3 Examples using Unique Prime Factorization Theorem:

1. Write the (unique) prime factorization of 10!

\[ 10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 = \\
(2 \times 5)(3 \times 3)(2 \times 2 \times 2)(7)(2 \times 3)(5)(2 \times 2)(3)(2) = \\
(2^8)(3^4)(5^2)(7) \]

2. Use prime factorization to find the greatest common divisor of 700 and 240.

\[ 700 = 7 \times 100 = 7 \times 10 \times 10 = (2^2)(5^2)(7) \]
\[ 240 = 24 \times 10 = (4 \times 6)(2 \times 5) = (2 \times 2 \times 2 \times 3)(2 \times 5) = (2^4)(3^1)(5) \]
\[ \text{GCD} = (2^2)(5) = 20 \]

3. Suppose \((2^5)(3^2)(5^9)x = (3^5)(7^2)y\). What can we say about \(x\) and \(y\)?

\(x\) is a multiple of 27 and 49. \(y\) is a multiple of \((2^5)(5^9)\).
Claim: $(\forall a \in \mathbb{N}^+)(\forall q \in \mathbb{N}_{\text{prime}})[q|a^2 \rightarrow q|a]$.

Proof:

Let $a \in \mathbb{N}^+$, selected arbitrarily, and let $q$ be an arbitrary prime.

Assume $q|a^2$. [I must show $q|a$.]

Consider the prime factorization of $a$:

$$a = (p_1)^{e_1}(p_2)^{e_2}(p_3)^{e_3} \cdots (p_k)^{e_k}$$

$$a^2 = (p_1)^{2e_1}(p_2)^{2e_2}(p_3)^{2e_3} \cdots (p_k)^{2e_k}$$

Since $q$ is a prime that divides $a^2$, $q$ must appear somewhere in this factorization, so $q = p_i$ for some $0 \leq i \leq k$.

Therefore $q|a$. □
Claim: $\sqrt{3}$ is irrational.

Proof:

Suppose (BWOC) $\sqrt{3}$ were rational.
$\sqrt{3} = a/b$ for some $a, b \in \mathbb{Z}$, with $b \neq 0$.
$3 = a^2/b^2$
$3b^2 = a^2$. \[1\]

Consider the prime factorization of $a$:
$a = (2)^{e_1}(3)^{e_2}(5)^{e_3} \ldots (p_k)^{e_k}$. \[Note that some exponents may be 0.\]
$a^2 = (2)^{2e_1}(3)^{2e_2}(5)^{2e_3} \ldots (p_k)^{2e_k}$
Note that $a^2$ has $2e_2$ factors of 3.

Consider the prime factorization of $b$:
$b = (2)^{f_1}(3)^{f_2}(5)^{f_3} \ldots (p_m)^{f_m}$
$b^2 = (2)^{2f_1}(3)^{2f_2}(5)^{2f_3} \ldots (p_m)^{2f_m}$
Note that $b^2$ has $2f_2$ factors of 3.

Reconsider equation \[1\]:
The number of 3's on the R.H.S. is $2e_2$.
The number of 3's on the L.H.S. is $2f_2 + 1$.
So we must have $2e_2 = 2f_2 + 1$. But this is impossible, since the L.H.S. is even and the R.H.S. is odd. ☒ ☐
Examples with Modular Congruence:

(4 questions)

17 $\equiv_5 33$ (True/false?)

1000 $\equiv_{10} 17163461$ (True/false?)

$3x \equiv_3 3y + 1$ (where $x, y \in \mathbb{Z}$). Possible?

$7x + 5 \equiv_7 49y + 3$ (where $x, y \in \mathbb{Z}$). Possible?
Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 1$, selected arbitrarily. Assume $a \equiv_n c$ and $b \equiv_n d$.

**Claim 1:** $(a + b) \equiv_n (c + d)$

**Proof:**

Since $a \equiv_n c$, $n|(a - c)$, so $a - c = nk$ for some $k \in \mathbb{Z}$. \[1\]

Since $b \equiv_n d$, $n|(b - d)$, so $b - d = nm$ for some $m \in \mathbb{Z}$. \[2\]

Adding [1] with [2]:

$a - c + b - d = nk + nm$

$(a + b) - (c + d) = n(k + m)$

$n|((a + b) - (c + d))$

$(a + b) \equiv_n (c + d)$

**Claim 2:** $(a - b) \equiv_n (c - d)$

**Proof:**

Since $a \equiv_n c$, $n|(a - c)$, so $a - c = nk$ for some $k \in \mathbb{Z}$. \[3\]

Since $b \equiv_n d$, $n|(b - d)$, so $b - d = nm$ for some $m \in \mathbb{Z}$. \[4\]

Subtracting [4] from [3]:

$a - c - (b - d) = nk - nm$

$(a - b) - (c - d) = n(k - m)$

$n|((a - b) - (c - d))$

$(a - b) \equiv_n (c - d)$
Claim 3: \((ab) \equiv_n (cd)\)

Proof:
Since \(a \equiv_n c\), \(a = c + nk\) for some \(k \in \mathbb{Z}\).

Since \(b \equiv_n d\), \(b = d + nm\) for some \(m \in \mathbb{Z}\).

\[ab = (c + nk)(d + nm)\]

\[ab = cd + n(cm) + n(kd) + n^2km\]

\[ab - cd = n[cm + kd + nkm]\]

\[n| (ab - cd)\]

\[ab \equiv_n cd.\]

Claim 4: \(a^m \equiv_n c^m\)

Sketch of proof:
Since \(a \equiv_n c\), by Claim #3,

\[a \ast a \equiv_n c \ast c\]

Apply it again:
\[a(a \ast a) \equiv_n c(c \ast c)\]

Repeat \(m\) times.
Using Modular Arithmetic (3 examples):

1. What is $17^6 \mod 5$?

Note that $17 \equiv_5 2$.
$17^6 \equiv_5 2^6 \equiv_5 4$.

2. What is $1000000000000 \mod 9$?

Note that $10 \equiv_9 1$.
$10^{12} \equiv_9 1^{12} \equiv_9 1$

3. Is $2^{777} + 1$ divisible by 3?

Note that $2 \equiv_3 -1$.
$2^{777} \equiv_3 (-1)^{777}$
$2^{777} + 1 \equiv_3 -1 + 1$
So yes!
Claim: For all natural numbers, \( n \): \( n \) is divisible by 3 if and only if the sum of the digits of \( n \) is divisible by 3.

Proof:
Let’s enumerate the digits of \( n \) as \( d_0, d_1, d_2 \ldots d_k \):
\[
n = 10^k d_k + 10^{k-1} d_{k-1} \ldots 10^3 d_3 + 10^2 d_2 + 10^1 d_1 + 10^0 d_0.
\]
Observe that 10 \( \equiv_3 1 \).
By M.A.T., For any \( m \in \mathbb{N} \), 10\(^m\) \( \equiv_3 1^m \), i.e. 10\(^m\) \( \equiv_3 1 \).
So any term 10\(^m\)d\(_m\) \( \equiv_3 d_m \).

Therefore:
\[
10^k d_k + 10^{k-1} d_{k-1} + \ldots + 10^2 d_2 + 10^1 d_1 + 10^0 d_0 \equiv_3 d_k + d_{k-1} + \ldots + d_2 + d_1 + d_0.
\]
We may now reason as follows:
\[
n \text{ is divisible by 3} \iff \\
n \equiv_3 0 \iff \\
10^k d_k + 10^{k-1} d_{k-1} \ldots 10^3 d_3 + 10^2 d_2 + 10^1 d_1 + 10^0 d_0 \equiv_3 0 \iff \\
d_k + d_{k-1} + \ldots d_3 + d_2 + d_1 + d_0 \equiv_3 0 \iff \\
The sum of the digits of \( n \) are a multiple of 3.
\]
\( \square \)