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

Prove by induction (on n)

Base case: $n = 1$

$a \equiv b$ (mod m)

We know this is true, by assumption.

Inductive step:

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

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

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

$\iff$

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

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

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

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

So $a^{n+1} \equiv b^{n+1}$ (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 $ax \equiv 1$ (mod m) has a solution, show that $gcd(a, m) = 1$

We know that since $m > 1$, then $1 = m(0) + 1$, so numbers in this congruence class have a remainder 1

We know that $ax \equiv 1$ (mod m), by assumption

So ax is also in the congruence class with remainder 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 $ax \equiv 1$ (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 belongs to the congruence class with remainder 1

And we know $1 = m(0) + 1$, which is in the congruence class with remainder 1

So $ax \equiv 1$ (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) inaccessible, but every integer n satisfying $n > N$ is (a, m) accessible.

Assuming a, m relatively prime, show that $N = am - a - m$ is the largest inaccessible by (a, m)

We know that positive integers $ra + sm$ are (a, m) accessible for every non-negative integer r, s

We know that $0, a, 2a...(m-1)a$ form a complete set of congruence class representatives modulo m

For every integer r between 0 and $m - 1$, the congruence class $C(ra)$ consists of all integers congruent to ra modulo m

Then the integers in any congruence class $C(ra)$ take the form $...ra - 2m, ra - m, ra, ra + m, ra + 2m...$

We know that integers are only accessible if they are a non negative combination, so the only integers that are accessible within a given $C(ra)$ must be greater than or equal to ra

So within any given $C(ra)$, the smallest integer that is (a, m) accessible is ra

So within any given $C(ra)$, the largest integer that is not (a, m) accessible is $ra - m$

The largest integer r would be $r = m - 1$

Then the largest integer that is not (a, m) accessible is $(m - 1)a - m$

This is equal to $N = am - a - m$

Then all integers greater than N must be (a, m) accessible

Show that N is (a, m) inaccessible)

The number N belongs to $C((m - 1)a)$

The smallest number accessible in $C((m - 1)a)$ is $(m - 1)a$, so N is not accessible.

5.4 Assume p prime, $p|bc$ for $b, c \in \mathbb{Z}$

Show that if $p \not| b$, then $p|c$.

The divisors of p are $1, p$

$p \not| b$, so $gcd(p, b) = 1$

So (p, b) relatively prime

Know by theorem 3.4 that since p, b relatively prime, and $p|bc$, then $p|c$

5.8 a, b are integers greater than 1 with prime factorizations

$a = p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$

$a = p_1^{f_1} p_2^{f_2} ... p_r^{f_r}$

Where the exponents are nonnegative integers and $p_1, ...p_r$ are distinct prime numbers.

Let g_i equal the smaller of the exponents e_i, f_i for each index.

Prove that $gcd(a, b) = p_1^{g_1} p_2^{g_2} ... p_r^{g_r}$

Let d be any divisor of a, b.

$d|a$, so by theorem 5.8, any divisor of a must be in the form $d = p_1^{g_1} p_2^{g_2} ... p_r^{g_r}$, and must have exponents $g_i \leq e_i$ for each p_i.

We also know that $d|b$, so $g_i \leq f_i$ for each p_i

So for each index p_i, $g_i \leq e_i$ AND $g_i \leq f_i$

So all common divisors of a, b have prime facorizations in the form $d = p_1^{g_1} p_2^{g_2} ... p_r^{g_r}$ for $g_i \leq e_i, g_i \leq f_i$

The greatest common denominator occurs when each exponent g_i is the maximal amount while maintaining $g_i \leq e_i, g_i \leq f_i$

This occurs at $g_i = min(e_i, f_i)$

Extra 1 Compute the last digit of 7^{58}, by successive squaring

Finding the last two digits is the same as finding 7^{58} mod 10

$7^1 \equiv 7 \pmod{10}$

$7^2 \equiv 7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 9^2 \equiv 1 \pmod{10}$

$7^{4n} \equiv 1 \pmod{10}$

$7^{58} = 7^{4*14+2} \equiv 1 * 9 \bmod (10)$

So the last digit of 7^{58} is 9

Extra 2 Compute the last two digits of 12^{25}, by successive squaring

Finding the last two digits is the same as finding 12^{25} mod 100

$12^1 \equiv 12 \pmod{100}$

$12^2 \equiv 12^2 \equiv 44 \pmod{100}$

$12^4 \equiv 44^2 \equiv 36 \pmod{100}$

$12^8 \equiv 36^2 \equiv 96 \pmod{100}$

$12^{16} \equiv 96^2 \equiv 16 \pmod{100}$

Know that $12^{25} = 12^{16+8+1}$

So $12^{25} \equiv 16 * 96 * 12 \equiv 32 \pmod{100}$