Preliminaries to the proof that $|P|$ is infinite:

Consider $n \in \mathbb{Z}^+$

Let $P = \{2, 3, 5, 7, 11, \ldots\}$ the set of primes

$= \{p_1, p_2, p_3, \ldots\}$ so p_i denotes the i'th prime for $i \in \mathbb{Z}^+$ } not necessary for our proof.

Defn:

- Prime: $\forall n \in P \left(f_n = \{1, n\} \right)$ where f_n is the set of factors of n.
  i.e. n has no factors less than n.
- Composite: $\forall n \notin P \left(f_n = \{1, n, a_1, a_2, \ldots a_m\} \right)$ a finite set with $a_m < n$

Lemma 1: Any number can be written as a product of prime factors (in addition to 1).

If $n \in P$, $f_n = \{1, n\}$

If $n \notin P$ $\quad n = 2^{\ell} 3^{k} 5^{m} 7^{r} \cdots$

Intuition $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdots$

$4 = (2 \cdot 2)$, $6 = (2 \cdot 3)$, $8 = (2 \cdot 2 \cdot 2)$, $9 = (3, 3)$

Corollary $\quad f_n^P \subseteq f_n$ where f_n^P is the set of prime factors of n.

Lemma 2: $\forall n \notin P \left(\frac{n}{q_i} \in \mathbb{Z}^+ \right)$ Dividing a composite number by one of its factors is an int.

Lemma 3: $\forall n, m \in \mathbb{Z}^+$ (If $n = m + 1$ then $f_n \cap f_m = \{1\}$)

(Two consecutive integers can only share 1 as a common factor)

$(n \in P) \vee (m \in P)$ (either/or n or m are prime)

Case 1: tm $f_n \wedge f_m = \{1\}$ //

case 2 $\neg(n \vee m) \equiv (n \notin P) \wedge (m \notin P)$

If neither is prime, then both are composite: $\neg(a \vee b) = \neg a \wedge \neg b$.

Let $f_n = \{1, n, a_1, a_2, \ldots\}$

$f_m = \{1, m, b_1, b_2, \ldots\}$

Given $n = m + 1$

$n - m = 1$

$a_i\left(\frac{n}{a_i}\right) - b_j\left(\frac{m}{b_j}\right) = 1$

If n, m share common factor, $\exists_{i,j}: a_i = b_j$

$a_i\left[\frac{n}{a_i} - \frac{m}{a_i}\right] = 1$ (since $a_i = b_j$)

$\left\lfloor \frac{n}{a_i} - \frac{m}{a_i} \right\rfloor = \frac{1}{a_i} \in \mathbb{Z}$ since $\frac{n}{a_i} \in \mathbb{Z}$ and $\frac{b}{a_i} \in \mathbb{Z}$ Lemma 2

$\therefore a_i = 1$

$f_n \wedge f_m = \{1\}$ //

Back to proof of Q = the set of prime numbers is infinite

$= \forall n \in \mathbb{Z}\ \exists p > n$, where p is prime.

Proof by non-constructive existence.

Consider $y = n! + 1$ ← pick with much "cleverness"

$f_{n!} = \{1, n, 2, 3, 4, \ldots, (n-1)\}$ and $f^p_{n!} = \forall e \in f_{n!} : e \equiv$ prime.

$f_{n!} \cap f_y = \{1\}$ by lemma 3 (since $y - n! = 1$)

<u>case 1</u>: y is prime; $f_y = \{1, y\}$ and $y \in p > n$ //

<u>case 2</u>: y is composite; $f_y = \{1, y, a_1, a_2, \ldots\}$

$\forall a_i \in f_y : a_i > n$ since $f_{n!} \cap f_y = \{1\}$
and $f_{n!} = \{1, n, 2, 3, 4, \ldots, (n-1)\}$

subcase 1: $a_i \in p$ then $\exists p > n$ //

subcase 2: $a_i \notin p$

By lemma 1 a_i can be written as a product of primes.

$a_i \notin f_{n!}$ by lemma 3. also $a_i \notin f^p_{n!}$ *

$f^p_{a_i} = \{1, a_i, b_1, \ldots\}$ where $b_i \notin f_{n!}$ (lemma 3)

Thus there exists a $b \in p$ and $b > n$. //

* Note we made use of the fact that $f^p_n \subseteq f_n$; so if $f_n \cap f_m = \{1\}$
then $f^p_n \cap f^p_m = \{1\}$