Math 100 Tricks with Professor Sucharit Sarkar

Brendan Connelly

September to December 2024

Introduction

Definition (Mathematical Induction (Weak Induction))**.** Let $P(n)$ be a statement about an integer n. The principle of *mathematical induction* states that if the following two conditions are satisfied:

(i) **Base case:** $P(n_0)$ is true for some initial integer n_0,

(ii) **Inductive step:** For all $n \geq n_0$, if $P(n)$ is true, then $P(n+1)$ is also true,

then $P(n)$ is true for all integers $n \geq n_0$.

Definition (Strong Induction)**.** Let $P(n)$ be a statement about an integer n. The principle of *strong induction* states that if the following two conditions are satisfied:

(i) **Base case:** $P(n_0)$ is true for some initial integer n_0,

(ii) **Inductive step:** For all $n \geq n_0$, if $P(k)$ is true for all $k \leq n$, then $P(n+1)$ is also true,

then $P(n)$ is true for all integers $n \geq n_0$.

Theorem (Bertrand's Postulate)**.** Bertrand's Postulate states that for every integer $n \geq 2$, there exists at least one prime number p such that

$$n < p < 2n.$$

In other words, for any $n \geq 2$, there is always a prime number between n and $2n$.

Definition (Fibonacci Sequence)**.** The Fibonacci sequence is a sequence of numbers where the first two numbers are defined as $F_0 = 1$ and $F_1 = 1$, and each subsequent number is the sum of the previous two numbers, i.e.,

$$F_n = F_{n-1} + F_{n-2} \quad \text{for} \quad n \geq 2.$$

Theorem (Fibonacci Identity)**.** For all natural numbers n, the following identity holds:

$$F_{2n+1} = F_{n+1}^2 + F_n^2.$$

Theorem (Euler's Formula for Planar Connected Graphs)**.** Let G be a connected planar graph with V vertices, E edges, and F faces (including the outer, infinite face). Euler's Formula states that

$$V - E + F = 2.$$

Proof by Induction:
We will prove Euler's Formula using mathematical induction on the number of edges E in the graph G.
Base Case: $E = V - 1$
When $E = V - 1$, the graph G is a **tree**. A tree is a connected graph with no cycles. For a tree:

$$F = 1 \quad \text{(only the outer face)}.$$

Plugging into Euler's Formula:

$$V - E + F = V - (V - 1) + 1 = 2.$$

Thus, the base case holds.
Inductive Step:
Assume that Euler's Formula holds for all connected planar graphs with E edges, i.e.,

$$V - E + F = 2.$$

Now, consider a connected planar graph G' with $E' = E + 1$ edges.
There are two possibilities for G':

1. **Adding an Edge That Does Not Create a Cycle:**

   Adding an edge to G that does not form a cycle increases the number of edges by 1 and the number of faces by 1 (since a new face is created). Thus:

   $$V' = V, \quad E' = E + 1, \quad F' = F + 1.$$

   Plugging into Euler's Formula:

   $$V' - E' + F' = V - (E + 1) + (F + 1) = V - E + F = 2.$$

   The formula still holds.

2. **Adding an Edge That Creates a Cycle:**

   Adding an edge that forms a cycle does not change the number of faces. In this case:

   $$V' = V, \quad E' = E + 1, \quad F' = F.$$

   However, since a cycle is formed, we have:

   $$V' - E' + F' = V - (E + 1) + F = (V - E + F) - 1 = 2 - 1 = 1,$$

   which does not satisfy Euler's Formula. **This scenario cannot occur in a tree** because trees do not contain cycles. Therefore, to maintain the inductive hypothesis, we consider only the addition of edges that do not create cycles.

To resolve the discrepancy in the second case, we refine our approach by ensuring that every added edge maintains the property $V - E + F = 2$. This is achieved by only considering the addition of edges that either:

- Increase the number of faces by 1 without creating a cycle, or
- Close a cycle in a way that the overall balance $V - E + F$ remains unchanged.

Alternatively, a more streamlined inductive approach involves removing an edge that is part of a cycle:

2. **Removing an Edge from a Cycle:**
   Suppose G' has a cycle. Remove an edge e from this cycle to obtain a new graph G with:
   $$V' = V, \quad E = E' - 1, \quad F = F' - 1.$$
   Since e was part of a cycle, removing it reduces the number of edges by 1 and the number of faces by 1. Applying Euler's Formula to G:
   $$V - E + F = 2.$$
   Therefore, for G':
   $$V' - E' + F' = V - (E - 1 + 1) + (F - 1 + 1) = V - E + F = 2.$$
   Hence, Euler's Formula holds for G'.

Thus, by induction, Euler's Formula $V - E + F = 2$ holds for all connected planar graphs.

Theorem (Pigeonhole Principle)**.** The Pigeonhole Principle states that if $nk + 1$ objects are placed into k containers, then at least one container must contain at least $n + 1$ objects.

Proof: Assume there are $nk+1$ objects and k containers. If each container could hold at most n objects, the total number of objects would be at most nk. Since there are $nk + 1$ objects, which is greater than nk, it follows that at least one container must contain more than n objects, i.e., at least $n + 1$ objects.

Inequalities

Theorem (Arithmetic Mean-Geometric Mean Inequality (AM-GM))**.** For any set of non-negative real numbers $a_1, a_2, \ldots, a_n$, the arithmetic mean is always greater than or equal to the geometric mean. Specifically,
$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n},$$
with equality if and only if $a_1 = a_2 = \cdots = a_n$.

Theorem (Weighted AM-GM Inequality)**.** For any set of non-negative real numbers $a_1, a_2, \ldots, a_n$ and corresponding non-negative weights $w_1, w_2, \ldots, w_n$, the following inequality holds:
$$\frac{w_1 a_1 + w_2 a_2 + \cdots + w_n a_n}{w_1 + w_2 + \cdots + w_n} \geq (a_1^{w_1} a_2^{w_2} \cdots a_n^{w_n})^{\frac{1}{w_1 + w_2 + \cdots + w_n}},$$
with equality if and only if $a_1 = a_2 = \cdots = a_n$.

Proof Summary:

1. **Base case (P(2)):** The inequality holds for $n = 2$, where it simplifies to $\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$. This can be proven by considering the non-negativity of squared differences.

2. **Inductive Step 1: From $P(n)$ to $P(2n)$:** Assuming the inequality holds for n, we prove it for $2n$ by applying the AM-GM inequality to two groups of n numbers, and then combining the results.

3. **Inductive Step 2: From $P(n)$ to $P(n-1)$:** The inequality for $n-1$ can be derived by adding a zero or a very small number to the set and applying the inequality for n, then letting the added number tend to zero.

4. **Extension to rationals:** The inequality for rational numbers is obtained by considering rational approximations of real numbers and applying the inequality for integer n.

5. **Extension to reals:** Extending to real numbers is achieved by taking limits, using the continuity of the arithmetic and geometric mean functions.

6. **Extension to weighted case:** The weighted AM-GM inequality is derived by reducing the weighted case to an unweighted form through partitioning the numbers according to their weights.

7. **Extension to weighted rationals and reals:** The weighted version is extended to rationals and reals similarly to the unweighted case, using rational approximations and taking limits.

Theorem (Jensen's Inequality (not in class in this form))**.** Let f be a concave function defined on an interval, and let $x_1, x_2, \ldots, x_n$ be points in this interval. For any non-negative weights $p_1, p_2, \ldots, p_n$ such that $p_1 + p_2 + \cdots + p_n = 1$, Jensen's inequality states that

$$f\left(\sum_{i=1}^{n} p_i x_i\right) \geq \sum_{i=1}^{n} p_i f(x_i).$$

Equality holds if $x_1 = x_2 = \cdots = x_n$ or if f is affine on the interval.

Theorem (Functional Weighted AM-GM Inequality)**.** Let f be a continuous, concave function on an interval that contains the points $x_1, x_2, \ldots, x_n$. For non-negative weights $p_1, p_2, \ldots, p_n$, the following inequality holds:

$$f\left(\frac{p_1 x_1 + p_2 x_2 + \cdots + p_n x_n}{p_1 + p_2 + \cdots + p_n}\right) \geq \frac{p_1 f(x_1) + p_2 f(x_2) + \cdots + p_n f(x_n)}{p_1 + p_2 + \cdots + p_n},$$

with equality if $x_1 = x_2 = \cdots = x_n$ or if f is affine over the given interval.
This inequality follows directly from Jensen's inequality for concave functions. Furthermore, this functional inequality generalizes the AM-GM inequality: by choosing $f(x) = \ln(x)$, which is concave, we recover the AM-GM inequality. Specifically, applying ln to the terms of the AM-GM inequality transforms it into a form where Jensen's inequality can be applied.

Definition (Weighted k-th Power Mean)**.** Let $a_1, a_2, \ldots, a_n$ be non-negative real numbers, and let $p_1, p_2, \ldots, p_n$ be non-negative weights. The weighted k-th power mean M_k is defined as

$$M_k(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n) = \left(\frac{\sum_{i=1}^{n} p_i a_i^k}{\sum_{i=1}^{n} p_i}\right)^{\frac{1}{k}},$$

for any real number $k \neq 0$. When $k = 0$, the weighted mean is defined as the geometric mean:

$$M_0(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n) = \prod_{i=1}^{n} a_i^{\frac{p_i}{\sum_{i=1}^{n} p_i}}.$$

Additionally, the following special cases hold:

- When $k = \infty$, the weighted power mean represents the maximum value of the elements:

$$M_\infty(a_1, a_2, \ldots, a_n) = \max(a_1, a_2, \ldots, a_n).$$

- When $k = -\infty$, the weighted power mean represents the minimum value of the elements:

$$M_{-\infty}(a_1, a_2, \ldots, a_n) = \min(a_1, a_2, \ldots, a_n).$$

Examples:

1. *Harmonic Mean* ($k = -1$):

$$M_{-1}(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n) = \frac{\sum_{i=1}^n p_i}{\sum_{i=1}^n \frac{p_i}{a_i}} = \frac{p_1 + p_2 + \cdots + p_n}{\frac{p_1}{a_1} + \frac{p_2}{a_2} + \cdots + \frac{p_n}{a_n}}.$$

2. *Quadratic Mean* ($k = 2$):

$$M_2(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n) = \sqrt{\frac{\sum_{i=1}^n p_i a_i^2}{\sum_{i=1}^n p_i}} = \sqrt{\frac{p_1 a_1^2 + p_2 a_2^2 + \cdots + p_n a_n^2}{p_1 + p_2 + \cdots + p_n}}.$$

Theorem (Monotonicity of Power Means)**.** Let $a_1, a_2, \ldots, a_n$ be non-negative real numbers, and let $p_1, p_2, \ldots, p_n$ be non-negative weights such that $p_1 + p_2 + \cdots + p_n = 1$. For any real numbers $k_1 \leq k_2$, the corresponding weighted power means satisfy

$$M_{k_1}(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n) \leq M_{k_2}(a_1, a_2, \ldots, a_n; p_1, p_2, \ldots, p_n).$$

Equality holds if and only if $a_1 = a_2 = \cdots = a_n$.

Theorem (Mean Value Theorem (MVT))**.** Let f be a function that is continuous on the closed interval $[x, x + h]$ and differentiable on the open interval $(x, x + h)$. Then there exists some $y \in (x, x + h)$ such that

$$f(x + h) = f(x) + hf'(y).$$

Theorem (Taylor Expansion with Remainder)**.** Let f be n-times differentiable on an interval containing $[x, x + h]$. Then, using the Taylor expansion with the remainder term in Lagrange form, we have:

$$f(x + h) = f(x) + \frac{h}{1!}f'(x) + \frac{h^2}{2!}f''(x) + \cdots + \frac{h^{n-1}}{(n-1)!}f^{(n-1)}(x) + \frac{h^n}{n!}f^{(n)}(y),$$

for some $y \in (x, x + h)$.

Explanation:

- The expression $f(x + h) = f(x) + hf'(y)$ from the Mean Value Theorem (MVT) is essentially the first-order Taylor approximation with a remainder involving $y \in (x, x + h)$.
- The Taylor expansion generalizes this by expanding $f(x + h)$ to a higher degree, with the remainder involving a higher-order derivative evaluated at some point $y \in (x, x + h)$.
- If $f^{(n)} \geq 0$ for all x, it implies that the function grows at a non-decreasing rate, which can be used to establish bounds on $f(x + h)$ based on the Taylor expansion.

Theorem (Cauchy-Schwarz Inequality)**.** The Cauchy-Schwarz inequality is a fundamental inequality in linear algebra and analysis. It can be written in several equivalent forms.

General Form: For any real or complex vectors $\vec{a} = (a_1, a_2, \ldots, a_n)$ and $\vec{b} = (b_1, b_2, \ldots, b_n)$, the following inequality holds:

$$\left(\sum_{i=1}^n a_i b_i\right)^2 \leq \left(\sum_{i=1}^n a_i^2\right)\left(\sum_{i=1}^n b_i^2\right).$$

Inner Product Form: For vectors $\vec{a}, \vec{b} \in \mathbb{R}^n$ or $\mathbb{C}^n$, the inequality can be stated in terms of the inner product:

$$|\langle \vec{a}, \vec{b} \rangle|^2 \leq \langle \vec{a}, \vec{a} \rangle \cdot \langle \vec{b}, \vec{b} \rangle,$$

where $\langle \vec{a}, \vec{b} \rangle = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$ is the standard inner product.

Expanded Form: Another way to express the Cauchy-Schwarz inequality is:

$$(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)^2 \leq (a_1^2 + a_2^2 + \cdots + a_n^2)(b_1^2 + b_2^2 + \cdots + b_n^2).$$

Justification:

- The inequality can be thought of as stating that the cosine of the angle between two vectors is always between -1 and 1, which geometrically means that the projection of one vector onto another cannot exceed the product of their magnitudes.
- For vectors $\vec{a}$ and $\vec{b}$, equality holds if and only if the vectors are linearly dependent, i.e., $\vec{a} = \lambda \vec{b}$ for some scalar λ.

Number Theory

Theorem (Euclidean Algorithm)**.** The Euclidean Algorithm is an efficient method for finding the greatest common divisor (gcd) of two integers a and b, where $a, b \in \mathbb{Z}$ and $a, b > 0$. The gcd of a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b without leaving a remainder.

Algorithm Description: Given two integers a and b, with $a > b$:

1. Divide a by b, obtaining a quotient q and a remainder r such that

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

2. If $r = 0$, then $\gcd(a, b) = b$.
3. If $r \neq 0$, replace a with b and b with r, and repeat the process.

The algorithm terminates when the remainder is zero, and the gcd is the non-zero remainder from the previous step.

Example: Find the gcd of 252 and 105:

- Step 1: $252 = 105 \cdot 2 + 42$ (remainder 42).
- Step 2: $105 = 42 \cdot 2 + 21$ (remainder 21).
- Step 3: $42 = 21 \cdot 2 + 0$ (remainder 0).
- Therefore, $\gcd(252, 105) = 21$.

Justification:

- The Euclidean Algorithm works based on the property that $\gcd(a, b) = \gcd(b, r)$, where r is the remainder when a is divided by b. This property follows from the fact that any divisor of both a and b must also divide r.

- The algorithm reduces the problem size at each step, ensuring that the remainder r gets smaller until it reaches zero, at which point the gcd is found.

Theorem (Bézout's Identity)**.** Let $a, b \in \mathbb{Z}$, and let $d = \gcd(a, b)$ be the greatest common divisor of a and b. Then there exist integers x and y such that

$$ax + by = d.$$

In other words, d can be expressed as a linear combination of a and b with integer coefficients x and y.

Example: Find integers x and y such that $252x + 105y = \gcd(252, 105)$.

- From the Euclidean Algorithm:

$$252 = 105 \cdot 2 + 42,$$
$$105 = 42 \cdot 2 + 21,$$
$$42 = 21 \cdot 2 + 0.$$

  Thus, $\gcd(252, 105) = 21$.

- Now, back-substitute to express 21 as a linear combination of 252 and 105:

$$21 = 105 - 42 \cdot 2.$$

  Substitute $42 = 252 - 105 \cdot 2$:

$$21 = 105 - 2(252 - 105 \cdot 2) = 5 \cdot 105 - 2 \cdot 252.$$

  Therefore, $x = -2$ and $y = 5$, and we have

$$252(-2) + 105(5) = 21.$$

Justification:

- Bézout's Identity follows from the steps of the Euclidean Algorithm, where we successively express the remainders as linear combinations of a and b.
- Since the gcd d is the last non-zero remainder in the Euclidean Algorithm, it can always be written as a linear combination of the original numbers a and b.

Theorem (Unique Factorization into Primes (Fundamental Theorem of Arithmetic))**.** Every integer $n > 1$ can be factored uniquely into a product of prime numbers, up to the order of the factors. Specifically, if

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m,$$

where p_i and q_j are primes, then $k = m$ and, after reordering, $p_i = q_i$ for all i.

Proof Summary:

- *Existence:* We prove by induction that every $n > 1$ can be factored into primes.
  1. *Base Case:* $n = 2$ is a prime.
  2. *Inductive Step:* Assume true for all $k < n$. If n is prime, it is its own factorization. If n is composite, we can write $n = ab$ with $a, b < n$. By the inductive hypothesis, a and b have prime factorizations, which gives a prime factorization for n.

- *Uniqueness:* Assume two different factorizations exist. By the property of primes, each prime in one factorization must divide some term in the other factorization, leading to a contradiction unless the factorizations are identical. Cancel one prime at a time.

Theorem (Basic Properties of Modular Arithmetic)**.** Let n be a positive integer, and let $a, b, c, d \in \mathbb{Z}$. The following properties hold under modulo n arithmetic:

- *Congruence Preservation:* If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
  1. $a + c \equiv b + d \pmod{n}$
  2. $a \cdot c \equiv b \cdot d \pmod{n}$
- *Addition and Multiplication:*
  - *Commutative Law:* $(a + b) \equiv (b + a) \pmod{n}$ and $(a \cdot b) \equiv (b \cdot a) \pmod{n}$.
  - *Associative Law:* $(a + b) + c \equiv a + (b + c) \pmod{n}$ and $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}$.
  - *Distributive Law:* $a \cdot (b + c) \equiv (a \cdot b) + (a \cdot c) \pmod{n}$.
- *Raising to a Power:* If $a \equiv b \pmod{n}$, then for any non-negative integer k, we have

  $$a^k \equiv b^k \pmod{n}.$$

  This follows by applying the congruence repeatedly, using the property that multiplication preserves congruence.

Well-Defined Operations on $\mathbb{Z}/n\mathbb{Z}$:
In the set $\mathbb{Z}/n\mathbb{Z}$, we define addition and multiplication as follows:

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab],$$

where $[a]$ denotes the equivalence class of a modulo n.

To show that these operations are well-defined, we need to verify that if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then:

1. $[a + b] = [a' + b']$:
   Since $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, we have $a = a' + kn$ and $b = b' + ln$ for some integers k, l. Then:
   $$a + b = (a' + kn) + (b' + ln) = (a' + b') + n(k + l),$$
   which implies $a + b \equiv a' + b' \pmod{n}$, so $[a + b] = [a' + b']$.
2. $[ab] = [a'b']$:
   Since $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, we have $a = a' + kn$ and $b = b' + ln$ for some integers k, l. Then:
   $$ab - a'b' = (ab - a'b) + (a'b - a'b') = b(a - a') + a'(b - b').$$
   Since $a \equiv a' \pmod{n}$, we have $a - a' = kn$, and similarly $b - b' = ln$. Therefore,
   $$ab - a'b' = b(kn) + a'(ln) = n(bk + a'l),$$
   which implies $ab \equiv a'b' \pmod{n}$, so $[ab] = [a'b']$.

Therefore, addition and multiplication are well-defined in $\mathbb{Z}/n\mathbb{Z}$.

Theorem (Divisibility Rules for 9 and 11)**.** Let n be a positive integer with decimal representation $n = a_k a_{k-1} \cdots a_1 a_0$, where a_i represents the digits of n. The following divisibility rules apply:

Divisibility by 9:

- n is divisible by 9 if and only if the sum of its digits is divisible by 9.

Divisibility by 11:

- n is divisible by 11 if and only if the alternating sum and difference of its digits is divisible by 11. Specifically, let
$$S = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k.$$
Then n is divisible by 11 if and only if S is divisible by 11.

Theorem (Fermat's Little Theorem)**.** Let p be a prime number, and let a be any integer. Fermat's Little Theorem can be expressed in several equivalent forms:

Form 1: General Congruence

- If p is a prime and $p \nmid a$ or $\gcd(p, a) = 1$, then
$$a^{p-1} \equiv 1 \pmod{p}.$$

Form 2: Special Case When a Is Not Divisible by p

- If p is a prime and a is not divisible by p, then $a^{p-1} - 1$ is divisible by p:
$$p \mid (a^{p-1} - 1).$$

Form 3: Congruence for Any Integer a

- If p is a prime and a is any integer, then
$$a^p \equiv a \pmod{p}.$$

Form 4: Congruence for Small Values

- When $a \equiv 1 \pmod{p}$, Fermat's Little Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$, confirming the periodicity in raising to the power.

Definition (Euler's Totient Function)**.** Euler's totient function, denoted $\varphi(n)$, is defined as the number of positive integers less than or equal to n that are coprime to n (i.e., they share no common factors with n other than 1).

Closed Form Formula:

- If n has the prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then Euler's totient function can be expressed as:
$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Example: To compute $\varphi(12)$:

- The prime factorization of 12 is $2^2 \times 3$.
- Using the formula:
$$\varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$
Thus, there are 4 positive integers less than or equal to 12 that are coprime to 12: $1, 5, 7, 11$.

Theorem (Euler's Theorem)**.** Let n be a positive integer and let a be an integer coprime to n (i.e., $\gcd(a, n) = 1$). Then Euler's theorem states that

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

where $\varphi(n)$ is Euler's totient function.

Note: Euler's theorem generalizes Fermat's Little Theorem. Specifically, Fermat's Little Theorem is the special case of Euler's theorem when n is a prime number p. In this case, $\varphi(p) = p - 1$, and the theorem reduces to

$$a^{p-1} \equiv 1 \pmod{p},$$

which is Fermat's Little Theorem.

Theorem (Highest Power of a Prime Dividing $n!$)**.** Let p be a prime number, and let n be a positive integer. The highest power of p that divides $n!$ is given by:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots,$$

where the sum continues until $p^k > n$.

Example: To find the highest power of 3 dividing 10!:

- $\left\lfloor \frac{10}{3} \right\rfloor = 3$
- $\left\lfloor \frac{10}{3^2} \right\rfloor = 1$
- $\left\lfloor \frac{10}{3^3} \right\rfloor = 0$

Thus, the highest power of 3 dividing 10! is $3 + 1 = 4$.

Theorem (Chinese Remainder Theorem)**.** Let $n_1, n_2, \ldots, n_k$ be positive integers that are pairwise coprime (i.e., $\gcd(n_i, n_j) = 1$ for all $i \neq j$). For any sequence of integers $a_1, a_2, \ldots, a_k$, the system of congruences

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

has a unique solution modulo $X = n_1 n_2 \cdots n_k$.

Proof by Induction:
We prove the theorem by induction on k, the number of congruences.
Base Case ($k = 2$):
For $k = 2$, we have two congruences:

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

where $\gcd(n_1, n_2) = 1$. By Bézout's identity, there exist integers y_1, y_2 such that

$$n_1 y_1 + n_2 y_2 = 1.$$

We construct a solution x as

$$x = a_1 n_2 y_2 + a_2 n_1 y_1.$$

We verify that x satisfies both congruences:

- $x \equiv a_1 n_2 y_2 + a_2 n_1 y_1 \equiv a_1 (n_2 y_2) \pmod{n_1}$. Since $n_1 y_1 + n_2 y_2 = 1$, it follows that $n_2 y_2 \equiv 1 \pmod{n_1}$. Therefore, $x \equiv a_1 \cdot 1 \equiv a_1 \pmod{n_1}$.

- $x \equiv a_1 n_2 y_2 + a_2 n_1 y_1 \equiv a_2(n_1 y_1) \pmod{n_2}$. Similarly, $n_1 y_1 \equiv 1 \pmod{n_2}$, so $x \equiv a_2 \cdot 1 \equiv a_2 \pmod{n_2}$.

Thus, a solution exists, and it is unique modulo $X = n_1 n_2$.

Inductive Step:

Assume that the theorem holds for k congruences. That is, for pairwise coprime $n_1, n_2, \ldots, n_k$, there exists a unique solution modulo $X_k = n_1 n_2 \cdots n_k$ for the system

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

Now consider $k+1$ congruences:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_{k+1} \pmod{n_{k+1}},$$

where $n_1, n_2, \ldots, n_{k+1}$ are pairwise coprime.

By the induction hypothesis, there exists a unique solution x_0 modulo $X_k = n_1 n_2 \cdots n_k$ for the first k congruences. We now need to solve the system

$$x \equiv x_0 \pmod{X_k}, \quad x \equiv a_{k+1} \pmod{n_{k+1}}.$$

Since X_k and n_{k+1} are coprime (as n_{k+1} is coprime with each n_i for $1 \leq i \leq k$), we can apply the base case (which we proved for two congruences) to find a unique solution modulo $X_{k+1} = X_k \cdot n_{k+1}$. Thus, there exists a unique solution modulo X_{k+1}.

Conclusion:

By induction, the system of congruences has a unique solution modulo $X = n_1 n_2 \cdots n_k$ for any positive integer k.

Facts

- Any triangle can be cut up into 6 or more similar triangles.
- Every odd square is $\equiv 1 \mod 8$