6 Théorème d'Euler

6.1 Montrer que si $\text{pgcd}(a, m) = 1$ et si $\text{pgcd}(b, m) = 1$, alors $\text{pgcd}(a\,b, m) = 1$.

Indication : il y a deux preuves possibles :

1) utiliser les théorèmes de Bézout et de Bachet de Mériziac ;
2) utiliser la proposition de la page 4.1.

6.2 Montrer que si $\text{pgcd}(a, m) = 1$, alors $\text{pgcd}(a^n, m) = 1$ pour tout $n \in \mathbb{N}$.

Ordre d'un élément

6.3 Calculer $2, 4, 8, 16, 32, 64, \ldots, 2^n$

1) modulo 7
2) modulo 10

Que remarque-t-on ?

6.4 Montrer que si on élève un entier a à des puissances positives : $a, a^2, a^3, \ldots$, alors nécessairement deux de ces puissances seront congrues modulo m.

Indication : combien d'éléments y a-t-il dans $\mathbb{Z}/m\mathbb{Z}$?

6.5 Montrer que les conditions suivantes sont équivalentes :

1) a et m sont premiers entre eux ;
2) il existe $k \in \mathbb{N}$ avec $1 \leqslant k < m$ tel que $a^k \equiv 1 \mod m$.

Indications :

1) Supposons qu'il existe $k \in \mathbb{N}$ avec $1 \leqslant k < m$ tel que $a^k \equiv 1 \mod m$.
   Montrer que a et m sont premiers entre eux, grâce à la proposition de la page 4.1.
2) Supposons a et m premiers entre eux.
   (a) Justifier, à l'aide de l'exercice 6.2, que les classes $\overline{1}$, $\overline{a}$, $\overline{a^2}$, $\overline{a^3}$, …, $\overline{a^{m-1}}$ sont des unités de $\mathbb{Z}/m\mathbb{Z}$.
   (b) Combien y a-t-il au plus d'unités dans $\mathbb{Z}/m\mathbb{Z}$?
   (c) En déduire qu'il existe $n \geqslant 0$ et $1 \leqslant k \leqslant m-1$ tels que $\overline{a^{n+k}} = \overline{a^n}$, c'est-à-dire $a^{n+k} \equiv a^n \mod m$.
   (d) Conclure que $a^k \equiv 1 \mod m$, grâce à l'exercice 4.2.

Soit a un entier premier à m. L'exercice précédent implique l'existence d'un entier k avec $1 \leqslant k < m$ tel que $a^k \equiv 1 \mod m$.

Le plus petit entier positif α tel que $a^\alpha \equiv 1 \mod m$ s'appelle l'**ordre** de a modulo m.

6.6 Trouver l'ordre des éléments non nuls de $\mathbb{Z}/5\mathbb{Z}$.

6.7 Trouver l'ordre des unités de $\mathbb{Z}/9\mathbb{Z}$.

6.8 Trouver l'ordre de $\overline{2}$ dans $\mathbb{Z}/m\mathbb{Z}$ pour les valeurs 11, 17, 31, 9 et 14 de m.

6.9 Trouver l'ordre des éléments non nuls de $\mathbb{Z}/11\mathbb{Z}$.

Théorème d'Euler

Si a et m sont premiers entre eux, alors $a^{\varphi(m)} \equiv 1 \mod m$.

6.10 Le but de cet exercice est de prouver le théorème d'Euler.

1) Soit $(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{r}_1 ; \overline{r}_2 ; \ldots ; \overline{r}_{\varphi(m)}\}$ l'ensemble des unités de $\mathbb{Z}/m\mathbb{Z}$.
   (a) Justifier, à l'aide de l'exercice 6.1, que $\overline{a\, r_i}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ quel que soit $1 \leqslant i \leqslant \varphi(m)$.
   (b) Montrer que l'application
   $$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* \\ \overline{r_i} & \longmapsto & \overline{a\, r_i} \end{array}$$
   est bijective.
2) En déduire que $(a\, r_1)\,(a\, r_2)\,(a\, r_3)\,\ldots\,(a\, r_{\varphi(m)}) \equiv r_1\, r_2\, r_3\,\ldots\, r_{\varphi(m)} \mod m$ et conclure que $a^{\varphi(m)} \equiv 1 \mod m$.

6.11 Soit $\overline{a}$ une unité de $\mathbb{Z}/m\mathbb{Z}$. Montrer que son inverse vaut $\overline{a^{\varphi(m)-1}}$.

6.12 **(Petit) théorème de Fermat**
Si p est premier et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \mod p$.

Démontrer ce théorème à l'aide du théorème d'Euler.

6.13 Soient a et m deux entiers premiers entre eux. Montrer que si l'ordre de a modulo m est α et si $a^k \equiv 1 \mod m$, alors α divise k.

Indication : la division euclidienne de k par α donne $k = \alpha\, q + r$ avec $0 \leqslant r < \alpha$; montrer que $r = 0$.

6.14 Trouver l'ordre des éléments non nuls de $\mathbb{Z}/13\mathbb{Z}$.

6.15 Trouver l'ordre des éléments non nuls de $\mathbb{Z}/17\mathbb{Z}$.

6.16 Trouver l'ordre des unités de $\mathbb{Z}/24\mathbb{Z}$.

6.17 Trouver le plus petit résidu non négatif de 2^{47} modulo 23.

6.18 Montrer, à l'aide du petit théorème de Fermat, que si 7 ne divise pas n, alors 7 divise $n^{12} - 1$.

6.19 Montrer que $n^{13} - n$ est divisible par 2, 3, 5, 7 et 13 pour tout entier n.

Indication : montrer par exemple que $n^{13} \equiv n \mod 5$ en montrant que ou bien 5 divise n, ou bien $n^4 \equiv 1 \mod 5$.

6.20 Montrer que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ est un entier pour tout entier n.

Indication : multiplier l'expression par 15 et montrer que l'entier obtenu est divisible par 5 et par 3 en utilisant le petit théorème de Fermat.

Réponses

6.3 1) $2^n \equiv \begin{cases} 2 & \text{si } n \equiv 1 \mod 3 \\ 4 & \text{si } n \equiv 2 \mod 3 \\ 1 & \text{si } n \equiv 3 \mod 3 \end{cases}$ 2) $2^n \equiv \begin{cases} 2 & \text{si } n \equiv 1 \mod 4 \\ 4 & \text{si } n \equiv 2 \mod 4 \\ 8 & \text{si } n \equiv 3 \mod 4 \\ 6 & \text{si } n \equiv 4 \mod 4 \end{cases}$

Les puissances de 2^n reprennent de façon cyclique les puissances précédentes.

6.6

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
Ordre :	1	4	4	2

6.7

Élément :	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
Ordre :	1	6	3	6	3	2

6.8

m :	11	17	31	9	14
Ordre :	10	8	5	6	non inversible

6.9

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
Ordre :	1	10	5	5	5	10	10	10	5	2

6.14

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
Ordre :	1	12	3	6	4	12	12	4	3	6	12	2

6.15

Élément :	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$
Ordre :	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

6.16

Élément :	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$	$\overline{19}$	$\overline{23}$
Ordre :	1	2	2	2	2	2	2	2

6.17 8