Seja $f(x) = x^2 - 1$ um polinômio com coeficiente em $\mathbb{Z}_{30}$.

$\mathbb{Z}_{30} = \{0, 1, \ldots, 29\}$

$f(x) = x^2 - 1$

$f(1) = 1^2 - 1 = 0$ ✓

$f(2)^2 = 4 - 1 = 3$

$f(3)^2 = 9 - 1 = 8$

$f(4)^2 = 16 - 1 = 15$

$f(5)^2 = 25 - 1 = 24$

$f(6) = 36$

$6 - 1 = 5$

$f(7) = 49 \longrightarrow 19 - 1 = 18$

$f(8) = 64 \longrightarrow 4 - 1 = 3$

$f(9) = 81 \longrightarrow 21 - 1 = 20$

$f(10) = 100 \longrightarrow 10 - 1 = 9$

$f(11) = 121 \longrightarrow 1 - 1 = 0$ ✓

$f(12) = 144 \longrightarrow 24 - 1 = 23$

$f(13) = 169 \longrightarrow 19 - 1 = 18$

$f(14) = 196 \longrightarrow 16 - 1 = 15$

$f(15) = 225 \Rightarrow 15 - 1 = 14$

$f(16) = 256 \longrightarrow 16 - 1 = 15$

$f(17) = 289 \longrightarrow 19 - 1 = 18$

$f(18) = 324 \longrightarrow 24 - 1 = 23$

$f(19) = 361 \longrightarrow 1 - 1 = 0$ ✓

$f(20) = 400 \longrightarrow 10 - 1 = 9$

$f(21) = 441 \longrightarrow 21 - 1 = 20$

$f(22) = 484 \longrightarrow 24 - 1 = 23$

$f(23) = 529 \longrightarrow 19 - 1 = 18$

$f(24) = 576 \longrightarrow 6 - 1 = 5$

$f(25) = 625 \longrightarrow 25 - 1 = 24$

$f(26) = 676 \to 16 - 1 = 15$

$f(27) = 729 \to 9 - 1 = 8$

$f(28) = 784 \to 24 - 1 = 23$

$f(29) = 841 \to 1 - 1 = 0$

Portanto todas as raízes de $f(x)$ em $\mathbb{Z}_{30}$ são: 29, 19, 11, 1, todos números primos cujo seus quadrados mod 30 dão resto 1.

Explique porque sobre este anel o número de raízes é maior que o grau do polinômio.

Pelo teorema 10.35: Temos R sendo DFU, e r, s elementos de R. Temos $f(x)$ e $g(x)$ sendo polinômios primitivos em $R[x]$ sendo que: $r f(x) = s g(x)$. Então r e s são associados em R e $f(x)$ e $g(x)$ são associados em $R[x]$.

Portanto como $f(x)$ possui raízes $\neq 1$, então em $\mathbb{Z}_{30}$ terá raízes. Mas como em $\mathbb{Z}_{30}$ alguns elementos ao quadrado cujos os valores mod 30 é 1, então:

$1 \longrightarrow 121 \to 361 \to 841$

Temos $f(x)$ é uma primitiva, e:

$1 = 1^2 \rightarrow 121 = 11^2 \rightarrow 361 = 19^2 \rightarrow 841 = 29^2$

Então em $\mathbb{Z}_{30}$ a $f(x)$ se torna cíclica para valores de $f(x) = 0$.