Number Theory, Lecture 2b

Multiplicative order, Cyclic Groups, Fermat's and Euler's thms

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

Summary

Summary

Definition

$(G, *, e)$ is a group if for all $a, b, c \in G$,

1. $a * (b * c) = (a * b) * c$,
2. $a * e = e * a = a$,
3. exists unique $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$.

If $a * b = b * a$ always, then abelian group.

Lemma

If R commutative unitary ring, then $R^* = \{ r \in R | r$ is a unit $\}$ is an abelian group under multiplication. In particular, if R field, then $R^* = R \setminus \{0\}$.

Remember: in $\mathbb{Z}_n$, $g = [a]_n$ invertible iff $\gcd(a,n) = 1$.

Definition

$\mathbb{Z} \ni n > 1$.

- $\mathbb{Z}_n^* = \{\, [a]_n | \gcd(a,n) = 1 \,\}$.
- $\phi(n) = |\{\, 1 \leq a < n | \gcd(a,n) = 1 \,\}| = |\mathbb{Z}_n^*|$.

Example

$\mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$, $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$.

Example

Multiplication in $\mathbb{Z}_5^*$ and $\mathbb{Z}_8^*$

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition

- G finite group, $g \in G$.
- $g^2 = g * g$, $g^3 = g * g * g$, et cetera.
- $g^{-2} = g^{-1} * g^{-1} = (g * g)^{-1}$.
- $g^i * g^j = g^{i+j}$.
- $g \in G$ has order $o(g) = n$ if $g^n = 1$ but $g^m \neq 1$ for $1 \leq m < n$.
- Exists since $g^i = g^j$ implies $g^{i-j} = g^0 = 1$.
- $g^s = 1$ iff $n|s$.
- $g^i = g^j$ iff $i \equiv j \mod n$.
- Say that a has (multiplicative) order n modulo m if $o([a]_m) = n$, i.e. if $a^n \equiv 1 \mod m$ but not for smaller power.

Example

- $3^2 = 9 \equiv 1 \mod 8$, so 3 has multiplicative order 2 modulo 8.
- $3^2 = 9 \equiv 4 \mod 5$, $3^3 = 27 \equiv 2 \mod 5$, $83^4 = 81 \equiv 1 \mod 5$, so 3 has multiplicative order 4 modulo 5.

Definition

- G group, $*$ operation, 1 unit
- $g \in G$
- $\langle g \rangle = \{ g^n | n \in \mathbb{Z} \}$
- Subgroup of G, smallest that contain g
- Cyclic subgroup generated by g
- If $G = \langle g \rangle$ then G cyclic group, g generator
- Additively: $(G, +, 0)$, $\langle g \rangle = \{ ng | n \in \mathbb{Z} \}$

Lemma

- $o(g) = |\langle g \rangle|$
- $(\mathbb{Z}_n, +, [0]_n) = \langle [1]_n \rangle$
- $\mathbb{Z} = \langle 1 \rangle$
- $\mathbb{Z}_5^* = \langle [2]_5 \rangle$
- $\mathbb{Z}_8^*$ *not cyclic*

Isomorphic groups

- G, H groups
- $f : G \to H$ bijection, $f(g_1 * g_2) = f(g_1) * f(g_2)$
- $G \simeq H$, G and H isomorphic
- Same structure, different name for elements

- All properties preserved
- In particular, up to iso, only one cyclic of size n, call it C_n.
- $(\mathbb{Z}_n, +) \simeq C_n$
- $(\mathbb{Z}, +) \simeq C_\infty$,
- $(\mathbb{Z}_5^*, *) \simeq C_4$

Definition

- G, H groups
- $G \times H = \{ (g,h) | g \in G,\ h \in H \}$
- Componentwise addition and multiplication

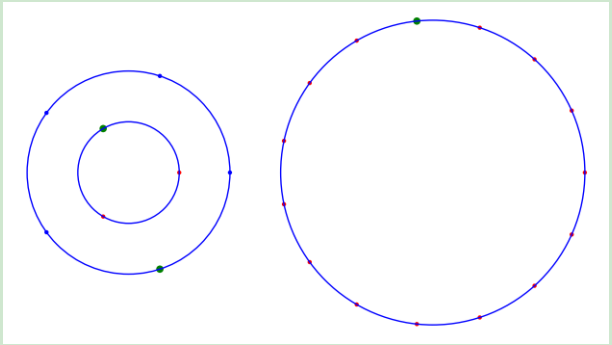
Lemma

1. *G, H groups*
2. *$g \in G$, $h \in H$, finite orders*
3. *$(g,h) \in G \times H$*
4. *Then $o((g,h)) = \mathrm{lcm}(o(r), o(s))$*

Theorem

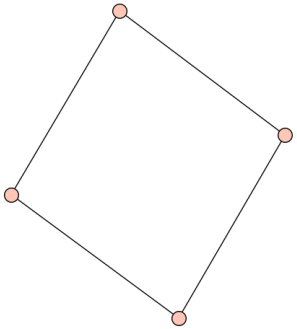
$C_{mn} \simeq C_m \times C_n$ *iff* $\gcd(m,n) = 1$

Example

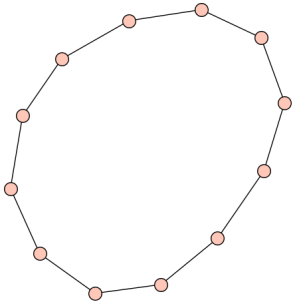
- $C_3 \times C_5 \simeq C_{15}$
- $([4]_3, [4]_5) \longleftrightarrow [4]_{15}$
- 

Cycle graphs I

- Introduced by shanks in "Solved and Unsolved Problems in Number Theory"
- Draw each cycle $1 \to g \to g^2 \to \cdots \to g^n = 1$
- Remove sub-cycles

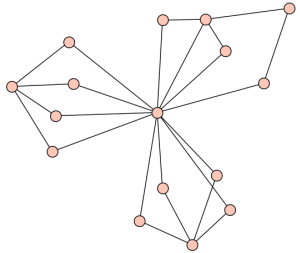


- C_4



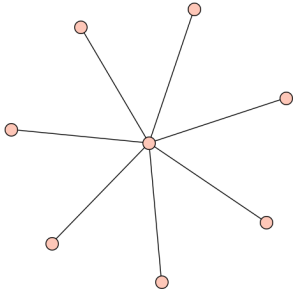
$C_4 \times C_3$

Cycle graphs II



- $C_4 \times C_4$

Cycle graphs III



- $C_2 \times C_2 \times C_2$

Theorem (Lagrange)

- G *group*
- $|G| = n < \infty$
- $g \in G$
- *Then* $o(g) | n$

Proof.

Not hard at all, but needs some machinery (cosets). □

We will prove this for the important special case $G = \mathbb{Z}_n^*$, using elementary methods.

Theorem (Euler)

If $\gcd(a,n)=1$ *then*

$$a^{\phi(n)} \equiv 1 \mod n \qquad (*)$$

Equivalently, $[a]_n^{\phi(n)} = [1]_n \in \mathbb{Z}_n^*$.

Proof.

Put $s=\phi(n)$. Let $T=\{t_1,\ldots,t_s\}$ be a choice of one elem from each class in $\mathbb{Z}_n^*$. Claim: aT also one from each. All at_i non-congruent modulo n, as before. Since $\gcd(t_i,n)=1$ and $\gcd(a,n)=1$ then $\gcd(at_i,n)=1$.

$$1*(t_1t_2\cdots t_s) \equiv (at_1)(at_2)\cdots(at_s) \equiv a^s(t_1t_2\cdots t_s) \mod n$$

Cancel $t_1t_2\cdots t_s$, you are allowed! □

Example

- $n = 8,\ T = \{1,3,5,7\},$
- $a = 5,\ aT = \{5,15,25,35\} \equiv \{5,7,1,3\} \mod 8,$
- $5t_1 * 5t_2 * 5t_3 * 5t_4 \equiv 5 * 7 * 1 * 3 \equiv 1 * 3 * 7 * 5 \equiv 1 \mod 8$
- $5t_1 * 5t_2 * 5t_3 * 5t_4 \equiv 5^4 * t_1t_2t_3t_4 \equiv 5^4 * 1 * 3 * 5 * 7 \equiv 1 * 1 \mod 8$
- $n = 3,\ T = \{1,2\},$
- $a = 2,\ aT = \{2,4\} \equiv \{2,1\} \mod 3,$
- $2t_1 * 2t_2 \equiv 2 * 1 \equiv 1 * 2 \equiv 2 \mod 3$
- $2t_1 * 2t_2 \equiv 2^2 * t_1 * t_2 \equiv 2^2 * 1 * 2 \equiv 2^2 * 2 \mod 3$

Theorem (Fermat)

Suppose p prime, $p \not| a$. Then

$$a^{p-1} \equiv 1 \mod p \qquad (**)$$

Equivalently, $[a]_p^{p-1} = [1]_p \in \mathbb{Z}_p^*$.

Proof.

$\phi(p) = p - 1$. □

Example

What is the remainder when dividing 1247^{1231} with 7?

$$\begin{aligned}
1248^{1231} &\equiv (178*7+2)^{205*6+1} \mod 7 \\
&\equiv 2^{205*6+1} \mod 7 \\
&\equiv 2^{205*6} * 2^1 \mod 7 \\
&\equiv (2^6)^{205} * 2^1 \mod 7 \\
&\equiv 1^{205} * 2^1 \mod 7 \\
&\equiv 2 \mod 7
\end{aligned}$$

Example (Repeated squaring)

What is 3^{19} modulo 23?

$$3^0 \equiv 1 \mod 23$$
$$3^1 \equiv 3 \mod 23$$
$$3^2 \equiv 3^2 \equiv 9 \mod 23$$
$$3^4 \equiv (3^2)^2 \equiv 81 \equiv 12 \mod 23$$
$$3^8 \equiv (3^4)^2 \equiv 12^2 \equiv 6 \mod 23$$
$$3^{16} \equiv (3^8)^2 \equiv 6^2 \equiv 13 \mod 23$$

so

$$3^{19} = 3^{16+2+1} = 3^{16} * 3^2 * 3^1 \equiv 13 * 9 * 3 \equiv 6 \mod 23$$

Example (Fermat)

What is 3^{19} modulo 17?

$$3^{19} = 3^{16+3} = 3^{16} * 3^3 \equiv 3^3 \equiv 10 \mod 17$$

Example (CRT)

What is $x = 3^{19}$ modulo $17 * 23 = 391$?

$$x \equiv 10 \mod 17$$
$$x \equiv 6 \mod 23$$

so

$$x \equiv 230 \mod 391$$

Definition

- R, S commutative, unitary rings
- $T = R \times S = \{ (r,s) | r \in R, s \in S \}$
- Componentwise addition and multiplication
- $R \simeq S$ iff exists bijection $F : R \to S$ which preserves multiplication and addition:
  1. $F(a+b) = F(a) + F(b)$
  2. $F(ab) = F(a)F(b)$

Theorem

1. R, S *commutative, unitary rings*
2. $T = R \times S$
3. *Then* $T^* \simeq R^* \times S^*$

Theorem

- $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ *iff* $\gcd(m,n) = 1$
- *If* $\gcd(m,n) = 1$ *then* $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

Example

- $m = 3,\ n = 4$
- $\gcd(m, n) = 1$
- $\mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$ as rings
- $\mathbb{Z}_3^* \simeq C_2$, $\mathbb{Z}_4^* \simeq C_2$
- $\mathbb{Z}_{12}^* \simeq C_2 \times C_2 \not\simeq C_4$
- Multiplication tables:

$\mathbb{Z}_3^*$

$*$	1	2
1	1	2
2	2	1

$\mathbb{Z}_4^*$

$*$	1	3
1	1	3
3	3	1

$\mathbb{Z}_{12}^*$

$*$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1