ක්වොන්ටම් පරිගණක විද්‍යාව හා ගණිතය

ටෙඕ අන්ද්‍රෝ

ජූනි 18, 2025

පටුන

රූපාවලිය

වගුවාවලිය

පරිච්ඡේදය 1

පූර්වාවශ්‍යතා

1.1 සමූහ මත වූ සාධාරණත්ව

නිර්වචනය 1

$$G \times G \to G$$
$$(a, b) \mapsto a \cdot b$$

යන ද්විමය කර්මය උපාධාර කොටගත් G කුලකයක් **සමූහයකි**. *මෙහි,*

- *$\cdot$ කර්මය සාංගමික වේ. එනම්, $\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
- *G හි අනන්‍යතා අවයවයක් පවතියි. එනම්, $\exists e \in G,\ \forall a \in G,\ e \cdot a = a \cdot e = a$.*
- *සෑම $a \in G$ සඳහාම එහි ප්‍රතිලෝම අවයවයක් පවතියි. එනම්, $\forall a \in G,\ \exists a^{-1} \in G,\ a \cdot a^{-1} = a^{-1} \cdot a = e$.*

ඉහත නිර්වචනය 1 හි දක්වා ඇති $(G, \cdot)$ හි $\cdot$ කර්මය සාංගමික හා G හි අනන්‍යතා අවයවයක් පැවත, ප්‍රතිලෝම අවයවයක් නොපවතියි නම් එය **ඒකාභයක්** ලෙස හැඳින්වේ.

උදාහරණය 1 $(\mathbb{Z}, +)$ *සමූහය. $e = 0,\ a^{-1} = -a$.*

උදාහරණය 2 $(\mathfrak{S}_3, \circ)$ *හි $\circ$ ශ්‍රිත සංයුතිය වන සමූහය. මෙහි $\mathfrak{S}_3 = \{f : \{1, 2, 3\} \to \{1, 2, 3\}$ සමක්ෂේපණය$\}$.*

නිර්වචනය 2 *$\forall a, b \in G,\ a \cdot b = b \cdot a$ වූ $(G, \cdot)$ සමූහයක්* **ඇබේලියානු** *සමූහයක් ලෙස හැඳින්වේ.*

ඉහත උදාහරණය 2 හි සමූහය ඇබේලියානු නොවේ.

නිර්වචනය 3 $(G,\cdot)$ සමූහයක් හා $x \in G$ සඳහා, x හි **ගණය** යනු $\#\{x^n \in G : n \in \mathbb{Z}\}$ වේ. මෙහි $x^n = x \cdot x \cdots x$ (n වතාවක්) ලෙස අර්ථ දක්වයි. වඩා ප්‍රත්‍යක්ෂව $\min\{k \geq 1 : x^k = e\}$ වන k හි අගය x හි ගණය වේ.

උදාහරණය 3 $(\mathbb{Z}/5\mathbb{Z},+)$ සලකන්න. මෙම සමූහය සඳහා $\mathbb{Z}$ කුලකයට "$n \sim m \leftrightarrow n-m$ 5හි ගුණාකාරයක් වේ" යන තුල්‍යතා සම්බන්ධය පනවනු ලැබේ. නිදසුනක් ලෙස $2 \sim 7 \sim 12$ වේ. එය $2 \equiv 7 \equiv 12 \pmod 5$ ලෙස ද අංකනය කළ හැක. යුක්ලිඩියානු විභාජනයෙන්, ඕනෑම $n = 5k+r$ ($n,k \in \mathbb{Z}$, $0 \leq r < 5$) ලෙස දැක්විය හැක. මෙය $\overline{n} \equiv \overline{r}$ ලෙස ද අංකනය කළ හැක. $\overline{n}$ මඟින් n හි තුල්‍යතා පන්තිය දක්වයි. මෙම අංකනය අනුගමනය කරමින්, පහත පරිදි සුළු කිරීම් සිදු කළ හැක: $\overline{2}+\overline{6} = \overline{2+6} = \overline{8} = \overline{3}$. $(\mathbb{Z}/5\mathbb{Z},\times)$ සමූහය සඳහා ද එපරිදි ම සුළු කිරීම් සිදු කළ හැක. එහිදී $\overline{2}\times\overline{3} = \overline{6} = \overline{1}$ වේ.

දැන්, $(\mathbb{Z}/5\mathbb{Z},+)$ සලකන්න. එම සමූහයේ $\overline{2}$ හි ගණය සෙවීමට පහත පියවර අනුගමනය කළ හැක:

$$\begin{aligned}
&\overline{2}^1 && && = \overline{2}\\
&\overline{2}^2 = \overline{2+2} && && = \overline{4}\\
&\overline{2}^3 = \overline{2+2+2} && = \overline{6} && = \overline{1}\\
&\overline{2}^4 = \overline{2+2+2+2} && = \overline{8} && = \overline{3}\\
&\overline{2}^5 = \overline{2+2+2+2+2} && = \overline{10} && = \overline{0}
\end{aligned}$$

එනයින්, $(\mathbb{Z}/5\mathbb{Z},+)$ සමූහයේ 2 හි ගණය 5 වේ. මෙය $\mathrm{ord}(2) = 5$ ලෙස ද අංකනය කළ හැක.

දැන් $\mathbb{Z}/5\mathbb{Z}$ පාදක කොටගෙන ගුණ්‍යත සමූහය ව්‍යුත්පන්න කිරීම සැලකූ විට අවධානය යොමු කළ යුතු කරුණක් වන්නේ එම කුලකයේ ඇත්තේ 5හි මාපාංකානුකූල ව ප්‍රතිලෝමී අවයවයන් පමණක් බවයි. එනම්, $(\mathbb{Z}/5\mathbb{Z})^\times = \{x \in \mathbb{Z}/5\mathbb{Z} : \exists y \in \mathbb{Z}/5\mathbb{Z},\ x\cdot y = 1\}$ ලෙස ගුණ්‍යත කුලකය අර්ථ දැක්වෙයි. $2 \in (\mathbb{Z}/5\mathbb{Z})^\times$ මක්නිසාදයත්, $2\cdot 3 = 6 \equiv 1 \pmod 5$.

දැන්, $((\mathbb{Z}/5\mathbb{Z})^\times,\times)$ සමූහයේ $\overline{2}$ හි ගණය සෙවීමට පහත පියවර අනුගමනය කළ හැක:

$$\begin{aligned}
&\overline{2}^1 && && = \overline{2}\\
&\overline{2}^2 = \overline{2\times 2} && && = \overline{4}\\
&\overline{2}^3 = \overline{2\times 2\times 2} && = \overline{8} && = \overline{3}\\
&\overline{2}^4 = \overline{2\times 2\times 2\times 2} && = \overline{16} && = \overline{1}
\end{aligned}$$

එනයින්, $((\mathbb{Z}/5\mathbb{Z})^\times,\times)$ සමූහයේ $\mathrm{ord}(2) = 4$. අතිරේක වශයෙන්, $((\mathbb{Z}/5\mathbb{Z})^\times,\times)$ සමූහයේ 2 ට එම සමූහය තුළ අත් කර ගත හැකි උපරිම ගණය ඇති

බැවින්, 2 එම සමූහයේ ජනකයක් ලෙස හඳුන්වා දිය හැක. මෙය පසුව අර්ථ දක්වනු ලැබේ.

ප්‍රමේයය 1 (ලග්‍රේන්ජ්) *සමූහ $(G, \cdot)$ හි $\forall x \in G$ සඳහා,* $\mathrm{ord}(x) \mid |G|$.

සාධනය. මඟහරින ලදී. □

ප්‍රමේයය 1 උපයෝගී කොටගෙන ගණ ගණනය පහසු කර ගත හැක. උදාහරණයක් ලෙස, $G = (\mathbb{Z}/15\mathbb{Z}, +)$ සමූහයේ 2 හි ගණය සඳහා $|G| = 15$හි සාධක වන $1, 3, 5, 15$ යන අගයන් පමණක් පරීක්ෂා කිරීම ප්‍රමාණවත් වේ.

උපසාධ්‍යය 1 *පූර්ණ සාධාරණත්වයෙන්, ඕනෑම $n \geq 2$ සඳහා $(\mathbb{Z}/n\mathbb{Z}, +)$ සමූහයක් වේ. මෙහි, $\mathbb{Z}/n\mathbb{Z}$ කුලකය යනු $k \sim k' \leftrightarrow k - k'$ nහි ගුණාකාරයක් වේ යන සම්බන්ධයෙන් ජනිත වූ තුල්‍යතා පන්ති කුලකය වන අතර $\overline{k} + \overline{k'} = \overline{k + k'}$ ලෙස අර්ථ දක්වෙයි.*

සාධනය. මඟහරින ලදී. □

එපරිදි ම ගුණ්‍යතා නීතියක් ද $\overline{k} \times \overline{k'} = \overline{k \times k'}$ ලෙස අර්ථ දැක්විය හැකිය.

උදාහරණය 4 *$((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$ සමූහයේ ප්‍රතිලෝමී අවයවයන් මොනවා ද? සරල නිදසුනක් ලෙස $(\mathbb{Z}/12\mathbb{Z})^{\times}$ සලකන්න. පැහැදිළිව $0 \notin (\mathbb{Z}/12\mathbb{Z})^{\times}$ මක්නිසාදයත් $\forall n \in \mathbb{Z}/12\mathbb{Z}$, $0 \times n = 0 \neq 1$. (1, $((\mathbb{Z}/12\mathbb{Z})^{\times}, \times)$ සමූහයේ අනන්‍යතා අවයවය වේ). $1 \times 1 \equiv 1 \pmod{12}$ බැවින්, 1, $(\mathbb{Z}/12\mathbb{Z})^{\times}$හි ප්‍රතිලෝමී අවයවයක් වේ. $2 * k \equiv 1 \pmod{12}$ වන පරිදි $k \in \mathbb{Z}/12\mathbb{Z}$ නොමැති බැවින් 2, $(\mathbb{Z}/12\mathbb{Z})^{\times}$ හි ප්‍රතිලෝමී අවයවයක් නොවේ. එපරිදිම $3, 4, 6, 8, 9, 10$ ද ප්‍රතිලෝමී අවයවයන් නොවන බව පෙන්විය හැක. $5 \times 5 \equiv 1 \pmod{12}$ වන බැවින් 5 ප්‍රතිලෝමී අවයවයක් වේ. එපරිදි අනෙක් ප්‍රතිලෝමී අවයවයන් $7, 11$ බව පෙන්විය හැකිය. ඉහත දී 9 ප්‍රතිලෝමී අවයවයක් නොවන්නේ $9k = 12m + 1$ වන පරිදි m, k නිඛිල දෙකක් නොපවතින බැවිනි. එසේ වන්නේ $9k - 12m = 3(3k - 4m)$ යන්න 3හි ගුණාකාරයක් වන බැවිනි. 8 හා 10 සඳහා ද ඉහත ආකාරයෙන් ප්‍රතිලෝමී නොවන බවට සාධනය කළ හැකිය.*

ප්‍රස්තුතය 1 *$\overline{k}$, $\mathbb{Z}/n\mathbb{Z}$ හි ගුණ්‍යතව ප්‍රතිලෝමී වන්නේ $\gcd(k, n) = 1$ නම් හා නම්ම පමණි.*

සාධනය.

$$\begin{aligned}
\overline{k}\ \text{ප්‍රතිලෝමී වේ} &\Leftrightarrow \exists \overline{k'},\ \overline{kk'} = \overline{1} \\
&\Leftrightarrow \exists k', m \in \mathbb{Z},\ kk' = 1 + mn \\
&\Leftrightarrow \exists k', m \in \mathbb{Z},\ kk' + (-m)n = 1 \\
&\Leftrightarrow \gcd(k, n) = 1.
\end{aligned}$$

□

ඉහත අවසාන පියවර **බේසෝ** නීතිය ලෙස ද හැඳින්වේ. RSA කේතනය ට පහත ප්‍රස්තුතය වැදගත් වේ.

ප්‍රස්තුතය 2

$$\begin{aligned}|(\mathbb{Z}/n\mathbb{Z})^{\times}| &= \#\{k : 1 \leq k \leq n,\ \gcd(k,n) = 1\} \\ &= \phi(n).\end{aligned}$$

සාධනය. සරල සාධනයකි. □
ඉහත $\phi(n)$ ශ්‍රිතය, ඔයිලර් මූළස ශ්‍රිතය ලෙස ද හැඳින්වේ.

ප්‍රමේයය 2 (චීන ශේෂ ප්‍රමේයය-විශේෂ) *$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ($p_1, \ldots, p_r$ අගයයන් ප්‍රභින්න ප්‍රථමක සංඛ්‍යා වේ) වේ නම්*

$$\mathbb{Z}/n\mathbb{Z} \overset{f}{\cong} \mathbb{Z}/p_1^{\alpha_1} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}.$$