Arithmétique dans l'ensemble des entiers relatifs

1 Programme officiel

Les éléments en italique sont des ajouts ou précisions personnels, hors programme officiel.

a) Divisibilité et division euclidienne	
Divisibilité dans $\mathbf{Z}$, diviseurs, multiples.	Caractérisation des couples d'entiers associés.
Théorème de la division euclidienne.	
b) PGCD et algorithme d'Euclide	
PGCD de deux entiers naturels dont l'un au moins est non nul.	Notation $a \wedge b$. Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbf{N}$) de l'ensemble des diviseurs communs à a et b.
Algorithme d'Euclide.	L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$. $a \wedge b$ est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b. Pour $k \in \mathbf{N}^*$, PGCD de ka et kb.
Extension au cas de deux entiers relatifs.	
Relation de Bezout.	Détermination d'un couple de Bezout par l'algorithme d'Euclide étendu.
PPCM.	Notation $a \vee b$.
c) Entiers premiers entre eux	
Couples d'entiers premiers entre eux.	
Théorème de Bézout.	Forme irréductible d'un rationnel.
Lemme de Gauss.	
Si a et b premiers entre eux divisent n, alors ab divise n.	
Si a et b sont premiers à n, alors ab est premier à n.	
PGCD d'un nombre fini d'entiers, relation de Bezout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	

d) Nombres premiers	
Nombre premier.	Crible d'Eratosthène.
L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	
Pour p premier, valuation p-adique.	Notation $v_p(n)$.
Valuation p-adique d'un produit.	Caractérisation de la divisibilité en termes de valuations $p-$ adiques. Extension du PGCD et du PPCM à l'aide des valuations p-adiques.
e) Congruences	
Relation de congruence modulo un entier sur $\mathbf{Z}$.	Notation $a \equiv b\ [n]$.
Opérations sur les congruences : somme, produit.	Les anneaux $\mathbf{Z}/n\mathbf{Z}$ sont hors programme.
Utilisation d'un inverse modulo n pour résoudre une congruence modulo n.	
Petit théorème de Fermat.	

2 Exercices à savoir refaire

Et preuves sur lesquelles insister davantage.

- Existence et unicité de la division euclidienne (diviseur strictement positif).
- $(a \wedge b)(a \vee b) = ab$ sur $\mathbf{N}^*$.
- Lemme de Gauss.
- Si $a|c$ et $a'|c$ avec $a \wedge a' = 1$, alors $aa'|c$.
- Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier.
- Infinité des nombres premiers.
- Résolution $5x + 7y = 1$ ou équivalent sur $\mathbf{Z}$.
- Soit $(a, n) \in \mathbf{N}^* \times \mathbf{N}^*$ tel que $n \geqslant 2$. Notons $d = a \wedge n$. Montrer que ad divise $(a+1)^n - 1$.
- Exercice 86 CCINP

  1) Soit $(a, b, p) \in \mathbf{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
  2) Soit p un nombre premier.
     (a) Prouver que $\forall k \in [\![1,\, p-1]\!]$, p divise $\binom{p}{k} k!$, puis en déduire que p divise $\binom{p}{k}$.
     (b) Prouver que: $\forall n \in \mathbf{N},\ n^p \equiv n\ [p]$. *Indication*: procéder par récurrence.
     (c) En déduire, pour tout entier naturel n, que :

$$p \text{ ne divise pas } n \Longrightarrow n^{p-1} \equiv 1\ [p].$$

- Exercice 94 CCINP

  1) Énoncer le théorème de Bézout dans $\mathbf{Z}$.
  2) Soit a et b deux entiers naturels premiers entre eux.
     Soit $c \in \mathbf{N}$. Prouver que: $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
  3) On considère le système (S): $\begin{cases} x \equiv 6 \quad [17] \\ x \equiv 4 \quad [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbf{Z}$.
     (a) Déterminer une solution particulière x_0 de (S) dans $\mathbf{Z}$.
     (b) *Déduire des questions précédentes* la résolution dans $\mathbf{Z}$ du système (S).