Multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

$a \in \mathbb{Z}/n\mathbb{Z}$ has an inverse $\Leftrightarrow$ a is coprime to n ($\gcd(a,n)=1$).

($\Leftarrow$) can solve $Xa \equiv 1 \bmod n \Leftrightarrow \gcd(a,n)=1$).

Using this $\Rightarrow$ can solve equations like

$$10x \equiv 5 \bmod 17.$$

Using this $\Rightarrow$ Chinese Remainder theorem about solving

$$X \equiv a \bmod m$$
$$X \equiv b \bmod n$$

$\gcd(m,n)=1$.

Established by giving a way to solve it $\rightarrow$

$x \equiv a \pmod{m}$ $\quad x = qm + a$

$x \equiv b \pmod{n}$

$qm + a \equiv b \pmod{n}$

$qm \equiv b - a \pmod{n}$.

Solve for q.

Using Euclidean algorithm to compute multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$ (or mod n).

Example: (Ex 5-(1)) Inverse of 131 mod 1979

(equivalently, inverse of 131 in $\mathbb{Z}/1979\mathbb{Z}$)

Step 1: Run Euclidean algorithm:

$1979 = 15 \cdot 131 + 14$

$131 = 9 \cdot 14 + 5$

$14 = 2 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1 \leftarrow \gcd = 1.$

$4 = 4 \cdot 1 + 0$

Step 2: unfold to solve gcd equation $1979x + 131y = 1$.

$1 = 1 \cdot 5 - 1 \cdot 4$

$= 1 \cdot 5 + -1(14 - 2 \cdot 5)$

$= 3 \cdot 5 + -1(14)$

$= 3 \cdot (131 - 9 \cdot 14) + -1(14)$

$= 3 \cdot 131 - 28 \cdot 14$

$= 3 \cdot 131 - 28(1979 - 15 \cdot 131)$

$= (3 + 28 \cdot 15)131 - 28 \cdot 197$

$= (423)131 - 28 \cdot 197$

So $423(131) - 28 \cdot 1979 = 1$

$\Rightarrow 423 \cdot 131 \equiv 1 \bmod 1979$

So 423 is the mult. inverse of 131 in $\mathbb{Z}/1979\mathbb{Z}$.

Divisibility conditions:

Recall from Tuesday video:

Theorem: A positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Example: Is 101 divisible by 3? No, because $1+0+1=2$ is not.

Proof: n a positive integer, write it as

$n = a_k a_{k-1} \cdots a_0$ ← digits, i.e.

$n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10 a_1 + a_0$.

Take mod 3 we get

$$n \equiv 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10 a_1 + a_0 \bmod 3$$

$10 \equiv 1 \bmod 3$ so $10^k \equiv 1^k \equiv 1 \bmod 3$

so $n \equiv a_k + a_{k-1} + \dots + a_0 \bmod 3.$

↑ sum of digits

$3 \mid n \iff n \equiv 0 \bmod 3$ so by above

$\iff a_k + \dots + a_0 \equiv 0 \bmod 3$

$\iff 3 \mid a_k + \dots + a_0.$

Exercise 4 — do similar for divisibility by 9 and 11.

Key observation for divisibility by 11

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

$10^k \equiv (-1)^k \pmod{11}$

$a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots + 10^k a_k$

$\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11}$