10-Klèmeuhrz !

Ces fiches sont des résumés de cours du plus important selon l'auteur, excepté dans les dernières feuilles,où l'on peut trouver des démonstrations ou parties de démonstrations useless dues à la fatigue de l'auteur.

En revanche, ces fiches peuvent très bien pour d'autre ne pas suffire à la compréhension et/ou la maîtrise du cours

L'utilisateur final est invité à relire en diagonal son cours après lecture des fiches pour vérifier que rien n'y manquait, quand bien même l'auteur aurrait signalé une lacune de cours à un endroit donné.

L'auteur décline toute responsabilité dans d'éventuels oublies, erreurs, crises cardiaque à la vue de l'écriture, surmenage lors d'opération de décryptage des documents, complications visuelles lors du déchiffrage, et folie passagère ou permanente en cours d'apprentissage, qui surviendraient suite à la lecture de ce document.

Blah blah, blah blah, blah blah

Paumier Edouard, Promo 2011, L1, Groupe B, jeune, beau et brillant, cherchant femme disponible,

Recto

Ch 7 : Arithmétique

I Intro

☺ étude de $\mathbb{N}$ ou de $\mathbb{Z}$

→ $(\mathbb{Z}, +)$ est un groupe abélien

→ $(\mathbb{Z}, +, \cdot)$: anneau commutatif unitaire et intègre

II Divisibilité

• $m \mid a \Leftrightarrow a = m\lambda, \quad \lambda \in \mathbb{Z}$

• ρ "$\leq$" : ρ d'ordre dans $\mathbb{N}$, pas dans $\mathbb{Z}$, Ordre partiel : $a \mathcal{R} b \Leftrightarrow b \mid a$

($\mathbb{Z}$) • $m \mid a \Leftrightarrow -m \mid a \Leftrightarrow -m \mid -a \Leftrightarrow m \mid -a$

• $m \mid a \Rightarrow |m| \leq |a|$ → 0 ne divise que 0

• $\forall a \in \mathbb{Z}$, $1, -1, a, -a$ divisent a

III Division euclidienne

• $\forall (a, b) \in \mathbb{N}^* \quad \exists (q, r) \in \mathbb{N}^2 \mid a = bq + r$ avec $0 \leq r \leq b-1$

• a dividende, b diviseur, q quotient, r reste

$\Rightarrow (q, r)$ est unique

IV Congruence

1) ⓘ $a \equiv b\ [n] \Leftrightarrow n \mid (a-b)$

"même reste par la div/n"

- relation d'équivalence dans $\mathbb{Z}$
- f° symétrique
  - ↳ réflexive
  - ↳ transitive

- Classe d'équivalence de a : $\{b \mid a \equiv b\ [n]\}$ $= \dot{a}$
- Ensemble quotient de $\mathbb{Z}$ par la congruence noté $\mathbb{Z}/n\mathbb{Z}$

→ $\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dots, \dot{n-1}\}$

$n \mid (x-i) \Leftrightarrow x \in \dot{i}$

soit

→ soit k et $l \in \{0, \dots, n-1\}$, $l \neq k$, $\dot{k} \neq \dot{l}$

→ i est le représentant de $\dot{i}$

→ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire

$\dot{a}+\dot{b} = \dot{a+b}$ $\quad \dot{a}\dot{b} = \dot{ab}$

Non intègre si $n=6$: $\dot{2}\cdot\dot{3} = \dot{6} = \dot{0}$

Ch 7 : Fr
2p

2 petits Théorèmes

- $a \equiv b\,[m]$ et $c \equiv d\,[m]$
($\Rightarrow a = b + \lambda m$ et $c = b + \lambda' m$)

$\Rightarrow a + c \equiv b + d\,[m]$

$\Rightarrow a\,c \equiv b\,d\,[m]$

$\Rightarrow a^k \equiv b^k\,[m]$

→ **Appli** : Division euclidienne par 7 de $a = 59^{45}$

$a = 59^{45}$ $\quad a\,[7]$ $\quad 59 \equiv 3\,[7]$

$59^{45} \equiv 3^{45}\,[7]$

$a \equiv 3^{45}\,[7]$

$3^0 \equiv 1\,[7]$ $\quad 3^1 \equiv 3\,[7]$

$3^2 \equiv 2\,[7]$

$3^3 \equiv 6\,[7]$

$3^4 \equiv 4\,[7]$

$3^5 \equiv 5\,[7]$

$3^6 \equiv 1\,[7] \equiv 3^0 \equiv 7$;

$3^k \equiv 3^{k[6]}\,[7]$

3^k est périodique de période 6 dès $k \geq 3$

$45 \equiv 3\,[6]$

$3^{45} \equiv 3^3 \equiv 27 \equiv 6\,[7]$

$a \equiv 6\,[7]$

Appli(cation): critères de divisibilités

→ Applis critères de divisibilités

En base 10, $p = \overline{b_{n-1} b_{n-2} \dots b_1 b_0}^{10}$

$p = b_{n-1} 10^{n-1} + \dots + b_1 10 + b_0$

$a | p \Leftrightarrow p \equiv 0[a] \Leftrightarrow b_{n-1} 10^{n-1} + \dots + b_1 10 + b_0 \equiv 0[a]$

I Nombres premiers

$n \in \mathbb{N}^*$ est 1er s'il n'est divisible que par 1 et n

Méthode 1) Crible d'Eratosthène

(1) (2) (3) ~~4~~ (5) ~~6~~ (7) ~~8~~ ~~9~~ ~~10~~
(11) 12 13 14 15 ...
(29) ....
... .
91 - - - -
100

On retire tous les multiples des premiers de la 1ère ligne ($< \sqrt{110}$). Ce qui reste est premier

- nb premiers infinis
  $\forall n \in \mathbb{N}, \exists$ nb premier $> n$

car | Soit $p = n! + 1$, $p > n$, p pas divisible par $1, 2, \dots, n$
- p premier ⇒ p plus grand que n
- p ~~n'est pas~~ ⇒ p ~~pas premier~~ divisible par qqch $> n$

ch 7 : §3

Meth 2e) Euler

$f(n) = n^2 + n + 41$ est premier $\forall n$ < 40

1/3 des $f(n)$ sont premiers

Meth 4e) $f(n) = 2 + (2(2!) \bmod (n+1))$

Ça donne tous les nombres premiers

$f(2) = 2 + (2 \times 2 [3]) = 3$

Si n est 1er, $f(n-1) = 1$

si n n'est pas 1er, $f(n) = 2$

5e) Mersenne : $M_n = 2^n - 1$

M_n est 1er avec n 1er

VI Factorisation 1ère

Soit $a \geq 2$ n entier

il a et a la plus petit diviseur $\neq 1$ premier

Soit ~~p_1 est a et p_2 est~~ $a = p_1 \cdot a_1$

(a_1 premier : a multiple de premier

a_1 pas premier : $a_1 = p_2 \cdot a_2$ ...

→ factorisation unique

Soit $a = \prod_{j=1}^{j=k} p_j^{\alpha_j}$ $\alpha_j \geq 1$

a	p_1
a_1	p_2
a_2	...
...	...

Supposons d | a, alors $d = \prod_{j=1}^{j=k} p_j^{\beta_j}$ avec $0 \leq \beta_j \leq \alpha_j$.

→ Nb diviseurs de $a = \prod_{j=1}^{j=k} (\alpha_j + 1)$

VII PGCD & PPCM

Soient a et $b \in \mathbb{N}^*$ $\{q_j\}$ la factorisation de

- $PPCM(a,b) = a \vee b = \prod_{j=1}^{j=k} (q_j)^{\sup(\alpha_j, \beta_j)}$ a ou b
- $PGCD(a,b) = a \wedge b = \prod_{j=1}^{j=k} (q_j)^{\inf(\alpha_j, \beta_j)}$
- $(a \vee b)(a \wedge b) = a \cdot b$

VII Principaux théorèmes

1°) Bezout

Soient a et $b \in \mathbb{N}^*$ avec $a \geq b$
$\exists (u,v) \in \mathbb{Z}^2 \mid d = au + bv$,

$d \mid a$, $d \mid b$, $d \mid a \wedge b$
or $a \wedge b \mid a$, $a \wedge b \mid b$, $a \wedge b \mid (au + bv)$
donc $d = a \wedge b$ (c'est arithmétique)

1. $d = a \wedge b \Rightarrow \exists (u,v) \in \mathbb{Z}^2 \mid d = au + bv$

2. $a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$

2°) Gauss

$a \mid bc$ et $a \wedge b = 1$
$\Rightarrow a \mid c$

3°) Divers

- $a \wedge b = 1$ et $a \wedge c = 1 \Rightarrow a \wedge bc = 1$
- $\forall (n,m) \in \mathbb{N}^2$ $a \wedge b \Rightarrow a^n \wedge b^m = 1$

II Algorithme d'Euclide

$a = bq + r \rightarrow$ si $r = 0$, $a = bq$, $a \wedge b = b$

$\rightarrow$ si $r \neq 0$, $r = a - bq$:

$a \wedge b \mid a$ et $a \wedge b \mid b$ donc $a \wedge b \mid r$

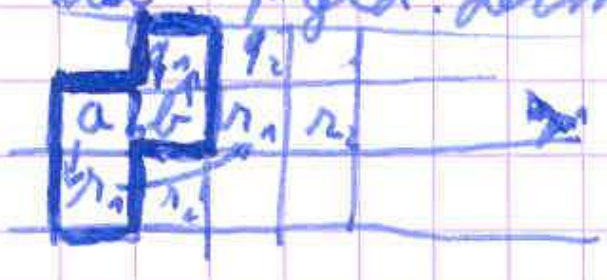
$\rightarrow a \wedge b \mid b \wedge r$

$b \wedge r \mid a \wedge b$ et $b \wedge r \mid b$ donc $b \wedge r \mid a$

$\rightarrow b \wedge r \mid a \wedge b$

$\Rightarrow a \wedge b = b \wedge r$

- On effectue des suites de divisions. 1 seul reste nul : pgcd : dernier reste non nul



- trouver les beaux :

On calcule l'expression des restes en fonction de a et b à partir de l'expression

$r_1 = a - bq_1$

$r_2 = b - r_1 q_2$

$r_3 = r_1 - r_2 q_3$

...

ch 7 : A 5

I Equations diophantiennes

de $\mathbb{Z}$: $Ax+By=C$ (1) où $AB \neq 0$

→ 0. A et $B \in \mathbb{N}^*$ (en changeant de variable $y=-y$, ...)

→ 1. on calcule $d = A \wedge B$
- → par fact° 1ère
- → par algo d'Euclide

⚠ Si $d \nmid c$ ⟹ (1) impossible

on

(2) on pose $a = Ad$, $b = Bd$, $c = Cd$
$ax+by=c$

→ 2. On trouve les bezous de a et de b

(3) $au+bv=1$ $(u,v) \in \mathbb{Z}^2$

→ 3. (4) = (3) × c : $\begin{cases} acu+bcv=c \\ (2)\ ax+by=c \end{cases}$

(4) − (2) : $a(x-cu) = b(-y+cv)$

→ 4. Gauss : $a \mid (-y+cv)$ $b \mid (x-cu)$

$\begin{cases} x = \lambda b + cu \\ y = -\lambda a + cv \end{cases}$ $\lambda \in \mathbb{Z}$

→ 5. Vérifier en remplaçant x et y dans (1)