factoring, in the sense that if we have an algorithm for factoring we can easily modify it to do primality testing, but if we have an algorithm for primality testing it is not clear how to use it to quickly find a factor when the given number happens to be composite. In mathematical jargon, we say primality testing reduces to factoring.

A PTIME algorithm for the primality testing problem was found by Manindra Agrawal, Neeraj Kayal and Nitin Saxena of IIT Kanpur in 2002. Resonance has carried an article about this earlier [2]. So now we know that not only addition and multiplication but also primality testing can be done in PTIME. Is there an algorithm waiting to be found which will show that factoring falls into the same class of problems? The opinion among computing scientists is divided.

Suggested Reading


Erratum


Please note the correct dates for the course given below:

Refresher Course in Experimental Chemistry
June 15–29, 2009
at School of Chemistry, University of Hyderabad, Hyderabad 500 046

See website for further details:
http://www.ias.ac.in/resonance/March2009/p307-309.pdf