104	Nombres premiers	Th. fondamental de l'arithmétique (Monier p.119)	Monier alg. MPSI De Biasi Damphousse Sorosina alg.

Prérequis:
Arithmétique dans $\mathbb{Z}$ (divisibilité, Pgcd, Ppcm, Th. Bézout, Th. Gauss).
Congruences, Anneaux $\mathbb{Z}/n\mathbb{Z}$.

I. Généralités.

Def.1: Un élément p de $\mathbb{N}$ est dit **premier** ssi p≥2 et: $\forall a \in \mathbb{N}^*, \quad (a \mid p \Rightarrow (a=1 \text{ ou } a=p))$.

Un entier n≥2 non premier est dit **composé**. On peut dire qu'un entier relatif n est premier ssi |n| l'est.

Prop.1: Soient p premier, et a∈$\mathbb{Z}^*$. On a:
$p \mid a$ ou $p \wedge a = 1$.
Si un nombre est premier, il est **premier avec tous les nombres qu'il ne divise pas**. (BIA)

Corollaires:
Si p, q sont deux nombres premiers distincts (positifs), alors $p \wedge q = 1$.
Si p est premier, il est **premier avec tous les entiers non nuls qui lui sont inférieurs**. (BIA)

Prop.2: Soient p premier et n∈$\mathbb{Z}^*$, $x_1,...,x_n \in \mathbb{Z}^*$. On a:
$p \mid \prod_i x_i \Leftrightarrow \exists i : p \mid x_i$
Cette proposition est le "premier théoème d'Euclide". (DAM)

II. Décomposition en facteurs premiers.

Th.1: **Décomposition en facteurs premiers**.
Tout élément de $\mathbb{N}$-{0;1} admet une décomposition en facteurs premiers, unique à l'ordre des facteurs près.

Exemples: $9100=2^2.5^2.7.13$, et $1848=2^3.3.7.11$.

Remarque 1: cette décomposition s'appelle aussi "décomposition primaire".

Remarque 2 (DAM) : L'unicité de cette décomposition ne va pas de soi; dans l'ens. des entiers pairs, 60=6x10=2x30.

Corollaire: Tout entier a de $\mathbb{Z}$-{-1;0;1} admet au moins un diviseur premier.

Th.2: L'ensemble des nombres premiers est **infini**.(1)

Crible d'Eratosthène (BIA) : C'est la table des $\mathbb{N}^*$, par ex. de 1 à100, ds laquelle on raye ts les multiples de 2, puis de 3, puis de p premier (à partir de p^2, avt c'est déjà fait).

Prop.4: **Pgcd, Ppcm**. Soit $(a,b) \in (\mathbb{N}-\{0;1\})^2$,
$a = \prod_{i=1}^{N} p_i^{r_i}, b = \prod_{i=1}^{N} p_i^{s_i}$, où $N \in \mathbb{N}^*$,
$p_1,..., p_N$ sont premiers et deux à deux distincts,
$r_1,..., r_N, s_1,..., s_N \in \mathbb{N}$ éventuellement nuls.
On a: $a \wedge b = \prod_{i=1}^{N} p_i^{Min(r_i,s_i)}$ et $a \vee b = \prod_{i=1}^{N} p_i^{Max(r_i,s_i)}$.

Exemples:
$9100 \wedge 1848 = 2^2.7^1 = 28$
$9100 \vee 1848 = 2^3.3^1.5^2.7^1.11^1.13^1 = 600\ 600$

Corollaire: Les lois $\wedge$ et $\vee$ sont **distributives** l'une sur l'autre dans $\mathbb{Z}^*$.

°Prop.5:
Soient a,b∈$\mathbb{Z}^*$. On a: $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |ab|$

Application (BIA): **Nombre de diviseurs d'un nombre**. Si $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha_i}$, les diviseurs de n sont les termes du développement du produit: $(1+p_1+p_1^2+...+p_1^{\alpha_1})...(1+p_i+p_i^2+...+p_i^{\alpha_i})$.
Leur nombre est $(1+\alpha_1)(1+\alpha_2)...(1+\alpha_i)$.

Exemple (BIA): $252=2^2.3^2.7$ possède 3.3.2=18 diviseurs.

Th.3 (BIA): **Petit théorème de Fermat**: (2)
∀n∈$\mathbb{N}^*$, ∀p premier, $n^p - n$ est divisible par p.
Si de plus p ne divise pas n, p divise $n^{p-1}-1$.

Le pt th. de Fermat est une condition nécessaire de primalité. Il est utilisé pour analyser la décomposition en facteurs premiers de certains entiers, générer de grands nombres premiers ou tester la primalité d'un nombre (cryptographie).

III. Quelques applications aux structures algébriques.

Prop.3: Soit p∈$\mathbb{N}^*$. Les trois propriétés suivantes sont équivalentes:
(i) p est **premier**
(ii) $\mathbb{Z}/p\mathbb{Z}$ est un **corps** (commutatif)
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre (3)

°Prop.4 (BIA): A un isomorphisme près, il n'existe qu'un seul **groupe d'ordre p premier**; ce groupe est cyclique et isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +)$. (4)

IV. Nombres particuliers.

On présente ici quelques-unes des catégories de nombres qui ont été explorées dans la tentative de mieux comprendre la structure des nombres premiers.

A. Les nombres de Fermat (1607-1665) (BIA)

Def.2: Les nombres de Fermat sont les $F_n = 2^{(2^n)} + 1$, où $n \in \mathbb{N}$.

Exercice: Mq deux nombres de Fermat distincts sont premiers entre eux. (5)
Fermat croyait ces nombres tous premiers, mais Euler a montré que F_5 est divisible par 641.

B. Les nombres de Mersenne (1588-1648) (BIA)

Def.3: Les nombres de Mersenne sont les $M_p = 2^p - 1$ est appelé nbre de Mersenne d'indice p.

Mersenne croyait ces nombres premiers pour p∈{2;3;5;7;13;17;19;31;67;127;257} et composés pour les autres p premiers <257. Or M_{61}, M_{89}, M_{107} sont premiers et M_{67} et M_{257} ne le sont pas.
La recherche des M_p premiers est un problème ouvert.

C. Les nombres parfaits (DAM)

Def.4: n∈ℕ* est dit parfait s'il est égal à la somme de ses diviseurs stricts.

Exemples: 6=1+2+3 ; 28=1+2+4+7+14.

Prop.5*: Les nombres parfaits pairs sont les nombres d'Euclide $E_p = 2^{p-1}(2^p - 1)$,où p et $2^p - 1$ sont premiers.(6) (Euler)
A ce jour, on ignore si les nombres parfaits impairs existent.

V. Notes.

Pierre Damphousse, (B.U. Ref:511DAM).
°Modifs /ordre du bouquin.

(1)Infinitude des nombres premiers; démo "classique" prise dans le Sorosina algèbre p.40.
→ Par l'absurde, supposer l'ensemble J des nombres premiers infini.
→ Poser n=Card(J), $\{p_1,...,p_n\}$ =J, et introduire: $N = 1 + \prod_{i=1}^{n} p_i$.
→ Considérer p un facteur premier de N, justifier que: $p \mid N - \prod_{i=1}^{n} p_i$, i.e. p|1, et conclure: p=1, donc N=1, contradiction.

(2)Petit théorème de Fermat (BIA): Soient p premier et $k \in [\![1; p-1]\!]$. On sait que :

$$C_p^k = \frac{p(p-1)...(p-k+1)}{k!},$$

qui représente le nbre combinaisons de p éléments (parties à p élts) parmi n, est entier. Donc k! divise C_p^k.
Pour k<p, tous les facteurs de k! sont <p, et donc sont premiers avec p puisque p est premier. Donc k! est premier avec p.
Ainsi $\begin{cases} k! \mid C_p^k \\ k! \wedge p = 1 \end{cases} \Rightarrow k! \mid (p-1)...(p-k+1)$,
donc (p-1)...(p-k+1)=λk!, et par suite :
$C_p^k = \lambda p, \lambda \in \mathbb{N}$, i.e. $C_p^k \equiv 0[p]$.

Alors ∀a,b∈ℕ,

$$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{n-k} \equiv C_p^0 b^p + C_p^p a^p \equiv a^p + b^p [p]$$

Par récurrence,∀n∈ℕ*,
$(a_1 + ... + a_n)^p \equiv a_1^p + ... + a_n^p [p]$.
Pour $a_1 = ... = a_n = 1$, il vient $n^p \equiv n[p]$,
i.e. $n^p - n \equiv 1[p]$,i.e. $n^p - n$ est divisible par p.
Ona donc $p \mid n(n^{p-1} - 1)$, et si $p \nmid n$, $p \mid n^{p-1} - 1$.

(3)ℤ/pℤ corps (BIA) : C'est un anneau; Elts inversibles? $\overline{a} \neq \overline{0}$ inversible ssi $\exists\, \overline{a}'$ tq $\overline{a}.\overline{a}' = \overline{1}$,
i.e. $\exists \overline{a'}$ tq $\overline{aa'} = \overline{1}$, i.e. ∃a'∈ℤ,k∈ℤ tq: aa'=1-kp,
i.e. ∃a'∈ℤ,k∈ℤ tq. aa'+kp=1, i.e. (Bézout) $a \wedge p = 1$.
Finalement, a non nul inversible ⇔ $a \wedge p = 1$.
Ainsi ts les élts non nuls sont inversibles (corps) ssi p est premier.

(4)Groupe d'ordre p (BIA):Soit G d'ordre premier p, l'ordre de ses sg divise p, donc ses sg sont {e} ou G. En particulier l'ordre de tt élt de G (ordre du sg engendré) est 1 ou p, donc si g∈G-{e}, alors G=<g>. Donc G est cyclique et par suite isomorphe à ℤ/pℤ.

(5)Deux nombres de Fermat sont premiers entre eux(BIA):

Soient F_n et F_{n+k}. Poser $X = 2^{2^n}$, alors $F_n = X + 1$ et $F_{n+k} = X^{2^k} + 1$. D'où :

$$F_{n+k} - 2 = X^{2^k} - 1$$

$$= (X+1)(X^{2^k-1} - X^{2^k-2} + X^{2^k-3} - ... - 1)$$

où le second facteur est un entier. Donc $F_n \mid F_{n+k} - 2$.
Par suite, toout diviseur de F_n et de F_{n+k} est un diviseur de 2; or F_n et F_{n+k} sont impairs par construction, donc ce diviseur commun à F_n et F_{n+k} est 1, i.e. $F_n \wedge F_{n+k} = 1$

(6) Nombres parfaits (DAM) /(BIA):

Attention, un nombre parfait est égal au **DOUBLE** de la somme de ses diviseurs (il est égal à leur somme simple si on exclut le nbre lui-même de la liste des diviseurs).

($\Leftarrow$) On note $\sigma \equiv$ somme des diviseurs.

$\sigma\left(2^{p-1}.\left(2^p-1\right)\right) = \sigma(2^{p-1})^{(1)}.\sigma(2^p-1)^{(2)} = 2^p.\left(2^p-1\right)$ (1): somme d'une série géom. (2): premier par hyp.

($\Rightarrow$)Soit P nbre parfait pair, par ex. $P = 2^{n-1}q$, avec q impair (donc n>1). 2^{n-1} et q sont premiers entre eux, donc $\sigma\left(2^{n-1}q\right) = \sigma(2^{n-1})^{(1)}.\sigma(q) = (2^n-1).\sigma\left(q\right)$ (a')

Or 2^{n-1}q est parfait donc $\sigma\left(2^{n-1}q\right) = 2P = 2^n q$ (a).

Ainsi $\underbrace{\left(2^n-1\right)}_{\text{impair}}.\sigma(q) = \underbrace{2^n}_{\text{pair}}.q$, donc $\left(2^n-1\right) \mid q$,

i.e. $\exists r \in \mathbb{N}^* / \underbrace{q = \left(2^n-1\right)r}_{(b)}$, i.e. $\underbrace{q+r = 2^n r}_{(c)}$, d'où:

q est un diviseur de q, et d'après (b), r aussi, donc $\sigma(q) \geq q+r$;

Donc $\left(2^n-1\right).\sigma(q) \geq \left(2^n-1\right)(q+r) \underset{(c)}{=} \underline{\left(2^n-1\right)}2^n \underset{(b)}{\underline{r}} = 2^n q$

$\underset{(a)}{=} \sigma\left(2^{n-1}q\right) \underset{(a')}{=} \left(2^n-1\right).\sigma(q)$, ainsi la 1° inég. est une =,

i.e. $\left(2^n-1\right).\sigma(q) = \left(2^n-1\right)(q+r) \Rightarrow \sigma(q) = q+r$;

ainsi q et r sont les seuls diviseurs de q, or un nombre admet au moins ses diviseurs propres, donc r=1. Finalement, q n'dmet pour diviseurs que 1 et lui-même, donc q est premier. De plus, (b) $\Rightarrow$ q=<u>(2^n-1) premier</u>.

On a posé au départ P=2^{n-1}q,

donc P=2^{n-1}(2^n-1), avec (2^n-1) premier ; vu la def° des nombres d'Euclide, il reste à montrer que n est premier. On a (2^n-1) premier. Si n est composé, n=ab, il vient: $2^n-1 = 2^{ab}-1 = (2^a)^b-1 = (2^a-1).[(2^a)^{b-1}+(2^a)^{b-2}+\ldots+1]$, et cette factorisation contredit (2^n-1) premier, ce qui achève la démonstration.