The infinitude of primes — three proofs

Lesson 25 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

Practice problems

1. Suppose $S = \{p_1, p_2, \ldots, p_n\}$ is a finite set of primes that does not contain the prime 2. Prove that the number $P = (p_1 \cdot p_2 \cdot \cdots \cdot p_n) + 1$ must be divisible by 2.

2. Using the factorial method, prove that there is at least one prime p such that $10 < p \leq 11! + 1$.

3. Prove that for any $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is always odd.

Solutions

1. Suppose $S = \{p_1, p_2, \ldots, p_n\}$ is a finite set of primes that does not contain the prime 2. Prove that the number $P = (p_1 \cdot p_2 \cdot \cdots \cdot p_n) + 1$ must be divisible by 2.

   - Since $2 \notin S$, every prime p_i in S must be an odd prime.
   - The product of any number of odd integers is always odd.
   - Therefore, the product $p_1 \cdot p_2 \cdot \cdots \cdot p_n$ is odd.
   - Adding 1 to an odd number results in an even number.
   - Since P is even, it is divisible by 2.

   Answer: P is even, so $2 \mid P$.

2. Using the factorial method, prove that there is at least one prime p such that $10 < p \leq 11! + 1$.

   - Let $n = 10$.
   - Consider the number $Q = 10! + 1$.
   - By the Fundamental Theorem of Arithmetic, Q must have at least one prime factor p.
   - If $p \leq 10$, then p would divide 10!.
   - If p divides both Q and 10!, it must divide their difference: $Q - 10! = 1$.
   - No prime divides 1, so p must be strictly greater than 10.
   - Since p is a factor of Q, $p \leq Q = 10! + 1$.

   Answer: Any prime factor of $10! + 1$ satisfies the condition.

3. Prove that for any $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is always odd.

   - The term 2^{2^n} is a power of 2 with a positive exponent 2^n.
   - Any positive power of 2 is an even integer.
   - Adding 1 to an even integer always results in an odd integer.
   - Therefore, F_n is odd for all $n \geq 1$.

   Answer: F_n = \texteven + 1 = \textodd.
