Arithmétique dans $\mathbb{Z}$

I Division

1. la relation « divise » dans $\mathbb{Z}$, ensembles $\mathcal{D}(a)$ des diviseurs et $a\mathbb{Z}$ des multiples de a. Division euclidienne dans $\mathbb{Z}$.
   Application aux sous-groupes de $(\mathbb{Z}, +)$.
2. Congruences. Propriétés, applications.
3. Décomposition en base S d'un nombre entier. Cas $S = 10$ et $S = 2$.
   Application : description d'un algorithme plus rapide de division euclidienne, algorithme d'exponentiation rapide.

II Outils et résultats fondamentaux

1. P.G.C.D de deux entiers, noté $a \wedge b$: définition, premières propriétés, algorithme d'Euclide, coefficients de Bezout.
2. P.P.C.M. de deux entiers, noté $a \vee b$: définition, propriétés élémentaires.
3. nombres premiers entre eux : définition, théorème de Bezout, forme irréductible d'une fraction rationnelle, lemme de Gauss.
4. Exemple d'équation diophantienne linéaire.
5. P.G.C.D. de plus de deux entiers. Nombres premiers entre eux 2 à 2 et dans leur ensemble.

III Nombres premiers

Définition, théorème fondamental de l'arithmétique (décomposition en produit de nombres premiers).
Valuations p-adique. Écriture du théorème fondamental à l'aide des valuations. Critère de divisibilité. Ecriture du pcgd, du ppcm.
Crible d'Eratosthène, l'ensemble des nombres premiers est infini.
Petit théorème de Fermat.

Questions de cours

Q1. Enoncé et démonstration de la division euclidienne sur $\mathbb{Z}$, celle sur $\mathbb{N}$ étant connue.

Q2. `[facultatif]` Décomposition en base S d'un entier naturel : énoncé et démonstration -algorithmique- de l'existence.

Q3. `[facultatif]` Décomposition en base S d'un entier naturel : énoncé et démonstration de l'unicité.

Q4. `[facultatif]` Décomposition d'un entier naturel en base S : énoncé et implémentation en python.

Q5. Si la décomposition en base 2 de n s'écrit $n = \sum_{k=1}^{p_n} \varepsilon_k 2^k$ avec $\varepsilon_p \neq 0$, donner un majoration de p_n en fonction de n. En déduire une majoration si $n = 10^q$.

Q6. `[facultatif]` Donner une implémentation python de l'algorithme d'exponentiation rapide. Donner une majoration du nombre d'opérations effectuées.

Q7. Algorithme d'Euclide de recherche du p.g.c.d. de deux entiers (présentation de l'algorithme et justification par variant/invariant de boucle).

Q8. Présenter clairement l'algorithme d'Euclide étendu pour déterminer explicitement $734 \wedge 214$ ainsi qu'une relation de Bezout.

Q9. Enoncé et démonstration du théorème de Bezout (on admet l'algorithme d'Euclide étendu) et du lemme de Gauss.

Q10. Si $a, b, c \in \mathbb{Z}$, résolution de l'équation $(E) : ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

Q11. Soient $a, x_1, ..., x_n \in \mathbb{N}^*$.
Démontrer que si pour tout $k \in [\![1, n]\!]$, $x_i \wedge a = 1$, alors $\left(\prod_{i=1}^{n} x_i\right) \wedge a = 1$.

Q12. Soient $a, x_1, ..., x_n \in \mathbb{N}^*$. Démontrer que si pour tout $i \in [\![1, n]\!]$, $x_i | a$ et si pour tout $(i, j) \in [\![1, n]\!]^2$, $i \neq j \Rightarrow x_i \wedge x_j = 1$, alors $\left(\prod_{i=1}^{n} x_i\right)$ divise a.

Q13. Démontrer que l'ensemble $\mathbb{P}$ des nombres premiers est infini (théorème d'Euclide).

Q14. Valuation p-adique : définition ; $v_p(m \times n) = v_p(m) + v_p(n)$ (à démontrer), conditions (à énoncer) sur les v_p pour que $m \mid n$, pour que $m \wedge n = 1$. Ecriture à l'aide des valuations de la décomposition en facteur premier, du pgcd et du ppcm (énoncé seul).

À venir : structures algébriques.