Cryptography

Problem set 7 - 22-23 V 2013

Problem 1 The n^{th} Fermat number is of the form $F_n = 2^{2^n} + 1$. Prove that any Fermat number is a pseudoprime to the base 2. Use the Fermat test to prove that F_5 is composite.

Problem 2 Prove that a Carmichael number has at least three different prime factors.

Problem 3 Use the Miller-Rabin test to prove that the fifth Fermat number F_5 is composite. Compare the efficiency of the test with the efficiency of the Fermat test.

Problem 4 During a lecture, we defined:

Definition (Miller-Rabin Compositeness Witness) Let $d = (n-1)/2^s$ where 2^s is the largest power of 2 that divides $n-1$. We call a a *witness* for the compositeness of n if $gcd(a, n) = 1$ and a satisfies neither: $a^d = 1 \bmod n$ nor $a^{2^r d} = -1 \bmod n$ for all $r \in \{0, 1, \ldots, s-1\}$.

We proved the following theorem:

Theorem 0.1 *(Efficiency of Miller-Rabin test) If $n \geq 3$ is an odd composite number, then the set $\{1, \ldots, n-1\}$ contains at most $(n-1)/4$ numbers that are prime to n and not witnesses for the compositeness of n.*

Determine the number of Miller-Rabin witnesses for the compositeness of 221 in $\{1, 2, \ldots, 220\}$. Compare your result with the bound in the Theorem.

Problem 5 Use the $p-1$ method to factor $n = 138277151$.

Problem 6 Factor 11111 using the quadratic sieve.

Problem 7 Find a system of (quadratic) equations corresponding to a problem of factoring $N = pq = 64349$ (express p and q in Zeckendorf representation).

1. Find solutions of this equation using *i.e.,* Mathematica.
2. Present how JOFA algorithm would find a solution. You may assume that p has in the representation Fib_{12} while p, Fib_{13}.

Problem 8 Use the baby-step giant-step algorithm to compute the discrete logarithm of 693 to the base 3 mod 1823.