Challenge Examples/Exercise –

for those who are interested to explore

Problem 1. Show that there do not exist two integers $n, m \in \mathbb{Z}$ such that $n^4 - 4m = 2$.

Hint: Proof by contradiction, i.e. assume that there exist two integers $n, m \in \mathbb{Z}$ such that $n^4 - 4m = 2$ and reach a contradiction.

Solution. Suppose there exist integers $n, m \in \mathbb{Z}$ satisfying $n^4 - 4m = 2$. If n is odd, then n^4 is odd, so $n^4 - 4m$ is odd, which contradicts $n^4 - 4m = 2$. If n is even, then $n = 2k$ for some integer $k \in \mathbb{Z}$, and consequently $n^4 = 16k^2$. Then

$$n^4 - 4m = 16k^2 - 4m = 4(4k^2 - m),$$

which is divisible by 4. But our assumption is that thhis quantity is equal to 2, which is not divisible by 2. Therefore, we have a contradiction whether n is odd or even, so we conclude that no such integers exist.

Problem 2. A natural number $n \in \mathbb{N}$ which is only divisible by 1 and n is said to be a *prime* number. Prove that there are infinitely many prime numbers.

Hint: Proof by contradiction, i.e. assume that there exist finitely many primes $\{p_1, p_2, \ldots p_N\}$, and then try to reach a contradiction. (Clue: Consider the number $P = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$. Is this a prime ?)

Solution. First we prove a Lemma: *every natural number greater than* 1 *has a prime factor greater than* 1. To prove the lemma, we start with a natural number $n \in \mathbb{N}$ and find a prime number $p > 1$ such that $n = ap$ for some integer a. If n is prime, then we are done. Otherwise, n is divisible by a natural number r_1 satisfying $1 < r_1 < p$ and $n = k_1 r_1$ for some k_1. If r_1 is prime, then we are done.

Continue along this process: for each number r_i constructed, stop if r_i is prime. Otherwise, r_i is divisible by a natural number r_{i+1} satisfying $1 < r_{i+1} < r_i$ and $r_i = k_{i+1} r_{i+1}$. Notice that at each step, we decrease the factor. That is, we have a chain of inequalities

$$1 < \cdots < r_3 < r_2 < r_1 < n.$$

This process must stop with at most n steps, so we arrive at a prime number r_m (for some final step m) satisfying

$$n = k_1 r_1 = k_1(k_2 r_2) = k_1(k_2(k_3 r_3)) = \cdots = (k_1 k_2 \cdots k_m) r_m.$$

Therefore, r_m is a prime factor of n, satisfying $n = ap$ for $a = k_1 k_2 \cdots k_m$. Finally, since each r_i was greater than 1 by construction, we have $r_m > 1$, proving the lemma. In fact, if we apply the lemma to the natural number $\frac{n}{r_m} <$ (which is less than n), we find another prime factor of n. Continuing in this until we reach a quotient of 1, we find an even stronger result: *every natural number greater than* 1 *is equal to a product of primes, each greater than* 1.

We proceed with the main proof by contradiction. Assume the result is false, that there are *not* infinitely many primes. Then there are only finitely many primes, say N of them, and we can arrange the primes into a set $\{p_1, p_2, \ldots, p_N\}$. Form the product

$$Q = p_1 p_2 \cdots p_N,$$

and define the number $P = Q + 1$. By the lemma above, P has a prime factor $r > 1$ satisfying $P = ar$ for some integer a.

Since r is prime, it must be in our list, so $r = p_i$ for some $i \in \{1, 2, \ldots, N\}$. Therefore,

$$Q = p_1 p_2 \cdots p_{i-1} p_i p_{i+1} \ldots p_N = (p_1 p_2 \cdots p_{i-1} p_{i+1} \ldots p_N) p_i = br.$$

Where we define $b = p_1 p_2 \cdots p_{i-1} p_{i+1} \ldots p_N$. Recalling the definition of P, $P = Q + 1$, we now have the two equations

$$\begin{aligned} Q + 1 &= ar \\ Q &= br. \end{aligned}$$

Subtracting these two equations, we find $1 = (a - b)r$, so 1 is divisible by r. But $r > 1$, and 1 is not divisible by any number greater than 1, so we arrive at a contradiction. Therefore, we conclude that our original assumption was not true, and there *are* infinitely many primes.