Un **anneau est ordonné par**  ssi   
Un **anneau est totalement ordonné par**  ssi est ordonné et ordre total.  
Un **anneau est archimédien** ssi   
 est un anneau unitaire commutatif, intègre, totalement ordonné, archimédien.  
Toute partie non vide de majorée admet un maximum pour .  
Toute partie non vide de minorée admet un minimum pour .  
 n’est ni majoré ni minoré pour .En posant , . est un modèle de Peano valide  
 et   
Les éléments inversibles de sont  :   
   
,   
**Divisibilité.**  
Un entier non nul  **divise**  / /  **est un multiple de /**  ssi .  
Dans ce cas est unique, est appelé **quotient de par** , et noté L’ensemble des diviseurs d’un entier est   
L’ensemble des diviseurs positifs d’un entier est   
L’ensemble des diviseurs négatifs d’un entier est   
 est une partition de . donc   
L’ensemble des multiples d’un entier est   
L’ensemble des multiples positifs d’un entier est   
L’ensemble des multiples négatifs d’un entier est   
   
   
   
**Division euclidienne.** Pour et ,   
 est **le quotient de la division euclidienne de par** , est **le reste de la division euclidienne de par** . On note .  
**Congruences.**Un entier est congru à un entier modulo un entier , et on note ssi ssi   
Etre congru modulo est une relation d’équivalence sur .  
Si alors   
Si alors   
Si alors   
Si alors   
Si alors   
Si est le reste de la DE de par , alors   
Si avec alors avec reste de la DE de par .  
**PGCD.**  
Le plus grand diviseur commun (PGCD) de deux entiers non nuls est noté et peut se définir par l’une des définitions équivalentes suivantes :  
   
   
   
Le PGCD est toujours strictement positif.   
Le PGCD est associatif et commutatif. . .  
On peut donc généraliser la définition du PGCD pour variables.   
, ,   
Etre un diviseur commun, c’est diviser le PGCD.   
   
**PPCM.**  
Le plus petit multiple commun (PPCM) de deux entiers non nuls est noté et peut se définir par l’une des définitions équivalentes suivantes :  
   
   
   
Le PPCM est toujours strictement positif.   
Le PPCM est associatif et commutatif. . .   
On peut donc généraliser la définition du PPCM pour variables.   
,   
Etre un multiple commun, c’est être multiple du PPCM.   
   
   
**Nombres premiers entre eux.  
Deux entiers sont premiers entre eux** ssi ssi   
 **entiers sont premiers entre eux dans leur ensemble** ssi ssi   
**Théorème de Bézout.**    
**Théorème de Bézout n.**    
Etre des nombres premiers entre eux dans leur ensemble, signifie avoir une combinaison linéaire qui donne 1.  
**Caractérisation du PGCD.**   
**Caractérisation du PGCD n.**   
**Relation de Bézout.**   
**Relation de Bézout n.**   
**Théorème de Gauss.**  si alors   
Autrement dit si et , alors   
Si un entier divise un produit, et est premier avec l’un des facteurs, alors il divise le produit des autres facteurs.  
**Corollaire 1 de Gauss.**   
**Corollaire 1 de Gauss n.**   
Un entier est premier avec chacun des entiers d’une famille, ssi il est premier avec leur produit.  
**Corollaire 2 de Gauss.** Si alors   
**Corollaire 2 de Gauss n.** Si alors   
Un multiple commun à des entiers premiers entre eux dans leur ensemble, est un multiple de leur produit.  
**Algorithme d’Euclide.** Permet de calculer le PGCD de 2 entiers.Pour , on peut construire une suite par récurrence :  
   
 on pose   
. L’algorithme d’Euclide s’arrête toujours. .   
**Nombres premiers.**Un **entier est inversible** ssi .   
**Deux éléments de sont associés ssi** ssi il existe un inversible tel que  divise , et divise càd Un **entier naturel ∖{1} est premier/irréductible**   
ssi ssi   
ssi càd il est premier avec tout naturel qu’il ne divise pas.  
ssi càd il est premier avec tout naturel strictement positif et inférieur.  
ssi ou càd est non inversible et en écrivant comme produit de deux facteurs, l’un doit être inversible, et l’autre doit être associé à .  
ssi si alors ou   
Un **entier ∖{-1 ; 1} est premier/irréductible**  
ssi est un naturel premier.  
ssi ssi   
ssi ou càd est non inversible et en écrivant comme produit de deux facteurs, l’un doit être inversible, et l’autre doit être associé à .  
ssi si alors ou   
ssi l’idéal est premier.  
En général, les questions de divisibilité ne dépendent pas du signe. On se restreint à étudier les premiers uniquement dans .   
**Propriétés des nombres premiers.**  
On note l’ensemble des entiers naturels premiers.  
Un entier premier est n’a pour diviseurs positifs que lui-même et , donc exactement deux.  
Un entier premier est premier avec tout entier naturel qu’il ne divise pas.  
Un entier premier est premier avec tous les naturels non nuls strictement inférieurs.  
**Lemme d’Euclide.** Un entier premier qui divise un produit, divise l’un des facteurs.  
L’ensemble des nombres premiers est infini.  
Tout entier (en valeur absolue) admet au moins un diviseur premier.  
La valuation -adique d’un entier , notée est la plus grande puissance de qui divise , elle vaut ssi ne divise pas .  
**Décomposition en facteurs premiers.**   
 tels que   
En notant la suite croissante des naturels premiers,  
   
Dans ce cas n’est autre que la valuation de dans .  
Un entier peut s’écrire puisque à partir d’un certain rang les valuations sont nulles.  
**Conséquences.**  
Le nombre de diviseurs positifs d’un entier naturel est   
Pour et on peut calculer PGCD et PPCM.  
   
   
**Théorème d’Euler.**   
, alors   
**Petit théorème de Fermat.**   
 premier Si ne divise pas alors   
 premier   
**Théorème des restes chinois  
Dans Z.** Si sont 2 a 2 premiers entre eux et alors  
l’application est un isomorphisme d’anneaux.  
**Wilson.** Un entier est premier ssi   
Un **nombre de Mersenne** est un nombre de la forme avec premier.  
Un **nombre de Fermat** est un nombre premier de la forme avec .  
Pour un nombre de Fermat , on a . On ne sait pas s’il y a un nombre de Fermat pour .  
Les nombres de Fermat sont premiers entre eux 2 à 2. Il y a une infinité de nombre premiers.  
La racine -ieme d’un entier est soit entière soit irrationnelle.  
Il y a une infinité de nombres premiers de la forme , .  
Pour , il existe une infinite de nombre premiers de la forme .  
En notant le nombre de premiers inferieurs a , alors