6

The field $\mathbb{F}_7[x]/(x^2+1)$ is a field with 49 elements, which for the moment we denote by $\mathbb{F}_{49}$. (See Example 2.58 for a convenient way to work with $\mathbb{F}_{49}$.)

a

Is $2+5x$ a primitive root in $\mathbb{F}_{49}$?

✓ **Answer**

$$
\begin{aligned}
&49-1=48=2^4\cdot 3\\
&(2+5x)^{24}\\
&=(2-2x)^{24}\\
&=(4-8x+4x^2)^{12}\\
&=(x)^{12}\\
&=(x^2)^6\\
&=(-1)^6\\
&=1
\end{aligned}
$$

Thus, $2+5x$ is not a primitive root of $\mathbb{F}_{49}$

b

Is $2+x$ a primitive root in $\mathbb{F}_{49}$?

✓ **Answer**

$$
\begin{aligned}
&(2+x)^{24}\\
&=(4+4x+x^2)^{12}\\
&=(3+4x)^{12}\\
&=(9+24x+16x^2)^6\\
&=(3x)^6\\
&=(9x^2)^3\\
&=(5)^3\\
&=-1
\end{aligned}
$$

$$
\begin{aligned}
&(2+x)^{16}\\
&=(5)^2\\
&=3
\end{aligned}
$$

Thus, $2+x$ is a primitive root of $\mathbb{F}_{49}$

c

Is $1+x$ a primitive root in $\mathbb{F}_{49}$? (Hint. Lagrange's theorem says that the order of $u \in \mathbb{F}_{49}$ must divide 48. So if $u^k \neq 1$ for all proper divisors k of 48, then u is a primitive root.

✓ **Answer**

$$
\begin{aligned}
&(1+x)^{24} \\
&= (2x)^{12} \\
&= (-4)^6 \\
&= (2)^3 \\
&= 1
\end{aligned}
$$

Thus, $1+x$ is not a primitive root in $\mathbb{F}_{49}$