MATH 321: 10-6 IN-CLASS WORK

Recall that if n and d are integers then there are unique integers q and r so that $0 \leq r < d$ and $n = qd + r$. In other words, we can do integer division with remainder. We call q the *quotient* of n divided by d and r the *remainder* of n divided by d. This motivates the following definition.

Definition. Let a and b be integers and n be a positive integer. Then a and b are *equivalent modulo n*, written $a \equiv b \mod n$, if a and b have the same remainder divided by n.

Equivalently, we could define that $a \equiv b \mod n$ if a and b differ by a multiple of n. That is, there is $k \in \mathbb{Z}$ so that $a = b + kn$. (This equivalent formulation is usually nicer for use in proofs.)

A simple but useful observation: if $a \equiv b \mod n$ and $0 \leq a, b < n$ then $a = b$.

For example, consider the case $n = 12$. Then adding integers modulo 12 is exactly like dealing with clocks. E.g. if it is currently 8 then in 6 hours it will be $2 \equiv 8 + 6 \mod 12$.

Exercise 1. *Let a, a', b, b' be integers and n be a positive integer. Prove that if $a \equiv a' \mod n$ and $b \equiv b \mod n$ then $a + b \equiv a' + b' \mod n$ and $ab \equiv a'b' \mod n$.*

Exercise 2. *Let p be a prime number and suppose $0 < a < p$. Prove there is an integer b so that $ab \equiv 1 \mod p$.*

Often in mathematics we don't just want to prove that an object exists, we want to prove it's unique. Remember that $\exists! x\ P(x)$ is an abbreviation for $\exists x\ (P(x) \wedge \forall y\ (P(y) \rightarrow x = y))$. And this is equivalent to $\exists x\ P(x) \wedge \forall y, z\ (P(y) \wedge P(z) \rightarrow y = z)$. So to prove $\exists x\ P(x)$ you have two things to prove: that there is an object x so that $P(x)$ and that if two objects both satisfy P then they must be the same.

Exercise 3. *Let p be a prime number and suppose $0 < a < p$. Prove there is a unique integer b so that $ab \equiv 1 \mod p$ and $0 < b < p$.*

Exercise 4. *Let n be a positive integer and a be an integer. Prove there is a unique integer b so that $a + b \equiv 0 \mod n$ and $0 \leq b < n$.*