$\mathbb{Z}/4\mathbb{Z}$.

$[6] = [2]$

<u>Notation</u> $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes mod n.

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots [n-1]\}$ cyclicity in picking representatives.

<u>Operations on $\mathbb{Z}/n\mathbb{Z}$</u>.

$$\left.\begin{aligned} [a] + [b] &= [\overset{\text{arithmetic sum}}{a+b}] \\ [a][b] &= [ab] \end{aligned}\right\} \text{finite set defined in terms of representatives.}$$

These operations are <u>well-defined</u>: $[a] = [a'] \wedge [b] = [b'] \Rightarrow \begin{cases} [a+b] = [a'+b'] \\ [ab] = [a'b'] \end{cases}$

Congruence mod 0 IS $\mathbb{Z}$!

$+, \cdot \rightarrow$ both are commutative and associative.

multiplication distributes over addition.

$[a] + [0] = [0] + [a] = [a]$. $[0]$ neutral for addition.

$[a] \cdot [1] = [1] \cdot [a] = [a]$ $[1]$ neutral for multiplication.

Each class $[a]$ has inverse wrt $+$ $([-a])$.

- But not always for $\cdot$.

$\rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ has an algebraic structure similar to $\mathbb{Z}$! Compressed version of integers?

↳ This is called a <u>ring</u>. Structure that has $\oplus$ and $\odot$

$\rightarrow$ Preserves operation properties.

<u>Warning</u>: in $\mathbb{Z}/n\mathbb{Z}$, may occur that: $[a] \cdot [b] = 0$, yet $[a], [b] \neq 0$. ?

$\exists$ zero divisors. <u>Ex</u> $n = 6$ so $\mathbb{Z}/6\mathbb{Z}$ $[2] \cdot [3] = [6] = [0]$.

Notice n is not prime LOL.

<u>Ex</u> Multiplication tables. $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$. <u>careful</u> primeness of mod.

$\cdot$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

zero divisor

$\cdot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

$\rightarrow$ Symmetric reflects <u>commutativity</u>.

↳ No zeros here, unlike $\mathbb{Z}/4\mathbb{Z}$.

Each line/column contain numbers $1 \rightarrow 4$, a scrambling / permutation

KNOW!

<u>Def</u> $a \in \mathbb{Z}$ invertible mod n if

$\exists b \in \mathbb{Z} : ab \equiv 1 \mod n$.

In $\mathbb{Z}/n\mathbb{Z}$, $[a]$ invertible if

$\exists [b] \in \mathbb{Z}/n\mathbb{Z} : [a][b] = [1]$ (same notion!).

<u>example</u> $[1]$ invertible, $[0]$ never invertible.

super easy to check!

Thm: $a \in \mathbb{Z}$ invertible mod $n \iff \boxed{\gcd(a, n) = 1}$ ↳ this criterion is <u>intrinsic</u>

Discrete: Group Theory

Thm: $a \in \mathbb{Z}$ invertible mod $n \iff \gcd(a,n) = 1$

proof: $(\Rightarrow)$ assume a invertible mod n to show $\gcd(a,n) = 1$.

$\rightarrow \exists b : ab \equiv 1 \bmod n \rightarrow n \mid ab - 1$.

Let $d = \gcd(a,n)$. Then, $d \mid a \Rightarrow d \mid ab$

$d \mid n \wedge n \mid ab - 1 \Rightarrow d \mid ab - 1$ $\therefore d = 1$. (transitivity)

$(\Leftarrow)$ assume $\gcd(a,n) = 1$. show a invertible mod n.

$\gcd(a,n) = 1 \Rightarrow 1 = ax + ny$. $(x, y \in \mathbb{Z})$.

$\Rightarrow 1 \equiv ax \bmod n$

(or $ax - 1 = n(-y)$ $ax \equiv 1 \bmod n$) . so $b = x$ ∎

in $\mathbb{Z}/n\mathbb{Z}$: Diophantine general sol.

$[a]$ invertible mod $n \iff \gcd(a,n) = 1$.

However, in $\mathbb{Z}/n\mathbb{Z}$, inverse of $[a]$ is unique. (as opposed to $ax \equiv 1 \bmod n$)

! p prime $\Rightarrow$ in $\mathbb{Z}/p\mathbb{Z}$, all elements $\neq 0$

namely $[1], [2], [p-1] \ldots \leftarrow$ relatively prime to p.

$\hookrightarrow$ all of them are <u>invertible</u>. !

$a \in \{1, \ldots, p-1\}$ rel. prime to $p \Rightarrow [a]$ invertible

In general, $\mathbb{Z}/n\mathbb{Z}$ is "loosely" like $\mathbb{Z}$.

for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is like $\begin{cases} \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \end{cases}$ $\rightarrow$ <u>a field</u>.

$\mathbb{Z}/p\mathbb{Z}$ is a finite field.

<u>Fact</u> There are finite fields of size 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19.

wait, wtf ? powers of primes !

<u>Even Cooler Discrete Lecture</u>

<u>Invertibility</u>: in $\mathbb{Z}$: a invertible mod n if $ab \equiv 1 \bmod n$ for some b.

in $\mathbb{Z}/n\mathbb{Z}$: $[a]$ invertible if $[a][b] = [1]$ for some $[b] \in \mathbb{Z}/n\mathbb{Z}$

<u>Remark</u>: Such $[b]$ is UNIQUE.

<u>Proof</u>: Let $[b'] \in \mathbb{Z}/n\mathbb{Z}$ also satisfy $[a][b'] = [1]$.

$(\underbrace{[b][a]}_{[1]})[b'] = [b]\underbrace{([a][b'])}_{[1]}$ hence, $[b] = [b']$, so, $[b]$ is <u>the</u> inverse of $[a]$.

Denote $[b] = [a]^{-1}$ (because of uniqueness).

Viet

Discrete: Lecture

Euclid's Algorithm: Let $a, b \in \mathbb{N}$, say, $a > b$,

$a = bq_1 + r_1 \qquad 0 \le r_1 < b$.

$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$

$\vdots$

$r_{n-1} = r_n q_{n+1} + r_{n+1} \qquad 0 \le \boxed{r_{n+1} = 0} \to r_n$ is the gcd.

$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) \ldots$

$\gcd(r_n, r_{n+1}) = r_n$, $r_{n+1} = 0$

↳ Provide a sequence of simplifications of the gcd.

Theorem: Let $\gcd(a,b) = d$, then, $\exists x, y \in \mathbb{Z} : d = ax + by$. ← linear combination w/ coefs. $= x, y$.

proof: Let $r_1 \ldots r_n$ sequence of remainders in steps. Euclid's Alg. Prove by induction on k that

$$r_k = ax_k + by_k \quad \text{for some } x_k, y_k \in \mathbb{Z}$$

$(\text{then}, (r_n = d) = ax_n + by_n)$.

base: $k = 1$ $\qquad r_1 = a - bq_1 = ax_1 + by_1$ for $\begin{cases} x_1 = 1 \\ y_1 = -q_1 \end{cases}$

Assume known for k and $k-1$.

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_{k+1} \\ &= ax_{k-1} + by_{k-1} - (ax_k + by_k) q_{k+1} \\ &= a(x_{k-1} - q_{k+1} x_k) + b(y_{k-1} - y_k q_{k+1}), \quad x_{k+1}, y_{k+1} \in \mathbb{Z}. \ \blacksquare \end{aligned}$$

Cor. $\gcd(a,b) = 1 \Rightarrow 1 = ax + by$ for some $x, y \in \mathbb{Z}$.

ex: $\gcd(64, 27) = 1 \qquad ?\, x, y : 1 = 64x + 27y$.

$64 = 27 \cdot 2 + 10 \quad \rightsquigarrow (64, 27)$

$27 = 10 \cdot 2 + 7 \quad (27, 10)$

$10 = 7 \cdot 1 + 3 \quad (10, 7)$

$7 = 3 \cdot 2 \boxed{+1} \quad (7, 3)$.

$1 = 7 - 3 \cdot 2 = 7 - (10 - 7) \cdot 2 = 7 \cdot 3 - 10 \cdot 2 = (27 - 10 \cdot 2) \cdot 3 - 10 \cdot 2 =$

$27 \cdot 3 - 10 \cdot 8 = 27 \cdot 3 - (64 - 27 \cdot 2) \cdot 8 = 27 \cdot 19 - 64 \cdot 8$

$(x, y) = (-8, 19) \to$ Not unique

Cor (of the previous cor.): Assume $a, b \in \mathbb{Z}$ st. $\gcd(a,b) = 1$.

① $a \mid bc \Rightarrow a \mid c$.

② $a \mid c \wedge b \mid c \Rightarrow ab \mid c$

Remark ① generalizes Euclid's lemma

proof: ① $1 = ax + by$ for some $x, y \in \mathbb{Z}$

$a \mid bc \Rightarrow a \mid (by)c \Rightarrow a \mid (1 - ax)c \Rightarrow a \mid c - (ax)c$

$a \mid axc$, so it follows that $a \mid c$ $\blacksquare$