Problem

Show that if P = NP, you can factor integers in polynomial time. (See the note in Problem 7.38.)

Step-by-step solution

Step 1 of 1

An integer can be factorized in multinomial time if $P = NP$ has given.

• Consider the language

$L = \{\langle n, x, y\rangle \mid n \text{ has a factor } p \text{ in the range } x \le p \le y\}$.

• Assume $P = NP$ and the above language can be decided by a polynomial algorithm.

• Each time the search space is divided into half by using repeated applications of the algorithm.

• The repetition is done by asking “Is a factor exists in the range $\left(x, \frac{x+y}{2}\right)$?”. If the factor is not in this region then it can be said that there is a factor in other range.

• The number of times the algorithm applied here is sufficient to $\log n$. In other words it can also be said that, it will take $O(k)$, if k is the number of bits exists in n. So, one factor can be isolated by using the algorithm which consist polynomial number of applications.

Since it has maximum $O(k)$ factors, therefore it can be said that, every factors can be found in polynomial time.

Comment