

Intractable problems with composites

Consider the set of integers: (e.g. for $n=1024$)

$$\mathbb{Z}_{(2)}(n) := \{ N = p \cdot q \text{ where } p, q \text{ are } n\text{-bit primes} \}$$

Problem 1: Factor a random N in $\mathbb{Z}_{(2)}(n)$ (e.g. for $n=1024$)

Problem 2: Given a polynomial $\mathbf{f(x)}$ where $\text{degree}(f) > 1$
and a random N in $\mathbb{Z}_{(2)}(n)$

find x in \mathbb{Z}_N s.t. $f(x) = 0$ in \mathbb{Z}_N