Correction des exercices

Exercice 28 p. 27

Exercice 28 p. 27

$45 =$

Exercice 28 p. 27

$45 = 9 \times 5 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 = 2^3 \times 5^2 \times 7$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 = 2^3 \times 5^2 \times 7$

$735 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 = 2^3 \times 5^2 \times 7$

$735 = 7 \times 105 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 = 2^3 \times 5^2 \times 7$

$735 = 7 \times 105 = 7 \times 5 \times 21 =$

Exercice 28 p. 27

$45 = 9 \times 5 = 3^2 \times 5$

$1400 = 14 \times 100 = 2 \times 7 \times (2 \times 5)^2 = 2^3 \times 5^2 \times 7$

$735 = 7 \times 105 = 7 \times 5 \times 21 = 3 \times 5 \times 7^2$

Exercice 30 p. 27

Exercice 30 p. 27

$$\frac{76}{24} =$$

Exercice 30 p. 27

$$\frac{76}{24} = \frac{2^2 \times 19}{2^3 \times 3} =$$

Exercice 30 p. 27

$$\frac{76}{24} = \frac{2^2 \times 19}{2^3 \times 3} = \frac{19}{2 \times 3} = \frac{19}{6}$$

Exercice 30 p. 27

$$\frac{76}{24} = \frac{2^2 \times 19}{2^3 \times 3} = \frac{19}{2 \times 3} = \frac{19}{6}$$

$$\frac{13650}{1785} =$$

Exercice 30 p. 27

$$\frac{76}{24} = \frac{2^2 \times 19}{2^3 \times 3} = \frac{19}{2 \times 3} = \frac{19}{6}$$

$$\frac{13650}{1785} = \frac{2 \times 3 \times 5^2 \times 7 \times 13}{3 \times 5 \times 7 \times 17} =$$

Exercice 30 p. 27

$$\frac{76}{24} = \frac{2^2 \times 19}{2^3 \times 3} = \frac{19}{2 \times 3} = \frac{19}{6}$$

$$\frac{13650}{1785} = \frac{2 \times 3 \times 5^2 \times 7 \times 13}{3 \times 5 \times 7 \times 17} = \frac{2 \times 5 \times 13}{17} = \frac{130}{17}$$

Exercice 32 p. 27

Exercice 32 p. 27

Un diviseur positif de a est de la forme $3^{\alpha} \times 5^{\beta}$ avec $\alpha \in \{0, 1, 2\}$ et $\beta \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

Exercice 32 p. 27

Un diviseur positif de a est de la forme $3^{\alpha} \times 5^{\beta}$ avec $\alpha \in \{0, 1, 2\}$ et $\beta \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ donc a possède $3 \times 8 = 24$ diviseurs positifs.

Exercice 32 p. 27

Un diviseur positif de a est de la forme $3^\alpha \times 5^\beta$ avec $\alpha \in \{0, 1, 2\}$ et $\beta \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ donc a possède $3 \times 8 = 24$ diviseurs positifs.

Un diviseur positif de b est de la forme $2^\alpha \times 11^\beta$ avec $\alpha \in \{0, 1\}$ et $\beta \in \{0, 1, 2, 3\}$

Exercice 32 p. 27

Un diviseur positif de a est de la forme $3^\alpha \times 5^\beta$ avec $\alpha \in \{0, 1, 2\}$ et $\beta \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ donc a possède $3 \times 8 = 24$ diviseurs positifs.

Un diviseur positif de b est de la forme $2^\alpha \times 11^\beta$ avec $\alpha \in \{0, 1\}$ et $\beta \in \{0, 1, 2, 3\}$ donc b possède $2 \times 4 = 8$ diviseurs positifs.

Exercice 161 p. 39

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$,

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$ et $N_5 = 41 \times 271$.

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$ et $N_5 = 41 \times 271$.
3. a. Dressons un tableau de restes modulo 10 :

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$ et $N_5 = 41 \times 271$.
3. a. Dressons un tableau de restes modulo 10 :

Reste de n modulo 10	0	1	2	3	4	5	6	7	8	9
Reste de n^2 modulo 10	0	1	4	9	6	5	6	9	4	1

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$ et $N_5 = 41 \times 271$.
3. a. Dressons un tableau de restes modulo 10 :

Reste de n modulo 10	0	1	2	3	4	5	6	7	8	9
Reste de n^2 modulo 10	0	1	4	9	6	5	6	9	4	1

Comme on suppose que n^2 est un rep-unit, le chiffre des unités de n^2 est 1 donc $n^2 \equiv 1\ [10]$.

Exercice 161 p. 39

1. L'écriture décimale d'un rep-unit se termine par un 1 donc un rep-unit n'est jamais divisible par 2 ni par 5.
2. $N_3 = 111 = 3 \times 37$, $N_4 = 11 \times 101$ et $N_5 = 41 \times 271$.
3. a. Dressons un tableau de restes modulo 10 :

Reste de n modulo 10	0	1	2	3	4	5	6	7	8	9
Reste de n^2 modulo 10	0	1	4	9	6	5	6	9	4	1

Comme on suppose que n^2 est un rep-unit, le chiffre des unités de n^2 est 1 donc $n^2 \equiv 1\ [10]$. On déduit donc du tableau que $n \equiv 1\ [10]$ ou $n \equiv 9\ [10]$.

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$n^2 =$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$n^2 = (1+10m)^2 =$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$n^2 = (1+10m)^2 = 1+20m+100m^2 =$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2)$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$n^2 =$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 =$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 =$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2)$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$.

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k =$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 =$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 = 11+100\times\underbrace{11\cdots1}_{k-2 \text{ fois}} =$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 = 11+100\times\underbrace{11\cdots1}_{k-2 \text{ fois}} = 11+20\times\underbrace{55\cdots5}_{k-2 \text{ fois}} \equiv 11\ [20]$$

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 = 11+100\times\underbrace{11\cdots1}_{k-2 \text{ fois}} = 11+20\times\underbrace{55\cdots5}_{k-2 \text{ fois}} \equiv 11\ [20]$$

donc, comme $0 \leqslant 11 < 20$,

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 = 11+100\times\underbrace{11\cdots1}_{k-2 \text{ fois}} = 11+20\times\underbrace{55\cdots5}_{k-2 \text{ fois}} \equiv 11\ [20]$$

donc, comme $0 \leqslant 11 < 20$, le reste de N_k modulo 20 est 11 ce qui contredit le fait que $n^2 \equiv 1\ [20]$.

b. Si $n \equiv 1\ [10]$ alors il existe un entier m tel que $n = 1 + 10m$ donc

$$n^2 = (1+10m)^2 = 1+20m+100m^2 = 1+20(m+5m^2) \equiv 1\ [20]$$

et si $n \equiv 9\ [10]$ alors il existe un entier m tel que $n = 9 + 10m$ donc

$$n^2 = (9+10m)^2 = 81+180m+100m^2 = 1+20(4+9m+5m^2) \equiv 1\ [20]$$

Ainsi, dans tous les cas, $n^2 \equiv 1\ [20]$.
Remarque. Pour le cas $n \equiv 9\ [10]$, on pouvait aussi remarquer que, dans ce cas, $n \equiv -1\ [10]$ donc $n^2 \equiv (-1)^2\ [10] \equiv 1\ [10]$ et on se ramenait ainsi au premier cas.

c. Par hypothèse, il existe un entier $k \geqslant 2$ tel que $n^2 = N_k$. Or,

$$N_k = \underbrace{11\cdots1}_{k-2 \text{ fois}}00+11 = 11+100\times\underbrace{11\cdots1}_{k-2 \text{ fois}} = 11+20\times\underbrace{55\cdots5}_{k-2 \text{ fois}} \equiv 11\ [20]$$

donc, comme $0 \leqslant 11 < 20$, le reste de N_k modulo 20 est 11 ce qui contredit le fait que $n^2 \equiv 1\ [20]$.
On conclut que, pour tout entier $k \geqslant 2$, N_k n'est pas le carré d'un entier.

Propriété 30

Soit un entier $n \geqslant 2$. Si la décomposition de n en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Propriété 30

Soit un entier $n \geqslant 2$. Si la décomposition de n en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Démonstration.

D'après la propriété 27, un entier $d \geqslant 1$ divise n si et seulement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$.

Propriété 30

Soit un entier $n \geqslant 2$. Si la décomposition de n en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Démonstration.

D'après la propriété 27, un entier $d \geqslant 1$ divise n si et seulement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$. Ainsi, les diviseurs positifs de n sont exactement les nombres de la forme $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ où, pour tout entier i entre 1 et k, β_i est un entier compris entre 0 et α_i.

Propriété 30

Soit un entier $n \geqslant 2$. Si la décomposition de n en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Démonstration.

D'après la propriété 27, un entier $d \geqslant 1$ divise n si et seulement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$. Ainsi, les diviseurs positifs de n sont exactement les nombres de la forme $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ où, pour tout entier i entre 1 et k, β_i est un entier compris entre 0 et α_i. Ainsi, pour tout entier i entre 1 et k, il y a $\alpha_i + 1$ choix pour β_i

Propriété 30

Soit un entier $n \geqslant 2$. Si la décomposition de n en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors le nombre de diviseurs positifs de n est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Démonstration.

D'après la propriété 27, un entier $d \geqslant 1$ divise n si et seulement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$. Ainsi, les diviseurs positifs de n sont exactement les nombres de la forme $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ où, pour tout entier i entre 1 et k, β_i est un entier compris entre 0 et α_i. Ainsi, pour tout entier i entre 1 et k, il y a $\alpha_i + 1$ choix pour β_i et donc n possède $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ diviseurs positifs. □

Exemple 31

Déterminer le nombre de diviseurs positifs de 1911 puis trouver tous ces diviseurs.

Exemple 31

Déterminer le nombre de diviseurs positifs de 1911 puis trouver tous ces diviseurs.

La décomposition de 1911 en produit de facteurs premiers est $1911 = 3 \times 7^2 \times 13$.

Exemple 31

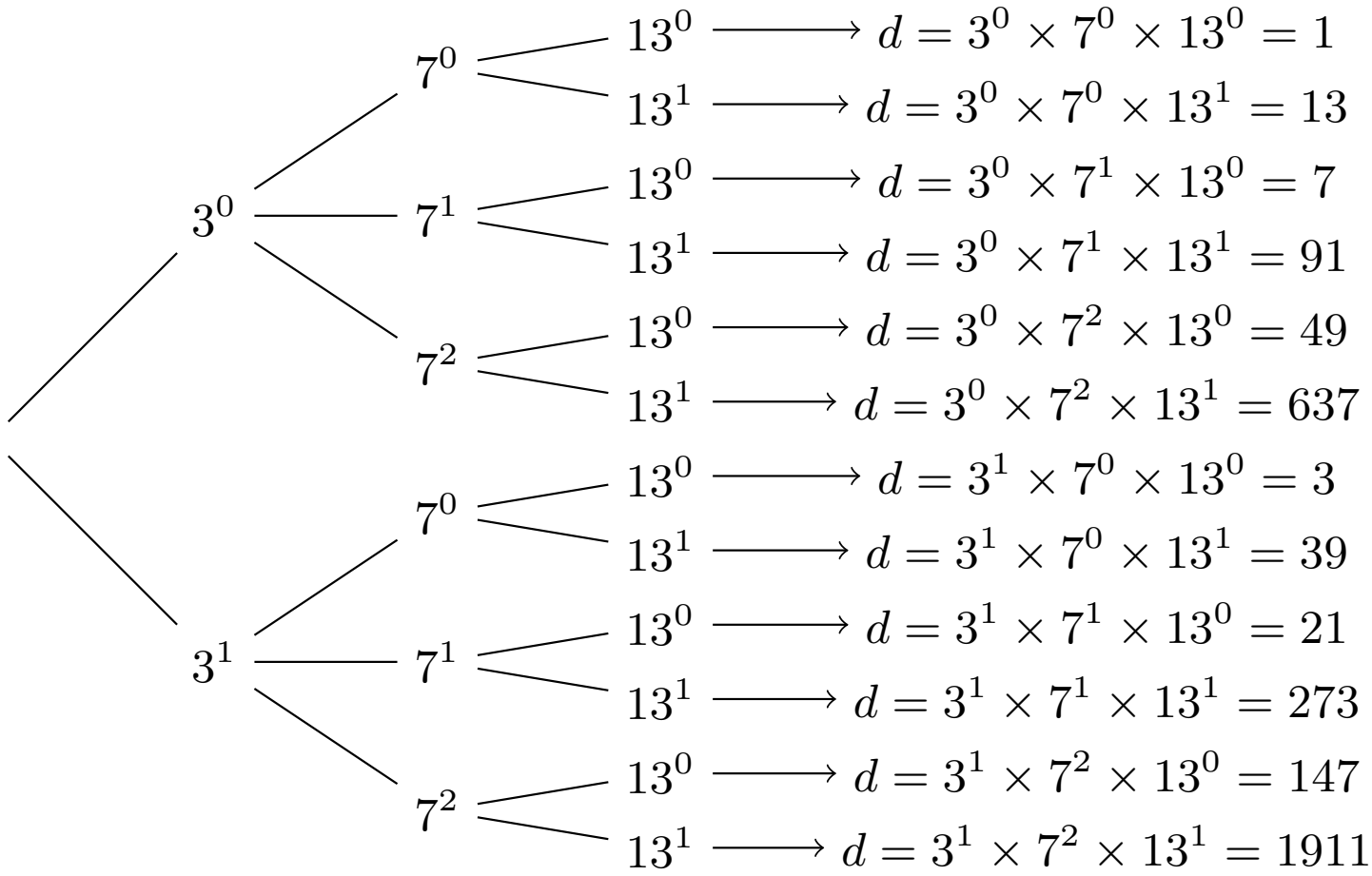
Déterminer le nombre de diviseurs positifs de 1911 puis trouver tous ces diviseurs.

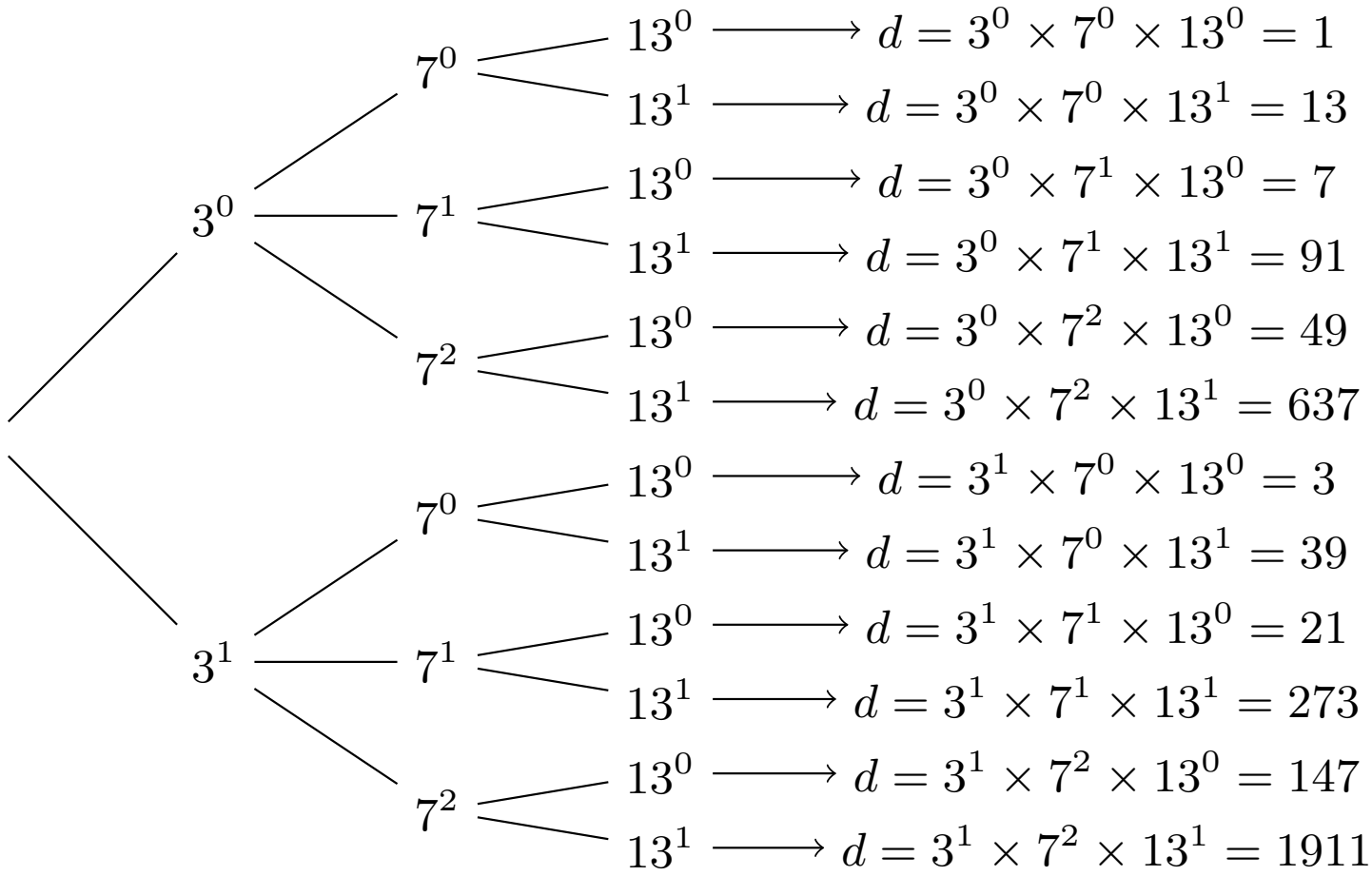
La décomposition de 1911 en produit de facteurs premiers est $1911 = 3 \times 7^2 \times 13$. Ainsi, 1911 possède $(1+1) \times (2+1) \times (1+1) = 12$ diviseurs positifs.

Exemple 31

Déterminer le nombre de diviseurs positifs de 1911 puis trouver tous ces diviseurs.

La décomposition de 1911 en produit de facteurs premiers est $1911 = 3 \times 7^2 \times 13$. Ainsi, 1911 possède $(1+1) \times (2+1) \times (1+1) = 12$ diviseurs positifs.
Pour trouver ces diviseurs de façon systématique, on peut utiliser un arbre :


3^0
3^1
7^0
7^1
7^2
7^0
7^1
7^2
$13^0 \longrightarrow d = 3^0 \times 7^0 \times 13^0 = 1$
$13^1 \longrightarrow d = 3^0 \times 7^0 \times 13^1 = 13$
$13^0 \longrightarrow d = 3^0 \times 7^1 \times 13^0 = 7$
$13^1 \longrightarrow d = 3^0 \times 7^1 \times 13^1 = 91$
$13^0 \longrightarrow d = 3^0 \times 7^2 \times 13^0 = 49$
$13^1 \longrightarrow d = 3^0 \times 7^2 \times 13^1 = 637$
$13^0 \longrightarrow d = 3^1 \times 7^0 \times 13^0 = 3$
$13^1 \longrightarrow d = 3^1 \times 7^0 \times 13^1 = 39$
$13^0 \longrightarrow d = 3^1 \times 7^1 \times 13^0 = 21$
$13^1 \longrightarrow d = 3^1 \times 7^1 \times 13^1 = 273$
$13^0 \longrightarrow d = 3^1 \times 7^2 \times 13^0 = 147$
$13^1 \longrightarrow d = 3^1 \times 7^2 \times 13^1 = 1911$



Ainsi, l'ensemble des diviseurs positifs de 1911 est $\{1, 3, 7, 13, 21, 39, 49, 91, 147, 273, 637, 1911\}$.

IV. — Petit théorème de Fermat

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1 \ [p]$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.

Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$
$0 \leqslant k \leqslant p-1$

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$. En ajoutant membre à membre $[*]$ et $[**]$,

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$. En ajoutant membre à membre $[*]$ et $[**]$, on obtient $-(p-1) \leqslant k-j \leqslant p-1$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$. En ajoutant membre à membre $[*]$ et $[**]$, on obtient $-(p-1) \leqslant k-j \leqslant p-1$. Or, le seul multiple de p compris entre $-(p-1)$ et $p-1$ est 0

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$. En ajoutant membre à membre $[*]$ et $[**]$, on obtient $-(p-1) \leqslant k-j \leqslant p-1$. Or, le seul multiple de p compris entre $-(p-1)$ et $p-1$ est 0 donc $k-j=0$ i.e. $k=j$.

IV. — Petit théorème de Fermat

Théorème 32. — Petit théorème de Fermat

Soit a un entier et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1\ [p]$.

Démonstration. Notons, pour tout entier $k \in [\![0, p-1]\!]$, r_k le reste de ka modulo p.
Montrons que, pour tous entiers k et j compris entre 0 et $p-1$, si $k \neq j$ alors $r_k \neq r_j$. Pour cela, considérons deux entiers k et j compris entre 0 et $p-1$ tels que $r_k = r_j$. Alors, par théorème, $ka \equiv ja\ [p]$ donc p divise $ka - ja = (k-j)a$. Or, p ne divise pas a donc, par le lemme d'Euclide, p divise $k-j$. De plus, $[*]$ $0 \leqslant k \leqslant p-1$ et $0 \leqslant j \leqslant p-1$ donc $[**]$ $-(p-1) \leqslant -j \leqslant 0$. En ajoutant membre à membre $[*]$ et $[**]$, on obtient $-(p-1) \leqslant k-j \leqslant p-1$. Or, le seul multiple de p compris entre $-(p-1)$ et $p-1$ est 0 donc $k-j=0$ i.e. $k=j$. Ainsi, si $k \neq j$, $r_k \neq r_j$.

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$.

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$.

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$).

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$r_1 \times r_2 \times \cdots \times r_{p-1} \equiv 1a \times 2a \times \cdots \times (p-1)a \ [p]$$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \end{aligned}$$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$ donc p divise $(p-1)! \times a^{p-1} - (p-1)! =$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$ donc p divise $(p-1)! \times a^{p-1} - (p-1)! = \left[a^{p-1} - 1\right] \times (p-1)!$.

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$ donc p divise $(p-1)! \times a^{p-1} - (p-1)! = \left[a^{p-1} - 1\right] \times (p-1)!$. Or, d'après l'exercice 20, p est premier avec $(p-1)!$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$ donc p divise $(p-1)! \times a^{p-1} - (p-1)! = \left[a^{p-1} - 1\right] \times (p-1)!$. Or, d'après l'exercice 20, p est premier avec $(p-1)!$ donc, par le lemme d'Euclide, on conclut que p divise $a^{p-1} - 1$

Remarquons, de plus, que $0 \times a = 0$ donc $r_0 = 0$. On en déduit que r_1, r_2, ..., r_{p-1} sont $p-1$ entiers différents compris entre 1 et $p-1$. Ainsi, $\{r_1, r_2, ..., r_{p-1}\} = \{1, 2, ..., p-1\}$ (mais on n'a pas forcément $r_1 = 1$, $r_2 = 2$, ..., $r_{p-1} = p-1$). En particulier, on en déduit que

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!.$$

Par ailleurs,

$$\begin{aligned} r_1 \times r_2 \times \cdots \times r_{p-1} &\equiv 1a \times 2a \times \cdots \times (p-1)a \ [p] \\ &\equiv (1 \times 2 \times \cdots \times (p-1))(\underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}}) \ [p] \\ &\equiv (p-1)! \times a^{p-1} \ [p]. \end{aligned}$$

Ainsi, $(p-1)! \equiv (p-1)! \times a^{p-1} \ [p]$ donc p divise $(p-1)! \times a^{p-1} - (p-1)! = \left[a^{p-1} - 1\right] \times (p-1)!$. Or, d'après l'exercice 20, p est premier avec $(p-1)!$ donc, par le lemme d'Euclide, on conclut que p divise $a^{p-1} - 1$ i.e. $a^{p-1} \equiv 1 \ [p]$. $\square$

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a,

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$.

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$. Sinon, p divise a

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$. Sinon, p divise a donc $a \equiv 0 \ [p]$.

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$. Sinon, p divise a donc $a \equiv 0 \ [p]$. Or, $p > 0$ donc $a^p \equiv 0 \ [p]$

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$. Sinon, p divise a donc $a \equiv 0 \ [p]$. Or, $p > 0$ donc $a^p \equiv 0 \ [p]$ et ainsi $a^p \equiv a \ [p]$.

Corollaire 33 : Petit théorème de Fermat (version 2)

Soit a un entier et p un nombre premier. Alors, $a^p \equiv a \ [p]$.

Démonstration.

Si p ne divise pas a alors, par le théorème précédent, $a^{p-1} \equiv 1 \ [p]$ donc, en multipliant par a, $a^p \equiv a \ [p]$. Sinon, p divise a donc $a \equiv 0 \ [p]$. Or, $p > 0$ donc $a^p \equiv 0 \ [p]$ et ainsi $a^p \equiv a \ [p]$.
Dans tous les cas, $a^p \equiv a \ [p]$. □

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$,

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$n^{13} - n =$$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$n^{13} - n = n(n^{12} - 1) =$$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] =$$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1)$$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$.
Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2. Il s'ensuit que PPCM$(2, 7 \times 13)$ divise $n^{13} - n$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2. Il s'ensuit que PPCM$(2, 7 \times 13)$ divise $n^{13} - n$ et, comme 7×13 est impair, 7×13 est premier avec 2

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que $\text{PPCM}(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi $\text{PPCM}(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2. Il s'ensuit que $\text{PPCM}(2, 7 \times 13)$ divise $n^{13} - n$ et, comme 7×13 est impair, 7×13 est premier avec 2 donc $\text{PPCM}(2, 7 \times 13) = 2 \times 7 \times 13$.

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2. Il s'ensuit que PPCM$(2, 7 \times 13)$ divise $n^{13} - n$ et, comme 7×13 est impair, 7×13 est premier avec 2 donc PPCM$(2, 7 \times 13) = 2 \times 7 \times 13$. On conclut donc que $2 \times 7 \times 13$ divise $n^{13} - n$

Exercice 34

Démontrer que, pour tout $n \in \mathbb{N}$, 182 divise $n^{13} - n$.

Solution. Soit $n \in \mathbb{N}$. Comme $182 = 2 \times 7 \times 13$, il suffit de montrer que $n^{13} - n$ est divisible par 2, 7 et 13.
D'après le théorème de Fermat (version 2), comme 13 est premier, 13 divise $n^{13} - n$. De même, comme 7 est premier, 7 divise $n^7 - n$. Or,

$$\begin{aligned} n^{13} - n = n(n^{12} - 1) = n\left[(n^6)^2 - 1^2\right] = n(n^6 - 1)(n^6 + 1) \\ = (n^7 - n)(n^6 + 1) \end{aligned}$$

donc $n^7 - n$ divise $n^{13} - n$. Par transitivité, on conclut que 7 divise $n^{13} - n$. On en déduit que PPCM$(13, 7)$ divise $n^{13} - n$. Or, 7 et 13 sont premiers et distincts donc premiers entre eux et ainsi PPCM$(13, 7) = 7 \times 13$. Ainsi, 7×13 divise $n^{13} - n$. Enfin, comme n et n^{13} ont la même parité, $n^{13} - n$ est pair i.e. $n^{13} - n$ est divisible par 2. Il s'ensuit que PPCM$(2, 7 \times 13)$ divise $n^{13} - n$ et, comme 7×13 est impair, 7×13 est premier avec 2 donc PPCM$(2, 7 \times 13) = 2 \times 7 \times 13$. On conclut donc que $2 \times 7 \times 13$ divise $n^{13} - n$ i.e. 182 divise $n^{13} - n$.