

#53: Whenever $\mathbb{Z}_p$ has an ^{element} number i st. $i^2 + 1 = 0$
the factorization $(X^2 + i)(X^2 - i)$ is possible.

Whenever $\mathbb{Z}_p$ has an element z st. $z^2 - 2 = 0$
the factorization $(X^2 + zX + 1)(X^2 - zX + 1)$ is possible.

Whenever $\mathbb{Z}_p$ has an element u st. $u^2 + 2 = 0$
the factorization $(X^2 + uX - 1)(X^2 - uX - 1)$ is possible.

If two of the above hold (eg if we have elements i, z)
then they hold all three (namely in this example $u = iz$
satisfies $u^2 = i^2 z^2 = (-1)(2) = -2$; and ~~similarly~~
similarly in the other cases), and then we have the
factorization $(X - 2^{-1}(iz + z))(X - 2^{-1}(iz - z))(X - 2^{-1}(-iz + z))(X - 2^{-1}(-iz - z))$
This latter case does not ~~happen~~ ^{apply} for $p = 2$ (where 2^{-1} doesn't exist).

Factorizations of $X^4 + 1$ are:

$$(X+1)^4 \quad \text{in } \mathbb{Z}_2[X]$$

$$(X^2 + X - 1)(X^2 - X - 1) \quad \text{in } \mathbb{Z}_3[X]$$

$$(X^2 + 2)(X^2 - 2) \quad \text{in } \mathbb{Z}_5[X]$$

$$(X^2 - 3X + 1)(X^2 + 3X + 1) \quad \text{in } \mathbb{Z}_7[X]$$

$$(X^2 + 3X - 1)(X^2 - 3X - 1) \quad \text{in } \mathbb{Z}_{11}[X]$$

$$(X^2 + 5)(X^2 - 5) \quad \text{in } \mathbb{Z}_{13}[X]$$

$$(X-2)(X+2)(X-8)(X+8) \quad \text{in } \mathbb{Z}_{17}[X]$$

$$(X^2 - 6X - 1)(X^2 + 6X - 1) \quad \text{in } \mathbb{Z}_{19}[X]$$

$$(X^2 - 5X + 1)(X^2 + 5X + 1) \quad \text{in } \mathbb{Z}_{23}[X]$$

$$(X^2 + 12)(X^2 - 12) \quad \text{in } \mathbb{Z}_{29}[X]$$

p	$x^2 + 1 = 0$	$x^2 - 2 = 0$	$x^2 + 2 = 0$
2	1	0	0
3	DNE	DNE	1
5	2	DNE	DNE
7	DNE	3	DNE
11	DNE	DNE	3
13	5	DNE	DNE
17	4	6	7
19	DNE	DNE	6
23	DNE	5	DNE
29	12	DNE	DNE