1 Divisibilité dans $\mathbb{Z}$. 1
1.1 Diviseurs et multiples. . . . 1
1.2 Division euclidienne. . . . 2
1.3 Congruences. . . . 3
1.4 Nombres premiers. . . . 4

2 PGCD et PPCM. 5
2.1 PGCD de deux entiers. . . . 5
2.2 Calculs effectifs : l'algorithme d'Euclide. . . . 6
2.3 PPCM de deux entiers. . . . 8
2.4 Extension à un nombre fini d'entiers. . . . 8

3 Entiers premiers entre eux. 10
3.1 Couples d'entiers premiers entre eux. . . . 10
3.2 Produit de diviseurs, diviseurs d'un produit. . . . 11
3.3 Le cas des diviseurs premiers. . . . 11
3.4 Famille d'entiers premiers entre eux. . . . 11
3.5 Inversibilité modulo n. . . . 12
3.6 Petit théorème de Fermat. . . . 13

4 Théorème fondamental de l'arithmétique et applications. 14
4.1 Le TFAr. . . . 14
4.2 Valuations p-adiques. . . . 14

Exercices 16

1 Divisibilité dans $\mathbb{Z}$.

1.1 Diviseurs et multiples.

Définition 1.

Soit $(a, b) \in \mathbb{Z}^2$. On dit que b **divise** a (on note $b \mid a$) s'il existe un entier $k \in \mathbb{Z}$ tel que $a = kb$.
Si b divise a, on dit encore que b est un **diviseur** de a ou encore que a est un **multiple** de b.

Proposition 2 (Faits immédiats).

Tous les entiers divisent 0 et 1 divise tous les entiers. Ajoutons que pour $(a, b, c) \in \mathbb{Z}^3$,

1. Si b est un diviseur de a et si $a \neq 0$, alors $|b| \leq |a|$.
2. Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$, pour tous u et v dans $\mathbb{Z}$.
   En particulier, si c divise a et b, il divise aussi $a + b$ et $a - b$.

Notation (locale).

L'ensemble des diviseurs *positifs* de a sera noté dans ce cours

$$\mathcal{D}(a) = \{b \in \mathbb{N} : b \mid a\}$$

Par exemple, on a $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$. Pour $a \in \mathbb{Z}$, il est clair que $\mathcal{D}(-a) = \mathcal{D}(a)$.

Proposition 3.

1. Si a est un entier relatif non nul, alors $\mathcal{D}(a)$ est un ensemble fini et son maximum est $|a|$.
2. $\mathcal{D}(0) = \mathbb{N}$.

Notation.

L'ensemble des multiples de a dans $\mathbb{Z}$ est noté

$$a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}.$$

On peut écrire une relation de divisibilité à l'aide des ensembles de multiples :

$$b \mid a \quad \iff \quad a\mathbb{Z} \subset b\mathbb{Z}.$$

On se souvient que, définie sur $\mathbb{N}$, divise était une relation d'ordre. Ce n'est plus le cas dans $\mathbb{Z}$.

Proposition 4.

Sur $\mathbb{Z}$, la relation *divise* est réflexive, transitive, mais pas antisymétrique. On a

$$\forall (a, b) \in \mathbb{Z}^2 \qquad (a \mid b \text{ et } b \mid a) \iff (a = b \text{ ou } a = -b).$$

Dans ce cas où $(a \mid b$ et $b \mid a)$ on dit que a et b sont **associés**. On a facilement que

$$(a = \pm b) \quad \iff \quad \mathcal{D}(a) = \mathcal{D}(b) \quad \iff \quad a\mathbb{Z} = b\mathbb{Z}.$$

1.2 Division euclidienne.

Théorème 5.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

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

Proposition 6.

Soit a et b deux entiers relatifs (b non nul).
L'entier b divise a si et seulement le reste dans la division euclidienne de a par $|b|$ est nul.

1.3 Congruences.

Définition 7.

Soit $n \in \mathbb{Z}$. On dit que deux entiers relatifs sont **congrus modulo** n, ce que l'on note $a \equiv b\ [n]$ s'il existe un entier relatif k tel que $a = b + kn$.

Proposition 8 (Propriétés des relations de congruence dans $\mathbb{Z}$).

Soit $n \in \mathbb{Z}$.

1. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ (*réflexive, symétrique et transitive*).
2. $\forall a \in \mathbb{Z} \quad n \mid a \iff a \equiv 0\ [n]$. En particulier, $n \equiv 0\ [n]$.
3. Compatibilité avec les sommes et produits

$$\forall (a, b, a', b') \in \mathbb{Z}^4 \quad \begin{cases} a \equiv b & [n] \\ a' \equiv b' & [n] \end{cases} \implies \begin{cases} a + a' \equiv b + b' & [n] \\ a \times a' \equiv b \times b' & [n]. \end{cases}$$

La compatibilité avec le produit amène, par simple récurrence,

$$\forall (a, b) \in \mathbb{Z}^2 \quad \forall \ell \in \mathbb{N} \qquad a \equiv b\ [n] \implies a^\ell \equiv b^\ell\ [n].$$

Proposition 9 (Classes de congruence).

Soit $n \in \mathbb{N}^*$.

1. Pour tout $a \in \mathbb{Z}$, il existe un unique $r \in [\![0, n-1]\!]$ tel que $a \equiv r\ [n]$.
   L'entier r est le reste de la division euclidienne de a par n.
2. Il y a exactement n classes d'équivalences pour la relation de congruence modulo n.
   Ce sont les classes de $0, 1, ...n-1$.

Exemple 10 (Multiples de 3).

— Déterminer les entiers naturels n tels que 3 divise $2^n + 1$.
— Démontrer qu'un entier naturel est un multiple de 3 si et seulement si la somme de ses chiffres (en écriture décimale) est un multiple de 3. Idem en remplaçant 3 par 9.

1.4 Nombres premiers.

Définition 11.

Un entier $p \in \mathbb{N} \setminus \{0, 1\}$ est dit **premier** si ses seuls diviseurs positifs sont 1 et p.

Exemples. 2, 3, 5, 7, 11, 13...

Exemple 12 (*Two is the oddest prime*).

Le nombre 2 est le seul entier premier et pair.

Proposition 13.

Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

Puisque tout nombre non premier possède un diviseur premier, on comprend vite que tout entier s'écrit comme un produit de nombres premiers. Ainsi, les nombres premiers sont comme les atomes de l'arithmétique : insécables, et briques élémentaires pour construire les autres nombres. Cette intuition deviendra un théorème dans la partie 4 de ce cours.

On peut affiner « quantitativement » le résultat précédent.

Proposition 14.

Pour tout entier naturel n non premier et supérieur à 2 admet un diviseur premier inférieur à $\sqrt{n}$.

Application : crible d'Eratosthène. Un nombre *non* premier inférieur à 100 a d'après ce qui précède un diviseur premier inférieur à 10. Ainsi, une fois éliminés de la grille ci-dessous tous les multiples (non triviaux) de 2, 3, 5 et 7, il ne restera que les entiers premiers inférieurs à 100.

0	1	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

Théorème 15 (d'Euclide).

Il existe une infinité de nombres premiers.

2 PGCD et PPCM.

2.1 PGCD de deux entiers.

Soient a et b deux entiers relatifs. L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ est celui de leurs diviseurs communs.
Si l'un des deux entiers a et b est non nuls, l'un des deux ensembles $\mathcal{D}(a)$ ou $\mathcal{D}(b)$ est fini, et $\mathcal{D}(a) \cap \mathcal{D}(b)$ est une partie de $\mathbb{Z}$ majorée par $\max(|a|, |b|)$.

Définition 16 (Le PGCD : un maximum pour $\leq$).

Soient a et b deux entiers relatifs.

- Si $(a, b) \neq (0, 0)$, on appelle **Plus Grand Commun Diviseur** de a et b, et on note $a \wedge b$ ou encore $\text{PGCD}(a, b)$ le plus grand entier qui divise a et b.
- Si $a = b = 0$, on pose $a \wedge b = 0$.

Remarque. Par définition, pour $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, on a

$$a \wedge b = \max\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right),$$

où le max est compris pour l'ordre naturel $\leq$ sur les entiers relatifs.

Exemple.
Calculer $\text{PGCD}(12, 28)$ en écrivant les ensembles de diviseurs (*il faudra proposer une méthode plus efficace !*)

Proposition 17 (Propriétés élémentaires du PGCD).

Soient a et b deux entiers relatifs.

1. Le PGCD de a et b est un entier naturel.
2. $a \wedge b = b \wedge a = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b)$.
3. Si b divise a et $a \in \mathbb{N}^*$ alors $a \wedge b = a$.
4. *Le cas de zéro.* Si $a \in \mathbb{N}$, alors $a \wedge 0 = a$.

Théorème 18 (Caractérisation du PGCD par une relation de Bézout).

Soient a et b deux entiers relatifs dont l'un au moins est non nul.

$$\exists (u, v) \in \mathbb{Z}^2 \quad au + bv = a \wedge b.$$

L'égalité ci-dessus est appelée une **relation de Bézout**.
Le couple (u, v) peut-être désigné comme un couple de *coefficients de Bézout*, il n'est pas unique.

$a \wedge b$ est le plus petit entier naturel non nul qui s'écrit sous la forme $au + bv$, avec $(u, v) \in \mathbb{Z}^2$.

Remarque. Lorsque $a = b = 0$, on peut aussi écrire une relation de Bézout (tout couple (u, v) convient !) mais le PGCD vaut alors 0 et l'assertion encadrée devient fausse.

Proposition 19 (Les diviser tous les deux, c'est diviser leur PGCD).

Soit $(a, b) \in \mathbb{Z}^2$. Alors

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$

En français : les diviseurs communs de a et b sont exactement les diviseurs de leur PGCD.

Corollaire 20 (Le PGCD : un maximum pour la relation $|$).

Le PGCD de deux entiers naturels a et b est le *plus grand* diviseur commun de a et b pour divise, relation d'ordre sur $\mathbb{N}$.

Plus précisément, pour a et b deux entiers naturels, on a

1. $a \wedge b \in \mathcal{D}(a) \cap \mathcal{D}(b)$
   i.e. $a \wedge b$ est un diviseur commun de a et b.
2. $\forall \delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \quad \delta \in \mathcal{D}(a \wedge b)$
   i.e. $a \wedge b$ est le plus grand des diviseurs communs positifs au sens de la relation d'ordre divise.

Proposition 21.

$$\forall (a, b) \in \mathbb{Z}^2, \quad \forall k \in \mathbb{Z}, \quad \text{PGCD}\,(ka, kb) = |k| \cdot \text{PGCD}(a, b).$$

2.2 Calculs effectifs : l'algorithme d'Euclide.

Proposition 22 (Réduction du problème).

Soit $(a, b, c, q) \in \mathbb{Z}^4$ tel que $a = bq + c$.
Alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(c)$. En particulier, $a \wedge b = b \wedge c$.

On rappelle que si $(a, b) \in \mathbb{Z}^2$, on a $a \wedge b = |a| \wedge |b|$. C'est donc sans perte de généralité qu'on présente ci-dessous l'algorithme d'Euclide pour des entiers naturels.

Théorème 23 (Algorithme d'Euclide).

Soit $(a, b) \in \mathbb{N}^2$, $b \neq 0$.

- On note $r_0 = a$ et $r_1 = b$.
- Tant qu'il existe $i \in \mathbb{N}^*$ tel que r_i est non nul, on définit r_{i+1} comme le reste dans la division euclidienne de r_{i-1} par r_i.

Cet algorithme termine : il existe $p \in \mathbb{N}^*$ tel que $r_1, \ldots, r_p$ sont non nuls et $r_{p+1} = 0$. Alors,

$$\boxed{a \wedge b = r_p}.$$

Une exécution ressemble à ça :

$$\begin{aligned} \overbrace{r_0}^{=a} &= \overbrace{r_1}^{=b} q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\dots \\ r_{p-2} &= r_{p-1} q_p + \boxed{r_p} \longleftarrow a \wedge b \\ r_{p-1} &= r_p q_{p+1} + 0 \end{aligned}$$

Algorithme 24 (Algorithme d'Euclide).

En Python :

```
def PGCD(a,b):
    while b!=0:
        a,b=b,a%b    # a%b : reste dans la div.eucl. de a par b
    return a
```

En OCaml :

```
let rec pgcd a b =
    if b = 0 then a
    else pgcd b (a mod b)    (* (a mod b) : reste dans la div.eucl. de a par b *)
```

Exemple 25 (Éxécution de l'algorithme d'Euclide).

Calculer le PGCD de 342 et 95 puis donner $\mathcal{D}(342) \cap \mathcal{D}(95)$.

Méthode (Algorithme d'Euclide étendu).

Pour $a, b \in \mathbb{N}$ avec $b \neq 0$, on note $r_0, \dots, r_p$ la suite des restes écrits en exécutant l'algorithme d'Euclide, avec $p \in \mathbb{N}^*$ le rang du dernier reste non nul. On rappelle : $r_0 = a$, $r_1 = b$ et $r_p = a \wedge b$.

Pour tout $i \in [\![1, p]\!]$

$$\exists (u_i, v_i) \in \mathbb{Z}^2 \quad a u_i + b v_i = r_i.$$

C'est vrai en particulier pour $i = p$: (u_p, v_p) est un couple de coefficients de Bézout pour r_p, le PGCD de a et b.

Les coefficients (u_i, v_i) se calculent de proche en proche, en *remontant* l'algorithme de Bézout (voir exemple ci-après).

Exemple 26 (Éxécution de l'algorithme d'Euclide étendu).

Calculer $118 \wedge 24$ et donner une relation de Bézout pour ce PGCD.

2.3 PPCM de deux entiers.

Soient a et b deux entiers relatifs. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est celui de leurs multiples communs.
Si a et b sont non nuls, son intersection avec $\mathbb{N}^*$ est non vide puisqu'elle contient au moins $|a| \cdot |b|$.

Définition 27 (Le PPCM : un minimum pour $\leq$).

Soient a et b deux entiers relatifs.

- Si a et b sont non nuls, on appelle **Plus Petit Commun Multiple** de a et b, noté $a \vee b$, ou encore $\mathrm{PPCM}(a, b)$, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.
- Si a ou b vaut 0, on pose $a \vee b = 0$.

Par exemple, le PPCM de 12 et 16 vaut 48. Si $a \in \mathbb{Z}$, alors $a \wedge 1 = |a|$.

Proposition 28.

Pour tout couple d'entiers relatifs $(a, b) \in \mathbb{Z}^2$,

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

Corollaire 29 (Le PPCM : un minimum pour la relation $|$).

Pour deux entiers naturels a et b non nuls, le PPCM est le *plus petit* diviseur commun de a et b pour divise, relation d'ordre sur $\mathbb{N}$.

Plus précisément, pour a et b deux entiers naturels non nuls, on a

1. $a \mid a \vee b$ et $b \mid a \vee b$, *(le PPCM est un multiple commun)*
2. $\forall \mu \in \mathbb{Z} \quad (a \mid \mu \text{ et } b \mid \mu) \Longrightarrow a \vee b \mid \mu$, *(tout multiple commun est multiple du PPCM).*

Proposition 30.

$$\forall (a, b) \in \mathbb{Z}^2 \quad \mathrm{PGCD}(a, b) \times \mathrm{PPCM}(a, b) = |a \times b|.$$

2.4 Extension à un nombre fini d'entiers.

Définition 31.

Soit $n \in \mathbb{N}^*$ et $(a_1, \ldots, a_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$.
Le plus grand diviseur positif commun à $a_1, \ldots, a_n$ est appelé leur **PGCD** et noté

$$a_1 \wedge \cdots \wedge a_n.$$

On convient que le PGCD de n entiers nuls vaut 0.

Les deux propositions ci-après se démontrent comme dans le cas $n = 2$ traité plus haut.

Proposition 32 (Relation de Bézout).

Soit $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \dots, 0)\}$.

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad a_1 \wedge \cdots \wedge a_n = a_1 u_1 + \cdots + a_n u_n.$$

Une telle égalité est appelée **relation de Bézout**.

$a_1 \wedge \cdots \wedge a_n$ est le plus petit entier strictement positif s'écrivant comme une combinaisons linéaire de Bézout des entiers $a_1, \dots, a_n$.

Proposition 33 (Les diviser tous, c'est diviser leur PGCD).

Soit $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n$. On a

$$\bigcap_{k=1}^{n} \mathcal{D}(a_k) = \mathcal{D}(a_1 \wedge \cdots \wedge a_n).$$

Lemme 34 (Associativité du PGCD).

Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_{n+1}$ des entiers relatifs. Alors,

$$a_1 \wedge \cdots \wedge a_n \wedge a_{n+1} = (a_1 \wedge \cdots \wedge a_n) \wedge a_{n+1}.$$

Preuve. Notons

$$d_n = a_1 \wedge \cdots \wedge a_n, \qquad d_{n+1} = a_1 \wedge \cdots \wedge a_n \wedge a_{n+1} \quad \text{et} \quad d'_{n+1} = d_n \wedge a_{n+1}.$$

D'une part, d'_{n+1} divise d_n donc divise $a_1, \dots, a_n$. Comme il divise aussi a_{n+1}, c'est un diviseur commun à $a_1, \dots, a_{n+1}$: d'_{n+1} divise leur PGCD d_{n+1}.

D'autre part, d_{n+1} divise $a_1, \dots, a_n$ donc divise leur PGCD d_n. Il divise aussi a_{n+1} donc divise $d_n \wedge a_{n+1}$, c'est-à-dire divise d'_{n+1}.

Ceci amène que d_{n+1} et d'_{n+1} sont associés, et donc égaux car positifs.

□

Proposition 35.

$$\forall (a_1, \dots, a_n) \in \mathbb{Z}^n, \quad \forall k \in \mathbb{Z}, \quad \text{PGCD}\,(ka_1, \dots, ka_n) = |k| \cdot \text{PGCD}(a_1 \dots, a_n).$$

Preuve. Récurrence sur n en utilisant l'associativité du PGCD. □

3 Entiers premiers entre eux.

3.1 Couples d'entiers premiers entre eux.

Définition 36.

On dit que deux entiers sont **premiers entre eux** si leur PGCD est égal à 1.

Ainsi, deux entiers sont premiers entre eux si et seulement leurs seuls diviseurs communs sont 1 et -1.
Si deux entiers sont premiers entre eux, au moins l'un d'entre eux est non nul.

On remarquera que la notion d'entiers *premiers entre eux* est définie sans recours aux *nombres premiers*.

Exemple. Deux entiers consécutifs sont toujours premiers entre eux.

Proposition 37.

Deux entiers naturels non nuls a et b sont premiers entre eux si et seulement si $a \vee b = |ab|$.

Proposition 38 (se ramener à deux entiers premiers entre eux).

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $d = a \wedge b$.
Si a' et b' sont les deux entiers relatifs tels que $a = da'$ et $b = db'$, alors $a' \wedge b' = 1$.

Soit $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$. Notons $d = p \wedge q$. Il existe $(p', q') \in \mathbb{Z} \times \mathbb{Z}^*$ tels que $p = dp'$, $q = dq'$ et $p' \wedge q' = 1$. On a

$$\frac{p}{q} = \frac{dp'}{dq'} = \frac{p'}{q'}.$$

Puisque p' et q' sont sans facteur commun non trivial, on dit que l'écriture $\dfrac{p'}{q'}$ est **irréductible**.

Théorème 39 (de Bézout).

$$\forall (a, b) \in \mathbb{Z}^2 \qquad a \wedge b = 1 \quad \iff \quad \exists (u, v) \in \mathbb{Z}^2 \quad au + bv = 1.$$

Corollaire 40.

Soit $(a, b, c) \in \mathbb{Z}^3$.

1. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.
2. Plus généralement, si a est premier avec chacun des m entiers $b_1, \ldots, b_m$, où $m \in \mathbb{N}^*$, alors il est premier avec leur produit $b_1 \cdots b_m$.
3. Si $a \wedge b = 1$, alors pour tout $(n, p) \in \mathbb{N}^2$, $a^n \wedge b^p = 1$.

3.2 Produit de diviseurs, diviseurs d'un produit.

Remarque naïve : 4 et 6 divisent 12 mais 4×6 ne divise pas 12.

Proposition 41 (Produit de diviseurs premiers entre eux).

$$\forall (a_1, a_2, b) \in \mathbb{Z}^3 \qquad \begin{cases} a_1 \mid b \text{ et } a_2 \mid b \\ a_1 \wedge a_2 = 1 \end{cases} \implies a_1 a_2 \mid b.$$

Remarque naïve : 4 divise 2×6 mais 4 ne divise ni 2, ni 6...

Théorème 42 (Lemme de Gauss).

$$\forall (a, b, c) \in \mathbb{Z}^3 \qquad \begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c.$$

3.3 Le cas des diviseurs premiers.

Proposition 43.

Deux entiers relatifs sont premiers entre eux si et seulement si ils n'admettent aucun nombre premier comme diviseur commun.

Proposition 44 (Deux entiers, dont l'un est premier).

Si a est un entier et p un nombre premier, alors p divise a ou p est premier avec a.

Proposition 45 (quand un nombre premier divise un produit).

Soit $(a, b) \in \mathbb{Z}^2$ et p un nombre premier.

1. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (lemme d'Euclide).
2. Plus généralement, si p divise un produit d'entiers, alors p divise un des facteurs.

3.4 Famille d'entiers premiers entre eux.

Dans ce paragraphe, n est un entier naturel supérieur à 2.

Définition 46.

Des entiers relatifs $a_1, \ldots, a_n$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD est égal à 1, ou de manière équivalente si 1 et -1 sont les seuls diviseurs communs.

Les entiers $a_1, \dots, a_n$ sont **deux à deux premiers entre eux** si

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \implies a_i \wedge a_j = 1.$$

Exemple 47 (*dans leur ensemble* VS *deux à deux*).

Justifier que si n entiers sont premiers entre eux deux à deux, ils le sont dans leur ensemble.
Justifier que la réciproque est fausse en général.

Proposition 48 (Théorème de Bezout généralisé).

Soit $(a_1, \dots, a_n) \in \mathbb{Z}^n$

$a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble $\iff$ $\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad \sum_{i=1}^{n} a_i u_i = 1.$

Proposition 49 (Produit de diviseurs deux à deux premiers entre eux).

Soient n entiers relatifs $a_1, a_2, \dots, a_n$ et un entier b.

Si tous les a_i divisent b et si les a_i sont deux à deux premiers entre eux,
alors le produit $a_1 \cdots a_n$ divise b.

3.5 Inversibilité modulo n.

Proposition 50 (Inversibilité modulo n).

Soit $n \in \mathbb{N}^*$, et a un entier relatif premier avec n.
Il existe un entier relatif b tel que $ab \equiv 1\ [n]$ (la réciproque étant vraie).
Pour tous entiers x et y, on a

$$ax \equiv y\ [n] \quad \iff \quad x \equiv by\ [n].$$

Preuve. Supposons que a et n sont premiers entre eux. Le théorème de Bézout donne alors l'existence d'un couple (u,v) d'entiers relatifs tels que $au + nv = 1$. Posons $\boxed{b = u}$ et passons modulo n : on obtient

$$ab + 0v \equiv 1\ [n] \quad \text{i.e.} \quad ab \equiv 1\ [n]$$

ce qui montre que b est un *inverse* de a modulo n. Pour x et y dans $\mathbb{Z}$, on a

$$ax \equiv y\ [n] \quad \iff \quad abx \equiv by\ [n]$$

(on multiplie par b dans le sens direct, et par a dans l'autre sens). Puisque $ab \equiv 1[n]$, on a bien le résultat. □

Exemple 51.

Résoudre l'équation $7x \equiv 11\ [31]$.

Corollaire 52.

Soit $n \in \mathbb{N}^*$, ainsi que deux entiers relatifs a et y.
L'équation $ax \equiv y\ [n]$ possède une solution dans $\mathbb{Z}$ si et seulement si $a \wedge n$ divise y.
Dans le cas où une solution existe, elle est unique modulo $\frac{n}{a \wedge n}$.

Preuve. Les entiers relatifs a et y sont fixés ainsi que $n \in \mathbb{N}^*$.
• Supposons qu'il existe $x \in \mathbb{Z}$ tel que $ax \equiv y[n]$. Alors, il existe $k \in \mathbb{Z}$ tel que $y = ax + kn$.
Puisque $a \wedge n$ divise a et n, il divise y.
• Supposons réciproquement que $a \wedge n$ divise y. Notons alors $d = a \wedge n$; il existe a' et n' premiers entre eux tels que $a = da'$, $n = dn'$ et $y = dy'$. Pour $x \in \mathbb{Z}$, on a

$$ax \equiv y[n] \iff da'x \equiv dy'[dn'] \iff a'x \equiv y'[n']$$

On a pu simplifier par d : puisque n n'est pas nul, d ne l'est pas non plus.
Or, a' et n' sont premiers entre eux : il existe b' tel que $a'b' \equiv 1[n']$ et l'équation $a'x \equiv y'[n']$ possède by' comme unique solution modulo n', c'est-à-dire modulo $\frac{n}{a \wedge n}$. □

3.6 Petit théorème de Fermat.

Proposition 53.

Soit p un nombre premier.

1. Pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
2. $\forall (a,b) \in \mathbb{Z}^2 \quad (a+b)^p \equiv a^p + b^p\ [p]$.

Théorème 54 (Petit théorème de Fermat).

Soit n un entier relatif et p un nombre premier. On a $\boxed{n^p \equiv n\ [p]}$.

Si de surcroît n n'est pas un multiple de p, alors $n^{p-1} \equiv 1\ [p]$.

Exemple 55 (Plus petit nombre de Carmichael).

1. Vérifier que
$$561 \equiv 1\ [2], \qquad 561 \equiv 1\ [10], \qquad 561 \equiv 1\ [16].$$
2. Démontrer que pour tout entier n,
$$n^{561} \equiv n\ [3], \qquad n^{561} \equiv n\ [11], \qquad n^{561} \equiv n\ [17].$$
3. Démontrer que pour tout entier relatif n, on a $n^{561} \equiv n\ [561]$.
4. *Le petit théorème de Fermat n'est pas un critère de primalité.* Expliquer.

4 Théorème fondamental de l'arithmétique et applications.

4.1 Le TFAr.

Théorème 56 (Théorème fondamental de l'arithmétique).

Soit n est un entier supérieur à 2. Il existe un entier naturel r non nul et r nombres premiers $p_1 < p_2 < \cdots < p_r$, ainsi que des entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$ tels que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Cette décomposition de n en facteurs premiers (ou décomposition *primaire*) est unique.

Exemple. La décomposition primaire de trente six milliards (36×10^9) est $2^{11}\ 3^2\ 5^9$.

Remarques. Assouplissement des notations.

1. Soit $\{p_1, \ldots, p_r\}$ les nombres premiers intervenant dans la décomposition en facteurs premiers d'un entier n. Considérons $\{q_1, \ldots, q_s\}$ une famille de nombres premiers qui contient tous les p_i.
   Alors, on peut écrire n sous la forme
   $$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$
   Il suffit en effet d'autoriser les β_i à valoir 0 quand q_i ne figure pas dans la décomposition primaire de n.
2. Si a et b sont deux entiers et $\{p_1, \ldots, p_r\}$ la famille des nombres premiers intervenant dans la décomposition primaire de a *ou* dans celle de b. On peut décomposer a et b sur cette famille *commune* :
   $$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$
   avec $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ des entiers naturels *éventuellement nuls*.
3. La même idée permet de décomposer 1 sur n'importe quelle famille de nombres premiers $\{p_1, \ldots, p_r\}$:
   $$1 = p_1^0 p_2^0 \cdots p_r^0.$$

4.2 Valuations p-adiques.

Définition 57.

Soit p un nombre premier et n un entier naturel non nul.
On appelle **valuation p-adique** de n, notée $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers (cet exposant valant 0 si p ne figure pas dans la décomposition).

Par exemple, si $n = 3^{15} \cdot 7^3 \cdot 11$, alors $v_3(n) = 15$, $v_7(n) = 3$ et $v_{11}(n) = 1$.
De plus, pour tout nombre premier $p \notin \{3, 7, 11\}$, $v_p(n) = 0$.

Proposition 58.

Soit p un nombre premier.

1. $\forall (m, n) \in (\mathbb{N}^*)^2 \quad v_p(mn) = v_p(m) + v_p(n)$.
2. $\forall n \in \mathbb{N}^* \ \forall k \in \mathbb{N} \quad v_p(n^k) = k v_p(n)$.

Exemple 59.

Soit n un entier supérieur à 2. Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est le carré d'un entier.

Proposition 60.

Soient m et n deux entiers naturels non nuls,

$$m \text{ divise } n \quad \text{si et seulement si} \quad \text{pour tout nombre premier } p,\ v_p(m) \leq v_p(n).$$

Théorème 61 (Description des diviseurs d'un entier).

Soit n un entier naturel supérieur ou égal à 2, s'écrivant

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Ses diviseurs positifs sont exactement les entiers de la forme

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \qquad \text{avec } \forall i \in [\![1, r]\!]\ 0 \leq \beta_i \leq \alpha_i.$$

Exemple 62 (Un cas particulier important).

Soit p un nombre premier et α un entier naturel non nul. Quels sont les diviseurs de p^α ?

Exemple 63.

Combien de diviseurs possède le nombre trente six milliards ?

Proposition 64 (Décomposition primaire du PGCD, du PPCM).

Soient a et b deux entiers naturels non nuls, dont une décomposition sur une même famille de nombres premiers $p_1 < \cdots < p_r$ est

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

où les α_i et β_i sont des entiers naturels éventuellement nuls. On a alors

$$a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}, \quad \text{et} \quad a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

De manière équivalente, pour tout nombre premier p,

$$v_p(a \wedge b) = \min\left(v_p(a), v_p(b)\right), \quad \text{et} \quad v_p(a \vee b) = \max\left(v_p(a), v_p(b)\right).$$

Exercices

Divisibilité

18.1 **[♦◇◇]** Soit $n \in \mathbb{N}^*$. Déterminer le reste dans la division euclidienne de $\sum_{k=1}^{n} k$ par n.

18.2 **[♦◇◇]** Soit $n \in \mathbb{N}$. Que vaut le PGCD de $3n+1$ et de $2n$?

18.3 **[♦♦◇]** Soient deux entiers relatifs a et b tels que $a^2 \mid b^2$. Montrer que $a \mid b$.

18.4 **[♦◇◇]** Soient a et b deux entiers strictement positifs et premiers entre eux.
Montrer que $\dfrac{\ln(a)}{\ln(b)}$ est irrationnel.

18.5 **[♦♦◇]** Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

1. Montrer que a et b sont premiers entre eux si et seulement si $a+b$ et ab sont premiers entre eux.
2. Simplifier $(a+b) \wedge (a \vee b)$.

18.6 **[♦♦♦]** Soient $(n,p,q) \in (\mathbb{N}^*)^3$ tel que $n \geq 2$.

1. On note r le reste de la division euclidienne de p par q.
   Montrer que $n^r - 1$ est le reste de la division euclidienne de $n^p - 1$ par $n^q - 1$.
2. En déduire que
$$(n^p - 1) \wedge (n^q - 1) = n^{p \wedge q} - 1.$$

18.7 **[♦♦◇]** Soit $(q_1, q_2) \in \mathbb{Q}^2$.
Démontrer qu'il existe trois entiers relatifs a, b, c premiers entre eux dans leur ensemble tels que
$$q_1 = \frac{a}{c} \quad \text{et} \quad q_2 = \frac{b}{c}.$$

Nombres premiers et théorème fondamental.

18.8 **[♦◇◇]** Trouver un entier dont le produit des diviseurs vaut $2^{60}3^{75}$.

18.9 **[♦♦◇]** Soit $n \geq 1$ un entier et p un nombre premier. Soit N tel que $p^N \geq n$.

1. Soit $q \in \mathbb{N}^*$. Combien y-a-t-il de multiples de q dans $[\![1, n]\!]$?
2. Soit $k \in \mathbb{N}^*$ et $A_k = \{m \in [\![1,n]\!] \mid v_p(m) = k\}$. Calculer le cardinal de A_k.
3. En déduire que
$$v_p(n!) = \sum_{k=1}^{N} \left\lfloor \frac{n}{p^k} \right\rfloor.$$
4. Déterminer par combien de zéros se termine l'écriture décimale de 1000!.

18.10 **[♦♦♢]** [Nombres de Fermat]

1. Soit $(a,m) \in \mathbb{N}^2$. On suppose que a^m+1 est premier et que $a \geq 2$ et $m \neq 0$.
   Montrer que a est pair et que m est une puissance de 2.
2. Pour $n \in \mathbb{N}$, on note $F_n = 2^{2^n}+1$.
   Culture : pour tout $i \in [\![0,4]\!]$, les nombres F_i sont premiers.
   Ceci a fait conjecturer à Fermat que tous les F_n le sont. C'est faux : F_5 est composé.
   (a) Montrer que pour tout $n \in \mathbb{N}^*$, $F_n = 2 + \prod_{k=0}^{n-1} F_k$
   (b) En déduire que si n et m sont deux entiers naturels distincts, F_n et F_m sont premiers entre eux.
   (c) Déduire de la question précédente que l'ensemble des nombres premiers est infini.

Congruences.

18.11 **[♦♢♢]** Soit $n \in \mathbb{N}^*$ et a, b deux entiers relatifs tels que $a \equiv b\ [n]$. Démontrer que

$$a^n \equiv b^n\ [n^2].$$

18.12 **[♦♦♢]** Un nombre palindrome est un nombre qui se lit indifféremment de gauche à droite ou de droite à gauche. Par exemple, 2002 et 12321 sont des nombres palindromes. Prouver qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11

18.13 **[♦♦♢]** Déterminer les entiers relatifs n tels que $n^{13} \equiv n[42]$.

18.14 **[♦♦♢]** [Banque oraux CCINP (numéro 94)]
On considère le système (S) : $\begin{cases} x \equiv 6 \ [17] \\ x \equiv 4 \ [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

1. Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
2. Résoudre alors dans $\mathbb{Z}$ le système (S).

18.15 **[♦♦♦]** [Progression arithmétique]

1. Montrer que tout entier naturel congru à 3 modulo 4 admet un diviseur premier congru à 3 modulo 4.
2. Démontrer qu'il existe une infinité de nombres premiers de la forme $4n+3$ avec $n \in \mathbb{N}$.

Le théorème de la progression arithmétique (Dirichlet, 1838) énonce que si a et b sont deux entiers naturels premiers entre eux, il existe une infinité de nombres premiers de la forme $an+b$ avec n entier.
