Proof of lemma of AKS algorithm

lemma: suppose $a, n \in \mathbb{Z}$ and $\gcd(a, n) = 1$
then n is prime iff $(X + a)^n \equiv (X^n + a) \bmod n$

Proof:

The coefficient of x^i in $((x+a)^n - (x^n+a))$
is ${}^nC_i \, a^{n-i}$
where,
$0 < i < n$

let suppose n is prime, then ${}^nC_i \equiv 0 \bmod n$

Hence all coefficients are zero and we are done.

Now, let's prove in ~~another~~ backward direction,
let us suppose n is composite, let us consider a prime q that is a factor of n and $q^k | n$, where $k \geq 1$

let $n = q^k . t$

Here q^k does not divide $\binom{n}{q}$ and coprime to q^q

since $\binom{n}{q} = \frac{n(n-1)--(n-q+1)}{q!}$, when numerator is divisible by q^k and not by q^{k+1} and denominator is divisible by q

therefore coefficient of x^{n-q} is not 0 mod n. thus $(x+a)^n - (x^n + a)$ is not identically zero over Z/nZ.

Hence our lemma proved.