

L'ARITHMETIQUE

1) REPPEL

1) Divisibilité dans \mathbb{Z} .

Définition :

Soient a et b deux entiers relatifs tels que $b \neq 0$; on dit que l'entier relatif b divise a s'il existe un entier relatif k tel que $a = kb$; on écrit : $b|a$.

On dit que a est divisible par b ou a est un multiple de b

Définition :

- Si $b|m$ et $b|n$ on dit que b est un diviseur commun de m et n
- Si $b|m$ et $b'|m$, on dit que m est un multiple commun de b et b' .

Propriété :

Etant donné des entiers relatifs non nuls. On a les assertions suivantes :

- ① $\begin{cases} a|b \\ b|a \end{cases} \Rightarrow |a| = |b|$
- ② $\begin{cases} a|b \\ b|c \end{cases} \Rightarrow a|c$
- ③ $\begin{cases} a|m \\ a|n \end{cases} \Rightarrow a|\alpha m + \beta n$ où α et β sont des entiers relatifs quelconques.

Application :

Soient $a_n = 2n + 1$ et $b_n = 5n + 4$

1- Montrer que tout diviseur commun de a_n et b_n divise 3.

2- Déterminer tous les diviseurs communs de a_n et b_n

Propriété :

- ① $\begin{cases} d|a \\ \delta|b \end{cases} \Rightarrow d\delta|ab$
- ② $a|b \Leftrightarrow a^n|b^n$
- ③ $\begin{cases} d|a \\ d|a+b \end{cases} \Rightarrow d|b$

2) Division Euclidienne

Propriété :

Considérons a et b deux entiers relatifs tels que $b \neq 0$ ils existent un entiers relatif q et un entier naturel r tels que : $a = bq + r$ où $0 \leq r < |b|$

- L'entier a s'appelle : **Le divisé**
- L'entier b s'appelle : **Le diviseur**
- L'entier q s'appelle : **Le quotient**
- L'entier r s'appelle : **Le reste**

Exercice 1 :

Montrer que le reste de la division euclidienne de n^2 par 3 ne peut pas être égale à 2.

Exercice 2 :

a) Montrer que tout nombre premier s'écrit de la forme $p = 6n + 1$ ou $p = 6n + 5$

b) L'inverse est-il vraie ?

3) Les nombres premiers

Définitions

- On dit que l'entier d est un diviseur **effectif** de l'entier relatif a si $d|a$ et $|d| \neq 1$ et $|d| \neq |a|$
- On dit qu'un entier relatif non nul p est **premier** s'il est différent de 1 et s'il n'admet pas de diviseurs effectifs.

Remarque :

- Un nombre premier p admet exactement deux diviseurs positifs 1 et $|p|$.

- Si p est un nombre premier positif alors p n'admet pas de diviseurs effectifs de même $-p$ n'admet pas de diviseurs effectif d'où : $-p$ est aussi premier ;
Pour l'étude des nombres premiers on se contente d'étudier les nombres premiers positifs.

Propriété :

Soit a un entier naturel non nul différent de 1 et non premier, le plus petit diviseur de a différent de 1 est un nombre premier

Propriété :

Soit n un entier naturel non nul, différent de 1 et non premier, il existe un nombre premier p qui divise l'entier n et qui vérifie $p^2 \leq n$.

Remarque :

Cette propriété nous permet de déterminer si un nombre est premier ou non.

Corolaire :

Si un entier n n'est divisible par aucun entier premier p et qui vérifie $p^2 \leq n$ alors n est premier.

Crible d'Eratosthène. Les nombres premiers inférieurs à 100

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Application : Montrer que le nombre 2003 est premier.

Théorème :

L'ensemble des nombres premiers est infini.

4) Plus grand diviseurs commun**Définition :**

On dit que le nombre d est le **plus grand diviseur commun** de deux entiers relatifs a et b lorsque d divise a et d divise b et qu'il n'y a pas d'autre plus grands diviseurs de ces deux nombres. On note $d = PGDC(a, b) = a \wedge b$

Propriétés :

- $a \wedge a = |a|$
- $1 \wedge a = 1$
- $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- Si $b|a$ alors $a \wedge b = |b|$
- $\begin{cases} d|a \\ d|b \end{cases} \Rightarrow d|(a \wedge b)$
- $a \wedge b = a \wedge (a - b)$

Exercice :

- 1- Montrer que tout diviseur commun de $a = 2n + 3$ et $b = 5n + 1$ est un diviseur de 13
- 2- Déterminer tous les diviseurs commun de a et b .
- 3- Déterminer les valeurs de n pour lesquels $a \wedge b = 13$.

Définition :

On dit que deux entiers relatifs a et b sont premiers entre eux si $a \wedge b = 1$.

5) L'algorithme d'Euclide.**Théorème :**

Soit a un entier naturel et b un entier naturel non nul on a : $a = bq + r$ où $0 \leq r < b$ on a : $a \wedge b = b \wedge r$

L'algorithmme d'Euclide.

Soient a et b deux entiers naturels ($b \neq 0$) on a :

$$a = bq_1 + r_1 \text{ si } r_1 \neq 0 \text{ alors :}$$

$$b = r_1q_2 + r_2 \text{ si } r_2 \neq 0 \text{ alors :}$$

$$r_1 = r_2q_3 + r_3 \text{ si } r_3 \neq 0 \text{ alors :}$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n \text{ si } r_n \neq 0 \text{ alors :}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1} \text{ si } r_{n+1} = 0 \text{ on arrête le processus.}$$

Et d'après la propriété précédente : $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$ car : $r_n | r_{n-1}$

Propriété :

Soient a et b deux entiers naturels non nuls.

Le plus grand diviseur commun de a et b est le dernier reste non nul dans les divisions euclidiennes successives.

Application :

1- Trouver le PGDC(362154, 82350).

2- Déterminer tous les diviseurs communs de 362154 et 82350.

Propriété :

Soient a et b deux entiers relatifs non nuls et $\delta = a \wedge b$, on a les diviseurs communs de a et b sont les diviseurs de δ . On peut dire que : $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_{a \wedge b}$

6) Le plus petit multiple commun.**Définition :**

On dit que le nombre entier naturel m est le **plus petit multiple commun** de deux entiers relatifs a et b lorsque m est un multiple de a et de b et qu'il n'y a pas d'autre plus petit multiple non nuls de ces deux nombres. On note : $m = PPCM(a, b) = a \vee b$

Propriétés :

- $a \vee a = |a|$
- $a \vee b = b \vee a$
- $a \vee 1 = |a|$
- Si $b|a$ alors $a \vee b = |a|$
- $a \vee (b \vee c) = (a \vee b) \vee c$
- $a|(a \vee b)$; $b|(a \vee b)$ et $(a \vee b)|ab$

Propriété :

Considérons a et b deux entiers relatifs.

Si $a \vee b = m$ et M un multiple commun de a et b alors $m|M$.

7) la congruence modulo n .**Définition :**

Soient a et b deux entiers relatifs ; et n un entier naturel non nul. on dit que : **a est congrue à b modulo n** si $n|(b - a)$. On écrit : $a \equiv b \pmod{n}$

Propriété :

Si $a \equiv b \pmod{n}$ alors a et b ont le même reste de la division euclidienne sur n

Propriété fondamentale :

- $(\forall a \in \mathbb{Z})(a \equiv a \pmod{n})$ on dit que la relation de congruence est **réflexive**.
- $(\forall (a, b) \in \mathbb{Z}^2)(a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n})$, on dit que la relation de congruence est **symétrique**.
- $(\forall (a, b, c) \in \mathbb{Z}^3) \left(\begin{matrix} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{matrix} \Rightarrow a \equiv c \pmod{n} \right)$, on dit que la relation de congruence est **transitive**.

Définition :

Puisque la relation de congruence est réflexive, symétrique et transitive on dit que la relation de congruence est une **relation d'équivalence**

Propriété et définition :

Soit n un entier naturel non nul. Si $a \equiv b [n]$ et $c \equiv d [n]$ alors ;

- $a + c \equiv b + d [n]$; On dit que la relation de congruence est compatible avec l'addition dans \mathbb{Z}
- $ac \equiv bd [n]$; On dit que la relation de congruence est compatible avec la multiplication dans \mathbb{Z}

Corolaire :

Si $a \equiv b [n]$ alors pour tout k dans \mathbb{N} on a : $a^k \equiv b^k [n]$

Applications

- 1 Déterminer le reste de la division euclidienne de 4587^{2018} par 9
- 2 Déterminer le reste de la division euclidienne de 25614^{6512} par 13
- 3 Montrer que pour tout n entier naturel : $3^{2n+1} + 2^{n+2}$ est divisible par 7
- 4 Montrer que pour tout n entier naturel, $5n^3 + n$ est divisible par 6
- 5 Montrer que si n n'est pas un multiple de 7, alors : $n^6 - 1$ est un multiple de 7
- 6 Montrer que pour tout entier naturel, le nombre $n(n^2 + 5)$ est divisible par 6

8) Les classes d'équivalences.**Définition :**

Soit n un entier naturel non nul. L'ensemble des entiers relatifs qui ont le même reste r de la division euclidienne par n s'appelle **la classe d'équivalence de r** et se note : \bar{r} ou \dot{r}

$$\bar{r} = \{m \in \mathbb{Z} / m \equiv r [n]\} = \{nk + r \text{ où } k \in \mathbb{Z}\}$$

Définition :

Soit n un entier naturel non nul. On définit dans $\mathbb{Z}/n\mathbb{Z}$ les deux lois :

- **L'addition** : On pose : $\bar{a} + \bar{b} = \overline{a + b}$
- **La multiplication** : On pose : $\bar{a} \times \bar{b} = \overline{a \times b}$

Exemple :

Dans $\mathbb{Z}/6\mathbb{Z}$: $\bar{3} \times \bar{4} = \bar{0}$ $\bar{5} + \bar{4} = \bar{3}$

Exercice :

1- Dresser les tables des opérations de $\mathbb{Z}/7\mathbb{Z}$

2- Résoudre dans $\mathbb{Z}/7\mathbb{Z}$ les équations :

a) $\bar{2}x = \bar{1}$ b) $\bar{4}x + \bar{1} = x + \bar{3}$ c) $\bar{5}x^2 + \bar{3}x + \bar{1} = \bar{0}$

9) Décomposition d'un entier en facteurs des nombres premiers**Théorème :**

- Chaque entier **naturel** m non nul s'écrit d'une façon unique comme le produit des facteurs premiers comme suite : $m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^n p_k^{\alpha_k}$
- Chaque entier **relatif** m non nul s'écrit d'une façon unique comme le produit des facteurs premiers comme suite : $m = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \varepsilon \prod_{k=1}^n p_k^{\alpha_k}$ où $\varepsilon \in \{-1, 1\}$

Propriété 1:

Soit a un entier relatif dont la décomposition est de la forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$; un entier d non nul divise l'entier a si et seulement si d à une décomposition de la forme :

$$d = \varepsilon' p_1^{\delta_1} \times p_2^{\delta_2} \times p_3^{\delta_3} \times \dots \times p_n^{\delta_n} \text{ où } (\forall i \in \llbracket 1, n \rrbracket)(0 \leq \delta_i \leq \alpha_i)$$

Soit a un entier relatif dont la décomposition est de la forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$ et $d = \varepsilon' p_1^{\delta_1} \times p_2^{\delta_2} \times p_3^{\delta_3} \times \dots \times p_n^{\delta_n}$ un diviseur de a le nombre des valeurs possibles de δ_i est $\alpha_i + 1$

On en déduit que :

Propriété 2:

Si $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$ est un entier, le nombre des diviseurs de a est : $2(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1)$

Application :

1- Décomposer le nombre 2975 en facteurs des nombres premiers

2- Déterminer le nombre des diviseurs de 2975.

3- Déterminer tous les diviseurs positifs de 2975.

Propriété 3 :

Soit a un entier relatif dont la décomposition est de la forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$; un entier m est un multiple de a si et seulement si $m = \varepsilon' p_1^{\mu_1} \times p_2^{\mu_2} \times p_3^{\mu_3} \times \dots \times p_n^{\mu_n}$ où $(\forall i \in \llbracket 1, n \rrbracket)(\alpha_i \leq \mu_i)$

9.1 Le P.G.C.D de deux nombres.

Soient $a = \varepsilon \prod_{k=1}^n p_k^{\alpha_k}$ et $b = \varepsilon' \prod_{k=1}^n p_k^{\beta_k}$ deux entiers ; si $d = \varepsilon'' \prod_{k=1}^n p_k^{\delta_k}$ est un diviseur commun de a et b alors :

$$(\forall k \in \llbracket 1, n \rrbracket) \begin{cases} 0 \leq \delta_k \leq \alpha_k \\ 0 \leq \delta_k \leq \beta_k \end{cases}$$

On en déduit que le P.G.C.D (a, b) est l'entier $\delta = \prod_{k=1}^n p_k^{\delta_k}$ où $(\forall k \in \llbracket 1, n \rrbracket)(\delta_k = \inf(\alpha_k, \beta_k))$

Propriété :

Si $a = \varepsilon \prod_{k=1}^n p_k^{\alpha_k}$ et $b = \varepsilon' \prod_{k=1}^n p_k^{\beta_k}$ deux entiers alors $a \wedge b = \prod_{k=1}^n p_k^{\inf(\alpha_k, \beta_k)}$

Exercice :

1- Décomposer les nombres 362154 et 82350 en produit des facteurs premiers

2- Déterminer le P.G.C.D de 362154 et 82350

3- Déterminer tous les diviseurs communs de 362154 et 82350

9.2 Le P.P.C.M de deux nombres.

Soient $a = \varepsilon \prod_{k=1}^n p_k^{\alpha_k}$ et $b = \varepsilon' \prod_{k=1}^n p_k^{\beta_k}$ deux entiers ; si $m = \varepsilon'' \prod_{k=1}^n p_k^{\mu_k}$ est un multiple commun de a et b alors :

$$(\forall k \in \llbracket 1, n \rrbracket) \begin{cases} \alpha_k \leq \mu_k \\ \beta_k \leq \mu_k \end{cases}$$

On en déduit que le P.P.C.M (a, b) est l'entier $\mu = \prod_{k=1}^n p_k^{\mu_k}$ où $(\forall k \in \llbracket 1, n \rrbracket)(\mu_k = \sup(\alpha_k, \beta_k))$

Propriété :

Si $a = \varepsilon \prod_{k=1}^n p_k^{\alpha_k}$ et $b = \varepsilon' \prod_{k=1}^n p_k^{\beta_k}$ deux entiers alors $a \vee b = \prod_{k=1}^n p_k^{\sup(\alpha_k, \beta_k)}$

Propriété :

Soient a et b deux entiers relatifs non nuls, on a les assertions suivantes :

- $(a \wedge b) \times (a \vee b) = |ab|$
- $ca \vee cb = c(a \vee b)$
- $ca \wedge cb = c(a \wedge b)$

Exercice :

Si $d|a$ et $d|b$ alors : $d|(a \wedge b)$.

II) THEOREMES PRINCIPAUX.

1) Théorème de Bézout :

Théorème 1 :

Soient a et b et des entiers relatifs non nuls :

$$a \wedge b = d \Leftrightarrow \exists (\alpha, \beta) \in \mathbb{Z}^2 ; \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \wedge \beta = 1 \end{cases}$$

Preuve :

(\Rightarrow) On suppose que $a \wedge b = d$

On a $d|a$ et $d|b$ donc $\exists (\alpha, \beta) \in \mathbb{Z}^2$ tel que : $a = \alpha d$ et $b = \beta d$ donc :

$$\begin{aligned} d &= \alpha d \wedge \beta d \\ &= |d|(\alpha \wedge \beta) \text{ et puisque } d \in \mathbb{N}^* \text{ alors } \alpha \wedge \beta = 1 \end{aligned}$$

(\Leftarrow) On suppose que $\exists (\alpha, \beta) \in \mathbb{Z}^2 ; \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \wedge \beta = 1 \end{cases}$ On a :

$$a \wedge b = \alpha d \wedge \beta d = |d|(\alpha \wedge \beta) = d \text{ car } (|d| = d \text{ et } \alpha \wedge \beta = 1)$$

Théorème 2 :

Soient a et b et des entiers relatifs non nuls : $a \wedge b = d \Rightarrow \exists(u, v) \in \mathbb{Z}^2 ; d = au + bv$

Preuve :

1- Si $a|b$ alors $a \wedge b = |b|$

- si $b > 0$ alors $b = 0a + 1b$
- si $b < 0$ alors $b = 0a + (-1)b$

2- Si $b|a$ (même raisonnement)

3- On suppose que $b \nmid a$ tel que $0 < b < a$

d'après l'algorithme d'Euclide on a

$$a = bq_0 + r_0 \text{ si } r_0 \neq 0 \text{ alors :}$$

$$b = r_0q_1 + r_1 \text{ si } r_1 \neq 0 \text{ alors :}$$

$$r_0 = r_1q_2 + r_2 \text{ si } r_2 \neq 0 \text{ alors :}$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n \text{ si } r_n \neq 0 \text{ alors :}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1} \text{ si } r_{n+1} = 0 \text{ on arrête le processus .}$$

Et d'après la propriété précédente : $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$ car : $r_n | r_{n-1}$

et $0 < r_n < r_{n-1} < \dots < r_1 < r_0 < b$

On obtient :

$$r_0 = a - bq_0 = u_0a + v_0b \text{ où } u_0 = 1 \text{ et } v_0 = -q_0$$

$$r_1 = b - r_0q_1 = b - (a - bq_0)q_1 = -aq_1 + b(1 + q_0q_1) = u_1a + v_1b \text{ où } u_1 = -q_1 \text{ et } v_1 = (1 + q_0q_1)$$

On répète le processus et à chaque fois on montre que : $r_k = au_k + bv_k$ cette opération est valable pour tous les reste r_k en particulier pour le dernier reste r_n qui est $a \wedge b$ donc : $\exists(u_n, v_n) \in \mathbb{Z}^2 ; a \wedge b = au_n + bv_n$.

Remarque

- Dans l'écriture $\exists(u, v) \in \mathbb{Z}^2 ; a \wedge b = au + bv$ le couple (u, v) n'est pas unique.
 $12 \wedge 9 = 3$ on a $3 = 1 \times 12 + (-1) \times 9$ et $3 = (-2) \times 12 + 3 \times 9$
- La réciproque du théorème n'est pas vraie :
 $2 \times 12 + (-2) \times 9 = 6$ mais $12 \wedge 9 = 3 \neq 6$

Théorème (Théorème de Bézout)

Soient a et b et des entiers relatifs non nuls : $a \wedge b = 1 \Leftrightarrow \exists(u, v) \in \mathbb{Z}^2 ; 1 = au + bv$

(\Rightarrow) C'est le théorème précédent.

(\Leftarrow) On suppose que $1 = au + bv$

Soit $d = a \wedge b$ on aura : $\begin{cases} d|a \\ d|b \end{cases}$ donc $\begin{cases} d|ua \\ d|vb \end{cases}$ par suite $d|ua + vb = 1$ donc $d = 1$ ($d \in \mathbb{N}^*$)

et donc $a \wedge b = 1$

Exemples :

- $(5n + 3) \wedge (2n + 1) = 1$ car : $2 \times (5n + 3) + (-5) \times (2n + 1) = 1$
- $(n + 2) \wedge (n^2 + 2n - 1) = 1$ car $n \times (n + 2) + (-1) \times (n^2 + 2n - 1) = 1$

Application :

❶ L'utilisation de l'algorithme d'Euclide pour déterminer les coefficients de *Bezout*

Montrons que : $360 \wedge 84 = 12$ et déterminons u et v dans \mathbb{Z} tels que $360u + 84v = 12$

on a : $360 = 2^3 \cdot 3^2 \cdot 5$ et $84 = 2^2 \cdot 3 \cdot 7$ donc $360 \wedge 84 = 2^2 \cdot 3 = 12$

D'autre part :

$$360 = 84 \times 4 + \boxed{24} \longrightarrow 24 = \boxed{a - (b \times 4)}$$

$$84 = 24 \times 3 + \boxed{12} \longrightarrow b - \left(\overset{24}{\overbrace{a - (b \times 4)}} \right) \times 3 = 12$$

$$24 = 12 \times 2 + 0$$

$$\text{Donc : } -3a + 13b = 12$$

❶ Considérons dans \mathbb{Z}^2 l'équation (E): $17x + 36y = 1$ et déterminons une solution particulière de (E).

On a $17 \wedge 36 = 1$ donc d'après le théorème de Bézout ; il existe u et v tels que : $17u + 36v = 1$ donc (E) admet une solution.

On pose $a = 36$ et $b = 17$ on obtient :

$$a = 2b + 2$$

$$b = 8 \times 2 + 1$$

$$\text{Donc : } 2 = a - 2b \text{ et } b = 8 \times (a - 2b) + 1$$

D'où : $-8a + 17b = 1$ donc le couple $(-8, 17)$ est une solution de l'équation (E).

2) Application du théorème de Bézout :

Théorème de Gauss

$$\text{Soient } a, b \text{ et } c \text{ des entiers relatifs non nuls : } \begin{cases} c|ab \\ c \wedge b = 1 \end{cases} \Rightarrow c|a$$

Preuve :

On a : $c \wedge a = 1$ d'après le théorème de Bézout : $(\exists(u, v) \in \mathbb{Z}^2)(au + vc = 1)$ d'où $bau + bvc = b$

Et puis que $c|ab$ alors $ab = kc$ (où $k \in \mathbb{Z}$) donc $kcu + bvc = b$ d'où $c(ku + bv) = b$ et $ku + bv \in \mathbb{Z}$ donc $c|b$.

Remarque :

La condition $c \wedge b = 1$ dans le théorème de Gauss est indispensable ; $6|4 \times 3$ mais $6 \nmid 3$ et $6 \nmid 4$

Théorème

$$\text{Soient } a, b \text{ et } c \text{ des entiers relatifs non nuls : } \begin{cases} a|c \text{ et } b|c \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c$$

Preuve :

On a : $a|c$ et $b|c$ donc ils existent k et h tels que : $c = ka = hb$ et puisque $a \wedge b = 1$ alors :

$$(\exists(u, v) \in \mathbb{Z}^2)(au + vb = 1)$$

$$\begin{aligned} \text{Donc : (on multiplie par } c) \quad c &= cau + cvb \\ &= hbau + kavb \\ &= ab(hu + kv) \text{ et par suite } ab|c \end{aligned}$$

Remarque :

La condition $c \wedge b = 1$ dans le théorème précédent est indispensable ; $6|12$ et $3|12$ mais $6 \times 3 = 18 \nmid 12$.

Propriétés :

Soient a, b et c des entiers relatifs non nuls :

$$\text{❶ } \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge bc = 1 \quad \text{❷ } a \wedge b = 1 \Leftrightarrow a \wedge b^n = 1 \quad \text{❸ } a \wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1 \quad (n \in \mathbb{N}^*)$$

Preuve :

❶

$$(\Rightarrow) \text{ On suppose que } \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \text{ donc : } \begin{cases} (\exists(u, v) \in \mathbb{Z}^2)(au + vb = 1) \\ (\exists(\alpha, \beta) \in \mathbb{Z}^2)(a\alpha + \beta c = 1) \end{cases}$$

Par le produit on obtient : $(au + vb)(a\alpha + \beta c) = 1$; d'où après développement on obtient :

$$a^2u\alpha + au\beta c + vb\alpha a + vb\beta c = 1 \text{ et donc } (au\alpha + u\beta c + vb\alpha)a + (v\beta)bc = 1 \text{ donc et d'après Bézout } a \wedge bc = 1$$

$$(\Leftarrow) \text{ On suppose que } a \wedge bc = 1 \text{ donc } (\exists(u, v) \in \mathbb{Z}^2)(au + vbc = 1)$$

$$\text{D'où } au + (vb)c = 1 \text{ donc } a \wedge c = 1 \text{ et } au + (vc)b = 1 \text{ donc } a \wedge b = 1$$

②

(\Rightarrow) On suppose que $a \wedge b = 1$ et on montre par récurrence que : $a \wedge b^n = 1$

- Pour $n = 1$ la propriété est vraie.
- On suppose que la propriété est vraie pour n
- On montre qu'elle est vraie pour $n + 1$

On a : $\begin{cases} a \wedge b^n = 1 \\ a \wedge b = 1 \end{cases}$ donc et d'après ① on a : $a \wedge bb^n = 1$ d'où $a \wedge b^{n+1} = 1$

Donc si $a \wedge b = 1$ alors $a \wedge b^n = 1$ pour tout n dans \mathbb{N}^* .

(\Leftarrow)

On suppose que $a \wedge b^n = 1$ donc et d'après le théorème de Bézout ($\exists(u, v) \in \mathbb{Z}^2$)($au + vb^n = 1$)

Donc : $au + (vb^{n-1})b = 1$ donc ($\exists(u', v') \in \mathbb{Z}^2$)($au' + v'b = 1$) et par suite $a \wedge b = 1$

③ Est un résultat immédiat de ②.

3) L'équation $ax + by = c$

Théorème : (fondamental)

L'équation (E) : $ax + by = c$ admet une solution si et seulement si $(a \wedge b) | c$

Preuve :

- On suppose que $d = (a \wedge b) | c$ alors : ($\exists k \in \mathbb{Z}$)($c = kd$) et on a : ($\exists(u, v) \in \mathbb{Z}^2$)($au + vb = d$)
 $kd = k(a \wedge b) = (ku)a + (kv)b$

C'est-à-dire : $c = (ku)a + (kv)b$ donc l'équation (E) admet (x_0, y_0) comme solution où $\begin{cases} x_0 = ku \\ y_0 = kv \end{cases}$

- Inversement : On suppose que : $ax + by = c$ admet une solution (x_0, y_0) , donc :

$ax_0 + by_0 = c$ puisque : $\begin{cases} (a \wedge b) | a \\ (a \wedge b) | b \end{cases}$ alors $\begin{cases} (a \wedge b) | x_0 a \\ (a \wedge b) | y_0 b \end{cases}$ donc $(a \wedge b) | (ax_0 + by_0) = c$ donc : $(a \wedge b) | c$.

Théorème :

Si le couple (x_0, y_0) est une solution de l'équation (E) : $ax + by = c$ alors, l'ensemble des solutions de (E) est : $S = \left\{ \left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b} \right) / k \in \mathbb{Z} \right\}$

Démonstration :

On pose : $A = \left\{ \left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b} \right) / k \in \mathbb{Z} \right\}$ et on montre que $\begin{cases} A \subset S \\ S \subset A \end{cases}$

- Montrons que $A \subset S$: il suffit de montrer que le couple $\left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b} \right)$ est solution de l'équation (E) :

$$\begin{aligned} \text{On a : } a \left(x_0 + \frac{kb}{a \wedge b} \right) + b \left(y_0 - \frac{ka}{a \wedge b} \right) &= ax_0 + \frac{akb}{a \wedge b} + by_0 - \frac{bka}{a \wedge b} \\ &= ax_0 + by_0 = c \end{aligned}$$

Donc le couple $\left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b} \right)$ (pour $k \in \mathbb{Z}$) est solution : d'où : $A \subset S$.

- Inversement : On suppose que le couple $(x, y) \in S$

Donc (x, y) es solution de l'équation (E) d'où $ax + by = c$; or : (x_0, y_0) est une solution de l'équation (E) , donc : $ax_0 + by_0 = c$ donc (différence membre à membre) $a(x - x_0) = -b(y - y_0)$

Soit $d = a \wedge b$ on a : ($\exists(\alpha, \beta) \in \mathbb{Z}^2$) $\begin{cases} a = \alpha d & \text{et } b = \beta d \\ \alpha \wedge \beta = 1 \end{cases}$

Donc :

$$\begin{aligned} (x, y) \in S &\Leftrightarrow a(x - x_0) = -b(y - y_0) \\ &\Leftrightarrow \alpha d(x - x_0) = -\beta d(y - y_0) \\ &\Leftrightarrow \alpha(x - x_0) = -\beta(y - y_0) \quad (*) \quad (d \neq 0) \end{aligned}$$

On conclut que : $\beta | \alpha(x - x_0)$ et puisque : $\alpha \wedge \beta = 1$ alors (d'après T. Gauss) $\beta | (x - x_0)$

Donc ($\exists k \in \mathbb{Z}$)($(x - x_0) = k\beta$) et par suite : (*) $ak\beta = -\beta(y - y_0)$ d'où : $y - y_0 = -k\alpha$

Par suite : $(x, y) \in S \Leftrightarrow \begin{cases} (y - y_0) = -k\alpha \\ (x - x_0) = k\beta \end{cases}$ où $k \in \mathbb{Z}$ en remplaçant $\begin{cases} \alpha & \text{par } \frac{a}{d} \\ \beta & \text{par } \frac{b}{d} \end{cases}$ on obtient :

$$(x, y) \in S \Leftrightarrow x = x_0 + \frac{kb}{d} \text{ et } y = y_0 - \frac{ka}{d} \text{ C.Q.F.D.}$$

Exemple :

Considérons l'équation (E): $756x - 245y = 14$

- 1- Montrer l'équation (E) admet une solution.
- 2- Déterminer une solution particulière de (E)
- 3- Résoudre l'équation (E)

Solution :

$$756 = 2^2 \times 3^3 \times 7 \text{ et } 245 = 5 \times 7^2$$

1- On a : $756 \wedge 245 = 7$ et $7|14$ donc l'équation (E) admet une solution dans \mathbb{Z}^2 .

2- En utilisant l'algorithme d'Euclide on obtient $a = 756$ et $b = 245$

$$a = 3 \times b + 21$$

$$b = 11 \times 21 + 14$$

$$21 = 14 + 7$$

On a donc :

$$21 = a - 3b$$

$$b = 11 \times (a - 3b) + 14 \Leftrightarrow 14 = 34b - 11a$$

$$7 = (a - 3b) - (34b - 11a) \Leftrightarrow 7 = 12a - 37b$$

Finalement :

$14 = 24a - 74b$ et donc le couple $(24, 74)$ est une solution particulière de (E) d'où

$$S = \left\{ \left(24 - \frac{k \times 245}{7}, 74 - \frac{k \times 756}{7} \right) / k \in \mathbb{Z} \right\} = \{(24 - 35k, 74 - 108k) / k \in \mathbb{Z}\} = \{(24 + 35k, 74 + 108k) / k \in \mathbb{Z}\}$$

4) La congruence modulo n , complément.**Théorème :**

Soient a, b et c des entiers relatifs non nuls. et $n \in \mathbb{N}^*$ et $d = n \wedge c$ on a : $ac \equiv bc [n] \Leftrightarrow a \equiv b \left[\frac{n}{d} \right]$

Preuve :

(\Rightarrow)

On suppose : $ac \equiv bc [n]$, donc $n|(ac - bc) = c(a - b)$ donc $\frac{n}{d} | \frac{c}{d}(a - b)$ et comme $\frac{n}{d} \wedge \frac{c}{d} = 1$

Alors : (D'après théorème de Gauss)

$$\frac{n}{d} | (a - b) \text{ donc : } a \equiv b \left[\frac{n}{d} \right]$$

(\Leftarrow)

On suppose que : $a \equiv b \left[\frac{n}{d} \right]$ donc $a = b + k \frac{n}{d}$ ($k \in \mathbb{Z}$) donc $da = db + kn$ ($d = n \wedge c \Rightarrow c = \alpha d$)

Donc : $ada = \alpha db + akn$ d'où $ca = cb + hn$ donc $ac \equiv bc [n]$.

Propriété :

① $\begin{cases} ac \equiv bc [n] \\ c \wedge n = 1 \end{cases} \Rightarrow a \equiv b [n]$ ② $\begin{cases} a \equiv b [n] \\ m|n \end{cases} \Rightarrow a \equiv b [m]$ ③ $\begin{cases} ac \equiv bc [p] \\ p \text{ premier et } p \nmid c \end{cases} \Rightarrow a \equiv b [m]$

Preuve :

Ce sont des résultats immédiats du théorème précédent.

5) Le P.G.D.C et le P.P.M.C de plusieurs nombres.**Définition :**

Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls, le plus grand entier naturel d qui divise en même temps tous les nombres a_1, a_2, \dots, a_n s'appelle le plus grand diviseur commun des nombres a_1, a_2, \dots, a_n et se note :

$$d = a_1 \wedge a_2 \wedge \dots \wedge a_n$$

Théorème :

Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls ; on a :

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = (a_1 \wedge a_2 \wedge \dots \wedge a_{n-2}) \wedge (a_{n-1} \wedge a_n)$$

Exemple :

$$756 \wedge 350 \wedge 616 = 756 \wedge (350 \wedge 616) = 756 \wedge 14 = 14$$

Théorème (Généralisation de Bézout)

$$\text{Si } d = a_1 \wedge a_2 \wedge \dots \wedge a_n \text{ alors } \exists (\alpha_i)_{1 \leq i \leq n} \text{ telle que : } d = \sum_{i=1}^n \alpha_i a_i$$

Preuve : par récurrence

Définition :

$$\text{On dit que les entiers relatifs non nuls } a_1, a_2, \dots, a_n \text{ sont premiers entre eux si } a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$$

Remarque :

Les entiers relatifs non nuls a_1, a_2, \dots, a_n sont premiers entre eux ne veut pas dire que les entiers a_1, a_2, \dots, a_n sont premiers entre eux deux à deux.

Exemple :

3, 5 et 6 sont premiers entre eux.

Théorème (Généralisation de Bézout)

$$\text{Si } a_1 \wedge a_2 \wedge \dots \wedge a_n = 1 \text{ si et seulement si } \exists (u_i)_{1 \leq i \leq n} \text{ telle que : } 1 = \sum_{i=1}^n u_i a_i$$

Définition :

Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls, le plus petit entier naturel m qui est multiple en même temps tous les nombres a_1, a_2, \dots, a_n s'appelle le plus grand diviseur commun des nombres a_1, a_2, \dots, a_n et se note : $d = a_1 \vee a_2 \vee \dots \vee a_n$

6) Propriétés des nombres premiers.

Théorème :

- ① Si p et q sont des nombres premiers positifs alors ils sont premier entre eux.
- ② Si p est premier alors il est premier avec tout nombre entier non nul a tel que $p \nmid a$

Preuve : En exercice.

Remarque :

La réciproque de ① n'est pas vraie ; 14 et 9 sont premiers entre eux mais aucun d'eux n'est premiers.

Propriétés :

$$\begin{aligned} \textcircled{1} \left\{ \begin{array}{l} p \text{ premier} \\ p|ab \Rightarrow p|b \\ p \nmid a \end{array} \right. & \quad \textcircled{2} \left\{ \begin{array}{l} p \text{ premier} \\ p|ab \Rightarrow p|a \text{ ou } p|b \end{array} \right. & \quad \textcircled{3} \left\{ \begin{array}{l} p \text{ premier} \\ p|a_1 a_2 \dots a_n \Rightarrow \exists i \in \{1, 2, \dots, n\} p|a_i \end{array} \right. \\ \textcircled{4} \left\{ \begin{array}{l} \forall i \in \{1, 2, \dots, n\}; p_i \text{ premier} \\ p \text{ premier} \\ p|p_1 p_2 \dots p_n \end{array} \right. & \Rightarrow \exists i \in \{1, 2, \dots, n\} p = p_i \end{aligned}$$

Preuve : Résultat du théorème de Gauss.

7) Le petit théorème de Fermat.

Théorème :

$$\text{Si } p \text{ est un nombre premier et } a \text{ un entier relatif non nul et pas divisible par } p \text{ alors : } a^{p-1} - 1 \text{ est divisible par } p \text{ c'est-à-dire } a^{p-1} \equiv 1 [p] \text{ ou encore : } a^p \equiv a [p]$$

Preuve :

Soient p un nombre premier et k un entier naturel tel que $1 \leq k \leq p - 1$

On a p premier et $p > k$ donc $p \nmid k$ et par suite $p \wedge k = 1$ d'autre part :

$$kC_p^k = k \frac{p!}{k!(p-k)!} = \frac{p \times (p-1)!}{(k-1)!(p-k)!} = pC_{p-1}^{k-1}$$

Donc $p | kC_p^k$ et comme $p \wedge k = 1$ alors d'après T. Gauss $p | C_p^k$

Montrons que $p | (a+1)^p - a^p - 1$

On a d'après la formule de binôme On a : $(a+1)^p = a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a + 1$

Donc $(a+1)^p - a^p - 1 = C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a$

Et comme $p | C_p^k$ pour $1 \leq k \leq p - 1$ alors $p | (a+1)^p - a^p - 1$

On a donc : $(a+1)^p - 1 \equiv a^p \pmod{p}$.

Montrons par récurrence sur a (On prend pour le moment $a \in \mathbb{N}$) que $a^p \equiv a \pmod{p}$

- Pour $a = 0$ la propriété est vraie car $0^p = 0 \equiv 0 \pmod{p}$
- On suppose que la propriété est vraie pour a c'est-à-dire $a^p \equiv a \pmod{p}$
- Montrons que la propriété est vraie pour $(a+1)$ c'est-à-dire $(a+1)^p \equiv a+1 \pmod{p}$
On a : d'après les questions précédente $(a+1)^p \equiv a^p + 1 \pmod{p}$.
Or d'après H.R $a^p \equiv a \pmod{p}$ donc : $(a+1)^p \equiv a+1 \pmod{p}$.
Donc $(\forall a \in \mathbb{N})(\forall p \in \mathbb{P})(a^p \equiv a \pmod{p})$

Si $a < 0$ alors $-a > 0$

- Si $p = 2$ on aura $a^2 = (-a)^2 \equiv (-a) \pmod{2}$ et $-a \equiv a \pmod{2}$ car $2|(a - (-a)) = 2a$
- si $p \geq 3$ alors p est impaire et $(-a)^p = -a^p$ et $(-a)^p \equiv (-a) \pmod{p}$ on en déduit que $-a^p \equiv -a \pmod{p}$ et finalement $a^p \equiv a \pmod{p}$

D'où le théorème.

Exemple :

Montrons que : $(\forall n \geq 2) n^5 \equiv n \pmod{30}$

On a : d'après le petit théorème de Fermat : $n^5 \equiv n \pmod{5}$

Donc $5 | n^5 - n$

D'autre part : $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2 + 1)$

Donc $2 | n(n-1)$ et $3 | (n-1)n(n+1)$ et puisque 2 et 3 sont premiers alors $6 = (2 \times 3) | n^5 - n$

Finalement :

$$\begin{cases} 6 | n^5 - n \text{ et } 5 | n^5 - n \\ 6 \wedge 5 = 1 \end{cases} \Rightarrow (30 | n^5 - n)$$

Exercices

- 1 Soient p et q deux nombres premiers distincts ; montrer que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$
- 2 Considérons dans \mathbb{Z} l'équation (E) : $x^4 + 781 = 3y^4$ et soit S son ensemble de solution :
 - 1- Montrer que $(\forall x \in \mathbb{Z})(x^4 \equiv 1 \pmod{5} \text{ ou } x^4 \equiv 0 \pmod{5})$
 - 2- Montrer que $(\forall x \in \mathbb{Z})(x^4 + 781 \equiv 2 \pmod{5} \text{ ou } x^4 + 781 \equiv 1 \pmod{5})$
 - 3- Déterminer l'ensemble S .

Remarque :

La réciproque du théorème de Fermat n'est pas vraie : $7^{25} \equiv 1 \pmod{24}$ mais 25 n'est pas premier.

III) SYSTEMES DE NUMERATION

1) Théorème et définition

Théorème :

Soit b un entier naturel tel que : $b > 1$
 Chaque entier naturel non nul n s'écrit d'une façon unique de la forme :

$$n = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$$

 Où : les $(a_i)_{1 \leq i \leq m}$ sont des entiers naturel $0 \leq a_i \leq b - 1$ et $a_m \neq 0$

Preuve :

En utilisant la division Euclidienne de n sur b on obtient : $n = q_1 b + a_0$ où $0 \leq a_0 < b$

- Si $q_1 \leq b - 1$ on s'arrête et $a_1 = q_1$
- si $q_1 \geq b$, On effectue une autre division Euclidienne de q_1 sur b on obtient : $q_1 = q_2 b + a_1$ et par suite $n = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0$.
 - Si $q_2 \leq b - 1$ on s'arrête et $a_2 = q_2$
 - Si non on continue le processus

Notation :

Si $n = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$ on écrit : $n = \overline{a_m a_{m-1} \dots a_1 a_0}_{(b)}$ cette écriture s'appelle l'écriture de l'entier n dans la base b

Exemple :

Le nombre $n = 2987$ s'écrit $n = \overline{2987}_{(10)}$ car $n = 2 \times 10^4 + 9 \times 10^3 + 8 \times 10^2 + 7$

Essayons d'écrire n dans la base 6 :

On a :

$2987 = 6 \times 497 + 5$

$497 = 6 \times 82 + 5$

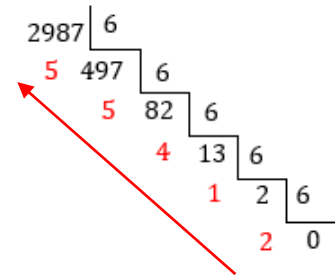
$82 = 6 \times 13 + 4$

$13 = 6 \times 2 + 1$

$2 = 6 \times 0 + 2$

Donc $2987 = 2 \times 6^4 + 1 \times 6^3 + 4 \times 6^2 + 5 \times 6 + 5 = \overline{21455}_{(6)}$

Cette succession de divisions Euclidiennes se représente comme ci-contre :



2) Les opérations dans une base de numération

2.1 La somme :

On peut effectuer la somme dans une base donnée b par deux façons différentes :

- La décomposition :

$$\begin{aligned} \overline{2534}_{(7)} + \overline{631}_{(7)} &= (2 \times 7^3 + 5 \times 7^2 + 3 \times 7 + 4) + (6 \times 7^2 + 3 \times 7 + 1) \\ &= 2 \times 7^3 + (5 + 6) \times 7^2 + (3 + 3) \times 7 + (4 + 1) \\ &= 3 \times 7^3 + 4 \times 7^2 + 6 \times 7 + 5 \\ &= \overline{3465}_{(7)} \end{aligned}$$

$5 + 6 = 7 + 4$

- Calcul direct avec le retenu

$$\begin{array}{r} 1 \\ \overline{2534}_{(7)} \\ + \overline{631}_{(7)} \\ \hline = \overline{3465}_{(7)} \end{array}$$

2.2 Le produit :

Il est préférable d'effectuer le produit en utilisant **le calcul direct avec le retenu** car la décomposition risque d'être longue :

$$\begin{array}{r}
 14 \\
 25 \\
 \times 327_{(8)} \\
 \hline
 56_{(8)} \\
 + 2412 \\
 \hline
 2063 \\
 \hline
 = 23242_{(8)}
 \end{array}$$

Pour vérifier :

$$\begin{aligned}
 \overline{327}_{(8)} \times \overline{56}_{(8)} &= (3 \times 8^2 + 2 \times 8 + 7) \times (5 \times 8 + 6) \\
 &= 9890 \\
 &= \overline{23242}_{(8)}
 \end{aligned}$$

2.3 Opérations dans différentes bases :

Pour effectuer des opérations dans différentes base on développe les deux nombres dans la base 10 ; on effectue l'opération et on écrit le résultat dans la base demandée.

Exemple : effectuer dans la base 9

$$\begin{aligned}
 \overline{6432}_{(7)} \times \overline{54}_{(8)} &= (6 \times 7^3 + 4 \times 7^2 + 3 \times 7 + 2) \times (5 \times 8 + 4) \\
 &= 100188 \\
 &= 1 \times 9^5 + 6 \times 9^4 + 2 \times 9^3 + 3 \times 9^2 + 8 \times 9 + 0 \\
 &= \overline{162380}_{(9)}
 \end{aligned}$$

IV) CRITERES DE DIVISIBILITE DES NOMBRES 5,25,3,9,11 ET 4

Théorème :

Soit x un entier naturel non nul tel que : $x = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$ où $0 \leq a_i \leq 9$; on a :

- $x \equiv 0 [5] \Leftrightarrow a_0 = 0$ ou $a_0 = 5$
- $x \equiv 0 [25] \Leftrightarrow \overline{a_1 a_0} \in \{0,25,50,75\}$
- $x \equiv 0 [3] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [3]$
- $x \equiv 0 [9] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [9]$
- $x \equiv 0 [11] \Leftrightarrow \sum_{i=0}^n (-1)^i a_i \equiv 0 [11]$
- $x \equiv 0 [4] \Leftrightarrow \overline{a_1 a_0} \equiv 0 [4]$

Preuve en exercice :

V) L'ENSEMBLE $\mathbb{Z}/p\mathbb{Z}$ OU p EST UN NOMBRE PREMIER.

Théorème :

Pour tous entiers relatifs non nuls a et b ; $a \wedge n = 1 \Leftrightarrow (\exists m \in \mathbb{Z})(am = 1 [n])$

Preuve :

(\Rightarrow) On suppose que : $a \wedge n = 1$, alors d'après T. Bézout $(\exists(m, u) \in \mathbb{Z}^2)(ma + un = 1)$

Donc : $(\exists(m, u) \in \mathbb{Z}^2)(un = 1 - ma)$ donc $n | ma - 1$ et finalement : $am = 1 [n]$

(\Leftarrow) On suppose que : $(\exists m \in \mathbb{Z})(am = 1 [n])$ donc $n | (am - 1)$ donc $(\exists k \in \mathbb{Z})(am - 1 = kn)$

donc : $am - kn = 1$ et d'après T. Bézout inverse $a \wedge n = 1$

Théorème :

Si p est un nombre premier positif alors tout élément $\bar{x} \neq \bar{0}$ admet un inverse dans $\mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$

Preuve :

Soit p un nombre premier positif ; on pose $E = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$

$x \in E \Leftrightarrow (\exists \alpha \in \{1, 2, \dots, p-1\})(\bar{x} = \bar{\alpha})$

p étant, premier donc p ne divise aucun nombre de l'ensemble $\{1, 2, \dots, p-1\}$ d'où $p \wedge \alpha = 1$

Et d'après la propriété précédente : $(\exists y \in \mathbb{Z}^*)(y\alpha \equiv 1[p])$

Donc : $\bar{\alpha}\bar{y} = \bar{1}$

D'où : $\bar{\alpha}\bar{y} = \bar{1}$ et comme $\bar{x} = \bar{\alpha}$ donc $\bar{x}\bar{y} = \bar{1}$