Osservazione preliminare.
Sia $(A, +, \cdot)$ un dominio d'integrità. Consideriamo un elemento $a \in A$ non nullo e non-invertibile (quindi $a \notin \mathcal{U}(A)$); siamo interessati a fattorizzare a e cioè ad esprimerlo come $a = mn$. Vogliamo fattorizzarlo come prodotto di due elementi non-invertibili [1]. (Ovviamente non possiamo esprimerlo come prodotto di due invertibili, perché altrimenti a sarebbe lui stesso invertibile, contro l'ipotesi.) Ciò porta alla seguente definizione.
Definizione. Sia $(A, +, \cdot)$ un dominio d'integrità. Un elemento $a \in A$ non nullo e non-invertibile è detto irriducibile se $a = xy$ e $x \notin \mathcal{U}(A) \Rightarrow y \in \mathcal{U}(A)$.
A parole: a non ammette fattorizzazioni con entrambi i fattori non-invertibili.
Esempio. $p \in \mathbb{Z}$ è un numero primo [2] se e solo se p è un elemento irriducibile del dominio d'integrità $(\mathbb{Z}, +, \cdot)$. La verifica è un semplice esercizio.
Definizione. Sia $(A, +, \cdot)$ un dominio d'integrità. Un elemento $a \in A$ non nullo e non-invertibile è detto primo se $a|xy \Rightarrow a|x$ oppure $a|y$.
A parole: se a divide un prodotto allora a divide uno dei due fattori.

Proposizione. Sia $(A, +, \cdot)$ un dominio di integrità. Se $a \in A$ è primo allora a è irriducibile.
Dimostrazione. Supponiamo che $a = xy$. Vogliamo dimostrare che se uno dei due fattori *non* è un invertibile, allora l'altro fattore è un invertibile.
Da $a = xy$ segue che $a|xy$. Dato che a è primo, ne segue che $a|x$ oppure $a|y$. Se $a|x$ allora $x = ra$ per qualche r e quindi $a = ary$ da cui $ry = 1$ e quindi y è un invertibile. Se $a|y$, allora, analogamente, x è un invertibile. Quindi, se $a = xy$ e uno dei fattori non è un invertibile [3] allora l'altro fattore deve necessariamente essere invertibile; quindi a è irriducibile.

[1] è sempre possibile fattorizzarlo come prodotto di un invertibile e di un non invertibile; ad esempio $a = x(x'a)$ con $x \in \mathcal{U}(A)$ e x' il suo inverso

[2] gli unici divisori di p sono ± 1 e $\pm p$

[3] come già osservato, a non può essere prodotto di due invertibili