Risposta al quesito posto nella Nota storica_8

§23

L'enunciato di riferimento è la nostra Proposizione 8.7, secondo cui gli elementi invertibili (che sono, in particolare, cancellabili) dell'anello $\mathbb{Z}_m$, con $m > 1$, sono tutti e soli quelli della forma $[a]_n$, ove a è un intero coprimo con m. Nel testo di Gauss, si afferma, precisamente, che se a è coprimo con m, ogniqualvolta e, f sono interi tali che $[e]_m \neq [f]_m$, si ha $[ae]_m \neq [af]_m$ (una riformulazione equivalente è: se $[a]_m[e]_m = [a]_m[f]_m$, allora $[e]_m = [f]_m$).

§24

L'enunciato di riferimento è contenuto nel nostro Esempio 9.3 (b). Lì si osserva che, ogniqualvolta a è un intero coprimo con l'intero $m > 1$, la congruenza lineare $ax \equiv b \pmod{m}$ ammette sempre soluzione. In altri termini, al variare di x in $\mathbb{Z}$, $[ax]_m$ percorre l'intero insieme $\mathbb{Z}_m$. Ma allora ciò vale anche per $[ax + b]_m$.