↳ **Fundamental theorem of arithmetic**: for any integer $n \geq 2$, one can write $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ where p_i are distinct primes and $s_i \geq 1 \; \forall \, 1 \leq i \leq k$. This is unique up to reordering.

↳ the number of positive divisors of n is $\prod_{i=1}^{k} (a_i + 1)$

↳ $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k} \Rightarrow \gcd(m,n) = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where $e_i = \min(a_i, b_i)$
$\operatorname{lcm}(m,n) = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ where $f_i = \max(a_i, b_i)$

- There are infinitely many primes
- There are infinitely primes p such that $p+2$ is also prime.

Congruences

→ a is **congruent** to b modulo m if $m \mid (a-b)$

↳ $a \equiv b \bmod n \iff b \equiv a \bmod n \iff a - b \equiv 0 \bmod n$

↳ if $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$

↳ if $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$ and $ax + cy \equiv bx + dy \bmod n$ for $x, y \in \mathbb{Z}$

↳ if $a \equiv b \bmod n$ and $d \mid n$, then $a \equiv b \bmod d$

↳ if $a \equiv b \bmod n$ and $c \neq 0$, then $ac \equiv bc \bmod n$

→ A set $\{x_1, \dots, x_r\}$ is a **complete residue system** mod n if for every integer y, there's exactly one x_i such that $y \equiv x_i \bmod n$

↳ The residue class of a is the set $[a]_n = \{b \in \mathbb{Z} : b \equiv a \bmod n\}$

↳ $[a]_n = [b]_n \iff a \equiv b \bmod n$

↳ $[a]_n + [b]_n = [a+b]_n$

↳ $[a]_n \cdot [b]_n = [ab]_n$

↳ Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$ be a polynomial $\in \mathbb{Z}[x]$. If $a \equiv b \bmod n$, then $f(a) \equiv f(b) \bmod n$

↳ **Chinese Remainder Theorem**: Let p, q, r be pairwise coprime integers. The solution of the system of congruence equations

$$x = a_1 \bmod p \qquad x = a_2 \bmod q \qquad x = a_3 \bmod r$$

is given by

$$x = qr\,[qr]_p^{-1} a_1 + pr\,[pr]_q^{-1} a_2 + pq\,[pq]_r^{-1} a_3 \bmod pqr$$

Worked solution:

Let $f(x) = x^3 + x^2 + x \pmod{105}$ → $105 = 5 \cdot 7 \cdot 3$ $\quad [5\cdot 7]_3^{-1} = 2$; $[3\cdot 7]_5^{-1} = 1$; $[3\cdot 5]_7^{-1} = 1$

solve $f(x) \equiv 0 \bmod 3, 7, 5$

mod 3: $f(-1) = -1 \not\equiv 0 \bmod 3$, $f(0) = 0 \bmod 3$, $f(1) = 0 \bmod 3$ } $x = 0, 1 \bmod 3$

mod 5: $f(-2) = -1 \not\equiv 0 \bmod 5$, $f(-1) = -1 \not\equiv 0 \bmod 5$, $f(0) = 0 \bmod 5$, $f(1) = 3 \not\equiv 0 \bmod 5$, $f(2) = -1 \not\equiv 0 \bmod 5$ } $x \equiv 0 \bmod 5$

mod 7: $f(-3) = 0 \bmod 7$, $f(-2) = 1 \bmod 7$, $f(-1) = -1 \bmod 7$, $f(0) = 0 \bmod 7$, $f(1) = 3 \not\equiv 0 \bmod 7$, $f(2) = 0 \bmod 7$, $f(3) = 4 \not\equiv 0 \bmod 7$ } $x = 0, 2, -3 \bmod 7$

$x = a_1 \cdot 35 \cdot 2 + a_2 \cdot 21 \cdot 1 + a_3 \cdot 15 \cdot 1 \bmod 105$

$a_1 \in \{0,1\}, a_2 \in \{0\}, a_3 \in \{0, 2, -3\}$

↳ 6 solutions