Some theorems you need to know how to prove:

Theorem M1. If *p* is prime, then every non-zero element in $\mathbb{Z}_p$ is a unit

Theorem M2. If *p* is prime, then $\mathbb{Z}_p$ has no zero-divisors.

Theorem M3. If *p* is prime, and *a* and *b* are constants and $a \neq 0$ in $\mathbb{Z}_p$, then $ax + b = 0$ has a solution in $\mathbb{Z}_p$.

Theorem M4. If *p* is prime, and *a*, *b* and *c* are constants and $a \neq 0$ in $\mathbb{Z}_p$, then $ab = ac$ implies $b = c$.

Theorem M5. If *n* is not prime, then there exists a zero-divisor in $\mathbb{Z}_n$.

Theorem M6. If $a<n$ and $(a,n) > 1$ then *a* is a zero-divisor in $\mathbb{Z}_n$.

Theorem M7. If $a<n$ and $(a,n) = 1$ then *a* is a unit in $\mathbb{Z}_n$.

Examples you need to know:

1. Find numbers a,b,c,n such that $ab = ac$, and $a \neq 0$ but $b \neq c$ in $\mathbb{Z}_n$

2. Find numbers a,b,n, where $a \neq 0$, such that $ax + b = 0$ has more than one solution in $\mathbb{Z}_n$.

2. Find numbers a,b,n, where $a \neq 0$, such that $ax + b = 0$ has no solutions in $\mathbb{Z}_n$.