(Chapter 12 P83 − 84)

Observation: Let $n \geqslant 2$ be an integer. Then we can always find a prime q such that $q \mid n$.

Two cases: (1) n prime $q = n$

(2) n not prime $n = q_1 \cdots q_r$ with each being prime.

Theorem: There are infinitely many prime numbers.

Euclid's proof: (Proof by contradiction)

Assume that there are finitely many primes.

Then we can list all the primes $P_1, P_2, \cdots P_n$.

We look at

$$A = P_1 P_2 \cdots P_n + 1.$$

Let q be a prime such that $q \mid A$.

Then q should be one of $P_1, \cdots P_n$. For example $q = P_1$

However, $\gcd(P_1, A) = 1 \left(= \gcd(q, A)\right)$ since

$$A - (P_2 \cdot P_3 \cdots P_n) \cdot P_1 = 1.$$

This gives ① $q \mid A$.

② $\gcd(q, A) = 1$

This can never happen at the same time.

This means: we get a contradiction:

This implies: our assumption is wrong!

Therefore, there are infinitely many primes! $\square$

Euler's proof: He looked at

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots=\sum_{p \text{ prime}}\frac{1}{p}$$ infinite series.

He showed $\displaystyle\sum_{p \text{ prime}}\frac{1}{p}=\infty$.

Therefore, there are infinitely many primes.