGCD(a,b)$

$$\underbrace{d\mathbb{Z}}_{\{n \in \mathbb{Z} \mid n = dk,\ k \in \mathbb{Z}\}} = a\mathbb{Z} + b\mathbb{Z}$$

PGCD(a,b) = le + gd des diviseurs communs à a et b.

Remarque :

Tout diviseur commun à a et b est aussi un diviseur du PGCD.

PGCD$(a,b) = xa + yb$ $(*)$

Soit d un diviseur commun à a et b, $d \mid a$ et $d \mid b$

donc d'après $(*)$: $d \mid PGCD(a,b)$.

propriétés.

~~Algorithme d'Euclide~~ : $(a, b \geq 0)$

Propositions :

- PGCD$(a,0) = a$
- PGCD$(a,b) = $ PGCD$(b, \overbrace{a \bmod b})$ (avec $a \geq b$)

où $a \bmod b$ est le reste de la division euclidienne de a par b.

Démonstration :

$a = bq + r \iff r = bq - a$
$\Rightarrow PGCD(a,b) \mid r$
et $PGCD(a,b) \mid b$

d'où :
$PGCD(a,b) \mid PGCD(r,b)$
Comme $a = bq + r$, par le même raisonnement on montre que :
$$PGCD(r,b) \mid PGCD(a,b)$$

Donc, d'après un exo de TD :
$$PGCD(a,b) = PGCD(b,r). \quad \text{CQFD}$$

On a $0 \leq r < b$
d'où l'Algorithme d'euclide :
$$PGCD(a,b) = PGCD(b,r)$$

Exemple : $PGCD(\underbrace{100}_{a}, \underbrace{35}_{b})$

$\underbrace{100}_{a} = 2 \times \underbrace{35}_{b} + \underbrace{30}_{r}$

d'où $PGCD(100, 35) = PGCD(\underbrace{35}_{a}, \underbrace{30}_{b})$

$\underbrace{35}_{a} = 1 \times \underbrace{30}_{b} + \underbrace{5}_{r}$

d'où $PGCD(35, 30) = PGCD(\underbrace{30}_{a}, \underbrace{5}_{b})$

$\underbrace{30}_{a} = 6 \times \underbrace{5}_{b} + \underbrace{0}_{r}$

d'où $PGCD(30, 5) = PGCD(\underbrace{5}_{a}, \underbrace{0}_{b}) = 5$

Page 2 Théorème :

L'algorithme d'euclide calcule le PGCD (a,b)
Il consiste à remplacer le couple (a,b) par le couple (b,r).

Démonstration :

Il suffit de montrer que l'algo d'Euclide s'arrête après un nb fini d'itérat° car le PGCD (a,b) est invariant dans l'opération $(a,b) \mapsto (b,r)$.
On introduit la suite des restes $(r_k)_{k\in\mathbb{N}}$ avec :

$$r_0 = a \text{ et } r_1 = b \text{ et } r_2 = r_0 \bmod r_1 = a \bmod b$$

$$\underbrace{r_{k+1} = r_{k-1} \bmod r_k}_{r_2} \Longleftrightarrow r_{k-1} = q_k r_k + r_{k+1}$$

exemple : On reprend 100 et 35.

k	0	1	2	3	4
r_k	100	35	30	5	0
q_k	//	2	1	6	//

Point clé : $\boxed{r_{k+1} < r_k}$ $\forall k \in \mathbb{N}$

donc la suite des restes $(r_k)_{k\in\mathbb{N}}$ est strictement ↘
donc il existe 1 entier $n \in \mathbb{N}$ tel que $r_n \neq 0$, $r_{n+1} = 0$

$\Longrightarrow$ L'algo s'arrête !

Propositions :

- $q_k \geq 1$ pour $1 \leq k \leq n-1$
- $q_n \geq 2$ (en effet : par déf. $r_{n+1} = 0$. $r_{n-1} = q_n r_n$
  $r_n \neq 0$. or $r_n < r_{n-1} \Rightarrow q_n \geq 2$).

Démonstrations :

- Il suffit de montrer que $q_k \neq 0$ pour $1 \leq k \leq n-1$
  Si $q_k = 0$, on aurait $r_{k-1} = r_{k+1}$, ce qui est impossible car $r_{k+1} < r_{k-1}$.

- De plus si $q_n = 1$, on a :
  $$r_{n-1} = r_n$$
  ce qui contredit $r_{n-1} > r_n$.

Théorème :

On suppose $a > b > 0$ et on note $\theta = \underbrace{\frac{1+\sqrt{5}}{2}}_{\text{Nb d'or}}$,
Alors le nombre d'itérations de l'algo² d'Euclide est au + :

$$\boxed{\frac{\ln b}{\ln \theta} + 1 < 1,441 . \log_2(b) + 1}$$

on écrit :
$$b = 2^{\log_2(b)}$$
$$\ln(b) = \log_2(b) \cdot \ln(2).$$

$\ln b$ = logarithme népérien, càd le log dans la base du nb d'Euler $e = \sum_{n=0}^{\infty} \frac{1}{n!} \simeq 2,718$

Démonstration :

Il suffit de calculer le nombre d'itérations qd $PGCD(a,b) = 1$.
Supposons que $PGCD(a,b) = d$ (d qcq)
$d = r_n$ (r_n dernier reste non nul)
Si je prends $PGCD(\frac{a}{d}, \frac{b}{d})$ au lieu de $PGCD(a,b)$
On a : $\frac{r_n}{d} = \frac{d}{d} = PGCD(\frac{a}{d}, \frac{b}{d})$

Arithmétique de $\mathbb{Z}$ et corps finis

Page 3 On va montrer que si $r_n = 1$,
$$r_k \geq \theta^{n-k} \text{ pour } 0 \leq k \leq n$$

Posons $b = r_1 \geq \theta^{n-1}$ si on suppose que l'inégalité du dessus est vraie.

On prend le $\ln$:
$$\ln(b) \geq (n-1)\ln\theta$$
$$\iff \frac{\ln(b)}{\ln\theta} \geq n-1$$
$$\iff n \leq \frac{\ln(b)}{\ln\theta} + 1$$

Nous allons montrer que $r_k \geq \theta^{n-k}$ par récurrence descendante sur k.

pour $k = n$, $k = n-1$, ...

$\underline{k=n :}$ $r_n \geq \theta^0 = 1$ OK

$\underline{k=n-1 :}$ $r_{n-1} = \underbrace{q_n}_{\geq 2} - \underbrace{r_n}_{=1} \geq \theta^{-1} = \frac{1+\sqrt{5}}{2}$

Reste à vérifier qu'on a $r_k \geq \theta^{n-k}$. Si on suppose qu'on a cette inégalité $\forall k' \geq k$:
$$r_k = \underbrace{q_{k+1}}_{\geq 1} r_{k+1} + r_{k+2} \geq \underbrace{r_{k+1}}_{\geq \theta^{n-k-1}} + \underbrace{r_{k+2}}_{\theta^{n-k-2}} = \theta^{n-k}$$

propriété du Nb d'or

$\theta^2 + \theta - 1 = 0$.

$\theta = \frac{+1 \pm \sqrt{5}}{2}$ | $\theta = \frac{-1+\sqrt{5}}{2}$

$\frac{3}{2} < \theta < 2$

$\boxtimes$

Algo d'Euclide étendu :

$$\mathrm{PGCD}(a,b) = xa + yb \quad (x, y \in \mathbb{Z}) \quad (*)$$

L'algo d'Euclide étendu calcule les entiers x et y de la relation $(*)$.

On introduit les 2 suites $(x_k)_{k\in\mathbb{N}}$ et $(y_k)_{k\in\mathbb{N}}$ et on trouve x et y comme :

$$\boxed{x = (-1)^n x_n \text{ et } y = (-1)^{n+1} y_n}$$

$x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$

$x_{k+1} = q_k x_k + x_{k-1}$ et $y_{k+1} = q_k y_k + y_{k-1}$ $(0 \leq k \leq n)$

exemple :

	//	2	1	6	//
k	0	1	2	3	4
x_k	1	0	1	1	7
y_k	0	1	2	3	20

$n = 3$

On a repris $a = 100$ et $b = 35$ (cf tableau précédent)

$x = -1$ et $y = 3$

donc PGCD (100, 35) :

$5 = (-1) \times 100 + 3 \times 35$

Proposition :

$r_k = (-1)^k x_k a + (-1)^{k+1} y_k b$ pour tout $1 \leq k \leq n+1$

Remarque :

En particulier pour $k = n$, $r_n = \text{PGCD}(a,b) = xa + yb$

Démonstration : Par récurrence sur k.

$k = 0$, $r_0 = a = 1.a + (-1).0.b$ OK

$k = 1$, $r_1 = b = (-1).0.a + 1.b$

On suppose que c'est vrai $\forall k' < k$.

$$r_k = r_{k-2} - q_{k-1} r_{k-1} \iff r_k = \left((-1)^{k-2} x_{k-2} a + (-1)^{k-1} y_{k-2} b\right) - q_{k-1}\left((-1)^{k-1} x_{k-1} a + (-1)^k y_{k-1} b\right)$$

Page 1 Dém : (Suite)

$$= a\underbrace{\left((-1)^{k-2}x_{k-2} - q_{k-1}(-1)^{k-1}x_{k-1}\right)}_{=(-1)^k x_k} + b\underbrace{\left((-1)^{k-1}y_{k-2} - q_{k-1}(-1)^k y_{k-1}\right)}_{=(-1)^{k+1}y_k}$$

$$= (-1)^k x_k a + (-1)^{k+1} y_k b.$$

Nombres premiers :

Définition :

On dit qu'un entier $n \in \mathbb{N}$ est premier s'il a exactement 2 diviseurs, 1 et n.
Si n n'est pas premier, on dit qu'il est composé.

Nombres premiers : 2, 3, 5, 7, 11, 13, 17, 23, 29, ...

Théorème :

Tout nb entier $a > 1$ admet un diviseur premier.

Démonstration :

On considère tous les diviseurs positifs > 1 de a. C'est 1 ensemble fini et non vide, car $a | a$, et on considère le plus petit diviseur > 1 de a. Celui là est premier : $1 < p < a$ et $p | a$.
Si on suppose que p est composé, il admet 1 diviseur d et $d \neq 1$ et $d \neq p$.

$d < p < a$

Comme d/p et $p|a$, on a aussi $d|a$. Mais, comme p est le plus petit diviseur de a, on a $\perp$ contradiction ! Donc p est premier.

Théorème de Gauss :

Soient $a, b \in \mathbb{Z}$ et $\text{pgcd}(a,b) = 1$, alors :

(1) $a|bc \Rightarrow a|c$.

(2) $a|c$ et $b|c \Rightarrow ab|c$.

Démonstration :

(1) Si $\text{pgcd}(a,b) = 1$, alors il existe des entiers $x, y \in \mathbb{Z}$ tels que : $ax + by = 1 \quad) \times c$

$$acx + bcy = c \quad (*)$$

Si $a|bc$, alors a divise aussi $c = acx + bcy$.

(2) Il existe $k \in \mathbb{Z}$, $c = ka \Leftrightarrow c|a$

// $k' \in \mathbb{Z}$, $c = k'b \Leftrightarrow c|b$

On remplace dans $(*)$: $a(k'b)x + b(ka)y = c$

$$ab(k'x + ky) = c$$

$$\Rightarrow ab|c.$$

Proposition :

Soit p un nb premier ~~et soit~~ m, n des entiers quelconques. Si $p|mn$, alors $p|m$ ou $p|n$.

Page 2 **Démonstration :**

Si $p \mid mn$ $\begin{cases} p \mid m \text{ , OK.} \\ p \nmid m \iff pgcd(p,m) = 1 \end{cases}$ et d'après le th de Gauss (1), on obtient que $p \mid n$, OK.

Corollaire :

Si p divise un produit de nb premiers $\prod_{i=1}^{k} q_i$,

Alors p est égal à un des nb premiers q_i.

Démonstration :

Récurrence sur le nb de facteurs k.

- Si $k=1$, $p \mid q_1 \Rightarrow p = q_1$.
- Si on suppose que c'est vrai à l'ordre $k-1$ et que :

$$p \mid \prod_{i=1}^{k} q_i = q_1 q_2 \cdots q_k = q_1 (q_2 \cdots q_k)$$

On applique la proposition précédente avec $m = q_1$ et $n = q_2 \cdots q_k$.

Si $p \mid q_1 \cdots q_k \Rightarrow \underbrace{p \mid q_1}_{\Downarrow \; p = q_1}$ ou $\underbrace{p \mid q_2 \cdots q_k}_{\Downarrow \; p = q_i \text{ pour } i = 2, \dots}$ ← $(k-1)$ facteur

Cela montre l'hypothèse de récurrence à l'ordre k.

▨

Vient plus tard !

~~La fonction d'Euler :~~ (plus tard)

Soit $m \in \mathbb{N}^*$. On définit $\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^*\right|$

D'après la description précédente :

$$\varphi(m) = \#\{a \in \mathbb{N},\ 0 < a \leq m \text{ et } \operatorname{pgcd}(a,m) = 1\}$$

fonction d'Euler

Exemples :

1) $\varphi(12) = 4$
2) Si $m = p$ premier, alors $\varphi(p) = p - 1$
$= \#\{a \in \mathbb{N}, 0 < a < p, \cancel{\operatorname{pgcd}(a,p) = 1}\}$

Théorème :

On a la formule $\displaystyle\sum_{d/m} \varphi(d) = m$

Démonstration :

$$\sum_{d/m} \varphi(d) = \sum_{\substack{d/m \\ \frac{m}{d}/m}} \varphi(m/d)$$

l'applicat° $d \mapsto \frac{m}{d}$ est une bijection sur l'ensemble des diviseurs de m.

$$m = d\left(\frac{m}{d}\right)$$

$$\varphi\left(\frac{m}{d}\right) = \#\left\{a \in \mathbb{N}, 0 < a \leq \frac{m}{d}, \operatorname{pgcd}\left(a, \frac{m}{d}\right) = 1\right\}$$

$\Updownarrow$

$$= \#\{a \in \mathbb{N}, 0 < da \leq m, \operatorname{pgcd}(\underset{b}{da}, m) = d\}$$

$$\sum_{d/m} \varphi(m/d) = \# \underbrace{\bigsqcup_{\substack{d/m \\ d+m}} \{a \in \mathbb{N}, 0 < b \leq m, \operatorname{pgcd}(b,m) = d\}_{d=r}}_{\{b \in \mathbb{N}, 0 < b \leq m\}}$$

$$= m$$

Théorème :

Tout entier $a > 1$ peut s'écrire comme produit de nb premiers et les facteurs de ce produit sont uniques à 1 permutation près.

Démonstration :

* existence de la décomposition : par récurrence sur a.

OK

$a = 2$. Si on suppose que le théorème est vrai pour tous les entiers $< a$, on va vérifier que c'est vrai pour a. D'après le résultat précédent, a admet un diviseur premier $p > 1$.

$a = p_0 b \Rightarrow b = \frac{a}{p} < a$ Par hyp de récurrence

$b = p_1 \cdots p_k$ avec p_i premier $\Rightarrow a = p_0 p_1 \cdots p_k$ p_i premier

* Unicité de la décomposition :

Supposons qu'il existe 2 décompositions :

$a = p_1 \cdots p_k = q_1 \cdots q_l$ (p_i et q_j premiers)

Par récurrence sur a ($a = 2$ OK), on suppose que c'est vrai pour tout entier $< a$.

$p_1 | p_1 \cdots p_k = q_1 \cdots q_l$

D'après la proposition précédente, $p_1 = q_j$ avec $1 \leq j \leq l$ $\Rightarrow \underbrace{p_2 \cdots p_k}_{< a} = q_1 \, q_{j-1} q_{j+1} \, q_l$

pas de facteur q_j

par hypothèse de récurrence :

$\forall i \in \{2, \ldots, k\}, \exists m \in \{1, \ldots, l\}$ tel que :

$p_i = q_m$

Arithmétique de $\mathbb{Z}$ et corps finis

Page 3 **Remarque :**

1) il existe 1 infinité de nb premiers.

2)

$$F_n = 2^{2^n} + 1 \qquad \text{Fermat } (1601, 1665)$$

premiers $\begin{cases} F_0 = 3,\ F_1 = 5,\ F_2 = 17 \\ F_3 = 257,\ F_4 = 65\,537 \end{cases}$

Euler : $F_5 = 641 \cdot 6700417$.

montrer que $\mathrm{pgcd}(F_n, F_m) = 1 \quad \forall n \neq m$.

Congruences et classes résiduelles : $a, b, m \in \mathbb{Z}$.

Définition :

On dit que a est congru à b modulo m si :

$m \mid a - b$, et on écrit $\boxed{a \equiv b \bmod m}$

La congruence modulo m est une relation d'équivalence :

1) $a \equiv a \bmod m$.

2) Si $a \equiv b \bmod m$, alors $b \equiv a \bmod m$.

3) Si $a \equiv b \bmod m$ et $b \equiv c \bmod m$, alors $a \equiv c \bmod m$.

On peut donc considérer les classes d'équivalences par cette relation.

Les classes d'équivalences sont notées : $a + m\mathbb{Z}$.

$$a + m\mathbb{Z} = \{ b \in \mathbb{Z} \mid b \equiv a \bmod m \} \subset \mathbb{Z}$$

et sont appelées la classe résiduelle de a modulo m, notée $a \bmod m$, ou bien $\overline{a}$.

Exemples : $m = 4$

classe résiduelle $1+4\mathbb{Z} = \{\ldots -11, -7, -3, 1, 5, 9, 13, \ldots\}$

Notation :

$\mathbb{Z}/m\mathbb{Z}$ est l'ensemble des classes résiduelles modulo m.

Exemple :

$$\mathbb{Z}/4\mathbb{Z} = \{\underset{\overline{0}}{\underset{\parallel}{0+4\mathbb{Z}}}, \underset{\overline{1}}{\underset{\parallel}{1+4\mathbb{Z}}}, \underset{\overline{2}}{\underset{\parallel}{2+4\mathbb{Z}}}, \underset{\overline{3}}{\underset{\parallel}{3+4\mathbb{Z}}}\}$$

Définition :

Un ensemble de représentants des classes résiduelles modulo m est un ensemble ayant un unique élément dans chq classe résiduelle.

Exemple :

Un ensemble de représentants de $\mathbb{Z}/4\mathbb{Z}$ est $\{4, 5, 2, -1\}$ ou bien $\{\underline{0, 1, 2, 3}\}$

$$\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$$

Théorème :

Si $a \equiv b \bmod m$ et $c \equiv d \bmod m$, alors :

- $-a \equiv -b \bmod m$.
- $a+c \equiv b+d \bmod m$.
- $ac \equiv bd \bmod m$.

$\forall a, b, c, d \in \mathbb{Z}$.

Page 4 **Démonstration :**

- Si $m \mid a-b$, alors $m \mid b-a \Longleftrightarrow -a \equiv -b \bmod m$
- Si $m \mid c-d$, alors $m \mid (a-b)+(c-d) = (a+c)-(b+d)$

$$\Longleftrightarrow a+c \equiv b+d.$$

- $\left.\begin{array}{l} a = b + km, \text{ avec } k \in \mathbb{Z} \\ c = d + k'm, \text{ avec } k' \in \mathbb{Z} \end{array}\right)$

$$\begin{aligned} \Longrightarrow ac &= (b+km)(d+k'm) \\ &= bd + kmd + k'bm + kk'm^2 \\ &= bd + m(kd + k'b + kk'm) \\ &\Longrightarrow ac \equiv bd \bmod m. \end{aligned}$$

Définition :

opération

Une loi de composition sur un ensemble X est une application $X \cdot X \longrightarrow X$.

On va définir 2 opérations sur l'ensemble $\mathbb{Z}/m\mathbb{Z}$

$$(a+m\mathbb{Z}) + (b+m\mathbb{Z}) = (a+b) + m\mathbb{Z}$$
$$(a+m\mathbb{Z}) \cdot (b+m\mathbb{Z}) = (ab+m\mathbb{Z})$$

D'après la proposition précédente, ces opérations sont bien définies car elles ne dépendent pas du choix des représentants des classes résiduelles.

Arithmétique de $\mathbb{Z}$ et corps finis

Page 1 Exemples :

$$(3+5\mathbb{Z})+(2+5\mathbb{Z})=(5+5\mathbb{Z})$$
$$=0+5\mathbb{Z}$$

$$(3+5\mathbb{Z})\cdot(2+5\mathbb{Z})=6+5\mathbb{Z}=1+5\mathbb{Z}$$

On note aussi $3+2\equiv 5\equiv 0 \mod 5$

$3\cdot 2\equiv 1 \mod 5$

$\overline{3}+\overline{2}=\overline{0}$ de $\mathbb{Z}/5\mathbb{Z}$

$\overline{3}\cdot\overline{2}=\overline{1}$ de $\mathbb{Z}/5\mathbb{Z}$

$(X,\circ)$ ensemble avec une $\begin{cases}\text{loi de composition.}\\ \text{opération.}\end{cases}$

On dit que la loi $\circ$ est associative si $\forall x,y,z\in X$:
$(x\circ y)\circ z = x\circ(y\circ z)$

Elle est aussi commutative | Abélienne si $\forall x,y\in X$: $x\circ y=y\circ x$

Exemples :

$(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, associatives, commutatives
$(\mathbb{Z}/m\mathbb{Z},+)$, $(\mathbb{Z}/m\mathbb{Z},\cdot)$, associatives, commutatives.

Définitions:

1) $(X,\circ)$ est appelé semi-groupe si $\circ$ est associative.
2) $(X,\circ)$ admet un élément neutre, noté e,
si $x\circ e=e\circ x=x$, $\forall x\in X$.
3) Soit $(X,\circ)$ un semi-groupe avec un neutre $e\in X$.
On dit que $a\in X$ admet un inverse s'il existe un élément $b\in X$ tel que:
$$a\circ b=b\circ a=e.$$

Règles de calculs :

$(X,\circ)$ semi-groupe

$$a^n = \underbrace{a\circ a\circ a\circ \ldots \circ a}_{n \text{ fois}}, \forall n \in \mathbb{N}$$

On a les formules :

- $a^n \circ a^m = a^{n+m}$
- $(a^n)^m = a^{nm}$

de même si $(X,\circ)$ est abélien : $(a\circ b)^n = a^n \circ b^n$

Exemples :

1) $(\mathbb{Z}, +)$ semi-groupe abélien :
   - neutre $= 0$.
   - inverse de $a = -a$ (opposé de a)

2) $(\mathbb{Z}, \cdot)$ semi-groupe abélien :
   - neutre $= 1$.
   - a inversible : $a \cdot b = 1$
     $\Rightarrow a = \pm 1$

3) $(\mathbb{Z}/m\mathbb{Z}, +)$ semi-groupe abélien :
   - neutre $= 0 + m\mathbb{Z}$.
   - inverse de $a + m\mathbb{Z} = -a + m\mathbb{Z}$.

4) $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ semi-groupe abélien :
   - neutre $= 1 + m\mathbb{Z}$.
   - inversibles — vient plus tard.

Définition :

$(X,\circ)$ est un groupe si $(X,\circ)$ est :

- un semi-groupe (associative).
- $(X,\circ)$ admet un élément neutre.

Page 2 • Tout $x \in X$ admet un <u>inverse</u>.

Exemples :

1) $(\mathbb{Z}, +)$
3) $(\mathbb{Z}/m\mathbb{Z}, +)$ <u>groupes</u>

2) et 4) : $(\mathbb{Z}, .)$ et $(\mathbb{Z}/m\mathbb{Z}, .)$ ne sont pas des <u>groupe</u>

Soit $(G, .)$ un <u>groupe</u>, $a \in G$. L'inverse de a est noté a^{-1} et on pose $a^{-n} = (a^{-1})^n$, $\forall n \in \mathbb{N}$.

<u>Règles de simplifications</u> : ds un groupe $(G, .)$

$$\left.\begin{array}{l} ac = bc \\ ca = cb \end{array}\right\} \Rightarrow a = b$$

on multiplie à gauche/droite avec c^{-1}.

<u>Définition</u> :

Le nombre d'éléments dans un groupe G est appelé <u>l'ordre</u> du groupe, noté $|G|$.

Exemple :

$$|\mathbb{Z}/m\mathbb{Z}| = m.$$

<u>Définition</u> :

Un <u>anneau</u> est un triplet $(A, +, .)$ tel que
$(A, +) =$ groupe abélien
et $(A, .) =$ semi-groupe.
$(A, +, .)$ est commutatif (abélien) si $(A, .)$ est abélien.

De plus : $\left.\begin{array}{l} x\cdot(y+z) = xy+xz \\ (x+y)\cdot z = xz+yz \end{array}\right) \forall x,y,z \in A$

L'élément neutre de $(A,\cdot)$, s'il existe, est appelé l'<u>élément unité</u> de A.

Exemples :

1) $(\mathbb{Z},+,\cdot)$ est un anneau | commutatif ; unité $=1$
abélien

2) $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ est " " " : unité $=1+m\mathbb{Z}$

Définition :

$(A,+,\cdot)$ = anneau, $a \in A$.

- On dit que a est <u>inversible</u> ds $(A,+,\cdot)$ si a est inversible ds le semi-groupe $(A,\cdot)$
- On dit que a est <u>un diviseur de zéro</u> si $\boxed{a \neq 0}$ et s'il existe un $\boxed{b \neq 0}$ tel que $\boxed{a\cdot b = 0}$.

Exemple :

$(\mathbb{Z},+,\cdot)$ $\{\text{inversibles}\} = \{\pm 1\}$
pas de diviseur de zéro.

Proposition :

Les diviseurs de zéro de l'anneau $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ sont les classes $a+m\mathbb{Z}$, avec $1 < \text{pgcd}(a,m) < m$

Démonstration :

Si $a+m\mathbb{Z}$ est un diviseur de zéro ds $\mathbb{Z}/m\mathbb{Z}$, alors il existe $b+m\mathbb{Z}$ tel que $(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}) = 0$

$$\underset{ab+m\mathbb{Z}}{\overset{\|}{(a+m\mathbb{Z})\cdot(b+m\mathbb{Z})}} \Leftrightarrow m \mid ab$$

Arithmétique de $\mathbb{Z}$ et corps finis

Page 3 $\quad a+m\mathbb{Z} \neq m\mathbb{Z} \Leftrightarrow m \nmid a.$

$b+m\mathbb{Z} \neq m\mathbb{Z} \Leftrightarrow m \nmid b.$

montrons que $1 < \text{pgcd}(a,m) < m.$

Par l'absurde, supposons que a et m sont premiers entre eux.

Théorème de Gauss :

$m | ab$ et $\text{pgcd}(a,m) = 1 \Rightarrow m | b$

ce qui contredit l'hypothèse $m \nmid b.$

Inversement, si $1 < \text{pgcd}(a,m) < m$, on pose $b = \frac{m}{\text{pgcd}(a,m)}$, alors $b < m.$

$$b = \frac{m}{\text{pgcd}(a,m)} < m \Rightarrow m \nmid b$$

$\text{pgcd}(a,m).b = m$, on multiplie avec k défini par.

$a = \text{pgcd}(a,m).k \quad , k \in \mathbb{N}$

$ab = k\,\text{pgcd}(a,m)\,b = km$

$\Rightarrow m | ab$

$\Rightarrow a+m\mathbb{Z}$ est un diviseur de zéro de $\mathbb{Z}/m\mathbb{Z}$

$(a+n\mathbb{Z})(b+n\mathbb{Z}) = 0.$

Exemple :

$m = 15 \quad , \mathbb{Z}/15\mathbb{Z} \quad , a = \bar{5} \quad , b = \bar{3} \quad , ab = \overline{15} = \bar{0}$

$\Rightarrow \bar{5}$ et $\bar{3}$ sont des diviseurs de zéro de $\mathbb{Z}/15\mathbb{Z}$

Définition :

Un corps est un anneau $(A,+,\cdot)$ tel que tout $a \in (A,\cdot)$ non nul admet un inverse.

Exemples :

$(\mathbb{Q},+,\cdot)$
$(\mathbb{R},+,\cdot)$ sont des corps
$(\mathbb{C},+,\cdot)$

$\mathbb{Z}/m\mathbb{Z}$ corps $\Longleftrightarrow$ m premier

démontré plus tard

Définition :

Si $(A,+,\cdot)$ est un anneau, on note A^* le groupe des éléments inversibles.

Théorème :

La classe $a+m\mathbb{Z}$ de $\mathbb{Z}/m\mathbb{Z}$ est inversible
$\Longleftrightarrow$ pgcd $(a,m)=1$.

Démonstration :

• $\Longrightarrow$:

Supposons que $a+m\mathbb{Z}$ est inversible. Il existe $b\in\mathbb{Z}$ tel que :

$$(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}) = 1+m\mathbb{Z}$$
$$ab+m\mathbb{Z}$$
$$m \mid ab-1$$
$$ab-1=km$$

On peut écrire $1=ab-km$

$d=\text{pgcd}(a,m) \Rightarrow d \mid ab-km=1 \Rightarrow d=1$

26

Page 4 $\cdot \Leftarrow$:

Comme pgcd $(a,m)=1$, l'identité de Bézout donne des entiers $x, y \in \mathbb{Z}$ tels que $ax+my=1$.
On réduit modulo m : $ax+m\mathbb{Z} = 1+m\mathbb{Z}$

$$\overset{\shortparallel}{(a+m\mathbb{Z})(x+m\mathbb{Z})}$$

$\Longrightarrow a+m\mathbb{Z}$ inversible. $\boxtimes$

Exemple :

Les classes inversibles de $\mathbb{Z}/12\mathbb{Z}$ sont :

$0 \leq a < 11$

pgcd $(a,12)=1 \Leftrightarrow a = 5, 7, 11, 1$

4 classes inversibles, notamment

$$|(\mathbb{Z}/12\mathbb{Z})^*| = |\{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}| = 4$$

$$\bar{5}^2 = \bar{1} \quad , \quad \bar{7}^2 = (\overline{-3})^2 = \bar{1}$$
$$\overline{11}^2 = (\overline{-1})^2 = \bar{1}$$

Exercice :

On peut montrer que les 2 groupes $(\mathbb{Z}/12\mathbb{Z})^*$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont isomorphes.

Corollaire :

$\mathbb{Z}/m\mathbb{Z}$ corps $\Leftrightarrow$ m premier.

Démonstration :

$\mathbb{Z}/m\mathbb{Z}$ corps $\Leftrightarrow$ tout $a \in \mathbb{Z}/m\mathbb{Z}$, $a \neq 0$ est inversible

$\Leftrightarrow \forall a, 0 < a < m$, pgcd $(a,m)=1$

$\Leftrightarrow$ m premier.

La fonction d'Euler : (plus tard)

Soit $m \in \mathbb{N}^*$. On définit $\varphi(m) = \left| (\mathbb{Z}/m\mathbb{Z})^* \right|$

D'après la description précédente :

$$\varphi(m) = \# \{ a \in \mathbb{N},\ 0 < a \leq m \text{ et } \operatorname{pgcd}(a,m) = 1 \}$$

fonction d'Euler

Exemples :

1) $\varphi(12) = 4$
2) Si $m = p$ premier, alors $\varphi(p) = p - 1$
$= \# \{ a \in \mathbb{N},\ 0 < a < p\ \cancel{\operatorname{pgcd}(a,p)} = 1 \}$

Théorème :

On a la formule $\displaystyle\sum_{d/m} \varphi(d) = m$

Démonstration :

$$\sum_{d/m} \varphi(d) = \sum_{\substack{d/m \\ \frac{m}{d}/m}} \varphi(m/d)$$

l'applicat° $d \mapsto \frac{m}{d}$ est une bijection sur l'ensemble des diviseurs de m.

$$m = d\left(\frac{m}{d}\right)$$

$$\varphi\left(\frac{m}{d}\right) = \# \left\{ a \in \mathbb{N},\ 0 < a \leq \frac{m}{d},\ \operatorname{pgcd}\left(a, \frac{m}{d}\right) = 1 \right\}$$

$\Updownarrow$

$$= \# \{ a \in \mathbb{N},\ 0 < da \leq m,\ \operatorname{pgcd}(\underbrace{da}_{b}, m) = d \}$$

$$\sum_{d/m} \varphi(m/d) = \# \underbrace{\bigsqcup_{\substack{d/m \\ d \neq m}} \{ a \in \mathbb{N},\ 0 < b \leq m,\ \operatorname{pgcd}(b,m) = d \}_{d \in \dots}}_{\{ b \in \mathbb{N},\ 0 < b \leq m \}}$$

$= m$.

—

Ordre d'un élément :

G = groupe, noté multiplicativement.

Définition :

Soit $g \in G$. S'il existe un entier positif $r \in \mathbb{N}^*$ tel que $g^r = e$, on appelle ordre de g, noté $\mathrm{ord}_G(g)$, le plus petit des entiers non nuls ayant cette propriété.

$\mathrm{ord}_G(g)$ est aussi l'ordre du s/-groupe $\langle g \rangle$ engendré par g.

$\langle g \rangle = \{e, g, g^2, g^3, g^4, \dots\}$ si ce groupe est fini.

EXEMPLE :
$(\mathbb{Z}, +)$
le seul élément d'ordre fini est 0.

Théorème :

Soit $g \in G$ et $n \in \mathbb{Z}$. Alors $g^n = e$ si et seulement si :

$$\left[\left\{ g^n \overset{\text{déf}}{=} (g^{-1})^{-n} \text{ si } n < 0 \right\}\right]$$

n est divisible par $\mathrm{ord}_G(g) = r$.

Démonstrat°:

$\boxed{\Leftarrow}$ Si $n = rk$, $g^n = g^{rk} = (g^r)^k = e^k = e$

$\boxed{\Rightarrow}$ Si on suppose que $g^n = e$, on considère la division euclidienne de n par l'ordre r :

$$n = qr + a \quad (\text{avec } 0 \leq a < r)$$

$$g^a = g^{n-qr} = (\underbrace{g^n}_{e}) \cdot (\underbrace{g^r}_{e})^{-q} = e$$

$$e^{-q} = e$$

par déf° de l'ordre $r = \mathrm{ord}_G(g)$

$\Longrightarrow a = 0$ (car r minimal)

$\Longrightarrow n = qr$.

<u>Corollaire :</u>

Soit $g \in G$ et $\ell, m \in \mathbb{Z}$. Alors $g^{\ell} = g^{m} \Leftrightarrow \ell \equiv m \bmod r$

<u>Démonstrat° :</u>

On multiplie par g^{-m} :

$$g^{\ell} = g^{m} \Longleftrightarrow g^{\ell - m} = e$$
$$\underset{\text{prop préc}}{\Longleftrightarrow} r / (\ell - m)$$
$$\Longleftrightarrow \ell \equiv m \bmod r$$

<u>Exemple :</u>

Voir TD : $\mathrm{ord}_{(\mathbb{Z}/7\mathbb{Z})^*}(\overline{2}) = \ldots$

<u>Théorème :</u>

Soit $g \in G$ un élm^t d'ordre fini $\mathrm{ord}_G(g) = r$.
Alors : $\mathrm{ord}_G(g^n) = \dfrac{\cancel{n}\ r}{\mathrm{PGCD}(r,n)}$.

<u>Démonstrat° :</u>

- $(g^n)^{\frac{r}{\mathrm{PGCD}(r,n)}} = g^{\frac{rn}{\mathrm{PGCD}(r,n)}} = \underbrace{(g^r)}_{e,\ \text{car } r = \mathrm{ord}_G(g)}^{\frac{n}{\mathrm{PGCD}(r,n)} \in \mathbb{Z}}$

Donc $\dfrac{r}{\mathrm{PGCD}(r,n)}$ est un multiple de $\mathrm{ord}(g^n)$

d'après le théo précédent.

Page 2 • Soit k tel que $(g^n)^k = g^{nk} = e$.
D'après le théo précédent, nk est un multiple de $r = ord_G(g)$:

$\Longleftrightarrow r$ divise nk.

$\Longleftrightarrow \frac{r}{PGCD(r,n)}$ divise $\frac{n}{PGCD(r,n)} k$,

Comme $pgcd\left(\frac{r}{pgcd(r,n)}, \frac{n}{pgcd(r,n)}\right) = 1$ par le lemme de Gauss : donc $\frac{r}{PGCD(r,n)}$ divise aussi k

en particulier si $k = ord_G(g^n)$, on a montré que $\frac{r}{PGCD(r,n)}$ divise $ord_G(g^n)$. donc $ord_G(g^n) = \frac{r}{PGCD(r,n)}$.

Définition :

Soit G un groupe. On dit qu'un ss-ensemble H de G est un ss-groupe de G si H est aussi un groupe.

Définition :

Soit G un groupe. On dit que G est cyclique, s'il existe un élément $g \in G$ tel que :
$\langle g \rangle = G \Longleftrightarrow ord_G(g) = |G|$ (ds le cas où G est un groupe fini)

Exemples :

1) $G = (\mathbb{Z}/7\mathbb{Z})^*$, $g = \bar{3}$

$\langle \bar{3} \rangle = \langle \bar{5} \rangle = (\mathbb{Z}/7\mathbb{Z})^*$

$\Rightarrow (\mathbb{Z}/7\mathbb{Z})^*$ est un groupe cyclique.

2) Par contre $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ n'est pas cyclique car ses élmts sont d'ordre 1 ou 2.

Théorème :

Si G est cyclique et fini, alors G admet exactem^t $\varphi(|G|)$ générateurs.

Remarque :

$h \in G$, h générateur $\Longleftrightarrow \mathrm{ord}_G(h) = |G|$.

Démonstrat$^{\circ}$:

$$G = \langle g \rangle = \{e, g, g^2, \dots, g^k, \dots\}$$
$$= \{g^k \,/\, 0 \leq k < |G|\}$$

$$\mathrm{ord}_G(g^k) \underset{\substack{\uparrow \\ \text{théo} \\ \text{préc}}}{=} \frac{\overset{=|G|}{\mathrm{ord}_G(g)} \cancel{|G|}}{\mathrm{PGCD}(k, |G|)} = \frac{|G|}{\mathrm{PGCD}(k, |G|)}$$

Donc g^k est un générateur $\Longleftrightarrow \mathrm{PGCD}(k, |G|) = 1$

$\#$ générateurs de $G = \# \{0 \leq k < |G| \,/\, \mathrm{PGCD}(k, |G|) = 1\}$

$$= \varphi(|G|).$$

Théorème : (Lagrange)

Soit G un groupe fini et H un ss-groupe de G. Alors $|H|$ divise $|G|$.

Démonstration :

On va montrer que G est une réunion disjointe de ss-ensembles ayant le m̂ cardinal $= |H|$.

① Soit $g \in G$ et considérons l'applicat$^{\circ}$:

$$\mu_g : H \longrightarrow G$$
$$h \longmapsto gh$$

Page 3 On montre d'abord que l'applicat° u_g est injective.

$$gh_1 = gh_2 \in G$$

On multiplie par l'inverse g^{-1} de g.

$$(g^{-1}g)h_1 = (g^{-1}g)h_2 \Longleftrightarrow h_1 = h_2$$

On va noter $\underset{G}{\underset{\cap}{gH}}$ l'image de l'applicat° u_g.

⚠ gH n'est pas un ss-groupe de G et u_g n'est pas un homom de groupes.

gH est un ss-ens de G.

② On va montrer :

Si $gH \cap g'H \neq \emptyset$, alors $gH = g'H$.

Soit $x \in gH \cap g'H \Longleftrightarrow$ il existe $h \in H$ et $h' \in H$ tels que $x = gh = g'h'$ (à droite, on multiplie par $(h')^{-1}$)

$$\Rightarrow gh(h')^{-1} = g'\underbrace{h'(h')^{-1}}_{e}$$

$$gh(h')^{-1} = g'$$

Donc $\underset{\forall h'' \in H}{\overset{||}{g'h''}} = g\underbrace{h(h')^{-1}h''}_{\underset{H}{\in}} \in gH$

$g'H \in gH$

et on obtient donc une égalité $g'H = gH$, car ces ensembles ont le m̂ cardinal.

③ $G = \bigcup_{g \in G} gH$, $g = g.e \in gH$ $\{gH\}_{g\in S}$

$\Longrightarrow$ Comme on peut extraire de la famille $\{gH\}_{g\in G}$

$$G = \coprod_{g \in S} gH.$$

une ss-famille qui donne une réunion disjointe, on a prouvé que $|G| = |H| \cdot (\#S)$

Définition :

L'entier $\frac{|G|}{|H|}$ est appelé l'indice de $|H|$ de $|G|$.

* Théorème : EULER

Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ avec $PGCD(a,n) = 1$.
Alors $a^{\varphi(n)} \equiv 1 \mod n$.

Corollaire : (Théorème de FERMAT)

Si $n = p$ premier $(\varphi(p) = p-1)$ et p ne divise pas a, alors $a^{p-1} \equiv 1 \mod p$.

---

* Corollaire :

Soit $g \in G$, groupe fini, alors :

$$\boxed{ord_G(g) \text{ divise } |G|}$$

Démonstrat° :

Applique Lagrange au ss-groupe $H = \langle g \rangle$.

Démonstration : (EULER)

Il suffit d'appliquer le th de Lagrange au ss-groupe $H = \langle \bar{a} \rangle$ de $G = (\mathbb{Z}/n\mathbb{Z})^*$

$$\Rightarrow ord_G(\bar{a}) \text{ divise } |G| = \varphi(n)$$

Page 4 $\Rightarrow (\bar{a})^{\varphi(n)} = \bar{1}$ ds $\mathbb{Z}/n\mathbb{Z}$.

$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$.

Théorème : (Restes Chinois) (introduct°)

Soient $m_1, m_2, \dots, m_k$ des entiers 2 à 2 premier entre eux, et $a_1, \dots, a_k$ des entiers qcq.

Problème : Trouver ts les entiers x vérifiant le système de congruences :

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

Il y a k congruences.

On introduit : $M_i = \dfrac{\prod_{j=1}^{k} m_j}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j$

on pose $m = \prod_{j=1}^{k} m_j = m_1 \cdot m_2 \cdots m_k$

comme les nbs m_i sont 2 à 2 premiers entre eux,
$PGCD(\underbrace{M_i}_{\prod_{j\neq i} m_j}, m_i) = 1$,

et on peut donc considérer l'inverse de $M_i \bmod m_i$.
On le note y_i. C'est un entier vérifiant
$y_i M_i \equiv 1 \bmod m_i$.

Remarque :

On calcule y_i en utilisant l'algo d'Euclide étendu avec le couple (m_i, M_i) et on pose :

$$x = \sum_{j=1}^{m} a_j y_j M_j \bmod m \quad , \; m_i M_i = m$$

Remarque :

x est bien défini car $m_i M_i = m$, $\forall i \in \{1, \dots, n\}$.

Vérifions que cet x est solut° du système des n congruences.

Il faut vérifier que $x \equiv a_i \bmod m_i$.

$$x = \sum_{j=1}^{n} a_j y_j M_j \bmod m_i$$

$$= \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j y_j M_j + a_i \underbrace{(y_i M_i)}_{\equiv 1 \bmod m_i} \bmod m_i \equiv a_i \bmod m_i$$

$$M_j = \prod_{k \neq j} m_k \quad , \quad M_j \equiv 0 \bmod m_i$$

si $j \neq i$, m_i divise M_j.

Il reste à montrer l'unicité de la solut° modulo $m = \prod_i m_i$.

Soient donc 2 solution x et x' du système de congruences $x \equiv a_i \bmod m_i$

$x' \equiv a_i$

$x - x' \equiv 0 \bmod m_i$.

$m_i \mid x - x'$

Comme les m_i sont premiers 2 à 2, on a $\prod m_i = m \mid x - x'$

$x \equiv x' \bmod m$

Théorème : (Restes Chinois) (même notation)

Ou suppose que les k entiers $m_1, \dots, m_k$ sont 2 à 2 premiers entre eux.

$m = \prod m_i$ On a un isomorphisme d'anneaux :

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/m_k\mathbb{Z})$$

$$(x \bmod m) \longmapsto (x \bmod m_1, \dots, x \bmod m_k)$$

Démonstrat° :

① homom. d'anneau.

② Surjectivité Φ : Pb donné par le système de congruences, la solut° existe.
injectivité Φ = unicité de la solution mod m.

Page 1 Une formule pour la fonction d' Euler

- $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*| = \#\{1 \leq a \leq n,\ \text{pgcd}(a,n)=1\}$

Théorème :

Si m_1 et m_2 sont premiers entre eux, alors :

$$\varphi(m_1 m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

Démonstration :

$$\underset{\text{isomorphisme d'anneaux}}{\mathbb{Z}/m_1 m_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \cdot \mathbb{Z}/m_2\mathbb{Z}} \quad \text{(Th restes chinois)}$$

Cet isomorphisme induit un isomorphisme entre les groupes multiplicatifs :

$$(\mathbb{Z}/m_1 m_2\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z})^* \cdot (\mathbb{Z}/m_2\mathbb{Z})^*$$

Théorème :

Soit n un entier quelconque. Alors

$$\boxed{\varphi(n) = n \prod_{\substack{p/n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)}$$

en d'autres mots, si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (p_i premiers, $\alpha_i \in \mathbb{N}^*$)

décomposition en nbs premiers

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

$$= \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

Démonstration:

$p_i^{\alpha_i}$ est premier à $p_j^{\alpha_j}$ à cause du théorème précédent.

$$i \neq j \Rightarrow \varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$$

Il reste donc à montrer que $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$

$$\varphi(p^\alpha) = \#\{1 \leq a \leq p^\alpha,\ \underbrace{\operatorname{pgcd}(a,p^\alpha) = 1}_{\Leftrightarrow\ \operatorname{pgcd}(a,p)=1}\}$$

p premier

$\alpha \in \mathbb{N}^*$

$$= p^\alpha - \#\{1 \leq a \leq p^\alpha,\ \operatorname{pgcd}(a,p) \neq 1\}$$

$\Updownarrow$

$p | a \Leftrightarrow a = pb$

$1 \leq pb \leq p^\alpha$

$\Leftrightarrow$

$\frac{1}{p} \leq 1 \leq b \leq p^{\alpha-1}$

$\|$

$p^{\alpha-1}$

$$= p^\alpha - p^{\alpha-1}.$$

Polynômes à coeff dans un anneau A:

A = anneau commutatif avec unité, p. ex.

$$A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}/m\mathbb{Z}, \ldots$$

Définition :

Un polynôme f en une variable X sur A est une somme :

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

a_i = coeff du polynôme f, $a_i \in A$

$a_n \neq 0$, a_n = coeff dominant

n = degré de f, noté $\deg(f)$.

Page 2 On a deux opérations sur l'ensemble des polynômes en X à coeff dans A, noté A[X].

① Addition : $\underbrace{\left(\sum_{i=1}^{n} a_i X^i\right)}_{f} + \underbrace{\left(\sum_{i=1}^{m} b_i X^i\right)}_{g} = \underbrace{\sum_{i=1}^{n}(a_i+b_i)X}_{f+g}$

$n = \deg(f)$
$m = \deg(g)$

$m \leq n$
$b_i = 0,\ m < i \leq n$

② Multiplication :

$f.g = \sum_{i=1}^{n+m} c_i X^i$ avec $c_k = \sum_{i+j=k} a_i b_j \quad \begin{pmatrix} 1 \leq i \leq n \\ 1 \leq j \leq m \end{pmatrix}$

$(A[X], +, \cdot)$ est un anneau commutatif
unité $= 1 =$ polynôme constant
$1 \in A \in A[X]$
$\deg(1) = 0$

À partir de maintenant, on considère $K[X]$, avec K = corps.

Proposition :

L'anneau $K[X]$ n'a pas de diviseur de zéro.

Démonstration :

$f.g = 0 \leftarrow$ polynôme cst $\quad f \neq 0,\ g \neq 0$

$a_n b_m X^{n+m} + \dots = 0$
$\Rightarrow n = m = 0$
et $\underset{\neq 0}{a_0}\underset{\neq 0}{b_0} = 0$.

$f = \overset{\neq 0}{a_n} X^n + \dots$
$g = \underset{\neq 0}{b_m} X^m + \dots$

Prop :

$\underset{\neq 0}{f}, \underset{\neq 0}{g} \in K[X]$, alors $\deg(fg) = \deg(f) + \deg(g)$

Preuve : évident.

Théorème : (DIVISION EUCLIDIENNE)

Soient $f, g \in K[X]$ et $g \neq 0$. Il existe 2 polynômes $q, r \in K[X]$ tels que $f = gq + r$
avec $\deg(r) < \deg(g)$
q et r sont uniques.

Démonstration :

- Si $f = 0$, on prend $q = r = 0$.
- si $f \neq 0$ et si $\deg(f) < \deg(g)$, alors on prend $q = 0$, $r = f$.

Donc on suppose $\deg(f) \geq \deg(g)$ et on va montrer l'existence de q et r par récurrence sur $\deg(f)$.

H_n : Le couple (q, r) existe pour tout polynôme f de degré $< n$.
On vient de montrer que $H_{\deg(g)}$ est vrai et on suppose que H_n est vraie et on va montrer H_{n+1}.

Soit donc f, $\deg(f) = n$; $f = \underset{\neq 0}{a_n} X^n + \dots$
$g = \underset{\neq 0}{b_m} X^m + \dots$

Alors on pose $f_1 = f - \frac{a_n}{b_m} X^{n-m} g$ (*)

Page 3 <u>On observe :</u> $\deg(f_1) < n$

Donc on peut appliquer H_n au polynôme f_1.
Donc il existe q_1, r_1 avec $\deg(r_1) < \deg(g)$
tel que $f_1 = q_1 g + r_1$

On remplace dans l'équation #:

$$f = (q_1 g + r_1) + \frac{a_n}{b_m} X^{n-m} g = \left(q_1 + \frac{a_n}{b_m} X^{n-m}\right) g + r_1$$

donc on prend $r = r_1$ et $q = q_1 + \frac{a_n}{b_m} X^{n-m}$

Il reste à montrer que le couple (q, r) est unique
Par l'absurde, si (q_1, r_1) et (q_2, r_2) conviennent.

$$f = q_1 g + r_1 = q_2 g + r_2 \text{ avec } \deg(r_i) < \deg(g)$$

$$\underbrace{(q_1 - q_2)}_{\neq 0} g = \underbrace{r_2 - r_1}_{\deg(r_2 - r_1) < \deg(g).}$$

si $(q_1 - q_2) \neq 0$, alors.

$\underbrace{\deg(q_1 - q_2)}_{\geq 0} + \deg(g)$ ~~est un multiple de deg (g)~~ $\geq \deg(g)$ or $\deg(r_2 - r_1) < \deg(g)$ contradiction.

$\Rightarrow q_1 - q_2 = 0.$

$\Rightarrow q_1 = q_2 \Rightarrow r_1 = r_2 \Rightarrow \text{cste} = 0 \Rightarrow r_1 = r_2$ □

Ce qu'on a vu ds l'anneau $\mathbb{Z}$ est aussi vrai ds l'anneau $K[X]$, en autres, on peut définir $\mathrm{PGCD}(f, g) \in K[X]$ et l'algo d'Euclide étendu fonctionne ds l'anneau $K[X]$.
(calcule $x, y \in K[X]$ tels que $xf + yg = \mathrm{PGCD}(f, g)$)

Rappels : (qlqs résultats déjà montrés en TD)

(1) $f \in K[X]$ est divisible par $X - a$ ssi $f(a) = 0$.
et $a \in K$

(2) 1 polynôme $f \in K[X]$ de degré n a au plus n racines distinctes.

Définition :

On dit qu'un polynôme $f \in K[X]$ est irréductible s'il ne peut pas s'écrire comme un produit $f = ab$ avec $a, b \in K[X]$ et $\deg(a) < \deg(f)$ et $\deg(b) < \deg(f)$.

Constructions des corps finis :

On a déjà vu quelques corps finis $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p premier)

On les appelles les corps finis premiers.

Pour construire d'autres corps finis, on considère $\mathbb{F}_p$ et $f \in \mathbb{F}_p[X]$ et on regarde les classes résiduelles modulo f ds l'anneau $\mathbb{F}_p[X]$.

Pour tout $g \in \mathbb{F}_p[X]$: $g + f\,\mathbb{F}_p[X] = \{g + fh \text{ avec } h \in \mathbb{F}_p[X]\}$

classe résiduelle mod f notée $\overline{g}$

L'ensemble des classes résiduelles modulo f est notée $\mathbb{F}_p[X]/(f)$

Remarque :

Cette construction est l'analogue dans $\mathbb{F}_p[X]$ de la construction de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

(42 bis)

Dém : (1) On écrit la division Euclidienne de f par $X-a$

$$f = q\cdot(X-a) + r \quad \text{avec } r \in K.$$

En remplaçant X par a, on obtient $r = f(a)$.

Ainsi $r=0 \Leftrightarrow f(a)=0$.

(2) Si f admet $\geq n+1$ racines distinctes, f serait (~~fpa~~ (dém par récurrence) divisible par le polynôme $\prod_{i=1}^{n+1}(X-a_i)$ de degré $n+1$, contradiction. et

($\operatorname{pgcd}(X-a, X-b) = 1$ si $a \neq b$)

On montre d'abord par récurrence que si f ~~est~~ admet k racines distinctes $a_1, \ldots, a_k$ alors f est divisible par $\prod_{i=1}^{k}(X-a_i)$

Page 4 **Prop :**

1) Si f est un polynôme quelconque ~~non nul~~, alors $\mathbb{F}_p[X]/_{(f)}$ est un anneau.

2) Si f est un polynôme irréductible de degré n, alors $\mathbb{F}_p[X]/_{(f)}$ est un corps fini d'ordre p^n. Il est noté $\mathbb{F}_{p^n}$.

Démonstration :

Plus tard.

Exemple :

$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

Il faut un polynôme irréductible de $\mathbb{F}_2[X]$ de degré 2. p.ex : $f = X^2+X+1$

élém^ts de $\mathbb{F}_4 = \mathbb{F}_2[X]/_{(f)}$ restes de la div° euclidienne par f.

α = classe du polynôme X modulo f.

Il y a 4 élém^ts $\{\bar{0}, \bar{1}, \alpha, \bar{1}+\alpha\} = \mathbb{F}_4$

Table de multiplication de $\mathbb{F}_4$:

$\bullet$	$\bar{1}$	α	$1+\alpha$
$\bar{1}$	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$\bar{1}+\alpha$	$1+\alpha$	1	α

$\alpha^2+\alpha+1=0$

$\alpha^2 = \alpha+1$

$(1+\alpha)^2 = 1+\alpha^2 = 1+\alpha+1 = \alpha$

$\alpha(1+\alpha) = 1$

$\mathbb{F}_{p^n}$

Proposition

1) Soit f un polynôme quelconque dans $\mathbb{F}_p[X]$. Alors l'ensemble des classes résiduelles mod f ~~est un~~ noté $\mathbb{F}_p[X]/(f)$ est un anneau commutatif avec unité.

2) Si f est irréductible, alors $\mathbb{F}_p[X]$ est un corps fini à p^n éléments, où $n = \deg(f)$.

3) Le corps fini $\mathbb{F}_p[X]/(f)$ est un espace vectoriel sur le corps $\mathbb{F}_p$ de dimension n.

Démonstration:

1) Par définition, une classe résiduelle

$$g = \{G + Hf, \text{ avec } H \in \mathbb{F}_p[X]\} \subset \mathbb{F}_p[X]$$

sous-ensemble de $\mathbb{F}_p[X]$.

$G \in \mathbb{F}_p[X]$ est un représentant de la classe g.

loi de composition dans l'anneau $\mathbb{F}_p[X]/(f)$

$$g = \{G + Hf \mid H \in \mathbb{F}_p[X]\} \qquad G = \text{représentant de la classe } g$$

$$g' = \{G' + Hf \mid H \in \mathbb{F}_p[X]\} \qquad G' = \text{———}$$

On définit • $g+g' = \{G+G'+Hf\}$ et on vérifie que la classe $g+g'$ ne dépend pas du choix des représentant G et G'.

• $gg' = \{GG' + Hf \mid H \in \mathbb{F}_p[X]\}$ pareil, on vérifie que gg' ne dépend pas du choix des représentants G et G'.

L'unité de l'anneau $\mathbb{F}_p[X]/(f)$ est :

$$\bar{1} = \{ \underset{\mathbb{F}_p}{\overset{\cap}{1}} + Hf \text{, avec } H \in \mathbb{F}_p[X] \}.$$

c'est-à-dire $\bar{1} \cdot g = g \quad \forall g \in \mathbb{F}_p[X]/(f)$.

Comme $\mathbb{F}_p[X]$ est un anneau commutatif, $\mathbb{F}_p[X]/(f)$ l'est aussi.

2) Pour montrer que $K = \mathbb{F}_p[X]$ est un corps, il suffit de montrer que tout $g \in K$, $g \neq 0$, est inversible.

On choisit un représentant quelconque $G \in \mathbb{F}_p[X]$ de $g \in K$, c'est-à-dire

$$g = \{ G + Hf \text{ avec } H \in \mathbb{F}_p[X] \}$$ et on applique l'algorithme d'Euclide étendu aux polynômes f et G.

L'algo. d'Euclide étendu donne $U, V \in \mathbb{F}_p[X]$ et $PGCD(f, G) \in \mathbb{F}_p[X]$ tel que

$$Uf + VG = PGCD(f, G). \quad \leftarrow \text{identité de Bézout}$$

or on sait que f est irréductible et $g = G \bmod f \neq 0 \Rightarrow f$ ne divise pas le polynôme G

$\Rightarrow PGCD(f, G)$ est un polynôme constant non nul. noté $\sigma \in (\mathbb{F}_p)^*$

$$Uf + VG = \sigma$$

on multiplie par σ^{-1} : $\underbrace{\sigma^{-1}U}_{\in \mathbb{F}_p[X]} f + \sigma^{-1} V G = 1$.

et on passe aux classes résiduelles modulo f

$$\overline{\sigma^{-1}V} \cdot \overline{G} = \bar{1} \quad \text{égalité dans } K.$$

$$h \cdot g = \bar{1}$$

donc h est l'inverse de g dans K.

3) Si on note $1, x, x^2, \dots, x^{n-1}$ les classes résiduelles des monômes $1, X, X^2, \dots, X^{n-1}$ dans $\mathbb{F}_p[X]$ dans $\mathbb{F}_p[X]/(f) = K$.

alors tout $g \in K$ peut être représenté par un $G \in \mathbb{F}_p[X]$ de $\deg(G) \leq n-1$. (prendre un G qcq et le remplacer par le reste de la div. euclidienne par g !)

donc on peut écrire de manière unique $g = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$.

de plus les éléments $1, x, \dots, x^{n-1}$ sont linéairement indépendants. ($a_i = 0 \ \forall i \Rightarrow g = 0$.)

donc $K = \bigoplus_{i=0}^{n} \mathbb{F}_p \cdot a_i$ $\quad \dim_{\mathbb{F}_p}(K) = n$.

Remarques :

① On peut montrer que tout corps fini est isomorphe à un corps $\mathbb{F}_p[X]/(f)$ pour un polynôme f irréductible dans $\mathbb{F}_p[X]$. Donc tout corps fini a un ~~ca~~ ordre $= p^n$ avec p premier.

② $\forall$ couple (p, n) avec p premier et $n > 1$, $\exists$ un polynôme irréductible dans $\mathbb{F}_p[X]$ de degré n.

Réf : Demazure : Cours d'algèbre.

Théorème : Soit K un corps fini à $p^n = q$ éléments. Soit $K^* = K \setminus \{0\}$ le groupe multiplicatif de K d'ordre $q-1$. Alors pour tout diviseur d de $q-1$, il existe exactement $\varphi(d)$ éléments ds K d'ordre d. En particulier (comme $\varphi(q-1) > 0$) $\exists$ éléments d'ordre $q-1$, de K^*. Donc K^* est un groupe cyclique.

Dém. : Soit d un diviseur de $q-1$. On appelle $\psi(d)$ le nb. d'éléments $x \in K^*$ ayant un ordre $= d$.
On va donc montrer que $\psi(d) = \varphi(d)$.

D'abord, on suppose $\psi(d) > 0$ et soit $a \in K^*$ un élément d'ordre d, c'est-à-dire $a^d = 1$ et les puissances $1, a, a^2, \dots, a^{d-1}$ sont toutes distinctes.

D'autre part, l'équation $x^d - 1 = 0$ a au plus d racines et comme les éléments $1, a, .., a^{d-1}$ sont des racines distinctes, cette équation admet exactement d racines. Ainsi si x est un élément d'ordre d, alors x peut s'écrire $x = a^k$ avec $0 \leqslant k \leqslant d-1$. le sous-groupe engendré par a dans K est un groupe cyclique d'ordre d et $\operatorname{ord}(a^k) = \dfrac{d}{\operatorname{pgcd}(k,d)}$ (← résultat montré dans ce cours)

donc a^k est d'ordre d ssi $\operatorname{pgcd}(k,d) = 1$
donc il y en a $\varphi(d) = \# \{0 \leqslant k \leqslant d-1 ; \operatorname{pgcd}(k,d) = 1\}$

Conclusion : si $\psi(d) > 0$, alors $\psi(d) = \varphi(d)$

Il reste à montrer que $\psi(d) \neq 0$ $\forall$ diviseur d de $q-1$

or
$$q-1 = \sum_{d \mid q-1} \psi(d) \leqslant \sum_{d \mid q-1} \varphi(d) = q-1$$
résultat du cours.

car $K^* = \bigsqcup_{d \mid q-1} \{x \in K^* \mid \operatorname{ord}(x) = d\}$

et $\# \{x \in K^* \mid \operatorname{ord}(x) = d\} = \psi(d)$

$\Rightarrow$ $\psi(d) = \varphi(d)$ pour tout diviseur d de $q-1$.

Déf : On appelle élément primitif de K^* un générateur du groupe $(K^*, \cdot)$.

Remarque: Si $K = (\mathbb{Z}/p\mathbb{Z})$, le problème de déterminer les éléments primitifs dans $(\mathbb{Z}/p\mathbb{Z})^*$ est en général très compliqué.

Exemple: $(\mathbb{Z}/23\mathbb{Z})^*$ = groupe cyclique d'ordre 22

cas particulier si $p-1$ a "peu" de facteurs premier, il suffit de tester avec certaines puissances.

Comme l'ordre de g divise $22 = 2\cdot 11$, il suffit de calculer g^2 et g^{11}

dans $\mathbb{Z}/23\mathbb{Z}$

g	2	3	5	7	11	13	17
g^2	4	9	2	3	6	8	18
g^{11}	1	1	-1	-1	-1	1	-1

$\Rightarrow$ 5, 7, 11, 17 mod 23 sont des éléments primitifs.

Il y en a $\varphi(22) = (2-1)(11-1) = 10$.

Aussi: 21, 10, 14, 15, 20, 19

Donc les éléments primitifs de $(\mathbb{Z}/23\mathbb{Z})^*$ sont.

5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

Rappel : Thm de Fermat $a^{p-1} \equiv 1 \mod p$ p premier. $p \nmid a$.

et $\boxed{a^p \equiv a \mod p \quad \text{pour tout entier } a.}$

Or ceci n'est plus vrai pour le thm. d'Euler.

Rappel : Thm d'Euler : $a^{\varphi(n)} \equiv 1 \mod n$ $n \geq 2$ entier qcq. et pgcd$(a,n) = 1$.

mais $\boxed{a^{\varphi(n)+1} \not\equiv a \mod n \quad \text{pour tout entier } a.}$

Par exemple : $n = 4$ et $a = 2$, $\varphi(4) = 4 - 2 = 2$ donc $a^2 \equiv 1 \mod 4$ si pgcd$(a,4) = 1$

mais $2^{\varphi(4)+1} = 8 \equiv 0 \mod 4$
$\not\equiv 2 \mod 4$.

Définition : On dit qu'un entier n est sans facteur multiple s'il n'est divisible par le carré d'aucun entier > 1 c'est-à-dire s'il est produit de nb. premier distincts.

Par exemple : $15 = 3 \cdot 5$ est sans facteur multiple.
mais $12 = 2^2 \cdot 3$ ne l'est pas $4 \mid 12$.

Proposition (Thm d'Euler renforcé)
Soit $n \geq 2$ un entier sans facteur multiple et $r = k \cdot \varphi(n)$ avec $k \in \mathbb{N}$. Alors $a^r \equiv 1 \mod n$ pour a

$\boxed{a^{r+1} \equiv a \mod n \quad \text{pour tout entier } a.}$

Dém. : Comme n est sans facteur multiple, $n = \prod_{p \mid n} p$

$\varphi(n) = n \cdot \prod_p \left(1 - \frac{1}{p}\right) = \prod_{p \mid n} (p-1)$ donc $p - 1 \mid k \cdot \varphi(n) = r$

Par le thm. de Fermat on a :

$a^{p-1} \begin{cases} \equiv 1 \mod p & \text{si } p \nmid a \\ \equiv 0 \mod p & \text{si } p \mid a. \end{cases}$ ~~pgcd(p, pta)~~

donc $a^r \equiv \begin{cases} 1 \mod p & \text{si } p \nmid a \\ 0 \mod p & \text{si } p \mid a \end{cases}$

donc $a^{r+1} \equiv a \mod p$ pour tout entier a.

Comme $n = \prod_{p|n} p$ on a $p \mid a^{r+1} - a \Rightarrow n \mid a^{r+1} - a$

$\Rightarrow a^{r+1} \equiv a \mod n$

et $a^r \equiv 1 \mod n$ si $pgcd(a,n) = 1$.

Rem.: Dans la suite (~~RSA~~ méthode RSA en cryptographie à clé publique)

on va appliquer la prop. précédente avec $n = p.q$ où p, q nb. premiers.

Cryptographie à clés publiques et Nombres premiers : la méthode RSA

Principe de la cryptographie à clé publique :

M = ensemble de message, le même pour chaque interlocuteur.

pour simplier on suppose qu'il y a $\boxed{2}$ interlocuteurs appelées A (= Alice) et B (= Bob).

Ils veulent s'échanger des messages sans qu'une troisième personne puisse lire les message envoyé (on suppose que le canal de transmission est "public", facilement accessible).

Principe : A dispose de 2 fonctions (bijections)

$c_A : M \to M$ et $d_A : M \to M$ tel que $\boxed{\begin{array}{l} d_A \circ c_A = id_M \\ \text{et } c_A \circ d_A = id_M \end{array}}$

c_A = fonction de chiffrement

d_A = fonction de déchiffrement. d_A est la fonction réciproque de c_A

Pareil, B dispose de 2 fonctions

$$c_B : M \longrightarrow M \quad \text{et} \quad d_B : M \longrightarrow M$$

tel que $c_B \circ d_B = id_M$
et $d_B \circ c_B = id_M$.

~~Domaine~~ Fonctions "clé" "publique" c_A et c_B (connus par tous les interlocuteurs)
"secrète" d_A et d_B (connus seulement par leur "propriétaire" c'est-à-dire d_A connu par A
d_B ——— B.).

Si Alice veut envoyer un message $m \in M$ à Bob, elle envoie le message $\boxed{m' = c_B(d_A(m))}$

Bob reçoit m' de Alice et applique la fonction $c_A \circ d_B$ à m' et obtient donc $c_A(d_B(c_B(d_A(m))$

clé publique (c_A) — sa clé secrète (d_B)

$$= c_A(d_A(m))$$

$$= m.$$

Pareil, si Bob veut envoyer un message $m \in M$ à Alice, il envoie le message $\boxed{m' = c_A(d_B(m))}$

et Alice applique la fonction $c_B \circ d_A$ pour récupérer m.

Rem : Pour que ceci fonctionne dans la pratique :

1)* c_A, c_B, d_A, d_B calculables par algo. rapides.

2)* décryptage compliqué ~~c'est-à-dire~~ : calculer d_A ~~est~~ fonction de c_A ~~c'est-à-dire~~ ~~c'est~~ "récupérer m à partir de $c_A(m)$" demande un temps de calcul prohibitif.

(1977) méthode RSA (= Rivest, Shamir, Adleman)

on prend $M = \mathbb{Z}/n$ et $n = p \cdot q$ avec p, q nb. premiers.

et s un entier premier à $\varphi(n) = (p-1)(q-1)$. ; $\mathrm{pgcd}(s, \varphi(n)) = 1$

n et s sont des entiers "publics"

$$c : M \to M \qquad \text{fonction de chiffrement}$$
$$m \mapsto m^s \bmod n$$

la clé privée/secrète est l'entier t, ~~des entiers des~~

où t est tel que $\boxed{st \equiv 1 \mod \varphi(n)}$ $\Leftrightarrow$ $s \cdot t = 1 + k \cdot \varphi(n)$

$\Leftrightarrow$ $\bar{s}$ est l'inverse de $\bar{t}$ dans $\left(\mathbb{Z}/\varphi(n)\mathbb{Z}\right)^*$.

$$d : M \to M \qquad \text{fonction de déchiffrement.}$$
$$m \mapsto m^t \bmod n$$

Alors d'après le théorème d'Euler renforcé (voir ~~cha~~ section précédente)

$$d \circ c\,(m) = d(m^s) = (m^s)^t = m^{st}$$
$$= m^{1+k\varphi(n)}$$
$$\equiv m \mod n$$

idem $\mathrm{cod}(m) = m^{ts} \equiv m \mod n$.

Ainsi (n, s) sont des entiers publics

décrypter consiste à trouver t (= inverse de s mod. $\varphi(n)$)

consiste à trouver $\varphi(n)$.

or connaissant n et $\varphi(n)$ on peut recalculer p et q.

décrypter $\Longleftrightarrow$ décomposer n en $p \cdot q$.

RSA repose sur difficulté de factoriser un entier.

Comment trouver des entiers premiers ?

• Tests de primalité

1) n composé s'il existe ~~a~~ un diviseur a de n tel que $\boxed{1 < a \leq \sqrt{n}.}$

~~algo~~ méthode : tester ts les div. de 2 jusqu'à $\sqrt{n}$.

• Contraposée du Thm de Fermat : p premier $\Rightarrow$ pour tout $1 \leq a < n \Rightarrow a^{n-1} \equiv 1 \mod n$.

2) $\boxed{n \text{ est composé s'il existe } a \text{ avec } a^{n-1} \not\equiv 1 \mod n \text{ et } 1 < a < n.}$

~~On appelle témoin~~

Remarque : Si n est composé, alors si $\text{pgcd}(a,n) \neq 1$, on a nécessairement $a^{n-1} \not\equiv 1 \mod n$.

en effet, si $a^{n-1} \equiv 1 \mod n \Rightarrow a$ est inversible mod n (d'inverse a^{n-2})
donc $\text{pgcd}(a,n) = 1$.

Déf : On appelle un témoin de Fermat de l'entier n (composé) un entier a avec $\text{pgcd}(a,n) = 1$ avec $a^{n-1} \not\equiv 1 \mod n$.

Rem : Il existe des nb. composés n non détectés par le test de Fermat, c'est-à-dire tel que pour tout a avec $\text{pgcd}(a,n) = 1$, on a

$$a^{n-1} \equiv 1 \mod n.$$

et $a^n \equiv a \mod n$ pour tout a

$3 \times 17 = 51$, 510, 51, 561

ce sont les nb de Carmichael (le plus petit est 561) $= \boxed{3 \cdot 11 \cdot 17}$

54

si n premier $\neq 2$ et $1 < a < n$

alors $a^{n-1} \equiv 1 \mod n$.

$$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \mod n.$$

or $x^2 = 1$ n'a que 2 solutions dans $\mathbb{Z}/n\mathbb{Z}$

$x = +1$ et $x = -1$

donc $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$

3) ~~n~~ impair composé s'il existe a avec $a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod n$ et $1 < a < n$.

Rem : Il existe des nb. composés n pour lesquels on a $\forall a$ premier à n $a^{\frac{n-1}{2}} \equiv 1 \mod n$

par exemple $1729 = 7 \cdot 13 \cdot 19$

$\boxed{\text{FIN DU COURS}}$