Lecture 11

Another corollary of Lagrange's theorem is:

<u>Corollary</u> Let G be a finite group, and $a \in G$. Then

$$a^{|G|} = e.$$

<u>Proof</u> A previous corollary says $o(a) \mid |G|$, where $o(a) = |\langle a \rangle|$ is the order of a. We also know $o(a)$ is the smallest positive integer such that $a^n = e$.

So $a^{o(a)} = e$.

Now write $|G| = o(a) \cdot m$, then

$$a^{|G|} = a^{o(a) \cdot m} = (a^{o(a)})^m = e^m = e. \quad \blacksquare$$

A nice application of this fact is Euler's theorem in number theory. Recall $[a] \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a,n) = 1$.

$\mathbb{Z}_n^\times = \{[a] \mid [a] \text{ has a multi. inverse}\}$ is a group under multiplication.

Define $\varphi(n) = |\mathbb{Z}_n^\times| = |\{k \mid 0 < k < n \text{ and } \gcd(k,n) = 1\}|$

this is called Euler's totient function φ.

$\mathbb{Z}_2^\times = \{[1]\}$ $\qquad \varphi(2) = 1$

$\mathbb{Z}_3^\times = \{[1], [2]\}$ $\qquad \varphi(3) = 2$

$\mathbb{Z}_4^\times = \{[1], [3]\}$ $\qquad \varphi(4) = 2$

$\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$ $\qquad \varphi(5) = 4$

$\mathbb{Z}_6^\times = \{[1], [5]\}$ $\qquad \varphi(6) = 2$

__Euler's Theorem__ if $\gcd(a,n)=1$, then

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

__Proof__ $\mathbb{Z}_n^\times$ is a group, and $[a] \in \mathbb{Z}_n^\times$ since $\gcd(a,n)=1$. So by the corollary of Lagrange's theorem,

$[a]^{\varphi(n)} = [1]$ in $\mathbb{Z}_n^\times$, which is equivalent to $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\blacksquare$

If p is a prime number, every a with $0 < a < p$ satisfies $\gcd(a,p)=1$. Thus $\mathbb{Z}_p^\times = \{[1],[2],\ldots,[p-1]\}$ and $\varphi(p) = p-1$

__Fermat's Little Theorem:__ For any integer a and prime p,

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

__Proof__ if $a \equiv 0 \bmod p$, then $a^p \equiv 0 \bmod p$, and so

$a^p \equiv 0 \equiv a \pmod{p}$

If $a \not\equiv 0 \bmod p$, then $\gcd(a,p)=1$, so by Euler's theorem,

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

But $\varphi(p) = p-1$, so

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

Multiplying both sides by a, $a^p \equiv a \pmod{p}$ in this case as well $\blacksquare$

E.g. 3457 is prime. So $2^{3457} \equiv 2 \pmod{3457}$

Equivalence Relations and Partitions

Let X be a set. Define $X \times X = \{(x,x') \mid x \in X,\ x' \in X\}$ to be the set of ordered pairs of elements of X.

Example: What is $\mathbb{R} \times \mathbb{R}$? A: it is $\mathbb{R}^2$, the plane.

A relation on X is a subset $R \subseteq X \times X$.
We write $x \sim x'$ or $x \sim_R x'$ to mean $(x,x') \in R$

A relation is an equivalence relation if it is reflexive, symmetric and transitive:

Reflexive $\forall x \in X$, $x \sim x$, $(x,x) \in R$.

Symmetric $\forall x, x' \in X$, $x \sim x'$ if and only if $x' \sim x$
$(x,x') \in R \iff (x',x) \in R$

Transitive $\forall x,y,z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$
$[(x,y) \in R \text{ and } (y,z) \in R] \Longrightarrow (x,z) \in R.$

Example ① X any set, $\sim$ is the relation $=$
$R = \{(x,x') \mid x = x'\} = \{(x,x) \mid x \in X\}$

$x = x$ reflexive
$x = y \Rightarrow y = x$ symmetric
$x = y$ and $y = z \Rightarrow x = z$ transitive.

② Fix $n \in \mathbb{N}$. $X = \mathbb{Z}$. Say $x \sim y$ if $x \equiv y \pmod{n}$

$$R = \{(x,y) \mid x \equiv y \pmod{n}\} = \{(x,y) \mid n \mid (y-x)\}$$

Already checked the three properties

③ X = students at U of I: $x \sim y$ if x and y are same age.
This is an equivalence relation.

④ X = students at U of I: $x \sim y$ if ages differ by at most one year.
Not transitive: if $x \sim y$ and $y \sim z$, then x and z could differ by 2 years.

⑤ $X = \mathbb{Z}$ $x \sim y$ if $x < y$.
Not reflexive: $x < x$ is false.
· $x \leq y$ is reflexive but not symmetric
But both $<$ and $\leq$ <u>are</u> transitive.

⑥ G a group, H a subgroup. for $a, b \in G$, say $a \sim b$ if $a^{-1}b \in H$.

- $a^{-1}a = e \in H$ so $a \sim a$.
- if $a \sim b$, $a^{-1}b \in H$, so $(a^{-1}b)^{-1} = b^{-1}a \in H$ so $b \sim a$.
- if $a \sim b$ and $b \sim c$ then $a^{-1}b \in H$ and $b^{-1}c \in H$, so $a^{-1}bb^{-1}c = a^{-1}c \in H$, so $a \sim c$.

Hence this is an equivalence relation.

If X is a set, then a <u>partition</u> of X is a collection of subsets of X, call it Ω, such that

- For all $A, B \in \Omega$, $A \cap B = \emptyset$ or $A = B$
- $X = \bigcup_{A \in \Omega} A$

i.e. Ω is a collection of subsets that are pairwise disjoint and whose union is X.

<u>Examples</u>: ① X any set, take $\Omega = \{\{x\} \mid x \in X\}$

$\forall \{x\}, \{y\} \in \Omega$, $\{x\} \cap \{y\} = \emptyset$ or $\{x\} = \{y\}$ depending on whether $x = y$ or not.

$X = \bigcup_{x \in X} \{x\}$ is true. So Ω is a partition.

② $X = \mathbb{Z}$, $\Omega = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
the set of congruence classes modulo n.

$[a] \cap [b] \neq \emptyset \iff a \equiv b \pmod{n} \iff [a] = [b]$

$\mathbb{Z} = [0] \cup [1] \cup \dots \cup [n-1]$ so this is a partition.

③ X = students at U of I. For each n, define
$A_n = \{s \in X \mid s \text{ is } n \text{ years old today}\}$

Then $\Omega = \{A_n \mid n \geq 0 \text{ and there is a student of age } n\}$ is a partition of X.

④ G a group, $H \leq G$. Ω = left cosets of $H = \{aH \mid a \in G\}$
We have already seen this is a partition.