MODULAR ARITHMETIC

PART-01

Writer:

Ariful Islam Shanto

Software Engineering Department, SUST.

https://Shanto-swe029.github.io

mailto:ariful.shanto@gmail.com

https://facebook.com/shanto3585

বিসমিল্লাহির রাহমানির রাহিম

MODULAR ARITHMETIC

মডুলার পাটীগণিত

(প্রথম অংশ)

অনুসমতাঃ

১২ এবং ১৯ – এই দুটি সংখ্যাকে ৭ দিয়ে ভাগ করলে উভয় ক্ষেত্রেই ভাগশেষ ৫ থাকে। আবার ২২ এবং ৩১ – এই দুটি সংখ্যাকে ৯ দিয়ে ভাগ করলে উভয় ক্ষেত্রেই ভাগশেষ ৪ থাকে।

এখন আমরা যদি ভাগফলকে মাথা থেকে ঝেড়ে ফেলে দিয়ে কেবল ভাগশেষ নিয়ে কাজ করি, তাহলে ৭ দিয়ে ভাগ করার ক্ষেত্রে ১২ কে ভাগ করা যেই কথা, ১৯ কে ভাগ করাও একি কথা। কারণ দুই ক্ষেত্রেই ভাগশেষ সমান। এই লাইনটিকে মডুলার এরিদমেটিকের ভাষায় এভাবে লেখা হয় - $১২ \equiv ১৯ \pmod{৭}$। আবার ৯ দিয়ে ভাগ করার ক্ষেত্রে ২২ কে ভাগ করা যেই কথা, ৩১ কে ভাগ করাও সেই একি কথা। তাহলে এই লাইনটিকে মডুলার এরিদমেটিকের ভাষায় লেখা হবে এভাবে - $২২ \equiv ৩১ \pmod{৯}$।

তাহলে আমরা যদি একটু সাধারণভাবে যেকোনো নাম্বারের জন্য এই কথাটি বলতে চাই, তাহলে আমরা বলতে পারি যে –

a এবং b দুটি সংখ্যাকে c দিয়ে ভাগ করলে যদি একই ভাগশেষ থাকে, তাহলে মডুলার এরিদমেটিকের ভাষায় বলা যাবে : $a \equiv b \pmod{c}$.

"$a \equiv b \pmod{c}$" লেখাটিকে পড়া হয় এভাবেঃ **"a is congruent to b mod c"** এবং এখানে **c** বলা হয় **moduli** বা **divisor**, বাংলায় **উৎপাদক**। **Congruent** এর বাংলা অর্থ **অনুসমতা**।

কিছু উদাহরণঃ

(১) ঘড়িতে ১২.০০ টার পর ১.০০ টা বাজে। কারণ $১৩ \equiv ১ \pmod{১২}$ ।

(২) সপ্তাহে ৭ দিন। ৭ নম্বর দিনের পর সপ্তাহের ৮ নম্বর দিন না এসে ১ নম্বর দিন পুণরায় আসে। কারণ $৮ \equiv ১ \pmod{৭}$ ।

(৩) ১২ মাসে ১ বছর। ১২ নম্বর মাস শেষে ১৩ নম্বর মাস আসে না, আবার ১ নম্বর মাস আসে।

(৪) কোণের মান ১ ডিগ্রি, ২ ডিগ্রি, করে করে ৩৬০ ডিগ্রি পর্যন্ত হয়ে আবার ১ ডিগ্রিতেই ফিরে আসে।

এমন আর অনেক উদাহরণ তুমি নিজেই খুজে বের করতে পারবে। বাস্তব জীবনে আমরা মডুলার পাটীগণিত সম্পর্কে কোন পড়ালেখা না করেও ক্রমাগত ব্যবহার করে যাচ্ছি। মডুলার পাটীগণিতের সাহায্যে আমরা আমাদের অনেক হিসাব অনেক সহজে করে ফেলতে পারি। বিশেষ করে বড় বড় হিসাবের ক্ষেত্রে এটি প্রচুর ব্যবহৃত হয়। সেগুলো তোমরা ধীরে ধীরে দেখতে পাবে। এবার চল মডুলার পাটীগণিতের সহজ কিছু সূত্র শিখে ফেলি!

যদি $a \equiv b \pmod{c}$ হয়, তাহলে যেকোনো পূর্ণসংখ্যা k এর জন্য –

(১) $a + k \equiv b + k \pmod{c}$

(২) $a - k \equiv b - k \pmod{c}$

(৩) $ak \equiv bk \pmod{c}$

(৪) $a^k \equiv b^k \pmod{c}; k \geq 0$

(৫) $-a \equiv -b \pmod{c}$

অর্থাৎ $a \equiv b \pmod{c}$ এই অনুসমতার দুই পাশে আমরা যেকোনো পূর্ণসংখ্যা যোগ, বিয়োগ কিংবা গুণ করতে পারি। তাতে অনুসমতায় কোন ভুল হবে না। কিন্তু আমরা এভাবে সরাসরি যোগ, বিয়োগ কিংবা গুণ করতে পারলেও ভাগ করতে পারি না। ভাগ করতে হলে আমাদের কিছু

অতিরিক্ত কাজ করতে হয়। সেটি আমরা পরে দেখবো। ১, ২, ৩ ও ৫ নম্বর সূত্র তোমরা নিজেরা প্রমান করার চেষ্টা করো। আমি এখানে তোমাদের ৪ নম্বর সূত্রের প্রমাণ দেখাবো।

প্রমাণঃ

মনে করি, a কে c দিয়ে ভাগ করলে ভাগশেষ থাকে r।
তাহলে মডুলার পাটীগণিতের শর্ত অনুযায়ী, b কে c দিয়ে ভাগ করলেও ভাগশেষ r থাকবে।
এবার খেয়াল করো –

$$a \equiv r \ (mod\ c)$$
$$\therefore a \times a \times a \times \dots\dots \times a \equiv r \times r \times r \times \dots\dots \times r \ (mod\ c)$$
$$\therefore a^k \equiv r^k \ (mod\ c) \dots\dots\dots\dots\dots (i)$$

একই ভাবে দেখানো যায় যে,

$$\therefore b^k \equiv r^k \ (mod\ c) \dots\dots\dots\dots\dots (ii)$$

সুতরাং উপরের দুইটি সমীকরণের আলোকে বলা যায় -

$$\therefore a^k \equiv b^k \ (mod\ c) \quad [\text{প্রমাণিত}]$$

বাকি প্রমাণগুলোও তোমরা একইভাবে করে ফেলতে পারবে।

সূত্রগুলো বুঝতে কোন সমস্যা থাকলে নিজে নিজে কিছু উদাহরণ নিয়ে যাচাই করে দেখতে পারো। এতে করে তোমাদের কনসেপ্ট স্বচ্ছ হবে। যদি তুমি সূত্রগুলো ঠিকভাবে বুঝে থাক তাহলে পরবর্তী অংশ পড়তে পারো। নয়তো এখন রেখে দাও, পরে কোন একসময় আবার চেষ্টা করে দেখো। এরপরও যদি না বুঝো, কার সাহায্যে নিও।

আশা করি - তুমি আগের সূত্রগুলো ঠিকমতো বুঝে এই অংশ পড়া শুরু করেছো। এই অংশে আমরা আরো কিছু নতুন সূত্র নিয়ে আলোচনা করবো। চলো সূত্রগুলো দেখে ফেলা যাক।

যদি $a_1 \equiv b_1 (mod\ c)$ এবং $a_2 \equiv b_2 \ (mod\ c)$ হয়, তাহলে –

(১) $a_1 + a_2 \equiv b_1 + b_2 \ (mod\ c)$

(২) $a_1 - a_2 \equiv b_1 - b_2 \ (mod\ c)$

(৩) $a_1 \times a_2 \equiv b_1 \times b_2 \ (mod\ c)$

সূত্রগুলো নিজেরা প্রমাণ করার চেষ্টা করো। না পারলে অন্য কারো সাহায্যে নাও। কিছু উদাহরণের সাহায্যে সূত্রগুলোর সত্যতা যাচাই করে দেখো। এরপর তোমরা পরবর্তী অংশ পড়া শুরু করতে পারো।

এখন আমরা আরো তিনটি বেসিক প্রোপার্টি দেখবো। এই তিনটি প্রোপার্টি আপাতত তোমাদের কাছে ইউজলেস মনে হলেও এগুলো আমরা নিজেদের অজান্তেই অনেক বেশি ব্যবহার করবো। তাই চলো একবার দেখে নিই।

(১) $a \equiv a \ (mod\ n)$
(২) $a \equiv b \ (mod\ n)$ হলে, $b \equiv a \ (mod\ n)$
(৩) $a \equiv b \ (mod\ n)$ এবং $b \equiv c \ (mod\ n)$ হলে, $a \equiv c \ (mod\ n)$

এগুলো তুমি তোমরা জীবনে একবার দেখে নিলেই হবে। আর কোনোদিন দেখতে হবে না!

শুধু তাই নয়, এর আগের ৮টি সূত্রও তোমরা আর দেখার প্রয়োজন নেই। তুমি এমনিতেই এগুলো পারবে এখন। আরো মজার ব্যাপার হচ্ছে – এতক্ষণ পর্যন্ত আমরা যা কিছু আলোচনা করেছি তার কোনোকিছুই তোমাকে আর দ্বিতীয়বার দেখতে হবে না যদি তুমি ঠিকভাবে আমার প্রতিটি কথা অনুসরণ করে থাকো। তাহলে চলো এবার আমরা পরবর্তী অংশে যাই।

অনুসমতার ভাগঃ

আমাদের কাছে একটি অনুসমতা আছে - $16 \equiv 30 \ (mod\ 7)$

আমরা দেখতে পাচ্ছি, 16 এবং 30 দুজনকেই 2 দিয়ে ভাগ করা যায়। আমরা যদি ভাগ করে দিই, তাহলে অনুসমতাটি দাঁড়ায় - $8 \equiv 15 \ (mod\ 7)$

আমরা দেখতে পাচ্ছি, অনুসমতাটি ঠিকই আছে। আটকে সাত দিয়ে ভাগ করলে ভাগশেষ ১ থাকে, অন্যদিকে পনেরোকে সাত দিয়ে ভাগ করলেও ভাগশেষ ১ থাকে। তাহলে ভাগ করতে সমস্যা কোথায়?

চলো আরেকটি অনুসমতা নিয়ে কাজ করা যাক - $15 \equiv 25 \ (mod\ 10)$

এখানে আমরা দেখতে পাচ্ছি, 15 এবং 25 দুজনকেই 5 দিয়ে ভাগ করা যায়। আমরা যদি ভাগ করে দিই, তাহলে অনুসমতাটি দাঁড়ায় - $3 \equiv 5 \ (mod\ 10)$

এবার কি ঠিক আছে? না, ঠিক নেই। অর্থাৎ সবসময় ভাগ করলে অনুসমতা ঠিক থাকে না। ভাগ করার জন্য একটি নিয়ম মেনে ভাগ করতে হয়। নিয়ম হল – "**আমরা যেই সংখ্যা দিয়ে অনুসমতার দুই পাশে ভাগ করছি, সেই সংখ্যার সাথে মডুলির গ.সা.গু. দিয়ে মডুলি-কেও ভাগ করতে হবে**"। দ্বিতীয় উদাহরণে আমরা দুই পাশে 5 দিয়ে ভাগ করেছি। 5 এর সাথে মডুলি 10 এর গ.সা.গু. হচ্ছে 5, তাই 10 কে 5 দিয়ে ভাগ করে দিলেই অনুসমতা ঠিক থাকবে।

তাহলে অনুসমতাটি হবে - $3 \equiv 5 \ (mod\ 2)$

আমরা দেখতে পাচ্ছি এবার অনুসমতাটি ঠিক আছে!

তাহলে এখান থেকে আমরা ভাগ করার সূত্রটি লিখে ফেলতে পারি –

যদি $k \times a \equiv k \times b \ (mod\ c)$ হয়, তাহলে $a \equiv b \ (mod \frac{c}{\gcd(k,c)})$

তাহলে প্রথম উদাহরণে অনুসমতা ঠিক ছিল কেন? তুমি কি বলতে পারবে? ন এখনি না বলতে পারলে একটু সময় নাও। নিজে চিন্তা করে খুঁজে বের করার চেষ্টা করো। একেবারেই না পারলে কার সাহায্যে নাও।

এবার আমরা অনুসমতা সংক্রান্ত ২টি নতুন প্রোপার্টি শিখব যা আমাদের বাস্তব জীবনের হিসাবকে অনেক বেশি সহজ করে দেবে। চলো প্রোপার্টিগুলো দেখে নিই।

(i) যদি $a + b = c$ হয়, তাহলে $a\ (mod\ n) + b\ (mod\ n) \equiv c\ (mod\ n)$ হবে।
(ii) যদি $a \times b = c$ হয়, তাহলে $a\ (mod\ n) \times b\ (mod\ n) \equiv c\ (mod\ n)$ হবে।

এই দুটো প্রোপার্টি যে যত ভাল ব্যবহার করতে পারবে, অনুসমতার সমাধানে সে তত ফাস্ট হবে। দেখে খুব বেশি ইউজফুল মনে না হলেও, যখন প্রবলেম সলভ করবে তখন এদের কদর বুঝবে।

এখন তোমাদের কাজ হবে বিভিন্ন উদাহরণ দিয়ে উপরের প্রোপার্টি দুটি যাচাই করে দেখা। আর কেও যদি প্রমান করে ফেলতে পারো তাহলে তো আরো ভাল হয়! এবার চলো আমরা কিছু সহজ প্রবলেমের সমাধান করার চেষ্টা করি। তোমরা প্রথমে নিজে চেষ্টা করবে, পরে আমার সমাধান দেখবে। আমার সমাধানের অ্যাপ্রোচগুলো একটু ভালভাবে খেয়াল করবে। তোমরা চেষ্টা করবে আমার অ্যাপ্রোচ অনুসরণ করার। তাহলে পরবর্তীতে তোমাদের জন্য প্রবলেম সল্ভিং অনেকটাই সহজ হয়ে যাবে এবং ক্যাল্কুলেশন করতে সহজ হবে। তাহলে আর কথা না বাড়িয়ে পরবর্তী অংশে চলে যাই।

সমাধানসহ কিছু প্রবলেমঃ

(১) ঘড়িতে এখন 7.00টা বাজে। 1000 ঘণ্টা পর কয়টা বাজবে? (24 ঘণ্টা ফরম্যাট)

সমাধানঃ

যেহেতু 24 ঘণ্টা পর পর একই সময় ফিরে আসে, তাই আমরা মোট সময়কে 24 ঘণ্টা দিয়ে মড করবো।

$$\begin{aligned} \mathbf{1000} &\equiv \mathbf{16 + (24 \times 41)\ (mod\ 24)} \\ &\equiv \mathbf{16 + (0 \times 41)\ (mod\ 24)} \\ &\equiv \mathbf{16\ (mod\ 24)} \end{aligned}$$

অর্থাৎ 1000 ঘণ্টা পর ঘড়িতে সময় যত হবে, 16 ঘণ্টা পরও ঘড়িতে সেই একই সময় হবে।

$\therefore$ 1000 ঘণ্টা পর ঘড়িতে $16 + 7 = 23$টা বাজবে।

(২) $123 + 324 + 32 + 56 + 22 + 12 + 78$ কে 3 দিয়ে ভাগ করলে ভাগশেষ কত থাকবে?

সমাধানঃ

$$\begin{aligned} &\mathbf{123 + 324 + 32 + 56 + 22 + 12 + 78\ (mod\ 3)} \\ &\equiv \mathbf{0 + 0 + 2 + 2 + 1 + 0 + 0\ (mod\ 3)} \\ &\equiv \mathbf{5\ (mod\ 3)} \qquad \equiv \mathbf{2\ (mod\ 3)} \end{aligned}$$

(৩) $8 \times 16\ (mod\ 7) \equiv ?$

সমাধানঃ

$$\begin{aligned} \mathbf{8 \times 16} &\equiv \mathbf{1 \times 2}(\boldsymbol{mod}\ \mathbf{7}) \\ &\equiv \mathbf{2}\ (\boldsymbol{mod}\ \mathbf{7}) \end{aligned}$$

(৪) $3^{16}\ (mod\ 4)$ এর মান কত?

সমাধানঃ

$$3^2 \equiv 9 \equiv 1\ (mod\ 4)$$

সূচকের প্রোপার্টি ব্যবহার করে -

$$\begin{aligned} 3^{16}\ (mod\ 4) &\equiv (3^2)^8\ (mod\ 4) \\ &\equiv (1)^8\ (mod\ 4) \\ &\equiv 1(mod\ 4) \end{aligned}$$

(৫) 17^{17} এর এককের ঘরের সংখ্যা কতো?

সমাধানঃ

কোনো সংখ্যাকে ১০ দিয়ে ভাগ করলে যেই ভাগশেষ পাওয়া যায়, সেটাই তার এককের ঘরের সংখ্যা। তাহলে এখানে আমরা $17^{17}\ (mod\ 10)$ হিসাব করলেই উত্তর পেয়ে যাব।

$$\begin{aligned} 17^{17} &\equiv 7^{17} && \equiv (7^2)^8 \times 7 && (mod\ 10) \\ &\equiv (49)^8 \times 7 && \equiv (9)^8 \times 7 && (mod\ 10) \\ &\equiv (9^2)^4 \times 7 && \equiv (81)^4 \times 7 && (mod\ 10) \\ &\equiv (1)^4 \times 7 && \equiv 1 \times 7 && (mod\ 10) \\ &\equiv 7\ (mod\ 10) \end{aligned}$$

সুতরাং, 17^{17} এর এককের ঘরের সংখ্যা হল 7।

(৬) 2^{40} এর শেষ তিনটি অংক কি কি?

সমাধানঃ

কোনো সংখ্যাকে ১০ দিয়ে ভাগ করলে যেই ভাগশেষ পাওয়া যায়, সেটাই তার শেষ তিনটি অংক নির্দেশ করে। তাহলে এখানে আমরা $2^{40}\ (mod\ 1000)$ হিসাব করলেই উত্তর পেয়ে যাব।

$$2^{40} = (2^{10})^4 = 1024^4$$

$$\begin{aligned} 1024^4 &\equiv 24^4 (mod\ 1000) \\ &\equiv 576^2\ (mod\ 1000) \end{aligned}$$

এখন,

$$576^2 = (500 + 76)^2$$

$$or, 576^2 = 500^2 + 2 \times 500 \times 76 + 76^2$$
$$\therefore 576^2 = 250000 + 76000 + 5776$$

সুতরাং,

$$576^2 \ (mod\ 1000) \equiv 0 + 0 + 776 \ (mod\ 1000)$$
$$\equiv 776 \ (mod\ 1000)$$
$$\therefore 2^{40} \equiv 776 \ (mod\ 1000)$$

সুতরাং, 2^{40} এর শেষ তিনটি অংক 776.

এবার এই প্রবলেমগুলো তোমরা নিজেরা চেষ্টা করোঃ

(1) $2^{123456789} \pmod 7 \equiv ?$

(2) তাহমিদ ২১ আগস্ট, ২০২০ আমাকে তার জন্মদিনের পার্টিতে আমন্ত্রণ জানিয়েছে। পার্টিতে যাবার পর তাহমিদ আমাকে সবার সাথে পরিচয় করিয়ে দিলো। পার্টিতে উপস্থিত থাকা তাহমিদের ছোট ভাই তামজিদ আমাকে জিজ্ঞেস করলো – "ভাইয়া, আজ তো শুক্রবার এবং আজ তাহমিদ ভাইয়ার ২০তম জন্মদিন। তুমি কি বলতে পারবে তাহমিদ ভাইয়া কি বারে জন্মগ্রহন করেছিলো?" আমি বললাম –"হ্যাঁ, পারবো!" এরপর আমি কিছুক্ষণ হিসাব করে তাহমিদের জন্মবার বলে দিলাম। তুমি কি বলতে পারবে তাহমিদ কি বার জন্মগ্রহণ করেছিলো? অবশ্যই ক্যালেন্ডার না দেখে!

(3) $6^{6^{6^{6^{6}}}}$ কে দিয়ে 7 ভাগ করলে ভাগশেষ কতো হবে?

(4) $1! + 2! + 3! + \ldots\ldots\ldots + 50!$ কে $5!$ দিয়ে ভাগ করলে ভাগশেষ কতো হবে?

(5) $1111111\ldots\ldots\ldots 1 \ (mod\ 271) \equiv ?$

(6) $1 \times 10^1 + 2 \times 10^2 + 3 \times 10^3 + \ldots\ldots\ldots + 2015 \times 10^{2015}$ কে 11 দিয়ে ভাগ করলে ভাগশেষ কতো হবে?

(7) তাহমিদ 2015 কে ক্রমাগত $1, 2, 3, 4, \ldots\ldots\ldots 1000$ দিয়ে ভাগ করে যাচ্ছে এবং প্রতি ক্ষেত্রে ভাগশেষগুলোকে খাতায় লিখে রাখছে। তাহমিদ যেই ভাগশেষগুলো লিখেছে তাদের মধ্যে সবথেকে বড় ভাগশেষটি কতো?

~~~ সমাপ্ত ~~~
~~~