Arithmétiques Dans Z

56 PGCD & PPCM

$$\boxed{d = a \wedge b} \iff \left| \begin{array}{l} \boxed{d \text{ divise } a} \;;\; \boxed{d \text{ divise } b} \\ \boxed{\begin{array}{l} d' \text{ divise } a \\ d' \text{ divise } b \end{array}} \Rightarrow \boxed{d' \leq d} \end{array} \right.$$

$$\boxed{m = a \vee b} \iff \left| \begin{array}{l} \boxed{a \text{ divise } m} \;;\; \boxed{b \text{ divise } m} \\ \boxed{\begin{array}{l} a \text{ divise } m' \\ b \text{ divise } m' \end{array}} \Rightarrow \boxed{m' \geq m} \end{array} \right.$$

$$(ac) \wedge (bc) = |c| \cdot (a \wedge b)$$

$$(ac) \vee (bc) = |c| \cdot (a \vee b)$$

$$(a \wedge b) \cdot (a \vee b) = |ab|$$

$$(a \wedge b)^n = a^n \wedge b^n$$

Avec a, b et c sont des éléments de $\mathbb{Z}$.
et n est un élément de $\mathbb{N}^*$.

57 Réduction de a ∧ b = d :

$$d = a \wedge b \iff \left| \begin{array}{l} \exists\, (\alpha, \beta) \in \mathbb{Z}^2 \;;\; \left| \begin{array}{l} \text{et } \; a = \alpha d \\ \text{et } \; b = \beta d \end{array} \right. \\ \text{avec } \; \alpha \wedge \beta = 1 \end{array} \right.$$

Avec a et b sont deux éléments de $\mathbb{Z}^*$.

58 Algorithme d'Euclide :

$$\begin{array}{l|l} a & \underline{b} \\ c & d \end{array} \Rightarrow \boxed{a \wedge b = b \wedge c}$$

Avec a, b, c et d sont des éléments de $\mathbb{Z}$. Et $b \neq 0$.

59 PGCD & PPCM

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

Avec a et b appartiennent à $\mathbb{Z}$.

60 Théorème de Bezout :

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

Avec a et b appartiennent à $\mathbb{Z}^*$.

61 Théorème de Gauss :

$$\left. \begin{array}{r} a \text{ divise } bc \\ a \wedge c = 1 \end{array} \right| \Rightarrow a \text{ divise } b$$

Avec a, b et c sont des éléments de $\mathbb{Z}^*$.

62 Le produit diviseur :

$$\left. \begin{array}{r} a \text{ divise } c \\ b \text{ divise } c \\ a \wedge b = 1 \end{array} \right| \Rightarrow ab \text{ divise } c$$

63 Nombres premiers entre eux :

$$\left. \begin{array}{r} a \wedge b = 1 \\ a \wedge c = 1 \end{array} \right| \iff a \wedge bc = 1$$

$$a \wedge b = 1 \iff a^m \wedge b^n = 1$$

Avec a, b et c sont dans $\mathbb{Z}^*$. Et m et n sont dans $\mathbb{N}^*$.

64 L'équation ax + by = c :

$$\left. \begin{array}{r} ax + by = c \quad \text{est} \\ \text{solvable dans } \mathbb{Z}^2 \end{array} \right| \iff (a \wedge b) \text{ divise } c$$

Avec a, b et c sont dans $\mathbb{Z}^*$.

65 Division Euclidienne :

$$\left. \begin{array}{r} a \in \mathbb{Z} \\ b \in \mathbb{Z}^* \end{array} \right| \Rightarrow \exists\, (r, q) \in \mathbb{Z}^2 \;;\; \begin{cases} a = qb + r \\ 0 \leq r < b \end{cases}$$

66 La relation modulo (≡) :

$$a \equiv b\,[n] \iff n \text{ divise } (a - b)$$

Avec a, b deux entiers relatifs .

67 modulo est une relation d'équivalence :

$$\begin{cases} a \equiv a\,[n] \quad ; \quad \forall\, a \in \mathbb{Z} \\ a \equiv b\,[n] \quad \Leftrightarrow \quad b \equiv a\,[n] \\ \left.\begin{array}{l} a \equiv b\,[n] \\ b \equiv c\,[n] \end{array}\right| \quad \Rightarrow \quad a \equiv c\,[n] \end{cases}$$

Avec a, b deux relatifs et n un entier naturel non nul.

68 Division Euclidienne vs modulo :

$$a \equiv b\,[n] \quad \Leftrightarrow \quad \left|\begin{array}{l} a \text{ et } b \text{ ont le même} \\ \text{reste quand on divise} \\ a \text{ et } b \text{ sur le nbr } n \end{array}\right.$$

Avec a, b et n sont des entiers naturels non- nuls.

69 La relation modulo est compatible avec l'addition et la multiplication

$$\left.\begin{array}{l} a \equiv b\,[n] \\ c \equiv d\,[n] \end{array}\right| \quad \Rightarrow \quad ac \equiv bd\,[n]$$

$$a \equiv b\,[n] \quad \Rightarrow \quad a^k \equiv b^k\,[n]$$

$$\left.\begin{array}{l} a \equiv b\,[n] \\ c \equiv d\,[n] \end{array}\right| \quad \Rightarrow \quad (a+c) \equiv (b+d)\,[n]$$

$$a \equiv b\,[n] \quad \Rightarrow \quad ka \equiv kb\,[n]$$

Avec a, b, d et d sont dans $\mathbb{Z}$.
Et $n \in \mathbb{N}^*$; $k \in \mathbb{N}$.

70 Réduire une égalité modulo n :

$$ac \equiv bc\,[n] \quad \Leftrightarrow \quad a \equiv b \left[\frac{n}{c \wedge n}\right]$$

Avec a, b et c sont dans $\mathbb{Z}^*$. Et $n \in \mathbb{N}^*$.

71 Réduire une égalité modulo :

- $\mathbb{Z}/n\mathbb{Z} = \left\{ \overline{0}\,; \overline{1}\,; \overline{2}\,; \cdots ; \overline{(n-1)} \right\}$
- $\overline{r} = \{ x \in \mathbb{Z} \ ; \ x \equiv r\,[n] \}$

Avec : $n \in \mathbb{N}^*$; $r \in \mathbb{N}$; $0 \leq r \leq n-1$.

- $\overline{x} + \overline{y} = \overline{x+y}$
- $\overline{x} \times \overline{y} = \overline{x \times y}$
- $\overline{n} = \overline{0}$
- $-\overline{x} = \overline{0-x} = \overline{n-x}$

Avec : $x\,, y \in \mathbb{Z}$.

72 La relation modulo dans Z/nZ :

$$a \equiv b\,[n] \quad \Leftrightarrow \quad \overline{a} = \overline{b}$$

Avec : $n\,, a\,, b \in \mathbb{N}^*$.

73 Certificat de primalité :

$$\left.\begin{array}{c} n \text{ est un} \\ \text{nombre} \\ \text{premier} \end{array}\right| \quad \Leftrightarrow \quad \left|\begin{array}{l} \text{Tous les nombres} \\ \text{premiers dont le carré} \\ \text{est inférieur à } n \\ \text{ne divisent pas } n \end{array}\right.$$

Avec : $n \in \mathbb{N}^*$.

74 Nombres premiers entre eux dans P :

$$\left.\begin{array}{c} (p,q) \in \mathbb{P}^2 \\ p \neq q \end{array}\right| \quad \Rightarrow \quad p \wedge q = 1$$

75 Le premier qui divise un produit :

$$\left.\begin{array}{r} p \text{ est premier} \\ p \text{ divise } ab \end{array}\right| \quad \Rightarrow \quad \left|\begin{array}{l} \text{oubien } p \text{ divise } a \\ \text{oubien } p \text{ divise } b \end{array}\right.$$

Avec a et b sont deux entiers relatifs non nuls.

76 Théorème de Fermat (Forme Générale) :

$$\left.\begin{array}{c} p \text{ est premier} \\ a \in \mathbb{Z} \end{array}\right| \quad \Rightarrow \quad a^p \equiv a\,[p]$$

77 Théorème de Fermat (Forme Réduite) :

$$\left.\begin{array}{c} p \text{ est premier} \\ a \wedge p = 1 \end{array}\right| \quad \Rightarrow \quad a^{p-1} \equiv 1\,[p]$$

78 Décomposition en produit de facteurs premiers :

$$a \in \mathbb{N} \quad \Rightarrow \quad \left|\begin{array}{l} \exists!\ (p_1, \cdots, p_k) \in \mathbb{P}^k \\ \exists!\ (\alpha_1, \cdots, \alpha_k) \in \mathbb{N}^k \\ a = {p_1}^{\alpha_1} \times \cdots \times {p_k}^{\alpha_k} \end{array}\right.$$

2	3	5	7	11	13
17	19	23	29	31	37
41	43	47	53	59	61
67	71	73	79	83	89
97	101	103	107	109	113

79 PGCD & PPCM :

- $(p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}) \wedge (p_1^{\beta_1} \times \cdots \times p_k^{\beta_k}) = (p_1^{\gamma_1} \times \cdots \times p_k^{\gamma_k})$
- $(p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}) \vee (p_1^{\beta_1} \times \cdots \times p_k^{\beta_k}) = (p_1^{\sigma_1} \times \cdots \times p_k^{\sigma_k})$

$$Avec \quad : \quad \left| \begin{array}{l} \gamma_i = inf(\alpha_i\,;\,\beta_i) \\ \sigma_i = sup(\alpha_i\,;\,\beta_i) \\ 1 \leq i \leq k \end{array} \right.$$

80 Nombres de diviseurs d'un entier :

l'entier naturel $a = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_n}$ *admet exactement* $(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_n)$ *diviseurs positifs dont on trouve les nombres 1 et a*

81 L'équation ax = b [n] dans Z :

$$\left. \begin{array}{r} ax \equiv b\,[n] \text{ est} \\ \text{solvable dans } \mathbb{Z} \end{array} \right| \quad \Leftrightarrow \quad (a \wedge n) \text{ divise } b$$

Avec $a, b \in \mathbb{N}$ et $n \in \mathbb{N}^*$

et $S = \left\{ x_0 + \left(\frac{n}{a\wedge n}\right) k \;\; ; \;\; k \in \mathbb{Z} \right\}$.

x_0 est une solution particulière de l'équation .

82 Généralisation du Théo de Gauss :

$$\left. \begin{array}{r} a \wedge bc = d \\ a \wedge b = 1 \end{array} \right| \quad \Rightarrow \quad a \wedge c = d$$

Avec : $a, b, c \in \mathbb{Z}^*$.

$$\left. \begin{array}{r} a \wedge b = d \\ c \text{ divise } b \end{array} \right| \quad \Rightarrow \quad a \wedge c = d$$

83 Produit d'entiers consécutifs :

Le produit de k nombres entiers naturels consécutifs est toujours divisible par les nombres $1, 2, 3, 4, 5, 6, 7, \cdots \cdots, k$.

Avec : $a, b \in \mathbb{N}$ et $n \in \mathbb{N}^*$.

84 La division au carré :

$$a^2 \text{ divise } b^2 \quad \Leftrightarrow \quad a \text{ divise } b$$

Avec a et b sont deux entiers relatifs.

85 diviser le diviseur :

$$\left. \begin{array}{l} d \text{ divise } a \\ d \text{ divise } b \end{array} \right| \quad \Rightarrow \quad d \text{ divise } (a \wedge b)$$

Avec a et b sont deux entiers relatifs.

86 Le produit exponentiel :

$$\left. \begin{array}{r} ab = c^n \\ a \wedge b = 1 \end{array} \right| \quad \Rightarrow \quad \exists\, (\alpha, \beta) \in \mathbb{N}^2 \;\; ; \;\; \left| \begin{array}{l} a = \alpha^n \\ b = \beta^n \end{array} \right.$$

Avec a, b et n sont des entiers naturels. $n \neq 0$

87 La partie entière E(x)

- $E(x) = n \iff n \leq x < n+1 \;\; ; \;\; \forall x \in \mathbb{R}$
- $E(x) \leq x < E(x) + 1 \;\; ; \;\; \forall x \in \mathbb{R}$
- $\left| \begin{array}{l} \forall n \in \mathbb{Z} \\ \forall x \in \mathbb{R} \end{array} \right. \;\; ; \;\; E(x+n) = E(x) + n$
- $E(x) + E(-x) = \begin{cases} 0 & si \;\; x \in \mathbb{Z} \\ -1 & si \;\; x \notin \mathbb{Z} \end{cases}$
- $E(x) + E(y) \leq E(x+y) \leq E(x) + E(y) + 1$
- $0 \leq E(nx) - n\,E(x) \leq n - 1 \;\; ; \;\; \forall n \in \mathbb{N}^*$
- $n\,E(x) \leq nx < n\,E(x) + n \;\; ; \;\; \forall n \in \mathbb{N}^*$
- $E\left(\frac{E(nx)}{n}\right) = E(x) \;\; ; \;\; \forall x \in \mathbb{R} \;\; ; \;\; \forall n \in \mathbb{Z}$
- $E(x) \leq \frac{E(nx)}{n} \leq x \;\; ; \;\; \forall x \in \mathbb{R} \;\; ; \;\; \forall n \in \mathbb{Z}$
- $\sum_{k=1}^{n-1} E\left(\frac{km}{n}\right) = \frac{(m-1)(n-1)}{2} \;\; ; \;\; \left| \begin{array}{l} \forall\, m, n \in \mathbb{N}^* \\ m \wedge n = 1 \end{array} \right.$
- $\sum_{k=1}^{n-1} E\left(\frac{km}{n}\right) = \frac{(m-1)(n-1) + m \wedge n - 1}{2} \;\; ; \;\; \forall\, m, n \in \mathbb{N}^*$

88 Égalité modulo un produit

$$a \equiv b\,[mn] \quad \Rightarrow \quad \begin{cases} Et \;\; a \equiv b\,[m] \\ Et \;\; a \equiv b\,[n] \end{cases}$$

$$\begin{cases} Et \;\; a \equiv b\,[m] \\ Et \;\; a \equiv b\,[n] \\ Et \;\; m \wedge n = 1 \end{cases} \quad \Rightarrow \quad a \equiv b\,[mn]$$