Modular Arithmetic:

গোড়ার কথাঃ

ধর, তুমি তোমার এক বন্ধুকে জিজ্ঞেস করলে, ' কয়টা বাজে?'
তোমার বন্ধু তোমাকে বলল, " 453 কোটি 14 লক্ষ 84 হাজার 378 ঘণ্টা" কেমন লাগবে তখন?
পৃথিবীর শুরুর দিন থেকে হিসাব করে আসলে হয়ত এরকম করেই সময় হিসেব করতে হত আমাদের। কিন্তু আমরা সৌভাগ্যবান যে এভাবে আমাদের সময় হিসেব করতে হয়না।
তো চল, এবার সেই মজার বিষয়টার গল্প বলি যেটার কারণে এই বাড়তি কষ্টটা করতে হচ্ছে না। এর জন্য একটু কষ্ট করতে হবে।
তোমার বাসার দেয়াল ঘড়িটার দিকে তাকাও। একবার চিন্তা করে দেখ, প্রতি 12 ঘণ্টা পর পর তুমি কি করছ? হ্যাঁ, ঠিক ধরেছ। আবার একই জায়গায় ফিরে আসছ। 11:59 বাজার পর ই তুমি তাকে ফিরিয়ে নিয়ে আবার 00:00 করে দিচ্ছ। একটা অদৃশ্য চক্রের মত।
অনেকটা এরকম চিন্তা থেকেই গণিতের রাজপুত্র গাউস নাম্বার থিওরিতে কনগ্রুয়েন্স এর ধারণা দেন।
কনগ্রুয়েন্স বা মডুলার এরিথমেটিক বা অনুসমতা হল নাম্বার থিওরির সবচাইতে চমৎকার বিষয়গুলোর একটি। কাঠখোট্টা নাম হলেও একেবারেই সহজ এই বিষয়টা। শুধু গুণ-ভাগের ধারণা থাকলেই যে কাউকে এর বেসিকটা বুঝিয়ে ফেলা যায়। কিন্তু সহজ হলেও এর গুরুত্ব অনেক। বিশেষ করে, অনেক কঠিন একটা হিসেব যেটা সাধারণভাবে করতে গেলে হয়ত তোমাকে সুপার কম্পিউটারের সাহায্য নিতে হবে সেটা তুমি এই অনুসমতার ধারণা ব্যবহার করে খুবই সহজে করে ফেলতে পারবে।
এবার আরেকটু চিন্তা কর। তোমাকে আমি বললাম 20 কে 6 দিয়ে ভাগ করতে। তুমি বললে, ভাগফল 3 আর ভাগশেষ 2, এই ভাগশেষেই সব কাহিনী আসলে। সবখানে ভাগফল কাজে লাগে আর এখানে ভাগশেষ! একদমই উল্টো অবস্থা। এটাই সবচাইতে আকর্ষণীয় ব্যপার। কনগ্রুয়েন্সের ক্ষেত্রে একটা বিষয় তোমাকে মনে রাখতে হবে, যে এখানে ভাগফল নিয়ে মাথাব্যথার কিছু নাই। যত মাথাব্যথা সব হল ভাগশেষ নিয়ে।
তো যেটা বলছিলাম, 20 কে 6 দিয়ে ভাগ করলে ভাগশেষ 2, আবার 26 কে 6 দিয়ে ভাগ করলেও ভাগশেষ 2! আগেই বলেছি আমাদের যত মাথাব্যথা সব ভাগশেষ নিয়ে। এখন 20 আর 26 এর ভাগশেষ যখন একই তখন এদের একটা ফ্যামিলি বানিয়ে ফেলা যাক! এখন থেকে এরা 2 জন হচ্ছে একে অপরের ভাইভাই। শর্ত একটাই, এদের ভাজকটা একই হতে হবে। মানে এরা ততক্ষণই ভাই-ভাই যতক্ষন এদের 6 দিয়ে ভাগ দেয়া হচ্ছে। শুধু এরাই না, কোন সংখ্যা দিয়ে ভাগ করলে ভাগশেষ একই হয় এরকম যত সংখ্যা আছে দুনিয়ায়, তাদের সবাই একে অপরের ভাইভাই। এই ভাতৃত্বের নামই হল অনুসমতা বা কনগ্রুয়েন্স। আর এরা 2 জন একে অপরের ভাই, মানে হল একে অপরের অনুসম বা কনগ্রুয়েন্ট।

এবার আনুষ্ঠানিক সংজ্ঞায় আসা যাক।

মনে কর, a আর b দু' টো সংখ্যা যাদেরকে আরেকটা সংখ্যা m দিয়ে ভাগ করা হলে ভাগশেষ একই হয়। যেমন আগের উদাহরণের 20 আর 26, দুইটাকেই 6 দিয়ে ভাগ করলে ভাগশেষ একই। তাহলে এই কথাটাকে এত বড় করে না বলে একটা ছোট্ট ইকুয়েশন দিয়ে লেখার একটা নিয়ম আছে। তো, ইকুয়েশনটা দেখতে এরকম,

$a \equiv b \pmod{m}$

অ্যাঁ! ! এইটা আবার কিরকম ইকুয়েশন? পাশে আবার ব্র্যাকেটে কি লেখা??

এটা পড়তে হয় এভাবে, " **a is equivalent to b, modulo m**" । অর্থাৎ, a আর b ভাই-ভাই (মানে অনুসম বা কনগ্রুয়েন্ট) , সবসময় না। তখন, যখন এদের m দিয়ে ভাগ দেয়া হচ্ছে ।
মানে ব্যাপারটা এমন যে আমরা পুরোপুরি আলাদা একটা দুনিয়া বানিয়ে ফেললাম, যেখানে congruent হওয়াটাই আমাদের কাছে গুরুত্বপূর্ণ, equal হওয়াটা না।
এতক্ষণ তো 20 আর 26 এর উদাহরণ দেখানো ছিল। ধর, দুইটা সংখ্যা 20 আর 10026। দুইটা সংখ্যার মধ্যে যত বিশাল পার্থক্যই থাকুক না কেন, এদেরকে 6 দিয়ে ভাগ করলে ভাগশেষ থাকে একই, 2। তাই modulo 6 জগতে এরা congruent. ব্যাপারটা এভাবে বলা যায়,

$20 \equiv 2 \pmod{6}$

$10026 \equiv 2 \pmod{6}$

এবং $10026 \equiv 20 \pmod 6$

এবার এখান থেকে আরেকটা জিনিস দেখা যাক। ধরি,

$a \equiv b \pmod m$

তাহলে। m দিয়ে ভাগ করলে a ও b এর ভাগশেষ একই। ধরি এই ভাগশেষ d। তাহলে একটা জিনিস সম্বন্ধে নিশ্চিত হয়ে নাও। a ও b, উভয়কেই লিখা যাবে $mk + d$ এই আকৃতির কোন সংখ্যা হিসেবে। আবার যদি আগের mod 6 এর উদাহরণে যাই তাহলে যেমন

$20 = 6 \times 3 + 2$

$10036 = 6 \times 1672 + 2$

তাহলে ধরি,
$a = mk+d$
$b = mj+d$
তাহলে $a-b = m(k-j)$ । তাহলে এবার ভাবো, (a-b) কে m দিয়ে ভাগ করলে ভাগশেষ কত? শূন্য।
তাহলে এটা লেখা যায় যে,

$a-b \equiv 0 \pmod m$

কারণ স্বভাবতই 0 কে যেকোন সংখ্যা দিয়েই ভাগ করলে ভাগফল-ভাগশেষ সবই তো 0 আসবে।
এই লাইনটা আবার নতুন করে একটু খেয়াল কর। কারণ এখান থেকে আমরা congruence এর আরেকটা সংজ্ঞা পাব। এখান থেকে আমরা বলতে পারি যদি (a-b), m দিয়ে বিভাজ্য হয় তাহলেও বলা যায় $a \equiv b \pmod m$।

$a \equiv b \pmod m$ এবং $m|(a-b)$ কথা দুইটি সমতুল্য ।

এবার আমাদের সেই ঘড়ির উদাহরণে ফিরে আসি। আর কনগ্রুয়েন্সের ইকুয়েশন যেহেতু শিখেই গেছ তাহলে ঘড়ির সময় দেখার ব্যাপারটাকে ইকুয়েশন দিয়ে লেখার চেষ্টা করি। এবার অবশ্য তোমাকে ঘড়ি হাতে না নিলেও চলবে! :P যেহেতু আমরা 12 ঘন্টা পর পর আবার আগের হিসেবে ফিরে যাই, তাই আমরা ভাগও করব 12 দিয়ে। অর্থাৎ এই ক্ষেত্রে আমাদের সেই শর্ত হল 12!

তাহলে যখন রাত 00:00 বাজে, তখনকার জন্য, $00 \equiv 0 \pmod{12}$
কারণ শূন্যকে 12 দিয়ে ভাগ করলে ভাগশেষ থাকে শূন্য! :)
রাত 3টার জন্য, $03 \equiv 3 \pmod{12}$ [এখানেও একই ঘটনা]
বেলা 11টার জন্য $11 \equiv 11 \pmod{12}$ [একই ঘটনা]
কিন্তু বেলা 12টার জন্য $12 \equiv 0 \pmod{12}$
কারণ 12 কে 12 দিয়ে ভাগ করলে ভাগশেষ হল শূন্য।
এবার আবার বেলা 13টার জন্য $13 \equiv 1 \pmod{12}$
অর্থাৎ যেই 13টা বাজছে সেই আমরা একে 13 থেকে আবার 1 বানিয়ে দিচ্ছি।

এটাই হল কনগ্রুয়েন্সের মজা! একটু গুণ- ভাগ কাজে লাগিয়ে কত সহজে হিসেব করে ফেলা যায়! এই পর্যন্ত ছিল একেবারে প্রাথমিক কিছু ধারণা! এবার কনগ্রুয়েন্স এর কিছু বৈশিষ্ট্য জানা দরকার। তবে এ পর্যন্ত যা জানলে সেটা দিয়ে নিচের এই প্রশ্নগুলোর উত্তর দেয়ার চেষ্টা করতো!

1) $20 \equiv 26 \pmod 6$ হলে $26 \equiv ? \pmod 6$ এখানে '?' চিহ্নিত অংশে সংখ্যা বসাও।

2) $20 \equiv 2 \pmod 6$ হলে $25 \equiv ? \pmod 6$ এখানে '?' চিহ্নিত অংশে সংখ্যা বসাও।

এই প্রশ্নগুলোর প্রত্যেকটার অনেকগুলো করে উত্তর হতে পারে। উত্তরগুলো একেবারে নেগেটিভ ইনফিনিটি থেকে শুরু করে পজিটিভ ইনফিনিটি পর্যন্ত হতে পারে। কিন্তু সবগুলো প্রশ্নেরই একটা সবচাইতে সহজ উত্তর আসলে প্রশ্নটাতেই বলে দেয়া আছে। বলতে পারবে সেটা?
হ্যাঁ! অবশ্যই পারবে। কিন্তু সেজন্য মডুলার অ্যারিথমেটিক বা কনগ্রুয়েন্স এর বেসিক কিছু বৈশিষ্ট্য জানতে হবে।

মডুলার পাটিগণিতের প্রাথমিক ধর্মঃ

1. একেবারে প্রথম প্রশ্নটার দিকে তাকাও। কনগ্রুয়েন্স এর যে বৈশিষ্ট্যের কারণে আমি এই প্রশ্নটার সবচাইতে সহজ উত্তরটা দেখেই বলে দিতে পারি সেটাই প্রথমে বলি। $a \equiv b \pmod m$ হলে এর ভাইস-ভার্সাটাও সত্য। মানে হল,

$a \equiv b \pmod m$ হলে $b \equiv a \pmod m$

একেবারে উদাহরণ দিয়েই দেখে ফেলি।
$20 \equiv 26 \pmod 6$ হলে $26 \equiv 20 \pmod 6$ হবে।
আরে! এটা তো সেই 1 নম্বর প্রশ্নটার উত্তর হয়ে গেল! হ্যাঁ, ঠিকই ধরেছ। বলেছিলাম না, এর সবচাইতে সহজ উত্তরটা প্রশ্নেই দেয়া আছে?

2. যদি $a \equiv b \pmod m$ আর $b \equiv c \pmod m$ হয়, তাহলে $a \equiv c \pmod m$ হবে

$26 \equiv 20 \pmod 6$ এবং $20 \equiv 2 \pmod 6$ হলে $26 \equiv 2 \pmod 6$ সত্য হচ্ছে ।
উপরের সম্পর্ক দেখে আমরা বলতে পারি mod m এর জগতে a,b,c ভাই ভাই !

3. যদি $a \equiv b \pmod m$ হয়, তখন $a \pm c \equiv b \pm c \pmod m$ হবে।

$a \equiv b \pmod m$ হলে লেখা যায়, $m|(a-b)$।
এখন, $a - b = (a \pm c) - (b \pm c)$।
তাহলে $m|((a \pm c) - (b \pm c))$।
অতএব বলে ফেলে যায় , $a \pm c \equiv b \pm c \pmod m$

4.যদি $a \equiv b \pmod m$ হয়, তখন $a \equiv b \pm mk \pmod m$ হবে।

যেহেতু $a \equiv b \pmod m$। তাহলে $m|(a-b)$, তাহলে $m|[a-(b \pm mk)]$, যেকোন পূর্ণ সংখ্যা k এর জন্য। অর্থাৎ, $a \equiv b \pm mk \pmod m$.

5. যোগ-বিয়োগ তো গেল! এবার আসি গুনের কথাতে। এখানে অবশ্য নতুন করে বলার কিছুই নেই। কারণ যোগ-বিয়োগের এর ক্ষেত্রে আমরা যেমন মডুলো কে একইরকম রেখে ডানপক্ষ আর বামপক্ষে একই জিনিস যোগ বা বিয়োগ করতে পারি, তেমনি একই জিনিস গুণও করতে পারি। মানে হল,

যদি, $a \equiv b \pmod m$ হয়, তাহলে $ac \equiv bc \pmod m$ হবে।

এখানে একটা কথা বলে রাখা ভালো, যোগ আর গুণের মধ্যে কিন্তু মূলত কোন পার্থক্য নাই। কোন সংখ্যাকে c দিয়ে গুণ করা আর সংখ্যাটিকে c বার যোগ করা একই ব্যাপার। যোগের ক্ষেত্রে যেহেতু এরকম সম্পর্ক খাটে গুণের ক্ষেত্রে খাটতে দোষ কি?
এখানে আরেকটা জিনিস বলে রাখি। $a \equiv b \pmod m$ হলে তো মডুলো m এ a ও b অনুসম। তার মানে দুইদিকে একই জিনিস দিয়ে গুণ করতে গিয়ে আমরা একদিকে a আরেকদিকে b গুণ করতে পারি একই ভাবে। তাহলে কি দাঁড়ায়?
$a^2 \equiv b^2 \pmod m$
একই কাজ আবার কর। আসবে $a^3 \equiv b^3 \pmod m$
এভাবে বারবার গুণ করতে থাকলে যেকোন ঘাত পর্যন্তই যাওয়া সম্ভব। তো আমরা আরকটা বৈশিষ্ট্য পেলাম,

6.যদি, $a \equiv b \pmod m$ হয় তাহলে $a^n \equiv b^n \pmod m$

7. $a \equiv b \pmod m$ এবং $c \equiv d \pmod m$ হলে , $a+c \equiv b+d \pmod m$ হবে

a≡b(mod m) এবং c≡d(mod m) হওয়ায় এমন দুটি পূর্ণসংখ্যা k,l আছে যেন a=b+mk এবং c=d+ml হয় (উপরে 4নং দেখো) । তাহলে a+c=b+d+m(k+l)

অতএব, a+c≡b+d(mod m)

8. a≡b(mod m) এবং c≡d(mod m) হলে , ac≡bd(mod m) হবে

এটার প্রমাণ নিজেরাই করে ফেলো !

9. a≡b(mod m) হলে a≡b(mod d) হবে যেখানে d হল m এর ধনাত্মক উৎপাদক ।

20≡1(mod 10) । এখন যেহেতু 5 ,10 এর উৎপাদক অতএব 20≡1(mod 5) সত্য হচ্ছে ! এটার প্রমাণ তোমরা নিজেরা চেষ্টা করলে করে ফেলতে পারবে । তাই আর দেয়া হল না ।

10. a,b,m এর সাধারণ উৎপাদক c হলে a≡b (mod m) হবে যদি ও কেবল যদি a/c ≡ b/c (mod m/c) হয়।

এটার প্রমান নিজেই করার চেষ্টা কর।

11.যদি ca≡cb (mod m) হয় তবে a≡b (mod m/gcd(m,c)) হবে. আরো বলা যায়, যদি c,m সহমৌলিক হয় তবে ca≡cb (mod m) হলে a≡b (mod m) হবে।

প্রমাণঃ
এখানে ca≡cb (mod m) অর্থাৎ c(a-b)=km , যেখানে k একটি পূর্ণসংখ্যা।
ধরি , d=gcd(c,m) । তাহলে, (a-b) c/d=km/d ।
এখানে m/d দ্বারা ডানপক্ষ বিভাজ্য তাই বলা যায় এটি বামপক্ষ কেও নিঃশেষে ভাগ করে।
আবার c/d ও m/d সহমৌলিক ।
অতএব (m/d) |(a-b) অর্থাৎ a ≡ b (mod m)

উদাহরণ ১ : প্রমাণ কর যে, যদি 2x+3y, 17 দ্বারা বিভাজ্য হয় তবে 9x+5y ও 17 দ্বারা বিভাজ্য হবে ।
প্রশ্নমতে, 2x+3y ≡ 0 (mod 17)
বা, 13(2x+3y) ≡ 0 (mod 17)
বা, 26x+39y≡ 0 (mod 17)
বা, 26x+39y-17(x+2y) ≡ 0 (mod 17)
বা, 9x+5y≡ 0 (mod 17)

আরও কিছু বৈশিষ্ট্যঃ

এতক্ষণ ধরে যে আমরা মডুলার অ্যারিথমেটিক নিয়ে কথা বলছি, বলছি এটা নাকি সাধারণ যোগ-বিয়োগের মতই সাধারণ গণিতে পূর্ণ সংখ্যা হতে পারে ধনাত্মক বা ঋণাত্মক। আমরা এখন পর্যন্ত ঋনাত্মক সংখ্যাকে সযত্নে এড়িয়ে গেছি। এড়িয়ে যাওয়ার মত আসলে কিছু নেই। ঋনাত্মক সংখ্যার আচরণে কোনই পার্থক্য নেই। এখন তুমি জিজ্ঞেস করতে পারো a ≡ b (mod m) বলতে তো আমরা বুঝি m দিয়ে ভাগ করলে a আর b এর একই ভাগশেষ থাকবে। ঋনাত্মক সংখ্যার ভাগশেষ কিভাবে পাওয়া যাবে? এইটা নিয়ে কিছু কথা বলা যাক। একটা ভাগ প্রক্রিয়ায় আমরা কিছু জিনিস শিখে এসেছিলাম ভাজ্য, ভাজক, ভাগফল, ভাগশেষ। আমরা শিখেছিলাম ভাজ্য = ভাজকxভাগফল + ভাগশেষ। কোন সংখ্যা a'র ক্ষেত্রেঃ

a = bq + r, এই আকৃতিতে লিখা যায়। r হচ্ছে এখানে ভাগশেষ, q ভাজক। এবং অবশ্যই r<q। এরকম অবস্থায় আমরা যখন বলব a ≡ r (mod b), এখানে r হচ্ছে ভাগশেষ। মানে r হচ্ছে এ ধরণের সবচেয়ে ছোট ধনাত্মক সংখ্যা। অনেক সময়েই এই সবচেয়ে ছোট সংখ্যাকে দরকার হয়। এখন এই r কে প্রকাশ করা হয় সাধারণত a mod b এই কথাটা দিয়ে। যেমন 31 mod 10 = 1, 445 mod 3 = 1, 732 mod 12 = 0 ইত্যাদি।

উদাহরণ ২ : 31^{742} কে 10 দিয়ে ভাগ করলে ভাগশেষ কত ?

সমাধান : প্রথমে খেয়াল কর $31 \equiv 1 \pmod{10}$
তাহলে $31^{742} \equiv 1^{742} \equiv 1 \pmod{10}$ । [প্রাথমিক ধর্ম 6 নং দেখো]

উদাহরণ ৩ : 29^{742} কে 10 দিয়ে ভাগ করে ভাগশেষ বের কর ।

সমাধান : এবার? $29 \equiv 9 \pmod{10}$
বা, $29^{742} \equiv 9^{742} \pmod{10}$ এইটাই বা কিভাবে করে ?

বরং লিখা যাক $29 \equiv 9 - 3\times10 \equiv -1 \pmod{10}$ এবার বল কি হবে?

$29^{742} \equiv (-1)^{742} \equiv 1 \pmod{10}$, অর্থাৎ এক্ষেত্রেও ভাগফল থাকবে 1। এভাবে মডুলার অ্যারেথমেটিকে অনেকসময় ঋণাত্মক সংখ্যা নিয়ে হিসাব করলে হিসাব অনেক সহজ হয়ে যায়। বিশেষত যখন বেশি ঘাতের হিসাব থাকে r এর মান যত কম হয় তত ভালো। এটা আরও উদাহরণসহ সামনে দেখবে।

উদাহরণ ৪ : 4^{100} কে 17 দিয়ে ভাগ করলে ভাগশেষ কত থাকে?

সমাধান : $4^2 \equiv 16 \equiv -1 \pmod{17}$ so, $4^{100} \equiv (4^2)^{50} \equiv (-1)^{50} \equiv 1 \pmod{17}$

উদাহরণ ৫ : 5^{15} কে *7*দিয়ে ভাগ করলে ভাগশেষ কত ?

সমাধান : $5 \equiv -2 \pmod{7}$
এখন , $5^{15} \equiv (-2)^{15} \equiv (-8)^5 \equiv (-1)^5 \equiv -1 \pmod{7}$
তাহলে ভাগশেষ দাঁড়াচ্ছে 6

উদাহরণ ৬ : দেখাও যে, 2^k+5 একটি যৌগিক সংখ্যা যেখানে k, 2^n আকারের একটি সংখ্যা । n একটি ধনাত্মক পূর্ণসংখ্যা ।

সমাধানঃ ধরি, $N=2^k+5$

যখন n=1 তখন k=2এবং N=9 ।

আবার যখন n=2 তখন k=4এবং N=21;

আমরা অনুমান করতে পারি যে, N, 3 দ্বারা বিভাজ্য । এটি প্রমান করতে হবে ।

এখন, $2 \equiv -1 \pmod{3}$। যেহেতু k একটি জোড় সংখ্যা সেহেতু $2^k \equiv (-1)^k \equiv 1 \pmod{3}$ ।

অতএব, $N \equiv 1+5 \equiv 0 \pmod{3}$ ।

আরেকটা ব্যাপার বলে রাখি। একটু আগে যখন দুইটা প্রশ্ন করা হয়েছিল তার পরপরই একটা কথা বলা হয়েছিল " এই প্রশ্নগুলোর প্রত্যেকটার অনেকগুলো করে উত্তর হতে পারে। উত্তরগুলো একেবারে নেগেটিভ ইনফিনিটি থেকে শুরু করে পজিটিভ ইনফিনিটি পর্যন্ত হতে পারে।" এটা আশা করি বুঝতে পেরেছ এরই মধ্যে। চিন্তা কর, যেসব সংখ্যাকে 6 দিয়ে ভাগ করলে 2 অবশিষ্ট থাকে (যেমন, 20, 26) এরকম সংখ্যাগুলোকে যদি আমি একটা পরিবার ধরি তাহলে এই পরিবারের সদস্য আর কে কে হবে? 32, 38, 42 এরকম আরও অনেকে। অর্থাৎ 6 পর পর আমি একটা একটা সংখ্যা পাই যারা এই পরিবারের সদস্য। একটু কষ্ট করলে এদের একটা সাধারণ পদও বের করে ফেলা যায়। $6k + 2$ আকারের সকল সংখ্যা এই পরিবারের সদস্য হবে। মনে হতে পারে এতক্ষণ ধরে খুবই স্বাভাবিক একটা ব্যাপারকে পেঁচিয়ে বর্ণনা করছি। তা করার মূল কারণ আমরা এতক্ষণ পর্যন্ত মডুলার যোগ-বিয়োগ-গুণ এইসব হিসেবই দেখেছি। একটু পর মডুলার সমীকরণ পাব বিভিন্ন চলকসহ। যেমন একটা সমীকরণ যদি পাইঃ
$x \equiv 2 \pmod{17}$ তাহলে বলতে পারব এর সাধারণ সমাধান $x = 17k + 2$, যেখানে k যেকোন পূর্ণসংখ্যা।

Divisibility Criteria (ভাগ যাওয়ার শর্ত):

কখন একটা সংখ্যা 2 দিয়ে বিভাজ্য হয়? বা 3 দিয়ে? 5, 7 বা 11 দিয়ে? এরকম কিছু শর্ত নিয়ে আলোচনা করা যাকঃ

2 দিয়ে বিভাজ্যতাঃ

2 দিয়ে বিভাজ্য সংখ্যাকে কি বলে? জোড় সংখ্যা। এখন একটা সংখ্যা জোড় কিনা কিভাবে বুঝা যায় এক ঝলকেই? শুধু দেখতে হবে শেষ অঙ্কটা জোড় কিনা। যেমন 352, জোড় সংখ্যা। কিন্তু 4443, প্রথম 3টি অঙ্কই জোড় হওয়া সত্যেও সংখ্যাটি বিজোড় কারণ শেষ অঙ্ক বিজোড়।

4 দিয়ে বিভাজ্যতাঃ

আরেকটু কঠিনে আসি। আর এবার আমাদের কনগ্রুয়েন্সের জ্ঞাণ ব্যবহার করা যাক। তার আগে কিছু জিনিস খেয়াল করতে হবে। যেকোন সংখ্যাকে দশের বিভিন্ন ঘাত দিয়ে খুব সহজেই প্রকাশ করা যায়। যেমন

$4132 = 4\times1000+1\times100+3\times10+2$

$22587 = 2\times10000 +2\times1000+5\times100+8\times10+7$

$373 = 3\times100+7\times10+3$

$28 = 2\times10+8$

এখন এখানে ভালোমত খেয়াল করে দেখ, 10000,1000,100 এসবই 4 দিয়ে বিভাজ্য। যেহেতু $10^n = 2^n x5^n$ তাই n, 2 এর সমান বা বড় হলেই 10^n, 4 দিয়ে ভাগ যাবে। অর্থাৎ 10 এর চেয়ে বড় 10 এর সকল ঘাত 4 দিয়ে ভাগ যাবে। তাহলে যেহেতু এদের সবার সম্বন্ধে বলা যায় $10^n \equiv 0 \pmod 4$, তাহলে উপরের সংখ্যাগুলোর ক্ষেত্রে পাই,

$4132 \equiv 32 \pmod 4$

$22587 \equiv 87 \pmod 4$

$373 \equiv 73 \pmod 4$

তারমানে যেকোন সংখ্যাকে 4 দিয়ে ভাগ করলে যে ভাগশেষ থাকে তার শেষ দুই অঙ্ককে 4 দিয়ে ভাগ করলেও একই ভাগশেষ থাকে। অর্থাৎ **কোন সংখ্যা 4 দিয়ে বিভাজ্য হবে যদি শেষ দুই অঙ্ক দিয়ে গঠিত সংখ্যা 4 দিয়ে বিভাজ্য হয়।** পরীক্ষা করে দেখ কিছু সংখ্যার জন্য। এক কাজ কর, তোমার ফোন নম্বর নাও। এবার বল সেটি 4 দিয়ে বিভাজ্য কিনা।

8 দিয়ে বিভাজ্যতাঃ

4 দিয়ে বিভাজ্যতার জ্ঞান থেকে এটা বলতে পারবে না? 100 থেকে বড় সকল 10 এর ঘাত 8 দিয়ে বিভাজ্য। তাহলে এটার ক্ষেত্রে বলা যায় **কোন সংখ্যা 8 দিয়ে বিভাজ্য হবে যদি তার শেষ 3 অঙ্ক 8 দিয়ে বিভাজ্য হয়।**

এবার এক কাজ কর, সাধারণভাবে 2^n সংখ্যাটি দিয়ে কোন সংখ্যা নিঃশেষে বিভাজ্য হওয়ার শর্ত কি বের করে ফেল।

5 দিয়ে বিভাজ্যতাঃ

5 দিয়ে বিভাজ্যতার জন্যও সংখ্যাকে 10 এর ঘাত দিয়ে নির্দেশ করা যাক। এবং আবার খেয়াল কর যে এর ক্ষেত্রেও শেষ অঙ্কটি দেখলেই হবে কারণ বাকি অংশটুকু 5 দিয়ে সবসময়ই বিভাজ্য হবে। এখন শেষ অঙ্ক কত হলে 5 দিয়ে বিভাজ্য হতে পারে? 0 বা 5।

5 এর ঘাত যেমন 25, 125 ইত্যাদি দিয়ে বিভাজ্যতাও 2 এর ঘাত দিয়ে বিভাজ্যতার মত। সেই শর্তগুলো সহজেই তোমরা বের করে নিতে পারবে।

11 দিয়ে বিভাজ্যতাঃ

এটা একটু মজার। একটা জিনিস খেয়াল কর একটু।

$10 \equiv -1 \pmod{11}$,

$10^2 \equiv (-1)^2 \equiv 1 \pmod{11}$

$10^3 \equiv (10^2)\times(10) \equiv -1 \pmod{11}$

$10^4 \equiv 1 \pmod{11}$

এখন আমরা যে উদাহরণগুলো 2 দিয়ে বিভাজ্যতার ক্ষেত্রে দেখছিলাম সেগুলো যদি 11 এর ক্ষেত্রেও দেখি তাহলে কি দাঁড়ায়?

$4132 = 4\times1000+1\times100+3\times10+2$

$22587 = 2\times10000 +2\times1000+5\times100+8\times10+7$

$373 = 3\times100+7\times10+3$

$28 = 2\times10+8$

তাহলে $4132 \equiv 4\times(-1) + 1\times1 + 3\times(-1) + 2 \equiv -4+1-3+2 \equiv 4 \pmod{11}$
$22587 \equiv 2 -2+5-8+7 \equiv 4 \pmod{11}$
$373 \equiv 3-7+3 = -1 \equiv 10 \pmod{11}$
$28 \equiv -2+8 \equiv 6 \pmod{11}$

অর্থাৎ 11 এর ক্ষেত্রে কি পেলাম আমরা? আমরা **কোন সংখ্যার অঙ্কগুলো alternatingly যোগ-বিয়োগ করে(একটা যোগ, একটা বিয়োগ) আমরা তার 11 দিয়ে ভাগ করলে ভাগশেষ বের করতে পারব। এই যোগ-বিয়োগ করে প্রাপ্ত সংখ্যা 11 দিয়ে বিভাজ্য হলে সংখ্যাটি নিজেও 11 দিয়ে বিভাজ্য হবে।**

উদাহরণঃ 1331 -> 1-3+3-1 = 0, 1331, 11 দিয়ে বিভাজ্য। 123321 -> 1-2+3-3+2-1 = 0, 123321, 11 দিয়ে বিভাজ্য। 14641 -> -1+4-6+4-1 = 0, তাই 14641, 11 দিয়ে বিভাজ্য।

3 ও 9 দিয়ে বিভাজ্যতাঃ

আবারও আমরা ঐ 10 এর ঘাতেরই সাহায্য নিব। এবং এক্ষেত্রে আসলে ব্যাপারটা আরও সহজ।

$10 \equiv 1 \pmod 3$, তার মানে $10^2 \equiv 10^3 \equiv 10^4 \equiv 1 \pmod 3$

9 এর ক্ষেত্রেও ব্যাপারটা একইরকমই।

$10 \equiv 1 \pmod 9$, তার মানে $10^2 \equiv 10^3 \equiv 10^4 \equiv 1 \pmod 9$

তাহলে কি পাওয়া যায়?

$4132 \equiv 4\times1 + 1\times1 + 3\times1 + 2 \equiv 4+1+3+2 \equiv 10 \equiv 1 \pmod 3$
$22587 \equiv 2 + 2+ 5 + 8 +7 \equiv 24 \equiv 0 \pmod 3$
$393 \equiv 3+9+3 = 15 \equiv 0 \pmod 3$
$28 \equiv 2+8 \equiv 10 \equiv 1 \pmod 3$

আবার

$4132 \equiv 4\times1 + 1\times1 + 3\times1 + 2 \equiv 4+1+3+2 \equiv 10 \equiv 1 \pmod 9$
$22797 \equiv 2 + 2+ 7 + 9 +7 \equiv 27 \equiv 0 \pmod 9$
$3735 \equiv 3+7+3 + 5 = 18 \equiv 0 \pmod 9$
$28 \equiv 2+8 \equiv 10 \equiv 1 \pmod 9$

তাহলে তোমরা নিশ্চয়ই বুঝতে পারছ যে **যে সংখ্যাগুলো 0 (mod 9) হচ্ছে সেগুলো 9 দিয়ে বিভাজ্য আর যেগুলো 0 (mod 3), সেগুলো 3 দিয়ে বিভাজ্য।**

এভাবে 7, 13 এই সংখ্যাগুলো দিয়ে ভাগ যাওয়ার শর্তও বের করা যেতে পারে তবে সেগুলো আরও কম কার্যকরী। তাই সেগুলো নিয়ে আলাপ করছি না, তোমরা নিজেরা সেগুলো বের করে নিতে পারো একটু কষ্ট করে।

উদাহরণ ৭ : p এবং p^2+2 উভয়েই মৌলিক সংখ্যা এমন সকল p নির্ণয় কর।

সমাধান : খেয়াল কর যে $p^2 \equiv 0$ or $1 \pmod 3$ যেকোন p এর জন্য।
$p^2 \equiv 0 \pmod 3$ হলে $p \equiv 0 \pmod 3$
এরকম একমাত্র মৌলিক সংখ্যা 3 । এর জন্য $p^2+2 = 11$ যা মৌলিক সংখ্যা।
এখন অন্য সকল সংখ্যার জন্য $p^2 \equiv 1 \pmod 3$ অর্থাৎ $p^2+2 \equiv 1+2 \equiv 0 \pmod 3$
সুতরাং p মৌলিক সংখ্যা হলে p^2+2, 3 এর গুণিতক হবে যা মৌলিক হওয়া সম্ভব না।
সুতরাং এরকম একমাত্র $p = 3$

উদাহরণ ৮ : দেখাও যে, $4k+3$ এই আকারের কোন পূর্ণসংখ্যা দুটি বর্গসংখ্যার যোগফল হতে পারে না ।

সমাধানঃ মনে করি , a এবং b দুটি সংখ্যা এবং $N= a^2+b^2$ । এখন যদি a জোড় সংখ্যা হয় তাহলে ধরি, $a=2k$, যেখানে k পূর্ণসংখ্যা । তাহলে, $a^2=4k^2 \equiv 0 \pmod 4$ ।

আবার, যদি a বিজোড় সংখ্যা হয় তাহলে ধরি, $a=2k+1$, যেখানে k পূর্ণসংখ্যা। তাহলে, $a^2=4k^2+4k+1 \equiv 1 \pmod 4$ ।তাহলে লেখা যায় , $a^2 \equiv 0 \text{ or } 1 \pmod 4$ ।
অনুরুপভাবে লেখা যায় , $b^2 \equiv 0 \text{ or } 1 \pmod 4$ ।
দুটো কংগ্রুয়েন্স যোগ করে পাই, $N=a^2+b^2 \equiv 0 \text{ or } 1 \text{ or } 2 \pmod 4$ ।
উভয়ে জোড় হলে ভাগশেষ শূন্য, একটি জোড় অপরটি বিজোড় হলে এক এবং দুটিই বিজোড় হলে ভাগশেষ দুই । অতএব ভাগশেষ তিন হওয়া কখনও সম্ভব নয় ।

উদাহরণ ৯ : 3^{99} এর শেষ দুই অঙ্ক নির্ণয় কর।

সমাধানঃ সাধারণ পর্যবেক্ষণ আর তারপর হিসাবের মাধ্যমে এই সমস্যা সমাধান করা যেতে পারে। তবে কনগ্রুয়েন্সের ধারণার মাধ্যমে আমরা এটা বেশ সহজে করতে পারব। সেটাই দেখা যাক।

যেকোন সংখ্যাকে যদি 100 দিয়ে ভাগ করি তাহলে ভাগশেষ কি হবে? এর শেষ দুই অঙ্ক দিয়ে তৈরি সংখ্যা। যেমন 3234 কে 100 দিয়ে ভাগ করলে ভাগশেষ 34। 4692 কে 100 দিয়ে ভাগ করলে ভাগশেষ 92। তাহলে আমাদের বের করতে হবে $3^{99} \bmod 100$ ।

কিভাবে করা যায়? খেয়াল কর

$3^{99} \equiv (3^{49})^2 \times 3 \pmod{100}$

$3^{49} \equiv (3^{24})^2 \times 3 \pmod{100}$

$3^{24} \equiv (3^{12})^2 \pmod{100}$

$3^{12} \equiv (3^{6})^2 \pmod{100}$

$3^{6} \equiv (3^{3})^2 \pmod{100}$

এখন $3^3 \bmod 100 \equiv 27$

এই মানগুলো এবার বসাতে বসাতে যাওয়া যাক।

$3^6 \equiv (27)^2 \equiv 29 \pmod{100}$

$3^{12} \equiv (29)^2 \equiv 41 \pmod{100}$

$3^{24} \equiv (41)^2 \equiv 81 \pmod{100}$

$3^{49} \equiv (81)^2 x3 \equiv 83 \pmod{100}$

$3^{99} \equiv (83)^2 x3 \equiv 67 \pmod{100}$

তাহলে 3^{99} এর শেষ দুই অঙ্ক 6 ও 7 ।

(এবার নিজেই প্রশ্ন কর, কিভাবে ব্যাক ক্যালকুলেশন করলাম? খেয়াল কর প্রত্যেকবার অর্ধেক ঘাতের মডুলো আগে বের করে নিয়েছি। তাতে আমাদের হিসাব অনেক সহজ হয়ে গেছে)

ফার্মার থিওরেম (Fermat's Little Theorem) :

যদি p একটি মৌলিক সংখ্যা হয় এবং a ,p দ্বারা বিভাজ্য না হয় তবে $a^{p-1} \equiv 1 \pmod p$ ।

প্রমাণটি একটু জটিল হওয়ায় কড়াকড়ি প্রমাণ দেয়ার আগে একটা উদাহরণ দেয়া হল ।
যদি $p=5$ এবং $a=3$ হয় তবে a এর প্রথম p-1টি গুনিতক তথা প্রথম 4টি গুনিতক যথাক্রমে 3,6,9,12 ।
এদেরকে p অর্থাৎ 5 দিয়ে ভাগ করে দেখা যায় ,

$3 \equiv 3 \pmod 5$
$6 \equiv 1 \pmod 5$
$9 \equiv 4 \pmod 5$
$12 \equiv 2 \pmod 5$
তারমানে আমরা ভাগশেষ হিসেবে 1 থেকে p-1 তথা 1 থেকে 4 পর্যন্ত সঙ্খাগুলোই পেলাম ।

এবার উপরের কংগ্রুয়েন্সগুলো গুন করে পাই,
$3\times 6\times 9\times 12 \equiv 1\times 2\times 3\times 4 \pmod p$
বামপক্ষে প্রত্যেক পদ থেকে 3 কমন নেয়া যায় । আর $1\times 2\times 3\times 4$ হচ্ছে 4 এর ফ্যাক্টোরিয়াল যাকে 4! দ্বারা প্রকাশ করা হয় ।
$3^4\times 4! \equiv 4! \pmod p$
এবার উভয় পক্ষকে 4! দ্বারা ভাগ করে পাওয়া যায় ,
$3^4 \equiv 1 \pmod p$

প্রমাণ :

1, 2, 3, ..., p-1 এই সঙ্খাগুলোকে p দ্বারা ভাগ করলে ভাগশেষ প্রতি ক্ষেত্রে ভিন্ন হয় এবং ভাগশেষ যথাক্রমে 1, 2, 3, ..., p-1 হবে ।
a এর প্রথম p-1 টি ধনাত্মক গুনিতক যথাক্রমে ,
a, 2a, 3a, ... (p -1)a
1 থেকে p-1 এর মধ্যে দুটি ভিন্ন সংখ্যা r এবং s কল্পনা করি । মনে করি ra এবং sa কে pদ্বারা ভাগ করলে ভাগশেষ একই । যদি,
$ra \equiv sa \pmod p$ হয় তবে উভয়পক্ষকে a দ্বারা ভাগ করে দেখা যায় $r \equiv s \pmod p$ হবে ।
কিন্তু এটা সম্ভব না , কারণ r এবং s কে p দ্বারা ভাগ করলে ভাগশেষ ভিন্ন । তারমানে ra এবং sa কে p দ্বারা ভাগ করলে ভাগশেষ সব সময় ভিন্ন হতে হবে । তাহলে a, 2a, 3a, ... (p -1)a এই গুনিতকগুলোকে p দ্বারা ভাগ করলে প্রতি ক্ষেত্রে ভাগশেষ ভিন্ন । তাহলে অবশ্যই ভাগশেষ গুলো যেকোনো ক্রমে 1, 2, 3, ..., p-1 হতে হবে ।

এখন আমরা যদি উপরের উদাহরণ এর মত কতগুলো কংগ্রুয়েন্স কল্পনা করে সেগুলোকে গুন করে দেই তাহলে আমরা পাবো,
$a\times 2a\times 3a\times \ldots \times(p-1)a \equiv 1\times 2\times 3\times \ldots\times(p-1) \pmod p$
বা, $a^{p-1}\times(p-1)! \equiv (p-1)! \pmod p$
বা, $a^{p-1} \equiv 1 \pmod p$ প্রমাণ হয়ে গেল ।

এই থিওরেমের একটা অনুসিদ্ধান্ত আছে , $\mathbf{a^p \equiv a \pmod p}$ । উপরের থিওরেম থেকে এটা কিভাবে প্রমাণ করা যায় বল দেখি ?

উদাহরণ ১০ : 2^{68} কে 19 দ্বারা ভাগ করলে ভাগশেষ কত ?

সমাধান : $2^{18} \equiv 1 \pmod{19}$
এখন , $2^{68} = (2^{18})\times 2^{14} \equiv 1^3 \times 2^{14} \equiv 2^{14} \pmod{19}$
যেহেতু $2^4 = 16 \equiv -3 \pmod{19}$,
$2^{14} = (2^4)^3\times 2^2 \equiv (-3)^3\times 2^2 \equiv -27\times 4 \equiv 11\times 4 \equiv 44 \equiv 6 \pmod{19}$

উদাহরণ ১১ : দেখাও যে, n যেকোনো অঋণাত্মক পূর্ণ সংখ্যা হলে , $3^{6n}-2^{6n}$, 35 দ্বারা নিঃশেষে বিভাজ্য।

সমাধানঃ ফার্মার থিওরেম অনুসারে, $3^6 \equiv 1 \pmod 7$
বা, $(3^6)^n \equiv (1)^n \equiv 1 \pmod 7$
বা, $3^{6n} \equiv 1 \pmod 7$

আবার, $2^6 \equiv 1 \pmod 7$
বা, $(2^6)^n \equiv (1)^n \equiv 1 \pmod 7$
বা, $2^{6n} \equiv 1 \pmod 7$

বিয়োগ করে পাওয়া যায় , $3^{6n} - 2^{6n} \equiv 0 \pmod 7$

আবার, $2 \equiv -3 \pmod 5$
বা, $2^{2n} \equiv (-3)^{6n} \equiv 3^{6n} \pmod 5$
অতএব, $3^{6n} - 2^{6n} \equiv 0 \pmod 5$
যেহেতু 5,7 সহমৌলিক সেহেতু, $3^{6n} - 2^{6n} \equiv 0 \pmod{35}$ ।

সিউডো প্রাইমঃ

কোন সংখ্যা যৌগিক কিনা টা যাচাই করার জন্য $a^p \equiv a \pmod p$ এই অনুসিদ্ধান্ত ব্যাবহার করা যায় । প্রথমে আমরা a=2 এর জন্য দেখি । যদি কোন সংখ্যা nএর জন্য $2^n \equiv 2 \pmod n$ মিথ্যা প্রমানিত হয় তাহলে ওই সংখ্যাটি অবশ্যই যৌগিক । কিন্তু প্রশ্ন হল , যদি $2^n \equiv 2 \pmod n$ সত্য হয় তাহলে কি n মৌলিক হতে হবে ? উত্তর হচ্ছে না । যেমন n=341 এর জন্য ,
$2^{341} = (2^{10})^{34} \times 2 \equiv 2 \pmod{341}$
দেখা যাচ্ছে , n=341 এর জন্য $2^n \equiv 2 \pmod n$ সত্য হয় । অথচ $341 = 11 \times 31$

যেসব সংখ্যা n এর ক্ষেত্রে $2^n \equiv 2 \pmod n$ সত্য প্রমানিত হয় অথচ তারা মৌলিক সংখ্যা নয় তাদেরকে বলা হয় সিউডো প্রাইম ।

কারমাইকেল সংখ্যাঃ

সিউডো প্রাইম এর চেয়েও বিস্ময়কর উদাহরণ হল কারমাইকেল সংখ্যা । কারণ সিউডো প্রাইম শুধুমাত্র a=2 এর জন্য $a^n \equiv a \pmod n$ কে সিদ্ধ করে । কিন্তু কারমাইকেল সংখ্যা a এর যেকোনো মানের জন্য $a^n \equiv a \pmod n$ সম্পর্ককে সিদ্ধ করে । অথচ তারা যৌগিক ।

যেসব সংখ্যা n, a এর যেকোনো মানের জন্য $a^n \equiv a \pmod n$ সম্পর্ককে সিদ্ধ করে কিন্তু তারা মৌলিক নয় এরকম সংখ্যাকে কারমাইকেল সংখ্যা বলা হয় ।

এরকম একটি সংখ্যা হচ্ছে 561 । তাহলে বুঝতে পারছ আশা করি , যেসব সংখ্যার ক্ষেত্রে $a^n \equiv a \pmod n$ মিথ্যা হয় তারা অবশ্যই যৌগিক । কিন্তু যাদের ক্ষেত্রে সত্য হয় তারা মৌলিক এমন কোন নিশ্চয়তা নেই ।

উইলসনের থিওরেমঃ

P একটি মৌলিক সংখ্যা হবে যদি এবং কেবল যদি $(p-1)! \equiv -1 \pmod p$ হয় ।

প্রমানঃ এখানে "যদি এবং কেবল যদি" কথাটা দিয়ে দুটো অর্থ বুঝানো হচ্ছে । যদি p একটি মৌলিক সংখ্যা হয় তবে , $(p-1)! \equiv -1 \pmod p$ সত্য হবে । আবার , যেকোনো সংখ্যা m এর জন্য যদি $(m-1)! \equiv -1 \pmod m$ সত্য হয় তাহলে m অবশ্যই মৌলিক হবে । প্রথম অংশের প্রথম কিছুটা জটিল এবং একঘেয়ে , তাই আমরা সেদিকে যাব না । আমরা শুধু দ্বিতীয় অংশ প্রমাণ করবো ।

ধরি , যেকোনো সংখ্যা m এর জন্য $(m-1)! \equiv -1 \pmod m$ সত্য ।
যদি m একটি যৌগিক সংখ্যা হয় তবে এমন একটি t পাওয়া যাবে যেন $t|m$ যেখানে, $1<t<m$ ।
তাহলে, $t|(m-1)!$ বা, $(m-1)! \equiv 0 \pmod t$ ।
কিন্তু যেহেতু , t , m এর উৎপাদক ; মডুলার এরিথমেটিক এর 9 নং ধর্ম অনুসারে , $(m-1)! \equiv -1 \pmod t$
উপরের দুটি কংগ্রুয়েন্স থেকে বলা যায় , $-1 \equiv 0 \pmod t$ যা কেবলমাত্র t=1 এর জন্য সত্য ।
সুতরাং m এর কোন উৎপাদক t, 1 এর চেয়ে বড় হতে পারে না , ফলে m অবশ্যই মৌলিক । প্রমাণ হয়ে গেল !

প্রকৃতপক্ষে, যৌগিক m এর জন্য $(m-1)! \equiv 0 \pmod m$ হয় ।

উদাহরণ ১২ : দেখাও যে, p একটি বেজোড় মৌলিক সংখ্যা হলে, $2(p-3)! \equiv -1 \pmod{p}$ ।

সমাধানঃ উইলসন এর থিওরেম অনুসারে, $(p-1)! \equiv -1 \pmod{p}$
আবার, $(p-1)! \equiv (p-1)(p-2)(p-3)! \equiv (-1)(-2)(p-3)! \pmod{p}$
অতএব, $2(p-3)! \equiv -1 \pmod{p}$

উদাহরণ ১৩ : ধর, $y=82! / 21$; y কে 83 দ্বারা ভাগ করলে ভাগশেষ কত পাওয়া যাবে?

সমাধানঃ উইলসন এর থিওরেম অনুসারে, $21y = 82! \equiv -1 \pmod{83}$
আবার, $21.4 \equiv 1 \pmod{83}$
কংগ্রুয়েন্স দুটো যোগ করে পাই, $21(y+4) \equiv 0 \pmod{83}$
বা, $y+4 \equiv 0 \pmod{83}$
বা, $y \equiv -4 \pmod{83}$
বা, বা, $y \equiv -79 \pmod{83}$

অতএব ভাগশেষ থাকবে 79

উদাহরণ ১৪ : দেখাও যে, সকল মৌলিক সংখ্যা p এবং সকল পূর্ণ সংখ্যা a এর জন্য $a^p+(p-1)!$ a, p দ্বারা বিভাজ্য ।

সমাধানঃ উইলসন এর থিওরেম অনুসারে, $(p-1)! \equiv -1 \pmod{p}$
বা, $(p-1)!a \equiv -a \pmod{p}$

ফার্মার থিওরেম অনুসারে, $a^p \equiv a \pmod{p}$

যোগ করে পাওয়া যায় , $a^p+(p-1)!a \equiv 0 \pmod{p}$

মডুলার সমীকরণঃ

একঘাত সমীকরণঃ

একঘাত মডুলার সমীকরণ $ax \equiv b \pmod{m}$ । এই ধরনের সমীকরণগুলোর সমাধান থাকবে কিনা সেটা a,m এর gcd এর উপর নির্ভর করে ।

থিওরেমঃ

$ax \equiv b \pmod{m}$ কংগ্রুয়েন্স এর সমাধান থাকবে যদি এবং কেবল যদি b, gcd(a,m) দ্বারা বিভাজ্য হয় ।

প্রমানঃ যেহেতু $ax \equiv b \pmod{m}$ অতএব লেখা যায় $m|(ax-b)$, তাহলে $ax-b=mk$ যেখানে k যেকোনো পূর্ণসংখ্যা । পক্ষান্তর করে পাই ,

$ax+mk=b$

এবার ধরি , $gcd(a,m)=d$ । খেয়াল কর সমীকরণের বামপক্ষে a, m উভয় রাশি d দ্বারা বিভাজ্য । কেননা d তাদের gcd । অতএব সমীকরণের বামপক্ষ অবশ্যই d দ্বারা বিভাজ্য । যদি এর কোন সমাধান থাকে তবে অবশ্যই সমীকরণের ডানপক্ষও d দ্বারা বিভাজ্য হতে হবে । নয়ত কোন সমাধান থাকবে না । অতএব $ax \equiv b \pmod{m}$ কংগ্রুয়েন্স এর সমাধান থাকবে যদি এবং কেবল যদি b, gcd(a,m) দ্বারা বিভাজ্য হয় ।

আমরা দেখলাম , যে একটা একঘাত কংগ্রুয়েন্স কে ax+mk=b আকারে প্রকাশ করা যায় , যা কিনা একটা একঘাত ডায়োফ্যান্টাইন সমীকরণ । তাহলে যেভাবে ডায়োফ্যান্টাইন সমীকরণের সমাধান বের করা যায় একই নিয়মে একঘাত কংগ্রুয়েন্স এরও সমাধান করা যাবে । অথবা , $x=x_0+(mt)/d$ এই সূত্র ব্যাবহার করেও সমাধান করা যায় ।

এখানে , x_0 হল যেকোনো একটি সমাধান ।

d হচ্ছে a,m এর gcd ।

t একটি পূর্ণসংখ্যা । t এর মান 1,2,3... এভাবে পরিবর্তন করলে ভিন্ন ভিন্ন সমাধান পাওয়া যায় ।

উদাহরন ১৫: 1 $4x\equiv5 \pmod{16}$ এর সমাধান বের কর ।

সমাধানঃ এখানে , a=14, m=16 এবং d=gcd(a,m)=gcd(14,16)=2 ।
যেহেতু b=5 এবং তা 2 দ্বারা বিভাজ্য নয় কাজেই এই কংগ্রুয়েন্স এর কোন সমাধান থাকবে না ।

উদাহরণ ১৬: সমাধান কর , $10x\equiv 6 \pmod{12}$

সমাধানঃ a=10, m=12 এবং d=gcd(a,m)=gcd(10,12)=2 ।
যেহেতু b=6 এবং 6, 2 দ্বারা বিভাজ্য ; এই কংগ্রুয়েন্স এর সমাধান আছে । এখন প্রথমে যেকোনো একটি সমাধান বের করতে হবে । একটু খেয়াল করলেই দেখতে পাবে , x=3 একটা সমাধান । তাহলে আমরা x_0 মান পেয়ে গেলাম 3 । তাহলে সাধারন সমাধান হবে ,
$x=x_0+(mt)/d$
বা,$x=3+12t/2$
বা, $x=3+6t$

এখন t এর মান 1,2,3,... বসিয়ে যথাক্রমে x এর মান 9,15,21,... পাওয়া যায় । যাদের প্রত্যেকে এই কংগ্রুয়েন্স এর সমাধান । এই সমাধানকে কংগ্রুয়েন্স আকারে প্রকাশ করা হলে , $x\equiv 3 \pmod{12}$ ।

এবার একাধিক সমীকরণের সমাধান দেখা যাক । আমরা দুটি কংগ্রুয়েন্স $x\equiv b_1 \pmod{m_1}$ এবং $x\equiv b_2 \pmod{m_2}$ এর সমাধান দেখবো । জটিলতা পরিহার করার জন্য প্রথমেই ধরে m_1 এবং m_2 পরস্পর সহমৌলিক । m_1 এবং m_2 সহমৌলিক হলে সব সময় এই কংগ্রুয়েন্স গুলোর সমাধান থাকবে ।

প্রথমে , $x\equiv 2 \pmod{7}$ এবং $x \equiv 3 \pmod{4}$ এর সমাধান দেখি ।
আমরা প্রথমে যেকোনো একটির সাধারন সমাধান বের করবো । পরে ওই সমাধানে t এর বিভিন্ন মান বসিয়ে দেখবো সমাধানগুলো দ্বিতীয় কংগ্রুয়েন্সকে সিদ্ধ করে কিনা । একটু খেয়াল করলেই দেখা যাবে , প্রথম কংগ্রুয়েন্স এর একটি সমাধান হচ্ছে 2 । সাধারন সমাধান হবে $x_1=2+ t$। তাহলে এবার শুরু করা যাক,
$t=0, x_1=2 \equiv 2 \pmod{4}$
$t=1, x_1=9 \equiv 1 \pmod{4}$
$t=-1, x_1=-5 \equiv 3 \pmod{4}$
আমরা প্রথম সমাধান -5 পেয়ে গেলাম । কিন্তু আমরা হিসাব চালিয়ে যাব,
$t=2, x_1=16 \equiv 0 \pmod{4}$
$t=-2, x_1=-12 \equiv 0 \pmod{4}$
$t=3, x_1=23 \equiv 3 \pmod{4}$
আমরা দ্বিতীয় সমাধান 23 পেয়ে গেছি । খেয়াল করে দেখো , আমাদের প্রথম এবং দ্বিতীয় সমাধানের মধ্যে পার্থক্য 28 । তাহলে 23 এর সাথে 28 যোগ করলে আরেকটি সমাধান পাবো? 23+28=51 এবং এটি আরেকটি সমাধান !

এতো কিছু থাকতে পার্থক্য 28 করে আসছে , কারণ হল $28=4\times 7$ । **এই ব্যাপারে একটা থিওরেম আছে যা** Chinese Remainder Theorem নামে পরিচিত ।

Chinese Remainder Theorem আমাদেরকে বলে দেয় যে, m_1 এবং m_2 সহমৌলিক হলে $x\equiv b_1 \pmod{m_1}$ এবং $x\equiv b_2 \pmod{m_2}$ এরকম দুটি কংগ্রুয়েন্স এর সমাধান হবে $x=x_0+ m_1\times m_2\times t$ । যেখানে x_0 যেকোনো একটি সমাধান । সমাধানকে কংগ্রুয়েন্স আকারে প্রকাশ করা হলে , $x\equiv x_0 \pmod{m_1m_2}$ ।

উদাহরণ ১৭: সমাধান কর , $x\equiv 2 \pmod 7$ এবং $x \equiv 3 \pmod 5$ ।

সমাধানঃ আমরা দেখতে পাচ্ছি , $m_1=7$ এবং $m_2=5$ যারা সহমৌলিক । তাহলে কোনভাবে x_0 বের করে ফেলতে পারলেই ঝামেলা মিটে যায় । প্রথম কংগ্রুয়েন্স এর একটা সমাধান $x_1=2$ এবং সাধারন সমাধান $x= x_1+7t$ । এখন আমরা t এর মান 0,1,-1,2,-2 ... ... এভাবে বসিয়ে পরীক্ষা করে দেখবো । প্রাপ্ত মানগুলোর মধ্যে যেই মানটি দ্বিতীয় কংগ্রুয়েন্সকে সিদ্ধ করবে সেটাই হবে x_0 । তাহলে আমরা দেখতে থাকি,
$t=0, x_2=2 \equiv 2 \pmod 5$
$t=1, x_2=9 \equiv 4 \pmod 5$
$t=-1, x_2=-5 \equiv 0 \pmod 5$
$t=2, x_2=16 \equiv 1 \pmod 5$
$t=-2, x_2=-12 \equiv 3 \pmod 5$ আমরা পেয়ে গেছি!
তাহলে $x_0=-12$ এবং সাধারন সমাধান $x= -12+7\times5\times t= -12+35t$
বা , $x \equiv -12 \pmod{35}$

যদি m_1, m_2 সহমৌলিক না হয় তখন সমাধান $x\equiv x_0 \pmod{m_1m_2}$ এর পরিবর্তে $x\equiv x_0 \pmod{\text{lcm}(m_1,m_2)}$ । আকারে আসবে । অর্থাৎ m_1, m_2 গুনফলের পরিবর্তে তাদের ল.সা.গু নিতে হবে ।

দুটো কংগ্রুয়েন্স সমাধান তো আমরা সহজেই পেয়ে গেলাম । যদি তিনটা থাকতো? তিনটা কংগ্রুয়েন্স সমাধান করার জন্য প্রথমে যেকোনো দুটি কংগ্রুয়েন্স এর সাধারন সমাধান বের করবে । এরপর সেখানে t এর বিভিন্ন মান বসিয়ে দেখবে কোন মানটি তৃতীয় কংগ্রুয়েন্স কে সিদ্ধ করে । সেটাই হবে x_0 । সাধারন সমাধান হবে $x=x_0+ m_1\times m_2\times m_3\times t$ ।

উদাহরণ ১৮: নিচের তিনটি কংগ্রুয়েন্স সাধারন সমাধান বের কর ,
$x \equiv 2 \pmod 7$, $x \equiv 3 \pmod 5$ $x \equiv 2 \pmod 3$

সমাধানঃ প্রথম দুটি কংগ্রুয়েন্স সমাধান আমরা আগেই বের করেছি , $x_2= -12+35t$ । এবার t এর মানগুলো বসিয়ে পাই ,
$t=0, x_3=-12 \equiv 0 \pmod 3$
$t=1, x_3=23 \equiv 2 \pmod 3$
এবার খুব তাড়াতাড়িই পেয়ে গেলাম !

তাহলে $x_0=23$ এবং সাধারন সমাধান $x= 23+7\times5\times3\times t= 23+105t$ বা, $x \equiv 23 \pmod{105}$ ।

এতো গেল একটি অজ্ঞাত রাশি বিশিষ্ট কংগ্রুয়েন্স এর সমাধান । যদি দুটি থাকে ? তাহলে কিভাবে করবে?

উদাহরণ ১৯: কনগ্রুয়েন্স যুগলের সমাধান নির্ণয় করঃ $3x-7y\equiv 4 \pmod{19}$, $7x-3y\equiv 1 \pmod{19}$

সমাধানঃ প্রথম কনগ্রুয়েন্স এর ক্ষেত্রে $7(3x-7y) \equiv 7.\ 4 \pmod{19}$ অর্থাৎ $21x-49y\equiv 28 \pmod{19}$
একই ভাবে ,$3(7x-3y)\equiv 3.\ 1 \pmod{19}$ বা, $21x-9y \equiv 3 \pmod{19}$
বিয়োগ করে পাই, $-40y\equiv 25 \pmod{19}$ বা, $-2y\equiv 6 \pmod{19}$
অতএব $y \equiv -3 \pmod{19}$
প্রথম কংগ্রুয়েন্স এ yএর পরিবর্তে -3 বসিয়ে পাওয়া যায়, $3x\equiv -17 \pmod{19}$
বা,$3x\equiv -17+38 \pmod{19}$
বা, $3x\equiv 21 \pmod{19}$
বা,$x\equiv 7 \pmod{19}$ [প্রাথমিক ধর্ম 11 নং দেখো]
অর্থাৎ নির্ণেয় সমাধান, $x\equiv 7 \pmod{19}$; $y\equiv 16 \pmod{19}$

অনুশীলনীঃ

সমস্যা ১ : দেখাও যে, যেকোনো 3 টি ক্রমিক সংখ্যার গুণফল 6 দ্বারা নিঃশেষে বিভাজ্য ।

সমস্যা ২ : দেখাও যে, $4k+3$ এই আকারের কোন পূর্ণসংখ্যা দুটি বর্গসংখ্যার যোগফল হতে পারে না ।

সমস্যা ৩ : 7^{13} কে 11 দিয়ে ভাগ করলে ভাগশেষ কত ?

সমস্যা ৪ : 3^{91} কে 23 দ্বারা ভাগ করলে ভাগশেষ কত হবে ?

সমস্যা ৫ : 3^{999} কে 28 দিয়ে ভাগ করলে ভাগশেষ কত হবে?

সমস্যা ৬ : 43^{37} কে 11 দ্বারা ভাগ করলে ভাগশেষ কত থাকবে?

সমস্যা ৭ : দেখাও যে, $5^{23}+1$, 47 দ্বারা নিঃশেষে বিভাজ্য ।

সমস্যা ৮ : $(5^{97}+11^{33})^8$ কে 24 দিয়ে ভাগ করলে ভাগশেষ কত ?

সমস্যা ৯ : $1\times2\times3\times\ldots6$ কে 7 দিয়ে ভাগ করলে ভাগশেষ কত হবে?

সমস্যা ১০ : n যেকোন একটি ধনাত্মক পূর্ণ সংখ্যা। এর জন্য নিচের ঘটনাগুলো প্রমাণ কর।

- $n^2 \equiv 0$ or $1 \pmod 3$
- $n^2 \equiv 0$ or $\pm 1 \pmod 5$
- $n^2 \equiv 0$ or $1 \pmod 4$
- $n^2 \equiv 0$ or 1 or $4 \pmod 8$
- $n^3 \equiv 0$ or $\pm 1 \pmod 9$
- $n^4 \equiv 0$ or $1 \pmod{16}$

সমস্যা ১১ : $x^2+y^2 = 100003$ সমীকরণটির কয়টি ধনাত্মক পূর্ণ সংখ্যা সমাধান আছে?

সমস্যা ১২ : $x^2+3y^2 = 422$ সমীকরণটির কয়টি ধনাত্মক পূর্ণ সংখ্যা সমাধান আছে?

সমস্যা ১৩ : 6, 12, 18, 13 সংখ্যাগুলো দিয়ে বিভাজ্যতার শর্ত বের কর। তারপর বল 1 _ _ 3 6 আকৃতির 52 দিয়ে বিভাজ্য সর্বনিম্ন পাঁচ অঙ্কের সংখ্যাটি নির্ণয় কর।

সমস্যা ১৪ : এমন কতগুলো সংখ্যা আছে যাদেরকে 3 দিয়ে ভাগ করলে ভাগশেষ 5 এবং 5দিয়ে ভাগ করলে ভাগশেষ 3 ?

সমস্যা ১৫ : এমন সকল ধনাত্মক পূর্ণসংখ্যা d বের কর যেন n^2+1 এবং $(n+1)^2+1$ উভয়ে d দ্বারা বিভাজ্য হয় ।

সমস্যা ১৬ : $x^2 \equiv 2 \pmod{17}$ কনগ্রুয়েন্স এর সকল সমাধান বের কর ।

সমস্যা ১৭ : মনে কর , p হল 2 বা 5 বাদে অন্য যে কোন মৌলিক সংখ্যা । প্রমাণ কর যে , এমন একটি ধনাত্মক পূর্ণসংখ্যা k আছে যার জন্য $10^k \equiv 1 \pmod{p}$ ।

সমস্যা ১৮ : প্রমাণ কর যে , nযেকোনো ধনাত্মক পূর্ণসংখ্যা হলে $n^{17}-n \equiv 0 \pmod{170}$ ।

সমস্যা ১৯ : যদি p , 7 এর চেয়ে বড় মৌলিক সংখ্যা হয় তবে প্রমাণ কর যে , $p^4 \equiv 1 \pmod{240}$ ।

সমস্যা ২০ : মনে কর, একটি মৌলিক সংখ্যা এবং $a^p+b^p=c^p$ হলে, p, a+b-c নিঃশেষে ভাগ করে।

সমস্যা ২১ : দেখাও যে, যেকোনো মৌলিক সংখ্যা p>5 , 9999...999 আকারের অসংখ্য সংখ্যা কে নিঃশেষে ভাগ করে ।

সমস্যা ২২ : 56! কে 59 দ্বারা ভাগ করলে ভাগশেষ কত পাওয়া যাবে?

সমস্যা ২৩ : n এর সকল পূর্ণ সাংখ্যিক মান নির্ণয় কর যেন $n(n+1) \mid (n-1)!$, এখানে n>1 ।

সমস্যা ২৪ : সমাধান কর : $143x \equiv 4 \pmod{315}$ ।

সমস্যা ২৫ : সমাধান করঃ $64x \equiv 897 \pmod{1001}$

সমস্যা ২৬ : সমাধান করঃ $108x \equiv 171 \pmod{529}$

সমস্যা ২৭ : কনগ্রুয়েন্স যুগলের সমাধান নির্ণয় করঃ $3x-7y \equiv 4 \pmod{15}$; $7x-3y \equiv 1 \pmod{15}$