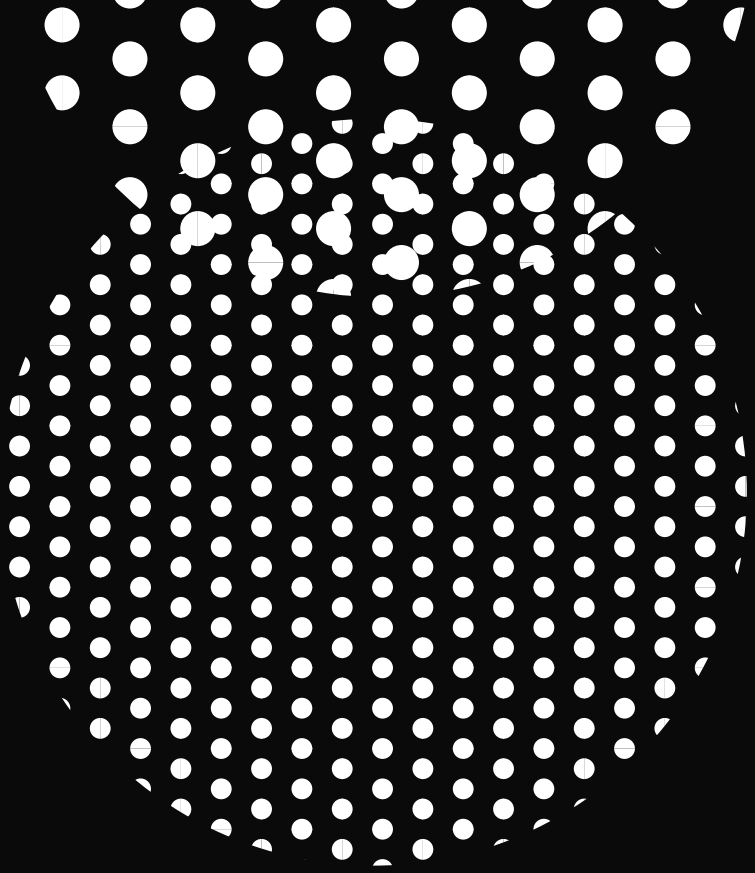

Exercice 10

$$
\begin{array}{r|l}
X^{2n} & X^2-1 \\
\hline
X^{2n}-X^{2n-2} & X^{2n-2}+X^{2n-4}+\dots+1 \\
\hline
X^{2n-2} & \\
\vdots & \\
\hline
X^2 & \\
\hline
X^2-1 & \\
\hline
1 &
\end{array}
$$

$$
\begin{aligned}
X^{2n} &\equiv (X^2)^n \quad [X^2-1] \\
&\equiv 1^n \quad [X^2-1] \\
&\equiv 1 \quad [X^2-1]
\end{aligned}
$$

$$
\begin{aligned}
X^{21}+X^{19}+X^{17} &\equiv X^{20}X + X^{18}X + X^{16}X \quad [X^2-1] \\
&\equiv X + X + X \quad [X^2-1] \\
&\equiv 3X \quad [X^2-1] \\
&\equiv
\end{aligned}
$$

b) $X^{45}-X^{43}+1 \equiv 1^{45}-1^{43}+1 \quad [X-1]$

$\equiv 1-1+1 \quad [X-1]$

$\equiv 1 \quad [X-1]$

$X \equiv 1 \quad [X-1]$

$X^{45}-X^{43}+1 = X^{43}(X^2-1)+1$

$= \underbrace{X^{43}(X-1)(X+1)}_{Q} + \underbrace{1}_{R}$ reste est : 1

$P(X) = X^{45}-X^{43} = X^{43}(X-1)(X+1)$ donc $X-1 \mid X^{45}-X^{43}$

$P'(X) = 45X^{44}-43X^{42}$ donc $P'(1) = 45-43 = 2 \neq 0$

d'où $(X-1)^2 \nmid P(X)$

$P = (X-1)^2 Q \qquad P' = 2(X-1)Q + (X-1)^2 Q'$

$= (X-1)\underbrace{(2Q + (X-1)Q')}_{Q'}$

$X^{45} - X^{43} + 1 = (X^{43}(X+1))(X-1) + 1$ $\qquad X^2 \equiv 2X-1 \ [X^2-2X+1]$

$X^{43}(X+1) \equiv 2 \qquad [X-1]$

$X^{43}(X+1) = (X-1)Q + 2$

d'où $X^{45} - X^{43} + 1 = ((X-1)Q+2)(X-1) + 1$

$= (X-1)^2 Q + 2X - 1$

donc le reste est $2X-1$

c) $X^{96} - X^{29} \equiv (X^2)^{48} - (X^2)^{11} X \ [X^2+1]$

$\equiv (-1)^{48} - (-1)^{11} X \ [X^2+1]$

$\equiv 1 + X \ [X^2+1]$

Exercice 12

a)

$X^3 - X^2 + X - 1$	$X-1$
$X^3 - X^2$	X^2+1
$X - 1$	
$X - 1$	
0	

$(X^2+1)(X-1) = X^3 - X^2 + X - 1 = X^2(X-1) + (X-1)$

$= \underbrace{(X^2+1)(X-1)}_{P}$

$(X^2 - X + 1)^n - X^{2n} + X^n - 1 =: Q_n$

$P \mid Q_n \iff X-1 \mid Q_n$ et $X^2+1 \mid Q_n$ car $(X-1) \wedge (X^2+1) = 1$

$Q_n(1) = 1^n - 1^{2n} + 1^n - 1 = 1 - 1 + 1 - 1 = 0 \quad \forall n \in \mathbb{N}^*$

$Q_n \equiv (-1-X+1)^{4n} - (-1)^n + X^n - 1 \quad [X^2+1]$

$\equiv (-X)^n - (-1)^n + X^n - 1 \quad [X^2+1]$

$\equiv X^n(1 + (-1)^n) - (1 + (-1)^n) \quad [X^2+1]$

$\equiv (X^n - 1)(1 + (-1)^n) \quad [X^2+1]$

Si n impair $Q_n \equiv 0 \ [X^2+1]$ donc $P \mid Q_n$

Si n pair $\exists n' \in \mathbb{N}$ tq $n = 2n'$

$Q_n \equiv 2(X^{2n'} - 1) \ [X^2+1]$

$\equiv 2((-1)^{n'} - 1) \ [X^2+1]$

Si n' pair $\exists n'' \in \mathbb{N}$ tq $n' = 2n''$, $Q_n \equiv 0 \ [X^2-1]$ donc $P \mid Q_n$

Si n' impair $Q_n \equiv -4 \ [X^2-1]$ donc $P \nmid Q_n$

finalement, $P \mid Q_n \iff n$ impair ou $4 \mid n$.

Exercice 15

Soient $m, n \geq 1$ et $d = m \wedge n$

a) $\exists z \in \mathbb{C}$ tq $z^m = z^n = 1$

XYITA $\iff (z^d)^{m'} = (z^d)^{n'} = 1$

$\Rightarrow \left((z^d)^{m'}\right)^{\frac{1}{m'}} = 1^{\frac{1}{m'}}$

$\Rightarrow z^d = 1$

$\exists u, v \in \mathbb{Z}$ tq $d = um + vn$

$(*)$ et $z^d = z^{um+vn} = (z^m)^u \cdot (z^n)^v = 1^u \cdot 1^v = 1$

$\Rightarrow z^d = 1$

racine de l'unité

$X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z)$ et $|\mathbb{U}_n| = n$ avec $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$

$= \{ e^{\frac{2ik\pi}{n}}, k \in \{1, \dots, n\} \}$

$X^m - 1 = \prod_{z \in \mathbb{U}_m} (X - z)$

$\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_d$ car $\mathbb{U}_n \cap \mathbb{U}_m \subset \mathbb{U}_d$ par (*)

$\mathbb{U}_d \subset \mathbb{U}_n \cap \mathbb{U}_m$ car si $z \in \mathbb{U}_d$ $z^n = (z^d)^{\frac{n}{d}} = 1$

$z^m = (z^d)^{\frac{m}{d}} = 1$

donc $(X^n - 1) \wedge (X^m - 1) = \prod_{z \in \mathbb{U}_d} (X - z) = X^d - 1$

b) On suppose $m \geq n$ et $m \equiv r [n] \Rightarrow \exists k \in \mathbb{N}$ tq $m = kn + r$

$X^m - 1 \equiv X^{qn+r} - 1 \equiv (X^n)^q X^r - 1 \quad [X^n - 1]$

$\equiv 1^q X^r - 1 \quad [X^n - 1]$

$\equiv X^r - 1 \quad [X^n - 1]$

$(X^m - 1) \wedge (X^n - 1) = (X^n - 1) \wedge (X^r - 1) = \dots = \dots = X^d - 1$

donc a)

c) $P \in \mathbb{C}[X]$

(i) $\text{pgcd}(X^m - 1, X^n - 1) = X^d - 1 \iff \exists U, V \in \mathbb{C}[X]$

$U(X^m - 1) + V(X^n - 1) = X^d - 1$

donc $\underbrace{(U \circ P)}_{U' \in \mathbb{C}[X]} (P^m - 1) + \underbrace{(V \circ P)}_{V' \in \mathbb{C}[X]} (P^n - 1) = P^d - 1$

$U'(P^m - 1) + V'(P^n - 1) = P^d - 1$

d'où $\operatorname{pgcd}(p^n-1, p^m-1) \mid p^d-1$

Identité de Bernoulli :

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})$$

On a : $p^n - 1 = (p^d)^{n'} - 1$ avec $n' \in \mathbb{N}$ tq $n = n'd$

$= (p^d - 1)\underbrace{((p^d)^{n-1} + \dots + 1)}_{\in \mathbb{Z}[X]}$ donc $p^d - 1 \mid p^n - 1$

de même $p^d - 1 \mid p^m - 1$

donc $p^d - 1 \mid \operatorname{pgcd}(p^n - 1, p^m - 1)$

Finalement, $\operatorname{pgcd}(p^n - 1, p^m - 1) = p^d - 1$

(ii) Si $m \wedge n = 1$, $(p^n - 1) \wedge (p^m - 1) = p - 1$

On a : $p^{nm} - 1 = (p^n)^m - 1 = (p^n - 1) \cdot Q$

$= (p^m)^n - 1 = (p^m - 1) \cdot Q'$

et $p^{nm} - 1 = (p-1)Q''$ donc $p - 1 \mid p^{nm} - 1$

$p^n - 1 \mid p^{nm} - 1$

$p^m - 1 \mid p^{nm} - 1$

Donc $\dfrac{p^n - 1}{p - 1} \mid \dfrac{p^{nm} - 1}{p - 1}$ et $\dfrac{p^m - 1}{p - 1} \mid \dfrac{p^{nm} - 1}{p - 1}$

et $\left(\dfrac{p^n - 1}{p - 1}\right) \wedge \left(\dfrac{p^m - 1}{p - 1}\right) = 1$

donc $\left(\dfrac{p^n - 1}{p - 1}\right)\left(\dfrac{p^m - 1}{p - 1}\right) \mid \dfrac{p^{nm} - 1}{p - 1}$

Soit en multipliant par $(p-1)^2$

$$(p^n - 1)(p^m - 1) \mid (p - 1)(p^{nm} - 1)$$

d)

$$A_n := 1 + x^q + \dots + x^{qn} = \frac{(x^q)^{n+1} - 1}{x^q - 1}$$

$$A_m := 1 + x^q + \dots + x^{qm} = \frac{(x^q)^{m+1} - 1}{x^q - 1}$$

$$A_n \mid A_m \Rightarrow (x^q)^{n+1} - 1 \mid (x^q)^{m+1} - 1$$

$$\Rightarrow \gcd(q(n+1), q(m+1)) = q(n+1)$$

$$\Rightarrow q(n+1) \mid q(m+1)$$

$$\Rightarrow n+1 \mid m+1$$

$\square$