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। :)

Search

Archives

- October 2013
- July 2013
- December 2012
- May 2012

Recent Posts

- বিন্যাস করা যাক (পর্ব: ২)
- বিন্যাস করা যাক (পর্ব: ১)
- Chinese Remainder Theorem
- খাতা-কলমে Extended Euclid Method
- Extended Euclidean Algorithm এবং একটুখানি Modular Multiplicative Inverse

Recent Comments

- ops on বিন্যাস করা যাক (পর্ব: ১)

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

$Z = 4 \pmod 5$

$Z = 6 \pmod 7$

$Z = 3 \pmod{11}$

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 সুত্র হলো:

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

$B = 5 \times 7 \times 11 = 385$

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:

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

- Muhammad Minhazul Haque on বিন্যাস করা যাক (পর্ব: ২)
- Duronto Habib on বিন্যাস করা যাক (পর্ব: ১)
- Abu Asif Khan Chowdhury on Chinese Remainder Theorem
- TripleM Zim on Chinese Remainder Theorem

Blog Traffic

Pages

Pages | Hits | Unique

- Last 24 hours: 16
- Last 7 days: 463
- Last 30 days: 841
- Online now: 2

Get Updates

Join 3 other subscribers

Email Address

Subscribe

Meta

- Log in
- Entries RSS

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

$B_1X_1 \equiv 1 \pmod{b_1}$

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

$\Rightarrow (77-80)\ X_1 \equiv 1 \pmod{5}$ **[4 এর গুণিতক দ্বারা 5 কে বিয়োগ করে]**

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

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

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]**

- Comments RSS
- WordPress.org

=> (-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:

$Z = B_1X_1c_1 + B_2X_2c_2 + B_3X_3c_3$

=> Z = 77x(-2)x4 + 55x(-1)x6 + 35x(-5)x11 = -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 (mod 8)

Z = 1 (mod 9)

Z = 4 (mod 11)

Keep coding… :)

Share this:

Chinese Remainder Theorem , *Extended Euclid* , *Modular Multiplicative Inverse*

খাতা-কলমে Extended Euclid Method

বিন্যাস করা যাক (পর্ব: ১)

TripleM Zim

B1X1 ≡ 1 (mod b1)

এই লাইন কিভাবে হলো বুঝতেছিনা...

http://abuasifkhan.blogspot.com/ Abu Asif Khan Chowdhury

B1 modulo b1 এর মাল্টিপ্লিকেটিভ ইনভার্স হলো X1. এটাকে আসলে এমনভাবে লেখা হয়,

B1^-1 ≡ X1 (mod b1)

আমি সেখান থেকে সমাধানের সুবিধার্থে এমন ভাবে লিখেছি,

B1X1 ≡ 1 (mod b1)

উইকিতে এই আর্টিকেলটার Example Section টা দেখে নিতে পারো।

http://en.wikipedia.org/wiki/Modular_multiplicative_inverse

TripleM Zim

আসলে এই লাইন এর মানে বুঝছি... Bi এবং ci এর modular multiplicative inverse বের করতে হলে এদের গ।সা।গু ১ হতে হবে সেক্ষেত্রে আমরা extended euclid চালিয়ে (Bi আর Ci এর ওপরে)এদের modular multiplicative inverse বের করতে পারব... কিন্তু Bi , ci এরা যে সহমৌলিক তার প্রমাণ কি? আর modular multiplicative inverse বের করলাম Bi , ci এর সেক্ষেত্রে এই লাইনটা (B1X1 ≡ 1 (mod b1)) true হল কিভাবে এইটা বুঝিনি...

Thanks in advance....

http://abuasifkhan.blogspot.com/ Abu Asif Khan Chowdhury

প্রশ্নটা আসলে আমি খুব ভালো বুঝতে পেরেছি কিনা বলতে পারছি না তবে আমরা চাচ্ছি Xi এর মান বের করতে, যেটা Bi এবং bi (Ci নয়) এর মডুলার মাল্টিপ্লিকেটিভ ইনভার্স। তুমি বলতে চাচ্ছো GCD(Bi, bi) = 1 হবে, অর্থাৎ কো-প্রাইম হতে হবে। কিন্তু সেটা তো নাও হতে পারে, তাইতো? আসলে যদি তুমি ইউক্লিড পদ্ধতিতে Bi, bi যদি কো প্রাইম না নিয়েও করো তাইলে দেখতে পাবে যে এদের সকল গুননিয়ক এই পদ্ধতিতে বাদ চলে যেয়ে সব থেকে বড় গুণনিয়কটা থাকে। এবং সেটার জন্য gcd এর মান ১ হয়ে যায়। মানে বলতে চাচ্ছি যে Bi, bi কো-প্রাইম হতে হবে এমন কোনো বাধ্যবাধকতা নাই। এই পদ্ধতিতে তাদের সকল ছোট গুননিয়কগুলা বাদ চলে যেয়ে কেবল বড়টাই রেখে দেয়া হয়। গুণনিয়কগুলা বাদ যাওয়ার আগে gcd এর মানে ওই গুণনিয়কগুলার গুণফলের সমান থাকে।

TOP

আসিফের হ-য-ব-র-ল