Faculté des Sciences ; Rabat	Arithmétique (Prérequis)

Théorème "Division euclidienne" : $\forall(a,b)\in\mathbb{Z}\times\mathbb{Z}^*, \exists(q,r)\in\mathbb{Z}\times\mathbb{N}^*,\ a=b.q+r$ avec $0\leq r<|b|$

➔ Cette opération s'appelle « **la division euclidienne de *a* par *b*** ».

➔ Les nombres *a*, *b*, *q* et *r* sont appelés respectivement le **dividende**, le **diviseur**, le **quotient** et le **reste** de cette division

La division	**Les classes d'équivalences**	**La congruence**
Soit $(a,b)\in\mathbb{Z}^2$. S'il existe un entier relatif k tel que $a=kb$, on dit que : ▪ b divise a ▪ b est un diviseur de a ▪ a est un multiple de b On note : b/a.	Soient $(a,n)\in\mathbb{Z}\times\mathbb{N}^*$et r le reste de la division euclidienne de a par n. L'ensemble des entiers relatifs qui ont le même reste r de la division par n est appelé ***la classe d'équivalence de a modulo n.*** Il est noté par $\bar{a}^n$, ou simplement $\bar{a}$. $\bar{a}=\{b\in\mathbb{Z}/\exists k\in\mathbb{Z},\ b=kn+r\}$	Soit $(a,b,n)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{N}^*$. Si $n/b-a$, on dit que a et b sont congrus modulo n et on note : $a\equiv b\ [n]$ ou $a\equiv b\ \mathbf{mod}(n)$
➔ b/a ⇔ b/−a ⇔ −b/−a ➔ b/a et a/b ⇔ |b| = |a| ➔ a/b et a′/b′ ⇒ aa′/bb′ ➔ x/a et a/z ⇒ x/z ➔ Si a/b et b≠0 alors |a|≤|b|. ➔ a/b et a/c ⇒ a/α.b + β.c	➔ $\bar{a}=\bar{b}\ \Leftrightarrow\ b\in\bar{a}$ ➔ $\forall a\in\mathbb{Z},\exists!\, r\in\{0;1;\dots;n-1\}$: $\bar{a}=\bar{r}$ ➔ L'ensemble des classes d'équivalences modulo n sera noté par $\mathbb{Z}/n\mathbb{Z}$. Et on a : $\mathbb{Z}/n\mathbb{Z}=\{\bar{0};\bar{1};\cdots;\overline{n-1}\}$ ➔ $\bar{0}$ **est l'ensemble de multiples de *n*** ➔ $\bar{x}=\bar{0}\ \Leftrightarrow\ n/x$	➔ a ≡ b [n] ⇔ a ≡ b [n] ⇔ ∃k ∈ ℤ; b = a + kn ➔ Si n∧c =d, alors : $ac=bc[n]\Leftrightarrow a=b[\frac{n}{d}]$ ➔ a ≡ b [n] et m/n ⇒ a ≡ b [m] ➔ a∧n =1⇔ ∃m ∈ ℤ; am ≡ 1[n]
$n/b-a\ \Leftrightarrow\ \overline{b-a}=\bar{0}\ \Leftrightarrow\ \bar{b}=\bar{a}\ \Leftrightarrow\ a\equiv b\ [n]\ \Leftrightarrow\ \exists k\in\mathbb{Z};\ b=a+kn$		
Théorème de Fermat Soit p un nombre premier et a un entier: - Si p ne divise pas a, alors $a^{p-1}\equiv 1$ [p]. - Pour tout entier x, $x^p\equiv x$ [p].	Si $\bar{a}=\bar{b}$ et $\bar{x}=\bar{y}$, alors : ➔ $\overline{\alpha.a+\beta.x}=\overline{\alpha.b+\beta.y}\quad\forall(\alpha,\beta)\in\mathbb{Z}^2$ ➔ $\overline{a.x}=\overline{b.y}$ ➔ $\overline{a^k}=\overline{b^k}\quad\forall k\in\mathbb{N}$	Si a ≡ b [n] et x ≡ y [n], alors : ➔ α.a + β.x ≡ α.b + β.y [n] ∀(α,β) ∈ ℤ² ➔ a.x ≡ b.y [n] ➔ $a^k\equiv b^k[n]\quad\forall k\in\mathbb{N}$
Soit $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier : $\forall\bar{a}\neq\bar{0},\exists\bar{b}\neq\bar{0}:\ \bar{a}\,\bar{b}=\bar{1}$	**Addition et produit des classes d'équivalence :** $\bar{a}+\bar{b}=\overline{a+b}$ et $\bar{a}.\bar{b}=\overline{a.b}$ ➔ $\overline{\alpha.a+\beta.x}=\alpha.\bar{a}+\beta.\bar{b}\quad\forall(\alpha,\beta)\in\mathbb{Z}^2$ ➔ $\overline{a^k}=\bar{a}^k\quad\forall k\in\mathbb{N}$	**Théorème :** Soient $0\leq a<n$ *et* $0\leq b<n$. On a : $a=b[n]\Leftrightarrow$ **a=b**

Nombres premiers	PGCD	PPCM
Un entier relatif p est dit **premier** s'il admet **que** quatre diviseurs : p, -p, 1 et -1.	Soient a et b deux entiers non tous deux nuls. **Le plus grand commun diviseur de a et b** (noté pgcd (a,b) ou a∧b) est le plus grand entier **positif** divisant à la fois a et b.	Soient a et b des entiers non nuls. **le plus petit commun multiple de a et b** (noté ppcm(a,b) ou a∨b) est le plus petit entier **positif** qui est à la fois multiple de a et de b.
Crible d'Ératosthène : Si un entier naturel a n'est pas premier, alors il admet un diviseur premier p vérifiant $p^2 \leq a$. **En pratique** : Si tous les nombres premiers p vérifiant $p \leq \sqrt{a}$ ne divisent pas n, alors n est aussi premier.	Deux entiers non nuls sont dits **premiers entre eux** lorsque a∧b = 1	
Théorème : L'ensemble des nombres premiers est infini.	➢ a∧1 = 1; a∧0 =|a|; a∧b= b∧a ➢ $a/b \Leftrightarrow$ a∧b = $\|a\|$ ➢ (ka)∧(kb) =|k| × (a∧b) ➢ k/a et $k/b \Longrightarrow \frac{a}{k} \wedge \frac{b}{k} = \frac{1}{\|k\|} \times$ (a∧b) ➢ a∧b=1 et a∧c=1 ⟹ a∧bc=1 En particulier : a∧b=1 ⟹ $a^n \wedge b^m = 1$ pour tous m et n de $\mathbb{N}^*$. ➢ Si a/n et b/n et si a∧b = 1, alors ab/n.	➢ a ∨ 1 = |a| ; a∨0 =0 ➢ a/b ⟺ a∨b = |b|. ➢ ka∨kb = $\|k\|$ × (a∨b) ➢ k/a et k/b ⟹ $\frac{a}{k} \vee \frac{b}{k} = \frac{1}{\|k\|} \times$ (a∨b) ➢ (a∧b) × (a∨b) = |ab| **En particulier :** Si a∧b=1, alors a∨b = |ab|
Le théorème fondamental de l'arithmétique : Tout entier non nul a ≠ 1 et -1 se décompose d'une manière unique en produit de nombres premier : $a = \varepsilon\, p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ tel que les p_i sont des nombres premiers positifs différents deux à deux et tel que $\varepsilon = 1$ si $a > 0$ et $\varepsilon = -1$ si $a < 0$. **Conséquence:** Le nombre des diviseurs positifs de a est : $N=(1+\alpha_1) \cdots (1+\alpha_n)$.	d/a et d/b ⟺ d/(a∧b)	a/m et /m ⟺ (a∨b)/m.
Pour un **nombre premier p** on a : ➢ p ne divise pas x ⟺ p ∧ x = 1 ➢ p/ab ⟺ p/a ou p/b ➢ p/a^n ⟺ p/a	**Théorème de Gauss :** a/bc et a∧b = 1 ⟹ a/c	**Théorème de Bézout** ➢ a∧b =d ⟹ $\exists (u,v) \in \mathbb{Z}^2 : ua + vb = d$ ➢ a∧b =1 ⟺ $\exists (u,v) \in \mathbb{Z}^2 : ua + vb = 1$
	Les équations diophantiennes : Une équation diophantienne d'*inconnue le couple* $(x,y) \in \mathbb{Z}^2$ est de la forme : (*) ax + by = c avec a , b et c des entiers. ➢ L'équation (*) a des solutions si et seulement si a∧b /c. ➢ Si (x_0, y_0) est une solution de l'équation (*), alors l'ensemble de solutions de (*) s'écrit de la forme : $S = \{(x_0 + kb_0; y_0 + ka_0)/k \in \mathbb{Z}\}$ avec $b_0 = \frac{b}{a \wedge b}$ et $a_0 = \frac{a}{a \wedge b}$	