CHAPITRE 10

ARITHMÉTIQUE DANS $\mathbb{Z}$

L'arithmétique est l'étude des propriétés de $\mathbb{Z}$ vis-à-vis de la relation de divisibilité. Nous commençons par rappeler les propriétés élémentaires de $\mathbb{N}$.

1. Axiomatique de $\mathbb{N}$.

Proposition 1.1

L'ensemble $\mathbb{N}$ vérifie les propriétés suivantes.

(1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

(2) Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.

(3) $\mathbb{N}$ n'admet pas de plus grand élément.

Théorème 1.2: Principe de récurrence

Soit $(P(n))_{\substack{n\in\mathbb{N}\\ n\geq n_0}}$ une famille de propositions. On suppose que

(1) $P(n_0)$ est vraie (initialisation) ;

(2) $\forall n \geq n_0$, $P(n) \implies P(n+1)$ (hérédité).

Alors $P(n)$ est vraie pour tout $n \geq n_0$.

Exemple 1.3

Les deux étapes : initialisation et hérédité, sont aussi importantes l'une que l'autre. Voici un exemple de démonstration par récurrence fausse.

Pour $n \in \mathbb{N}$, on note $P(n)$ la proposition $n^2 = n$.

— Prouvons que P_0 est vraie : $0^2 = 0$, donc P_0 est vraie.

— Soit n un entier quelconque fixé. Alors

$$\begin{aligned} n^2 = n &\implies n^3 = n^2 = n \\ &\implies n^3 - 1 = n - 1 \\ &\implies (n-1)(n^2+n+1) = n-1 \\ &\implies n^2 + n + 1 = 1 \\ &\implies n^2 + 2n + 1 = n + 1 \\ &\implies (n+1)^2 = n+1. \end{aligned}$$

Ainsi, si P_n est vraie, alors P_{n+1} est vraie.

— Par récurrence, la propriété P_n est vraie pour tout $n \in \mathbb{N}$.

Proposition 1.4: Récurrence d'ordre p

Soit $(P(n))_{\substack{n\in\mathbb{N}\\ n\geq n_0}}$ une famille de propositions. On suppose que

(1) $P(n_0), P(n_0+1), \ldots, P(n_0+p-1)$ sont vraies (initialisation) ;

(2) $\forall n \geq n_0$, $P(n)$ et $P(n+1)$ et $\ldots P(n+p-1) \implies P(n+p)$ (hérédité).

Alors $P(n)$ est vraie pour tout $n \geq n_0$.

Proposition 1.5: Récurrence forte

Soit $(P(n))_{\substack{n\in\mathbb{N}\\ n\geq n_0}}$ une famille de propositions. On suppose que

(1) $P(n_0)$ est vraie.

(2) $\forall n \geq n_0, \Big(\forall p \leq n, P(p) \text{ vraie } \implies P(n+1)\Big)$.

Alors $P(n)$ est vraie pour tout $n \geq n_0$.

Exemple 1.6: Théorème de Zermelo, 1912

Au jeu d'échecs, l'une des trois propositions ci-dessous est vraie.
- Le joueur blanc possède une stratégie gagnante.
- Le joueur noir possède une stratégie gagnante.
- Les deux joueurs ont une stratégie qui leur garantissent au moins la partie nulle.

2. Divisibilité

Définition 2.1

Soient p et n deux entiers relatifs. On dit que p *divise* n, ou que p *est un diviseur de* n, ou que n *est un multiple de* p s'il existe $k \in \mathbb{Z}$ tel que $n = kp$. On note cette situation $p|n$.

Exemple 2.2

Pour tout $n \in \mathbb{Z}$, on a $1|n$ et $n|0$.

Proposition 2.3

Soient a, b, c trois entiers.

(1) $a|a$.

(2) Si $a|b$ et $b|a$ alors $a = \pm b$.

(3) Si $a|b$ et $b|c$ alors $a|c$.

Proposition 2.4

Soient a, b, c trois entiers. Si $a|b$ et $a|c$, alors pour tous $u, v \in \mathbb{Z}$, $a|(ub + vc)$.

3. Division euclidienne

Proposition 3.1

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tels que

(1) $a = bq + r$;

(2) $0 \leq b < r$.

Les entiers q et r sont respectivement appelés *quotient* et *reste* dans la division euclidienne de a par b.

Théorème 3.2

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases}$$

Proposition 3.3

Soient $a, b \in \mathbb{N}^*$. Alors b divise a si et seulement si le reste dans la division de a par b est 0.

4. PGCD et PPCM

Définition 4.1

Soient a et b deux entiers. Le *PGCD* (plus grand commun diviseur) de a et b est le plus grand de tous les entiers qui divisent à la fois a et b. On le note $PGCD(a, b)$ ou $a \wedge b$.

Remarque 4.2

On note $\mathscr{D}$ l'ensemble de tous les diviseurs communs à a et b. La partie $\mathscr{D}$ est majorée par a, et non vide puisque $1 \in \mathscr{D}$, donc $\mathscr{D}$ admet un plus grand élément d. Ceci prouve que $a \wedge b$ existe.

Proposition 4.3

Soient a et b deux entiers et c un diviseur commun à a et b. Alors c divise $a \wedge b$.

Proposition 4.4: Algorithme d'Euclide

Soient a et b deux entiers. On note r le reste de la division de a par b. Alors $a \wedge b = b \wedge r$.

Remarque 4.5

Comme $r < b$, le calcul de $b \wedge r$ est plus aisé que $a \wedge b$. De plus, on peut itérer cette formule, obtenant des entiers de plus en plus petits, jusqu'à éventuellement obtenir un reste nul, auquel cas le calcul du PGCD est particulièrement aisé !

Définition 4.6

Soient a et b deux entiers. Le *PPCM de a et b* (Plus Petit Commun Multiple) est le plus petit entier qui soit à la fois un multiple de a et un multiple de b. On le note $a \vee b$.

Proposition 4.7

Soient a et b deux entiers et c un multiple commun à a et b. Alors c est un multiple de $a \vee b$.

5. Entiers premiers entre eux

Définition 5.1

On dit que deux entiers a et b sont *premiers entre eux* si leur PGCD vaut 1.

Théorème 5.2: Bézout

Soient a et b deux entiers. Alors a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Corollaire 5.3

Soient a et b deux entiers et d leur PGCD. Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$.

Théorème 5.4: Gauss

Soient a, b, c trois entiers tels que $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Corollaire 5.5

Soient a, b, c trois entiers tels que $a \wedge b = 1$, $a|c$ et $b|c$. Alors $ab|c$.

6. Décomposition en facteurs premiers

Définition 6.1

Un entier p est dit *premier* si ses seuls diviseurs sont ± 1 et $\pm p$.

Exemple 6.2: Crible d'Eratosthène

Pour déterminer tous les entiers positifs premiers inférieurs à 100 par exemple, on peut procéder de la façon suivante.

On commence par écrire tous les entiers de 2 à 100. Le premier de ces entiers est 2, il est premier. Les autres entiers pairs ne peuvent pas être premiers donc on les supprime du tableau. Le premier entier devient alors 3 qui est donc premier, on supprime ensuite tous les autres multiples de 3. Le premier entier restant est alors 5 qui doit donc être premier, et on supprime alors tous les multiples de 5, et ainsi de suite.

Crible d'Ératosthène (10×10)

Étape 1: Entiers à partir de $2 \ldots 100$

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Étape 2: On supprime les multiples de **2**

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Étape 3: On supprime les multiples de **3**

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Étape 4: On supprime les multiples de **5**

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Étape 5: On supprime les multiples de **7**

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Étape 6: Les entiers restants sont premiers.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème 6.3: Théorème Fondamental de l'arithmétique

Soit n un entier supérieur ou égal à 2. On peut écrire n sous la forme d'un produit de nombres premiers. Cette décomposition est unique.

Notation 6.4

Pour tout $n \in \mathbb{N}^*$, on note p_n le n-ième nombre premier. Pour tout $a \in \mathbb{N}^*$, on peut alors écrire $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ où les entiers α_i peuvent être nuls, et n choisi assez grand.

Définition 6.5

Soit p un nombre premier et $n \in \mathbb{N}$ un entier supérieur ou égal à 2. La *valuation p-adique de n* est l'exposant (éventuellement nul) de p dans la décomposition en facteurs premiers de n. On note cet entier $v_p(n)$.

Proposition 6.6

Soient a et b deux entiers supérieurs ou égaux à 2. Alors a divise b si et seulement si pour tout nombre premier p, $v_p(a) \leq v_p(b)$.

Proposition 6.7

Soient a et b deux entiers, $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ leur décomposition en produit de facteurs premiers. Alors $a \wedge b = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$.

Proposition 6.8

Soient a et b deux entiers, $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ leur décomposition en produit de facteurs premiers. Alors $a \vee b = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$.

Corollaire 6.9

Soient a et b deux entiers. Alors $ab = (a \wedge b)(a \vee b)$.

7. Congruence

Définition 7.1

Soient $n \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z}^2$. On dit que a est *congru à b modulo n* si n divise $b - a$. Dans ce cas, on écrit $a \equiv b[n]$.

Remarque 7.2

Pour tout $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$, $(n|a \iff a \equiv 0[n])$.

Proposition 7.3

Soit $n \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z}^2$. Alors $a \equiv b[n]$ si et seulement si a et b ont même reste dans la division euclidienne par n.

Corollaire 7.4

Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. Elle a exactement n classes d'équivalence : ce sont les ensembles $k\mathbb{Z}$ pour $k \in [\![0, n-1]\!]$.

Proposition 7.5: compatibilité avec l'addition

Soient $n \in \mathbb{N}^*$, a_1, a_2, b_1, b_2 quatre entiers tels que $a_1 \equiv b_1[n]$ et $a_2 \equiv b_2[n]$. Alors $a_1 + a_2 \equiv b_1 + b_2[n]$.

Proposition 7.6: compatibilité avec la multiplication

Soient $n \in \mathbb{N}^*$, a_1, a_2, b_1, b_2 quatre entiers tels que $a_1 \equiv b_1[n]$ et $a_2 \equiv b_2[n]$. Alors $a_1 a_2 \equiv b_1 b_2[n]$.

Théorème 7.7: Petit théorème de Fermat

Soient p un nombre premier et a un entier premier avec p. Alors $a^{p-1} \equiv 1[p]$.