Modular Arithmetic

Congruence: $a \equiv b \pmod{m}$

$\Updownarrow$

$b - a = m \cdot k$ for some $k \in \mathbb{Z}$

Mod Identities

Suppose $a \equiv b \pmod{m}$ and
$c \equiv d \pmod{m}$

Then:

$a + c \equiv b + d \pmod{m}$
$a - c \equiv b - d \pmod{m}$
$ac \equiv bd \pmod{m}$
$\forall p \quad a^p \equiv b^p \pmod{m}$

Residue Classes modulo 5

0: $\{\dots, -10, -5, 0, 5, 10, \dots\} \Leftrightarrow 5k + 0$

1: $\{\dots, -9, -4, 1, 6, 11, \dots\} \Leftrightarrow 5k + 1$

2: $\{\dots, -8, -3, 2, 7, 12, \dots\} \Leftrightarrow 5k + 2$

3: $\{\dots, -7, -2, 3, 8, 13, \dots\} \Leftrightarrow 5k + 3$

4: $\{\dots, -6, -1, 4, 9, 14, \dots\} \Leftrightarrow 5k + 4$

Congruence revisited: $-3 \equiv 12 \equiv 2 \pmod{5}$

$a \equiv b \pmod{m}$

$\Updownarrow$

a and b are in the same residue class modulo m

"Last Digit": work in modulo 10.

1 Party Tricks

You are at a party celebrating your completion of the CS 70 midterm. Show off your modular arithmetic skills and impress your friends by quickly figuring out the last digit(s) of each of the following numbers:

Residue classes modulo 10

0: $\{\ldots, -10, 0, 10, \ldots\}$

1: $\{\ldots, -9, 1, 11, \ldots\}$

$\vdots$

9: $\{\ldots, -1, 9, 19, \ldots\}$

(a) Find the last digit of 11^{3142}.

$$11 \equiv 1 \pmod{10}$$

$$11^{3142} \equiv 1^{3142} \pmod{10}$$

$$\equiv \boxed{1} \pmod{10}$$

(b) Find the last digit of 9^{9999}.

$$9 \equiv -1 \pmod{10}$$

$$9^{9999} \equiv (-1)^{9999} \pmod{10}$$

$$\equiv -1 \pmod{10}$$

$$\equiv \boxed{9} \pmod{10}$$

Inverses

Standard Arithmetic: $x^{-1} = \frac{1}{x}$

$$x^{-1} \cdot x = 1$$

Modular arithmetic:

x^{-1} = number you multiply x by to get 1

Utility: Suppose wanted to solve $ax \equiv b \pmod m$

$$a^{-1}(ax) \equiv a^{-1}b \pmod m \quad \text{if } a^{-1} \text{ exists}$$

Can't divide!!

$$\boxed{x \equiv a^{-1}b \pmod m}$$

$x^{-1} \pmod m$ exists iff $\gcd(m, x) = 1$

find a, b such that $\boxed{am + bx = \gcd(m, x) = 1}$

$$\Updownarrow$$

$$bx = (-a) \cdot m + 1$$

$$\Updownarrow$$

$$bx \equiv 1 \pmod m$$

$\boxed{b \text{ is } x^{-1} \pmod m}$

GCDs:

Euclid's algo $\boxed{\gcd(x, y) = \gcd(y, x \pmod y)}$

EGCD: helps us retrieve a and $\boxed{b}$ by bookkeeping during the GCD algorithm

2 Modular Potpourri

(a) Evaluate $4^{96} \pmod 5$.

$\{\dots, -10, -5, 0, 5, 10, \dots\}$

$\{\dots, -9, -4, 1, 6, 11, \dots\}$

$\{\dots, -8, -3, 2, 7, 12, \dots\}$

$\{\dots, -7, -2, 3, 8, 13, \dots\}$

$\{\dots, -6, -1, 4, 9, 14, \dots\}$

$4 \equiv -1 \pmod 5$

$4^{96} \equiv (-1)^{96} \pmod 5$

$\equiv 1 \pmod 5$

(b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod 6$.

$\underbrace{x = 16k + 3}_{x \text{ is odd}}$ for some $k \in \mathbb{Z}$

$\underbrace{x = 6j + 4}_{x \text{ is even}}$ for some $j \in \mathbb{Z}$

(c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

$\cancel{2}$

$2 \cdot$ each side

$2^{-1}(2x) \equiv 2^{-1}(4) \pmod{12}$

Does 2^{-1} exist $\pmod{12}$?

$\gcd(12, 2) = 2 \neq 1$

2^{-1} Does Not exist $\pmod{12}$

3 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

Base Case: $\gcd(F_1, F_0) = 1$ ✓

IH: Assume that $\gcd(F_k, F_{k-1}) = 1$

IS: Want to show $\gcd(F_{k+1}, F_k) = 1$

$$\gcd(F_{k+1}, F_k)$$

$$= \gcd(1 \cdot F_k + F_{k-1}, F_k)$$

$$= \gcd(F_k, F_{k-1})$$

$$= 1 \quad \square$$

In practice, usually easier to "brute force" the inverse.

E.g., What's $3^{-1} \pmod{13}$?

$3^{-1} \cdot 3 \equiv 1 \pmod{13}$

$3 \nmid 1$ $\quad (13 \cdot 0 + 1 = 1)$

$3 \nmid 14$ $\quad (13 \cdot 1 + 1 = 14)$

$3 \mid 27$ $\quad (13 \cdot 2 + 1 = 27)$

$\boxed{9} \cdot 3 = 27 \equiv 1 \pmod{13}$

$\boxed{9}$ is $3^{-1} \pmod{13}$