Assignment: Project 4 Decrypt Function
Name 1: Jonathan Smoley
Name 2: Samuel Sovi
GitHub Name: JT2M0L3Y

The affine cipher is a generalization of the Caesar cipher:

$$E_{\alpha,\beta}(x) = (\alpha x + \beta)\%26$$

Derive the analogous decrypt function. There is a distinction between the algebraic function, above, and the computational definition below. I'm referring to the algebraic function here.

Let x be plaintext, $\alpha \in Z$, $\beta \in [1 \,..\, 25]$, $y = E_{\alpha,\beta}(x)$ (or Ciphertext)

$y \equiv (\alpha x + \beta) \ (mod\ 26)$
$y - \beta \equiv \alpha x \ (mod\ 26)$
$\alpha^{-1}(y - \beta) \equiv \alpha^{-1}(\alpha x) \ (mod\ 26)$
$\alpha^{-1}(y - \beta) \equiv x \ (mod\ 26)$
$x \equiv \alpha^{-1}(y - \beta) \ \ (mod\ 26)$

Decryption function: $x \equiv \alpha^{-1}(y - \beta) \ \ (mod\ 26)$