ফাই ফাংশন ও অয়লারের উপপাদ্য
Phi Function and Euler's Theorem

মুতাসিম মিম

আগস্ট ২০১৬

১. অয়লার ফাংশন $\phi(n)$

সংজ্ঞা ১: (a, b) দ্বারা a ও b এর গ.সা.গু. বোঝানো হবে।

সংজ্ঞা ২: a ও b দুটি পূর্ণসংখ্যা হলে a ও b *সহমৌলিক* বলা হবে যদি a ও b এর মধ্যে কোন সাধারণ উৎপাদক না থাকে। যেমন: 27 ও 10 সংখ্যা দুটির মধ্যে কোন সাধারণ উৎপাদক নেই। তাই এরা সহমৌলিক। অন্যভাবে বলা যায়, $(a, b) = 1$ হলে a ও b সহমৌলিক।

সংজ্ঞা ৩: n একটি স্বাভাবিক সংখ্যা। 1 হতে n পর্যন্ত যেসব সংখ্যা n এর সাথে সহমৌলিক তাদের সংখ্যাকে $\phi(n)$ লেখা হয়। একে পড়া হয় ফাই অফ n. যেমন: 18 সংখ্যাটি দেখা যাক। 1 হতে 18 পর্যন্ত যেসব সংখ্যার সাথে 18 এর কোন সাধারণ উৎপাদক নেই সেগুলো হল, 1,5,7,11,13,17.এখানে 6 টি সংখ্যা আছে। সুতরাং $\phi(18) = 6$. আবার, 1 হতে 15 পর্যন্ত যেসব সংখ্যার সাথে 15 এর কোন সাধারণ উৎপাদক নেই সেগুলো হল 1,2,4,7,8,11,13,14. ফলে $\phi(n) = 8$.

অনুশীলন ১.১: 20 হতে 40 পর্যন্ত সবগুলো পূর্ণসংখ্যার ফাই ফাংশনের মান বের কর।

উপপাদ্য ১.১:

i) n একটি মৌলিক সংখ্যা হলে $\phi(n) = n - 1$ হবে।

ii) n এমন একটি স্বাভাবিক সংখ্যা যেন $\phi(n) = n - 1$. তাহলে n অবশ্যই মৌলিক সংখ্যা হবে।

প্রমাণ: n মৌলিক হলে 1 হতে $n-1$ পর্যন্ত সবগুলো সংখ্যাই n এর সাথে সহমৌলিক হবে।অর্থাৎ $\phi(n) = n-1$ হবে। আবার যদি n যৌগিক হয়, তাহলে 1 হতে $n-1$ পর্যন্ত অন্তত একটি সংখ্যা দ্বারা n বিভাজ্য হবে, ফলে $\phi(n) < n-1$ হবে। □

২. রিডিউসড রেসিডিউ সিস্টেম (Reduced Residue System)

একটি সেট S কে একটি Reduced Residue System$(\text{mod } m)$ বলা হবে যদি m এর সাথে সহমৌলিক যেকোন পূর্ণসংখ্যা a-এর জন্য S-এ কেবল মাত্র একটি সদস্য r থাকে যেন $a \equiv r \pmod{m}$ হয়।

$S = \{1, 3, 5, 7\}$ সেটটি দেখা যাক। S সেটটি একটি Reduced Residue System (mod 8). কারণ, ধরা যাক, পূর্ণ সংখ্যা a কে 8 দ্বারা ভাগ করলে ভাগফল q ও ভাগশেষ r হয়, অর্থাৎ, $a = 8q + r$. $0 \leq r \leq 8$. a ও 8 সহমৌলিক বলে, 8 ও r সহমৌলিক হবে। সুতরাং r হবে 1,3,5,7 এর কোন একটি। আবার, $a - r = 8q, a \equiv r \pmod 8$. অর্থাৎ a ও 8 সহ মৌলিক হলে $a \equiv 1, 3, 5, 7 \pmod 8$ এর কোন একটি হবে।

একইভাবে $T = \{-7, 3, 45, -41\}$ সেটটিও একটি Reduced Residue System (mod 8), কারণ a ও 8 সহ মৌলিক হলে $a \equiv 1, 3, 5, 7 \pmod 8$ এর কোন একটি হবে। এখন $a \equiv 1 \pmod 8$হলে, $a \equiv -7 \pmod 8$ হবে। আবার, $a \equiv 3 \pmod 8, a \equiv 5 \pmod 8, a \equiv 7 \pmod 8$ হলে যথাক্রমে $a \equiv 3 \pmod 8, a \equiv 45 \pmod 8, a \equiv -41 \pmod 8$ হবে। তাহলে দেখা যাচ্ছে 8 এর সাথে সহ মৌলিক যেকোনো a এর জন্যই T সেট এ কেবল একটি সংখ্যা r পাওয়া যাচ্ছে যেন $a \equiv r \pmod 8$ হয়। এজন্য T একটি Reduced Residue System (mod 8). লক্ষ্য কর, Reduced Residue System(mod m) এর সকল সদস্যই m এর সাথে সহমৌলিক। নিশ্চিতভাবেই বলা যায়, m একটি স্বাভাবিক সংখ্যা হলে একটি Reduced Residue System(mod m) এর সদস্য সংখ্যা হবে $\phi(m)$

সংখ্যাতত্ত্বে Reduced Residue System এর ধারণা খুবই গুরুত্বপূর্ণ। ধরা যাক, p একটা মৌলিক সংখ্যা। $S = \{1, 2, 3, \ldots, (p-1)\}$ সেটটি দেখা যাক। p দ্বারা বিভাজ্য নয় এমন যেকোনো a এর জন্য a ও p সহমৌলিক হবে। ধরা যাক,$a = pq + r$, যেখানে $0 < r < p$. $r \neq 0$, কারণ তাহলে p দ্বারা =বিভাজ্য হতো। $0 < r < p$ বা, $1 \leq r \leq p - 1$ হতে বলা যায়, r অবশ্যই S সেট এর সদস্য। $a = pq + r$ হতে বলা যায় $a \equiv r \pmod p$. তাহলে দেখা যাচ্ছে p এর সাথে সহমৌলিক যেকোনো a এর জন্য S-এ একটি সদস্য r আছে যেন $a \equiv r \pmod p$ হয়। আবার যদি কোন S এর কোন দুটি সদস্য c, d এর জন্য $a \equiv c \pmod p$, এবং $a \equiv d \pmod p$ হয়, তাহলে $c \equiv d \pmod p$ হবে, অর্থাৎ $p|c - d$ হবে। কিন্তু তা সম্ভব নয় কারণ c, d দুটির মানই p এর চেয়ে ছোট। তাহলে আমরা এই সিদ্ধান্তে আসতে পারি যে p এর সাথে সহ মৌলিক যেকোনো a এর জন্য S এ এমন কেবল একটি সংখ্যা r আছে যেন $a \equiv r \pmod p$ হয়। যার অর্থ হল S সেটটি একটি Reduced Residue System(mod p)
উপরের অনুচ্ছেদ এর সারমর্ম হল,

উপপাদ্য ২.১: যেকোনো মৌলিক সংখ্যা p এর জন্য $\{1, 2, 3, \ldots, p-1\}$ সেটটি একটি Reduced Residue System(mod p).

অনুসিদ্ধান্ত ২.১: মৌলিক সংখ্যা p এর Reduced Residue System এ $(p-1)$ টি উপাদান থাকবে।

নিশ্চিতভাবেই বলা যায়,

উপপাদ্য ২.২: m একটি স্বাভাবিক সংখ্যা হলে একটি Reduced Residue System(mod m) এর সদস্য সংখ্যা হবে $\phi(m)$.

অয়লারের উপপাদ্য প্রমাণে আরেকটি ফলাফল আমাদের দরকার হবে।

উপপাদ্য ২.৩: $\{r_1, r_2, r_3, \ldots, r_{p-1}\}$ একটি Reduced Residue System(mod p) হলে যেকোনো $(a, p) = 1$ এর জন্য ও একটি Reduced Residue System(mod p) হবে। (এখানে p কে মৌলিক হতে হবে এমন নয়)

প্রমাণ: $S = \{r_1, r_2, r_3, \ldots, r_{p-1}\}, T = \{ar_1, ar_2, ar_3, \ldots, ar_{p-1}\}$. S সেটটিতে $p-1$ সংখ্যক উপাদান আছে মধ্যে কোন দুটি উপাদান r_1, r_2 এর জন্যই $r_1 \equiv r_2 \pmod p$ নয়। T সেটেও $p-1$ সংখ্যক উপাদান আছে। এটা দেখানোই যথেষ্ট যে T এর কোন দুটি উপাদান ar_i, ar_j এর জন্যই $ar_i \equiv ar_j \pmod p$ নয়। যদি $ar_i \equiv ar_j \pmod p$ হয়, তাহলে $p|ar_i - ar_j$ বা, $p|a(r_i - r_j)$. কিন্তু a, p দ্বারা বিভাজ্য নয়। সুতরাং, $p|(r_i - r_j)$ কিন্তু তা সম্ভব

নয়। কারণ r_i, r_j দুটিই S সেট এর ভিন্ন ভিন্ন উপাদান। সুতরাং T হল একটি Reduced Residue System(mod p) □

এখন আমরা অয়লারের উপপাদ্য প্রমাণ করতে প্রস্তুত।

উপপাদ্য ২.৪ (অয়লারের উপপাদ্য)**:** a ও m দুটি সহমৌলিক পূর্ণসংখ্যা, অর্থাৎ $(a, m) = 1$. তাহলে

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

প্রমাণ: $\phi(m) = k$ ধরা যাক(লেখার সুবিধার্থে)। m এর কোন reduced residue system এ $\phi(m) = k$ সংখ্যক উপাদান থাকবে। ধরা যাক $S = \{r_1, r_2, r_3, \ldots, r_k\}$ একটি reduced residue system (mod m). যেহেতু $(a, m) = 1$, তাই আগের উপপাদ্য অনুসারে $T = \{ar_1, ar_2, ar_3, \ldots, ar_k\}$ ও একটি reduced residue system (mod m). S এর সদস্যগুলোকে m দ্বারা ভাগ করে প্রাপ্ত ভাগশেষগুলো এবং T এর সদস্যগুলোকে m দ্বারা ভাগ করে প্রাপ্ত ভাগশেষগুলো একই হবে। অর্থাৎ T এর সদস্য প্রত্যেকটি ar_i-এর জন্য S এ একটি অনন্য সদস্য r_j পাওয়া যাবে যেন $ar_i \equiv r_j \pmod{m}$ হয়। এমন সবগুলো অনুসমতা গুণ করলে পাওয়া যায়

$$\begin{aligned} & ar_1 \cdot ar_2 \cdot ar_3 \cdots ar_k \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_k \pmod{m} \\ \implies \quad & a^k(r_1 \cdot r_2 \cdot r_3 \cdots r_k) \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_k \pmod{m} \\ \implies \quad & (r_1 \cdot r_2 \cdots r_3 \cdot r_k)(a^k - 1) \equiv 0 \pmod{m} \end{aligned}$$

কিন্তু $(r_1, r_2, r_3, \cdots, r_k)$ সংখ্যাগুলোর কোনটির সাথেই aএর কোন সাধারণ উৎপাদক নেই। সুতরাং,

$$\begin{aligned} & m|(a^k - 1) \\ \implies \quad & a^k \equiv 1 \pmod{m} \\ \implies \quad & a^{\phi(m)} \equiv 1 \pmod{m} \end{aligned}$$

□

সমস্যা ১: দেওয়া আছে $\phi(40) = 16$. তাহলে 2949 কে 40 দিয়ে ভাগ করলে কত ভাগশেষ থাকে তা বের কর।

সমস্যা ২: অয়লারের উপপাদ্য ব্যাবহার করে ফার্মার উপপাদ্য প্রমাণ কর।

৩. ফাই ফাংশনের মান বের করা

ফাই ফাংশনের সংজ্ঞাটি আরেকবার উল্লেখ করা হল।

সংজ্ঞা ৪: n একটি স্বাভাবিক সংখ্যা। 1 হতে n পর্যন্ত যেসব সংখ্যা n এর সাথে সহমৌলিক তাদের সংখ্যাকে $\phi(n)$ লেখা হয়। একে পড়া হয় ফাই অফ n.

অয়লারের উপপাদ্য ব্যাবহার করার জন্য যেকোনো সংখ্যার ফাই ফাংশনের মান বের করতে পারতে হবে।

কয়েকটি ধাপে স্বাভাবিক সংখ্যা n এর জন্য $\phi(n)$ মান বের করার পদ্ধতি দেখান হল। সংজ্ঞা অনুসারে, $\phi(1) = 1$. আবার আমরা আগেই প্রমাণ করেছি মৌলিক সংখ্যা p এর জন্য $\phi(p) = p - 1$. এখন আমরা মৌলিক সংখ্যা p এর জন্য p^k এর মান বের করব।

উপপাদ্য ৩.১: p মৌলিক হলে $\phi(p^k) = p^k - p^{k-1}$

প্রমাণ: 1 হতে p^k পর্যন্ত সংখ্যাগুলোর মধ্যে কেবল p এর গুণিতকগুলোরই p^k এর সাথে সাধারণ উৎপাদক আছে। এরকম সংখ্যা গুলো হল $p, 2p, 3p, \ldots, (p^{k-1})p$, অর্থাৎ p^{k-1}টি। বাকি সংখ্যাগুলোর সাথে p^k এর কোন সাধারণ উৎপাদক নেই। বাকি সংখ্যা থাকে $p^k - p^{k-1}$টি। অর্থাৎ,

$$\phi(p^k) = p^k - p^{k-1}$$

□

উদাহরণ ১: $\phi(52) = 52 - 5 = 20.$ পরীক্ষা করে দেখ।

নিচের উপপাদ্যটির সাহায্যে একাধিক মৌলিক উৎপাদক বিশিষ্ট সংখ্যার ফাই ফাংশনের মান নির্ণয় করা যায়।

উপপাদ্য ৩.২: মনে করি, $n = a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}$, যেখানে $a_1, a_2 \ldots, a_k$ ইত্যাদি হল মৌলিক সংখ্যা। তাহলে,

$$\phi(n) = a_1^{s_1-1} a_2^{s_2-1} \cdots a_k^{s_k-1} (a_1 - 1)(a_2 - 1) \cdots (a_k - 1)$$