Toutes les définitions /énoncés du cours sont à connaître précisément.

Exercice de cours

Exercice 1 *Ex. de cours, chap. 11, IV* — Soit $n \in \mathbb{N}$. On pose : $M_n = 2^n - 1$.
Montrer que si M_n est premier, alors n est premier.

Exercice 2 *Résultat et ex. du cours, chap 11, III.3* —
1. Démontrer le lemme de Gauss.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $7x + 12y = 3$.

Exercice 3 *Résultats de cours, chap 11, III.3* — Soient $a, b, c \in \mathbb{Z}$.
1. Montrer que si : $a \wedge b = 1$ et $a \wedge c = 1$, alors : $a \wedge bc = 1$.
2. Montrer que si : $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors : $ab \mid c$.

Exercice 4 *Résultat, chap 11, IV.3* —
Soit $n \in \mathbb{N}$ et soit p un nombre premier. Montrer que $n^p \equiv n\ [p]$.

1 Divisibilité et division euclidienne

1.1 Diviseurs, multiples

Définition

Soient $a, b \in \mathbb{Z}$. On dit que b divise a ou que a est un multiple de b s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On note $b \mid a$.

- **Remarque.** Si $a \mid b$ et $b \mid a$: alors $a = \pm b$. On dit alors que a et b sont associés.

Théorème : Combinaisons linéaires

Si $d \in \mathbb{Z}$ vérifie $d \mid a$ et $d \mid b$, alors, pour tous $u, v \in \mathbb{Z}$: $d \mid ua + bv$.

1.2 Congruences

Définition

Soit $n \in \mathbb{N}$. Soient $a, b \in \mathbb{Z}$. On dit que *a est congru à b modulo n* si $n \mid a - b$.

- **Rappel.** La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Théorème : Compatibilité avec les opérations

Soient $a, a', b, b' \in \mathbb{Z}$ et $n \in \mathbb{N}$. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors :
- *Somme.* $a + a' \equiv b + b'\ [n]$
- *Produit.* $aa' \equiv bb'\ [n]$ et en particulier $a^k \equiv b^k\ [n]$ ceci pour tout $k \in \mathbb{N}$

En pratique : congruences et divisibilité

n divise a si et seulement si : $a \equiv 0\ [n]$.

1.3 Division euclidienne

Théorème

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :
1. $a = bq + r$ 2. $0 \leq r < b$ (ou encore $0 \leq r \leq b - 1$)
- q est le *quotient* de la division euclidienne de a par b.
- r est le *reste* de la division euclidienne de a par b.

En pratique : congruences et reste

a est congru à un seul élément de $[\![0, b-1]\!]$:à savoir le reste de la DE de a par b.

2 PGCD et algorithme d'Euclide

2.1 Définition du PGCD

Définition

Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$ ou $b \neq 0$. On appelle PGCD de a et b le plus grand diviseur commun à a et b. On le note $a \wedge b$. Par convention : $0 \wedge 0 = 0$

Théorème

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{Z}$: $a \wedge b = b \wedge (a - kb)$.

2.2 Algorithme d'Euclide pour le calcul du PGCD de $a, b \in \mathbb{N}^*$

Algorithme d'Euclide

On définit une suite finie d'entiers r_k par récurrence :
- On pose initialement $r_{-1} = a$ et $r_0 = b$.
- Pour $k \in \mathbb{N}$, *tant que* $r_k \neq 0$, on définit r_{k+1} comme le reste de la DE de r_{k-1} par r_k *i.e.* $r_{k-1} = q_k r_k + r_{k+1}$ avec $0 \leq r_{k+1} < r_k$

Théorème

1. *L'algorithme se termine.* La suite d'entiers naturels (r_k) est finie : il existe $n \in \mathbb{N}$ tel que $r_n > 0$ et $r_{n+1} = 0$.
2. *L'algorithme fournit le PGCD :* $\quad a \wedge b = r_n$.
$a \wedge b$ est le dernier reste non nul fourni par l'algorithme d'Euclide.

2.3 Propriétés du PGCD

Théorème : Relation de Bézout

Soient $a, b \in \mathbb{Z}$ Il existe $u, v \in \mathbb{Z}$ tels que : $\quad a \wedge b = au + bv$

En pratique, pour obtenir une relation de Bézout

En peut procéder par « remontées » dans l'algorithme d'Euclide en renversant toutes les divisions euclidiennes.

Théorème

Soient $a, b \in \mathbb{Z}$. Les diviseurs communs à a et b sont les diviseurs de leur PGCD *i.e.* pour tout $d \in \mathbb{Z}$: $\quad (d \mid a \quad \text{et} \quad d \mid b) \iff d \mid a \wedge b$.

Théorème : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}$: $\quad (ka) \wedge (kb) = k(a \wedge b)$

2.4 PPCM

Définition

Soient $a, b \in \mathbb{Z}^*$. Le *PPCM* de a noté $a \vee b$ est le plus petit multiple strictement positif commun à a et b. Pour $a \in \mathbb{Z}$, on pose par ailleurs : $\quad a \vee 0 = 0 \vee a = 0$

Théorème : PPCM et multiples communs

Soient $a, b \in \mathbb{Z}$. Pour tout $m \in \mathbb{Z}$: $\quad (a \mid m \quad \text{et} \quad b \mid m) \iff a \vee b \mid m$.

Théorème : Factorisation

Soient $a, b \in \mathbb{Z}$. Pour tout $k \in \mathbb{N}$: $\quad (ka) \vee (kb) = k(a \vee b)$

Théorème : Relation PGCD-PPCM

Soient $a, b \in \mathbb{N}$: $\quad (a \wedge b) \times (a \vee b) = ab$

- **Remarque.** Plus généralement, pour tous $a, b \in \mathbb{Z}$: $\quad (a \wedge b) \times (a \vee b) = |ab|$

3 Entiers premiers entre eux

Dans cette partie a, b, c sont des entiers relatifs.

3.1 Définition

Définition

On dit que a et b sont premiers entre eux si : $\quad a \wedge b = 1, \quad$ ou encore si leur seul diviseur positif commun est 1.

En pratique :

Si $a \wedge b = d > 1$ on peut écrire : $\quad a = da' \quad \text{et} \quad b = db' \quad \text{où :} \quad a' \wedge b' = 1$.

3.2 Théorème de Bézout et lemme de Gauss

Théorème : Théorème de Bézout

Il y a équivalence entre :
1. a et b sont premiers entre eux.
2. Il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Théorème : Lemme de Gauss

Si $a \mid bc$ et si $a \wedge b = 1$ alors $a \mid c$.

☢ **Attention** ☢ C'est faux si $a \wedge b \neq 1$, par exemple $a = 6$, $b = 4$ et $c = 9$.

- **Application classique.** Equations de la forme $ax + by = d$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

3.3 Conséquences classiques.

Théorème : Entier premier avec un produit

Si $a \wedge b = 1$ et si $a \wedge c = 1$, alors $a \wedge bc = 1$.

- **Extensions.** • Si : $a \wedge b_1 = 1, \ldots, a \wedge b_n = 1$ alors : $a \wedge (b_1 \ldots b_n) = 1$
  • Si $a \wedge b = 1$ alors pour tous $m, n \in \mathbb{N}$: $a^n \wedge b^m = 1$

Théorème : Divisibilité par deux entiers premiers entre eux

Si $a \mid c$ et $b \mid c$ et si $a \wedge b = 1$, alors $ab \mid c$.

- **Extension.** Si $a_1, \ldots, a_n$ divisent c et sont premiers entre eux deux à deux alors leur produit $a_1 \ldots a_n$ divise c

Attention C'est faux si $a \wedge b \neq 1$, par exemple $a = 4$, $b = 6$ et $c = 36$.

- **Forme irréductible d'un rationnel.**

3.4 Extension à un nombre fini d'entiers

PGCD de n entiers, relation de Bézout, entiers premiers entre eux dans leur ensemble

4 Nombres premiers

4.1 Généralités

Définition

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si $p \geq 2$ et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Théorème : Lemme d'Euclide

Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$. Si $p \mid ab$ alors : $p \mid a$ ou $p \mid b$.

Théorème

Soit $n \in \mathbb{N}$ tel que $n \geq 2$. L'entier n possède au moins un diviseur premier.

Théorème

$\mathbb{P}$ est infini.

4.2 Petit théorème de Fermat

Exemple 1 -♥- Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$.
1. $n^p \equiv n\ [p]$. 2. Si n n'est pas divisible par p, alors $n^{p-1} \equiv 1\ [p]$.

4.3 Valuation p-adique

Définition

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a, notée $v_p(a)$, est le plus grand $k \in \mathbb{N}$ tel que p^k divise a. Autrement dit, $v_p(a) = k$ ssi :
• p^k divise a et p^{k+1} ne divise pas a • ou encore si $a = p^k q$ où p ne divise pas q.

Théorème : Additivité des valuations p-adiques

Soit $a, b \in \mathbb{N}^*$ et $p \in \mathbb{P}$: $v_p(ab) = v_p(a) + v_p(b)$

4.4 La décomposition en facteurs premiers

Théorème : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_n}$ avec :
• $p_1, \ldots p_n \in \mathbb{P}$. • $p_1 < p_2 < \cdots < p_n$. • $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$

- **Retenir.** Pour tout $p \in \mathbb{P}$, $v_p(a)$ est l'exposant de p dans la décomposition en facteurs premiers de a.

Théorème

Soit $a, b \in \mathbb{N}^*$ et $p_1, \ldots, p_n$ les facteurs premiers apparaissant dans la décomposition de a ou de b. On peut écrire :
$a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$ où $\alpha_i = v_{p_i}(a)$ et $\beta_i = v_{p_i}(b)$ pour tout $i \in [\![1, n]\!]$.

1. $b \mid a$ ssi : $\forall i \in [\![1, n]\!], \quad \beta_i \leq \alpha_i$

   ou encore ssi : $\forall p \in \mathbb{P}, \quad v_p(b) \leq v_p(a)$

2. • $a \wedge b = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$ • $a \vee b = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$