2.8.1 Démontrer les propriétés de la relation de divisibilité suivantes :

a) si $m \mid n$ et $m \mid r$, alors $m \mid (n+r)$ et $m \mid (n-r)$;

b) si $m \mid n$ et $r \in \mathbb{Z}$, alors $m \mid r\,n$;

c) si r, m et $n \in \mathbb{Z}$, et $r \neq 0$, alors $m \mid n$ si et seulement si $r\,m \mid r\,n$;

d) si $m \mid n$ et si $n \mid r$, alors $m \mid r$.

a) $4 \mid 12$ et $4 \mid 36 \Rightarrow 4 \mid 48$

b) $4 \mid 12$, $17 \Rightarrow 4 \mid 204$

d) $4 \mid 12$, $12 \mid 36 \Rightarrow 4 \mid 36$

a) (si $m \mid n$ et $m \mid r$) $\Rightarrow m \mid (n+r)$

En effet, il existe p et q tels que $n = pm$ et $r = qm$. Donc $n + r = pm + qm = (p+q)m$, donc $m \mid (n+r)$

b) (si $m \mid n$ et $r \in \mathbb{Z}$) $\Rightarrow m \mid rn$

En effet, il existe p tels que $n = pm$, donc $rn = r \cdot pm = (rp)m$.
donc $m \mid rn$

c) et d) maison

2.8.2 Quels sont les diviseurs de 0 ?

$$\forall n \in \mathbb{Z}^*, \quad n \mid 0$$

2.8.4 Déterminer la décomposition en facteurs premiers du nombre 4027 à l'aide de la machine à calculer seulement.
Idem avec 716539 et 1488391.

Un nombre est premiers s'il admet exactement deux diviseurs.

4027 est premier

$\{2, 3, 5, 7, 11, \ldots\}$

716'539

2.8.7 Trouver une dizaine de nombres entiers congrus à 22 modulo 7.

0 modulo 7 : $\overline{0}_7 = \{ \ldots, -14, -7, 0, 7, 14, 21, \ldots \}$

$\overline{1}_7 = \{ \ldots, -6, 1, 8, 15, \ldots \}$

$$\begin{array}{r|l} 15 & 7 \\ -14 & 2 \\ \hline 1 & \end{array}$$

$\overline{2}_7 = \{ , -5, 2, 9, 16,$

$22 \in \overline{1}_7$: 1, 8, 15, 22, 29, 36, 43, 50, 57, 64

- $\overline{1}_7 + \overline{2}_7 = \overline{3}_7$, $\overline{a}_n + \overline{b}_n = (\overline{a+b})_n$

2.8.8 On donne un nombre naturel a. Chercher son reste après division par n.

a) $a = 111\,;\ n = 2, 3, 4, \ldots, 12\,;$

b) $a = 123456789 \cdot 987654321\,;\ n = 2,\ = 9,\ n = 11\,;$

c) $a = 22^{22},\ n = 3,\ n = 9,\ n = 10,\ n = 11\,;$

d) $a = 1234^5,\ n = 9,\ n = 11,\ n = 99\,;$

b) $a \equiv 1 \pmod 2$

$$a = \underbrace{123456789}_{p} \cdot \underbrace{987654321}_{q}$$

$p \equiv q \equiv 0 \pmod 9$

$a \equiv 0 \pmod 9$

$p = 11 \cdot 11'223'344 + 5 = 11 \cdot p' + 5$

$(11p'+5)(11q'+5)$

$q = 11 \cdot 89'786'756 + 5 = 11 q' + 5$

$p \cdot q = 121\, p' \cdot q' + 55(p' + q') + 25 \Rightarrow a \equiv 25 \pmod{11}$

$a \equiv 3 \pmod{11}$

c) $a = 22^{22}$, $n = 3$, $n = 9$, $n = 10$, $n = 11$;

- $22^{22} \equiv 1^{22} \equiv 1 \pmod{3}$

- $22^{22} \equiv 4^{22} \equiv (4^2)^{11} \equiv 7^{11} \equiv (-2)^{11} \pmod{9}$

  $\equiv (-2048) \equiv 4 \pmod{9}$

- $22^{22} \equiv 2^{22} \equiv 4 \pmod{10}$

- $22^{22} \equiv 0 \pmod{11}$

$$\begin{array}{r} -2048 \\ 1800 \\ \hline -248 \\ 270 \\ \hline 22 \end{array}$$

d) $a = 1234^5$, $n = 9$, $n = 11$, $n = 99$;

- $1234 \equiv 1 \pmod 9$

  $1234^5 \equiv 1 \pmod 9$

- $1234 \equiv 2 \pmod{11}$

  $2^5 \equiv 32 \equiv 10 \pmod{11}$

- $1234 \equiv 46 \pmod{99}$

  $1234^5 \equiv 46^5 \equiv 205'962'976 \equiv 10 \pmod{99}$

e) $a = 2^{64} - 1, = 2, n = 3, n = 9.$

- $2^{64} - 1 \equiv -1 \equiv 1 \pmod 2$

- $2^{64} \equiv (-1)^{64} \equiv 1 \pmod 3$

  $2^{64} - 1 \equiv 1 - 1 \equiv 0 \pmod 3$

- $2^{64} \equiv (2^8)^8 \equiv 256^8 \equiv 4^8 \equiv 16^4 \pmod 9$

  $\equiv 7^4 \equiv 2401 \equiv 7 \pmod 9$

2.8.9 Si n est un nombre naturel, la n-ième puissance d'un nombre a est, par définition, le produit de n facteurs égaux à a. Ainsi, d'après cette définition, le calcul de a^n nécessite $n-1$ multiplications. On peut cependant obtenir le même résultat en effectuant moins d'opérations.
Voici à titre d'exemple l'évaluation de a^{35}.

- On écrit l'exposant n comme une somme de puissance de 2. Ici, $35 = 32 + 2 + 1$;
- on calcule ensuite les puissances paires de a : $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$, $a^{16} = a^8 \cdot a^8$, $a^{32} = a16 \cdot a^{16}$.
- on multiplie pour terminer les « bons » carrés : $a^{35} = a32 \cdot a^2 \cdot a^1$;

  Le nombre de multiplications nécessaires est dans ce cas de 7, au lieu de 34.

a) Combien de multiplications nécessite cet algorithme pour calculer chacune des puissances suivantes : a^{10}, a^{61}, a^{1000} ?

b) Calculer $835^{25} \pmod{1073}$, en 6 multiplications.