

# সংখ্যার মৌলিকত্ব নির্ণয়

গৌতমকুমার পাল, অধ্যাপক, কম্পিউটার  
সায়েন্স এবং ইঞ্জিনিয়ারিং বিভাগ,  
যাদবপুর বিশ্ববিদ্যালয়

গুনলে মনে হবে এতো অতি সহজ সমস্যা! ২ থেকে শুরু করে সংখ্যাটির বর্গমূলের নিকটতম পূর্ণসংখ্যা দিয়ে বিভাজন করে যেতে থাকবে - যদি কোনও বিভাজক থাকে তবে সংখ্যাটি যৌগিক, নতুবা মৌলিক। কিন্তু সংখ্যাটি যদি খুব বড় হয়, ধরা যাক কয়েকশ বা কয়েক হাজার অঙ্কের সংখ্যা, তাহলে হাতে কলমে করার কথা না হয় ছেড়েই দিলাম, অতি শক্তিশালী কম্পিউটারে করতেও অকল্পনীয় বেশি সময় লেগে যাবে। এদিকে কম্পিউটার সায়েন্সে সমস্যাটির গুরুত্ব কিন্তু অপরিসীম - Network security, e-banking, e-commerce প্রভৃতি ক্ষেত্রে মৌলিকত্ব নির্ণয় এবং অনুরূপ বহু সমস্যা রীতিমত প্রাসঙ্গিক। এসব সমস্যা ও তার সমাধান নিয়ে গনিত ও কম্পিউটার সায়েন্সে একটি নতুন শাখারই সৃষ্টি হয়েছে, তার নাম Cryptography.

সংখ্যার মৌলিকত্ব নির্ণয় নিয়ে চর্চা কিন্তু চলে আসছে প্রায় আড়াই হাজার বছর ধরে। খ্রীষ্টপূর্ব তৃতীয় শতাব্দীতে গ্রীকদেশের বিজ্ঞানী Eratosthenes যিনি প্রথম পৃথিবীর মানচিত্র অঙ্কন করেন এবং পৃথিবীর

## প্রাচীন রহস্যের নবীন সমাধান

পরিধি নির্ণয় করেন (পৃথিবী পরিভ্রমণ না করেই!) মৌলিকত্ব নির্ণয়ের একটি পদ্ধতি (algorithm) আবিষ্কার করেন। তারপর থেকে সাম্প্রতিক কাল পর্যন্ত এ বিষয়ে বহু algorithm আবিষ্কৃত হয়েছে কিন্তু কোনওটিই খুব উৎকৃষ্ট (efficient) নয়। কম্পিউটার সায়েন্সের ভাষায় বলা চলে, সেগুলি exponential running time এর জন্য বিখ্যাত (বা কুখ্যাত!) ভারতীয় হিসেবে আমাদের অত্যন্ত গর্বের বিষয় যে সম্প্রতি কানপুর আই আই টি-র অধ্যাপক মনীন্দ্র আগরওয়াল এবং তাঁর দুই ছাত্র নীরজ কয়াল ও নীতিন সাক্সেনা সংখ্যার মৌলিকত্ব নির্ণয়ের একটি Polynomial time algorithm আবিষ্কার করে সারা পৃথিবীকে আশ্চর্য করে দিয়েছেন। এতদিন কেউ যেমন এরকম algorithm আবিষ্কার করেননি, তেমনই কেউ ভাবেনওনি যে কোনওদিন এরকম algorithm আবিষ্কার সম্ভব। বেশিরভাগ বিজ্ঞানীই বিশ্বাস করতেন যে সমস্যাটি intrinsically hard (আবও technical ভাষায় বলতে গেলে এটি একটি NP - Problem)। কিন্তু এই তিন ভারতীয় সেই ধারণাকে ভুল প্রমাণ করেছেন। আশা করা যায় এই আবিষ্কার সংখ্যা তত্ত্ব এবং তার ব্যবহারিক প্রয়োগ সংক্রান্ত গবেষণায় এক নতুন দিগন্তের সূচনা করবে।

এ বিষয়ে বিস্তৃতভাবে জানার জন্য উক্ত তিন বিজ্ঞানীর মূল গবেষণাপত্রটি দ্রষ্টব্য : Manindra Agarwal, Neeraj Kiyal, Nitin Saxena, "PRIMES is in P", Annals of Mathematics 160 (2) . pages 781 - 793 (2004).