CS2020A Discrete Mathematics

Tutorial 03 | 18/Aug/2025

Prove the following or give a counterexample.

Theorem 1 (Bézout$^+$). For any two integers a and b, the smallest positive integer that can be expressed as an integer linear combination of a and b is the greatest common divisor of a and b.

Theorem 2 (Euclid's Lemma for arbitrary products) If a prime p divides a product of integers $a_1 a_2 \cdots a_k$, then p divides at least one of them.

(Write the above proof rigorously using induction)

Theorem 3. The prime factorization of a number n contains at most $\log_2 n$ factors.

Theorem 4 (Fermat's Little Theorem) For any integer n and prime p, p divides $n^p - n$.

Complete the following proof.

Proof.

1. Imagine a sequence of p numbers, where each number is from $\{1, 2, \ldots, n\}$.
2. How many different sequences are possible?
3. How many of them are constant? (All p numbers are the same)
4. How many of them are non-constant?
5. Group the non-constant sequences so that each group consists of all the cyclic shifts of a single sequence. (For example if $n = 2, p = 3$, then the sequences $(1, 1, 2)$, $(1, 2, 1)$ and $(2, 1, 1)$ belong to the same group.
6. [Difficult Step] How many sequences are there in each group?
7. How many groups are there?
8. How does it prove Fermat's Little Theorem?