Problem

Show that *PRIMES* = {ml m is a prime number in binary} ? NP. (Hint: For p > 1, the multiplicative group Z^*_p = {xl x is relatively prime to p and 1 ≤ x < p} is both cyclic and of order p – 1 iff p is prime. You may use this fact without justifying it. The stronger statement *PRIMES* ? P is now known to be true, but it is more difficult to prove.)

Step-by-step solution

Step 1 of 2

Here, $\mathbf{PRIMES\,(P) = \{m \mid m \text{ is a prime number in binary}\} \in NP}$ can be proved by the following approach.

Now, consider two situations:

1. Consider a situation where $P>1$: (Because all prime numbers are greater than 1).

2. The multiplicative group $Z^*_P = \{X|X \text{ is relatively prime to P and } 1 \le x \le P\}$.

Comment

Step 2 of 2

Here, a situation is considered where *x* is a relative prime number the value of x lies between 0 and 1.

• Both conditions are cyclic as the both situations can be combined and can lie between 1 and P.

• **Order of these conditions is** $P\text{-}1$ **if** P **is prime as the range lies between 1 and P then the order between P-1. This fact is alone sufficient to prove the statement** $\text{PRIMES (P)} = \{m| \text{ m is a prime number in binary}\} \in NP$ and second considered situation are quite enough itself to justify the statement.

• It can be proved by **the fact of belonging of prime numbers to** $co\text{-}NP$ **and consider prime numbers belong to** $co\text{-}RP$**.**

• **Thus, required statement will be true as well, because belongingness of NP can be proved only if belongs to** $co\text{-}NP$ **and** $co\text{-}RP$ **as well.**

This it is quite obvious that, $\mathbf{PRIMES\,(P) = \{m \mid m \text{ is a prime number in binary}\} \in NP}$.

Comment