Math 8
Worksheet
Week 7, Tuesday

Modular Arithmetic

Collaborators:

We continue our study of the integers using a tool called modular arithemetic. If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we say

$$a \equiv b \pmod{m},$$

read "a is congruent to b modulo m", if $n \mid a - b$.

Example.

(a) Find the set of all integers congruent to 0 modulo 5.

(b) Find the set of all integers congruent to 5 modulo 5.

(c) Modulo 5, how many sets does $\mathbb{Z}$ decompose into? What are they?

Let $a, b, c, d \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$. Some useful facts:

(a) Modulo m, every integer is congruent to exactly one of 0, 1, ..., $m-1$.

(b) $a \equiv a \pmod{m}$

(c) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(f) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

(g) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

(h) If a and m are coprime and $ba \equiv ca \pmod{m}$, then $b \equiv c \pmod{m}$.

Example. Liebeck Ch 13.

(a) Show that every square is congruent to 0, 1, or -1 modulo 5.

(b) Let p be prime. Show that if x is an integer such that $x^2 \equiv x \pmod{p}$, then $x \equiv 0$ or $x \equiv 1 \pmod{p}$.

Homework. Liebeck Ch 13.

(a) Find r with $0 \leq r \leq 10$ such that $7^{137} \equiv r \pmod{11}$.

(b) Prove the "rule of 9": an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.