Chinese Remainder Theorem

Chinese Remainder Theorem একটা খুবই interesting theorem. প্রথমে বলি এটা কোন কোন প্রবলেমগুলার সাথে deal করতে পারে। এটা জানলেই বুঝবে কেন এটাকে এতটা interesting বলতেছি। আগেই বলে রাখি, এই থিওরেমটি শিখতে এবং প্রোগ্রামে কোড করতে হলে অবশ্যই **Modular Multiplicative Inverse** কিভাবে Extended Euclid Method এর সাহায্যে বের করতে হবে সেটা জেনে রাখা দরকার(এজন্য এই লিংকে চলে যাও)। যদিও খাতা-কলমে কিভাবে Modular Multiplicative Inverse বের করা যায় সেটা শেখাবো এখানে। তারপরও কোড করার জন্য ইউক্লিডের মেথডটা শিখে রাখার জন্য বলবো সবাইকে।

এখন আমরা জানি যে: **5 (mod 8) ≡ 5** আবার **13 (mod 8) ≡ 5, 21 (mod 8) ≡ 5**. এখন যদি তোমাকে একটা শর্ত দিয়ে দেয়া হয় যে **z (mod 3) ≡ 2** হতে হবে। এখানে **z = {5, 13, 21}**, তাইলে শর্তটা দেখা যাচ্ছে মোটামুটি **5** এর জন্য সত্য তবে **13** এবং **21** এর জন্য সত্য হচ্ছে না। অর্থাৎ এখানে একমাত্র **5** ই সঠিক মান যেটা সকল শর্ত পুরন করতেছে। এই ধরনের সমস্যার সমাধান Chinese Reminder Theorem দিতে পারে। অর্থাৎ একাধিক modular condition থাকবে যেটা থেকে এমন সব সঠিক মান বের করতে হবে যা সকল দেয়া শর্ত মেনে চলবে। অবশ্য এক্ষেত্রে উত্তর অসীম সংখ্যক হইতে পারে। সেগুলাও বের করার উপায়ও এই থিওরেমটি দিয়ে দেয়।

এখন কাজে আসি, একটা উদাহরন সমাধান করার মাধ্যমে থিওরেমটা শেখার চেষ্টা করি। কিছু শর্ত আছে ধরে নিলাম:

Z = 4 (mod 5)

Z = 6 (mod 7)

Z = 3 (mod 11)

এই শর্তগুলা সিদ্ধ করে এমন সব **Z** এর মান আমাদের বের করতে হবে। তো প্রথমে বলে রাখি এখানে রিমাইন্ডারগুলা হবে b_i এর মান। অর্থাৎ, **b = {5, 7, 11}** এবং c_i হবে প্রাপ্তমানগুলা অর্থাৎ **c = {4, 6, 3}**. প্রথমে যেটা করতে হবে সেটা হলো **B (big B)** এর মান বের করা। এটার সূত্র হলো:

$$B = b_1 \times b_2 \times b_3 \times \dots \times b_n$$

যার মানে হলো সকল b_i এর গুণফলগুলা হলো **B (big B)** এর মান। এক্ষেত্রে,

B = 5x7x11 = 385

এবার আমাদের কাজ হলো B_i এর মান বের করা। এটার সূত্র হলো:

$$B_i = B \div b_i$$

অর্থাৎ,

$$B_1 = 385/5 = 77$$

$$B_2 = 385/7 = 55$$

$$B_3 = 385/11 = 35$$

চায়নিজ রিমাইন্ডার থিওরেম থেকে Z এর মান বের করার সূত্রটা হলো:

$$Z = B_1X_1c_1 + B_2X_2c_2 + B_3X_3c_3 + \dots + B_nX_nc_n$$

এই উদাহরনটার ক্ষেত্রে:

$$Z = B_1X_1c_1 + B_2X_2c_2 + B_3X_3c_3$$

এখানে আমাদের B_i এবং c_i এর মান আগে থেকেই জানা। তবে এখানে X_i টা আবার কি জিনিস?? হুম, এই কাজেই আমাদের লাগবে Extended Euclid. এটা শেখার জন্য লিংকে যাও (যদিও লেখার শুরুতে একবার দিয়েছি লিংকটা)। এখানে আমরা B_i এবং b_i এর modular multiplicative inverse বের করবো। এ দুইটা মানের উপর Extended Euclid চালালে আমরা যে **X** এর মানটা পাই সেটাই এখানে X_i এর

মান।

এখন

$B_1X_1 \equiv 1 \pmod{b_1}$

$\Rightarrow 77\ X_1 \equiv 1 \pmod 5$

$\Rightarrow (77-80)\ X_1 \equiv 1 \pmod 5$ **[5 এর গুণিতক দ্বারা 77 কে বিয়োগ করে একটু ছোট করে নিলাম]**

$\Rightarrow (-3)\ X_1 \equiv 1 \pmod 5$

$\Rightarrow (-3)\ X_1 \equiv 6 \pmod 5$ **[$1 \pmod 5 \equiv 6 \pmod 5$]**

সুতরাং, **$X_1 = -2$**

আবার,

$B_2\ X_2 \equiv 1 \pmod{b_2}$

$\Rightarrow 55\ X_2 \equiv 1 \pmod 7$

$\Rightarrow (55-56)\ X_2 \equiv 1 \pmod 7$ **[55 থেকে 7 এর গুণিতক বিয়োগ করে]**

$\Rightarrow (-1)\ X_2 \equiv 1 \pmod 7$

সুতরাং, **$X_2 = -1$**

এভাবেই, **$35\ X_3 \equiv 1 \pmod{11}$ থেকে পাই, $X_3 = -5$. X** এর মানগুলার অনেক হতে পারে, তবে **Extended Euclid Method** ব্যবহার করলে এই মানগুলাই পাওয়া যায়।

এখন Chinese Reminder Theorem এর আসল সূত্রটাতে আসি:

$Z = B_1X_1c_1 + B_2X_2c_2 + B_3X_3c_3$

$\Rightarrow Z = 77 \times (-2) \times 4 + 55 \times (-1) \times 6 + 35 \times (-5) \times 11 = -1471$

যে মানটা পাইলাম সেটা দিয়ে দেয়া শর্তগুলার সবকয়টি সিদ্ধ হবে। সুতরাং এটা একটা উত্তর। তবে আমি আগেই বলেছি অসীম সংখ্যক উত্তর থাকবে এই সমস্যাটার জন্য। তাইলে আমরা সেগুলা কিভাবে বের করবো? খুবই simple, প্রাপ্ত **B (big B)** এর মানের যেকোনো গুণিতক দিয়ে **Z** এর প্রাপ্ত মানের সাথে যোগ অথবা বিয়োগ দিলেই হয়ে গেলো। অর্থাৎ **(4×385 – (-1471)) = 69**, এটাও একটি সঠিক মান। এভাবে তুমি যেকোনো লিমিটের জন্য একটা সাম্ভাব্য মান খুজে পেতে পারবে। এখন নিচের উদাহরনটি সমাধান করার ট্রাই করো:

$Z = 3 \pmod 8$

$Z = 1 \pmod 9$

$Z = 4 \pmod{11}$

Keep coding…