Exercice 1

Exercice 2

Exercice 3

Exercice 4

Exercice 5

1.

2.

3.

4.
$\forall a \in \mathbb{F}_p^\times, \mathrm{ord}(a) \mid p-1$

$$a^{p-1} = a^{b\ \mathrm{ord}(a)} = \left(a^{\mathrm{ord}(a)}\right)^b = 1^b = 1$$
$$a^{p-1} = 1 \mod p$$
$$\text{donc } a^p = a \mod p$$

5.
Montrons $\forall n \in \mathbb{N}, \mathcal{P}(n)$: “dans un anneau commutatif intègre un polunome non nul de degré n possède au plus n racines” par récurrence sur n.

Initialisation: $\mathcal{P}(0)$: Le polynome constant possède 0 racine

Hérédité:
Soit $n \in \mathbb{N}$ tq $\mathcal{P}(n-1)$. Soit P un polynome de degré $n+1$

Bon voilà

Exercice 6

1.
On cherche l'ordre de 5 dans $\mathbb{F}_{23}^\times$ $\mathbb{F}_p^\times$ est d'ordre $p-1 = 22 = 11 \times 2$

D'après le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe

donc l'ordre de 5 divise 22
- 1: $5^1 = 5 \neq 1 \mod 3$
- 2: $5^2 = 25 = 2 \neq 1 \mod 3$
- 11: $5^{11} = \left(5^2\right)^5 \times 5 = 22 \neq 1 \mod 3$
- 22 reste le seul ordre possible par élimination

Donc 5 est d'ordre $22 = p-1$ donc 5 est un générateur de $\mathbb{F}_{23}^X$

Exercice 7

Exercice 8

1.

2.

$x = 1 \bmod 9 \Leftrightarrow x = 1 + 9k, k \in \mathbb{Z}$
$x = 2 \bmod 8 \Leftrightarrow 1 + 9k = 2 \bmod 8$
$\Leftrightarrow k = 1 \bmod 8$
$\Leftrightarrow k = 1 + 8t$

$\ldots \Leftrightarrow t = 4 + 5u$

$\ldots \Leftrightarrow u = 6 + 7v$
On reporte dans le système $x = 2458 + 2520v$ donc $x = 2458 \bmod 2520$

Il y a des formules de con mais non notés car vraiment formules de con

Exercice 9

1.

Soit d vérifiant cette hypothèse. On a alors $7d = 1 \bmod 20 \Leftrightarrow d = 3 \bmod 20$.

2.

on veut calculer $14^3 \bmod 33$

$\begin{cases} c_p = 14 = 2 \bmod 3 \\ m_q = 14^3 = 2 \bmod 11 \end{cases}$

Exercice 10

1.

$\text{pgcd}(a, n) = 1 \Rightarrow a$ inversible $\bmod n$

Par déf $\text{ord}((\mathbb{Z}/n\mathbb{Z})^\times) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$

Théorème de Lagrange: $a \in (\mathbb{Z}/n\mathbb{Z})^\times, \text{ord}(a) \mid \text{ord}((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$ donc $\varphi(n) = l \ \text{ord}(a)$ donc $a^{\varphi(n)} = a^{l \times \ \text{ord}(a)} = 1^l = 1 \bmod n$

2.

Énoncé: Soit $a \in \mathbb{Z}$ et p premier, alors $a^p = a \bmod p$

- Si a est multiple de p: $a = lp$, $(lp)^p = 0 \bmod p = p \bmod p$
- Si a est n'est pas multiple de $p \Rightarrow \text{pgcd}(a, p) = 0$. D'après 1, $a^{\varphi(n)} = 1 \bmod p$ et $\varphi(n) = p - 1$ donc on multiplie par a, on a le résultat

3.

cf fiche.

4.

Si:

- $m = 0$ $(0^e)^d = 0 \bmod n$

- m est premier avec n. On dait que $ed = 1 \bmod \varphi(n) \Leftrightarrow ed = 1 + k\varphi(n)$
  donc $m^{ed} = m^{1+k\varphi(n)} = m \times 1 \bmod n$
- m n'est pas premier avec n n multiple de p, premier avec q ou m multiple de q, premier avec p cas symétriques, on suppose que m est multiple de p et premier avec q.
  p et q étant premiers entre eux, on peut appliquer le th des restes chinois. On a alors $m \bmod p = 0, m \bmod q = m_q$. On a alors $m_q^{ed} = m_q \bmod q$ car $m^{\varphi(q)} = 1 \bmod q$ et $ed = 1 + k\varphi(p)\varphi(q)$.

  On a donc $\begin{cases} x = 0 \bmod p \\ x = m_q \bmod q \end{cases}$. m vérifie cette équation, et d'après le théorème chinois c'est l'unique solution.