Cours du 22/11/2021. Arithmétique (L. Bétermin).

Théorème 1 (**Euclide**). *Il existe une infinité de nombres premiers.*

Pour démontrer ce résultat, nous avons besoin du lemme suivant.

Lemme 2 (**Existence d'un facteur premier**). *Soit $n \in \mathbb{N}$, $n \geq 2$. Soit p le plus petit diviseur de n supérieur ou égal à 2. Alors p est premier.*

Démonstration du lemme. Soit q un diviseur de p, alors $q|n$ et $q \leq p$. On a donc deux possibilités :

1. soit $q = p$ par minimalité de p ;
2. soit $q = 1$.

Ainsi, p n'admet que p et 1 comme diviseur, et donc p est premier. □

Démonstration du Théorème d'Euclide. On raisonne par l'absurde et on suppose que l'ensemble des nombres premiers est fini, noté $\{p_1, ..., p_k\}$. On considère le nombre

$$N = p_1 \times p_2 \times ... \times p_k + 1 = \prod_{i=1}^{k} p_i + 1.$$

On remarque que pour tout $j \in \{1, ..., k\}$, $p_j | \prod_{i=1}^{k} p_i$ donc p_j ne divise pas N. Ainsi, si p est le plus petit diviseur de N qui est supérieur ou égal à 2, alors $p \notin \{p_1, ..., p_k\}$. Par le lemme précédent, p est nécessairement premier donc on a une contradiction. On en déduit que l'ensemble des nombres premiers est infini. □

L'ensemble des nombres premiers est infini mais reste encore très mystérieux. Par exemple, il existe des intervalles de nombres entiers arbitrairement grand sans nombre premier.

Lemme 3 (**Existence d'intervalles arbitraires sans nombre premier**). *Pour tout $N \geq 2$, il existe N nombres entiers consécutifs non-premiers.*

Démonstration. Il suffit de considérer l'ensemble des N nombres entiers consécutifs $\{n_k\}_{1 \leq k \leq N}$ définis par :

$$\forall 1 \leq k \leq N, \quad n_k := (N+1)! + k + 1 = 1 \times 2 \times 3 \times ... \times (N+1) + k + 1.$$

En effet, pour tout $1 \leq k \leq N$, $(k+1)|(N+1)!$, donc $(k+1)|n_k$. Comme $k+1 \geq 2$, on en déduit que n_k n'est pas premier pour tout $k \in \{1, ..., N\}$. □

De plus, le plus grand nombre premier connu à ce jour (22/11/2021), c'est-à-dire pour lequel on a pu vérifier informatiquement qu'il n'était effectivement divisible que par 1 et par lui-même est

$$2^{82\,589\,933} - 1.$$

Ce nombre comporte 24 862 048 chiffres et a été découvert le 7 décembre 2018 par le Great Internet Mersenne Prime Search (GIMPS). Il s'agit d'un projet de calcul partagé : le calcul est réparti sur plusieurs microprocesseurs/unité centrales. Ce calcul est basé sur un test permettant de savoir si un nombre dit "nombre de Mersenne" de la forme $2^k - 1$, est premier ou non. Il est intéressant de tester ces nombres de Mersenne car on a le résultat suivant.

Lemme 4 (**Nombres de Mersenne**). *Si le nombre de Mersenne $M_k = 2^k - 1$ est un nombre premier, alors k est un nombre premier.*

Remarque 5. *La réciproque de ce résultat est malheureusement fausse : si k est un nombre premier, alors M_k n'est pas nécessairement premier.*
Par exemple, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier.

Démonstration. (Cf. TD 7, Exercice 7-9) On raisonne par contraposée. Si k n'est pas un nombre premier, alors on peut écrire $k = qn$ avec $n \in \mathbb{N}$ et $q \geq 2$. On a donc, en utilisant la formule de factorisation de $a^n - b^n$ avec $a = 2^q$ et $b = 1$,

$$2^k - 1 = 2^{qn} - 1 = (2^q)^n - 1 = (2^q - 1)\left((2^q)^{n-1} + (2^q)^{n-2} + ... + 2^q + 1\right).$$

Comme $q \geq 2$, on a donc $2^q - 1 > 1$ ainsi que $(2^q)^{n-1} + (2^q)^{n-2} + ... + 2^q + 1 > 1$. On en déduit que $2^k - 1$ n'est pas un nombre premier, ce qui termine la preuve. □

C'est pour cela que les nombres de Mersenne sont de bons candidats pour être des nombres premiers. Une fois que l'on connait un entier premier k, on teste si $2^k - 1$ est premier. Dans le cas du nombre premier $k = 82\,589\,933$, il a fallu 11 jours pour montrer que M_k est bien un nombre premier.

Voici un résultat important qui montre que les nombres premiers sont les "briques" permettant de construire tous les nombres entiers.

Théorème 6 (**Décomposition en facteurs premiers**). *Soit $n \geq 2$ un entier, alors il existe une unique écriture de n sous la forme*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où l'on a :

1. $\forall i \in \{1, ..., k\}$, p_i *est premier ;*
2. $\forall i \in \{1, ..., k\}$, $\alpha_i \in \mathbb{N}^*$ *;*
3. $p_1 < p_2 < ... < p_k$.

Démonstration. Admise. □

Remarque 7. *On voit qu'il est nécessaire que 1 ne soit pas premier pour avoir l'unicité de la décomposition. L'existence d'une telle décomposition se montre facilement par récurrence.*

Déterminer une telle décomposition peut se révéler extrêmement difficile. C'est un des fondements du chiffrement RSA (inventé par Rivest-Shamir-Adleman) utilisé pour échanger des données confidentielles sur Internet (commerce électronique notamment).

Une application directe de cette unique décomposition en produit de facteurs premiers est la généralisation de l'irrationalité de $\sqrt{2}$.

Proposition 8 (**Irrationalité de $\sqrt{N}$ quand N n'est pas un carré**). *Soit $N \in \mathbb{N}$ tel que $\sqrt{N} \notin \mathbb{N}$, alors $\sqrt{N} \in \mathbb{R}\backslash\mathbb{Q}$.*

Démonstration. On raisonne par l'absurde et on suppose que $\sqrt{N} \in \mathbb{Q}$. Il existe donc $p, q \in \mathbb{N}$ tels que $\sqrt{N} = \frac{p}{q}$. On obtient donc que

$$Nq^2 = p^2.$$

On remarque la chose suivante : n est un carré si et seulement si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ comme dans le théorème mais avec α_i pair pour tout $i \in \{1, ..., k\}$.

Comme N n'est pas un carré, il existe un nombre premier p_i avec pour exposant α_i impair dans sa décomposition en facteurs premiers. Ainsi, p_i apparaît dans la décomposition en facteur premiers de Nq^2 avec un exposant impair, ce qui ne peut pas être le cas pour p^2. On a donc une contradiction et $\sqrt{N}$ est irrationnel. □

La **division euclidienne** est celle que vous avez apprise à l'école primaire :

$$\begin{array}{r|l} 25 & 7 \\ \hline 4 & 3 \end{array} \qquad \text{Quotient} = 3 \text{ et Reste} = 4.$$

Proposition 9 (**Division euclidienne**). *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ d'entiers tels que*

1. $a = bq + r$
2. $0 \leq r < |b|$.

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

Démonstration. Admise. □

Définition 10 (**Plus Grand Commun Diviseur (PGCD)**). *Soit $(a, b) \in \mathbb{Z}^2$ tels que $(a, b) \neq (0, 0)$, alors l'ensemble des diviseurs communs à a et b*

$$\{n \in \mathbb{N}^* : n|a \text{ et } n|b\}$$

est fini et non-vide (car il contient $n = 1$). Il admet donc un plus grand élément noté $\text{PGCD}(a, b)$.

Exemple 11. *Si $a = 10$ et $b = 14$, alors*

- $\{n \in \mathbb{N}^* : n|10\} = \{1, 2, 5, 10\}$
- $\{n \in \mathbb{N}^* : n|14\} = \{1, 2, 7, 14\}$.

On a donc $\{n \in \mathbb{N}^* : n|10 \text{ et } n|14\} = \{1, 2\}$ et ainsi $\text{PGCD}(10, 14) = 2$.

Proposition 12 (**Homogénéité du PGCD**). *Soient $(a, b) \in \mathbb{Z}^2$ deux entiers non-nuls. Alors, $\forall k \in \mathbb{N}^*$,* $\text{PGCD}(ka, kb) = k \times \text{PGCD}(a, b)$.

Démonstration. Notons $d = \text{PGCD}(a, b)$ et $d' = \text{PGCD}(ka, kb)$.
Comme d divise a et b, kd divise ka et kb, donc kd divise leur PGCD d'. On écrit $d' = k'(kd)$ où $k' \in \mathbb{Z}$.
Comme d' divise ka et kb, $k'kd$ divise ka et kb. On en déduit que $k'd$ divise a et b et divise donc leur PCGD d. On a donc $k' = 1$ et donc $d' = k'(kd) = kd$. □

Méthodes de calcul du PGCD.

• *Méthode 1 : A partir de la décomposition en facteurs premiers de a et b.*
Inconvénient : il n'est pas facile de décomposer un entier en facteurs premiers.
Supposons qu'il existe k nombres premiers distincts $\{p_1, ..., p_k\}$ et $2k$ nombres entiers (éventuellement nuls) $\{\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_k\}$ tels que

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors on a $\mathrm{PGCD}(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$.

Exemple 13. *Considérons $a = 1071$ et $b = 462$, alors on a, en utilisant tous les facteurs premiers apparaissant dans a et b,*

- $a = 1071 = 3^2 \times 7 \times 17 = 2^0 \times 3^2 \times 7^1 \times 11^0 \times 17^1$
- $b = 462 = 2 \times 3 \times 7 \times 11 = 2^1 \times 3^1 \times 7^1 \times 11^1 \times 17^0$.

On trouve donc, en prenant le minimum de chaque exposant,

$$\mathrm{PGCD}(1071, 462) = 2^0 \times 3^1 \times 7^1 \times 11^0 \times 17^0 = 21.$$

• *Méthode 2 : L'algorithme d'Euclide.*

Remarque préliminaire : On se base sur la remarque suivante : les diviseurs communs à a et b sont aussi les diviseurs communs à b et $a-b$.

Preuve : En effet, si m divise à la fois a et b, alors il divise b et $a-b$. Réciproquement, si m divise b et $a-b$, alors m divise aussi la différence de ces deux entiers, c'est-à-dire $(a-b)-b=a$, et donc m divise à la fois a et b.

On en déduit que $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(b,a-b)$.

On a aussi $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(b,a)$ et $\mathrm{PGCD}(a,0)=a$.

Principe : quitte à échanger a et b, on peut supposer que $a\geq b$.

- si $b=0$, alors on a $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(a,0)=a$.
- si $b\neq 0$, alors on effectue la division euclidienne de a par b, $a=bq+r$ et on utilise la remarque préliminaire (q fois) pour dire que

$$\mathrm{PGCD}(a,b)=\mathrm{PGCD}(b,a-qb)=\mathrm{PGCD}(b,r).$$

On réitère ce principe jusqu'à obtenir $\mathrm{PGCD}(d,0)$ où d sera donc $d=\mathrm{PGCD}(a,b)$.

Exemple 14. *Soit $a=1071$ et $b=462$, alors*

1. $1071=2\times 462+147$
2. $462=3\times 147+\boldsymbol{21}$
3. $147=7\times 21+0$

Le dernier reste non-nul dans cette suite de divisions euclidiennes est

$$\mathrm{PGCD}(1071,462)=21.$$

Définition 15 (Plus Petit Commun Multiple (PPCM)). *Soient $(a,b)\in\mathbb{Z}^2$ tels que $(a,b)\neq(0,0)$, alors l'ensemble des multiples communs à a et b*

$$\{n\in\mathbb{N}^*: a|n \text{ et } b|n\}$$

est non-vide (car il contient ab). Il admet donc un plus petit élément noté $\mathrm{PPCM}(a,b)$.

Méthodes de calcul du PPCM.

• *Méthode 1 : A partir de la décomposition en facteurs premiers de a et b.*
Supposons qu'il existe k nombres premiers distincts $\{p_1, ..., p_k\}$ et $2k$ nombres entiers (éventuellement nuls) $\{\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_k\}$ tels que

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors on a $\text{PPCM}(a, b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$.

Exemple 16. *Considérons $a = 1071$ et $b = 462$, alors on a, en utilisant tous les facteurs premiers apparaissant dans a et b,*

- $a = 1071 = 3^2 \times 7 \times 17 = 2^0 \times 3^2 \times 7^1 \times 11^0 \times 17^1$
- $b = 462 = 2 \times 3 \times 7 \times 11 = 2^1 \times 3^1 \times 7^1 \times 11^1 \times 17^0$.

On trouve donc, en prenant le maximum de chaque exposant,

$$\text{PPCM}(1071, 462) = 2^1 \times 3^2 \times 7^1 \times 11^1 \times 17^1 = 23562.$$

• *Méthode 2 : En connaissant* $\text{PGCD}(a, b)$.
On remarque que l'on a, pour tout $(a, b) \in \mathbb{Z}^2$ tels que $(a, b) \neq (0, 0)$,

$$\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab.$$

Preuve : En effet, en utilisant la décomposition décrite dans la méthode 1 et le fait que pour tout réels (x, y), $\max(x, y) + \min(x, y) = x + y$, on obtient

$$\begin{aligned} \text{PGCD}(a, b) \times \text{PPCM}(a, b) &= \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)} \times \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)} \\ &= \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i)} \\ &= \prod_{i=1}^{k} p_i^{\alpha_i + \beta_i} = \prod_{i=1}^{k} p_i^{\alpha_i} \times \prod_{i=1}^{k} p_i^{\beta_i} = ab. \end{aligned}$$

Exemple 17. *Soit $a = 1071$ et $b = 462$, alors on a montré que* $\text{PGCD}(1071, 462) = 21$, *on a donc*

$$\text{PPCM}(1071, 462) = \frac{1071 \times 462}{\text{PGCD}(1071, 462)} = \frac{1071 \times 462}{21} = 23562.$$

Définition 18 (**Nombres premiers entre eux**). *Soient* $(a,b) \in \mathbb{Z}^2$. *On dit que* a *et* b *sont premiers entre eux si* $\mathrm{PGCD}(a,b) = 1$, *c'est-à-dire si le seul diviseur commun positif de* a *et* b *est 1.*

Exemple 19. *Les nombres* $7 = 3^0 \times 5^0 \times 7^1$ *et* $15 = 3^1 \times 5^1 \times 7^0$ *sont premiers entre eux, car* $\mathrm{PGCD}(7,15) = 3^0 \times 5^0 \times 7^0 = 1$.

Proposition 20. *Soient* $(a,b) \in \mathbb{N}^2$ *deux entiers non-nuls. Soit* d *un diviseur commun à* a *et* b *et posons* $a = da'$ *ainsi que* $b = db'$ *avec* $(a',b') \in \mathbb{N}$. *On a*

$$\mathrm{PGCD}(a,b) = d \iff a' \text{ et } b' \text{ sont premiers entre eux.}$$

Démonstration. Si $\mathrm{PGCD}(a,b) = d$, alors $d = \mathrm{PGCD}(da', db') = d \times \mathrm{PGCD}(a',b')$ par la propriété d'homogénéité du PGCD et donc $\mathrm{PGCD}(a',b') = 1$.
Réciproquement, si $\mathrm{PGCD}(a',b') = 1$, alors $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(da', db') = d \times \mathrm{PGCD}(a',b') = d$. □

Méthode pour déterminer $(a,b) \in \mathbb{N}^2$ **connaissant** $\mathrm{PGCD}(a,b)$ **et** $\mathrm{PPCM}(a,b)$

• *Etape 1 : On calcule* $\dfrac{\mathrm{PPCM}(a,b)}{\mathrm{PGCD}(a,b)}$. *Ce nombre est égal au produit de deux entiers premiers entre eux.*
En effet, on a $a = \mathrm{PGCD}(a,b) \times a'$ et $b = \mathrm{PGCD}(a,b) \times b'$ où a' et b' sont premiers entre eux d'après la proposition précédente. On a donc

$$ab = \mathrm{PGCD}(a,b) \times a' \times \mathrm{PGCD}(a,b) \times b' = \mathrm{PGCD}(a,b) \times \mathrm{PPCM}(a,b)$$

ce qui implique que

$$\frac{\mathrm{PPCM}(a,b)}{\mathrm{PGCD}(a,b)} = a' \times b', \quad \text{où } a' \text{ et } b' \text{ sont premiers entre eux.}$$

• *Etape 2 : On cherche tous les couples* (a',b') *premiers entre eux vérifiant l'égalité précédente.*
• *Etape 3 : On multiplie ces nombres par* $\mathrm{PGCD}(a,b)$ *pour obtenir toutes les couples* (a,b) *possibles.*

Exemple 21. *Déterminons* $(a,b) \in \mathbb{N}^2$ *tels que* $\mathrm{PGCD}(a,b) = 12$ *et* $\mathrm{PPCM}(a,b) = 252$. *On calcule* $\dfrac{\mathrm{PPCM}(a,b)}{\mathrm{PGCD}(a,b)} = \dfrac{252}{12} = 21$ *et on cherche tous les couples d'entiers naturels premiers entre eux dont le produit est* 21. *Les seules solutions sont* $(1,21)$ *et* $(3,7)$. *Ainsi, les solutions du problème sont* $(12,252)$ *et* $(3 \times 12, 7 \times 12) = (36,84)$.

Théorème 22 (**Identité de Bézout**). *Soient a et b deux entiers non nuls, alors il existe $(u, v) \in \mathbb{Z}^2$, appelés coefficients de Bézout, tels que*

$$au + bv = \text{PGCD}(a, b).$$

En particulier, si a et b sont premiers entre eux, alors il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.

Exemple 23. *Soient $a = 7$ et $b = 17$, alors $u = 5$ et $v = -2$ conviennent car*

$$7 \times 5 + 17 \times (-2) = 1.$$

Remarque 24. *Si a et b sont strictement positifs, alors u et v sont de signes opposés.*

Méthode pour déterminer les coefficients de Bézout u et v.
On "remonte" l'algorithme d'Euclide utilisé pour le calcul de $\text{PGCD}(a, b)$ en isolant les restes

Exemple 1 : $a = 17$ et $b = 7$. Calculons $\text{PGCD}(17, 7)$ par l'algorithme d'Euclide.

$$\begin{aligned} 17 &= 2 \times 7 + 3 \\ 7 &= 2 \times 3 + \mathbf{1} \\ 3 &= 3 \times 1 + 0. \end{aligned}$$

$\text{PGCD}(17, 7) = 1$, c'est le dernier reste non-nul. On remonte maintenant l'algorithme en remplaçant les restes par leurs expressions :

$$\begin{aligned} 1 &= 7 - 2 \times 3 && \textit{(On exprime 1 grâce à la deuxième équation)} \\ &= 7 - 2 \times [17 - 2 \times 7] && \textit{(On exprime 3 grâce à la première équation et on remplace)} \\ &= 7 - 2 \times 17 + 4 \times 7 && \textit{(On développe sans calculer)} \\ &= 5 \times 7 - 2 \times 17 && \textit{(On met en facteur a et b)} \end{aligned}$$

On obtient donc $u = -2$ et $v = 7$ qui vérifient $au + bv = 1$.

Exemple 2 : $a = 600$ et $b = 124$. Calculons $\mathrm{PGCD}(600, 124)$ par l'algorithme d'Euclide.

$$\begin{aligned} 600 &= 4 \times 124 + 104 \\ 124 &= 1 \times 104 + 20 \\ 104 &= 5 \times 20 + \mathbf{4} \\ 20 &= 5 \times 4 + 0. \end{aligned}$$

$\mathrm{PGCD}(600, 124) = 4$, c'est le dernier reste non-nul. On remonte maintenant l'algorithme en remplaçant les restes par leurs expressions :

$$\begin{aligned} 4 &= 104 - 5 \times 20 && \textit{(Identité de Bézout pour 104 et 20)} \\ &= 104 - 5 \times (124 - 104) \\ &= 6 \times 104 - 5 \times 124 && \textit{(Identité de Bézout pour 124 et 104)} \\ &= 6 \times (600 - 4 \times 124) - 5 \times 124 \\ &= 6 \times 600 - 29 \times 124 && \textit{(Identité de Bézout pour 600 et 124).} \end{aligned}$$

On obtient donc $u = 6$ et $v = -20$ qui vérifient $au + bv = \mathrm{PGCD}(a, b)$.

Remarque 25 (**Infinité des coefficients de Bézout**)**.** *Le couple* (u, v) *n'est pas unique, il y en a une infinité. En effet, pour tout* $k \in \mathbb{Z}$*,*

$$\begin{aligned} & au + bv = \mathrm{PGCD}(a, b) \\ \iff & au + bv + k\frac{ab}{\mathrm{PGCD}(a,b)} - k\frac{ab}{\mathrm{PGCD}(a,b)} = \mathrm{PGCD}(a, b) \\ \iff & a\left(u + k\frac{b}{\mathrm{PGCD}(a,b)}\right) + b\left(v - k\frac{a}{\mathrm{PGCD}(a,b)}\right) = \mathrm{PGCD}(a, b). \end{aligned}$$

Par définition, $\mathrm{PGCD}(a, b)|b$ *et* $\mathrm{PGCD}(a, b)|a$*, donc* $k\frac{b}{\mathrm{PGCD}(a,b)} \in \mathbb{Z}$ *et* $k\frac{a}{\mathrm{PGCD}(a,b)} \in \mathbb{Z}$*. On en déduit que si* (u, v) *sont des coefficients de Bezout, alors il en est de même pour tous les couples*

$$\left\{\left(u + k\frac{b}{\mathrm{PGCD}(a,b)}, v - k\frac{a}{\mathrm{PGCD}(a,b)}\right)\right\}_{k\in\mathbb{Z}}$$

En fait, on a l'équivalence suivante.

Proposition 26. *Soient* $(a, b) \in \mathbb{Z}^2$*, alors*

$$a \text{ et } b \text{ sont premiers entre eux } \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1.$$

Démonstration. Par l'identité de Bézout, il est clair que si a et b sont premiers entre eux, alors il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.
Supposons maintenant qu'il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$. Soit p un diviseur positif commun à a et b. Alors $p|au$ et $p|bv$, donc $p|au + bv$ et donc $p|1$. On en déduit que $p = 1$ et donc $\text{PGCD}(a, b) = 1$, ce qui veut dire que a et b sont premiers entre eux. □

Théorème 27 (**Théorème de Gauss**). *Soient $a, b, c \in \mathbb{Z}^*$ tels que a et b soient premiers entre eux. Si $a|bc$ alors $a|c$.*

Démonstration. Comme $\text{PGCD}(a, b) = 1$, par l'identité de Bézout il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$. En multipliant cette égalité par $c \neq 0$, on obtient

$$auc + (bc)v = c.$$

On sait que $a|auc$ et par hypothèse $a|bc$ donc $a|(bc)v$. On en déduit donc que $a|c$. □

Définition 28 (**Congruences**). *Soit $n \in \mathbb{N}^*$. On dit que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont congrus modulo n si $n|a - b$, c'est-à-dire si $\exists k \in \mathbb{Z}, \quad a = b + kn$.*
On écrit $a \equiv b\ [n]$.
C'est aussi équivalent à dire que les divisions euclidiennes de a par n et de b par n donnent le même reste.

Exemple 29. *On a $13 \equiv 1\ [12]$ car 12 divise $13-1 = 12$. On a aussi $143 \equiv 9\ [2] \equiv 1\ [2]$ car 2 divise à la fois $143 - 9 = 134$ et $9 - 1 = 8$ (mais aussi $143 - 1 = 142$).*

Proposition 30 (**Opérations sur les congruences**). *Soit $n \in \mathbb{N}^*$ et $(a, b, c, d) \in \mathbb{Z}^4$.*

1. *Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$.*
2. *Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $ac \equiv bd\ [n]$.*
3. *Si $a \equiv b\ [n]$, alors $\forall k \in \mathbb{N}^*$, $a^k \equiv b^k\ [n]$.*

Démonstration. Montrons 1. Comme $a \equiv b\ [n]$ et $c \equiv d\ [n]$, on sait que $n|a-b$ et $n|c-d$. On en déduit que $n|(a-b+c-d)$, c'est-à-dire $n|((a+c)-(b+d))$ ce qui veut dire que $a + c \equiv b + d\ [n]$.
Montrons 2. Pour la même raison que précédemment, on sait que $n|a-b$ et $n|c-d$. On écrit

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d),$$

et donc $n|(ac - bd)$ ce qui veut dire que $ac \equiv bd\ [n]$.
Montrons 3. par récurrence sur $k \in \mathbb{N}^*$ et notons P_k la propriété "$a^k \equiv b^k\ [n]$".

Initialisation : pour $k = 1$, c'est évident car $a \equiv b\,[n]$, donc P_1 est vraie.
Hérédité : soit $k \in \mathbb{N}^*$, supposons que P_k est vraie et montrons que P_{k+1} est vraie. Comme $a^k \equiv b^k\,[n]$ et $a \equiv b\,[n]$, on en déduit par 2. que $a^{k+1} \equiv b^{k+1}\,[n]$ ce qui montre que P_{k+1} est vraie.
On en déduit que P_k est vraie pour tout $k \in \mathbb{N}^*$. □

Applications des relations de Bézout.

• *Application 1 : Résolution d'équations diophantiennes dans $\mathbb{Z}$.*
Problème : Soient $a, b, c \in \mathbb{Z}$, trouver $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = c$.

Théorème 31 (**Existence d'une solution pour une équation diophantienne**). *Soient $a, b, c \in \mathbb{Z}$. L'équation $ax+by = c$ admet une solution $(x, y) \in \mathbb{Z}^2$ si et seulement si* $\mathrm{PGCD}(a, b)|c$.

Démonstration. Si $(x, y) \in \mathbb{Z}^2$ est une solution de $ax+by = c$, alors comme $\mathrm{PGCD}(a, b)|a$ et $\mathrm{PGCD}(a, b)|b$, on a $\mathrm{PGCD}(a, b)|(ax + by)$, c'est-à-dire que $\mathrm{PGCD}(a, b)|c$.
On suppose maintenant que $\mathrm{PGCD}(a, b)|c$. L'identité de Bézout pour $(a, b) \in \mathbb{Z}^2$ dit qu'il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = \mathrm{PGCD}(a, b).$$

Comme $\mathrm{PGCD}(a, b)|c$, il existe $k \in \mathbb{Z}$ tel que $c = k \times \mathrm{PGCD}(a, b)$. On obtient donc, en multipliant l'équation précédente par k,

$$kau + kbv = k \times \mathrm{PGCD}(a, b) = c.$$

On voir donc que $x = ku$ et $y = kv$ sont des solutions de $ax + by = c$, l'existence d'une solution est donc démontrée. □

Exemple 32 (**Solutions d'une équation diophantienne**). *On cherche à trouver toutes les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation*

$$7x + 5y = 3 \quad (*)$$

Etape 1 : Détermination d'une solution par l'identité de Bézout.
On utilise l'algorithme d'Euclide pour déterminer $(u, v) \in \mathbb{Z}$ tels que $7u+5v = \mathrm{PGCD}(7, 5)$:

$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$

$$2 = 2 \times 1 + 0.$$

On a $\mathrm{PGCD}(7,5) = 1$ *et on remonte l'algorithme de la façon suivante :*

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (7 - 5) \\ &= 3 \times 5 - 2 \times 7. \end{aligned}$$

On multiple maintenant par 3 *et on obtient :*

$$3 = 9 \times 5 - 6 \times 7 = 7 \times (-6) + 5 \times 9 \quad (**)$$

Etape 2 : Génération des autres solutions par le Théorème de Gauss.
Soit $(x, y) \in \mathbb{Z}^2$ *une solution de* $(*)$*, alors* $(**) - (*)$ *donne* $7(x+6) + 5(y-9) = 0$*, c'est-à-dire*

$$7(x+6) = -5(y-9) \quad (***).$$

Comme $7|7(x+6)$*, alors* $7| - 5(y-9)$*. Comme* 7 *et* 5 *sont premiers entre eux, par le Théorème de Gauss on obtient que* $7|-(y-9)$*. Il existe donc* $k \in \mathbb{Z}$ *tel que* $-(y-9) = 7k$*, c'est-à-dire*

$$y = 9 - 7k.$$

On remplace y *par* $9 - 7k$ *dans* $(***)$ *et on obtient* $7(x+6) = -5(-7k)$*, c'est-à-dire* $x = 5k - 6$.
Réciproquement, $\forall k \in \mathbb{Z}$*, le couple* $(x, y) \in \mathbb{Z}^2$ *défini par* $x = 5k - 6$ *et* $y = 9 - 7k$ *est solution de* $(*)$ *car*

$$7x + 5y = 7(5k - 6) + 5(9 - 7k) = 3.$$

L'ensemble des solutions de $(*)$ *est donc*

$$\{(5k - 6, 9 - 7k) : k \in \mathbb{Z}\}.$$

• *Application 2 : Résolution de systèmes de congruences.*

Théorème 33. *Soient a, b deux entiers naturels non-nuls premiers entre eux et soient $y, z \in \mathbb{Z}$. Alors le système d'inconnue $x \in \mathbb{Z}$*

$$\begin{cases} x \equiv y\ [a] \\ x \equiv z\ [b] \end{cases}$$

admet une unique solution x_0 dans $\{0, 1, ..., ab-1\}$ et les solutions dans $\mathbb{Z}$ sont de la forme $x = x_0 + kab$ pour $k \in \mathbb{Z}$.

Exemple 34 (**Résolution d'un système de congruences**). *On cherche à résoudre*

$$\begin{cases} x \equiv 3\ [4] \\ x \equiv 5\ [9] \end{cases}.$$

Etape 1 : On détermine l'identité de Bézout pour $a = 4$ et $b = 9$, c'est-à-dire un couple (u, v) et on écrit $x = u(ax) + v(bx)$.
L'algorithme d'Euclide s'écrit

$$9 = 2 \times 4 + 1$$
$$4 = 1 \times 4 + 0.$$

Ainsi $\mathrm{PGCD}(9, 4) = 1$ *et on remonte l'algorithme d'Euclide très simplement :*

$$1 = 9 - 2 \times 4.$$

Puis on multiple par x et on trouve

$$x = 9x - 2 \times 4x.$$

Etape 2 : On cherche $ax = 4x$ et $bx = 9x$ modulo $a \times b = 4 \times 9 = 36$.
On a $x \equiv 3\ [4] \Rightarrow \exists k_1 \in \mathbb{Z}, x = 4k_1 + 3 \Rightarrow 9x = 36k_1 + 27 \Rightarrow 9x \equiv 27\ [36]$.
On a $x \equiv 5\ [9] \Rightarrow \exists k_2 \in \mathbb{Z}, x9k_2 + 5 \Rightarrow 4x = 36k_2 + 20 \Rightarrow 4x \equiv 20\ [36]$.

Etape 3 : On combine les deux premières étapes pour obtenir une solution, puis toutes les solutions du système de congruences.
On a donc

$$x \equiv 9x - 2 \times 4x\ [36]$$

$$\equiv 27 - 2 \times 20 \ [36]$$
$$\equiv -13 \ [36]$$
$$\equiv -13 + 36 \ [36]$$
$$\equiv 23 \ [36].$$

Ainsi $x_0 = 23$ est une solution (la solution unique dans $\{0, 1, ..., 35\}$) et la forme générale d'une solution est donc

$$x = 23 + 36k, \quad k \in \mathbb{Z}.$$

Théorème 35 (**Bases de numération**). *Soit $b \geq 2$. Tout entier $x \in \mathbb{N}$ peut s'écrire d'une manière unique sous la forme*

$$x = a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0,$$

où $n \in \mathbb{N}$ et $\forall i \in \{0, ...n\}$, $a_i \in \{0, ..., b-1\}$. On dit alors que $x = \overline{a_n a_{n-1} ... a_0}^b$ (aussi noté $x = (a_n a_{n-1} ... a_0)_b$) est l'écriture de x en base b.

Exemple 36. *Pour $b = 10$, c'est l'écriture habituelle décimale. Par exemple*

$$125 = 100 + 2 \times 10 + 5 = 10^2 + 2 \times 10 + 5, \quad a_0 = 5, a_1 = 2, a_2 = 1.$$

Pour $b = 2$, c'est l'écriture binaire. Par exemple :

$$\begin{aligned} 105 &= 64 + 41 && \text{(64 est la plus grande puissance de 2 inférieure à 105)} \\ &= 64 + 32 + 91 && \text{(32 est la plus grande puissance de 2 inférieure à 41)} \\ &= 64 + 32 + 8 + 1 && \text{(8 est la plus grande puissance de 2 inférieure à 9)} \\ &= 2^6 + 2^5 + 2^3 + 2^0, && a_0 = 1, a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 0, a_5 = 1, a_6 = 1. \end{aligned}$$

donc $\overline{105}^{10} = \overline{1101001}^2$.