Consider the polynomial $x^4 - 2x^2 + 9$. Its roots over $\mathbb{Q}$ are easily checked to be $\pm \sqrt{2} \pm i$; over $\mathbb{R}$ it factors as $(x^2 - 2\sqrt{2}x + 3)(x^2 + 2\sqrt{2}x + 3)$ which does not have rational coefficients. Combining the linear factors in other ways does not even give real coefficients since the roots will not occur in conjugate pairs. Thus the polynomial is irreducible over $\mathbb{Q}$. One can also check this by noting that the splitting field of the minimal polynomial of $\sqrt{2} + i$ is $\mathbb{Q}(\sqrt{2}, i)$ since

$$i = \frac{1}{6} \left( (\sqrt{2} + i) + (\sqrt{2} + i)^3 \right) \quad \text{and} \quad \sqrt{2} = \frac{5}{6} (\sqrt{2} + i) - \frac{1}{6} (\sqrt{2} + i)^3.$$ 

Since $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$, the minimal polynomial has degree 4, hence must be $x^4 - 2x^2 + 9$.

**Theorem.** For any prime number $p$ the polynomial $x^4 - 2x^2 + 9$ is reducible in $\mathbb{Z}_p[x]$.

**Proof.** $p = 2$ is special. In this case $x^4 - 2x^2 + 9 \equiv x^4 + 1 \equiv (x + 1)^4 \pmod{2}$.

Now assume that $p$ is odd and note that the multiplicative group of $\mathbb{Z}_p$ modulo squares has exactly two elements: the kernel of the group homomorphism $\mathbb{Z}_p^* \to \mathbb{Z}_p^{*2}$ is $\{-1, 1\}$, so we get $\mathbb{Z}_p^* \cong \mathbb{Z}_p^{*2} \times \{-1, 1\}$. Thus there are exactly 2 cosets in $\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$. So the product of any two nonsquares is a square modulo $p$. From the equation $-1 \cdot 2 = -2$ we see that at most two of the 3 numbers $-1, 2, -2$ can be nonsquares. There are now 3 cases in factoring $x^4 - 2x^2 + 9$.

1. $2 = a^2$ in $\mathbb{Z}_p$. Then $x^4 - 2x^2 + 9 = (x^2 - 2ax + a^2 + 1)(x^2 + 2ax + a^2 + 1)$.
2. $-1 = a^2$ in $\mathbb{Z}_p$. Then $x^4 - 2x^2 + 9 = (x^2 - 2ax + a^2 - 2)(x^2 + 2ax + a^2 - 2)$.
3. $-2 = a^2$ in $\mathbb{Z}_p$. Then $x^4 - 2x^2 + 9 = (x^2 - 2ax + a^2 - 1)(x^2 + 2ax + a^2 - 1)$.

Is it true that the polynomial splits in $\mathbb{Z}_p[x]$ if and only if all three numbers are squares?

$\square$