Semaine 12

▶ Arithmétique dans $\mathbb{Z}$

- notion de diviseur, de multiple, propriété $(a|b) \Leftrightarrow (b\mathbb{Z} \subset a\mathbb{Z})$;
- propriété d'Archimède, division euclidienne (avec unicité du reste positif) ;
- sous–groupes de $(\mathbb{Z}, +)$;
- pgcd (défini comme élément de $\mathbb{N}^*$), notation $a \wedge b$;
- ppcm (défini comme élément de $\mathbb{N}^*$), notation $a \vee b$, lien au pgcd ;
- algorithme d'Euclide : validité et terminaison ;
- relation de Bézout entre deux entiers non nuls et leur pgcd ; algorithme d'Euclide étendu ;
- entiers premiers entre eux ;
- théorème de Bézout, deux entiers une fois divisés par leur pgcd sont premiers entre eux ;
- lemme de Gauss et applications : équations diophantiennes, fractions irréductibles dans $\mathbb{Q}$;
- généralisations diverses au cas de familles de plus de deux entiers des résultats précédents, entiers premiers entre eux dans leur ensemble ;
- nombres premiers (définis comme strictement positifs), crible d'Ératosthène ;
- tout entier différent de ± 1 admet un diviseur premier, il existe une infinité de nombres premiers ;
- décomposition (unique à l'ordre près des facteurs) en produit de facteurs premiers ;
- valuation p–adique d'un entier naturel, application au calcul du pgcd et ppcm lorsque l'on connaît sa décomposition en produit de facteurs premiers ;
- rappels sur les congruences, compatibilité à l'addition et à la multiplication ;
- si p est premier et $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p \ [p]$;
- petit théorème de Fermat.

✖***Aucune connaissance n'est exigible des étudiants sur les sujets suivants : crypto–systèmes RSA, anneaux*** $\mathbb{Z}/n\mathbb{Z}$***.***

▶ Questions de cours (*démonstrations*)

- tout énoncé ou définition est exigible ;
- sous–groupes de $\mathbb{Z}$;
- existence du pgcd de deux entiers relatifs ;
- terminaison de l'algorithme d'Euclide ;
- lemme de Gauss ;
- si p est premier et $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p \ [p]$.