pg.	onde se lê	leia-se
186	$\Leftrightarrow J_A = (s_A)^s \bmod n$	$\Leftrightarrow J_A = (s_A)^{-v}$ pois $(s_A)^{-v} = [(J_A)^{-s}]^{-v} = (J_A)^{sv} = J_A \bmod n$
187	(extrair $(x)_0^{-v}$ é ...	(extrair $(x)_0^{v^{-1}}$ é ...
187	$r^v[(s_A)^s(s_A)^v]^e \bmod n$, pois $J_A = (s_A)^s \bmod n$	$r^v[(s_A)^{-v}(s_A)^v]^e \bmod n$, pois $J_A = (s_A)^{-v} \bmod n$
204	1. Se z não satisfizer $1 \leq y \leq (p-1)$,...	1. Se y não satisfizer $1 \leq y \leq (p-1)$,...
205	1. z satisfaz $1 \leq z \leq (p-1)$.	1. y satisfaz $1 \leq y \leq (p-1)$.
205	A verificação $1 \leq z \leq (p-2)$ é ...	A verificação $1 \leq y \leq (p-1)$ é ...
266	Demonstre que se ...	Demonstre ser falso que se ...
267	$\ldots f_2x^2 + f_0$	$\ldots f_1x^2 + f_0$

Sobre Corpo de Galois

Substituir o parágrafo “Pode-se provar que ...” na pg 269 do livro pelo que segue.

Pode-se provar que existe pelo menos um polinômio irredutível $f(x)$ em $Z_p[x]$ para qualquer primo p e qualquer grau $m \geq 1$. Logo existe um corpo finito com p^m elementos para todo primo p e todo inteiro m. Pode existir mais de um polinômio irredutível de grau m em $Z_p[x]$. Pode-se provar que corpos finitos construídos considerando-se quaisquer dois polinômios irredutíveis de um certo grau fixo m em $Z_p[x]$ são isomorfos entre si. Assim, a menos de isomorfismo, existe um *único* corpo finito com p^m elementos (p primo, $m \geq 1$), que é denotado $GF(p^m)$ (também chamado *corpo estendido*). Mais ainda, pode-se provar que não existe corpo finito com k elementos a não ser que k seja da forma $k = p^m$ para algum inteiro $m \geq 1$ e p primo.