Chapitre 18 : Arithmétique

A) Divisibilité sur $\mathbb{Z}$

- Notion de divisibilité
- Couple d'entiers associés
- Divisibilité et division euclidienne.

B) PGCD,PPCM

- Définition PGCD, premières propriétés
- Algorithme d'Euclide étendu (donnant également les coefficients de Bézout)
- Terminaison de l'algorithme, vérification qu'il renvoit le PGCD et les coefficients de Bézout.
- Existence d'une relation de Bézout
- Conséquences de la relation de Bézout
- Entiers premiers entre eux
- Théorème de Bézout, Théorème de Gauss, Factorisation par le PGCD
- Forme irréductible d'un irattionnel
- Extension à un nombre fini d'entiers et aux entiers relatifs
- Définition PPCM et lien avec le PGCD
- Propriétés PPCM

C) Nombres premiers

- Définition nombre premier, nombre composé
- Tout entier admet un diviseur premier
- lien entre nombre premier et entiers premiers entre eux
- Crible d'Erastothène
- Décomposition en produit de facteurs premiers
- Valuation p-adique
- Valuation p-adique du produit
- Lien entre valuation p-adique et divisibilité
- Expression du pgcm et pgcd à l'aide de la valuation p-adique

D) Congruences

- Relation de congruence (relation d'équivalence)
- Opération sur les congruences
- Utilisation inverse modulo n pour résoudre congruences
- Petit théorème de Fermat

Questions de cours :

- On prouvera les résultats suivants :
  Soit p un nombre premier.

  1) Pour tout $k \in [1, p-1]$, le coefficient binomial $\binom{p}{k}$ est divisible par p.

  2) Pour tout $(a, b) \in \mathbb{Z}^2$, on a $(a+b)^p \equiv a^p + b^p [p]$

3) Soit $n \in \mathbb{N}$, montrer que $n^p \equiv n[p]$ (on explicitera la récurrence) puis que si $p \nmid n, n^{p-1} \equiv 1[p]$ (Petit théorème de Fermat).

- Montrer l'existence et l'unicité d'une décomposition en facteurs premiers pour tout nombre $n \geq 2$ (on reprouvera que tout nombre $n \geq 2$ est produit de nombre premiers).
- En admettant la terminaison et la validité de l'algorithme d'Euclide étendu, montrer les 3 résultats suivants :

  1) Le théorème de Bézout.

  2) Soit $(a, b, c) \in \mathbb{N}^3, a \wedge c = 1, b \wedge c = 1$, montrer que $ab \wedge c = 1$.

  3) Le lemme de Gauss.
- On prouvera les 3 résultats suivants :

  1) Si $a|c, b|c$ et $a \wedge b = 1$, alors (a.b) | c.

  2) Soit $(a, b) \in \mathbb{N}^2$, $a \wedge b = 1$ alors $a \vee b = ab$.

  3) En déduire que pour $(a, b) \in \mathbb{N}^2, a \wedge b.a \vee b = ab$.