Last time: • Proved that factorization of integers into primes is unique (up to order)

• reviewed equivalence relations and equivalence classes

• $a \equiv b \bmod n \iff n \mid b-a$. $\equiv \bmod n$ is an equivalence relation

$\mathbb{Z}_n$ = set of all equivalence classes of $\equiv \bmod n$

$= \{[0],[1],[2],\dots,[n-1]\}$

There are well-defined operations $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, $[a]+[b]=[a+b]$

and $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad [a]\cdot[b]=[a\cdot b]$.

Example $4^{1237} = 5q+r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < 5$.

What's r?

Solution $[r] = [4^{1237}]$ in $\mathbb{Z}_5$

Since $[a]\cdot[b]=[ab]$ in $\mathbb{Z}_n$, $[a^k] = [\underbrace{a\cdots a}_{k}] = \underbrace{[a]\cdots[a]}_{k} = ([a])^k$ in $\mathbb{Z}_n$ for all $k \ge 1$

(really this should be proved by induction on k)

$\Rightarrow [4^{1237}] = [4]^{1237}$

In $\mathbb{Z}_5$, $[4] = [-1]$. $\Rightarrow [4]^2 = ([-1])^2 = [(-1)^2] = [1]$.

$\Rightarrow \forall k \in \mathbb{Z}$ $[4]^{2k+1} = ([4]^2)^k \cdot [4] = [1]^k \cdot [4] = [4]$

$\Rightarrow [4]^{1237} = [4]$. $\Rightarrow r = 4$.

Example $a \in \mathbb{N}$ is divisible by 9 $\iff$ the sum of its digits is divisible by 9.

Proof Suppose $a = d_r d_{r-1} \cdots d_0$ in decimal notation,

That is, suppose $a = d_0 + d_1\cdot 10^1 + d_2 \cdot 10^2 + \cdots + d_r \cdot 10^r$

$9 \mid a \iff [a] = [0]$ in $\mathbb{Z}_9$.

$[10] = [1]$ in $\mathbb{Z}_9$. $\to [10^k] = ([10])^k = ([1])^k = [1^k] = [1]$ in $\mathbb{Z}_9$

$\Rightarrow [a] = [d_0 + d_1 10^1 + \cdots + d_r \cdot 10^r] = [d_0] + [d_1][10] + \cdots + [d_r][10]^r$

$= [d_0] + [d_1]\cdot[1] + [d_2][1]^2 + \cdots + [d_r][1]^r =$

$= [d_0 + d_1 t - \cdots + d_r]$.

Therefore

$$9 \mid \sum_{j=0}^{r} d_j 10^j \iff 9 \mid \sum_{j=0}^{r} d_j .$$

Properties of the operations $+$ and $\cdot$ on $\mathbb{Z}_n$:(Prop 1.7.7 in Goodman)

(a) $+$ is commutative and associative:

$[a]+[b] = [b]+[a]$, $\quad ([a]+[b])+[c] = [a]+([b]+[c])$ for all $[a],[b],[c] \in \mathbb{Z}_n$

(b) $[0]$ is the identity element for $+$: $\forall [a] \in \mathbb{Z}_n$

$$[0] + [a] = [a]$$

(c) For every $[a] \in \mathbb{Z}_n$ there is $[b] \in \mathbb{Z}_n$ st.

$$[a] + [b] = [0]$$

(we may take $[b] = [-a]$)

(d) $\cdot$ is commutative and associative:

$[a]\cdot[b] = [b]\cdot[a]$, $\quad [a]\cdot([b]\cdot[c]) = ([a]\cdot[b])([c]$

for all $[a],[b],[c] \in \mathbb{Z}_n$

(e) $[1]$ is the identity for $\cdot$:

$$[1]\cdot[a] = [a] \quad \text{for all } [a] \in \mathbb{Z}_n$$

(f) distributive law holds

$$[a]\cdot([b]+[c]) = ([a]\cdot[b]) + ([a]\cdot[c]).$$

for all $[a],[b],[c] \in \mathbb{Z}_n$

Proof exercise.

Definition. $[a] \in \mathbb{Z}_n$ is a unit if $\exists [b] \in \mathbb{Z}_n$ s.t.

$$[a]\cdot[b] = [1]$$

- $[a] \in \mathbb{Z}_n$ is a zero divisor if $[a] \neq [0]$ and $\exists [b] \in \mathbb{Z}_n$ s.t. $[a][b] = [0]$

Example In $\mathbb{Z}_6$ $[2]\cdot[3]=[0]$ so $[2]$, $[3]$ are zero divisors.

$[5]\cdot[5]=[25]=[1]$ $\Rightarrow$ $[5]$ is a unit.

Proposition 8.1 $[a]\in\mathbb{Z}_n$ is a unit $\Leftrightarrow$ $\gcd(a,n)=1$

Proof $\gcd(a,n)=1 \Leftrightarrow \exists\, x,y\in\mathbb{Z}$ s.t. $xa+yn=1$

$\Leftrightarrow$ $n \mid ax-1$

$\Leftrightarrow$ $[0]=[ax-1]=[a][x]+[-1]$

$\Leftrightarrow$ $[1]=[a][x]$

Ex Find $[x]\in\mathbb{Z}_8$ so that $[x][5]=[2]$ or prove that no such $[x]$ exists.

Solution $\gcd(5,8)=1 \Rightarrow [5]$ is a unit in $\mathbb{Z}_8$

$8=1\cdot 5+3$ (division algorithm)

$5=3+2$

$3=2+1$

$\Rightarrow 1=3-2=3-(5-3)=2\cdot 3-5=2\cdot(8-5)-5$

$=2\cdot 8+(-3)\cdot 5$

$\Rightarrow [1]=[-3]\cdot[5]$ in $\mathbb{Z}_8$

$\Rightarrow [2]=[2]\cdot[1]=[2]\cdot[-3]\cdot[5]=[-6]\cdot[5]=[2]\cdot[5]$

$\therefore [x]=[2]$.

Proposition 8.2 $[0]\neq[k]\in\mathbb{Z}_n$ is either a unit or a zero divisor.

Proof $[k]\in\mathbb{Z}_n$ is a unit $\Leftrightarrow$ $\gcd(k,n)=1$.

So if $[k]\in\mathbb{Z}_n$ is not a unit, $d=\gcd(k,n)>1$.

For $[k]\neq[0]$ we may assume $0<k<n$.

Since $d\mid k$, $\exists\, s\in\mathbb{N}$ s.t. $k=s\cdot d$

Since $d\mid n$ $\exists\, q\in\mathbb{N}$ s.t. $n=q\cdot d$. We have $0<q<n$.

Now $k\cdot q=s\cdot d\cdot q=s\cdot n$.

$\Rightarrow \quad [h][q] = [kq] = [s \cdot n] = [0] \quad$ in $\mathbb{Z}_n$

Since $0 < h, q < n$, $\quad [k], [q] \neq [0]$ in $\mathbb{Z}_n$

$\Rightarrow$ $[k]$ is a zero divisor. □