আমরা $\gcd(a,b)$ মানে ধরে নিব a আর b এর গ.সা.গু। আর $a|b$ এর মানে ধরে নিব যে a দিয়ে b বিভাজ্য।

[ফার্মার লিটল থিওরেম] যে কোন ধনাত্মক পূর্ণসংখ্যা a এবং মৌলিক সংখ্যা p এর জন্য $a^p - a, p$ দিয়ে বিভাজ্য। অনুসমতা ব্যবহার করে লিখলে $a^p \equiv a \pmod{p}$. যদি a, p দিয়ে বিভাজ্য হয় তাহলে তো এটা অবশ্যই সত্য। না হলে a, p এর সাথে সহমৌলিক। সেক্ষেত্রে $a^p - a = a(a^{p-1} - 1), p$ দিয়ে বিভাজ্য। যেহেতু p দিয়ে a বিভাজ্য না, তাহলে $a^{p-1} - 1, p$ দিয়ে বিভাজ্য। অন্য কথায়, $a^{p-1} \equiv 1 \pmod{p}$.

প্রমাণ. [1] আমরা একটি সংখ্যা 4 এবং একটি মৌলিক সংখ্যা 7 নিলাম, যারা সহমৌলিক। এখন আমরা নিচের অনুসমতাগুলো দেখি।

$$4 \cdot 1 \equiv 4 \pmod{7}$$
$$4 \cdot 2 \equiv 1 \pmod{7}$$
$$4 \cdot 3 \equiv 5 \pmod{7}$$
$$4 \cdot 4 \equiv 2 \pmod{7}$$
$$4 \cdot 5 \equiv 6 \pmod{7}$$
$$4 \cdot 6 \equiv 3 \pmod{7}$$

খেয়াল কর যে, এখানে 4 এর বিভিন্ন গুনিতককে 7 দিয়ে ভাগ করে ভিন্ন ভিন্ন ভাগশেষ পাওয়া যায়। ১ থেকে ৬ পর্যন্ত সংখ্যাগুলোকে ৪ দিয়ে গুন করে ৭ দিয়ে ভাগশেষগুলিও ১ থেকে ৬ হয়। এটা সম্ভব যদি আমরা প্রমাণ করতে পারি যে i এবং j যদি 7 এর চেয়ে ছোট কোন সংখ্যা হয় তাহলে $4i$ এবং $4j$ কে 7 দিয়ে ভাগ করলে ভাগশেষ এক হবে না। মানে তারা ভিন্ন ভিন্ন ভাগশেষ দিবে। এটা প্রমাণ করার জন্য, আমরা ধরে নেই যে $4i$ এবং $4j$ একই ভাগশেষ দেয়। তাহলে, $4i - 4j = 4(i-j)$ অবশ্যই 7 দিয়ে ভাগ যাবে। কিন্তু ৪ আর ৭ সহমৌলিক। তাই ৭ দিয়ে ভাগ গেলে $i - j$ ভাগ যাবে। কিন্তু এটা সম্ভব না। কারণ i, j উভয়ই ৭ হতে ছোট। তাই তাদের বিয়োগফল ও ৭ থেকে ছোট, এবং এ জন্য ৪ এর গুনিতক ও ভিন্ন ভিন্ন ভাগশেষ দিবে।[2] এখন, যেহেতু অনুসমতা গুন করা যায়, আমরা উপরের সবগুলি অনুসমতা গুন করে পাইঃ

$$4^6 \times (1 \cdot 2 \cdots 6) \equiv 1 \cdot 2 \cdots 6 \pmod{7}$$

আবার, $1 \cdot 2 \cdot 6, 7$ এর সাথে সহমৌলিক। তাই অনুসমতায় এটা দিয়ে ভাগ করা যাবে[3]। ভাগ করে ফেললেঃ

$$4^6 \equiv 1 \pmod{7}$$

এখানে অবশ্যই আমরা ৪ এর বদলে যে কোন সংখ্যা a এবং ৭ এর বদলে যে কোন প্রাইম নিলে ও একই কথা সত্যি হবে। তাই প্রমাণ আসলে হয়ে গেছে।

□

[1]এর অনেকগুলো প্রমাণ আছে। নিজে নিজে কোনটা বের করতে চেষ্টা কর।
[2]এই টেকনিক অনেক জায়গায় কাজে লাগে, এই নোটে ও পরে লাগবে। মাথায় রাখা ভাল
[3]এটা বুঝো কিনা ভাল করে খেয়াল কর। না বুঝলে চিন্তা কর। তাও না বুঝলে পরে জিজ্ঞাসা কর

Bezout's Identity যে কোন দুটি ধনাত্মক পূর্ণসংখ্যা a, b এর জন্য এমন পূর্ণসংখ্যা a আর b থাকবে যাতে

$$ax + by = \gcd(a, b)$$

হয়।

প্রমাণ. যেহেতু a এবং b উভয়ই তাদের গসাগু দিয়ে ভাগ যায়, তাই আমরা $a = \gcd(a, b) \times m, b = \gcd(a, b) \times n$ ধরতে পারি। এখানে m আর n এর সহমৌলিক হতে হবে। কারণ এদের মধ্যে ১ ছাড়া অন্য কিছু যদি কমন থাকে তাহলে ওটা ও গসাগুতে চলে যেত। পুরা সমীকরণকে গসাগু দিয়ে ভাগ করে দিলে,

$$mx + ny = 1$$

তার মানে এখন যদি আমরা প্রমাণ করতে পারি যে সহমৌলিক m, n এর জন্য এমন x, y থাকে তাহলেই প্রমাণ শেষ। আমরা এবার ও আগের ধারণাটাই কাজে লাগাই। খেয়াল করে দেখ, একইভাবে আমরা এটা ও প্রমাণ করতে পারি যে, m আর n যদি সহমৌলিক হয় তাহলে mi কে n দিয়ে ভাগ করলে ভিন্ন ভিন্ন ভাগশেষ দিবে যেখানে $1 \leq i \leq n - 1$। তাহলে নিশ্চয়ই এমন একটি সংখ্যা x থাকবে যাতে করে $m \cdot x$ কে n দিয়ে ভাগ করলে ভাগশেষ ১ হয়। যেমন উপরের উদাহরণে ৪ আর ৭ এর ক্ষেত্রে ৪ এর সাথে ২ কে গুন করলে ভাগশেষ ১ পাওয়া যায়। তখন n দিয়ে $mx - 1$ ভাগ যাবে। আমরা ধরে নেই, $mx - 1 = nz$. এখন যদি $z = -y$ বসানো হয়, তাহলেই প্রমাণ শেষ।

□

[অয়লার ফাংশন] একে ফাই ফাংশন অথবা টোসেন্ট(Totient) ফাংশন ও বলা হয়। n এর ছোট অথবা সমান যতগুলো সংখ্যা n এর সাথে সহমৌলিক সংখ্যা যতগুলি থাকে সে সংখ্যাটাই n এর ফাই ফাংশন। একে $\varphi(n)$ দিয়ে প্রকাশ করা হয়। যেমন, ৬ এর ছোট বা সমান সংখ্যা যেগুলো ৬ এর সাথে সহমৌলিক তারা হল ১ আর ৫। তাই, $\varphi(6) = 2$. একইভাবে, $\varphi(10) = 4$.

[অয়লারের উপপাদ্য] যদি a আর n সহমৌলিক হয় তাহলে,

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

প্রমাণ. এবার ও প্রমাণ আগেরটার মতই। ফার্মার উপপাদ্যে আমরা $1 \cdot 2 \cdots 6$ দিয়ে ভাগ করতে পেরেছিলাম কারণ 7 এর সাথে সহমৌলিক। যেহেতু সহমৌলিক হলে আমরা দুই পক্ষ হতে কেটে দিতে পারি, আমরা শুধু n এর সাথে যারা সহমৌলিক তাদের দিয়ে গুন করবো। যেমন আমরা যদি ১২ নেই তাহলে ১২ এর সাথে সহমৌলিক সংখ্যাগুলো হবে ১,৫,৭,১১। আমরা ১২ এর সাথে সহমৌলিক যে কোন সংখ্যা a দিয়ে গুন করলে ভাগশেষগুলো ভিন্ন হবে তা আমরা প্রমাণ করে ফেলেছি। এবং ভাগশেষগুলো ও হবে আসলে ১,৫,৭,১১ এরাই!! কারণ, যেহেতু ১২ এর সাথে a এবং ১,৫,৭,১১ সহমৌলিক, এদের যে কোনটার সাথে a গুন করে ১২ দিয়ে ভাগ করলে ভাগশেষ ও ১২ এর সাথে সহমৌলিক হবে। তার মানে,

$$a \cdot 1 \cdot a \cdot 5 \cdot a \cdot 7 \cdot a \cdot 11 \equiv 1 \cdot 5 \cdot 7 \cdot 11 \pmod{12}$$

দুইপাশ থেকে $1 \cdot 5 \cdot 7 \cdot 11$ ভাগ করে ফেললে,

$$a^4 \equiv 1 \pmod{12}$$

এখানে a এর পাওয়ার 4 কারণ $\varphi(12) = 4$.

$\square$

উপরের প্রমাণে আমাদের $\varphi(n)$ এর মান কিভাবে বের করতে হয় তা দরকার হয় নি। কিন্তু সমস্যা সমাধান করতে গেলে অনেক সময়ই দরকার হয়। এ জন্য $\varphi(n)$ এর মান বের করার সূত্র আমরা এখানে প্রমাণ ছাড়া সরাসরি ব্যবহার করি।[4]

[মন্তব্য] দেখো, ফার্মার উপপাদ্য আসলে অয়লারের উপপাদ্যের সাধারণ রূপ। অয়লারের উপপাদ্যে $n = p$ একটা প্রাইম বসিয়ে দিলেই হয়। কারণ, $\varphi(p) = p - 1$ যেহেতু, p মৌলিক, এটি এর আগের সব সংখ্যার সাথেই সহমৌলিক.

যদি n এর মৌলিক উৎপাদকে বিশ্লেষণ এমন হয়ঃ

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

তার মানে $p_1, p_2, ..., p_k$ এরা হচ্ছে n এর আলাদা আলাদা প্রাইম ভাজক, এবং $a_1, a_2..., a_k$ এরা হচ্ছে n এ তাদের পাওয়ার। যেমন, $12 = 2^2 \cdot 3^1$ হচ্ছে ১২ এর মৌলিক উৎপাদকে বিশ্লেষণ। তাহলে,

$$\varphi(n) = p_1^{a_1-1}(p_1 - 1) \times p_2^{a_2-1}(p_2 - 1) \cdots p_k^{a_k-1}(p_k - 1)$$

$$\varphi(12) = 2^{2-1}(2-1)3^{1-1}(3-1) = 4$$

1. সমস্যা

আমাদের এই নোটের মূল উদ্দেশ্য আসলে এই উপপাদ্যগুলি শিখানো না, এগুলো কিভাবে সমস্যা সমাধানে কাজে আসে তা দেখা। তাই আগে এগুলো আলোচনা করা হয়েছে।

সমস্যা **1.1**. প্রমাণ কর যে, $2011 | 2^{2010} - 1$. তার মানে, 2011 দিয়ে $2^{2010} - 1$ বিভাজ্য। [5]

Solution. এখানে $2010 = 2011 - 1$, এটা দেখেই ফার্মার উপপাদ্য মাথায় আসার কথা। তাহলে এক লাইনেই প্রমাণ শেষ। কিন্তু না!! তার আগে এটা প্রমাণ করা লাগবে যে ২০১১ একটা মৌলিক সংখ্যা।[6] এ জন্য

---

[4]জানার আগ্রহ হলে এবং না জানা থাকলে কোন ভাইয়ার সাথে যোগাযোগ কর

[5]খেয়াল করে দেখো, তুমি জানো ও না, যে এটা কত বড় সংখ্যা অথচ তুমি এটা জানো যে ২০১১ দিয়ে এটা ভাগ যায়

[6]এটা কি ২০১১ সালে খেয়াল করেছিলে?

২০১১ এর বর্গমূল বা তার চেয়ে ছোট প্রাইম সংখ্যাগুলো দিয়ে ভাগ করে দেখা যায়, যে কোনটা দিয়েই ২০১১ ভাগ যায় না। কিন্তু কোন সংখ্যা মৌলিক না হলে তার অন্তত একটা মৌলিক উৎপাদক থাকে যা তার বর্গমূলের চেয়ে ছোট বা সমান।[7]

সমস্যা **1.2**. প্রমাণ কর যে, $a^5 \equiv 0, \pm 1 \pmod{11}$.

Solution. এটা আমরা চাইলে এভাবে ও প্রমাণ করতে পারিঃ যে কোন সংখ্যাকে ১১ দিয়ে ভাগ করলে ভাগশেষ ০ থেকে ১০ এর মধ্যে থাকে। তখন ভাগশেষগুলোকে পাওয়ারে নিয়ে চেক করে দেখা যায়। কিন্তু যদি আমি ১১ এর জায়গায় ১০০০০০০০০৭(এটা একটা প্রাইম, চেক করে দেখতে পারো :p) দিতাম তাহলে নিশ্চয়ই এই পদ্ধতি আর কাজ করবে না। এখানে ও ফার্মা কাজ করে!! যেহেতু ১১ মৌলিক, আমরা ফার্মার ছোট(!) উপপাদ্য খাটাতে পারি।

প্রথমে, যদি a, 11 দিয়ে ভাগ যায় তাহলে তো $a^5 \equiv 0 \pmod{11}$ পাওয়া যায়। আর তা যদি না হয়, তাহলে a আর 11 সহমৌলিক। সেক্ষেত্রে,

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

একে এভাবে লেখা যায় $11|a^{10} - 1 = (a^5 + 1)(a^5 - 1)$. যেহেতু $a^5 - 1, a^5 + 1$ এর যে কোন একটি ভাগ যাবে।[8] তাহলে আমরা একে লিখতে পারিঃ

$$a^5 \equiv \pm 1 \pmod{11}$$

Solution. উপরের সমস্যাকে সাধারণরূপে লেখলে এভাবে লেখা যায়ঃ

$$a^{\frac{p-1}{2}} \equiv 0, \pm 1 \pmod{p}$$

এটা প্রমাণ করে ফেল।

সমস্যা **1.3**. প্রমাণ কর যে,

$$2013 | 2^{60} - 1$$

Solution. এর সমাধান ও আগেরগুলার মতই। খালি একটু অতিরিক্ত কষ্ট করা লাগবে। আগে এটা খেয়াল কর যে, $2013 = 3 \times 11 \times 61$. আমরা ফার্মার উপপাদ্য থেকে জানি,

$$2^{10} \equiv 1 \pmod{11}$$

যেহেতু অনুসমতা পাওয়ারে তোলা যায়, উভয়পাশে 30 পাওয়ারে তুলে দিলে,[9]

$$2^{60} \equiv 1 \pmod{11}$$

---

[7] এটা আগের কোন একটা নোটে ছিল সম্ভবত, না থাকলে ও ক্ষতি নেই নিজেই প্রমাণ করে নেও। সোজা!!

[8] দুটি একসংগে ভাগ যাবে না। কেন?

[9] এখন মনে হয় বুঝতে পারছো $\varphi(n)$ কেন দরকার। তুমি যদি কোনভাবে 1 ডানে পেয়ে যাও, তাহলে একে যত পাওয়ারেই তুলো, তা 1 এ থাকবে।

$$2^2 \equiv 1 \pmod 3$$
$$2^{60} \equiv 1 \pmod 3$$
$$2^{60} \equiv 1 \pmod{61}$$

এ থেকে লেখা যায়,

$$3, 11, 61 | 2^{60} - 1$$

যেহেতু এরা সবাই একে অন্যের সাথে সহমৌলিক, তাই তাদের লসাগু হচ্ছে তাদের গুনফল। আর কতগুলা সংখ্যা দিয়ে একটি সংখ্যা ভাগ গেলে, সংখ্যাগুলোর লসাগু দিয়ে ও ঐ সংখ্যাটি ভাগ যাবে। তাই, আমরা পাই

$$3 \times 11 \times 61 = 2013 | 2^{60} - 1$$

সমস্যা **1.4**. a যদি ২ এবং ৫ এর সাথে সহমৌলিক কোন সংখ্যা হয় তাহলে প্রমাণ কর যে এমন n আছে যাতে a^n এর দশমিক প্রকাশের শেষে 1 এবং তার আগে $n-1$ টি 0 থাকবে।

Solution. যেহেতু $a, 10$ এর সাথে সহমৌলিক, যে কোন k এর জন্য,

$$a^{\varphi(10^k)} \equiv 1 \pmod{10^k}$$

এর মানে হচ্ছে $a^{\varphi(10^k)} - 1, 10^k$ দিয়ে বিভাজ্য। অর্থাৎ এর শেষের k টি অঙ্ক হবে 0. তাহলে $a^{\varphi(10^n)}$ এর শেষের n টি অঙ্কের মধ্যে $n-1$ টি 0 এবং শেষ অঙ্ক 1 হবে। [10]

সমস্যা **1.5**. এমন সব ধনাত্মক পূর্ণসংখ্যা $n > 12$ বের কর যাতে $n^2 - 27n + 182$ একটি পূর্ণবর্গ হয়।

Solution. এই ধরনের কোন সমস্যা থাকলে সবসময় দেখতে চেষ্টা করবে যে কোন মানের জন্য এটা দুটি ক্রমিক পূর্ণবর্গের মাঝে পড়ে। কারণ দুটি ক্রমিক পূর্ণবর্গের মাঝে কোন পূর্ণবর্গ থাকতে পারে না। তখন তুমি কিছু মান পাবে যেগুলি দিয়ে দেখা লাগবে রাশিটা পূর্ণবর্গ হয় কিনা। এটা কিভাবে করা যায়? আগে নিজে একটু চিন্তা করে দেখো। না পারলে নিচে সমাধান দেখো।

$n^2-27n+182$ এর কাছাকাছি পূর্ণবর্গ $n^2-26n+169 = (n-13)^2$ এবং $n^2-28n+196 = (n-14)^2$. যদি আমরা দেখাতে পারি যে $n > 13$ এর জন্য $n^2-27n+182$ এদের মাঝে থাকে তাহলেই হয়ে যায়। এটা নিজেই দেখাও।

সমস্যা **1.6**. এমন সব ধনাত্মক পূর্ণসংখ্যা b বের কর যাতে $b^2 + b + 1$ একটি পূর্ণবর্গ হয়।

Solution. যদি $b > 0$ হয় তাহলে,

$$b^2 < b^2 + b + 1 < b^2 + 2b = 1 = (b+1)^2$$

সমস্যা **1.7**. এমন সব মৌলিক সংখ্যা p বের কর যাতে হয় এমন অসীম সংখ্যক পূর্ণসংখ্যা a থাকে যাতে $a^p + 1, 6p$ দিয়ে বিভাজ্য হয়, অথবা এমন কোন a থাকে না।

[10]এই সমস্যা Pegion Hole Principle or Box Principle দিয়ে ও সমাধান করা যায়। চেষ্টা কর।

Solution. a^p দেখলেই ফার্মার উপপাদ্যের কথা মনে হওয়ার কথা। আমাদের দরকারঃ

$$a^p + 1 \equiv 0 \pmod{6p}$$

আমাদের শুধু অসীম সংখ্যক a দরকার. ফার্মার উপপাদ্য আমাদের বলে এমন সব a নিতে যাতে $a+1, 6p$ দিয়ে বিভাজ্য হয়(কেন?)। কিন্তু এখন আমরা অন্য একটি সমাধান দেখি।

ফার্মার উপপাদ্য ছাড়া ও অন্যভাবে এটা করা যায়। নীচের সমীকরণটি সব বিজোড় n এর জন্য সত্যঃ

$$a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}\right) \tag{1.1}$$

তার মানে $a^n + b^n, a+b$ দিয়ে বিভাজ্য যদি n বিজোড় হয়।[11] এখন আমরা ধরে নেই যে p একটি বিজোড় মৌলিক সংখ্যা। তাহলে, $a^p + 1, a+1$ দিয়ে বিভাজ্য। তাই আমরা যদি শুধু a কে এমনভাবে নেই যাতে $a+1, 6p$ দিয়ে বিভাজ্য হয় তাহলে a^p+1 ও $6p$ দিয়ে বিভাজ্য হবে। যেহেতু আমরা নিজের মত করে a নিতে পারি, ধরে নেই $a+1 = 6kp$. এখানে k এর মান ১,২,৩,... এভাবে অসীম সংখ্যক হতে পারে। তাই এক্ষেত্রে অসীম সংখ্যক সমাধান থাকবে। এখন শুধু জোড় মৌলিক সংখ্যা অর্থাৎ $p = 2$ এর ক্ষেত্রে দেখানো বাকি। তখন আমাদের লাগবেঃ $a^2 + 1, 12$ দিয়ে বিভাজ্য। তাহলে a কে অবশ্যই বিজোড় হতে হবে। কিন্তু আমরা জানি যে বিজোড় সংখ্যার বর্গকে ৪ দিয়ে ভাগ করলে ভাগশেষ ১ হয়। তাই a^2+1 কে 4 দিয়ে ভাগ করলে ভাগশেষ হবে $1+1=2$, যা বুঝায় এটা 4 দিয়ে ভাগ যায় না। কিন্তু ১২ দিয়ে ভাগ যেতে হলে একে ৪ দিয়ে ভাগ যেতে হবে। তাই, এক্ষেত্রে কোন সমাধান থাকবে না।

সমস্যা **1.8**. যদি $m|n$ হয় তাহলে $a^m - 1|a^n - 1$.

Solution. এটা আসলে আগের সমীকরণ ব্যবহার করেই দেখানো যায়। যেহেতু $m|n, n = mk$ লেখা যায়।

$$\begin{aligned} a^n - 1 &= a^{mk} - 1 \\ &= (a^m)^k - 1 \end{aligned}$$

যা $a^m - 1$ দিয়ে বিভাজ্য।

সমস্যা **1.9**. এটা হচ্ছে আগেরটার উলটা সমস্যা। যদি $a^m - 1$ দিয়ে $a^n - 1$ বিভাজ্য হয়, তাহলে n ও m দিয়ে বিভাজ্য।

Solution. এটার জন্য আমরা আগের তথ্যটাই বারবার ব্যবহার করবো। আগে নিজে হাতে কিছুক্ষন করে দেখো।

আমরা জানি, যে $a|bc$ আর a, b এর সাথে সহমৌলিক হলে $a|c$. আবার $a|b, a|c$ হলে $a|b-c$.

$$a^m - 1|a^n - 1 \Longrightarrow a^m - 1|a^n - 1 - (a^m - 1) = a^n - a^m = a^m(a^{n-m} - 1)$$

[11] দেখাও যে, সকল n এর জন্য $a^n - b^n, a - b$ দিয়ে বিভাজ্য। $a^n - b^n = (a-b)S$ হলে $S = ?$ এটা ও অনেক কাজের জিনিস।

যেহেতু $a^m - 1$ দিয়ে a^m কে ভাগ করলে ভাগশেষ ১ থাকে, তাই এরা পরস্পর সহমৌলিক। তাহলে $a^m - 1|a^{n-m} - 1$. যদি এর পরে আমরা আবার $a^m - 1$ বিয়োগ করে a^m কমন নেই, তাহলে $a^m - 1|a^{n-2m} - 1$. কথা হচ্ছে, আমরা এভাবে কতদূর যেতে পারবো? যদি m দিয়ে n কে ভাগ করলে ভাগফল q আর ভাগশেষ r হয় তাহলে $n = mq + r$. এবং আমরা বলতে পারি,

$$a^m - 1|a^{mq} - 1$$

তাহলে,

$$a^m - 1|a^n - a^{mq} = a^{mq}(a^r - 1) \implies a^m - 1|a^r - 1$$

কিন্তু r, m এর চেয়ে ছোট, কারণ এ হচ্ছে ভাগশেষ। তাই, $a^r - 1 < a^m - 1$. কিন্তু এটা সম্ভব না যদি $a^r - 1 = 0$ হয়। তখন আমরা পাবো $r = 0$. তার মানে, $n = mq \implies m|n$.

■

সমস্যা **1.10**. নিজে করঃ এমন সব ধনাত্মক পূর্ণসংখ্যা a, m, n বের কর যাতে $a^m - 1|a^n + 1$.

সমস্যা **1.11**. এমন সব সহমৌলিক a, b বের কর যাতে জোড় n এর জন্য $a + b|a^n + b^n$.

সমস্যা **1.12**. সিকিনিয়া নামে কোন এক অদ্ভুত দেশে শুধু ২০১১ টাকা এবং ২০১৩ টাকার নোট পাওয়া যায়। ওরা কি যে কোন পরিমাণের টাকা আদান-প্রদান করতে পারবে?

Solution. এটা Bezout's Identity'র বেশ ভাল একটি প্রয়োগ, এবং বেশ মজার একটি সমস্যা। এখানে খেয়াল করে দেখো তুমি ২০১১ টাকা এবং ২০১৩ টাকা দিয়ে n দিতে পারবে যদি $n = 2011x + 2013y$ হিসেবে লিখতে পারো। কারণ আশা করি বুঝে ফেলেছো। এখানে x, y ধনাত্মক, ঋণাত্মক বা শূন্য হতে পারে। ধনাত্মক মানে তুমি ওই নোটটি নিবে, আর ঋণাত্মক মানে তুমি দিবে। যদি এভাবে তুমি এমন x আর y খুঁজে পেতে পারো যাতে তুমি x টি ২০১১ টাকার নোট আর y টি ২০১৩ টাকার নোট দিয়ে বা নিয়ে মোট n টাকা বানাতে পারো, তাহলেই হয়ে যায়।

ক্রুশিয়াল আইডিয়াঃ ২০১১ আর ২০১৩ সহমৌলিক। তাহলে Bezout's Theorem অনুযায়ী এমন পূর্ণসংখ্যা s, t থাকবে যাতে

$$2011s + 2013t = \gcd(2011, 2013) = 1$$

তার মানে তুমি ২০১১ টাকা আর ২০১৩ টাকার নোট ব্যবহার করে ১ টাকা দিতে পারবে। তখন ১ টাকার n টি নোট ব্যবহার করে n টাকা আদান-প্রদান করতে পারবে। তার মানে,

$$2011sn + 2013tn = n$$

এখন যদি আমরা $sn = x, tn = y$ ধরি তাহলেই সমাধান হয়ে যায়। আমরা আদান-প্রদান করার উপায় পেয়ে গেছি।

সমস্যা **1.13**. এবার নিজে নিজে এটা দেখাও যে, উপরের সমস্যায় তুমি চাইলে অসীম সংখ্যক উপায়ে এই আদান-প্রদান করতে পারবে।

সমস্যা **1.14**. উপরের সমস্যায় যদি বলা হয় শুধু ২০১৩ আর ২০১০ টাকার নোটই পাওয়া যায় তাহলে কি তুমি যে কোন টাকা পরিশোধ করতে পারবে? না পারলে কেন? আর n এর মান কত হলে তুমি পরিশোধ করতে পারবে?

সমস্যা **1.15**. আগেই বলে দেই, এ সমস্যাটি Bezout's Identity দিয়ে সমাধান করা যায়।
যদি $a^p \equiv b^p \pmod n, a^q \equiv b^q \pmod n$ হয় তাহলে প্রমাণ কর যে,

$$a^{\gcd(p,q)} \equiv b^{\gcd(p,q)} \pmod n$$

Hint. অনুসমতা গুন করা এবং পাওয়ারে তোলা যায়।

অনেক সমস্যায় কিছু বিশেষ ধরনের আইডিয়া কাজে লাগাতে হয়। যেমন, $a|b$ হলে b, a এর সবগুলো মৌলিক উৎপাদক দিয়ে ও বিভাজ্য। অর্থাৎ, $p|a$ হলে $p|b$. একে দেখতে নিরীহ মনে হলেও অনেক সমস্যায়ই দরকার হয়। বিশেষ করে, প্রায়ই a এর সবচেয়ে ছোট মৌলিক উৎপাদক নিতে হয়(কেন বুঝতে হলে নীচের সমস্যাটি দেখো)।

সমস্যা **1.16**. এমন সব ধনাত্মক পূর্ণসংখ্যা n বের কর যাতে $n|2^n - 1$.

Solution. n স্পষ্টতই বিজোড় হতে হবে। আমরা দেখাবো যে $n = 1$ ছাড়া আর কোন সমাধান নেই।[12]
আমরা ধরে নেই যে, n এর সবচেয়ে ছোট মৌলিক উৎপাদক p। তাহলে, $p|2^n - 1$.

$$2^n \equiv 1 \pmod p$$

এখন, ফার্মার উপপাদ্য অনুযায়ী,

$$2^{p-1} \equiv 1 \pmod p$$

উপরের সমস্যা অনুযায়ী,

$$2^{\gcd(n,p-1)} \equiv 1 \pmod p$$

এখানে p এর ছোট সব সংখ্যাই n এর সাথে সহমৌলিক। কারণ, তা না হলে যদি এমন কোন সংখ্যা থাকে যা p এর ছোট এবং n এর সাথে সহমৌলিক নয়, তাহলে ওই সংখ্যার একটি মৌলিক উৎপাদক থাকবে যা p এর চেয়ে ছোট এবং n কে ভাগ করে। কিন্তু p এর চেয়ে ছোট কোন মৌলিক উৎপাদক থাকা সম্ভব না।[13] তাহলে, $\gcd(n, p-1) = 1$.

$$2^1 \equiv 1 \pmod p \Rightarrow p|2 - 1 = 1$$

কিন্তু যে কোন মৌলিক সংখ্যাই ১ এর চেয়ে বড়। তাই এমন কোন মৌলিক সংখ্যাই আসলে পাওয়া যাবে না যা n কে ভাগ করে। সুতরাং, এটাই একমাত্র সমাধান।

সমস্যা **1.17**. যদি $n > 1$ বিজোড় হয়, তাহলে দেখাও যে,

$$n \nmid 3^n + 1$$

[12]তোমার এখন মনে হতে পারে যে, আমি কিভাবে বুঝবো এর সমাধান এটাই হতে পারে? আসলে বুঝার দরকার নেই। চিন্তা করে সমস্যা সমাধান করতে থাক, এক সময় তুমিই দেখলেই বলতে পারবে।

[13]এখন বুঝতে পারার কথা বিশেষ করে সবচেয়ে ছোটটা কেন স্পেশাল।

Solution. এবার ও n এর সবচেয়ে ছোট মৌলিক উৎপাদক নেই p. তাহলে p বিজোড় এবং যেহেতু এ দিয়ে $3^n + 1$ কে ভাগ করলে ভাগশেষ ১ থাকে, p এর মান ৩ হওয়া সম্ভব না। সেক্ষেত্রে,

$$3^{p-1} \equiv 1 \pmod p$$

$$3^n \equiv -1 \pmod p \Rightarrow 3^{2n} \equiv 1 \pmod p$$

$$3^{\gcd(p-1,n)} \equiv 1 \pmod p$$

যেহেতু $p - 1$ জোড় এবং $\gcd(n, p-1) = 1, \gcd(2n, p-1) = 2$. এ থেকে বলা যায়, $3^2 \equiv 1 \pmod p \Rightarrow p | 3^2 - 1 \Rightarrow p = 2$, যা সম্ভব নয়। এবার ও আগের মতই কোন মান পাওয়া যাবে না।

সমস্যা **1.18**. এমন সব মৌলিক সংখ্যা p এবং ধনাত্মক পূর্ণসংখ্যা a, b বের কর যাতে $p^a + p^b$ একটি পূর্ণবর্গ হয়।

Solution. এ সমস্যায় কয়েকটি ভাল আইডিয়া কাজে লাগে।

1. যদি দুটি সংখ্যার গুনফল পূর্ণবর্গ হয় এবং তারা সহমৌলিক হয়, তাহলে তারা নিজেরা পূর্ণবর্গ হবে।

2. কোথাও যদি সিমেট্রি পাওয়া যায় তাহলে তাদের ছোট থেকে বড় হিসেবে নিজের মত করে সাজিয়ে নেওয়া যায়। যেমন, $a + b = 12$ হলে (a, b) এর জায়গায় (b, a) বসালে ও একই থাকে। মানে রাশিটি a, b এর সাপেক্ষে সিমেট্রিক। এদের মধ্যে যে কোন একটি বড় হবে আরেকটি ছোট হবে। আমরা ধরে নিতে পারি যে, $a \geq b$.

3. ডায়োফ্যান্টাইন সমীকরণ সমাধান করা।

এখানে ও রাশিটি a, b এর সাপেক্ষে সিমেট্রিক। তাই আমরা ধরে নেই, $a \geq b$. যদি $a = b$ হয় তাহলে, $2p^a$ পূর্ণবর্গ হবে। যেহেতু এটি জোড়, তাই ৪ দিয়ে ভাগ যায়। সেজন্য, $p = 2$ হতে হবে। এখন আমরা ধরে নিতে পারি $a > b, a = b + k$.

$$p^a + p^b = p^b(p^k + 1)$$

এখানে p দিয়ে $p^k + 1$ কে ভাগ করলে ভাগশেষ ১। তাই, $p^k + 1$ আর p^b সহমৌলিক। p^b এবং $p^k + 1$ উভয়ই পূর্ণবর্গ। যার অর্থ হচ্ছে, b জোড় অর্থাৎ $b = 2l$. এখন আমাদের বের করতে হবে $p^k + 1$ কখন পূর্ণবর্গ হয়। আমরা ধরে নেই,

$$p^k + 1 = x^2$$

$$(x+1)(x-1) = p^k$$

এর মানে হচ্ছে $x + 1$ এবং $x - 1$ এ p ছাড়া আর কোন মৌলিক উৎপাদক থাকবে না। তাই $x + 1 = p^m, x - 1 = p^n$ ধরে নেওয়া যায় যেখানে $m > n \geq 0$.

$$p^m - p^n = 2$$

যদি $n = 0$ হয় তাহলে, $x - 1 = 1 \Rightarrow x = 2$. তা না হলে, $p^n(p^{m-n} - 1) = 2$ যা থেকে বলা যায়, $p = 2, n = 1, p^{m-n} - 1 = 1$ হতে হবে। এ থেকে $m = 2$.

সমস্যা **1.19**. $n(n+1) = m^2$ সমীকরণের সব পূর্ণসংখ্যায় সমাধান বের কর।

Solution. এখানে $\gcd(n, n+1) = 1$. তাই n এবং $n+1$ উভয়ই পূর্ণবর্গ। সেজন্য $n = x^2, n+1 = y^2 \Rightarrow y^2 - x^2 = 1 \Rightarrow (x + y(x-y) = 1 \Rightarrow x + y = 1, x - y = 1$. যার মানে, $x = 1, y = 0, n = 0$.

সমস্যা **1.20**. এবার $n(n+1)(n+2) = m^2$.

Solution. এটাকে কোন ভাবে আগের মত দুটি সহমৌলিক সংখ্যার গুনফল হিসেবে লেখা গেলে সোজা হয়ে যায়। তাই আমরা এভাবে লিখতে চেষ্টা করি।

$$(n^2 + 2n)(n+1) = m^2$$

$$\Rightarrow (n+1)\left((n+1)^2 - 1\right) = m^2$$

এখন $n+1$ আর $(n+1)^2 - 1$ সহমৌলিক। আবার আগের মত করে শেষ কর।

সমস্যা **1.21**. $a_n = 6^n + 8^n$ হলে a_{48} কে 49 দিয়ে ভাগ করলে ভাগশেষ থাকবে?

Hint. ফাই ফাংশন ব্যবহার কর। $6, 8$ উভয়ই 49 এর সাথে সহমৌলিক।

সমস্যা **1.22**. প্রমাণ কর যে, p একটি মৌলিক সংখ্যা আর $0 < i < p$ একটি পূর্ণসংখ্যা হলে

$$p | \binom{p}{i}$$

যেখানে

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Solution. এখানে আমরা একটি গুরুত্বপূর্ণ আইডেনটিটি দেখি।

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$$

এ থেকে,

$$i\binom{p}{i} = p\binom{p-1}{k-1}$$

সুতরাং, $p | i\binom{p}{i}$. কিন্তু $\gcd(p, i) = 1$. তাই,

$$p | \binom{p}{i}$$

সমস্যা **1.23**. উপরের আইডেন্টিটি ব্যবহার করেই দেখাও,

$$i|\binom{p-1}{i-1}$$

সমস্যা **1.24**. দেখাও যে, Bezout's Identity এর উল্টাটা ও সত্যি। যদি

$$ax + by = 1$$

হয় তাহলে a আর b সহমৌলিক।

সমস্যা **1.25** (IMO 1959, Problem 1). দেখাও যে, $\dfrac{21n+4}{14n+3}$ ভগ্নাংশটিকে n এর কোন মানের জন্যই ছোট করা যাবে না।

Solution. আমরা যদি দেখাতে পারি যে, সব n এর জন্যই $21n+3$ এবং $14n+4$ সহমৌলিক। এজন্য আমরা ভাগ পদ্ধতিতে গসাগু বের করে দেখাতে পারি। আবার উপরের সমস্যার মত করেই প্রমাণ করতে পারি।

$$3(14n+3) - 2(21n+4) = 1$$

অর্থাৎ $\gcd(14n+3, 21n+4) = g$ হলে $g|1 \Rightarrow g = 1$.(কেন?)

সমস্যা **1.26** (USAMO, 1979).

$$n_1^4 + n_2^4 + \ldots + n_{14}^4 = 1599$$

Solution. এখানে ভ্যারিয়েবল আছে ১৪ টা। আমরা সাধারণত দেখি যে যতগুলি চলক থাকে ততগুলি সমীকরণ লাগে সমাধানের জন্য। কিন্তু এর সমাধান কিভাবে বের করা যায়? দেখে একটু আন্দাজ করতে পারার কথা যে আসলে এর কোন সমাধান নেই। কিন্তু এটা কিভাবে প্রমাণ করবো? আমরা দেখাবো এই সমীকরণের দুই পাশে একই সংখ্যা দিয়ে ভাগ করলে ভিন্ন ভাগশেষ পাওয়া যায়, যা আসলে সম্ভব না। কিন্তু এই সংখ্যাটি কিভাবে নেওয়া যায়? এটা সমস্যার উপরে নির্ভর করে। এবং এই পদ্ধতিতে অনেক সমীকরণেরই সমাধান নেই বলে প্রমাণ করা যায়। শুধু সংখ্যাটি ঠিক মত বাছাই করতে হয়। এই জন্য নিচের অনুসমতাগুলো অনেক কাজে দেয়ঃ

1. $x^2 \equiv 0, 1 \pmod{3, 4}$.
2. $x^2 \equiv 0, 1, 4 \pmod{8}$.
3. $x^3 \equiv 0, \pm 1 \pmod{9}$.
4. $x^4 \equiv 0, 1 \pmod{16}$.
5. $x^5 \equiv 0, \pm 1 \pmod{11}$.

6. $x^{\frac{p-1}{2}} \equiv 0, \pm 1 \pmod p$ যেখানে p একটি মৌলিক সংখ্যা. এটা আগে আমরা প্রমাণ করে এসেছি।
[14]

তাহলে এই সমস্যায় কোনটা দরকার? অবশ্যই $\#4$. এটা কাজে লাগিয়ে, $n_1, n_2, \ldots, n_{14}$ এর যে কোন একটি n_i এর জন্য,

$$n_i^4 \equiv 0, 1 \pmod{16}$$

তাহলে, বামপাশে আমরা সর্বোচ্চ ভাগশেষ পেতে পারি 14(যখন সবগুলিই ভাগশেষ ১ করে দিবে) কিন্তু ডানপাশে ১৫৯৯ কে ১৬ দিয়ে ভাগ করলে ভাগশেষ ১৫। যা কোন ভাবেই পাওয়া সম্ভব না। তাই এই সমীকরণের কোন সমাধান নেই।

[14]এগুলো নিজেই প্রমাণ করে ফেল।