Spécialité mathématique : Arithmétique

I) Divisibilité et congruence dans Z

Divisibilité :

$-Soit\ (a,b) \in \mathbb{Z}^2, On\ sit\ que\ b|a\ si\ et\ seulement\ si\ \exists\ q \in \mathbb{Z}\ , a = bq$

$-Si\ a|b\ et\ b|c, alors\ a|c$

$-Si\ a|b, alors\ \forall c \in \mathbb{Z}\ , ac|bc$

$-Si\ a|b\ et\ \ a|c, alors\ \forall(q,q') \in \mathbb{Z}^2, a|qb + q'c$

$-Conséquence :\ Si\ a|b\ et\ a|c, alors\ a|b + c\ et\ a|b - c$

$-Si\ a|b\ et\ b|a, alors\ a = b\ ou\ a = -b$

$$\forall(a,b) \in\ \mathbb{Z}^2, \forall\ n \in \mathbb{Z}^*, a - b|a^n - b^n$$
$$Si\ n\ est\ impair, a - b|a^n + b^n$$

Division euclidienne :

$\forall\ a \in \mathbb{Z}, \forall\ b \in \mathbb{N},$
$\exists\ 1\ seul\ couple\ (q,r), q \in \mathbb{Z}, r \in \mathbb{N}\ tel\ que\ a = bq + r, avec\ 0 \leq r < b$

Effectuer la division euclidienne de l'entier relatif a par l'entier naturel non nul b, c'est déterminer l'unique couple (q,r), $q \in \mathbb{Z}, r \in \mathbb{N}$ tel que $a = bq$ avec :
- a le dividende
- b le diviseur
- q le quotient
- r le reste

$\forall\ a \in \mathbb{Z}, \forall\ b \in \mathbb{Z},$
$\exists\ 1\ seul\ couple\ (q,r), q \in \mathbb{Z}, r \in \mathbb{N}\ tel\ que\ a = bq + r, avec\ 0 \leq r < |b|$

PGCD :

Soient a et b deux entiers naturels non nuls. Le PGCD de a et b est le plus grand diviseur commun à a et b.
On note PGCD(a,b)

$Lemme\ d'Euclide$:
$Soit\ (a,b) \in \mathbb{N}^{*^2}, si\ q\ et\ r\ sont\ deux\ entier\ avec\ a = bq + r\ (r > 0)$
$Alors, PGCD(a,b) = PGCD(b,r)$

$- \textit{Les diviseurs communs à 2 entiers naturels non nuls sont les diviseurs de leur PGCD.}$

$- Soit\ (a, b, k) \in \mathbb{N}^{*3}, alors : PGCD(ka, kb) = k * PGCD(a, b)$

Soient a et b deux entiers relatifs non nuls. $\boldsymbol{PGCD(a,b) = PGCD(|a|,|b|)}$
On note PGCD(a,b)

Nombres premiers entre eux :

Deux entiers relatifs sont premiers entre eux si leur PGCD est égal à 1. C'est-à-dire que leurs seuls diviseurs communs sont 1 et -1.

$- Soit\ (a, b) \in \mathbb{Z}^{*2}, si\ PGCD(a, b) = d, alors :$
$il\ existe\ deux\ entiers\ relatifs, a', b'\ premiers\ entre\ eux\ tels\ que\ a = da'\ et\ b = db'.$

Fractions irréductibles :

$Soient\ (a, b) \in \mathbb{Z}^{*2},$
$\frac{a}{b}\ est\ une\ fraction\ irréductible\ si\ et\ seulement\ si\ a\ et\ b\ sont\ premiers\ entre\ eux.$

Congruence :

Soient a et b deux entiers relatifs, et n et entier naturel tel que n>1
On dit que a est congru à b modulo n lorsque a et b ont le même reste dans la division euclidienne par n.
On note : $\boldsymbol{a \equiv b[n]}$

$Soit\ (a; b) \in \mathbb{Z}^2, n \in \mathbb{N}, n \geq 2$ $\rightarrow\ a \equiv b[n] \Leftrightarrow n \mid a - b$ $\rightarrow\ a \equiv b[n] \Leftrightarrow \exists k \in \mathbb{Z}\ tel\ que\ a - b = kn$

$-Si\ a \equiv b\ [n] et\ c \equiv d\ [n], alors\ a + c \equiv b + d\ [n]$

$-Si\ a \equiv b\ [n] et\ c \equiv d\ [n], alors\ a - c \equiv b - d\ [n]$

$-Si\ a \equiv b\ [n] et\ c \equiv d\ [n], alors\ ac \equiv bd\ [n]$

$-Si\ a \equiv b\ [n], alors\ ac \equiv bc\ [n]$

$-Si\ a \equiv b\ [n], alors, \forall p \in \mathbb{N}, a^p \equiv b^p\ [n]$

$-Si\ a \equiv b\ [n] et\ c \equiv d\ [n], alors\ a \equiv c\ [n]$

$- Si\ a \equiv b\ [n], alors\ a - b \equiv 0\ [n]\ et\ b - a\ \equiv 0\ [n]$

II) Nombres premiers, PPCM

Dans ce chapitre, les entiers sont des nombres naturels.

Nombres premiers :

Un entier naturel est premier lorsqu'il admet exactement deux diviseurs dans $\mathbb{N}$ ***: 1 et lui-même***

$-Tout\ entier\ naturel\ distinct\ de\ 1\ admet\ au\ moins\ 1\ diviseur\ premier,$
$qui\ sera\ son\ plus\ petit\ diviseur\ dans\ \mathbb{N};\ autre\ que\ 1.$

$-Soit\ n \in \mathbb{N}, n \geq 2, si\ n\ n'estpas\ premier,$
$alors\ n\ admet\ un\ diviseur\ premier\ p\ tel\ que\ p^2 \leq n$

$-Un\ nombre\ premier\ est\ premier\ avec\ tous\ les\ entiers\ qu'ilne\ divise\ pas$

$Critère\ de\ primalité:$
$Soit\ n \in \mathbb{N}, n \geq 2.$
$Si\ n\ n'estdivisible\ par\ aucun\ entier\ premier\ p\ tel\ que\ p^2 \leq n, alors\ n\ est\ permier$

$-Théorème:\ Il\ existe\ une\ infinité\ de\ nombre\ premiers.$

Décomposition en facteurs premiers :

$Tout\ entier\ naturel\ supérieur\ ou\ égal\ à\ 2\ se\ décompose\ de\ manière\ unique$
$en\ produit\ de\ facteurs\ premiers\ (à\ l'ordredes\ facteurs\ près).$

$-Soit\ (a, b) \in \mathbb{N}^2, a \geq 2, b \geq 2,$
$b|a \Leftrightarrow tout\ facteur\ premier\ figurant\ dans\ la\ décomposition\ de\ b\ figure\ aussi$
$dans\ celle\ de\ a\ avec\ un\ exposant\ plus\ petit\ que\ celui\ de\ a.$

$-Si\ n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3} \ldots {p_n}^{\alpha_n}, alors\ le\ nombre\ de\ diviseurs\ positifs\ de\ n\ est\ égal\ à:$
$(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \ldots (\alpha_n + 1)$

PPCM :

Soient $(a, b) \in \mathbb{Z}^{*^2}$***, le plus petit multiple strictement positif commun à a et b est appelé plus petit multiple commun à a et b.***
On note PPCM(a,b).

$-L'ensembledes\ multiples\ communs\ à\ 2\ entiers\ naturels\ non\ nuls\ et\ l'ensemble\ des$
$multiples\ de\ leur\ PPCM.$

$-\ Soit\ (a, b, k) \in \mathbb{N}^{*^3}, alors: PPCM(ka, kb) = k * PPCM(a, b)$

-Soient a et b deux entiers naturels supérieurs ou égaux à 2.
Le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et de b avec pour chacun d'eux le plus petit exposant figurant dans la décomposition.

-Soient a et b deux entiers naturels supérieurs ou égaux à 2.
Le PPCM de a et b est égal au produit des facteurs premiers appartenant à au moins une des deux décompositions avec pour chacun d'eux le plus grand exposant figurant dans la décomposition.

-Le produit de deux entiers naturels est égal au produit de leur PPCM et de leur PGCD : $ab = PGCD(a,b) * PPCM(a,b)$

⇨ $Conséquence : si\ a\ et\ b\ dont\ premiers\ entre\ eux, PPCM(a,b) = ab.$

III) Nombres premiers, PPCM

Identité de Bézout :

$$Soient\ (a,b) \in {\mathbb{N}^*}^2, tel\ que\ PGCD(a,b) = d$$
$$Alors, \exists (u,v) \in \mathbb{Z}^2\ tel\ que\ au + bv = d$$

Théorème de Bézout :

$$Soient\ (a,b) \in {\mathbb{N}^*}^2, tel\ que\ PGCD(a,b) = 1$$
$$Alors, \exists (u,v) \in \mathbb{Z}^2\ tel\ que\ au + bv = 1$$

Théorème de Gauss :

$$Soient\ (a,b,c) \in \mathbb{N}^3,$$
$$Si\ a|bc, et\ si\ PGCD(a,b) = 1, alors\ a|c$$

$-Soient\ (a,b) \in {\mathbb{N}^*}^2, soit\ p\ un\ nombre\ premier, alors : si\ p|ab, alors\ p|a\ {}^{et}/_{ou}\ p|b$

$-Soient\ (a,b,c) \in \mathbb{N}^3, si\ PGCD(b,c) = 1\ et\ si\ b|a\ et\ c|a, alors\ bc|a$

Fractions irréductibles :

$Soient\ (a,b) \in {\mathbb{Z}^*}^2,$
$\frac{a}{b}\ est\ une\ fraction\ irréductible\ si\ et\ seulement\ si\ a\ et\ b\ sont\ premiers\ entre\ eux.$

$-Soient\ (a,b) \in {\mathbb{Z}^*}^2$,
$Toute\ fraction\ \dfrac{a}{b}\ est\ \text{é}gale\ \text{à}\ une\ unique\ fraction\ \dfrac{a'}{b'}\ irr\text{é}ductible\ (a',b') \in {\mathbb{Z}^*}^2$
$Toute\ fraction\ \frac{a}{b}\ est\ alors\ de\ la\ forme\ \frac{ka\prime}{kb\prime} n\ k \in \mathbb{Z}^*.$

Petit théorème de Fermat :

$Soit\ p\ un\ nombre\ premier\ qui\ ne\ divise\ pas\ a,$ $Alors : a^{p-1} \equiv 1\ [p]\ donc\ p \mid a^{p-1} - 1$

⇨ $Cons\text{é}quence : soit\ p\ un\ nombre\ premier, \forall a \in \mathbb{N}, p \mid a^p - a\ donc\ a^p \equiv a\ [p]$