CS2020A Discrete Mathematics

Tutorial 3 Submission

Submitted By

Kalakuntla Parjanya	**112401018**
Prachurjya Pratim Goswami	**102401023**
Chavva Srinivasa Saketh	**112401009**
Madeti Tarini	**112401020**
Vedant Singh	**142401041**

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.

Proof: Let S be the set of all positive integers that can be written as a linear combination of a and b. We see that there always exists a set of integers α, β such that $\alpha a + \beta b > 0$. Thus, S is not an empty set.

can not write see that. give one elem from S(1)

Now, let k be the least possible integer that exists in S. Then,

$$\alpha a + \beta b = k \qquad \text{for some } \alpha, \beta \in \mathbb{Z} \tag{1}$$

Claim: k divides a

Let,

$$\begin{aligned} a &= kq + r \quad (0 \leq r < k) \\ r &= a - kq \\ r &= a - (\alpha a + \beta b)q \quad \text{(From (1))} \\ r &= (1 - \alpha q)a + (-\beta q)b \\ r &= \alpha' a + \beta' b \end{aligned}$$

This shows that $r \in S \cup \{0\}$. But r can never be a part of S as k is the least value in it and $r < k$. Thus $r = 0$. So, k divides a.

Similarly, k divides b.

So, k is a common divisor of a and b.

Assume $a = q_1 k$ and $b = q_2 k$ .Then from (1),

$$\begin{aligned} \alpha(q_1 k) + \beta(q_2 k) &= k \\ \alpha q_1 + \beta q_2 &= 1 \end{aligned}$$

this is converse of Bezout's. Need some proof.

Then from Bézout's Lemma, q_1 and q_2 are co-primes. Due to this reason, there exist no greater common factors between a and b except k itself.

So, k is the GCD of a and b.

Theorem 2 (Euclid's Lemma for arbitrary products) : If a prime p divides a product of integers $a_1, a_2, \ldots, a_k$, then p divides at least one of them. (Write the above proof rigorously using induction)

Proof: Base case of Induction: taking k=1. This is a direct statement as $p|a_1$
Take k=2 for base case. Eles not prod of integers.
Now considering the induction hypothesis: Let the statement be true for all integers less than equal to l:
$\therefore p|(a_1 \cdot a_2 \cdot a_3 \cdots a_l) \implies p$ divides at least one of them.

Now showing that this statement also holds for $l+1$:
Let $p|(a_1 \cdot a_2 \cdot a_3 \cdots a_l \cdot a_{l+1})$, now taking $a_1 \cdot a_2 \cdot a_3 \cdots a_l$ as b, we have $p|b \cdot a_{l+1}$

We have p as the product of two integers b and a_{l+1}. Now from the above induction hypothesis, we know the statement holds true for $k = 2$. So, either $p|a_{l+1}$ or $p|b$.

Now if $p|a_{l+1}$, the statement becomes true for $l+1$.
And if $p|b$, that is $p|(a_1 \cdot a_2 \cdot a_3 \cdots a_l)$, from induction hypothesis, we know that p must divide at least one of them.
$\therefore$ The statement holds true for $k = l+1$ ✓

Therefore, if $p|(a_1 \cdot a_2 \cdot a_3 \cdots a_k)$, then p must divide one of them for all $k \in \mathbb{Z}$

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

Proof: Let n be the number being considered. The length of prime factorization is finite, so consider general format $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$.
Then, the prime factorization of n is:

$$n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \ldots\ldots, \text{ where } (\alpha, \beta, \ldots \in \mathbb{Z})$$

Now, taking log on base 2 on both sides,

$$\implies \log_2 n = \alpha + \beta \cdot \log_2 3 + \gamma \cdot \log_2 5 + \ldots\ldots$$
$$\implies \log_2 n = \alpha + \beta + \gamma \ldots + (\log_2 3 - 1) \cdot \beta + (\log_2 5 - 1) \cdot \gamma + \ldots$$
$$\implies \log_2 n \geq \alpha + \beta + \gamma \ldots\ldots \quad (\because \log_2 3 > 1, \log_2 5 > 1, \ldots)$$

Then use same idea with $p_i \geq 2$ $\forall i$

It is worth noting that $\alpha + \beta + \gamma \ldots\ldots$ is the total no. of factors of n. Thus, we have shown that $\log_2 n$ is the maximum no. of factors that any number n can have.

$\therefore$ The prime factorisation 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?

Solution:

4.2. For every number in we have n choices $\implies$ n^pdifferent sequences are possible.
4.3. All p numbers can be equal to any of the n numbers in the set $\implies$ There are n constant sequences.
4.4. $n^p - n$ sequences are non-constant.
4.6. For cyclic shifts of a particular group, there are 2 possibilities on the number of sequences possible.
Case I: Sequence repeats after p shifts
In this case, we are done.
Case II: Sequence repeats before p shifts
This means
$\exists k < p$ such that $k|p$ (since, there are p numbers in each sequence)
But this contradicts the fact that p is a prime number.

explain this part.

Thus, **number of such sequences possible is p.**
4.7. This means the total number of groups possible are

$$\frac{n^p - n}{p}$$

4.8 As the number of groups possible can only be a non-negative integer

$$p|n^p - n$$