Solving LINEAR CONGRUENCES (Ch 19 & Ch 20):

Using normal arithmetic, we can solve linear equations such as: $2x = 4$. (We'd get that $x = 2$.)
But suppose that instead we have a congruence such as $2x \equiv 4 \ mod \ m$. Does this imply $x \equiv 2 \ mod \ m$?

Case 1: Given a linear congruence of the form: $\boldsymbol{ax \equiv ab \ mod \ m}$, how can we solve it for x?
(meaning: how do we find all possible congruence classes of *x* modulo *m* that satisfy the given congruence)

We know: $ax \equiv ab \ mod \ m \Leftrightarrow m|a(x-b) \Leftrightarrow a(x-b) = mk$ for some integer k. Some easy cases:

Case 1: If a|m, then $a(x-b) = mk \Leftrightarrow x - b = \frac{m}{a}k \Leftrightarrow x \equiv b \ mod \ \left(\frac{m}{a}\right)$.

Case 2: If $gcd(a,m) = 1$, then $m|a(x-b) \Leftrightarrow m|(x-b) \Leftrightarrow x \equiv b \ mod \ m$
(since *m* and *a* have no common factors, so all the factors of m must divide x-b)

Proposition 19.3.1: **If $\boldsymbol{a \ divides \ m}$, then: $\boldsymbol{ab_1 \equiv ab_2 \ mod \ m \Leftrightarrow b_1 \equiv b_2 \ mod \ \left(\frac{m}{a}\right)}$**

Ex: $2x \equiv 4 \ mod \ 10 \Leftrightarrow x \equiv 2 \ mod \ 5$

Hence: $x \equiv$ ____ or ____ $mod \ 10$.

Proposition 19.3.2: **If $\boldsymbol{gcd(a,m) = 1}$, then $\boldsymbol{ab_1 \equiv ab_2 \ mod \ m \Leftrightarrow b_1 \equiv b_2 \ mod \ m}$**

Ex: $2x \equiv 4 \ mod \ 7 <=> x \equiv 2 \ mod \ 7$.

Case 2: More generally now, can we solve any linear congruence $\boldsymbol{ax \equiv b \ mod \ m}$**?**

Theorem 20.1.7: **A linear congruence $\boldsymbol{ax \equiv b \ mod \ m}$ has solutions if and only if $\boldsymbol{gcd(a,m) \mid b}$.**
(in which case it has precisely $\boldsymbol{gcd(a,m)}$ different solutions modulo *m*)

Examples:

a) Solve $14x \equiv 21 \ mod \ 35$.
Note: gcd(14,35)=7, which divides 21, so there should be 7 solutions modulo 35.

Solutions mod 5: $x \equiv 4 \ mod \ 5$
Solutions mod 35: $x \equiv 4, 9, 14, 19, 24, 29, or \ 34 \ mod \ 35$

b) Solve $14x \equiv 16 \ mod \ 35$.

c) How do we solve a congruence without obvious factors to "cancel", such as:

$$3x \equiv 7 \; mod \; 11?$$

Thm 20.1.7 guarantees that this has one solution mod 11 (since gcd(3,11)=1), but what is it?
If we could write 7 as a multiple of 3 (modulo 11), then we could use one of the previous methods.
Here's how to do it:

(1) first use the Euclidean Algorithm, as if we're trying to compute gcd(**3**,**11**):

(2) then work backwards, one equation at a time, starting with the one before last:

(solve for 1 in the 2^{nd} eq)

(solve for 2 in 1^{st} eq and replace in previous)

(collect all the coefficients of 3 and of 11)

we can thus determine how to write gcd(a,m) as a linear combination of *a* and *m*:

$$1 = 4 * 3 + (-1) * (11)$$

(3) This allows us to write $b = 7$ as a multiple of *a* :

$$7 = 7 * 1 = 7 * (4 * 3 - 11) = 28 * 3 - 7 * 11 \equiv 28 * 3 \; mod \; 11 \equiv 6 * 3 \; mod \; 11.$$

Replacing this in our congruence $3x \equiv 7 \; mod \; 11$, we get that: $3x \equiv 6 * 3 \; mod \; 11$
Hence, by Prop 19.3.2, we can now cancel the coefficient of x to get: $x \equiv 6 \; mod \; 11$.

This method described in c) is the gist of section 20.2.
EXERCISE: solve $23x \equiv 16 \; mod \; 107$.

(ans: $x \equiv 10 \; mod \; 107$)