Computational Number Theory (CS60094)

Spring Semester, 2023

Tutorial - 4

1. Explain why the functions $f(x) = x^2 \pmod{n}$ and $f(x) = x^2 - 2 \pmod{n}$ are not chosen in Pollard's rho method for factoring n.

2. We say that a positive integer n can be written as the sum of two squares if $n = a^2 + b^2$ for some positive integers a, b.

   - Show that if two odd integers m, n can be written as sum of two squares, then their product can also be so written.
   - Prove that no $n \equiv 3 \pmod{4}$ can be written as a sum of two squares,
   - Let a square-free composite integer n be a product of distinct primes each congruent to 1 (mod 4). Show that n can be written as a sum of two squares in (at least) two different ways.
   - Suppose n is a square-free composite number. Suppose that we know two ways of expressing n as a sum of two squares. Describe how n can be factored easily.

3. Write a pseudocode implementing Floyd's variant of Pollard's rho method with block GCD calculations.

4. In Floyd's variant of Pollard's rho method for factoring integer n, we compute the values of x_k and x_{2k} and then $gcd(x_k - x_{2k}, n)$ for $k = 1, 2, \cdots$. Suppose that we instead choose some $r, s \in \mathbb{N}$ and compute x_{rk+1} and x_{sk} and subsequently $gcd(x_{rk+1} - x_{sk}, n)$ for $k = 1, 2, \cdots$.

   - Deduce a condition relating r, s and the period τ' of the cycle such that this method is guaranteed to detect a cycle of period τ'.
   - Characterize all the pairs (r, s) such that this method is guaranteed to detect cycles of any period.

5. You are given a black box that given two positive integers n and k, returns in constant time the decision, whether n has a factor d in the range $2 \leq d \leq k$. Using this black box, devise an algorithm to factor a positive integer n in polynomial (in $\log(n)$) time. Deduce the running time of your algorithm.