Recall: New "ring" $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$

or simply $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

with 2 operations: $+$, $\times$:

e.g $[3]_5 + [4]_5 = [3+4]_5 = [7]_5 = [2]_5$

$([a]_n = [b]_n \Leftrightarrow a \equiv b \mod n \Leftrightarrow a-b$ div. by $n)$

If we write $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ then $3+4=2$ in $\mathbb{Z}_5$.

Recall: $a \in \mathbb{Z}_n$ has <u>inverse</u> $b \in \mathbb{Z}_n$ if $a \cdot b = 1$ in $\mathbb{Z}_n$ (i.e. $[a]_n \cdot [b]_n = [1]_n \Leftrightarrow ab \equiv 1 \mod n$ $\Leftrightarrow n \mid ab-1$)

<u>Proposition 2.15:</u> $a \in \mathbb{Z}_n$ is invertible $\Leftrightarrow$ $\gcd(a,n) = 1$ (i.e a and n are coprime)

<u>Corollary 2.16:</u> If n is prime $(n=p)$ then all non-zero elements of $\mathbb{Z}_p$ are invertible. Thus, $\mathbb{Z}_p = \{0,1,2,3,\dots,p-1\}$ is a field.

Note: $\underbrace{1+1+\dots+1}_{p} = 0$ in $\mathbb{Z}_p$, so $\mathbb{Z}_p$ <u>has characteristic p</u>

$\mathbb{R}, \mathbb{C}, \mathbb{Q}$ all <u>have characteristic zero</u>

Remark 2.17: $\mathbb{Z}_p$ is an example of a finite field (i.e. a field with finitely many elements).

Proof of 2.15: $(\Rightarrow)$ suppose a is invert. $\Rightarrow ab = 1$ for some $b \in \mathbb{Z}_n$

$\Rightarrow ab \equiv 1 \mod n \Rightarrow n \mid ab-1 \Rightarrow ab - 1 = nc \quad (c \in \mathbb{Z})$

$\Rightarrow ab - nc = 1 \Rightarrow$ by 1.9 $\gcd(a,n) = 1$.

$(\Leftarrow)$ $\gcd(a,n) = 1 \Rightarrow$ by 1.9 $ax + ny = 1 \quad (x,y \in \mathbb{Z}) \Rightarrow ax - 1 = ny$

$\Rightarrow n \mid ax - 1 \Rightarrow ax - 1 \equiv 0 \mod n \Rightarrow ax \equiv 1 \mod n$

$\Rightarrow [a]_n [x]_n = [1]_n \Rightarrow ax = 1$ in $\mathbb{Z}_n \Rightarrow \alpha$ is inv. in $\mathbb{Z}_n$.

Example 2.18: $n=83$, $a=13$, find $[13]_{83}$. In ex. 1.6 we found $\gcd(13,83)=1$

by doing backwards calculations, we get $32\cdot 13 - 5\cdot 83 = 1$.

hence $32\cdot 13 \equiv 1 \mod 83$, so $32\cdot 13 = 1$ in $\mathbb{Z}_{83}$, so $[13]_{83}^{-1} = [32]_{83}$

<u>Definition 2.20:</u> Suppose a is invertible in $\mathbb{Z}_n$. Then the <u>multiplicative order</u> of a in $\mathbb{Z}_n$ is

min $k \geq 1$ s.t. $a^k = 1$ in $\mathbb{Z}_n$ (we write $O(a)=k$).

Note: $O(1)=1$ (as $1^1=1$);

to find order of a we simply calculate $a, a^2, a^3, \ldots$ until we get $a^k = 1$.

Example 2.21: $O(2) = ?$ in $\mathbb{Z}_7 = \{0,1,2,\ldots,6\}$

$2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 1 \pmod 7$ so $O(2) = 3$

$3^1 = 3$, $3^2 = 2$, $3^3 = 3^2\cdot 3 = 2\cdot 3 = 6$, $3^4 = 6\cdot 3 = 4$, $3^5 = 4\cdot 3 = 5$, $3^6 = 1$ so $O(3) = 6$.

<u>Lemma 2.22:</u> Let $a \in \mathbb{Z}_n$ with $O(a) = m$. Let $x, y \in \mathbb{Z}$. Then $a^x = a^y$ in $\mathbb{Z}_n \Leftrightarrow x \equiv y \mod m$

In particular, the elements $a^0 = 1, a^1, a^2, \ldots, a^{m-1}$ are all distinct in $\mathbb{Z}_n$.

Proof: Exerc.

Note: $a^m = 1 = a^0$

$a^{m+1} = a^m \cdot a = a^1$

$a^{m+2} = a^m \cdot a^2 = a^2$

$\vdots$

Rest of section (primitive roots) in H/W, also

in Number Th. in Y3.

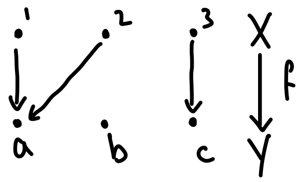
3 Maps

Definition 3.1: Let X, Y be sets. A map (or mapping, or function) $f: X \to Y$ is a rule which assigns to each $x \in X$ an element $f(x) \in Y$ ($f(x)$ is the image of x).

The image of f is $\operatorname{im} f = f(X) = \{f(x) \mid x \in X\} \subseteq Y$.

If $y \in Y$ then preimage of y is $f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$

Example 3.2: $X = \{1, 2, 3\}$, $Y = \{a, b, c\}$



$f: X \to Y$

images: $f(1) = a$, $f(2) = b$, $f(3) = c$

preimages: $f^{-1}(a) = \{1, 2\}$, $f^{-1}(b) = \emptyset$, $f^{-1}(c) = \{3\}$

$\operatorname{im} f = \{a, c\}$

Definition 3.3: $f: X \to Y$ is injective if distinct elements are mapped to distinct elements, i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$ or equivalently if $f(x_1) = f(x_2)$ then $x_1 = x_2$.