Math 4400
Week 3 - Tuesday
Modular Arithmetic

Definition: For n a positive integer and $a, b \in \mathbb{Z}$, we say ("Is congruent to") $a \equiv b \mod n$ if $n \mid (a-b)$

Example:

- $5 \equiv 3 \mod 2$ $\quad 0 \equiv -4 \mod 2$.
- $18 \equiv 4 \mod 7$ $\quad 7 \equiv -1 \mod 8$

Proposition: if $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a+c \equiv b+d \mod n$ and $ac \equiv bd \mod n$.

$$\begin{array}{ccc} 49 & & 1 \\ \| & & \| \end{array}$$

Example: $(7)^2 \equiv (-1)^2 \mod 8$

Proof of proposition: $b = a + qn \qquad d = c + sn$

$b + d \equiv a + qn + c + sn \equiv a + c \mod n.$

$bd = (a + qn)(c + sn) \equiv ac \mod n$

$= ac + qnc + snq + qsn^2 \equiv ac \mod n$

Application 1: $n \in \mathbb{N}$ is divisible by 3 if and only if the sum of the digits of n is divisible by 3.

Example: 101 is not divisible by 3 because $1 + 0 + 1$ is not.

Proof: $n = a_m \dots a_2 a_1 a_0$ (digits of n)

means $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_m \cdot 10^m$

$\equiv a_0 + a_1 \cdot 1 + a_2 \cdot (1)^2 + \dots + a_m \cdot (1)^m \mod 3$

$\equiv a_0 + a_1 + a_2 + \dots + a_m \mod 3.$

$3 \mid n \iff n \equiv 0 \bmod 3$

$\iff a_0 + \cdots + a_m \equiv 0 \bmod 3$

$\iff 3 \mid a_0 + \cdots + a_m.$

Application 2: ISBN-10.

10 digits $x_1 x_2 \cdots x_{10}$ (x_{10} is allowed to be 10; this is written as X).

such that $\sum_{i=1}^{10} i x_i \equiv 0 \bmod 11$

Eg. 1111111111 valid but not 1111111112.

Note $\sum_{i=1}^{11} i x_i \equiv 0 \bmod 11 \iff \sum_{i=1}^{9} i x_i + 10 x_{10} \equiv 0 \bmod 11$

$\iff \sum_{i=1}^{9} i x_i - x_{10} \equiv 0 \bmod 11$

$\iff \sum_{i=1}^{9} i x_i \equiv x_{10} \bmod 11.$

Lets you detect if a digit has been changed or 2 digits transposed.

Example: Suppose $x_1 \cdots x_{10}$ is a valid ISBN code,

then $y_1 y_2 \cdots y_{10} = x_1 x_2 \cdots x_{j+1} x_j \cdots x_{10}$

satisfies $\sum_{i=1}^{10} i y_i \equiv \sum_{i=1}^{10} i x_i + (x_j - x_{j+1}) \bmod 11$

$= x_j - x_{j+1} \bmod 11$

$\neq 0$ if $x_j \neq x_{j+1}$.

Can sometimes use to identify where the error is if you know enough — $x_j - x_{j+1} = \theta_{j+1} - \theta_j$ (Exercise).

Notation: $\mathbb{Z}/n\mathbb{Z}$ is the set

$0, 1, \ldots, n-1$

with addition, multiplication determined modulo n —

e.g. in $\mathbb{Z}/5\mathbb{Z}$ $\quad 2+3=0$ ($5 \equiv 0 \bmod 5$)

and $\quad 2 \cdot 3 = 1$ ($6 \equiv 1 \bmod 5$).

Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ obey the "normal" rules — commutative + associative laws for adding/multiplying, distributive law.

Example: $\mathbb{Z}/12\mathbb{Z}$ gives "clock arithmetic",

10 o'clock + 4 hours = 2 o'clock

$10 + 4 \equiv 2 \bmod 12$.