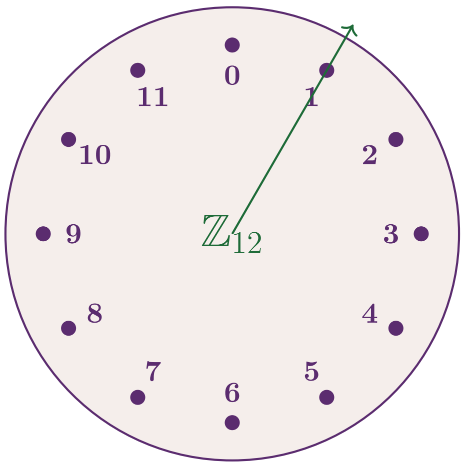
Josephite Math Club

মডুলার অ্যারিথমেটিক



Tawhid Bin Omar

June 8, 2026

এই হ্যান্ডআউটটি কাদের জন্য?

মডুলার অ্যারিথমেটিকের একেবারে মূল থেকে শুরু করে অলিম্পিয়াড স্তরের সমস্যা সমাধান করা।

Contents

1 ভিত্তিপ্রস্তর: ভাগের নিয়ম থেকে কনগ্রুয়েন্স **2**

1.1 বিভাজ্যতা এবং ইউক্লিডীয় ভাগ অ্যালগরিদম 2

1.2 কনগ্রুয়েন্স সম্পর্ক 2

1.3 ঘড়ির অ্যারিথমেটিক: $\mathbb{Z}_n$ চাক্ষুষভাবে 3

1.4 মডুলার অপারেশনসমূহ 4

1.5 মডুলার বিভাজন এবং মডুলার ইনভার্স 4

2 ধ্রুপদী উপপাদ্যসমূহ ও তাদের অন্তর্নিহিত শক্তি **6**

2.1 রৈখিক কনগ্রুয়েন্স 6

2.2 চীনা Remainder Theorem!! (CRT) 6

2.3 Fermat's Little Theorem 8

2.4 অয়লারের টোটিয়েন্ট ফাংশন এবং অয়লারের উপপাদ্য 8

3 অ্যালজেব্রাইক স্ট্রাকচার: অর্ডার এবং প্রিমিটিভ রুট **10**

3.1 মডুলার অর্ডার 10

3.2 প্রিমিটিভ রুট (Primitive Root) 10

3.3 উইলসনের উপপাদ্য (Wilson's Theorem) 11

4 কোয়াড্রেটিক রেসিডিউ এবং রেসিপ্রোসিটি **12**

4.1 কোয়াড্রেটিক রেসিডিউ 12

4.2 Legendre প্রতীক 12

4.3 গাউসের লেম্মা (Gauss's Lemma) 13

4.4 কোয়াড্রেটিক রেসিপ্রোসিটি (Law of Quadratic Reciprocity) 13

4.5 Jacobi প্রতীক 14

4.6 হেনসেলের লেম্মা (Hensel's Lemma) 14

5 অনুশীলনী **15**

5.1 সমস্যাসমূহ 15

5.2 সংকেত ও ইঙ্গিত 17

1 ভিত্তিপ্রস্তর: ভাগের নিয়ম থেকে কনগ্রুয়েন্স

1.1 বিভাজ্যতা এবং ইউক্লিডীয় ভাগ অ্যালগরিদম

গণিতের সবচেয়ে মৌলিক ধারণাগুলির মধ্যে একটি হলো বিভাজ্যতা। চলো আমরা একদম শুরু থেকে শুরু করি।

সংজ্ঞা 1.1 (বিভাজ্যতা). *ধরো $a, b \in \mathbb{Z}$ এবং $b \neq 0$। আমরা বলি b সংখ্যাটি a-কে বিভাজ্য করে (অথবা $b \mid a$ পড়া হয় ``b divides a") যদি এমন কোনো পূর্ণসংখ্যা k থাকে যেন $a = kb$।*

উদাহরণস্বরূপ: $3 \mid 12$ *কারণ* $12 = 4 \cdot 3$। *কিন্তু* $5 \nmid 13$ *কারণ* $13 = 2 \cdot 5 + 3$ *এবং ভাগশেষ* $3 \neq 0$।

উপপাদ্য ১.১ — ইউক্লিডীয় ভাগ অ্যালগরিদম (Euclidean Division Algorithm)

যেকোনো দুটি পূর্ণসংখ্যা a এবং $b > 0$-এর জন্য, অনন্যভাবে নির্ধারিত পূর্ণসংখ্যা q (ভাগফল) এবং r (ভাগশেষ) বিদ্যমান যেন:

$$a = qb + r, \quad 0 \leq r < b$$

প্রমাণ:

অস্তিত্ব: সেটটি বিবেচনা করো $S = \{a - kb : k \in \mathbb{Z},\ a - kb \geq 0\}$। $b > 0$ হওয়ায়, k-এর পর্যাপ্ত ঋণাত্মক মান নিলে $a - kb > 0$ পাওয়া যায়, তাই S অশূন্য। Well-ordering principle অনুযায়ী S-এর একটি সর্বনিম্ন উপাদান আছে; সেটিকে $r = a - qb$ বলি।

দাবি: $r < b$। ধরো $r \geq b$। তাহলে $r - b = a - (q+1)b \geq 0$, অর্থাৎ $r - b \in S$ এবং $r - b < r$। এটি r-এর সর্বনিম্নতার বিরোধিতা করে। সুতরাং $r < b$।

অনন্যতা: ধরো $a = q_1 b + r_1 = q_2 b + r_2$ যেখানে $0 \leq r_1, r_2 < b$। তাহলে $(q_1 - q_2)b = r_2 - r_1$। কিন্তু $|r_2 - r_1| < b$, তাই $b \mid (r_2 - r_1)$ তখনই সম্ভব যখন $r_1 = r_2$, এবং তখন $q_1 = q_2$। □

1.2 কনগ্রুয়েন্স সম্পর্ক

সংজ্ঞা 1.2 (কনগ্রুয়েন্স). *ধনাত্মক পূর্ণসংখ্যা n এবং পূর্ণসংখ্যা a, b-এর জন্য আমরা বলি a এবং b হলো n modulo-তে কনগ্রুয়েন্ট এবং লিখি:*

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

n-কে বলা হয় modulus।

উদাহরণ: $17 \equiv 5 \pmod 6$ কারণ $6 \mid (17 - 5) = 12$। আবার $-3 \equiv 9 \pmod{12}$ কারণ $12 \mid (-3 - 9) = -12$।

উপপাদ্য ১.২ — কনগ্রুয়েন্স একটি সমতুল্য সম্পর্ক (Equivalence Relation)

$\pmod n$ কনগ্রুয়েন্স সম্পর্কটি $\mathbb{Z}$-এ একটি equivalence relation। অর্থাৎ এটি নিচের তিনটি গুণ মানে:

(i) প্রতিফলনশীলতা (Reflexivity): সবসময় $a \equiv a \pmod n$।

প্রমাণ: $n \mid (a-a) = 0$. যেকোনো সংখ্যা 0-কে বিভাজ্য করে। ✓

(ii) প্রতিসমতা (Symmetry): যদি $a \equiv b \pmod n$ হয় তাহলে $b \equiv a \pmod n$।

প্রমাণ: $a \equiv b \pmod n$ মানে $n \mid (a-b)$। তাহলে $n \mid (-(a-b)) = (b-a)$, অর্থাৎ $b \equiv a \pmod n$। ✓

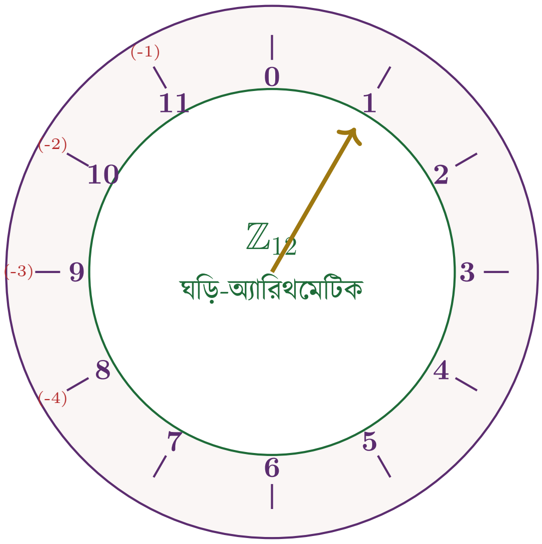
(iii) সংক্রান্তিশীলতা (Transitivity): যদি $a \equiv b$ এবং $b \equiv c \pmod n$ হয়, তাহলে $a \equiv c \pmod n$।

প্রমাণ: $n \mid (a-b)$ এবং $n \mid (b-c)$। তাহলে $n \mid \big[(a-b)+(b-c)\big] = (a-c)$। ✓

অতএব $\pmod n$ একটি সম্পূর্ণ equivalence relation। এটি $\mathbb{Z}$-কে nটি equivalence class-এ ভাগ করে: $[0], [1], [2], \ldots, [n-1]$। এই class-গুলোর সংগ্রহকে বলা হয় $\mathbb{Z}_n$ বা $\mathbb{Z}/n\mathbb{Z}$।

1.3 ঘড়ির অ্যারিথমেটিক: $\mathbb{Z}_n$ চাক্ষুষভাবে

মডুলার অ্যারিথমেটিক বোঝার সবচেয়ে সহজ উপায় হলো ঘড়ি কল্পনা করা। ১২ ঘণ্টার ঘড়িতে, ঘণ্টার কাঁটা 12-এর পরে আবার 1-এ ফেরে, ঠিক যেমন $\mathbb{Z}_{12}$-তে $12 \equiv 0$।



লাল সংখ্যাগুলো ঋণাত্মক সমতুল্য: যেমন $-1 \equiv 11 \pmod{12}$

1.4 মডুলার অপারেশনসমূহ

উপপাদ্য ১.৩ — মডুলার অ্যারিথমেটিকের মূল ধর্ম

যদি $a \equiv b \pmod{n}$ এবং $c \equiv d \pmod{n}$ হয়, তাহলে:

$$a + c \equiv b + d \pmod{n} \tag{1}$$

$$a - c \equiv b - d \pmod{n} \tag{2}$$

$$a \cdot c \equiv b \cdot d \pmod{n} \tag{3}$$

$$a^k \equiv b^k \pmod{n} \quad \text{যেকোনো ধনাত্মক পূর্ণসংখ্যা } k\text{-এর জন্য} \tag{4}$$

গুণফলের প্রমাণ (বাকিগুলো অনুরূপ):
$a = b + sn$ এবং $c = d + tn$ লেখা যায় কিছু পূর্ণসংখ্যা s, t-এর জন্য। তাহলে:

$$ac = (b + sn)(d + tn) = bd + btn + sdn + stn^2 = bd + n(bt + sd + stn)$$

সুতরাং $n \mid (ac - bd)$, অর্থাৎ $ac \equiv bd \pmod{n}$। □

কৌশল: বড় ঘাত গণনা করো দ্রুত

তুমি কি কখনো ভেবেছ $2^{100} \pmod{7}$ কত? সরাসরি গণনা অসাধ্য, কিন্তু pattern দেখো:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1 \pmod{7}$$

ঘুরে আসে! $100 = 33 \cdot 3 + 1$ হওয়ায়, $2^{100} = (2^3)^{33} \cdot 2^1 \equiv 1^{33} \cdot 2 = 2 \pmod{7}$। এই ধারণাটিই পরে ``order''-এর তত্ত্বে রূপ নেবে।

1.5 মডুলার বিভাজন এবং মডুলার ইনভার্স

যোগ, বিয়োগ, গুণ সব ঠিকঠাক কাজ করে, কিন্তু ভাগ? সতর্ক থাকতে হবে!

সাধারণ ভুল: অবিবেচনায় ভাগ করা

$6 \equiv 10 \pmod{4}$, এবং উভয় দিক 2 দিয়ে ভাগ করলে পাই $3 \equiv 5 \pmod{4}$। কিন্তু $3 - 5 = -2$, এবং $4 \nmid -2$! ভাগটি ভুল! সঠিক উত্তর হওয়া উচিৎ $3 \equiv 5 \pmod{2}$ (modulus $4/\gcd(2, 4) = 2$ দ্বারা ভাগ হয়)।
নিয়ম: $ac \equiv bc \pmod{n}$ হলে $a \equiv b \pmod{n/\gcd(c, n)}$ — modulus-ও ছোট হয়!

সংজ্ঞা 1.3 (মডুলার ইনভার্স). *a এবং n সহমৌলিক হলে ($\gcd(a, n) = 1$), সংখ্যা x যেন $ax \equiv 1 \pmod{n}$, তাকে a-এর মডুলার ইনভার্স বলা হয় এবং $a^{-1} \pmod{n}$ দিয়ে প্রকাশ করা হয়।*

উপপাদ্য ১.৪ — মডুলার ইনভার্সের অস্তিত্ব

$ax \equiv 1 \pmod{n}$-এর সমাধান বিদ্যমান তখন এবং কেবল তখন যখন $\gcd(a, n) = 1$।

প্রমাণ:

B□zout's identity অনুযায়ী, $\gcd(a, n) = 1$ তখন এবং কেবল তখন যখন পূর্ণসংখ্যা x, y বিদ্যমান যেন $ax + ny = 1$। এটি বোঝায় $ax - 1 = -ny$, অর্থাৎ $n \mid (ax - 1)$, তাই $ax \equiv 1 \pmod{n}$। উল্টোটাও সত্য: যদি $ax \equiv 1 \pmod{n}$ হয়, তাহলে $ax + ny = 1$ কোনো y-এর জন্য, সুতরাং $\gcd(a, n) \mid 1$, মানে $\gcd(a, n) = 1$। □

Extended Euclidean Algorithm দিয়ে ইনভার্স বের করা:

$17^{-1} \pmod{26}$ বের করতে চাই। Extended Euclidean algorithm চালাই:

$$\begin{aligned}
26 &= 1 \cdot 17 + 9 \\
17 &= 1 \cdot 9 + 8 \\
9 &= 1 \cdot 8 + 1 \\
8 &= 8 \cdot 1
\end{aligned}$$

পিছন থেকে: $1 = 9 - 1 \cdot 8 = 9 - 1 \cdot (17 - 9) = 2 \cdot 9 - 17 = 2(26 - 17) - 17 = 2 \cdot 26 - 3 \cdot 17$। সুতরাং $17 \cdot (-3) \equiv 1 \pmod{26}$, এবং $-3 \equiv 23 \pmod{26}$। তাই $17^{-1} \equiv 23 \pmod{26}$।

2 ধ্রুপদী উপপাদ্যসমূহ ও তাদের অন্তর্নিহিত শক্তি

2.1 রৈখিক কনগ্রুয়েন্স

উপপাদ্য ২.১ — রৈখিক কনগ্রুয়েন্সের সমাধান

$ax \equiv b \pmod{n}$-এর সমাধান বিদ্যমান তখন এবং কেবল তখন যখন $d = \gcd(a, n) \mid b$। সমাধান থাকলে ঠিক dটি অসম সমাধান থাকে $\pmod{n}$।

প্রমাণ:

$ax \equiv b \pmod{n}$ মানে $ax + ny = b$ কোনো পূর্ণসংখ্যা y-এর জন্য। B□zout অনুযায়ী এর সমাধান আছে iff $d \mid b$ (কারণ $ax + ny$-এর সব সম্ভাব্য মান d-এর গুণিতক)।

যদি $d \mid b$ হয়, সমীকরণটিকে $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ আকারে লিখতে পারি। এখন $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$, সুতরাং অনন্য সমাধান আছে $\pmod{n/d}$। এটি $\pmod{n}$-এ ঠিক dটি সমাধান দেয়। □

উদাহরণ 2.1. $15x \equiv 9 \pmod{21}$ *সমাধান করো।*

$d = \gcd(15, 21) = 3$। *যেহেতু* $3 \mid 9$, *সমাধান আছে। ভাগ করে:* $5x \equiv 3 \pmod{7}$। $5^{-1} \pmod{7}$ *বের করি:* $5 \cdot 3 = 15 = 2 \cdot 7 + 1$, *তাই* $5^{-1} \equiv 3 \pmod{7}$। *সুতরাং* $x \equiv 3 \cdot 3 = 9 \equiv 2 \pmod{7}$। *সম্পূর্ণ সমাধান:* $x \equiv 2, 9, 16 \pmod{21}$।

2.2 চীনা Remainder Theorem!! (CRT)

কল্পনা করো তুমি একটি সংখ্যা খুঁজছ যেটা 3 ভাগ করলে ভাগশেষ 2, 5 ভাগ করলে ভাগশেষ 3, এবং 7 ভাগ করলে ভাগশেষ 2 দেয়। CRT বলে এই সমস্যার সমাধান আছে এবং কীভাবে খুঁজবে তাও বলে!

উপপাদ্য ২.২ — Chinese Remainder Theorem

ধরো $n_1, n_2, \ldots, n_k$ পরস্পর সহমৌলিক (pairwise coprime), অর্থাৎ $i \neq j$ হলে $\gcd(n_i, n_j) = 1$। তাহলে যেকোনো $a_1, a_2, \ldots, a_k$-এর জন্য সমীকরণ সিস্টেম:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k}$$

এর $\pmod{N}$ তে একটি অনন্য সমাধান আছে, যেখানে $N = n_1 n_2 \cdots n_k$।

নির্মাণ:

$N_i = N/n_i$ ধরো। যেহেতু n_i-গুলো pairwise coprime, $\gcd(N_i, n_i) = 1$। তাই $M_i \equiv N_i^{-1} \pmod{n_i}$ বিদ্যমান। সমাধান হলো:

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{N}$$

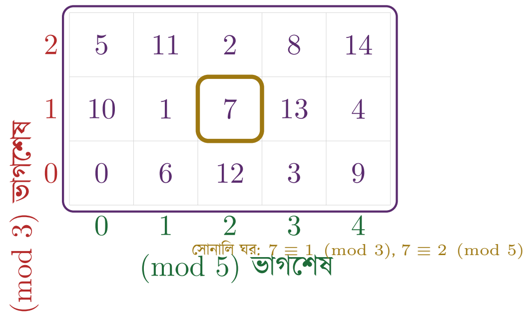
প্রমাণ যে এটি কাজ করে:

j-তম সমীকরণের জন্য: $j \neq i$ হলে $n_j \mid N_i$, তাই $a_i N_i M_i \equiv 0 \pmod{n_j}$। শুধু $i = j$ পদটি থাকে: $a_j N_j M_j \equiv a_j \cdot 1 = a_j \pmod{n_j}$। ✓

অনন্যতার প্রমাণ:

ধরো x এবং x' উভয়ই সমাধান। তাহলে প্রতি i-এর জন্য $n_i \mid (x - x')$। n_i-গুলো pairwise coprime হওয়ায় $N \mid (x - x')$, অর্থাৎ $x \equiv x' \pmod{N}$। □

$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$: CRT-এর চিত্র



***উদাহরণ 2.2** (CRT ব্যবহার). সমাধান করো:* $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$।

$N = 105$। $N_1 = 35, N_2 = 21, N_3 = 15$। $35^{-1} \pmod 3$: $35 \equiv 2$, $2^{-1} \equiv 2 \pmod 3$। তাই $M_1 = 2$। $21^{-1} \pmod 5$: $21 \equiv 1$, $1^{-1} \equiv 1 \pmod 5$। তাই $M_2 = 1$। $15^{-1} \pmod 7$: $15 \equiv 1$, $1^{-1} \equiv 1 \pmod 7$। তাই $M_3 = 1$।

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv 233 - 2 \cdot 105 = 23 \pmod{105}$$

উত্তর: $x \equiv 23 \pmod{105}$।

2.3 Fermat's Little Theorem

উপপাদ্য ২.৩ — Fermat's Little Theorem

p মৌলিক এবং $p \nmid a$ হলে $a^{p-1} \equiv 1 \pmod{p}$। অন্যভাবে, যেকোনো পূর্ণসংখ্যা a-এর জন্য $a^p \equiv a \pmod{p}$।

প্রমাণ ১ (গুণের গ্রুপ পদ্ধতি):

$p \nmid a$ হলে $a, 2a, 3a, \ldots, (p-1)a$ সংখ্যাগুলো $\pmod{p}$-তে সব আলাদা এবং $\{1, 2, \ldots, p-1\}$-এর একটি permutation। অতএব:

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

$(p-1)!$ এবং p সহমৌলিক হওয়ায় উভয় দিক $(p-1)!$ দিয়ে ভাগ করা যায়: $a^{p-1} \equiv 1 \pmod{p}$।
□

প্রমাণ ২ (Combinatorial — নেকলেস গণনা):

p রঙের পুঁতি দিয়ে p-পুঁতির নেকলেস তৈরির সংখ্যা গণনা করো। মোট arrangements p^p। Rotation-equivalent arrangements বাদ দিলে $p \mid (p^p - p \cdot \binom{\text{monochromatic}}{1})$ পাওয়া যায়। এটি $a^p \equiv a \pmod{p}$ দেয় সব a-এর জন্য।

FLT-এর কৌশলগত ব্যবহার

$a^{2023} \pmod{23}$ কত? $p = 23$ মৌলিক, তাই $a^{22} \equiv 1 \pmod{23}$। এখন $2023 = 22 \cdot 91 + 21$। তাই $a^{2023} \equiv a^{21} \pmod{23}$। আরো: $a^{21} = a^{22}/a \equiv 1/a \equiv a^{-1} \pmod{23}$!

সাধারণ কৌশল: $a^k \pmod{p}$ গণনায় k-কে $p-1$ দিয়ে ভাগ করো (যখন $\gcd(a, p) = 1$)।

2.4 অয়লারের টোটিয়েন্ট ফাংশন এবং অয়লারের উপপাদ্য

সংজ্ঞা 2.1 (অয়লারের টোটিয়েন্ট ফাংশন)**.** *$\phi(n)$ দিয়ে 1 থেকে n পর্যন্ত সংখ্যাগুলোর মধ্যে n-এর সাথে সহমৌলিক সংখ্যার সংখ্যা বোঝায়।*

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

উদাহরণ: $\phi(12) = 12 \cdot (1 - 1/2) \cdot (1 - 1/3) = 4$। সত্যিই $\{1, 5, 7, 11\}$ এই চারটি সংখ্যা 12-এর সাথে সহমৌলিক।

উপপাদ্য ২.৪ — ϕ-এর গুণাত্মক ধর্ম

$\gcd(m,n)=1$ হলে $\phi(mn)=\phi(m)\phi(n)$।

প্রমাণ (CRT দিয়ে): CRT বলে $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$ (যেহেতু $\gcd(m,n)=1$)। এই isomorphism ইউনিট (সহমৌলিক উপাদান) সংরক্ষণ করে। $\mathbb{Z}_{mn}$-এ ইউনিটের সংখ্যা $\phi(mn)$ এবং $\mathbb{Z}_m\times\mathbb{Z}_n$-এ ইউনিটের সংখ্যা $\phi(m)\phi(n)$। □

মৌলিক ঘাতের জন্য সূত্র: $\phi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$

উপপাদ্য ২.৫ — অয়লারের উপপাদ্য

$\gcd(a,n)=1$ হলে $a^{\phi(n)}\equiv 1\pmod n$।

প্রমাণ: $\{r_1,r_2,\ldots,r_{\phi(n)}\}$ হোক n-এর সাথে সহমৌলিক অবশিষ্টাংশের reduced residue system। তাহলে $\{ar_1,ar_2,\ldots,ar_{\phi(n)}\}$ও একই set $\pmod n$ (কারণ $\gcd(a,n)=1$)। গুণ করে:

$$a^{\phi(n)}\cdot r_1r_2\cdots r_{\phi(n)}\equiv r_1r_2\cdots r_{\phi(n)}\pmod n$$

উভয় দিক থেকে $r_1r_2\cdots r_{\phi(n)}$ বাদ দিলে $a^{\phi(n)}\equiv 1\pmod n$ পাই। □

বৈশিষ্ট্য	$\mathbb{Z}_p$ (মৌলিক modulus)	$\mathbb{Z}_n$ (যৌগিক modulus)
সব nonzero উপাদানের ইনভার্স?	হ্যাঁ (সবসময়)	শুধু সহমৌলিকদের
FLT/Euler প্রযোজ্য?	$a^{p-1}\equiv 1$	$a^{\phi(n)}\equiv 1$ (যদি সহমৌলিক হয়)
Primitive root আছে?	সবসময় হ্যাঁ	শুধু বিশেষ n-এর জন্য
$\mathbb{Z}_n^*$-এর গঠন	cyclic ($\cong\mathbb{Z}_{p-1}$)	জটিল, CRT দিয়ে ভাঙা যায়

3 অ্যালজেব্রাইক স্ট্রাকচার: অর্ডার এবং প্রিমিটিভ রুট

3.1 মডুলার অর্ডার

সংজ্ঞা 3.1 (উপাদানের অর্ডার). $\gcd(a,n)=1$ *হলে* a*-এর* n *modulo-তে অর্ডার হলো সর্বনিম্ন ধনাত্মক পূর্ণসংখ্যা* d *যেন* $a^d \equiv 1 \pmod{n}$*। এটি* $\text{ord}_n(a)$ *দিয়ে প্রকাশ করা হয়।*

উপপাদ্য ৩.১ — অর্ডারের মূল ধর্মাবলি

যদি $a^k \equiv 1 \pmod{n}$ হয়, তাহলে $\text{ord}_n(a) \mid k$। বিশেষত, $\text{ord}_n(a) \mid \phi(n)$।

প্রমাণ: $d = \text{ord}_n(a)$ ধরো। Euclidean algorithm দ্বারা $k = qd + r$ লেখা যায় যেখানে $0 \le r < d$। তাহলে:

$$a^k = a^{qd+r} = (a^d)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}$$

$a^k \equiv 1$ হওয়ায় $a^r \equiv 1 \pmod{n}$। কিন্তু $r < d$ এবং d হলো সর্বনিম্ন, তাই $r = 0$। সুতরাং $d \mid k$। Euler উপপাদ্য থেকে $a^{\phi(n)} \equiv 1$, তাই $d \mid \phi(n)$। □

উপপাদ্য ৩.২ — অর্ডারের একটি সুন্দর সূত্র

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{\gcd(k, \text{ord}_n(a))}$$

প্রমাণ: $d = \text{ord}_n(a)$ এবং $g = \gcd(k,d)$ ধরো। $(a^k)^{d/g} = a^{kd/g} = (a^d)^{k/g} \equiv 1$। এবং $(a^k)^m \equiv 1$ মানে $d \mid km$, অর্থাৎ $\frac{d}{g} \mid m$। সুতরাং $\text{ord}_n(a^k) = d/g$। □

3.2 প্রিমিটিভ রুট (Primitive Root)

সংজ্ঞা 3.2 (প্রিমিটিভ রুট). g*-কে* n *modulo-তে primitive root বলা হয় যদি* $\text{ord}_n(g) = \phi(n)$*, অর্থাৎ* g*-এর ঘাতগুলো* $\{1, 2, \ldots, n-1\}$*-এ* n*-এর সাথে সহমৌলিক সব উপাদানকে produce করে।*

উপপাদ্য ৩.৩ — $\mathbb{Z}_p^*$-এর চাক্রিক গঠন

প্রতিটি মৌলিক p-এর জন্য $\mathbb{Z}_p^*$ cyclic গ্রুপ, অর্থাৎ primitive root বিদ্যমান।

প্রমাণের সারাংশ: $\mathbb{Z}_p^*$-এ $d \mid (p-1)$-এর জন্য, সমীকরণ $x^d \equiv 1 \pmod{p}$-এর সর্বোচ্চ dটি সমাধান আছে (কারণ এটি $\mathbb{F}_p$-তে degree-d polynomial)। এর মানে, order-d উপাদানের সংখ্যা $\le \phi(d)$। মোট গণনা করলে: $\sum_{d|(p-1)}(\text{order-}d \text{ উপাদানসংখ্যা}) = p - 1 = \sum_{d|(p-1)} \phi(d)$। প্রতি d-এর জন্য সংখ্যাটি ঠিক $\phi(d)$, বিশেষত $d = p-1$-এর জন্য $\phi(p-1) \ge 1$ — primitive root আছে। □

Discrete Logarithm

g primitive root $\pmod p$ হলে, যেকোনো $a \not\equiv 0 \pmod p$-এর জন্য অনন্য $k \in \{0, 1, \ldots, p-2\}$ আছে যেন $g^k \equiv a \pmod p$। এই k-কে a-এর discrete logarithm বলে, $\log_g a$ লেখা হয়।
Discrete logarithm গণনা করা কঠিন — এটিই cryptography (যেমন Diffie-Hellman, DSA) এর নিরাপত্তার ভিত্তি!

3.3 উইলসনের উপপাদ্য (Wilson's Theorem)

উপপাদ্য ৩.৪ — উইলসনের উপপাদ্য

$$p \text{ মৌলিক} \iff (p-1)! \equiv -1 \pmod p$$

প্রমাণ ($\Rightarrow$ দিক):
p মৌলিক হলে $\mathbb{Z}_p^*$-এ প্রতিটি উপাদানের একটি unique inverse আছে। কোন উপাদানটি নিজের inverse? $a \equiv a^{-1}$ মানে $a^2 \equiv 1$, অর্থাৎ $p \mid (a-1)(a+1)$, তাই $a \equiv 1$ অথবা $a \equiv -1 \pmod p$। অন্য সব উপাদান আলাদা জোড়ায় জোড়া বাঁধে। $(p-1)!$-এ গুণ করলে এই জোড়াগুলো 1 দেয়, শুধু 1 এবং $p-1 \equiv -1$ থাকে:

$$(p-1)! \equiv 1 \cdot (-1) \cdot \underbrace{(2 \cdot 3 \cdots (p-2))}_{\text{জোড়ায় গুণ = 1}} \equiv -1 \pmod p \square$$

প্রমাণ ($\Leftarrow$ দিক): n যৌগিক হলে $n = ab$ যেখানে $1 < a, b < n$। তাহলে $a \mid (n-1)!$, কিন্তু $(n-1)! \equiv -1 \pmod n$ মানে $a \mid 1$, বিরোধাভাস।

উদাহরণ 3.1. *Wilson's theorem দিয়ে $p = 7$ verify করো:* $(7-1)! = 720 = 102 \cdot 7 + 6 \equiv 6 \equiv -1 \pmod 7$। ✓

4 কোয়াড্রেটিক রেসিডিউ এবং রেসিপ্রোসিটি

4.1 কোয়াড্রেটিক রেসিডিউ

সংজ্ঞা 4.1 (কোয়াড্রেটিক রেসিডিউ). *বিজোড় মৌলিক* p *এবং* $\gcd(a, p) = 1$*-এর জন্য* a*-কে quadratic residue (QR) বলা হয়* $\pmod p$ *যদি* $x^2 \equiv a \pmod p$*-এর কোনো সমাধান থাকে। না থাকলে* a *হবে quadratic non-residue (QNR)।*

$\mathbb{Z}_p^*$-এ QR-এর সংখ্যা $(p-1)/2$ এবং QNR-এরও $(p-1)/2$। প্রতিটি QR ঠিক দুটি মূলের (square root) সাথে সংগত।

4.2 Legendre প্রতীক

সংজ্ঞা 4.2 (Legendre Symbol). *বিজোড় মৌলিক* p *এবং* $p \nmid a$*-এর জন্য:*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{যদি } a \text{ QR হয়} \pmod p \\ -1 & \text{যদি } a \text{ QNR হয়} \pmod p \end{cases}$$

উপপাদ্য ৪.১ — অয়লারের মানদণ্ড (Euler's Criterion)

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

প্রমাণ: FLT থেকে $a^{p-1} \equiv 1$, তাই $\left(a^{(p-1)/2}\right)^2 \equiv 1$, মানে $a^{(p-1)/2} \equiv \pm 1 \pmod p$।
যদি a QR হয়: $a \equiv x^2$ কোনো x-এর জন্য, তাহলে $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod p$।
যদি a QNR হয়: g primitive root নাও। $a = g^k$ হবে k বিজোড়। $a^{(p-1)/2} = g^{k(p-1)/2}$। যেহেতু $\operatorname{ord}(g) = p-1$ এবং $k(p-1)/2$, $p-1$-এর গুণিতক নয় (k বিজোড় বলে), তাই $a^{(p-1)/2} \not\equiv 1$, তাই $\equiv -1 \pmod p$। □

Legendre প্রতীকের গুণাত্মক ধর্ম

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

প্রমাণ: Euler's criterion প্রয়োগ করো। $(ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \pmod p$.

4.3 গাউসের লেম্মা (Gauss's Lemma)

উপপাদ্য ৪.২ — Gauss's Lemma

বিজোড় মৌলিক p এবং $\gcd(a,p)=1$-এর জন্য, $a, 2a, 3a, \dots, \frac{p-1}{2}a$ সংখ্যাগুলোকে $\pmod p$-তে reduce করো এবং $(-p/2, p/2)$ range-এ প্রকাশ করো। ν হোক ঋণাত্মক মানের সংখ্যা। তাহলে:

$$\left(\frac{a}{p}\right) = (-1)^{\nu}$$

উদাহরণ 4.1. $\left(\frac{3}{7}\right)$ *গণনা করো।* $1\cdot 3=3,\ 2\cdot 3=6,\ 3\cdot 3=9\equiv 2 \pmod 7$*।* $(-7/2, 7/2) = (-3.5, 3.5)$ *range-এ:* $3\to +3,\ 6\to -1$ *(ঋণাত্মক),* $2\to +2$*।* $\nu=1$*, তাই* $\left(\frac{3}{7}\right)=(-1)^1=-1$*। অর্থাৎ* 3 *হলো QNR* $\pmod 7$*।*

4.4 কোয়াড্রেটিক রেসিপ্রোসিটি (Law of Quadratic Reciprocity)

গণিতের ইতিহাসে সবচেয়ে সুন্দর উপপাদ্যগুলির একটি। Gauss এটিকে ``Theorema Aureum'' (সোনালি উপপাদ্য) বলতেন।

উপপাদ্য ৪.৩ — কোয়াড্রেটিক রেসিপ্রোসিটি (QRP)

p এবং q আলাদা বিজোড় মৌলিক হলে:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

অন্যভাবে: যদি $p\equiv q\equiv 3 \pmod 4$ না হয়, তাহলে $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$। যদি উভয়ই $\equiv 3 \pmod 4$ হয়, তাহলে $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$।

সম্পূরক আইন:

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

QRP কীভাবে ব্যবহার করবে?

$\left(\frac{71}{73}\right)$ গণনা করো।

$71\equiv 3 \pmod 4$ এবং $73\equiv 1 \pmod 4$। তাই exponent $\frac{70}{2}\cdot\frac{72}{2}=35\cdot 36$, যেটি জোড়।

সুতরাং $\left(\frac{71}{73}\right)=\left(\frac{73}{71}\right)=\left(\frac{2}{71}\right)$।

$(71^2-1)/8=(5041-1)/8=630$, জোড়। তাই $\left(\frac{2}{71}\right)=1$। সুতরাং 71 হলো QR $\pmod{73}$।

4.5 Jacobi প্রতীক

সংজ্ঞা 4.3 (Jacobi Symbol). $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ *(বিজোড় ধনাত্মক) হলে:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1} \left(\frac{a}{p_2}\right)^{a_2} \cdots \left(\frac{a}{p_k}\right)^{a_k}$$

সতর্কতা: Jacobi symbol $+1$ *হলেই QR নিশ্চিত নয়, কিন্তু* -1 *হলে অবশ্যই QNR।*

4.6 হেনসেলের লেম্মা (Hensel's Lemma)

উপপাদ্য 8.8 — Hensel's Lemma

$f(x)$ হোক পূর্ণসংখ্যা coefficient-এর polynomial। ধরো $f(a) \equiv 0 \pmod{p}$ এবং $f'(a) \not\equiv 0 \pmod{p}$। তাহলে প্রতিটি $k \geq 1$-এর জন্য একটি অনন্য $a_k \pmod{p^k}$ আছে যেন $f(a_k) \equiv 0 \pmod{p^k}$ এবং $a_k \equiv a \pmod{p}$।

Lifting সূত্র: $a_{k+1} = a_k - f(a_k) \cdot [f'(a_k)]^{-1} \pmod{p^{k+1}}$

উদাহরণ: $x^2 \equiv 2 \pmod{7^3}$ সমাধান করো। প্রথমে $\pmod{7}$: $3^2 = 9 \equiv 2$, তাই $a_1 = 3$। $f(x) = x^2 - 2$, $f'(x) = 2x$।

Lift করো $\pmod{49}$: $f(3) = 7$, $f'(3) = 6$, $6^{-1} \pmod{7} = 6$ (কারণ $36 \equiv 1$)। $a_2 = 3 - 7 \cdot 6 = 3 - 42 \equiv 3 - 42 + 49 = 10 \pmod{49}$।

Lift করো $\pmod{343}$: $f(10) = 98 = 2 \cdot 49$, $f'(10) = 20$, $20^{-1} \pmod{49}$... এভাবে চলতে থাকে।

5 অনুশীলনী

সমস্যা সমাধানের আগে: সাধারণ কৌশলের তালিকা

মডুলার অ্যারিথমেটিক সমস্যায় blank page দেখলে এই প্রশ্নগুলো করো নিজেকে:

1. কোনো prime/prime power modulus কাজ করবে? FLT বা Euler প্রযোজ্য?
2. CRT দিয়ে modulus ভাঙা যাবে?
3. কোনো উপাদানের order কত? Divisibility ব্যবহার করা যাবে?
4. Quadratic residue হওয়া কি দরকার? Legendre symbol কাজ করবে?
5. Small cases check করো এবং pattern খোঁজো।

5.1 সমস্যাসমূহ

P1. [Basic] দেখাও যে $n^{61} \equiv n \pmod{1155}$ সব পূর্ণসংখ্যা n-এর জন্য।

P2. [Basic] কতগুলো পূর্ণসংখ্যা $n \in \{1, 2, \ldots, 2023\}$ আছে যেন $n^2 \equiv n \pmod{2023}$?

P3. [Basic] প্রমাণ করো যে $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ সব ধনাত্মক পূর্ণসংখ্যা $a > 1$ এবং m, n-এর জন্য।

P4. [Basic] সব জোড় $\pmod{100}$-এ: $n(n+1)(n+2)(n+3) \equiv 24 \pmod{100}$-এর কতটি সমাধান আছে $n \in \{0, 1, \ldots, 99\}$-এ?

P5. [**ISL 2000 N2 স্তর**] p মৌলিক এবং $a_1, a_2, \ldots, a_p$ হোক $\{0, 1, \ldots, p-1\}$-এর যেকোনো permutation। প্রমাণ করো যে $a_1a_2 + a_2a_3 + \cdots + a_{p-1}a_p \not\equiv 0 \pmod{p}$ সবসময় নয়।

P6. [Euler ও primitive root] p বিজোড় মৌলিক এবং g হলো primitive root $\pmod{p}$। দেখাও যে $g^{(p-1)/2} \equiv -1 \pmod{p}$।

P7. [CRT ও FLT] সব n-এর জন্য $n^{13} \equiv n \pmod{2730}$ প্রমাণ করো, যেখানে $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$।

P8. [**IMO 2005/4 প্রকার**] নির্ণয় করো সব মৌলিক p যেন $p \mid (2^{p-1} - 1)/p$ একটি পূর্ণসংখ্যা হয়। (Wieferich primes)

P9. [Quadratic Reciprocity] Legendre symbol $\left(\frac{5}{p}\right)$ গণনা করো সব বিজোড় মৌলিক $p \neq 5$-এর জন্য এবং ফলাফলকে $p \pmod{20}$-এর ভিত্তিতে শ্রেণীবদ্ধ করো।

P10. [**IMO স্তর**] ধনাত্মক পূর্ণসংখ্যা n দেওয়া আছে। প্রমাণ করো যে $\sum_{k=0}^{n} \binom{2n}{2k} \equiv 0 \pmod{2n+1}$ যদি এবং কেবল যদি $2n+1$ মৌলিক না হয়।

5.2 সংকেত ও ইঙ্গিত

সমস্যাওয়ারি সংকেত

P1:

$1155 = 3 \cdot 5 \cdot 7 \cdot 11$। CRT দিয়ে আলাদা করো। প্রতি prime p-এর জন্য FLT ব্যবহার করো: $p \mid (61-1)$? যাচাই করো $3-1=2$, $5-1=4$, $7-1=6$, $11-1=10$ এবং $\text{lcm}(2,4,6,10) = 60 \mid 60$।

P2:

$n^2 \equiv n$ মানে $n(n-1) \equiv 0 \pmod{2023}$। $2023 = 7 \cdot 17^2$ factor করো। CRT দিয়ে প্রতি prime power-এ সমাধান গণনা করো।

P3:

$d = \gcd(m,n)$ ধরো। প্রমাণ করো (i) $a^d - 1 \mid a^m - 1$ কারণ $d \mid m$; (ii) $a^d - 1 \mid a^n - 1$; (iii) যেকোনো common divisor $a^d - 1$ কে বিভাজ্য করে, Euclidean algorithm ব্যবহার করে।

P4:

$100 = 4 \cdot 25$। CRT: $\pmod 4$ এবং $\pmod{25}$ আলাদা করো। চারটি consecutive সংখ্যার গুণফল pattern দেখো।

P5:

একটি specific permutation construct করো যেখানে sum $\equiv 0 \pmod p$ হয়। Random permutations নিয়ে গড় গণনার approach বিবেচনা করো।

P6:

$g^{p-1} \equiv 1$ এবং $\text{ord}(g) = p-1$। তাই $g^{(p-1)/2}$ হলো 1-এর square root। কিন্তু $(p-1)/2$ কি $\text{ord}(g) = p-1$-এর গুণিতক?

P7:

$2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$। FLT প্রতি factor-এ প্রয়োগ করো। $12 = \text{lcm}(1,2,4,6,12)$ যাচাই করো।

P8:

Wieferich prime হলো p যেন $p^2 \mid 2^{p-1} - 1$। শুধু 1093 এবং 3511 পরিচিত। Fermat Quotient $q_p(2) = (2^{p-1}-1)/p \pmod p$ গণনা করো।

P9:

QRP ব্যবহার করো। $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ কখন? $p \pmod 5 \in \{1,4\}$ হলে $\left(\frac{p}{5}\right) = 1$, $p \pmod 5 \in \{2,3\}$ হলে -1। Sign ঠিক করতে এবং $p \pmod 4$-এর condition দেখো।

P10:

Lucas' theorem বা FLT ব্যবহার করো। $\sum_{k=0}^{n} \binom{2n}{2k} = 2^{2n-1} + \frac{1+(-1)^{2n}}{2} \cdots$ অথবা $(1+1)^{2n} + (1-1)^{2n}$ evaluate করো। $2n+1 \mid 2^{2n-1}$ কখন?

পরিশিষ্ট: রেফারেন্স কার্ড

উপপাদ্য	শর্ত	ফলাফল
FLT	p মৌলিক, $p \nmid a$	$a^{p-1} \equiv 1 \pmod{p}$
Euler	$\gcd(a, n) = 1$	$a^{\phi(n)} \equiv 1 \pmod{n}$
Wilson	p মৌলিক	$(p-1)! \equiv -1 \pmod{p}$
Euler's Criterion	p বিজোড় মৌলিক	$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
QRP	p, q আলাদা বিজোড় মৌলিক	$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$
Hensel	$f(a) \equiv 0,\ f'(a) \not\equiv 0 \pmod{p}$	সমাধান $\pmod{p^k}$-এ lift হয়
CRT	n_i pairwise coprime	অনন্য সমাধান $\pmod{N}$

শেষকথা: গণিতের পথে

মডুলার অ্যারিথমেটিক শুধু অলিম্পিয়াডের নয়, এটি আধুনিক সংখ্যাতত্ত্ব, ক্রিপ্টোগ্রাফি, এবং কম্পিউটার বিজ্ঞানের ভিত্তি। RSA encryption, elliptic curve cryptography — এগুলো সব এই একই বীজ থেকে জন্ম নিয়েছে যা তুমি আজ পড়লে।

``Mathematics is the queen of the sciences and number theory is the queen of mathematics"- Carl Friedrich Gauss