Ex 4:

Find a basis a for: $a^{13} \equiv 17 \pmod{31}$

1) usually a difficult problem, but 31 is prime!

Apply Prop. 7.5 to show that 17 is a primitive element modulo 31 (p. 53)

$\Leftrightarrow 17^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \quad \forall i = 1, \dots, k$, where $p-1 = \prod_{i=1}^{k} p_i^{e_i}$

here:

$p = 31 \Rightarrow p-1 = 30 = 2 \cdot 3 \cdot 5$

check: $17^{\frac{30}{2}} \equiv 30, \; 17^{\frac{30}{3}} \equiv 25, \; 17^{\frac{30}{5}} \equiv 8, \not\equiv 1 \pmod{31}$

$\Rightarrow$ 17 is a primitive element ✓

2) Knowing that 17 is a primitive element modulo 31

$\exists b: 17^b \equiv a \pmod{31}$

$(a^{13})^b \equiv a \pmod{31}$

$\rightarrow a^{13b-1} \equiv 1 \pmod{31}$

With Th. 6.2: Let $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

(Fermats' little theorem, p. 43)

here: $a^{\varphi(n)} \equiv a^{30} \equiv 1 \pmod{31}$

$a^{13b-1} \equiv a^{30} \equiv 1 \pmod{31}$

$\Leftrightarrow 13b - 1 \equiv 30 \pmod{30}$ (see Ex 3, $\mathrm{ord}_n(a) = \varphi(n)$)

$\Leftrightarrow 13b \equiv 1 \pmod{30}$

$\Leftrightarrow b \equiv 13^{-1} \pmod{30}$

EEA:

$30 = 13 \cdot 2 + 4$

$13 = 4 \cdot 3 + 1$

$1 = 13 - 4 \cdot 3$

$= 13 - (30 - 13 \cdot 2) \cdot 3$

$= 13 \cdot 7 - 30 \cdot 3$

$13^{-1} = b$

$\Rightarrow a \equiv 17^{7} \equiv 12 \pmod{31}$