Math 351 hints for this weekend's theorem proofs:
Hint 1's on this page
Hint 2's on the next page

Hints #1

**Theorem 30:** Given $a \in R$, suppose $a$ is both a unit and a zero-divisor:
--write down (using equations) what that means using the definitions of unit and zero-divisor.
--do some algebra
--get that 0 = something that's definitely not 0
--contradiction, therefore $a$ is not both.

<u>Please assume that you know $0 \cdot x = 0$ in a ring—we should have proved that first. Phooey.</u>

**Theorem 31 part 1:** Given $a \in \mathbb{Z}_n$ and $\gcd(a,n)=1$ prove that $[a]$ is a unit in $\mathbb{Z}_n$

Notice that in the gcd statement, we are working with the integers *a, d, n*, not the $\mathbb{Z}_n$ numbers, but when we say $a$ is a unit, we are talking about it as a number in $\mathbb{Z}_n$

--write down the only useful equation you can get from $\gcd(a,n)=1$
--do algebra
--try to get $a \cdot (...) \equiv 1 \pmod{n}$

**Theorem 33 part 1:** Given $[a] \in \mathbb{Z}_n$, $[a] \not\equiv [0] \pmod{n}$, and $\gcd(a,n)=d>1$ prove that $a$ is a zero-divisor.

Notice that in the gcd statement, we are working with the integers *a, d, n*, not the $\mathbb{Z}_n$ numbers.

Write down the 3 equations you know how to write for $\gcd(a,n)=d$

Look for some variables you can multiply together that you know will be $\equiv 0 \pmod{n}$.
You need to be able to regroup into two factors, where one factor is $a$ and the other factor can't be $n$ (or a multiple of $n$)

Hints #2:

**Theorem 30:** In one equation, *a* should be multiplied by another variable to give 1
In the other equation, *a* should be multiplied by another variable to give 0.
Pay attention to the definition of zero-divisor: what do you know about both variables?

What happens when you multiply all 3 variables together?
Remember the associative law? Try to use it.

(Note that while *a* doesn't necessarily commute with the other variable in the zero-divisor equation, it does commute with its multiplicative inverse).

**Theorem 31 part 1**
Use theorem 18.
You're trying to get:
$a\cdot(...)\equiv 1+n(...)\equiv 1 \pmod n$
That means $[a]\cdot[(...)]=1$ in $\mathbb{Z}_n$

**Theorem 33 part 1**
You don't need the equation from theorem 18, you only need the other two equations you got from $\gcd(a,n)=d>1$

Here's the number version of the proof. See if you can turn numbers into variables in a way that gives you a correct proof:

$\gcd(6,15)=3>1$
So $3|6$ and $3|15$
Specifically $6=3\cdot 2$ and $15=3\cdot 5$
Consider the product
$2\cdot 3\cdot 5=(2\cdot 3)\cdot 5=6\cdot 5$
also $2\cdot 3\cdot 5=2\cdot(3\cdot 5)=2\cdot 15$
Now, $6\neq 0$ in $\mathbb{Z}_{15}$ because that's given.
And $3\cdot 5=15$ and $3>1$ so $5<15$ and $5\neq 0$ in $\mathbb{Z}_{15}$
Also $6\cdot 5=2\cdot 15=0$ in $\mathbb{Z}_{15}$, so 6 is a zero-divisor in $\mathbb{Z}_{15}$