Arithmétique

1 Théorème de Fermat[1]

Théorème : soit p premier. Alors :
– $\forall a \in \mathbb{Z}$, $a^p \equiv a[p]$
– si $pgcd(a,p) = 1$, alors $\forall a \in \mathbb{Z}$, $a^{p-1} \equiv 1[p]$

Autre point de vue : (p premier, p ne divise pas a) $\Rightarrow a^{p-1} \equiv 1[p]$

Exemple : p premier, $a < p$ alors $a^{p-1} \equiv 1[p]$

2 Bezout

$pgcd(a,b) = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 \Leftrightarrow \exists (u',v') \in \mathbb{Z}^2$, $au' - bv' = 1$

2.1 Polynômes

$$\forall n \in \mathbb{N},\ a^n - 1 = (a-1)(a^{n-1} + ... + a + 1) = (a-1)(\sum_{k=1}^{n} a^{n-k})$$

$$\text{Si } n \text{ impair, } a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + ... - a + 1) = (a-1)(\sum_{k=1}^{n} (-1)^{k+1} a^{n-k})$$

Si n est pair, on ne peut rien dire.

3 pgcd , ppcm

$\forall a,b \in \mathbb{N} \times \mathbb{N}^*$, $\exists ! d \in \mathbb{Z}$ tq. $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. d s'appelle le $pgcd$ de a et b
$\forall a,b \in \mathbb{N} \times \mathbb{N}^*$, $\exists ! m \in \mathbb{Z}$ tq. $a\mathbb{Z} \bigcap b\mathbb{Z} = m\mathbb{Z}$. m s'appelle le $ppcm$ de a et b

Autre définition possible :
d est appelé $pgcd(a,b)$ si(si) $d|a, d|b$ et si $d'|a, d'|b$ alors $d'|d$
m est appelé $ppcm(a,b)$ si(si) m multiple de a et de b, et si m' multiple de a et b alors m' multiple de m

4 Division Euclidienne dans $\mathbb{Z}$

Théorème : Soient $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tq. $a = bq + r$, avec $0 < r \leqslant b$

5 Congruence dans $\mathbb{Z}$

Soient $x \equiv a[n]$ et $y \equiv b[n]$. Alors :

1. $x + y \equiv a + b[n]$
2. $x.y \equiv a.b[n]$

Soient $x \equiv a[n]$. Alors :

1. $p.x \equiv p.a[n]$, $\forall p \in \mathbb{Z}$
2. $x^k \equiv a^k[n]$, $\forall k \in \mathbb{N}^*$

Si $kx \equiv ky[n]$ et $pgcd(k,n) = 1$ alors $x \equiv b[n]$

[1] Sources : Dixmier, Terracher, Pernot. Tapé par Gwendal Haudebourg, réalisé avec LaTeX. Niveau : Capes. Compléments : cf. leçons 9-11. Mise à jour le 31/07/2007

6 Formulaire

1. $\forall (a, b \in \mathbb{Z}^2)$, $a.b = pgcd(a, b) * ppcm(a, b)$
2. $pgcd(na, nb) = n.pgcd(a, b)$, $ppcm(na, nb) = n.ppcm(a, b)$

Exemple : $pgcd(527, 408) = 17.pgcd(31, 24) = 17$ car $pgcd(31, 24) = 1$
$ppcm(527, 408) = 17.ppcm(31, 24) = 17.31.24$

6.1 Gauss

$$\begin{cases} a \mid c \\ b \mid c \end{cases} \text{ et } pgcd(a, b) = 1 \Rightarrow a.b \mid c$$

$$\begin{cases} a \mid bc \\ pgcd(a, b) = 1 \end{cases} \Rightarrow a \mid c$$

6.2 Divers

– Tout entier relatif $k \in \mathbb{Z}$ peut s'écrire : $k = 2^{\alpha}.q$, où q impair
– $\frac{impair}{pair} \neq entier$

Si $a \mid b$ et $a \mid c$, alors $a \mid bc$
Si $a \mid b$ et $a \mid c$, alors $a \mid bx + cy$, $\forall (x, y) \in \mathbb{Z}^2$

$$pgcd(a, b) = d \Rightarrow \begin{cases} a = da_1 \\ b = db_1 \end{cases} \text{ et } pgcd(a_1, b_1) = 1$$

7 Preuves Fermat

7.1 Preuve 1

Lemme : si p premier, alors $p \mid C_p^k$, $0 < k < p$

preuve : $k!\, C_p^k = p.(p-1)...(p-k+1)$, donc $p \mid k!\, C_p^k$
Or $pgcd(p, k!) = 1$ car p premier, et $k < p$, donc par le théorème de Gauss : $p \mid C_p^k$, $0 < k < p$ □

De plus : $(x+y)^p = x^p + C_p^1 x^{p-1} y + ... + C_p^{p-1} x y^{p-1} + y^p$
$p \mid C_p^1$,...,$p \mid C_p^{p-1}$ donc $(x+y)^p \equiv x^p + y^p [p]$, que l'on peut généraliser :

$$(x_1 + ... + x_n)^p = x_1^p + ... + x_n^p [p]$$

En prenant $x_1 = ... = x_n = 1$, on a $n^p \equiv n[p]$

7.2 Preuve 2

On notera $\mathbb{F}_p^{\times} = \mathbb{Z}/p\mathbb{Z}$ où p premier, $\mathbb{F}_p^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times} = (\mathbb{Z}/p\mathbb{Z})^*$ éléments inversibles (lorsque p premier). On notera $\overline{x} \in \mathbb{F}_p^{\times}$ par x pour simplifier les choses.

Dans un corps, tous les éléments sont inversibles sauf 0. $\mathbb{F}_p^{\times}$ a donc $p-1$ éléments.
Soit $x \in \mathbb{F}_p^{\times} \Rightarrow x^{p-1} = 1$ et $x \neq 0$ (ie p ne divise pas x)

Donc (p ne divise pas x) $\Rightarrow x^{p-1} \equiv 1[p]$
Et $\forall x \in \mathbb{Z}$, $x^p \equiv 1[p]$

7.3 Preuve 3

Soit ϕ : $\begin{array}{ccc} \mathbb{F}_p^\times & \to & \mathbb{F}_p^\times \\ x & \mapsto & a.x \end{array}$

On voit facilement que ϕ est bijective ($\phi(x) = \phi(x') \Rightarrow a.x = a.x' \Rightarrow a^{-1}.ax = a^{-1}.a.x'$ car a inversible, donc $x = x'$ donc ϕ injective. ϕ surjective car même nombre d'éléments au départ et à l'arrivée).

$$\prod_{x\in\mathbb{F}_p^\times} x = \prod_{x\in\mathbb{F}_p^\times} a.x \Rightarrow \prod_{x\in\mathbb{F}_p^\times} x = a^{p-1} \prod_{x\in\mathbb{F}_p^\times} x$$

or $\prod_{x\in\mathbb{F}_p^\times} x$ est inversible, donc $a^{p-1} = 1$ (ie classe de a^{p-1} est égale à la classe de 1 dans $\mathbb{F}_p^\times$).

Donc (p ne divise pas a) $\Rightarrow a^{p-1} \equiv 1[p]$
Et $\forall x \in \mathbb{Z}$, $x^p \equiv 1[p]$