

3.1.6 Soit p, q deux nombres premiers distincts. Quels sont les diviseurs positifs de $p^2 q$?

Exemple :

$$p = 3$$

$$q = 7$$

$$N = p^2 q = 9 \cdot 7 = 63$$

Les diviseurs positifs de $p^2 q$ sont

$$1, p, q, pq, p^2, p^2 q$$

3.1.12 Si p est premier, avec $p > 5$, alors 24 divise $p^2 - 1$.

Exemple :

1) $p = 11$

$$p^2 - 1 = 121 - 1 = 120 = 24 \cdot 5$$

2) $p = 97$

$$p^2 - 1 = 9409 - 1 = 9408 = 24 \cdot 392$$

3) $p = 99$ qui n'est pas premier

$$p^2 - 1 = 9801 - 1 = 9800 = 24 \cdot 408, \overline{3}$$

Démontrons ce résultat.

$$N = p^2 - 1 = (p-1)(p+1). \text{ On doit montrer que}$$

$$p^2 - 1 \equiv 0 \pmod{24}$$

La suite de nombres

$$\dots, \underbrace{p-1, p, p+1}_{\text{pair, impair, pair}}, \dots$$

multiple de 3 (comme p est premier, c'est $p-1$ ou $p+1$)

Donc $p^2 - 1$ est divisible par 12.

Soit $p-1$, soit $p+1$ est un multiple de 4.

Finalement, $p^2 - 1$ est divisible par 8 et 3, donc par 24.

Pour a et b dans $\mathbb{Z}$, on dit que a divise b s'il existe $z \in \mathbb{Z}$ tel que $a \cdot z = b$. Si a divise b , on le note $a \mid b$ et on dira de plus que a est un *diviseur* de b , ou que b est un *multiple* de a , ou encore que b est *divisible* par a . Si a ne divise pas b , on le note $a \nmid b$.

3.2.1 Soit a, b et c dans $\mathbb{Z}$. Montrer que

- a) $a \mid a, 1 \mid a$ et $a \mid 0$;
- b) $0 \mid a$ si et seulement si $a = 0$;
- c) $a \mid b$ si et seulement si $\neg$ d) $a \mid b$ et $a \mid c$ implique $a \mid (b+c)$;
- d) $a \mid b$ et $a \mid c$ implique $a \mid$ e) $a \mid b$ et $b \mid c$ implique $a \mid c$.
- e) $a \mid b$ et $b \mid c$ implique $a \mid c$.

Exemple : $8 \mid 24 \Leftrightarrow 8 \cdot 3 = 24$

a) $a \mid a$. En effet, si $z = 1$, on a $a \cdot 1 = a$

Preuve : $a = a \cdot 1 \Rightarrow a \mid a$

$$1 \mid a : 1 \mid a \Leftrightarrow 1 \cdot a = a$$

$$a \mid 0 : a \mid 0 \Leftrightarrow a \cdot 0 = 0$$

$$b) 0 \mid a \Leftrightarrow a = 0$$

$$\Rightarrow : 0 \mid a \Rightarrow a = 0$$

$$\text{il existe } z \in \mathbb{Z} \text{ tel que } 0 \cdot z = a \Rightarrow 0 = a$$

$$\Leftarrow : a = 0 \Rightarrow 0 \mid 0$$

$$0 \cdot z = 0, \text{ pour tout } z \in \mathbb{Z}, \text{ donc } 0 \mid 0$$

c) $a \mid b$ si et seulement si $-a \mid b$ si et seulement si $a \mid -b$;

$$a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b$$

Nous allons démontrer :

$$a \mid b \Rightarrow -a \mid b \Rightarrow a \mid -b \Rightarrow a \mid b$$

1) $a \mid b$, donc il existe $z \in \mathbb{Z}$ tel que $a \cdot z = b$,

$$\text{Donc } -a \cdot \underbrace{(-z)}_{z'} = b, \text{ et ainsi } -a \cdot z' = b, \text{ donc } -a \mid b$$

2) $-a \mid b$, donc il existe $z \in \mathbb{Z}$ tel que $-a \cdot z = b$.

$$\text{Donc } -(-a) \cdot z = -b \text{ et } a \cdot z = -b \Rightarrow a \mid -b$$

3) $a \mid -b$, donc il existe $z \in \mathbb{Z}$ tel que $a \cdot z = -b$.

$$-a \cdot z = -(-b) \text{ et } a \cdot (-z) = b \Rightarrow a \mid b.$$

d) $a \mid b$ et $a \mid c$ implique $a \mid (b + c)$;

- Si $a \mid b$, alors il existe $z_1 \in \mathbb{Z}$ tel que $a \cdot z_1 = b$.
- Si $a \mid c$, alors il existe $z_2 \in \mathbb{Z}$ tel que $a \cdot z_2 = c$.

Donc $b + c = a \cdot z_1 + a \cdot z_2 = a \cdot \underbrace{(z_1 + z_2)}_z = a \cdot z$

Ainsi $a \cdot z = b + c \Rightarrow a \mid b + c$

Exemple

$$\left. \begin{array}{l} 6 \mid 18 \\ 6 \mid 12 \end{array} \right\} 6 \mid 30$$

e) $a \mid b$ et $b \mid c$ implique $a \mid c$.

$$(a \mid b \text{ et } b \mid c) \Rightarrow a \mid c$$

$$a \mid b \Rightarrow \exists z_1 \in \mathbb{Z} \text{ tel que } a \cdot z_1 = b.$$

$$b \mid c \Rightarrow \exists z_2 \in \mathbb{Z} \text{ tel que } b \cdot z_2 = c.$$

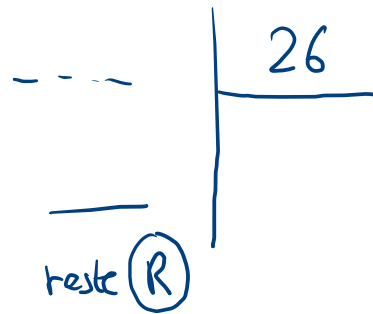
$$\text{On a } b \cdot z_2 = (a \cdot z_1) \cdot z_2 = a \cdot \underbrace{(z_1 \cdot z_2)}_z = a \cdot z = c$$

Donc $a \mid c$.

3.2.10 Quels sont tous les restes possibles après division entière par 26 ? Donner la liste de ces restes. $0, 1, \dots, 25$

3.2.11 Quels sont les nombres dont le reste après division par 26 donne 17 ? Peut-on en donner la liste complète ?

3.2.10



$$0 \leq R < 26$$

3.2.11

$$17 \equiv 17 \pmod{26}$$

$$43 \equiv 60 \equiv 77 \equiv -9 \equiv 17 \pmod{26}$$

3.2.19 Soit n un entier positif. Soit encore a et b deux entiers quelconques. On dit que a est *congru à b modulo n* si $n \mid (a - b)$, ce que nous écrivons $a \equiv b \pmod{n}$. Montrer que cela revient à demander que $a = b + n \cdot y$ pour $y \in \mathbb{Z}$.

$$a \equiv b \pmod{n} \quad \text{si} \quad n \mid (a - b)$$

Si $n \mid (a - b)$, il existe $z \in \mathbb{Z}$ tel que $n \cdot z = a - b$.

$$\text{Donc} \quad a = b + n \cdot z.$$

Table d'addition et de multiplication de $\mathbb{Z}_7$ et $\mathbb{Z}_8$

$$\mathbb{Z}_7 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \}$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

① $\bar{3} + \bar{4} \equiv \bar{7} \equiv \bar{0}$

$$\bar{3} : x = 3 + 7 \cdot z_1$$

$$\bar{4} : y = 4 + 7 \cdot z_2$$

$$\left. \begin{array}{l} \bar{3} : x = 3 + 7 \cdot z_1 \\ \bar{4} : y = 4 + 7 \cdot z_2 \end{array} \right\} \bar{3} + \bar{4} : x + y = 7 + 7(z_1 + z_2)$$

② $\bar{3} \cdot \bar{4} = \bar{12} = \bar{5}$

$$\begin{aligned} \bar{3} \cdot \bar{4} : x \cdot y &= (3 + 7z_1)(4 + 7z_2) = 12 + 7 \cdot 4z_1 + 3 \cdot 7z_2 + 7 \cdot 7z_1 \cdot z_2 \\ &= 12 + 7(4z_1 + 3z_2 + 7z_1 \cdot z_2) \end{aligned}$$

$$\mathbb{Z}/8\mathbb{Z}$$

wolframalpha.com

Addition table:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication table:

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1



$$\begin{aligned} \overline{4} \cdot \overline{2} &\equiv \overline{0} \pmod{8} \\ \overline{4} \cdot \overline{6} &\equiv \overline{0} \pmod{8} \end{aligned}$$