初等数论

吴 伊 涛

2022 年春

Prop. Congruence modulo m is an equivalence relation on the set of integers $\mathbb{Z}$, i.e.

1) $a \equiv a \pmod{m}$, $\forall a \in \mathbb{Z}$,

2) $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$, $\forall a, b \in \mathbb{Z}$,

3) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$ $\forall a, b, c \in \mathbb{Z}$.

We already see some examples and applications of congruence. Let's come back to the property " Cogruence modulo m is an equivalence relation on the set of integers $\mathbb{Z}$ ". (page 125).

It follows that we can divide the set of integers into equivalence classes.

Now, $\forall a \in \mathbb{Z}$, let

$\bar{a}$ = the set of integers congruent to a modulo m.

$$\therefore \bar{a} = \{ x \in \mathbb{Z} : x \equiv a \pmod{m} \}$$
$$= \{ a, a+m, a-m, a+2m, a-2m, \cdots \}$$
$$= \{ a+km : k \in \mathbb{Z} \}$$

E.g. Let $m=2$, then

$\bar{0} = \{$ even integers $\} = \{0, 2, -2, 4, -4, \cdots\}$

$\bar{1} = \{$ odd integers $\} = \{1, -1, 3, -3, \cdots\}$

Let $m=3$, then

$\bar{0} = \{$ 3k type integers $\} = \{0, 3, -3, 6, -6, \cdots\}$

$\bar{1} = \{$ 3k+1 type integers $\} = \{1, -2, 4, -5, 7, \cdots\}$

$\bar{2} = \{$ 3k+2 type integers $\} = \{2, -1, 5, -4, 8, \cdots\}$

Def: Fix $m \in \mathbb{Z}^+$, a set of the form $\bar{a} = \{a+km : k \in \mathbb{Z}\}$ is called a congruence class modulo m. (also called: residue class)

We have following consequences:

Prop. 1) $\bar{a} = \bar{b}$ iff $a \equiv b \pmod m$

2) $\bar{a} \neq \bar{b}$ iff $\bar{a} \cap \bar{b} = \phi$

3) There are exactly m congruence classes modulo m:

$\bar{0}, \bar{1}, \bar{2}, \cdots \overline{m-1}$.

Proof: 1) 2) Leave to the reader.

3). First, it is easy to see that $\bar{0}, \bar{1}, \bar{2}, \cdots \overline{m-1}$ are pairwise different.

Now, $\forall x \in \mathbb{Z}$, by division algorithm, $x = q \cdot m + r$, $0 \leq r \leq m-1$.

$\therefore x \equiv r \pmod m$. Thus $\bar{x} = \bar{r}$.

$\square$

Def: The set of congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$.

If $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_m$ are a complete set of congruence classes modulo m, i.e. $\{\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_m\} = \mathbb{Z}/m\mathbb{Z}$,

Then $\{a_1, a_2, \cdots a_m\}$ is called a complete set (system) of residues modulo m.

E.g. When $m=3$,

$\{0,1,2\}$, $\{11, 19, 30\}$, $\{-5, -25, -48\}$ are all complete sets of residues modulo 3.

When $m=4$,

$\{0,1,2,3\}$, $\{8, 26, 11, 48\}$, $\{4, 17, -2, -5\}$ are all complete sets of residues modulo 4.

Note that, we can define addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$:

$\forall\ \bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$.

$$\bar{a} + \bar{b} := \overline{a+b}$$

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

The proposition on page 126 tells us the above definition is well-defined. (If $\bar{a} = \bar{x}$, $\bar{b} = \bar{y}$, then $\overline{a+b} = \overline{x+y}$ ... etc.)

E.g. $m=11$, $\bar{6} + \bar{8} = \overline{14} = \bar{3}$.

$\bar{6} \cdot \bar{8} = \overline{48} = \bar{4}$.

The tables on page 122 can now be seen as the addition and multiplication tables in $\mathbb{Z}/3\mathbb{Z}$, we rewrite it below:

$\mathbb{Z}/3\mathbb{Z}$: " + "

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

" × "

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

In fact, the above addition and multiplication make $\mathbb{Z}/3\mathbb{Z}$ as a ring, called the quotient ring...

Exercise:

1. Write out the addition and multiplication tables of $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$.

In discussing arithmetic problems, some times, it's convenient to work with the notations of congruences (modulo m), some times it's convenient to work with the (ring) set $\mathbb{Z}/m\mathbb{Z}$. We shall switch back and forth between the two viewpoints as the situation demands.

Rmk: Note that, there is no division in $\mathbb{Z}/m\mathbb{Z}$.

E.g. $m=4$, then $\bar{2}\cdot\bar{3} = \bar{6} = \bar{2} = \bar{2}\cdot\bar{1}$.

Thus, if we conside "$\bar{2} \div \bar{2}$", then there are two answers: $\bar{1}$ and $\bar{3}$ ......

Prop. Let $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, $g.c.d.(a, m) = 1$.

If x runs through a complete set of residues modulo m, then $ax+b$ also runs through a complete set of residues modulo m.

Proof:

Assume x runs through a complete set of residues modulo m: $\{x_1, x_2, \cdots, x_m\}$

Then $ax+b$ runs through $\{ax_1+b, ax_2+b, \cdots, ax_m+b\}$.

Since there are exactly m congruent classes modulo m, it suffices to show that $\overline{ax_i+b} \neq \overline{ax_j+b}$ when $1 \leq i \neq j \leq m$.

i.e. $ax_i+b \not\equiv ax_j+b \pmod m$.

Assume not, $ax_i+b \equiv ax_j+b \pmod m$ for some $i \neq j$

Then $m \mid (ax_j+b-ax_i-b) \implies m \mid a(x_j - x_i)$

As $g.c.d.(a, m) = 1$, $\therefore$ $m \mid x_j - x_i$

Thus $x_i \equiv x_j \pmod m$, $\overline{x_i} = \overline{x_j}$.

Since $\{x_1, x_2, \cdots, x_m\}$ is a complete set of residues modulo m, $\overline{x_i} = \overline{x_j} \implies i = j$. A contradiction.

So $\{ax_1+b, ax_2+b, \cdots, ax_m+b\}$ is a set of m integers pairwisely not congruent modulo m. Thus it is a complete set of residues modulo m. $\square$

Prop. Let $m_1, m_2 \in \mathbb{Z}^+$, $g.c.d.(m_1, m_2) = 1$.

Assume x_1 runs through a complete system of residues modulo m_1,

x_2 runs through a complete system of residues modulo m_2,

Then $m_2 x_1 + m_1 x_2$ runs through a complete system of residues modulo $m_1 \cdot m_2$

Proof:

Assume x_1 runs through a complete set of residues modulo m_1:

$\{s_1, s_2, \cdots, s_{m_1}\}$

x_2 ...... m_2:

$\{t_1, t_2, \cdots, t_{m_2}\}$

Then $m_2 x_1 + m_1 x_2$ runs through $\{m_2 s_i + m_1 t_j : 1 \le i \le m_1, 1 \le j \le m_2\}$.

Since there are exactly $m_1 \cdot m_2$ congruence classes modulo $m_1 \cdot m_2$, it suffices to prove $m_2 s_i + m_1 t_j \not\equiv m_2 s_{i'} + m_1 t_{j'} \pmod{m_1 \cdot m_2}$ when $(i, j) \neq (i', j')$.

If $m_2 s_i + m_1 t_j \equiv m_2 s_{i'} + m_1 t_{j'} \pmod{m_1 m_2}$,

then $m_2 s_i + m_1 t_j \equiv m_2 s_{i'} + m_1 t_{j'} \pmod{m_2}$.

$\therefore$ $m_1 t_j \equiv m_1 t_{j'} \pmod{m_2}$, i.e. $m_2 \mid m_1 \cdot (t_{j'} - t_j)$.

As $g.c.d.(m_1, m_2) = 1$, we get $m_2 \mid t_{j'} - t_j$, i.e. $t_j \equiv t_{j'} \pmod{m_2}$.

Since $\{t_1, t_2, \cdots, t_{m_2}\}$ is a complete set of residues modulo m_2, it follows that $j' = j$.

Similarly, we get $i' = i$.

Thus $m_2 s_i + m_1 t_j \not\equiv m_2 s_{i'} + m_1 t_{j'} \pmod{m_1 m_2}$ when $(i, j) \neq (i', j')$.

Similarly as above, we get the ~~congruence~~ consequence.

$\square$

Use the same method, we can prove the following propositions.

Prop. Let $m_1, m_2, \cdots, m_k \in \mathbb{Z}^+$, pairwise coprime.

Let x_i runs through a complete system of residues modulo m_i, $i = 1, 2, \cdots, k$.

Then
$$M_1 x_1 + M_2 x_2 + \cdots + M_k x_k$$
runs through a complete system of residues modulo m, where $m = m_1 \cdot m_2 \cdots m_k$, $M_i = \frac{m}{m_i}$, $i = 1, 2, \cdots, k$.

Prop. Let $m_1, m_2, \cdots, m_k \in \mathbb{Z}^+$, x_i runs through a complete system of residues modulo m_i. $i = 1, 2, \cdots, k$.

Then
$$x_1 + m_1 x_2 + m_1 \cdot m_2 x_3 + \cdots + m_1 \cdot m_2 \cdots m_{k-1} x_k$$
runs through a complete system of residues modulo $m = m_1 \cdot m_2 \cdots m_k$.

The proof of above props are left to the reader.

Rmk: The above two props are principles of two algorithms of solving system of congruence equations via Chinese Remainder Theorem.

□

· Reduced residue system (modulo m)

Def: Given $m \in \mathbb{Z}^+$, if $a \in \mathbb{Z}$, g.c.d.$(a, m) = 1$, then we say the residue class (congruence class) $\bar{a}$ is a <u>residue class coprime to m</u>.

E.g. $m = 8$, then $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ are residue classes coprime to 8.

Now, given integers $a_1, a_2, \cdots, a_k$, if the following conditions hold:

1) g.c.d.$(a_i, m) = 1$, $i = 1, 2, \cdots, k$

2) If $i \neq j$, then $\bar{a_i} \neq \bar{a_j}$, i.e. $a_i \not\equiv a_j \pmod{m}$.

3) $\forall b$, s.t. g.c.d.$(b, m) = 1$, $\exists i_0$, $\bar{b} = \overline{a_{i_0}}$, i.e. $b \equiv a_{i_0} \pmod{m}$.

Then $\{a_1, a_2, \cdots a_k\}$ is called <u>a reduced set (system) of residues modulo m</u>.

E.g.

$m = 8$, $\{1, 3, 5, 7\}$ is a reduced residue set modulo 8.

$\{11, 13, 15, 17\}$ is also a reduced ......

$m = 6$ $\{1, 5\}$ is a reduced residue set modulo 6.

$\{-11, -19\}$ is also a ....

$m = p$, p is a prime, $\{1, 2, \cdots, p-1\}$ is a reduced residue set modulo p.

Now, we fix a positive integer m, let $\phi(m)$ be the number of integers between 0 and $m-1$ that coprime to m.

Def: Fix $m \in \mathbb{Z}^+$, we define Euler's ϕ-function as:

$$\phi(m) := \#\{n : 0 \leqslant n \leqslant m-1,\ g.c.d.(n,m)=1\}$$

E.g.

$\phi(4) = \#\{1,3\} = 2$.

$\phi(6) = \#\{1,5\} = 2$.

$\forall p$ prime, $\phi(p) = p-1$.

Clearly, a reduced residue system modulo m has $\phi(m)$ integers.

We'll introduce the calculation formula of $\phi(m)$ later. Let's see some propositions of residue system first.

Prop. (Compare to the prop. in page 134)

Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, $g.c.d.(a,m)=1$

If x runs through a reduced system modulo m,

then ax runs through a reduced system modulo m.

Rmk: Note that $ax+b$ may not runs through a reduced system modulo m! (Compare to the prop. in page 134). e.g. $m=8$, $x \in \{1,3,5,7\}$, $a=b=1$.

Proof:

Assume x runs through a reduced residue system modulo m:

$\{x_1, x_2, \cdots, x_{\phi(m)}\}$

Then ax runs through $\{ax_1, ax_2, \cdots, ax_{\phi(m)}\}$.

Since g.c.d. $(a, m) = 1$, g.c.d. $(x_i, m) = 1$, we get g.c.d. $(ax_i, m) = 1$.

So $\overline{ax_i}$ is also a residue class coprime to m.

Since there are exactly $\phi(m)$ residue class coprime to m, it suffices to show that $\overline{ax_i} \neq \overline{ax_j}$ when $1 \leq i \neq j \leq m$,

i.e. $ax_i \not\equiv ax_j \pmod{m}$ when $1 \leq i \neq j \leq m$.

Similar as the proof in page 134;

If $ax_i \equiv ax_j \pmod{m}$, then $m \mid a \cdot (x_j - x_i)$.

Since g.c.d. $(a, m) = 1$, $m \mid x_j - x_i$, i.e. $x_i \equiv x_j \pmod{m}$

So $\overline{x_i} = \overline{x_j}$.

Note that $\{x_1, x_2, \cdots, x_{\phi(m)}\}$ is a reduced residue system modulo m,. thus $\overline{x_i} = \overline{x_j}$ implies that $i = j$. $\square$

Rmk: Here we do not need the formula of $\phi(m)$, Prop. Let $m_1, m_2 \in \mathbb{Z}^+$, g.c.d. $(m_1, m_2) = 1$

Assume x_1 runs through a reduced residue system of m_1,

x_2 ... m_2.

Then $m_2 x_1 + m_1 x_2$ ... $m_1 \cdot m_2$.

Rmk: The prop looks like the prop in page 135. But the proof is totally different!

Proof:

Assume x_1 runs through a reduced residue system of m_1:

$\{s_1, s_2, \cdots, s_{\phi(m_1)}\}$

x_2 ... m_2:

$\{t_1, t_2, \cdots, t_{\phi(m_2)}\}$

Then $m_2 x_1 + m_1 x_2$ runs through $\left\{ m_2 s_i + m_1 t_j : \begin{array}{l} 1 \le i \le \phi(m_1), \\ 1 \le j \le \phi(m_2). \end{array} \right\}$

Claim 1: g.c.d. $(m_2 s_i + m_1 t_j, m_1 m_2) = 1$, $\forall i, j$.

Assume not, then $\forall p$ prime, $p \mid$ g.c.d. $(m_2 s_i + m_1 t_j, m_1 m_2)$.

$p \mid m_1 \cdot m_2 \Rightarrow p \mid m_1$ or $p \mid m_2$. WLOG, let $p \mid m_1$, then $p \nmid m_2$ as g.c.d. $(m_1, m_2) = 1$.

Also, $p \nmid s_i$ since g.c.d. $(m_1, s_i) = 1$.

So $p \nmid m_2 \cdot s_i$, thus $p \nmid m_2 s_i + m_1 t_j$. A contradiction.

Thus we know that $\overline{m_2 s_i + m_1 t_j}$ (residue class modulo $m_1 m_2$) is coprime to $m_1 \cdot m_2$.

Claim 2: When $(i,j) \neq (i',j')$

$$m_2 s_i + m_1 t_j \not\equiv m_2 s_{i'} + m_1 t_{j'} \pmod{m_1 \cdot m_2}$$

(Proof: Leave to the reader).

Claim 3: $\forall b$, s.t. $g.c.d.(b, m_1 m_2) = 1$.

$$\exists\, i_0, j_0, \quad b \equiv m_2 s_{i_0} + m_1 t_{j_0} \pmod{m_1 m_2}$$

Since $g.c.d.(m_1, m_2) = 1$, the Diophantine equation $m_2 x + m_1 y = b$ has solutions.

Let u, v be a solution of $m_2 x + m_1 y = b$, we claim that $g.c.d.(m_1, u) = 1$, $g.c.d.(m_2, v) = 1$.

In fact, if $d = g.c.d.(m_1, u) \neq 1$, then $d \mid m_2 u + m_1 v = b$, thus $d \mid g.c.d.(b, m_1 m_2) = 1$, a contradiction. $\therefore g.c.d.(m_1, u) = 1$.

Similarly, $g.c.d.(m_2, v) = 1$.

Since $\{s_1, \cdots s_{\phi(m_1)}\}$ is a reduced residue system of m_1, thus there exists (a unique) i_0, s.t. $u \equiv s_{i_0} \pmod{m_1}$

Similarly, $\exists!\, j_0$, s.t. $v \equiv t_{j_0} \pmod{m_2}$.

Now, $m_1 \mid s_{i_0} - u$, $\quad \therefore m_1 \cdot m_2 \mid m_2(s_{i_0} - u)$.

$m_2 \mid t_{j_0} - v$, $\quad \therefore m_1 \cdot m_2 \mid m_1(t_{j_0} - v)$.

$$\therefore b = m_2 u + m_1 v \equiv m_2 s_{i_0} + m_1 t_{j_0} \pmod{m_1 \cdot m_2}.$$

By definition of reduced residue system (page 137), we get the consequence. $\square$

Cor 1. Let $m_1, m_2 \in \mathbb{Z}^+$, $g.c.d.(m_1, m_2) = 1$

Then $\phi(m_1 \cdot m_2) = \phi(m_1)\phi(m_2)$.

(Thus $\phi(n)$ is a multiplicative function (page 49)).

Cor 2. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ where p_i are distinct primes.

Then $\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdots (p_l^{a_l} - p_l^{a_l-1})$

$= n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_l})$

Proof:

By Cor 1, we have:

$$\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdots \phi(p_l^{a_l}).$$

Claim: $\forall p$ prime, $\phi(p^k) = p^k - p^{k-1}$.

By definition, $\phi(p^k) = \#\{x : 0 \le x \le p^k - 1, g.c.d.(x, p^k) = 1\}$

Clearly, $g.c.d.(x, p^k) = 1 \iff g.c.d.(x, p) = 1$.

$\therefore \phi(p^k) = \#\{x : 0 \le x \le p^k - 1, g.c.d.(x, p) = 1\}$

$= \#\{x : 0 \le x \le p^k - 1, p \nmid x\}$

$= \#\{x : 0 \le x \le p^k - 1\} - \#\{x : 0 \le x \le p^k - 1, p \mid x\}$

$= p^k - [\frac{p^k}{p}] = p^k - p^{k-1}$.

Thus $\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdots \phi(p_l^{a_l})$

$= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_l^{a_l} - p_l^{a_l-1})$ □

Example

$10000 = 2^4 \times 5^4$

$\phi(10000) = (2^4 - 2^3) \times (5^4 - 5^3) = 8 \times 500 = 4000$

$\phi(10000) = 10000 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{5}) = 4000$

$1001 = 7 \times 11 \times 13$

$\phi(1001) = (7 - 1) \times (11 - 1) \times (13 - 1) = 6 \times 10 \times 12 = 720$

$\phi(1001) = 1001 \times (1 - \frac{1}{7}) \times (1 - \frac{1}{11}) \times (1 - \frac{1}{13}) = 720$

Example

a)Find the number of positive integers less than 2022 that are coprime to 2022.

b)Find the number of positive integers less than 8088 that are coprime to 2022.

c)Find the number of positive integers between 1111 and 9199 that are coprime to 2022.

d)Find the number of positive integers less than 2000 that are coprime to 2022.

Solution:

$2022 = 2 \times 3 \times 337$

a)The number of positive integers less than 2022 that are coprime to 2022 is just $\phi(2022) = (2-1) \times (3-1) \times (337-1) = 672$.

b)Note that any set of consecutive 2022 integers is a complete residue system modulo 2022. So:

$\{x \in \mathbb{Z} : 1 \leq x \leq 2022\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

Similarly,

$\{x \in \mathbb{Z} : 2023 \leq x \leq 4044\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

$\{x \in \mathbb{Z} : 4045 \leq x \leq 6066\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

$\{x \in \mathbb{Z} : 6067 \leq x \leq 8088\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

So there are $672 \times 4 = 2688$ integers coprime to 2022 in the set $\{x \in \mathbb{Z} : 1 \leq x \leq 8088\}$, since 8088 is not coprime to 2022, we find the number of positive integers less than 8088 that are coprime to 2022 is 2688.

c)Just like part b), since any set of consecutive 2022 integers is a complete residue system modulo 2022. we have:

$\{x \in \mathbb{Z} : 1111 \leq x \leq 3132\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

$\{x \in \mathbb{Z} : 3133 \leq x \leq 5154\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

$\{x \in \mathbb{Z} : 5155 \leq x \leq 7176\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

$\{x \in \mathbb{Z} : 7177 \leq x \leq 9198\}$ is a complete residue system modulo 2022, thus contains $\phi(2022) = 672$ integers coprime to 2022.

So there are $672 \times 4 = 2688$ integers coprime to 2022 in the set $\{x \in \mathbb{Z} : 1111 \leq x \leq 9198\}$, since 9199 is coprime to 2022, we find the number of positive integers between 1111 and 9199 that are coprime to 2022 is 2689.

d)We already know that there are 672 integers less than 2022 that are coprime to 2022, we need to count the number of positive integers in the set $\{x \in \mathbb{Z} : 2000 \leq x < 2022\}$ that are coprime to 2022.

Since $2022 = 2 \times 3 \times 337$, if x is coprime to 2022, then $2 \nmid x$, $3 \nmid x$, $337 \nmid x$.

So, 2000 is not coprime to 2022 since $2|2000$.

2001 is not coprime to 2022 since $3|2001$.

......

So $\{x \in \mathbb{Z} : 2000 \leq x < 2022, 2 \nmid x, 3 \nmid x, 337 \nmid x\}$

$= \{2003, 2005, 2009, 2011, 2015, 2017, 2021\}$

thus there are 7 integers in the set $\{x \in \mathbb{Z} : 2000 \leq x < 2022\}$ that are coprime to 2022.

Hence there are $672 - 7 = 665$ integers less than 2000 that are coprime to 2022.

Now, let's give a new proof of "There are infinitely many primes" via Euler's ϕ-function:

Proof:

Assume not, and $p_1, p_2, \cdots p_l$ are all primes.

Construct $n = p_1 \cdot p_2 \cdots p_l$.

Now, $\forall\, m > 1 \in \mathbb{Z}^+$, by Fundamental Theorem of Arithmetic, $m = p_1^{m_1} \cdot p_2^{m_2} \cdots p_l^{m_l}$. $m_1, m_2, \cdots m_l \geq 0$ and at least one of m_i is nonzero.

Thus, $g.c.d.(m, n) \neq 1$.

So $\phi(n) = \#\{x : 1 \leq x \leq n,\ g.c.d.(x, n) = 1\} = 1$.

But, by Euler's ϕ-function's formula:

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_l - 1)$$
$$\geq (2-1) \cdot (3-1) = 2.$$

A contradiction. $\square$

谢谢！