4.4 Show that if a mod m $\equiv b$ mod m, then a^n mod m $\equiv b^n$ mod m for every positive integer n.

Prove by induction (on n)

Base case: $n = 1$

a mod m $\equiv b$ mod m

We know this is true, by assumption.

Inductive step:

Inductive Hypothesis: Assume that a^n mod m $\equiv b^n$ mod m

Show that a^{n+1} mod m $\equiv b^{n+1}$ mod m

a^{n+1} mod m $\equiv b^{n+1}$ mod m

$\iff$

$a^n * a$ mod m $\equiv b^n * b$ mod m

We know that a mod m $\equiv b$ mod m, by assumption

We know that a^n mod m $\equiv b^n$ mod m by inductive hypothesis

Then by proposition 4.3, $a^n * a$ mod m $\equiv b^n * b$ mod m is true

So a^{n+1} mod m $\equiv b^{n+1}$ mod m is true

4.8 Let a and m be positive integers with $m > 1$.

Show that the congruence $ax \equiv 1($ mod m $)$ is solvable $\iff gcd(a, m) = 1$.

1. Assume ax mod m $\equiv 1$ mod m has a solution, show that $gcd(a, m) = 1$

We know by assumption that ax mod m $\equiv 1$ mod m has a solution

We know that since $m > 1$, then 1 mod $m = 1$

So ax mod m $= 1$

So $ax = mk + 1$ for some integer k

This is equivalent to $ax - mk = 1$

So by theorem 3.11, since $ax - mk = 1$ has a solution, $gcd(a, m)$ must divide 1

a, m are positive integers

So $gcd(a, m) = 1$

2. Assume $gcd(a, m) = 1$, show that ax mod m $\equiv 1$ mod m has a solution

According to Bezouts theorem, there exists integers r, s such that $1 = ar + ms$

This is equivalent to $ar = m(-s) + 1$

So ar mod m $= 1$

And we know 1 mod m $= 1$

So ax mod m $\equiv 1$ mod m has a solution.

4.12 Prove theorem 4.10 Let a and m be relatively prime integers greater than 1, and let $N = am - a - m$

Then N is (a, m) accessible, but every integer n satisfying $n > N$ is (a, m) accessible.

5.4

5.8

extra 2