Intro to Abstract Algebra
-MA136-

$(ab)^{-1} = b^{-1}a^{-1}$

e is unique and inverse is unique

binary operation

let S be a set, A binary operation $*$ is a rule s.t. given $s_1, s_2 \in S$, $s_1 * s_2 \in S$

commutative

$*$ commutative on S if $a*b = b*a$ $\forall a, b \in S$

associative

$*$ associative on S if $(a*b)*c = a*(b*c)$ $\forall a, b, c \in S$

Group

A group is a pair $(G, *)$. G set, $*$ binary operation satisfying:

(i) $\forall a, b \in G$, $a*b \in G$ [closure]

(ii) $\forall a, b \in G$, $(a*b)*c = a*(b*c)$ [associativity]

(iii) $\exists e \in G$ s.t. $\forall a \in G$, $a*e = e*a = a$ [identity]

(iv) $\forall a \in G$, $\exists b \in G$ s.t. $a*b = b*a = e$ [inverse]

[Growth multiplication and power rules apply]

examples

$(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^2, +)$ etc.

abelian

a group $(G, *)$ abelian if it also satisfies commutivity

(v) $\forall a, b \in G$, $a*b = b*a$

can have multiplicative or additive notation

General linear group

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \det(A) \neq 0 \right\}$

is a group under matrix multiplication

Congruence classes

$(\mathbb{Z}/m\mathbb{Z}, +)$ is an abelian group $m \geq 2$

order of an element

$a \in G$. order of a in G is the smallest positive integer n s.t. $a^n = 1$. If $\nexists n$, infinite order

G group, $g \in G$

(i) $\text{order}(g) = 1 \iff g = 1$

(ii) $g^m = 1 \iff \text{ord}(g) \mid m$

Proof: ...

order of a group

G group, order of G is the number of elements G has. $|G|$, $\# G$

U_n

U_n = set of nth roots of unity

$\zeta = e^{2\pi i/n}$

$U_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$

Subgroup

Let $(G, *)$ be a group, let $H \subseteq G$, suppose $(H, *)$ also a group. Then $(H, *)$ is a subgroup of $(G, *)$

Same binary op!

G and $\{1\}$ are subgroups of G

we want proper & non-trivial

Criteria

$H \subseteq G$ subgroup iff

(a) $1 \in H$

(b) $a, b \in H \Rightarrow ab \in H$

(c) if $a \in H \Rightarrow a^{-1} \in H$

e.g. planes are subgroups of $\mathbb{R}^3$

Special linear group

$SL_2(\mathbb{R}) = \{ A \in M_{2\times 2}(\mathbb{R}) \mid \det(A) = 1 \}$

proper subgroup

a subgroup not equal to G

trivial subgroup

that is $\{1\}$.

cyclic subgroup

$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \} = \{ \dots g^{-2}, g^{-1}, 1, \dots \}$

is a subgroup of G. $g \in G$.

g is a generator of G if $\langle g \rangle = G$

modular group

$SL_2(\mathbb{Z})$

Special orthogonal group

$SO_2(\theta) = \{ R_\theta \mid \theta \in \mathbb{R} \}$

Map(A)

the set of functions from A to itself

G group, $g \in G$, order$(g) = n$

$\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$

Proof: to sets equal show subsets of each other.

cyclic groups are abelian

permutations

$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \iff (a_1, a_2, \dots, a_n)$

Sym(A)

set of bijections from A to itself

S_n

Sym$\{1, \dots, n\}$

$|S_n| = n!$

every permutation can be written as the product of disjoint cycles

disjoint cycles commute

$n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

all subgroups of $\mathbb{Z}$ are cyclic

Isomorphism

Let $(G, \circ)$ and $(H, *)$ be groups

$\phi : G \longrightarrow H$ is an isomorphism is a bijection

$\phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2) \Rightarrow (G, \circ)$ and $(H, *)$ are isomorphic

Coset

Let G be a group H a subgroup $g \in G$. The cosets are

$$gH = \{gh \mid h \in H\} \text{ [left coset]}$$

$$Hg = \{hg \mid h \in H\} \text{ [right coset]}$$

e.g. $2\mathbb{Z}$ has 2 cosets, $2\mathbb{Z}$ and $1+2\mathbb{Z}$

e.g. $2\mathbb{Z}^2$ has 4 cosets etc...

e.g. a line in $\mathbb{R}^2$ is a subgroup $\iff$ it passes through the origin. If it does, its cosets are the lines parallel to it

related to the $\underline{x} = x_0 +$ ~~ker~~ nullspace(A) in MA106 & solutions to DEs in Diff Eqn MA133

NOTE: ~~for~~ non-abelian groups, we have a right cosets version. For additive abelian groups:

Let $(G,+)$ be an abelian group, let H be a subgroup. Let $g_1, g_2 \in G$ so that $g_1 + H$ and $g_2 + H$ are cosets. Then

(i) $g_1 + H = g_2 + H \iff g_1 - g_2 \in H$

(ii) $(g_1 + H) \cap (g_2 + H) = \emptyset \iff g_1 - g_2 \notin H$

Lagrange's Theorem

Thm: Let G be a finite group and H a subgroup. Then

$$|G| = [G:H] \cdot |H|$$

Corollaries:

- G finite group, H a subgroup. Then the order of H divides the order of G $|H| \mid |G|$
- G finite group. $g \in G$. Then $\text{order}(g) \mid |G|$
- Let G be a finite group of order n, $g \in G$. Then $g^n = 1$

Index

Let G be a group and H a subgroup. define the <u>index</u> of H in G $[G:H]$ to be the number of left cosets of H in G

$[\mathbb{Z} : 2\mathbb{Z}] = 2$, $[\mathbb{Z}^2 : 2\mathbb{Z}^2] = 4$

Example $\mathbb{S} = \{\alpha \in \mathbb{C} \mid |\alpha| = 1\}$. cosets of $\mathbb{S}$ are $\alpha\mathbb{S}$ where $\alpha \in \mathbb{C}$ so $\alpha = re^{i\alpha}$.

so $re^{i\alpha}\mathbb{S} = r\mathbb{S}$ where $r \in \mathbb{R}$ as just rotated so we have as many cosets as there are ~~as~~ real numbers: $[\mathbb{C}^* : \mathbb{S}] = \infty$

TWO FACTS

(1) Coset of a subgroup has same size as subgroup

Lemma: G group, H finite subgroup. If $g \in G$, then gH ~~have~~ and Hg have same # elements as H.

Pf: set up a bijection $\phi: H \to gH$ s.t. $h \mapsto gh$ & prove it is injective & surjective.

(2) Any two cosets of H are either equal or disjoint.

Lemma: G group, H subgroup. Let $g_1, g_2 \in G$ s.t. g_1H and g_2H both left cosets. Then

(i) $g_1H = g_2H \iff g_2^{-1}g_1 \in H$

(ii) $g_1H \cap g_2H = \emptyset \iff g_2^{-1}g_1 \notin H$

either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$

Pf: in notes

Proof: Let $g_1H, \dots, g_mH$ be the distinct left cosets of H. by fact (2), they are disjoint.

Suppose $g \in G$. Then gH = one of the g_iH but as $1 \in H$, then $g \in gH$ so every element of G belongs to exactly 1 coset so

$$|G| = |g_1H| + |g_2H| + \dots + |g_mH|$$

But we know

$$|g_1H| = \dots = |g_mH| = |H|$$

so $|G| = m \cdot |H|$ where m is the number of left cosets gH in G, so $m = [G:H]$

Pf of bullet 2: As G finite, order$(g) < \infty$ otherwise ~~$G \supseteq$~~ $\{g^n \mid n \in \mathbb{Z}\} \subset G$. We know order of subgroup $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ as $g^n = 1$ where n is order of g, so $|\langle g \rangle| = \text{order}(g)$. We know the order of a subgroup divides $|G|$ so

$$\text{order}(g) \mid |G|.$$

Quotient Groups

Def: Let $(G,+)$ be an additive abelian group and H a subgroup. Define the quotient group $(G/H,+)$ to be the set of cosets

$$G/H = \{a+H \mid a \in G\}$$

Note: addition defined by $(a+H)+(b+H) = (a+b)+H$ [we add cosets together]

need to check addition well defined & prove it is a group

Example: $a+m\mathbb{Z} = \bar{a}$ so congruence classes modulo n are the exact same group as the quotient group $(\mathbb{Z}/m\mathbb{Z},+)$

congruence multiplication: $\bar{a}=\overline{a'}$ and $\bar{b}=\overline{b'}$ in $\mathbb{Z}/m\mathbb{Z}$ then $\overline{ab}=\overline{a'b'}$

Examples

- $\mathbb{R}/\mathbb{Z} = \{a+\mathbb{Z} \mid a\in[0,1)\}$
- $f:\mathbb{R}\to S$, $f(\theta)=e^{2\pi i\theta}$ is **not** a bijection
  $\hat{f}:\mathbb{R}/\mathbb{Z}\to S$, $\hat{f}(\theta+\mathbb{Z}) = e^{2\pi i\theta}$ **is** a bijection
  $\to (\mathbb{R}/\mathbb{Z},+)$ and $(S,\cdot)$ are isomorphic
- $\mathbb{R}^2/\mathbb{Z}^2$: $\{(x,y): x\in[0,1), y\in[0,1)\}$

elements of order 2 in $\mathbb{R}^2/\mathbb{Z}^2$?, then

$$((x,y)+\mathbb{Z}^2)+((x,y)+\mathbb{Z}^2) = (0,0)+\mathbb{Z}^2$$

$\therefore$ $2x, 2y$ integers

$2x = \dots,-1,0,1,\dots \quad 2y=\dots,-1,0,1,\dots$

$x = \dots,-\frac{3}{2},-\frac{1}{2},0,\frac{1}{2},\dots$

so $x = 0,\frac{1}{2}$, $y=0,\frac{1}{2}$ so order 2 elements are

$(\frac{1}{2},0)+\mathbb{Z}^2$, $(0,\frac{1}{2})+\mathbb{Z}^2$, $(\frac{1}{2},\frac{1}{2})+\mathbb{Z}^2$

Every permutation can be written as a product of transpositions

$(1,2,3,4) = (1,4)(1,3)(1,2)$

nth alternating polynomial

$$P_n = \prod_{1\le i<j\le n}(x_i - x_j)$$

If $\sigma\in S_n$

$$\sigma(P_n) = \prod_{1\le i<j\le n}(x_{\sigma(i)} - x_{\sigma(j)})$$

Let $\tau\in S_n$ be a transposition then $\tau(P_n) = -P_n$

If $\sigma\in S_n$, $\sigma(P_n)=\pm P_n$.
If σ is a product of an even number of transpositions then $\sigma(P_n)=P_n$.
If σ product of an odd number of transpositions, then $\sigma(P_n) = -P_n$

Every permutation in S_n can be written as a product of either an even or an odd number of transpositions but not both

proof: suppose we can. Then $\sigma(P_n)=\sigma(P_n) \Rightarrow P_n = -P_n$ X

permutation
- even: can write as a product of an even # of transpositions
- odd: can write as a product of an odd number of transpositions

A_n

Let $n\geq 2$. The nth alternating group is

$$A_n = \{\sigma\in S_n \mid \sigma \text{ even}\}$$

Proof that A_n subgroup of S_n
- id even so id $\in A_n$
- if $\sigma,\tau\in A_n$ then $\sigma\tau$ even so $\sigma\tau\in A_n$
- suppose σ even
  $\sigma = \tau_1\dots\tau_m$
  $\sigma^{-1} = (\tau_1\dots\tau_m)^{-1}$
  $\sigma^{-1} = \tau_m^{-1}\dots\tau_1^{-1}$
  $= \tau_m\dots\tau_1$
  even so $\sigma^{-1}\in A_n$
  $\therefore$ A_n subgroup of S_n

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Pf: Lagrange says $|S_n| = [S_n:A_n]|A_n|$

WTS $[S_n:A_n]=2$

A_n is even permutations
does τA_n contain all odd?
Suppose σ odd. Then $\tau\sigma$ even and so $\tau\sigma\in A_n$
$\therefore$ $\tau(\tau\sigma)$ in coset τA_n.
but $\tau(\tau\sigma) = \tau^2\sigma = \sigma$
[transpositions have order 2]
$\therefore$ $\sigma\in\tau A_n$. cosets disjoint or equal so $[S_n:A_n]=2$.

Rings

R ring, $a\in R$, then $0\cdot a = 0 = a\cdot 0$
if $b\in R$ too, $-(a\cdot b) = (-a)\cdot b = a\cdot(-b)$

A ring is a triple $(R,+,\cdot)$ where R set, $+,\cdot$ binary operations such that the following 8 properties hold

1. closure: $\forall a,b\in R$, $a+b\in R$ and $a\cdot b\in R$
2. associativity addition: $\forall a,b,c\in R$, $(a+b)+c = a+(b+c)$
3. existence of additive identity: $\exists 0\in R$ s.t. $\forall a\in R$, $a+0=0+a=a$
4. existence of additive inverses: $\forall a\in R$ $\exists$ element denoted $-a$ such that $a+(-a)=(-a)+a=0$
5. commutativity of addition: $\forall a,b\in R$, $a+b=b+a$
6. associativity of multiplication: $\forall a,b,c\in R$ $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
7. distributivity: $\forall a,b,c\in R$, $a\cdot(b+c) = a\cdot b + b\cdot c$, $(b+c)\cdot a = b\cdot a + c\cdot a$
8. existence of multiplicative identity: $\exists 1\in R$ s.t. $\forall a\in R$: $1\cdot a = a\cdot 1 = a$

A ring $(R,+,\cdot)$ is commutative if it additionally satisfies 9. commutativity of multiplication: $\forall a,b\in R$, $a\cdot b = b\cdot a$

Examples: commutative rings: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[x]$, $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$
non-commutative rings: $M_{2\times2}(\mathbb{R})$, $M_{2\times2}(\mathbb{C})$ etc
non-rings: $(\mathbb{R}[x],+,\circ)$. distributivity fails. Take $f=x^2$, $h=g=x$

Note: can define multiplication in $\mathbb{R}^2$ in several ways.
$(a_1,b_1)\times(a_2,b_2) = (a_1a_2, b_1b_2)$ is obvious or using $\mathbb{C}$ geometry $(a_1,b_1)\times(a_2,b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)$
with multiplicative identity $(1,0)$! $(1+0i)$

Is $(\mathbb{R}^3,+,\times)$ a ring?

2/4

$\underline{i}\times(\underline{j}\times\underline{j}) = \underline{0}$
$(\underline{i}\times\underline{j})\times\underline{j} = -\underline{i}$
so cross product not associative. So **no**

Also $\underline{a}\times\underline{b} = -\underline{b}\times\underline{a}$ so $\underline{a}\times\underline{1} = \underline{1}\times\underline{a} = -\underline{a}$ so 8 fails

Subrings

$1_R \in S$

Let $(R,+,\cdot)$ be a ring. Let $S \subseteq R$ and suppose $(S,+,\cdot)$ is also a ring wrt same multiplicative identity. Then S is a subring of R
[$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$]

e.g $\mathbb{Z}$ subring of $\mathbb{R}$. $\mathbb{R}$ subring of $\mathbb{R}[x]$

$(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$ but $(2\mathbb{Z},+,\cdot)$ is not a subring of $(\mathbb{Z},+,\cdot)$ as $1 \notin 2\mathbb{Z}$

$\Rightarrow$ only subring of $\mathbb{Z}$ is itself! but $\mathbb{Z}$ has infinite subgroups

Unit

Def: Let R be a ring. $u \in R$ is a **unit** if $\exists v \in R$ s.t. $uv = vu = 1$

e.g an element u of R is a unit if it has a multiplicative inverse that belongs to R

units of $\mathbb{Z}$ are ± 1 so $\mathbb{Z}^* = \{-1, 1\}$

units of $M_{2\times2}(\mathbb{R})$ are the invertible matrices, those with non-zero determinant so $(M_{2\times2}(\mathbb{R}))^* = GL_2(\mathbb{R})$

But what about units of $M_{2\times2}(\mathbb{Z})$? $A = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$ but $A^{-1} = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 3/2 \end{pmatrix}$ so $A^{-1} \notin M_{2\times2}(\mathbb{Z})$

Back to unit def:
$\therefore AB = BA = I_2 \Rightarrow \det(A)\det(B) = 1$, $\det(A)$ and $\det(B)$ integers
$\because A, B \in M_{2\times2}(\mathbb{Z})$ so $\det(A) = \det(B) = \pm 1$.
so in all, $(M_{2\times2}(\mathbb{Z}))^* = \{A \in M_{2\times2}(\mathbb{Z}) \mid \det(A) = \pm 1\}$

Norm map

$N : \mathbb{Z}[i] \to \mathbb{Z}$ given by
$N(a+ib) = a^2 + b^2$, $a, b \in \mathbb{Z}$

$N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[i]$

Fields

every non zero element has a multiplicative inverse

A field $(F,+,\cdot)$ is a commutative ring which is not the zero ring s.t. every non-zero element is a unit

so a commutative ring F is a field
$\Longleftrightarrow$
its unit group $F^* = \{a \in F \mid a \neq 0\}$

e.g $\mathbb{Z}$ not a field since $2 \in \mathbb{Z}$ but 2 is not a unit.
$\mathbb{R}[x]$ not a field as $x \in \mathbb{R}[x]$, $x \neq 0$ but x is not a unit

Conditions to check

Let R be a ring. $S \subseteq R$ ring iff
(a) $0, 1 \in S$ [S contains additive & multiplicative identity elements of R]
(b) if $a, b \in S$, then $a+b \in S$
(c) if $a \in S$, then $-a \in S$
(d) if $a, b \in S$, then $ab \in S$

Easiest way to show a set is a ring is to show it is a subring of a known ring

Gaussian integers
$\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$

Pf that $\mathbb{Z}[i]$ is a ring: check (a), (b), (c), (d) true so subring of $\mathbb{C}$ $\Rightarrow$ ring

$S = \left\{\frac{a}{2^r} : a, r \in \mathbb{Z}, r \geq 0\right\}$ show it's a ring by showing S is a subring of $\mathbb{Q}$

The Unit Group of a Ring

Let R be a ring. We define the unit group of R to be the set
$$R^* = \{a \in R \mid a \text{ is a unit in } R\}$$

Unit group of $\mathbb{Z}[i]$

Let α be a unit, then $\exists \beta \in \mathbb{Z}[i]$ s.t. $\alpha\beta = 1 \Rightarrow N(\alpha)N(\beta) = 1$
$\Rightarrow \alpha = a+ib$ so $(a,b) = (\pm1, 0)$ or $(0, \pm 1)$
$\therefore \mathbb{Z}[i]^* = \{1, -1, i, -i\}$

Units in $\mathbb{Z}/m\mathbb{Z}$

Use multiplication tables;
$(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\}$
$(\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}$
$(\mathbb{Z}/3\mathbb{Z})^* = \{\bar{1}, \bar{2}\}$
$(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\}$
$(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

general relation on the last page!

Steps to show $\mathbb{Q}[i]$ is a field

① Show $\mathbb{Q}[i]$ commutative ring:
(a) enough to show $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$.
(b) $0 \in \mathbb{Q}[i]$, $1 \in \mathbb{Q}[i]$
closed under addition, multiplication, negation

② Need to show every non-zero element of $\mathbb{Q}[i]$ is a unit.
WTS $\exists \beta \in \mathbb{Q}[i]$ s.t. $\alpha\beta = \beta\alpha = 1$
so need to show $\frac{1}{\alpha}$ exists
and indeed $\frac{1}{\alpha} \in \mathbb{Q}[i] \Rightarrow \mathbb{Q}[i]$ field

relationship between the units of $\mathbb{Z}/m\mathbb{Z}$

Let $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$.

$\bar{a}$ unit in $\mathbb{Z}/m\mathbb{Z}$ $\iff \gcd(m,a)=1$

so $(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{a} \mid 0 \le a \le m-1 \text{ and } \gcd(a,m)=1\}$

'$\Rightarrow$'

Proof: Suppose $\bar{a}$ unit in $\mathbb{Z}/m\mathbb{Z}$. Then $\exists\, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ s.t. $ab \equiv 1 \pmod m \iff ab-1 = km$ for $k \in \mathbb{Z}$. Let $g = \gcd(a,m)$

$\Rightarrow g \mid a$ and $g \mid m$ $\therefore g \mid (ab-km) = 1 \Rightarrow g=1$

'$\Leftarrow$' Suppose $\gcd(a,m)=1$. By bezout's lemma $\exists\, b,c \in \mathbb{Z}$ s.t. $1 = ba + cm$

$\iff ab \equiv 1 \pmod m$

$\Rightarrow \bar{a}$ is a unit

$\boxed{\mathbb{Z}/p\mathbb{Z} \text{ field}}$

Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field

so $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

Proof: We know $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring $\forall m \ge 2$ so WTS every nonzero $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ is a unit [so is invertible]. Consider $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ non-zero. $a = 1, \dots, p-1$ so $a \nmid p$. As p prime, $\gcd(a,p)=1$ so by thm in top left of page, $\bar{a}$ is a unit so invertible in $\mathbb{Z}/p\mathbb{Z}$. $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ is a field.

Inverse of $\overline{19}$ in $\mathbb{Z}/256\mathbb{Z}$?

$\gcd(19, 256) = 1$. Using euclid's algorithm

$256 = 13 \times 19 + 9$

$19 = 2 \times 9 + 1$

$\Rightarrow 1 = 19 - 2 \times 9$

$1 = 19 - 2(256 - 13 \times 19)$

$1 = 27 \times 19 - 2 \times 256$

so $27 \times 19 \equiv 1 \pmod{256}$

$\Rightarrow \overline{27}$ inverse of $\overline{19}$ in $\mathbb{Z}/256\mathbb{Z}$

Think of the def of a unit here!

Fermat's Little Theorem

Let p be a prime, $a \in \mathbb{Z}$ s.t. $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod p$$

Proof: lets consider $a \pmod p$. We know $a \equiv b \pmod p$ where $b = 0, \dots, p-1$. As $p \nmid a \Rightarrow b \neq 0$ [$a \neq pk$]. By thm on units, $\bar{b} \in (\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \dots, \overline{p-1}\}$. ~~order~~ $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$, so by Lagrange's thm corollary, $\bar{b}^{p-1} = \bar{1} \Rightarrow b^{p-1} \equiv 1 \pmod p$

As $a \equiv b \pmod p$, $a^{p-1} \equiv 1 \bmod (p)$

trick - what is $2^{1000} \pmod{13}$?

13 prime, $2 \nmid 13$, FLT $\Rightarrow 2^{12} \equiv 1 \pmod{13}$

Note $1000 = 83 \times 12 + 4$

so $2^{1000} \equiv 2^{83 \times 12 + 4} \equiv (2^{12})^{83} \times 2^4 \equiv 16 \equiv 3 \pmod{13}$

neat!

Euler's φ function

order of the group $(\mathbb{Z}/m\mathbb{Z})^*$ is $\varphi(m)$

Euler's theorem

$m \ge 2$. $a \in \mathbb{Z}$ s.t. $\gcd(a,m)=1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod m$$

Pf: modify what's on the left!

formula

Write $m = p_1^{r_1} \cdots p_k^{r_k}$ where $p_1, \dots, p_k$ are distinct primes and $r_1, \dots, r_k$ positive integers. Then

$$\varphi(m) = (p_1^{r_1} - p_1^{r_1 - 1}) \cdots (p_k^{r_k} - p_k^{r_k - 1})$$

Proof: non-examinable!