(1) $a^{p-1}-1$ is a mult of p. for $a \in \mathbb{N}$ and p prime.

Suppose $p \in \mathbb{N}$ is prime. (prove that $1 \cdot 2 \cdot \ldots \cdot (p-1)+1$ is divisible by p)

Suppose that $a \in \mathbb{Z}/p\mathbb{Z}$ and that $a \neq 0$.
then by fermat's $\Rightarrow a^{p-1} \equiv 0 \pmod{p}$

Hence all $a \in \mathbb{Z}/p\mathbb{Z}$ except $a=0$ is a root.

So, $x^{p-1}-1 = (x-1) \ldots (x-(p-1)) = f(x)$

$$f(0) = \underbrace{(-1) \ldots -(p-1)}_{\text{even}} = (1) \ldots (p-1)$$

So $f(0) \bmod p \equiv p-1 \Rightarrow (f(0)+1) \bmod p \equiv 0$

Hence $p \mid 1 \cdot 2 \ldots \cdot (p-1)+1$

(2) Show that $x^4+1 \in \mathbb{Q}[x]$ is irreducible.

So x^4+1 has no linear factors bc if it had they must be $(x-1)$ or $(x+1)$ by rational root test.

but $f(\pm 1) \neq 0$.

So it must factor into two quadratics.

$$x^4+1 = (x^2+ax+b)(x^2+cx+d)$$
$$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$$

$$\begin{cases} a+c=0 \\ ac+b+d=0 \\ ad+bc=0 \\ bd=1 \end{cases} \Longrightarrow \begin{cases} b+d=a^2 \\ a(d-b)=0 \\ bd=1 \end{cases} \quad a,d,b \in \mathbb{Q}$$

Case: $a=0 \Rightarrow b^2=-1$, no $b \in \mathbb{Q}$ so can't happen $\lightning$

Case: $a \neq 0 \Rightarrow 2b = a^2$, no $a \in \mathbb{Q}$ bc $b = \pm 1$ so can't happen $\lightning$ ouch.

Hence x^4+1 is irreducible in $\mathbb{Q}$

(3) Show that x^4+1 splits modulo 2 and 3 explicitly.

$\mathbb{Z}/2\mathbb{Z}$: $x^4+1 \equiv x^4-1$

$x^4-1 = (x^2-1)(x^2+1)$

similarly $x^2+1 \equiv x^2-1$

so, $x^4-1 = (x^2-1)(x^2-1) = (x-1)(x+1)(x-1)(x+1)$

and $x+1 \equiv x-1$

so, $x^4-1 \equiv (x-1)^4$

$\mathbb{Z}/3\mathbb{Z}$: $f(\{0,1,2\}) \neq 0 \Rightarrow$ no linear factors.

must factor into two quadratics:

$$x^4+1 = (x^2+ax+b)(x^2+cx+d)$$
$$= x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd$$

$$\begin{cases} a+c=0 \\ ac+b+d=0 \\ ad+bc=0 \\ bd=1 \end{cases} \Rightarrow \begin{cases} b+d=a^2 \\ a(d-b)=0 \\ bd=1 \end{cases}$$

so either $b, d = (1,1)$ or $(2,2)$

if $b, d = (1,1) \implies$ No soln bc

so $b, d = (2,2) \implies a = 1$, $c = 1$

thus $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$

(4) Show that if m divides n $(m|n)$ then

$$f(x) = \frac{(x^m - 1)}{(x-1)} \text{ divides } \frac{(x^n-1)}{(x-1)} = g(x) \; ; \; g(x) = f(x)h(x)$$

$n = k \cdot m$

Suppose that m divides n, then $m = \frac{n}{k}$

$$f(x) = 1 + x + x^2 + \dots + x^{m-1} \; ; \; g(x) = 1 + x + x^2 + \dots + x^{n-1}$$

$$g(x) = 1 + x + \dots + x^{k \cdot m - 1} \quad \text{for some } k \in \mathbb{Z}$$

$$g(x) = \begin{cases} 1 + x + \dots + x^{m-1} = 1 + x + \dots + x^{m-1} \\ \quad + \qquad\qquad\qquad\qquad + \\ x^m + x^{m+1} + \dots + x^{2m-1} = x^m(1 + x + \dots + x^{m-1}) \\ \quad + \qquad\qquad\qquad\qquad + \\ x^{2m} + x^{2m+1} + \dots + x^{3m-1} = x^{2m}(1 + x + \dots + x^{m-1}) \\ \quad + \qquad\qquad\qquad\qquad + \\ \quad \vdots \\ x^{(k-1)m} + x^{(k-1)m+1} + \dots + x^{km-1} = x^{(k-1)m}(1 + x + \dots + x^{m-1}) \end{cases}$$

$$g(x) = \underbrace{(1 + x + \dots + x^{m-1})}_{f(x)} \underbrace{(1 + x^m + x^{2m} + \dots + x^{(k-1)m})}_{h(x)}$$

$$\Rightarrow f(x) \mid g(x) \checkmark$$