

#54: We have to show: if F is a field with infinitely many elements, then $p(x_i) = q(x_i)$ for all $x_i \in F$ implies $p = q$

Let $g := p - q$. We then have, by hypothesis,

$$g(x_i) = 0 \text{ for all } x_i \in F$$

But then $X - x_i$ must be a factor of g . This is impossible if F has more elements than $\deg g$

#55: By trying all possibilities (or by using the prime factor decomposition in $\mathbb{Z}$): the roots of X^2 in $\mathbb{Z}_{25}$ are: 0, 5, 10, 15, 20

$$X \cdot X = (X-5)(X+5) = (X-10)(X+10) = (X-15)(X+15) = (X-20)(X+20) \quad \text{are three (!) different factorizations of } X^2 \text{ in } \mathbb{Z}_{25}$$

Three only? - Yes. $X-5 = X+20$. Less delusively written:

$$X \cdot X = (X+5)(X+20) = (X+10)(X+15)$$

#56: The elements of $\mathbb{Z}_2[X]/I$ are:

$$\begin{aligned} [0]_I &=: 0 \\ [1]_I &=: i \\ [X]_I &=: j \\ [X+1]_I &= j+1 \\ [X^2]_I &= j^2 \\ [X^2+1]_I &= j^2+1 \\ [X^2+X]_I &= j^2+j \\ [X^2+X+1]_I &= j^2+j+1 \end{aligned}$$

Note: Since

$$[X^3+X+1]_I = [0]_I$$

$$\text{we have } j^3+j+1=0$$

I'll omit the trivial rows/columns 0 and 1 from the table.

	j	$j+1$	j^2	j^2+1	j^2+j	j^2+j+1
j	j^2	j^2+j	$j+1$	1	j^2+j+1	j^2+1
$j+1$	j^2+j	j^2+1	j^2+j+1	j^2	1	j
j^2	$j+1$	j^2+j+1	j^2+j	j	j^2+1	1
j^2+1	1	j^2	j	j^2+j+1	$j+1$	j^2+j
j^2+j	j^2+j+1	1	j^2+1	$j+1$	j	j^2
j^2+j+1	j^2+1	j	1	j^2+j	j^2	$j+1$

From the table we can read off now: $(j+1)^{-1} = j^2+j$