Arithmétique dans $\mathbb{Z}$

(École Normale Supérieure)

Définition : Divisibilité

Définition

Soient $a, b \in \mathbb{Z}$. On dit que b divise a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que

$$a = bq.$$

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.
- Si $a|1$, alors $a = +1$ ou $a = -1$.

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.
- Si $a|1$, alors $a = +1$ ou $a = -1$.
- $(a|b$ et $b|a) \implies b = \pm a$.

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.
- Si $a|1$, alors $a = +1$ ou $a = -1$.
- $(a|b \text{ et } b|a) \implies b = \pm a$.
- $(a|b \text{ et } b|c) \implies a|c$.

Exemples de divisibilité

Exemples

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.
- Si $a|1$, alors $a = +1$ ou $a = -1$.
- $(a|b \text{ et } b|a) \implies b = \pm a$.
- $(a|b \text{ et } b|c) \implies a|c$.
- $(a|b \text{ et } a|c) \implies a|(b+c)$.

Théorème : Division euclidienne

Théorème

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il existe des entiers $q, r \in \mathbb{Z}$ tels que :

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

De plus, q et r sont uniques.

Démonstration : Existence

Existence. On peut supposer $a \geq 0$ pour simplifier. Soit

$$N = \{n \in \mathbb{N} \mid bn \leq a\}.$$

C'est un ensemble non vide car $n = 0 \in N$. De plus N est toujours majoré, donc il admet un plus grand élément noté $q = \max N$.
Alors $qb \leq a$ car $q \in N$, et $(q+1)b > a$ car $q + 1 \notin N$. Donc :

$$qb \leq a < (q+1)b = qb + b.$$

Démonstration : Existence

Existence. On peut supposer $a \geq 0$ pour simplifier. Soit

$$N = \{n \in \mathbb{N} \mid bn \leq a\}.$$

C'est un ensemble non vide car $n = 0 \in N$. De plus N est toujours majoré, donc il admet un plus grand élément noté $q = \max N$.
Alors $qb \leq a$ car $q \in N$, et $(q+1)b > a$ car $q + 1 \notin N$. Donc :

$$qb \leq a < (q+1)b = qb + b.$$

On définit alors $r = a - qb$. Ce r vérifie :

$$0 \leq r = a - qb < b.$$

Démonstration : Unicité

Unicité. Supposons que q, r et q', r' soient deux entiers vérifiant les conditions du théorème. On a :

$$a = bq + r = bq' + r'.$$

Ainsi :

$$b(q - q') = r' - r.$$

Démonstration : Unicité

Unicité. Supposons que q, r et q', r' soient deux entiers vérifiant les conditions du théorème. On a :

$$a = bq + r = bq' + r'.$$

Ainsi :

$$b(q - q') = r' - r.$$

D'autre part, $0 \leq r' < b$ et $0 \leq r < b$, donc $-b < r' - r < b$. En substituant $r' - r = b(q - q')$, on obtient :

$$-b < b(q - q') < b.$$

En divisant par $b > 0$, on a :

$$-1 < q - q' < 1.$$

Comme $q - q'$ est un entier, la seule possibilité est $q - q' = 0$, donc $q = q'$. En revenant à $r' - r = b(q - q')$, on obtient maintenant $r = r'$.

Définition : PGCD

Définition

Soient $a, b \in \mathbb{Z}$ deux entiers, non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle le **plus grand diviseur commun** de a et b, et se note $\mathrm{pgcd}(a, b)$.

Exemples

Exemples

- $\text{pgcd}(21, 14) = 7$, $\text{pgcd}(12, 32) = 4$, $\text{pgcd}(21, 26) = 1$.

Exemples

Exemples

- $\mathrm{pgcd}(21, 14) = 7$, $\mathrm{pgcd}(12, 32) = 4$, $\mathrm{pgcd}(21, 26) = 1$.
- $\mathrm{pgcd}(a, ka) = a$, pour tout $k \in \mathbb{Z}$ et $a > 0$.

Exemples

Exemples

- $\mathrm{pgcd}(21, 14) = 7$, $\mathrm{pgcd}(12, 32) = 4$, $\mathrm{pgcd}(21, 26) = 1$.
- $\mathrm{pgcd}(a, ka) = a$, pour tout $k \in \mathbb{Z}$ et $a > 0$.
- **Cas particuliers.** Pour tout $a > 0$:

$$\mathrm{pgcd}(a, 0) = a \quad \text{et} \quad \mathrm{pgcd}(a, 1) = 1.$$

Lemme : Algorithme d'Euclide

Lemme

Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors :

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r).$$

En fait, on a même $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide, on applique le lemme avec q, le quotient.

Démonstration du lemme

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat, car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b, donc aussi bq.

Démonstration du lemme

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat, car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b, donc aussi bq.
- De plus, d divise a, donc d divise $a - bq = r$.

Démonstration du lemme

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat, car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b, donc aussi bq.
- De plus, d divise a, donc d divise $a - bq = r$.
- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.
  - Sinon, on continue avec b et r_1 :

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.
  - Sinon, on continue avec b et r_1 :
- $b = r_1 q_2 + r_2$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2)$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.
  - Sinon, on continue avec b et r_1 :
- $b = r_1 q_2 + r_2$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2)$.
- $r_1 = r_2 q_3 + r_3$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_2, r_3)$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.
  - Sinon, on continue avec b et r_1 :
- $b = r_1 q_2 + r_2$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2)$.
- $r_1 = r_2 q_3 + r_3$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_2, r_3)$.
- $\ldots$
- $r_{k-2} = r_{k-1} q_k + r_k$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_{k-1}, r_k)$.

Algorithme d'Euclide

On souhaite calculer le $\mathrm{pgcd}(a, b)$ avec $a, b \in \mathbb{N}^*$. Supposons $a > b$.

Étapes de l'algorithme :

- Division de a par b : $a = bq_1 + r_1$.
  - Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$.
  - Sinon, on continue avec b et r_1 :
- $b = r_1 q_2 + r_2$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2)$.
- $r_1 = r_2 q_3 + r_3$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_2, r_3)$.
- $\ldots$
- $r_{k-2} = r_{k-1} q_k + r_k$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_{k-1}, r_k)$.
- $r_{k-1} = r_k q_k + 0$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_k, 0) = r_k$.

Algorithme d'Euclide

Conclusion : À chaque étape, $0 \leq r_{i+1} < r_i$, donc l'algorithme se termine car les restes forment une suite strictement décroissante d'entiers positifs ou nuls :

$$b > r_1 > r_2 > \cdots > 0.$$

Exemple 4 : Calcul du PGCD

Calculons le $\mathrm{pgcd}(600, 124)$:

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

Ainsi :

$$\mathrm{pgcd}(600, 124) = 4.$$

Définition et exemple

Définition

Deux entiers a et b sont premiers entre eux si $\mathrm{pgcd}(a, b) = 1$.

Exemple

Pour tout $a \in \mathbb{Z}$, a et $a + 1$ sont premiers entre eux.

Démonstration

- Soit d un diviseur commun à a et $a+1$.
- Alors d divise aussi $a+1-a$, donc d divise 1.
- Ainsi, $d = \pm 1$, et le plus grand diviseur de a et $a+1$ est 1.

$$\therefore \operatorname{pgcd}(a, a+1) = 1.$$

Réduction au cas de nombres premiers entre eux

Remarque

Si deux entiers a et b ne sont pas premiers entre eux, on peut se ramener à un cas équivalent en divisant par leur pgcd

Exemple Pour deux entiers quelconques $a, b \in \mathbb{Z}$, notons $d = \mathrm{pgcd}(a, b)$. On peut écrire :

$$a = a_0 d \quad \text{et} \quad b = b_0 d,$$

avec $a_0, b_0 \in \mathbb{Z}$ et $\mathrm{pgcd}(a_0, b_0) = 1$.

Utilité : Cette décomposition est souvent utilisée pour simplifier les calculs impliquant deux entiers.

Théorème de Bézout

Théorème de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe des entiers $u, v \in \mathbb{Z}$ tels que :

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

Théorème de Bézout

Théorème de Bézout

Soient $a, b \in \mathbb{Z}$. Il existe des entiers $u, v \in \mathbb{Z}$ tels que :

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

Remarques

- La preuve découle de l'algorithme d'Euclide.
- Les entiers u, v ne sont pas uniques.
- Ils sont appelés *coefficients de Bézout* et s'obtiennent en "remontant " l'algorithme d'Euclide.

Exemple : Calcul des coefficients de Bézout

Exemple

Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. Nous reprenons les calculs pour trouver $\mathrm{pgcd}(600, 124) = 4$.

Exemple : Calcul des coefficients de Bézout

Exemple

Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. Nous reprenons les calculs pour trouver $\mathrm{pgcd}(600, 124) = 4$.

Algorithme d'Euclide

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

Exemple : Calcul des coefficients de Bézout

remontée (droite)

$$\begin{aligned} 4 &= 104 - 20 \times 5, \\ 4 &= 104 - (124 - 104 \times 1) \times 5, \\ 4 &= 124 \times (-5) + 104 \times 6, \\ 4 &= 600 \times 6 + 124 \times (-29), \end{aligned}$$

Ainsi, pour $u = 6$ et $v = -29$, on a :

$$600 \times 6 + 124 \times (-29) = 4.$$

Corollaire

Si $d \mid a$ et $d \mid b$, alors $d \mid \mathrm{pgcd}(a, b)$.

Corollaire

Si $d \mid a$ et $d \mid b$, alors $d \mid \mathrm{pgcd}(a, b)$.

Exemple

$$4 \mid 16 \quad \text{et} \quad 4 \mid 24 \quad \text{donc} \quad 4 \mid \mathrm{pgcd}(16, 24) = 8.$$

Démonstration

- Par hypothèse, $d \mid au$ et $d \mid bv$.
- Donc $d \mid (au + bv)$.
- Par le théorème de Bézout, $au + bv = \mathrm{pgcd}(a, b)$.
- Ainsi, $d \mid \mathrm{pgcd}(a, b)$.

Corollaire 2 : Nombres premiers entre eux

Corollaire

Soient $a, b \in \mathbb{Z}$. a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1.$$

Démonstration

- **Sens $\Rightarrow$:** Si a et b sont premiers entre eux, alors par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \mathrm{pgcd}(a, b) = 1.$$

Démonstration

- **Sens $\Rightarrow$:** Si a et b sont premiers entre eux, alors par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \mathrm{pgcd}(a, b) = 1.$$

- **Sens $\Leftarrow$:** Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.
  - Comme $\mathrm{pgcd}(a, b) \mid a$, on a $\mathrm{pgcd}(a, b) \mid au$.
  - De même, $\mathrm{pgcd}(a, b) \mid bv$.
  - Ainsi, $\mathrm{pgcd}(a, b) \mid (au + bv) = 1$.
  - Donc $\mathrm{pgcd}(a, b) = 1$, ce qui montre que a et b sont premiers entre eux.

Lemme de Gauss

Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors :

$$a \mid c.$$

Lemme de Gauss

Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors :

$$a \mid c.$$

Exemple

Si $4 \mid 7 \cdot c$ et comme 4 et 7 sont premiers entre eux ($\text{pgcd}(4, 7) = 1$), alors :

$$4 \mid c.$$

Démonstration du Lemme de Gauss

Hypothèse : $\text{pgcd}(a, b) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1.$$

Démonstration du Lemme de Gauss

Hypothèse : $\text{pgcd}(a, b) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1.$$

En multipliant cette égalité par c, on obtient :

$$acu + bcv = c.$$

Démonstration du Lemme de Gauss

Hypothèse : $\text{pgcd}(a, b) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1.$$

En multipliant cette égalité par c, on obtient :

$$acu + bcv = c.$$

- Par hypothèse, $a \mid bcv$ car $a \mid bc$,
- De même, $a \mid acu$.

Démonstration du Lemme de Gauss

Hypothèse : $\text{pgcd}(a, b) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1.$$

En multipliant cette égalité par c, on obtient :

$$acu + bcv = c.$$

- Par hypothèse, $a \mid bcv$ car $a \mid bc$,
- De même, $a \mid acu$.

Puisque $a \mid acu$ et $a \mid bcv$, donc $a \mid (acu + bcv)$ et par suite

$$a \mid c.$$

Équations $ax + by = c$

Proposition

Considérons l'équation :

$$ax + by = c \quad (E)$$

où $a, b, c \in \mathbb{Z}$.

Équations $ax + by = c$

Proposition

Considérons l'équation :

$$ax + by = c \quad (E)$$

où $a, b, c \in \mathbb{Z}$.

1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $\text{pgcd}(a, b) \mid c$.

Équations $ax + by = c$

Proposition

Considérons l'équation :

$$ax + by = c \quad (E)$$

où $a, b, c \in \mathbb{Z}$.

1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $\text{pgcd}(a, b) \mid c$.
2. Si $\text{pgcd}(a, b) \mid c$, alors il existe une infinité de solutions entières qui sont exactement de la forme :

$$(x, y) = (x_0 + \alpha k, y_0 + \beta k),$$

où $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ sont fixés, et $k \in \mathbb{Z}$.

Exemple : Résolution de $161x + 368y = 115$ (suite)

Première étape : Y a-t-il des solutions ? Utilisons l'algorithme d'Euclide pour calculer $\text{pgcd}(161, 368)$.

$$368 = 161 \times 2 + 46,$$

$$161 = 46 \times 3 + 23,$$

$$46 = 23 \times 2 + 0.$$

Donc, $\text{pgcd}(161, 368) = 23$. Comme $115 = 5 \times 23$, on a bien $\text{pgcd}(161, 368) \mid 115$. Par le théorème de Bézout, l'équation (E) admet des solutions entières.

Exemple : Résolution de $161x + 368y = 115$ (suite)

Deuxième étape : Trouver une solution particulière. On utilise la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.

$$23 = 161 - 3 \times 46,$$

$$23 = 161 - 3 \times (368 - 2 \times 161),$$

$$23 = 7 \times 161 - 3 \times 368.$$

Donc, une solution particulière est $x_0 = 7$ et $y_0 = -3$.

Exemple : Résolution de $161x + 368y = 115$ (suite)

Troisième étape: Recherche de toutes les solutions Trouver toutes les solutions entières de $161x + 368y = 115$. Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E).

Exemple : Résolution de $161x + 368y = 115$ (suite)

Troisième étape: Recherche de toutes les solutions Trouver toutes les solutions entières de $161x + 368y = 115$. Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E).

Méthode : Partons de deux solutions (x_0, y_0) et (x, y). On a :

$$161x + 368y = 115 \quad \text{et} \quad 161x_0 + 368y_0 = 115.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Troisième étape: Recherche de toutes les solutions Trouver toutes les solutions entières de $161x + 368y = 115$. Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E).

Méthode : Partons de deux solutions (x_0, y_0) et (x, y). On a :

$$161x + 368y = 115 \quad \text{et} \quad 161x_0 + 368y_0 = 115.$$

En soustrayant les deux égalités :

$$161(x - x_0) + 368(y - y_0) = 0.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Factorisons par le $\text{pgcd}(161, 368) = 23$:

$$23 \cdot 7 \cdot (x - x_0) + 23 \cdot 16 \cdot (y - y_0) = 0.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Factorisons par le $\text{pgcd}(161, 368) = 23$:

$$23 \cdot 7 \cdot (x - x_0) + 23 \cdot 16 \cdot (y - y_0) = 0.$$

En divisant par 23 :

$$7(x - x_0) = -16(y - y_0). \quad (*)$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Factorisons par le $\text{pgcd}(161, 368) = 23$:

$$23 \cdot 7 \cdot (x - x_0) + 23 \cdot 16 \cdot (y - y_0) = 0.$$

En divisant par 23 :

$$7(x - x_0) = -16(y - y_0). \quad (*)$$

Comme $\text{pgcd}(7, 16) = 1$, en appliquant le lemme de Gauss, on aura $7 \mid (y - y_0)$.

Exemple : Résolution de $161x + 368y = 115$ (suite)

Factorisons par le $\text{pgcd}(161, 368) = 23$:

$$23 \cdot 7 \cdot (x - x_0) + 23 \cdot 16 \cdot (y - y_0) = 0.$$

En divisant par 23 :

$$7(x - x_0) = -16(y - y_0). \quad (*)$$

Comme $\text{pgcd}(7, 16) = 1$, en appliquant le lemme de Gauss, on aura $7 \mid (y - y_0)$. Il existe donc $k \in \mathbb{Z}$ tel que :

$$y - y_0 = 7k.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Substitution dans $(*)$**.** En remplaçant $y - y_0 = 7k$ dans $(*)$, on obtient :

$$7(x - x_0) = -16 \cdot 7k.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Substitution dans $(*)$**.** En remplaçant $y - y_0 = 7k$ dans $(*)$, on obtient :

$$7(x - x_0) = -16 \cdot 7k.$$

En simplifiant par 7 :

$$x - x_0 = -16k.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Substitution dans $(*)$**.** En remplaçant $y - y_0 = 7k$ dans $(*)$, on obtient :

$$7(x - x_0) = -16 \cdot 7k.$$

En simplifiant par 7 :

$$x - x_0 = -16k.$$

Solutions générales : Les solutions entières sont donc de la forme :

$$(x, y) = (x_0 - 16k, y_0 + 7k), \quad k \in \mathbb{Z}.$$

Autrement dit , puisque $(x_0, y_0) = (35, -16)$, alors

$$(x, y) = (35 - 16k, -15 + 7k), \quad k \in \mathbb{Z}.$$

Exemple : Résolution de $161x + 368y = 115$ (suite)

Vérification : Prenez une valeur de k au hasard et vérifiez que (x, y) satisfait $161x + 368y = 115$.

Exemple : Résolution de $161x + 368y = 115$ (suite)

Vérification : Prenez une valeur de k au hasard et vérifiez que (x, y) satisfait $161x + 368y = 115$.

Conclusion : Toutes les solutions de $161x + 368y = 115$ sont données par

$$(x, y) = (35 - 16k, -15 + 7k), \quad k \in \mathbb{Z}.$$

Congruences : Définition et propriétés

Définition

Soit $n > 2$ un entier. On dit que a est **congru** à b modulo n, si n divise $b - a$. On note alors :

$$a \equiv b \pmod{n}.$$

Une autre formulation équivalente est :

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z},\ a = b + kn.$$

Remarque

$n \mid a \iff a \equiv 0 \pmod{n}$.

Propriétés des congruences

- La relation " congru modulo n " est une **relation d'équivalence** :
  - **Réflexivité :** $a \equiv a \pmod{n}$,
  - **Symétrie :** Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$,
  - **Transitivité :** Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

Propriétés des congruences

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n}.$$

Propriétés des congruences

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n}.$$

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a \cdot c \equiv b \cdot d \pmod{n}.$$

Propriétés des congruences

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n}.$$

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a \cdot c \equiv b \cdot d \pmod{n}.$$

- Si $a \equiv b \pmod{n}$, alors pour tout $k > 0$:

$$a^k \equiv b^k \pmod{n}.$$

Exemples des congruences

- $15 \equiv 1 \pmod 7$,

Exemples des congruences

- $15 \equiv 1 \pmod 7$,
- $72 \equiv 2 \pmod 7$,
- $3 \equiv -11 \pmod 7$,
- $5x + 8 \equiv 3 \pmod 5$ pour tout $x \in \mathbb{Z}$.

Équation de congruence : $ax \equiv b \pmod{n}$

Proposition

Soient $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$, et $n > 2$. Considérons l'équation $ax \equiv b \pmod{n}$, où $x \in \mathbb{Z}$.

1. Il existe des solutions si et seulement si $\text{pgcd}(a, n) \mid b$.

Équation de congruence : $ax \equiv b \pmod{n}$

Proposition

Soient $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$, et $n > 2$. Considérons l'équation $ax \equiv b \pmod{n}$, où $x \in \mathbb{Z}$.

1. Il existe des solutions si et seulement si $\text{pgcd}(a, n) \mid b$.
2. Les solutions sont de la forme :

$$x = x_0 + \ell \cdot \frac{n}{\text{pgcd}(a, n)}, \quad \ell \in \mathbb{Z},$$

où x_0 est une solution particulière. Il existe donc $\text{pgcd}(a, n)$ classes de solutions.

Exemple: Résolution de $9x \equiv 6 \pmod{24}$

Étape 1 : Vérification de l'existence des solutions.

- Calculons $\text{pgcd}(9, 24)$ avec l'algorithme d'Euclide :

$$24 = 2 \times 9 + 6,$$

$$9 = 1 \times 6 + 3,$$

$$6 = 2 \times 3 + 0.$$

Exemple: Résolution de $9x \equiv 6 \pmod{24}$

Étape 1 : Vérification de l'existence des solutions.

- Calculons $\text{pgcd}(9, 24)$ avec l'algorithme d'Euclide :

$$24 = 2 \times 9 + 6,$$

$$9 = 1 \times 6 + 3,$$

$$6 = 2 \times 3 + 0.$$

- Ainsi, $\text{pgcd}(9, 24) = 3$, et comme $3 \mid 6$, l'équation admet des solutions.

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 2 : Réduction de l'équation.

- L'équation $9x \equiv 6 \pmod{24}$ équivaut à :

$$9x - 24k = 6, \quad \text{ou encore } 3x - 8k = 2.$$

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 2 : Réduction de l'équation.

- L'équation $9x \equiv 6 \pmod{24}$ équivaut à :

$$9x - 24k = 6, \quad \text{ou encore } 3x - 8k = 2.$$

- En divisant par le pgcd, on simplifie l'équation.

Étape 3 : Trouver une solution particulière.

- Par inspection, une solution particulière est $x_0 = 6$, $k_0 = 2$.

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 4 : Écrire les solutions générales.

- Si (x, k) est une solution, alors par soustraction :

$$3(x - x_0) - 8(k - k_0) = 0.$$

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 4 : Écrire les solutions générales.

- Si (x, k) est une solution, alors par soustraction :

$$3(x - x_0) - 8(k - k_0) = 0.$$

- D'après le lemme de Gauss, 8 $3(x - x_0)$ et comme $pgcd(3, 8) = 1$ alors

$$x = x_0 + 8\ell, \quad \ell \in \mathbb{Z}.$$

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 4 : Écrire les solutions générales.

- Si (x, k) est une solution, alors par soustraction :

$$3(x - x_0) - 8(k - k_0) = 0.$$

- D'après le lemme de Gauss, 8 $3(x - x_0)$ et comme $pgcd(3, 8) = 1$ alors

$$x = x_0 + 8\ell, \quad \ell \in \mathbb{Z}.$$

- Les solutions sont donc de la forme $x = 6 + 8\ell$.

Exemple: Résolution de $9x \equiv 6 \pmod{24}$ (suite)

Étape 5 : Regrouper les solutions en classes modulo 24.

- Les solutions $x = 6 + 8\ell$ peuvent être exprimées sous forme de 3 classes modulo 24

$$x_1 = 6 + 24m, \quad x_2 = 14 + 24m, \quad x_3 = 22 + 24m, \quad m \in \mathbb{Z}.$$

Autrement dit

$$\bar{x_1} = \bar{6},\ \bar{x_2} = \bar{14},\ \bar{x_3} = \bar{22}.$$

Petit théorème de Fermat

Théorème: Petit théorème de Fermat

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

$$a^p \equiv a \pmod{p}.$$

Petit théorème de Fermat

Théorème: Petit théorème de Fermat

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

$$a^p \equiv a \pmod{p}.$$

Corollaire

Si p ne divise pas a, alors :

$$a^{p-1} \equiv 1 \pmod{p}.$$

Propriété des coefficients binomiaux

Lemme

Si $1 \leq k \leq p-1$, alors :

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Propriété des coefficients binomiaux

Lemme

Si $1 \leq k \leq p-1$, alors :

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Démonstration

- Par définition :

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

Propriété des coefficients binomiaux

Lemme

Si $1 \leq k \leq p-1$, alors :

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Démonstration

- Par définition :

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

- Ainsi, $p! = k!(p-k)!\binom{p}{k}$, et donc $p \mid \binom{p}{k}$ si $p \mid p!$.

Propriété des coefficients binomiaux

Lemme

Si $1 \leq k \leq p-1$, alors :

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Démonstration

- Par définition :
$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$
- Ainsi, $p! = k!(p-k)!\binom{p}{k}$, et donc $p \mid \binom{p}{k}$ si $p \mid p!$.
- Comme $1 \leq k \leq p-1$, $k!$ et $(p-k)!$ ne contiennent aucun facteur divisible par p.

Propriété des coefficients binomiaux

Lemme

Si $1 \leq k \leq p-1$, alors :

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Démonstration

- Par définition :
$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$
- Ainsi, $p! = k!(p-k)!\binom{p}{k}$, et donc $p \mid \binom{p}{k}$ si $p \mid p!$.
- Comme $1 \leq k \leq p-1$, $k!$ et $(p-k)!$ ne contiennent aucun facteur divisible par p.
- Par le lemme d'Euclide, on conclut que $p \mid \binom{p}{k}$, d'où $\binom{p}{k} \equiv 0 \pmod{p}$.

Preuve du Petit théorème de Fermat

Preuve : Par récurrence sur $a > 0$.

- **Cas de base :** Si $a = 0$, alors :

$$0^p \equiv 0 \pmod{p}.$$

Preuve du Petit théorème de Fermat

Preuve : Par récurrence sur $a > 0$.

- **Cas de base :** Si $a = 0$, alors :

$$0^p \equiv 0 \pmod{p}.$$

- **Hypothèse de récurrence** Supposons que pour un $a > 0$, on ait :

$$a^p \equiv a \pmod{p}.$$

Preuve du Petit théorème de Fermat

Preuve : Par récurrence sur $a > 0$.

- **Cas de base :** Si $a = 0$, alors :

$$0^p \equiv 0 \pmod{p}.$$

- **Hypothèse de récurrence** Supposons que pour un $a > 0$, on ait :

$$a^p \equiv a \pmod{p}.$$

- **Étape de récurrence** Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

Preuve du Petit théorème de Fermat

Preuve : Par récurrence sur $a > 0$.

- **Cas de base :** Si $a = 0$, alors :

$$0^p \equiv 0 \pmod{p}.$$

- **Hypothèse de récurrence** Supposons que pour un $a > 0$, on ait :

$$a^p \equiv a \pmod{p}.$$

- **Étape de récurrence** Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

- Par le lemme précédent, $\binom{p}{k} \equiv 0 \pmod{p}$ pour $1 \leq k \leq p-1$, donc :

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

Preuve du Petit théorème de Fermat

Preuve : Par récurrence sur $a > 0$.

- **Cas de base :** Si $a = 0$, alors :

$$0^p \equiv 0 \pmod{p}.$$

- **Hypothèse de récurrence** Supposons que pour un $a > 0$, on ait :

$$a^p \equiv a \pmod{p}.$$

- **Étape de récurrence** Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

- Par le lemme précédent, $\binom{p}{k} \equiv 0 \pmod{p}$ pour $1 \leq k \leq p-1$, donc :

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

Conclusion du Petit théorème de Fermat

Conclusion Par récurrence, nous avons prouvé que pour tout $a \in \mathbb{Z}$ et tout nombre premier p :

$$a^p \equiv a \pmod{p}.$$

Conclusion du Petit théorème de Fermat

Conclusion Par récurrence, nous avons prouvé que pour tout $a \in \mathbb{Z}$ et tout nombre premier p :

$$a^p \equiv a \pmod{p}.$$

Corollaire : Si $p \nmid a$, alors :

$$a^{p-1} \equiv 1 \pmod{p}.$$