Math 4400
Week 3 – Thursday
Inverses and the Chinese Remainder Theorem

Rough definition:

A number system* is a place where we can add, subtract, and multiply, subject to the usual rules of arithmetic (commutative, associative, distributive laws, $1 \cdot x = x$, $x + 0 = x$).

* Starting next week we'll say (commutative) ring.

Examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$.

⚠ Cannot always divide by all non-zero elements in a number system!

$\frac{x}{y} = x \cdot \frac{1}{y}$ — what is $\frac{1}{y}$?

Definition: $\frac{1}{y}$ is a number such that $y \cdot \frac{1}{y} = 1$;

such a number may not exist! If it does, we say it is a multiplicative inverse of y, and we can use it to divide by y.

Examples:

- In $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, if $y \neq 0$ then it has a multiplicative inverse.
- In $\mathbb{Z}$, only $y = 1$ and $y = -1$ have mult. inverses ($1 \cdot 1 = 1$, $(-1)(-1) = 1$). in $\mathbb{Z}$. But, e.g., 2 has a mult. inverse $\frac{1}{2}$ in $\mathbb{Q}$.
- In $\mathbb{Z}/15\mathbb{Z}$, $2 \cdot 8 = 1$, so 2 and 8 ($8 \cdot 2$) are mult. inverses of eachother.

But 3 does not:

In $\mathbb{Z}/15\mathbb{Z}$: $3 \cdot x =$

$x =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$3 \cdot x =$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12

Never 1!

So 3 does not have a mult. inverse in $\mathbb{Z}/15\mathbb{Z}$.

Restatement: An element $a \in \mathbb{Z}/n\mathbb{Z}$ has a mult. inverse if and only if, viewing a as an integer

there is an integer b such that $ab \equiv 1 \bmod n$. (in that case the mlt. inverse is the unique $0 \le k < n-1$ s.t. $k \equiv b \bmod n$)

Theorem: For $a, n \in \mathbb{Z}$, there is a $x \in \mathbb{Z}$ such that $ax \equiv 1 \bmod n$ if and only if $\gcd(a, n) = 1$.

Proof: Suppose $ax \equiv 1 \bmod n$.

Means $ax = 1 + ny$ for some $y \in \mathbb{Z}$

$ax + n(-y) = 1$

↖ gcd equation

RHS has to be a multiple of $\gcd(a, n)$

so gcd has to be 1.

Suppose $\gcd(a, n) = 1$.

FTA: Can find $x, y \in \mathbb{Z}$ such that

$ax + ny = 1$

$\Rightarrow ax = 1 - ny \equiv 1 \bmod n$

$ax \equiv 1 \bmod n$.

Note: can find inverse by finding a solution to $ax + ny = 1$ (e.g. by unfolding Euclidean alg.).

Example: Can use to solve equations in $\mathbb{Z}/n\mathbb{Z}$

• $17x = 5$ in $\mathbb{Z}/50\mathbb{Z}$.

Idea: multiply by $\frac{1}{17}$ i.e. a mult. inverse of 17.

$3(17x) = 3 \cdot 5$ in $\mathbb{Z}/50\mathbb{Z}$ — 3.

$x = 15$ in $\mathbb{Z}/50\mathbb{Z}$.

Systems of congruences:

Let m and n be 2 integers, $a \in \mathbb{Z}/m\mathbb{Z}$, $b \in \mathbb{Z}/n\mathbb{Z}$.

Q: Can I find $x \in \mathbb{Z}$ such that

$x \equiv a \bmod m$

$x \equiv b \bmod n$?

Example: Is there an $x \in \mathbb{Z}$ such that

• $x \equiv 1 \bmod 2$ and $x \equiv 2 \bmod 3$?

Yes, $x = 5 = 1 + 2 \cdot 2$

$= 2 + 3$

$x = 11 \rightsquigarrow 11 = 5 + 6 \equiv \begin{matrix} 5 \bmod 2 \\ 5 \bmod 3. \end{matrix}$

• $x \equiv 0 \bmod 2$ and $x \equiv 5 \bmod 6$?

$x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$

$x \bmod 2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1 ...
$x \bmod 6$	0	1	2	3	4	5	0	1	2	3	4	5	0	1 ...

Why was there no solution? If $x \equiv 5 \bmod 6$ $x = 5 + 6q \equiv \begin{matrix} 5 \bmod 2 \\ \equiv 1 \bmod 2. \end{matrix}$

• $x \equiv 3 \bmod 8$ $\quad x \equiv 5 \bmod 9$.

$\Updownarrow$

$x = 3 + 8k_A$ $\quad \nearrow \quad 3 + 8y \equiv 5 \bmod 9$

$8k_A = 2 \bmod 9$

for $y \in \mathbb{Z}$.

So can take $y = 7$, get $x = 59$.

Mult. inverse of 8 in $\mathbb{Z}/9\mathbb{Z}$ is 8.

$8 \cdot 8y \equiv 16 \bmod 9$

$y \equiv 7 \bmod 9$.

Chinese Remainder Theorem, version 1:

If m and n are coprime ($\gcd(m,n) = 1$) then for any $a \in \mathbb{Z}/m\mathbb{Z}$ and $b \in \mathbb{Z}/n\mathbb{Z}$, there is an integer x such that

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n.$$

Moreover, x is uniquely determined up to a multiple of mn.