Quiz 5

Problem 1
In the RSA cryptosystem, messages are represented as integers in the set $\mathbb{Z}_n$, where $n = pq$ is the product of two distinct odd primes p and q. To use the RSA cryptosystem, parameters $e, d \in \mathbb{Z}_n$ must be chosen such that

$$ed \equiv 1 \bmod \phi(n), \tag{1}$$

where $\phi(n) = (p-1)(q-1)$. To encrypt any plaintext $x \in \mathbb{Z}_n$, the sender computes $f(x) = x^e \bmod n$; to decrypt any ciphertext $y \in \mathbb{Z}_n$, the receiver computes $f^{-1}(y) = y^d \bmod n$.

Let $p = 7$, $q = 11$, and $e = 13$.

a) For the given values of p, q, e, how many integers $d \in \mathbb{Z}_n$ satisfy Equation 1?

b) List all integers $d \in \mathbb{Z}_n$ that satisfy Equation 1.

Carefully explain and justify your answers.