লিনিয়ার অনুসমতার সমাধান

Solutions to linear congruences

মুতাসিম মিম

আগস্ট ২০১৬

নিচের অনুসমতাটি দেখ $6x \equiv 1 \pmod{13}$. $x = 11$ এটিকে সিদ্ধ করে। আবার $x = -2, 24$ ও এটিকে সিদ্ধ করে। 11,-2,24 কে এই অনুসমতার সমাধান বলা হয়। $ax \equiv b \pmod{m}$ এই জাতীয় কনগ্রুয়েন্স কে *লিনিয়ার কনগ্রুয়েন্স* বলা হয়, যেখানে চলকের মাত্রা 1. এই ধরনের কনগ্রুয়েন্সের সমাধান করাই এই অধ্যায় এর উদ্দেশ্য। সবসময় এদের সমাধান থাকে না। প্রথমে দেখা যাক কোন কোন সময়ে এর সমাধান পাওয়া যাবে আর কখন সমাধান করাই যাবে না।

উপপাদ্য ১.১: যদি a ও m এর গ.সা.গু দ্বারা b বিভাজ্য না হয় তাহলে $ax \equiv b \pmod{m}$ সমাধান করা যাবে না।

প্রমাণ: x এর কোন মানের জন্য $ax \equiv b \pmod{m}$ সত্য হলে $(ax - b), m$ দ্বারা বিভাজ্য হবে, অর্থাৎ কোন পূর্ণসংখ্যা k এর জন্য $ax - b = km$ বা, $b = ax + km$ হবে. a, m এর গ.সা.গু দ্বারা ax এবং km বিভাজ্য। সুতরাং $ax + km$ ও a, m এর গ.সা.গু দ্বারা বিভাজ্য হবে। কাজেই b কেও a, m এর গ.সা.গু দ্বারা বিভাজ্য হতে হবে। তা না হলে $b = ax + km$ হওয়াও সম্ভব না। □

উপপাদ্য ১.২: a ও m এর গ.সা.গু দ্বারা b বিভাজ্য হলেই $ax \equiv b \pmod{m}$ অনুসমতাটি সমাধান করা যাবে।

তবে এটা প্রমাণ করার আগে আমাদের আরেকটা উপপাদ্য দেখতে হবে।

উপপাদ্য ১.৩: ধরা যাক, a ও m এর গ.সা.গু দ্বারা b বিভাজ্য এবং a ও m এর গ.সা.গু d দ্বারা a, b, m প্রত্যেককে ভাগ করে যথাক্রমে a_1, b_1, m_1 পাওয়া যায়। যদি $a_1 x \equiv b_1 \pmod{m_1}$ সমাধান করা যায়, তাহলে $ax \equiv b \pmod{m}$ সমাধান করা যাবে।

প্রমাণ: ধরা যাক a ও m এর গ.সা.গু d দ্বারা a, b, m প্রত্যেককে ভাগ করে যথাক্রমে a_1, b_1, m_1 পাওয়া গেল। যদি এমন x পাওয়া যায় যেন $a_1 x \equiv b_1 \pmod{m_1}$, তাহলে $m_1 | (a_1 - b_1)$, বা, $m_1 d | d(a_1 - b_1)$ বা, $m | (a - b)$, অর্থাৎ, $a \equiv b \pmod{m}$. সুতরাং, দেখা গেল $a_1 x \equiv b_1 \pmod{m_1}$ সমাধানযোগ্য হলে $a \equiv b \pmod{m}$ ও সমাধানযোগ্য হবে। □

লক্ষ্য কর উপরের উপপাদ্যে a_1, b_1 এর গ.সা.গু. হল 1

উপপাদ্য ১.৪: $(a, m) = 1$ হলে $ax \equiv b \pmod{m}$ অনুসমতাটির একটি ও কেবলমাত্র একটিই সমাধান আছে।

প্রমাণ: ধরা যাক, $\phi(m) = k, T = \{ar_1, ar_2, ar_3, \ldots, ar_k\}$,একটি reduced residue system $\pmod{m}$. লক্ষ্য কর, যেকোনো m এর জন্য $(1, m) = 1$. reduced residue system $\pmod{m}$ এর সংজ্ঞা অনুসারে, T-তে এমন একটি সদস্য ar_i আছে যেন $ar_i \equiv 1 \pmod{m}$ হয়। উভয় পক্ষকে b দ্বারা গুণ করে পাই, $a(br_i) \equiv b \pmod{m}$.সুতরাং br_i হল $ax \equiv b \pmod{m}$ এর একটি সমাধান।
লক্ষ্য কর, কেবলমাত্র একটি ar_i এর জন্যই $ar_i \equiv 1 \pmod{m}$. হবে। (reduced residue system $\pmod{m}$. এর সংজ্ঞা)। সুতরাং একটিই সমাধান পাওয়া যাবে। □

তাহলে উপপাদ্য ১.৩ আর ১.৪ মিলিয়ে ১.২ প্রমাণ হয়ে গেল।

উদাহরণ ১: ধরা যাক, $3x \equiv 4 \pmod{11}$ এর সমাধান বের করতে হবে। $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ একটি Reduced residue system (mod 11). যেহেতু, (3,11)=1, সুতরাং এটি সমাধান করা যাবে। সেটের সবগুলো সংখ্যাকে 3 দ্বারা গুণ করে প্রাপ্ত সংখ্যাগুলোর সেটও একটি Reduced residue system(mod 11)। গুণ করে প্রাপ্ত সেটটি হল, $\{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$. এই সংখ্যাগুলো পরীক্ষা করলে দেখা যায় $15 \equiv 4 \pmod{11}$. $15 = 3 \times 5$. সুতরাং 5 হল $3x \equiv 4 \pmod{11}$-এর সমাধান।