Chapitre 9

Arithmétique

Plan du chapitre

1 Relation de divisibilité

Définition 9.1 (Relation "divise")

On définit sur $\mathbb{Z}$ une relation binaire, notée $|$, de la manière suivante : pour tous $a, b \in \mathbb{Z}$,

$$b \mid a \iff \exists k \in \mathbb{Z} \quad a = bk$$

On dit alors que b divise a, ou encore que a est un multiple de b.
On note $\mathcal{D}(a)$ l'ensemble des entiers qui divisent a.

L'ensemble $b\mathbb{Z} := \{bk \mid k \in \mathbb{Z}\}$ correspond à l'ensemble des multiples de b.

Exemple 1. Soit $a \in \mathbb{Z}$.

1. $\mathcal{D}(0) = \mathbb{Z}$ car ...
2. $\{1,-1\} \subset \mathcal{D}(a)$ car ...
3. Si $a \neq 0$, alors $0 \notin \mathcal{D}(a)$. Par contre, $0 \in \mathcal{D}(0)$.
4. Si $a \neq 0$, alors $\mathcal{D}(a) \subset [\![-a,a]\!]$
5. $\mathcal{D}(a) = \mathcal{D}(-a)$.
6. $\mathcal{D}(1) = \mathcal{D}(-1) = \{-1,1\}$.

Remarque. La relation "divise" est réflexive et transitive. Toutefois :

- Ce n'est pas une relation d'équivalence car elle n'est pas symétrique : $1 \mid 2$ mais $2 \nmid 1$.
- Ce n'est pas une relation d'ordre car elle n'est pas antisymétrique : $1 \mid (-1)$ et $(-1) \mid 1$ mais $1 \neq -1$.

En revanche, si on restreint la relation "divise" à $\mathbb{N}$, on obtient une relation d'ordre (cf DS n°3).

Proposition 9.2

Soit $a,b \in \mathbb{Z}$. Alors

$$(a \mid b \quad \text{et} \quad b \mid a) \iff |a| = |b|$$

Dans ce cas, les entiers a et b sont dits associés.

On prendra garde au fait que $b \mid a$ n'entraine pas toujours $b \leq a$: par exemple $1 \mid 0$ mais $1 > 0$.

Proposition 9.3

Soit $a,b,c,d \in \mathbb{Z}$.

1. $(d \mid a \quad \text{et} \quad d \mid b) \implies \forall u,v \in \mathbb{Z} \quad d \mid (au+bv)$
2. $a \mid b \implies a \mid bc$
3. $(a \mid b \quad \text{et} \quad c \mid d) \implies ac \mid bd$
4. En particulier, $a \mid b \implies ac \mid bc$
5. Si $c \neq 0$, alors $ac \mid bc \implies a \mid b$

Démonstration. On ne montre que la première propriété.

□

2 Division euclidienne dans $\mathbb{Z}$

Lemme 9.4 (Hors-Programme)

Soit (x_n) une suite à valeurs dans $\mathbb{Z}$. Alors (x_n) est convergente si et seulement si (x_n) est stationnaire.

Démonstration. Si (x_n) est stationnaire, elle est constante à partir d'un certain rang, donc est évidemment convergente. Réciproquement, supposons que (x_n) est convergente et montrons qu'elle est stationnaire. Notons $\ell = \lim x_n \in \mathbb{R}$. Par définition, en prenant $\varepsilon = \frac{1}{3}$, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N \qquad |x_n - \ell| \leq \frac{1}{3} = \varepsilon$$

et donc pour tout $n \geq N$

$$x_n \in \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$$

Posons $J := \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$. J contient un entier car $x_N \in \mathbb{Z} \cap J$. Or, J est de longueur $\frac{2}{3}$ donc J contient au plus un entier. Ainsi, $J \cap \mathbb{Z} = \{x_N\}$. Or, pour tout $n \geq N$, $x_n \in \mathbb{Z} \cap J$, si bien que $x_n = x_N$. Ainsi, x_n est stationnaire (et en particulier $\ell = x_N$). □

Proposition 9.5 (Hors-Programme)

Toute partie de $\mathbb{Z}$ non vide et majorée admet un maximum.

Démonstration. Soit $X \subset \mathbb{Z}$ une partie non vide et majorée. Comme $X \subset \mathbb{R}$, X admet une borne supérieure, qu'on note s. Montrons que $s \in X$. Par caractérisation de la borne supérieure, il existe une suite $(x_n) \in X^{\mathbb{N}}$ telle que $x_n \to s$. En particulier, on a pour tout $n \in \mathbb{N}$, $x_n \in X \subset \mathbb{Z}$. Par le lemme 9.4, on en déduit que (x_n) est stationnaire. Ainsi, $x_n = s$ à partir d'un certain rang. On en déduit que $s \in X$. □

Théorème 9.6 (Division euclidienne)

Soit $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors il existe un *unique* couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < |b|$$

- q est appelé le quotient de la division euclidienne de a par b.
- r est appelé le reste de la division euclidienne de a par b.

Démonstration.

□

Exemple 2. Faire la division euclidienne de 53 par 3.

Proposition 9.7

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.
$b \mid a$ si et seulement si le reste de la division euclidienne de a par b est nul.

3 PGCD

3.1 PGCD dans $\mathbb{N}$

Pour tout $c \in \mathbb{Z}^*$, on montre facilement que l'ensemble $\mathcal{D}(c)$ est majoré par $|c|$.
Soit $a,b \in \mathbb{N}$ et $X := \mathcal{D}(a) \cap \mathcal{D}(b)$. X est donc l'ensemble des diviseurs communs à a et b. Si $(a,b) \neq (0,0)$, alors $\mathcal{D}(a)$ ou $\mathcal{D}(b)$ est majoré, donc X aussi. Ainsi, X est une partie de $\mathbb{Z}$ majorée et non vide (car $1 \in X$). Alors, par la Proposition 9.5, X admet un maximum. Cela justifie la définition suivante :

Définition 9.8 (PGCD)

Soit $a,b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$. Le PGCD de a et b est le plus grand des diviseurs communs à a et b. Il est noté $a \wedge b$.
Autrement dit, $a \wedge b := \max(\mathcal{D}(a) \cap \mathcal{D}(b))$.

Attention à ne pas écrire : ~~$0 \wedge 0$~~ en effet, $\mathcal{D}(0) \cap \mathcal{D}(0) = \mathbb{Z}$ n'a pas de maximum.

Exemple 3. $18 \wedge 12 = 6$ et $4 \wedge 7 = 1$

Exemple 4. Soit $a,b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$.

1. $a \wedge b \geq 1$
2. $a \wedge 1 = 1$
3. Si $a \neq 0$, $a \wedge 0 = a$
4. $a \wedge b = b \wedge a$
5. $a \wedge b = b \iff b \mid a$
6. $\forall c \in \mathbb{N}^* \quad (ca) \wedge (cb) = c(a \wedge b)$

Lemme 9.9

Soit $a,b \in \mathbb{N}$ avec $b \neq 0$. Soit $q,r \in \mathbb{N}$ tels que $a = bq + r$. Alors

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

donc en particulier $a \wedge b = b \wedge r$.

Démonstration. On raisonne par double inclusion. Soit $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$. Comme $d \mid a$ et $d \mid b$, on a $d \mid (a - bq)$, c'est-à-dire $d \mid r$. Ainsi $d \in \mathcal{D}(b) \cap \mathcal{D}(r)$.

Réciproquement, si $d \mid b$ et $d \mid r$, alors $d \mid (bq + r)$, d'où $d \mid a$. On en déduit que $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$.

Enfin, comme $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$, les maxima de ces deux ensembles sont égaux, donc $a \wedge b = b \wedge r$. □

Théorème 9.10

Soit $a,b \in \mathbb{N}$ avec $(a,b) \neq 0$. On pose $d = a \wedge b$. Alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d)$, càd

$$\forall n \in \mathbb{N} \quad (n \mid a \quad \text{et} \quad n \mid b) \iff n \mid d$$

Remarque. L'élément $d = a \wedge b$ est le seul entier naturel tel que $\mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$, ou encore le seul qui vérifie l'équivalence ci-dessus. En effet, si $d, d' \in \mathbb{N}$ vérifient cette équivalence, on en déduit (en prenant $n = d'$) que $d' \mid d$, et de même que $d \mid d'$, donc $d = d'$ (puisque $d, d' \in \mathbb{N}$).

Démonstration. Si $b = 0$, alors $d = a \wedge 0 = a$. On a alors trivialement que $\mathcal{D}(d) = \mathcal{D}(a) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
Montrons par récurrence forte sur $b \in \mathbb{N}^*$ que l'assertion suivante est vraie :

$$H_b : \quad \forall a \in \mathbb{N} \quad \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$$

- Initialisation : Si $b = 1$, alors $a \wedge b = 1$ et $\mathcal{D}(b) = \{-1, 1\} \subset \mathcal{D}(a)$. Ainsi,

  $$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) = \mathcal{D}(1) = \mathcal{D}(a \wedge b)$$

  Donc H_1 est vraie.

- Hérédité : Soit $b_0 \in \mathbb{N}$ tel que $b_0 \geq 2$. On suppose que H_b est vraie pour tout $b < b_0$. Montrons que H_{b_0} est vraie. Soit $a \in \mathbb{N}$. Montrons que $\mathcal{D}(a) \cap \mathcal{D}(b_0) = \mathcal{D}(a \wedge b_0)$.
  On utilise la division euclidienne de a par b_0 : il existe $q, r \in \mathbb{Z}$ tels que

$$a = b_0 q + r \qquad \text{et} \qquad 0 \leq r < |b_0|$$

  Par le lemme précédent, on a alors $\mathcal{D}(a) \cap \mathcal{D}(b_0) = \mathcal{D}(b_0) \cap \mathcal{D}(r)$ et $a \wedge b_0 = b_0 \wedge r$. Or, comme $r < b_0$, l'assertion H_r est vraie, si bien que $\mathcal{D}(b_0) \cap \mathcal{D}(r) = \mathcal{D}(b_0 \wedge r)$. Finalement,

$$\mathcal{D}(a) \cap \mathcal{D}(b_0) = \mathcal{D}(b_0) \cap \mathcal{D}(r) = \mathcal{D}(b_0 \wedge r) = \mathcal{D}(a \wedge b_0)$$

  Ainsi, H_{b_0} est vraie.
- Conclusion : la propriété H_b est vraie pour tout $b \in \mathbb{N}^*$.

□

3.2 Algorithme d'Euclide

L'algorithme d'Euclide permet de calculer un PGCD en effectuant des divisions euclidiennes successives.

Méthode (Algorithme d'Euclide)

Soit $a, b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$. Quitte à échanger a et b, on suppose que $b \neq 0$

1. On fait la division euclidienne de a par b : on trouve un reste r_1.
2. Puis on fait la division euclidienne de b par r_1 : on trouve un reste r_2.
3. Puis on fait la division euclidienne de r_1 par r_2 : on trouve un reste r_3, etc.
4. On s'arrête dès qu'on trouve un reste nul : $r_k = 0$ avec $k \geq 1$.
5. Alors, le PGCD de a et b est le *dernier reste non nul* qu'on a obtenu, à savoir :

$$r_{k-1} = a \wedge b \qquad (\text{si } k = 1, \text{ alors } r_{k-1} = r_0 := b)$$

Démonstration. En effet, on a $\mathcal{D}(r_k) = \mathcal{D}(0) = \mathbb{Z}$, donc, par le lemme 9.9

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r_1) = \cdots = \mathcal{D}(r_{k-1}) \cap \mathcal{D}(r_k) = \mathcal{D}(r_{k-1})$$

si bien que $r_{k-1} = a \wedge b$ par le Théorème 9.10. □

Exemple 5. Calculer le PGCD de 162 et 207.

L'algorithme d'Euclide est un grand classique qu'il faut savoir coder en Python !

```
1 def euclide(a,b):
2     """ calcule le PGCD de deux entiers naturels a et b avec b>0 """
3     while b!=0:
4         a,b=b,a%b
5     return a
```

3.3 PGCD de deux entiers relatifs

Définition 9.11

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. On définit le PGCD de a et b par :

$$a \wedge b := |a| \wedge |b| \in \mathbb{N}^*$$

et on a de même que $\mathcal{D}(a \wedge b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

3.4 Théorème de Bézout–Bachet

Théorème 9.12 (Théorème de Bézout–Bachet)

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. Il existe un couple $(u,v) \in \mathbb{Z}^2$ tels que

$$au + bv = a \wedge b$$

(u,v) est appelé un couple de coefficients de Bézout de a et b.

Démonstration. Tout d'abord, quitte à remplacer a par $-a$ (et u par $-u$), on peut supposer $a \in \mathbb{N}$. De même, on peut supposer $b \in \mathbb{N}$. Si $a = 0$, alors $a \wedge b = b$ si bien que le couple $(u,v) = (0,1)$ convient. Il suffit donc de montrer le théorème pour $a \in \mathbb{N}^*$.
Montrons par récurrence forte sur $b \in \mathbb{N}$ que l'assertion suivante est vraie :

$$H_b : \qquad \forall a \in \mathbb{N}^* \quad \exists (u,v) \in \mathbb{Z}^2 \qquad au + bv = a \wedge b$$

- Initialisation : si $b = 0$, alors de même que ci-dessus on peut prendre $(u,v) = (1,0)$. Donc H_0 est vraie.
-

□

Remarque. Les coefficients u et v ne sont pas uniques : si (u,v) sont des coefficients de Bézout pour a et b, il en va de même pour $(u + bk, v - ak)$ avec $k \in \mathbb{Z}$.

Méthode (Algorithme d'Euclide étendu)

On peut calculer un couple de coefficients de Bézout (u,v) avec l'algorithme d'Euclide, cf ci-dessous.

Exemple 6. Calculer $245 \wedge 200$ puis trouver $(u,v) \in \mathbb{Z}$ tels que $245u + 200v = 245 \wedge 200$.

4 Entiers premiers entre eux

4.1 Définition et théorème de Bézout

Définition 9.13 (Entiers premiers entre eux)

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Autrement dit, a et b sont premiers entre eux si les seuls diviseurs communs à a et b sont 1 et -1.

Théorème 9.14 (Théorème de Bézout)

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. Alors :

$$a \wedge b = 1 \iff \exists u,v \in \mathbb{Z} \quad au + bv = 1$$

Contrairement au théorème de Bézout-Bachet, il s'agit ici d'une équivalence.

Démonstration. Le sens direct est une conséquence immédiate du théorème de Bézout-Bachet. Pour le sens réciproque, on sait que $a \wedge b$ divise a et b, donc $a \wedge b$ divise $au + bv = 1$. Ainsi, $a \wedge b \in \{-1,1\}$. Comme $a \wedge b$ est positif, $a \wedge b = 1$. □

Exemple 7. Soit $a \in \mathbb{Z}$. Montrer que a et $a+1$ sont premiers entre eux.

Proposition 9.15 (Se ramener à des entiers premiers entre eux)

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$ et $d = a \wedge b$.
Alors il existe $a',b' \in \mathbb{Z}$ tels que

$$a = da' \qquad b = db' \qquad a' \wedge b' = 1$$

En particulier, $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont toujours premiers entre eux.

Démonstration. Comme $d \mid a$ et $d \mid b$, il existe $a',b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Enfin, par le théorème de Bézout-Bachet, il existe $u,v \in \mathbb{Z}$ tels que

$$au + bv = d$$

donc

$$da'u + db'v = d$$

ou encore $a'u + b'v = 1$, ce qui implique que $a' \wedge b' = 1$ par le théorème de Bézout. □

Définition 9.16 (Forme irréductible)

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. On pose $d = a \wedge b$. Alors la forme irréductible de $\dfrac{a}{b}$ est $\dfrac{a'}{b'}$ (avec $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$).

Exemple 8. On a $12 \wedge 18 = 6$ donc la forme irréductible de $\dfrac{18}{12}$ est $\dfrac{\frac{18}{6}}{\frac{18}{6}} = \dfrac{3}{2}$.

4.2 Trois théorèmes de divisibilité

Proposition 9.17 (Lemme de Gauss)

Soit $a,b,c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration. Comme $a \wedge b = 1$, il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$. Ainsi,

$$auc + bvc = c$$

Or, $a \mid auc$ et de plus $a \mid bc$ donc $a \mid bcv$. On en déduit que $a \mid c$. □

Proposition 9.18

Soit $a_1,a_2,b \in \mathbb{Z}$. Si $a_1 \wedge b = 1$ et $a_2 \wedge b = 1$, alors $(a_1a_2) \wedge b = 1$.

Démonstration. Par le théorème de Bézout, il existe $u_1,v_1,u_2,v_2 \in \mathbb{Z}$ tels que $\begin{cases} a_1u_1 + bv_1 = 1 \\ a_2u_2 + bv_2 = 1 \end{cases}$

En multipliant ces inégalités, on obtient :

$$a_1a_2\,(u_1u_2) + b\,(v_1a_2u_2 + v_2a_1u_1 + bv_1v_2) = 1$$

si bien que $(a_1a_2) \wedge b = 1$. □

Proposition 9.19

Soit $a,b,c \in \mathbb{Z}$. Si

$$(a \mid c \quad \text{et} \quad b \mid c \quad \text{et} \quad a \wedge b = 1) \implies ab \mid c$$

Démonstration. Comme $a \wedge b = 1$, il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$. Ainsi,

$$auc + bvc = c$$

Or, $b \mid c$ donc $ab \mid ac$ et de même $ab \mid bc$. Ainsi, $ab \mid (auc + bvc)$, ou encore $ab \mid c$. □

Exemple 9. Soit $n \in \mathbb{Z}$. Comme $2 \wedge 3 = 1$, on a $(2 \mid n \quad \text{et} \quad 3 \mid n) \implies 6 \mid n$.

4.3 PGCD de plusieurs entiers

Définition 9.20

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^n \setminus \{(0,0,\dots,0)\}$. Le PGCD de $a_1,\dots,a_n$ est le plus grand diviseur commun à tous les a_i. On le note

$$\bigwedge_{i=1}^{n} a_i := a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

La notation est cohérente car on peut montrer que $\wedge$ est associative :

$$a_1 \wedge (a_2 \wedge a_3) = (a_1 \wedge a_2) \wedge a_3$$

donc on peut enlever les parenthèses sans ambiguité.

Si un des a_i est nul, on peut l'enlever de la famille $(a_i)_{1 \le i \le n}$ sans modifier le PGCD. On peut donc toujours supposer $a_i \neq 0$.

Définition 9.21

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^*$. On dit que $a_1,\dots,a_n$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$.
On dit que $a_1,\dots,a_n$ sont premiers entre eux deux à deux si pour tous $i,j \in [\![1,n]\!]$ on a $a_i \wedge a_j = 1$.

Si $a_1,\dots,a_n$ sont premiers entre eux deux à deux alors ils le sont dans leur ensemble. La réciproque est fausse :

$$2 \wedge 3 \wedge 6 = 1 \qquad \text{mais} \qquad 6 \wedge 3 = 3 \neq 1$$

On peut généraliser à n entiers la plupart des résultats vu pour deux entiers. Les plus utiles (et au programme) sont les théorèmes de Bézout et de Bézout-Bachet :

Théorème 9.22 (Bézout-Bachet généralisé)

Soit $(a_1,\dots,a_n) \in \mathbb{Z}^*$. Il existe $u_1,\dots,u_n \in \mathbb{Z}$ tels que

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

Théorème 9.23 (Bézout généralisé)

Soit $(a_1,\dots,a_n)\in\mathbb{Z}^*$. Les entiers $a_1,a_2,\dots,a_n$ sont premiers entre eux dans leur ensemble si et seulement si

$$\exists u_1,u_2,\dots,u_n\in\mathbb{Z}\qquad a_1u_1+a_2u_2+\cdots+a_nu_n=1$$

Les preuves reposent entièrement sur une récurrence : l'exemple ci-dessous permet de mieux comprendre.

Exemple 10. Montrer que 7, 200 et 245 sont premiers dans leur ensemble.
Trouver $u,v,w\in\mathbb{Z}$ tels que $7u+200v+245w=1$.

5 PPCM

Pour tout $c\in\mathbb{Z}$, l'ensemble des multiples de c est $c\mathbb{Z}:=\{ck\mid k\in\mathbb{Z}\}$.
Soit $a,b\in\mathbb{N}^*$. L'ensemble $X:=a\mathbb{Z}\cap b\mathbb{Z}$ constitue l'ensemble des multiples communs à a et b. L'ensemble $X\cap\mathbb{N}^*$ est une partie non vide (car $ab\in X$) et minorée de $\mathbb{Z}$. Ainsi, $X\cap\mathbb{N}^*$ admet un minimum. Cela justifie la définition suivante.

Définition 9.24 (PPCM)

Soit $a,b\in\mathbb{N}^*$. Le PPCM de a et b, noté $a\vee b$, est le plus petit des multiples communs *strictement positifs* à a et b. Autrement dit,

$$a\vee b:=\min\left(a\mathbb{Z}\cap b\mathbb{Z}\cap\mathbb{N}^*\right)$$

Pour $a,b\in\mathbb{Z}^*$, on définit le PPCM de a et b par $a\vee b:=|a|\vee|b|$.

Exemple 11. Soit $a,b\in\mathbb{Z}^*$

1. $a\vee b\geq 1$
2. $a\vee b\leq|ab|$
3. $a\vee 1=|a|$
4. $a\vee b=b\vee a$
5. $a\vee b=|b|\iff a\mid b$
6. $\forall c\in\mathbb{N}^*\qquad(ca)\vee(cb)=|c|(a\vee b)$

Théorème 9.25

Soit $a, b \in \mathbb{Z}^*$ et $m = a \vee b$. Alors $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, ce qui veut dire que

$$\forall n \in \mathbb{Z} \qquad (a \mid n \qquad \text{et} \qquad b \mid n) \iff m \mid n$$

Remarque. $m = a \vee b$ est le seul élément de $\mathbb{N}^*$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, ou encore le seul qui vérifie l'équivalence ci-dessus.

Proposition 9.26

Soit $a, b \in \mathbb{Z}^*$. Alors

$$(a \vee b) \times (a \wedge b) = |a| \times |b|$$

Démonstration. Par définition du PGCD et du PPCM, il suffit de regarder le cas $a, b \in \mathbb{N}^*$.

- Supposons d'abord que $a \wedge b = 1$. Il suffit alors de montrer que $a \vee b = ab$. Tout d'abord, ab est un multiple commun à a et b, donc par définition, $(a \vee b) \mid ab$. Ensuite,

  $$a \mid (a \vee b) \qquad \text{et} \qquad b \mid (a \vee b) \qquad \text{et} \qquad a \wedge b = 1$$

  donc on en déduit (proposition 9.19) que $ab \mid (a \vee b)$. Donc ab et $a \vee b$ sont associés. Comme ab et $a \vee b$ sont positifs, on obtient $a \vee b = ab$.

-

□

6 Nombres premiers

6.1 Définitions et premières propriétés

Définition 9.27

On appelle nombre premier tout entier $p \geq 2$ tel que les seuls diviseurs positifs de p sont 1 et p.
Autrement dit, p est premier si $\mathcal{D}(p) \cap \mathbb{N} = \{1, p\}$.

Exemple 12. 1 n'est pas un nombre premier.
2 est un nombre premier. C'est l'unique nombre premier pair. En effet, si $n = 2k$ avec $k \geq 2$, alors $2 \mid n$ et $2 \notin \{1, n\}$, donc n n'est pas premier.

Remarque. Si $n \geq 2$ n'est pas premier, alors il existe $a, b \in [\![2, n-1]\!]$ tel que $n = ab$.
En effet, $\mathcal{D}(n) \cap \mathbb{N} \neq \{1, n\}$, donc il existe $a \in [\![2, n-1]\!]$ tel que $a \mid n$. En particulier, il existe $b \in \mathbb{Z}$ tel que $n = ab$.
On montre alors facilement que, comme $1 < a < n$, on a aussi $1 < b < n$.

Proposition 9.28

Soit $a \in \mathbb{Z}$ et p un nombre premier. Ou bien $p \mid a$, ou bien $p \wedge a = 1$.
En particulier, p est premier avec tout entier qu'il ne divise pas.

Démonstration. $p \wedge a \in \mathcal{D}(p) \cap \mathbb{N}$, donc deux cas sont possibles : ou bien $p \wedge a = 1$, ou bien $p \wedge a = p$. Or, on a vu (Exemple 4) que

$$p \wedge a = p \iff p \mid a$$

D'où le résultat. □

Corollaire 9.29

Soit p_1, p_2 deux nombres premiers. Si $p_1 \neq p_2$, alors $p_1 \wedge p_2 = 1$.
En particulier, si $p_1 \mid p_2$, alors $p_1 = p_2$.

Démonstration. Supposons $p_1 \neq p_2$. p_2 admet pour seuls diviseurs positifs 1 et p_2, et comme $2 \leq p_1 \neq p_2$, on en déduit que p_1 ne divise pas p_2. Par la proposition ci-dessus, $p_1 \wedge p_2 = 1$.
Montrons la contraposée de la seconde assertion. On suppose $p_1 \neq p_2$: montrons que p_1 ne divise pas p_2. Comme $p_1 \neq p_2$, par la première assertion, on a $p_1 \wedge p_2 = 1$. En particulier, par la proposition 9.28 (comme "ou bien" est exclusif), on en déduit que p_1 ne divise pas p_2. D'où le résultat. □

Proposition 9.30 (Lemme d'Euclide)

Soit $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (ou inclusif !).

Démonstration. Supposons que $p \mid ab$. Si $p \mid a$, alors c'est terminé. Sinon, par la proposition 9.28, on obtient $p \wedge a = 1$, donc par le lemme de Gauss, $p \mid b$. □

6.2 Décomposition en produit de facteurs premiers

Lemme 9.31

Tout entier $n \geq 2$ admet un diviseur qui est un nombre premier.

Démonstration. Par récurrence forte sur n : si $n = 2$, n admet 2 pour diviseur premier.
Soit $n \geq 3$. Si n est premier, alors n admet n pour diviseur premier. Sinon, n admet un autre diviseur $k \in [\![2, n-1]\!]$.
Par l'hypothèse de récurrence, k admet un diviseur premier p, donc n admet aussi p pour diviseur. □

Théorème 9.32 (Décomposition en produit de facteurs premiers)

Soit $n \geq 2$ un entier. Il existe $r \in \mathbb{N}^*$, des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$ tels que

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

De plus, les entiers $(p_i)_{1\leq i\leq r}$ et $(\alpha_i)_{1\leq i\leq r}$ sont uniques. Les nombres premiers $p_1, \ldots, p_r$ sont appelés les facteurs premiers de n.

Démonstration. **Existence.** On procède par récurrence forte sur n.

- Pour $n = 2$, on a $2 = 2^1$: on a bien une décomposition avec $p_1 = 2$ et $\alpha_1 = 1$ (et $r = 1$).
- Soit $n_0 \in \mathbb{N}$ avec $n_0 \geq 3$. On suppose que le résultat est vrai pour tout $n \in [\![2, n_0 - 1]\!]$. Montrons-le au rang n_0. Si n_0 est premier, alors $n_0 = n_0^1$ est la décomposition recherchée. Si n_0 n'est pas premier, alors par le lemme ci-dessus, il existe un nombre premier p tel que $p \mid n_0$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $n_0 = pk$.

  Or, comme n_0 n'est pas premier, on a nécessairement $1 < p < n_0$, et donc aussi $1 < k < n_0$. Par hypothèse de récurrence, il existe $r \in \mathbb{N}^*$, des nombres premiers $p_1 < \cdots < p_r$ et des entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$ tels que

  $$k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

  Alors,

  $$n_0 = p \times p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

  On en déduit que n_0 admet une décomposition en produits de facteurs premiers.

Unicité. Supposons que $n \geq 2$ admette deux décompositions :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

- Soit $i \in [\![1, r]\!]$. Montrons qu'il existe $j \in [\![1, s]\!]$ tel que $p_i \mid q_j$. Comme $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$, par le lemme d'Euclide, il existe $j \in [\![1, s]\!]$ tel que $p_i \mid q_j^{\beta_j}$. Supposons par l'absurde que p_i ne divise pas q_j. Alors $p_i \wedge q_j = 1$. Par la proposition 9.19, on en déduit que $p_i \wedge q_j^{\beta_j} = 1$. Ainsi, par la proposition 9.19, on en déduit que p_i ne divise pas $q_j^{\beta_j}$. Contradiction. Donc $p_i \mid q_j$.
- Comme $p_i \mid q_j$ et que q_j est premier, on en déduit que (corollaire 9.29) $p_i = q_j$. Ainsi, chaque p_i est égal à un q_j et un seul (car les q_j sont tous distincts). Réciproquement, chaque q_j est égal à un seul p_i. On en déduit que $r = s$. De plus, comme les familles (p_i) et (q_j) sont croissantes, on a $p_i = q_i$ pour tout $i \in [\![1, r]\!]$.
- Par ce qui précède, on a donc

  $$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$$

  Supposons par l'absurde qu'il existe i tel que $\alpha_i \neq \beta_i$ (par exemple $\alpha_i < \beta_i$). Alors en divisant par $p_i^{\alpha_i}$,

  $$\prod_{j\neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j\neq i} p_j^{\beta_j}$$

  Donc $p_i \mid \prod_{j\neq i} p_j^{\alpha_j}$. Comme au premier point, on en déduit qu'il existe $j \neq i$ tel que $p_i \mid p_j$. Comme p_i, p_j sont premiers, on a $p_i = p_j$. Or, c'est impossible puisque $j \neq i$. Contradiction. Donc pour tout i, on a $\alpha_i = \beta_i$.

Les deux décompositions obtenues sont donc bien égales. □

Exemple 13. $24 = 2^3 \times 3$ est la décomposition en facteurs premiers de 24.
$36 = 4 \times 3^2$ n'est pas la décomposition en facteurs premiers de 36 : c'est $36 = 2^2 \times 3^2$.

Exemple 14. Décomposer 630 en produits de facteurs premiers.

Corollaire 9.33

Il existe une infinité de nombres premiers.

Démonstration. On construit une infinité de nombres premiers par récurrence. On pose d'abord $p_1 = 2$, qui est premier. Ensuite, étant donnés n nombres premiers $p_1, p_2, \dots, p_n$ (avec $n \geq 1$), on pose

$$N := \prod_{i=1}^{n} p_i + 1$$

Soit $i \in [\![1, n]\!]$. Comme

$$N \times 1 - p_i \times \prod_{j \neq i} p_i = 1$$

par le théorème de Bézout, on en déduit que $N \wedge p_i = 1$. Par arbitraire sur i, aucun des p_i ne divise N. Or, par le lemme ci-dessus, N admet un diviseur premier q. Comme $q \mid N$ mais que chaque p_i ne divise pas N, on a forcément $q \neq p_i$. Ainsi, q est un nombre premier qui n'est pas dans $\{p_1, \dots, p_n\}$. On peut alors poser $p_{n+1} := q$. □

6.3 Valuation p-adique

Définition 9.34

Soit p un nombre premier. Pour tout entier $n \in \mathbb{N}^*$, on appelle valuation p-adique de n, un nombre noté $v_p(n)$, défini comme le plus grand entier $m \in \mathbb{N}$ tel que

$$p^m \mid n \qquad \text{et} \qquad p^{m+1} \nmid n$$

Autrement dit

$$v_p(n) := \max \left\{ k \in \mathbb{N} \quad | \quad p^k \mid n \right\}$$

Exemple 15.

- $v_2(8) = 3$ car $2^3 \mid 8$ mais $2^4 \nmid 8$.
- $v_5(100) = 2$.
- $v_3(4) = 0$.
- $v_p(1) = 0$ pour tout nombre premier p.

Proposition 9.35

On peut "lire" la valuation p-adique de n sur sa décomposition en produit de facteurs premiers : si

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

alors pour tout $i \in [\![1, r]\!]$, $v_{p_i}(n) = \alpha_i$, et pour tout nombre premier $p \notin \{p_1, \dots, p_r\}$, on a $v_p(n) = 0$.

Définition 9.36 (Décomposition généralisée)

Soit $n \in \mathbb{N}^*$. Soit $p_1 < \cdots < p_r$ des nombres premiers tels que $\{p_1, \ldots, p_r\}$ contienne tous les facteurs premiers de n. Il existe alors une décomposition généralisée de n selon $p_1, \ldots, p_r$:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad \text{avec } \alpha_i \in \mathbb{N}$$

et dans ce cas, $\alpha_i = v_{p_i}(n) \in \mathbb{N}$.

Dans la décomposition généralisée, on peut donc avoir $\alpha_i = 0$. Si les nombres $p_1, \ldots, p_r$ sont fixés, cette décomposition est unique.

Proposition 9.37

Soit $a, b \in \mathbb{N}^*$. Alors pour tout nombre premier p,

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $a \mid b$ si et seulement si $v_q(a) \leq v_q(b)$ pour tout nombre premier q.
3. Si $v_q(a) = v_q(b)$ pour tous les nombres premiers q, alors $a = b$.
4. $v_p(a \wedge b) = \min(v_p(a), v_p(b))$
5. $v_p(a \vee b) = \max(v_p(a), v_p(b))$

Démonstration. On ne prouve que les points 1 et 4. On note $p_1, \ldots, p_r$ tous les facteurs premiers qui apparaissent dans les décompositions de a et b. Il existe alors une décomposition généralisée de a et b selon $p_1, \ldots, p_r$:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad \alpha_i = v_{p_i}(a)$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} \qquad \beta_i = v_{p_i}(b)$$

Alors,

$$ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \ldots p_r^{\alpha_r+\beta_r}$$

On en déduit que pour tout i, $v_{p_i}(ab) = \alpha_i + \beta_i = v_{p_i}(a) + v_{p_i}(b)$. Donc l'assertion 1 est vraie.
Maintenant, si on pose $\gamma_i = \min(\alpha_i, \beta_i)$ et

$$d := p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_r^{\gamma_r}$$

on va montrer que $d = a \wedge b$. Comme $\gamma_i \leq \alpha_i$, on a $d \mid a$. De même $d \mid b$. Ainsi, $d \mid (a \wedge b)$. En particulier, pour tout i, on a $\gamma_i \leq v_{p_i}(a \wedge b)$. Supposons par l'absurde qu'il existe $j \in [\![1, r]\!]$ tel que $\gamma_j < v_{p_j}(a \wedge b)$. Quitte à échanger a et b, on peut par exemple supposer que $\min(\alpha_j, \beta_j) = \alpha_j$. Comme $\alpha_j + 1 \leq v_{p_j}(a \wedge b)$, on en déduit que $p_j^{\alpha_j+1} \mid (a \wedge b)$, donc que $p_j^{\alpha_j+1} \mid a$. Ainsi,

$$\alpha_j + 1 = v_{p_j}\left(p_j^{\alpha_j+1}\right) \leq v_{p_j}(a) = \alpha_j$$

Contradiction. Donc pour tout i, on a $v_{p_i}(d) = v_{p_i}(a \wedge b)$. On en déduit que $d = a \wedge b$. □

Exemple 16. Calculer le pgcd et le ppcm de 360 et 315.

6.4 Crible d'Ératosthène

Le crible d'Ératosthène est une méthode (laborieuse et non recommandée) pour trouver tous les nombres premiers plus petits qu'un certain nombre, par exemple inférieurs ou égaux à 23 dans le crible ci-dessous.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	...						

- On commence avec le nombre, 2, qu'on entoure. Puis on raye tous les multiples de 2.
- Puis on prend le nombre suivant 3, qu'on entoure. Puis on raye tous les multiples de 3.
- Le nombre 4 est rayé, on l'ignore. On recommence avec 5 : on l'entoure et on raye tous ses multiples.
- On continue jusqu'à ce que chaque nombre du crible soit ou rayé, ou entouré. Les nombres entourés seront alors les nombres premiers.

Remarque (Tester si un nombre est premier)**.** Soit un entier $n \geq 2$. Si n n'est divisible par aucun nombre premier $p \leq n-1$, alors n est premier. Mais en fait, il suffit de vérifier cela pour tout nombre premier $p \leq \sqrt{n}$.

Par exemple, si $n \leq 100$, n sera premier si aucun nombre premier inférieur à 10 ne divise n. Ainsi, 89 est premier car 89 n'est pas divisible par 2, 3, 5, 7.

7 Congruences

7.1 Définition et relation d'équivalence

Définition 9.38 (Congruences)

Soit un entier $n \geq 2$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $n \mid (b-a)$. On note alors

$$a \equiv b \quad [n]$$

Certains auteurs notent parfois $a \equiv b \pmod{n}$. Une caractérisation très utile est :

$$\boxed{a \equiv b \quad [n] \iff \exists k \in \mathbb{Z} \quad a - b = kn}$$

Remarque. $a \equiv 0 \quad [2]$ si et seulement si a est pair, ou encore $a \in 2\mathbb{Z}$. De même, $a \equiv 1 \quad [2] \iff a \in 2\mathbb{Z}+1$.

Exemple 17. $10 \equiv 3 \quad [7]$ et $3 \equiv -11 \quad [7]$.
Pour tout $k \in \mathbb{Z}$, on a $5k+8 \equiv 3 \quad [5]$.

Exemple 18. Résoudre l'équation $x \equiv 2 \quad [7]$.

Proposition 9.39 (Relation "congru modulo n")

Soit $a, b \in \mathbb{Z}$ et un entier $n \geq 2$.

1. La relation "congru modulo n" est une relation d'équivalence :
   - $a \equiv a \quad [n]$
   - si $a \equiv b \quad [n]$, alors $b \equiv a \quad [n]$.
   - si $a \equiv b \quad [n]$ et $b \equiv c \quad [n]$, alors $a \equiv c \quad [n]$.
2. $a \equiv b \quad [n]$ si et seulement si a et b ont le même reste quand on fait leur division euclidienne par n.
3. Il y a donc n classes d'équivalence pour la relation "congru modulo n" :

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}$$

(Une classe pour chaque reste possible)

7.2 Opérations et congruences

Proposition 9.40 (Opérations sur les congruences)

Soit $a, b, c, d \in \mathbb{Z}$ et un entier $n \geq 2$.

1. $a \equiv b \quad [n] \quad \Longrightarrow \quad \forall k \in \mathbb{Z} \quad a + kn \equiv b \quad [n]$
2. On peut additionner, soustraire ou multiplier les congruences :

$$\begin{cases} a \equiv b & [n] \\ c \equiv d & [n] \end{cases} \Longrightarrow \begin{cases} a + c \equiv b + d & [n] \\ a - c \equiv b - d & [n] \\ ac \equiv bd & [n] \end{cases}$$

3. En particulier, pour tout $k \in \mathbb{Z}$

$$a \equiv b \quad [n] \quad \Longrightarrow \quad ka \equiv kb \quad [n]$$

4. On peut passer à la puissance dans une congruence : pour tout $k \in \mathbb{N}$,

$$a \equiv b \quad [n] \Longrightarrow a^k \equiv b^k \quad [n]$$

Démonstration. On ne montre que le deuxième point. On suppose que $n \mid (b-a)$ et $n \mid (d-c)$. Donc,

$$\begin{array}{rlllll} & n \mid (b-a+d-c) & \text{et} & n \mid [b-a-(d-c)] & \text{et} & n \mid [(b-a)d + a(d-c)] \\ \Longrightarrow & n \mid [b+d-(a+c)] & \text{et} & n \mid [b-d-(a-c)] & \text{et} & n \mid (bd-ac) \\ \Longrightarrow & a+c \equiv b+d \quad [n] & \text{et} & a-c \equiv b-d \quad [n] & \text{et} & ac \equiv bd \quad [n] \end{array}$$

□

Exemple 19. Montrer que $9^{2017} \equiv -1 \quad [10]$.

Exemple 20. Calculer le reste de la division euclidienne de 7^{129} par 48.

7.3 La division et la congruence

Attention la division dans une congruence n'est pas autorisée en général :

$$9 \equiv 3 \quad [6] \qquad \text{mais} \qquad \frac{9}{3} \not\equiv \frac{3}{3} \quad [6]$$

Par contre, si a, b, n sont tous divisibles par un entier $d \in \mathbb{N}^*$, alors $a \equiv b \quad [n] \iff \frac{a}{d} \equiv \frac{b}{d} \quad \left[\frac{n}{d}\right]$. Par exemple

$$9 \equiv 3 \quad [6] \qquad \Longrightarrow \qquad 3 \equiv 1 \quad [2]$$

Définition 9.41 (Inverse modulo n)

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. On dit que a admet un inverse modulo n si

$$\exists b \in \mathbb{Z} \qquad ab \equiv 1 \quad [n]$$

Un entier $b \in \mathbb{Z}$ qui vérifie cela est appelé un inverse de a modulo n.

Cet inverse n'est pas unique : si b est un inverse de a modulo n, il en va de même pour $b + kn$ avec $k \in \mathbb{Z}$.

Proposition 9.42 (Passage à l'inverse dans une congruence)

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. Alors a admet un inverse modulo n si et seulement si $a \wedge n = 1$.
Dans ce cas, si on note b cet inverse, alors

$$\forall x, c \in \mathbb{Z} \qquad ax \equiv c \quad [n] \iff x \equiv bc \quad [n]$$

Méthode (Trouver un inverse modulo n)

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$ tels que $a \wedge n = 1$. Pour trouver un inverse de a modulo n, il suffit de trouver un couple de coefficients de Bézout (u, v) tels que

$$au + nv = 1$$

Dans ce cas, $au \equiv 1 \quad [n]$, donc u est un inverse de a modulo n.

Corollaire 9.43 (Division et congruence)

Si $ax \equiv ay \quad [n]$ et $a \wedge n = 1$, alors $x \equiv y \quad [n]$.

Exercice 1. Trouver un inverse de 5 modulo 7. En déduire les solutions de $5x \equiv 2 \quad [7]$.

Méthode (Résoudre une équation sur les congruences)

Étant donnés $A, B, N \in \mathbb{Z}$ fixés, on cherche à résoudre une équation de congruence de la forme $Ax \equiv B \quad [N]$ d'inconnue $x \in \mathbb{Z}$.

1. On détermine $d := A \wedge N$. Si d ne divise pas B, il n'y a pas de solution.
   - En effet, s'il existait une solution $x \in \mathbb{Z}$, alors il existerait $k \in \mathbb{Z}$ tel que $B = Ax + kN$. Or, $d \mid A$ et $d \mid N$ donc $d \mid (Ax + kN)$, càd $d \mid B$. Contradiction.
2. Si $d \mid B$, alors on pose
   $$a := \frac{A}{d} \in \mathbb{Z} \qquad b := \frac{B}{d} \in \mathbb{Z} \qquad n := \frac{N}{d} \in \mathbb{Z}$$
   et on divise toute la congruence par d : $Ax \equiv B \quad [N] \iff ax \equiv b \quad [n]$.
3. Par construction de a et n, nécessairement $a \wedge n = 1$. Alors on détermine un inverse de a modulo n : on le notera (ici) c.
4. $$ax \equiv b \quad [n] \iff x \equiv cb \quad [n] \iff \exists k \in \mathbb{Z} \quad x = cb + kn$$
   donc $\mathcal{S} = \{cb + kn \mid k \in \mathbb{Z}\}$.

7.4 Petit théorème de Fermat

Lemme 9.44

Soit p un nombre premier.
$$\forall a, b \in \mathbb{Z} \qquad (a+b)^p \equiv a^p + b^p \quad [p]$$

Démonstration. Par la formule du binôme, on a

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

On va montrer que pour tout $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$. Si on prouve cela, alors on aura

$$p \left| \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \right.$$

et donc $(a+b)^p \equiv a^p + b^p \quad [p]$.

Montrons donc que $p \mid \binom{p}{k}$. On a

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p}{k} \frac{(p-1)!}{(k-1)!(p-k)!} = \frac{p}{k} \frac{(p-1)!}{(k-1)!((p-1)-(k-1))!} = \frac{p}{k} \binom{p-1}{k-1}$$

Ainsi, $p\binom{p-1}{k-1} = k\binom{p}{k}$ et donc $p \mid k\binom{p}{k}$. Or, comme $1 \leq k \leq p-1$ et que p est premier, on a $p \wedge k = 1$. Par le lemme de Gauss, on en déduit que $p \mid \binom{p}{k}$. D'où le résultat. □

Théorème 9.45 (Petit théorème de Fermat)

Si p est un nombre premier et $a \in \mathbb{Z}$, alors

$$a^p \equiv a \quad [p]$$

De plus, si $a \wedge p = 1$, alors

$$a^{p-1} \equiv 1 \quad [p]$$

Démonstration. Si $a^p \equiv a \quad [p]$ et $a \wedge p = 1$, alors on peut diviser par a dans la congruence et en déduire que $a^{p-1} \equiv 1 \quad [p]$. Il suffit donc de montrer que $a^p \equiv a \quad [p]$.

On fait d'abord la preuve pour $a \in \mathbb{N}$, par récurrence sur a.

- Si $a = 0$, alors $0^p = 0$ donc $0^p \equiv 0 \quad [p]$. La propriété est vraie au rang 0.
- Supposons que $a^p \equiv a \quad [p]$ pour un $a \in \mathbb{N}$, et montrons que $(a+1)^p \equiv a+1 \quad [p]$. Par le lemme ci-dessus, comme p est premier,

$$\begin{aligned} (a+1)^p &\equiv a^p + 1^p \quad [p] \\ &\equiv a + 1^p \quad [p] \qquad \text{par hypothèse de récurrence} \\ &\equiv a+1 \quad [p] \end{aligned}$$

  Donc la propriété est vraie au rang $a+1$.
- Finalement, pour tout $a \in \mathbb{N}$, $a^p \equiv a \quad [p]$.

Faisons enfin la preuve pour $a \in \mathbb{Z} \setminus \mathbb{N}$. Comme $p \geq 2$, il existe $k \in \mathbb{N}$ (assez grand) tel que $a + kp \geq 0$. On pose alors $b := a + kp$. Par construction, $b \equiv a \quad [p]$ et donc $b^p \equiv a^p \quad [p]$. De plus, comme $b \geq 0$, on a montré que $b^p \equiv b \quad [p]$. Ainsi,

$$a^p \equiv b^p \equiv b \equiv a \quad [p]$$

□

Exemple 21. Quel est le reste de la division euclidienne de 14^{314} par 11 ?

8 Équations diophantiennes

Définition 9.46 (Équation diophantienne)

On appelle équation diophantienne une équation dont la ou les inconnues sont des entiers relatifs.

Exemple 22. L'équation $2x+7y=3$ d'inconnues $x,y\in\mathbb{Z}$.
L'équation $x^2+y^2=z^2$ d'inconnues $x,y,z\in\mathbb{Z}$.

La résolution de ces équations est souvent non triviale. Néanmoins, il y a un cas particulier d'équation qu'il faut savoir traiter sans indication : les équations diophantiennes du premier ordre à deux inconnues :

Méthode (Résolution d'une équation diophantienne du type $Ax+By=C$)

Soit $A,B,C\in\mathbb{Z}$. On cherche à résoudre l'équation $Ax+By=C$ d'inconnues $x,y\in\mathbb{Z}$.

1. On pose $d=A\wedge B$. Si $d\nmid C$, alors il n'y a pas de solution. Si $d\mid C$, on pose $a=\dfrac{A}{d}$, $b=\dfrac{B}{d}$, $c=\dfrac{C}{d}$, et alors on résoud à la place $ax+by=c$. Par construction, $a\wedge b=1$.
2. On cherche un couple de coefficients de Bézout pour a et b, qu'on note (u,v) : on a donc
$$au+bv=1$$
3. En multipliant par c cette équation, on obtient donc une solution particulière $(x_0,y_0)=(cu,cv)$.
4. Alors, $\mathcal{S}=\{(x_0-bk,y_0+ak)\mid k\in\mathbb{Z}\}$.

Démonstration. Justifions le dernier point : on vérifie directement que pour tout $k\in\mathbb{Z}$, $(x_0-bk,y_0+ak)\in\mathcal{S}$. Montrons l'autre inclusion : soit $(x,y)\in\mathcal{S}$. Alors
$$\begin{cases} ax+by=c \\ ax_0+by_0=c \end{cases} \implies a(x-x_0)+b(y-y_0)=0$$
Ainsi, $a(x-x_0)=-b(y-y_0)$: comme $a\wedge(-b)=a\wedge b=1$, par le lemme de Gauss, $a\mid(y-y_0)$, donc il existe $k\in\mathbb{Z}$ tel que $y=y_0+ak=cv+ak$. Alors,
$$x-x_0=-\frac{1}{a}b(y-y_0)=-bk$$
d'où $x=x_0-bk$. □