$d = \gcd((n+1)!+1, n!+1)$

d must divide any linear combination of $\underline{(n+1)!+1}$ & $\underline{n!+1}$.

Find some x, y such that $x((n+1)!+1) + y(n!+1)$. is "nice"

and then $d \mid$ "nice thing."

$\vdots$

$x(n+1)! + x + yn! + y$

$-(n+1)! - 1 + n! + 1.$

$n! - (n+1)!$

$= n!(1-(n+1))$

$= n!(-n)$

$= -n!n$

$d \mid (n!n)$

could assume for a contradiction that $d > 1$, and then the fundamental thm of arithmetic tells us that there exists a prime $p \mid d$.

$p \mid d \mid (n!n)$

$\Rightarrow p \mid (n!n)$

$\xRightarrow[\text{(p is prime)}]{\text{Euclid's lemma}} p \mid n!$ or $p \mid n$.

$\Rightarrow p \mid n!$

$p \mid n!$ $\quad p \mid (n!+1)$

$p \mid (n!+1) - n!$

$p \mid 1$

$n! \equiv 0 \pmod p$

$n!+1 \equiv 1 \pmod p$

So $n!+1$ is not div by p.

5.2 (b). $\gcd(a,42)=1$ $\qquad 168 = 3\cdot 7\cdot 8$ divides a^6-1.

$\uparrow$

$42 = 6\cdot 7 = 2\cdot 3\cdot 7.$

Saying $\gcd(a,42)=1$ means that a is not div. by 2 or 3 or 7.

Fermat's thm:

$$a^{2-1}\equiv 1 \pmod 2 \longrightarrow a\equiv 1 \pmod 2$$
$$a^{3-1}\equiv 1 \pmod 3 \longrightarrow a^2\equiv 1 \pmod 3$$
$$a^{7-1}\equiv 1 \pmod 7 \longrightarrow a^6\equiv 1 \pmod 7$$

$$\longrightarrow a^6\equiv 1 \pmod 2$$
$$\longrightarrow a^6\equiv 1 \pmod 3$$
$$\longrightarrow a^6\equiv 1 \pmod 7$$

Tells us that a^6-1 is div by 2 & 3 & 7.
Need to show that it's also div by 8.

$$\begin{aligned}(a^6-1) &= (a^3-1)(a^3+1)\\ &= (a-1)(a^2+a+1)(a^3+1)\\ &= (a-1)(a^2+a+1)(a+1)(a^2-a+1)\\ &= \underbrace{(a-1)}_{\text{even}}\underbrace{(a+1)}_{\text{even}}\,\underbrace{(a^2+a+1)(a^2-a+1)}_{\text{odd}}.\end{aligned}$$

consecutive evens, so one of them must be divisible by 4.

either $a+1$ or $a-1$ is of the form $4k$. the other one is still even, so it's of the form 2ℓ

$$(a^6-1) = 4k\cdot 2\ell\cdot (a^2+a+1)(a^2-a+1)$$
$$= 8\underbrace{k\ell(a^2+a+1)(a^2-a+1)}_{\text{integer}}.$$

so one gives me a factor of 4, the other gives me a factor of 2, so overall, I do get the factor of 8 that I needed.

$$a^6\equiv 1 \pmod 8 \Longrightarrow a^6\equiv 1 \pmod 2$$

false!