ASSIGNMENT - 05
COMP 544 - ALGORITHM
ALGORITHM ASSIGNMENT GROUP - 03

1. **Do problem 6.17 in the textbook. Consider Shank's algorithm—algorithm 6.4. Show that Shank's algorithm computes x, such that g x ≡p h, in time O(n log n), that is, in time O(√p log (√p)).**

Ans. Assuming that intersection of L_1 and L_2 are implemented optimally with $O(1)$ lookup time complexity (by using some kind of dictionary), we can say that Shank's baby step-giant step Algorithm runs in $O(N\ LogN)$, $where\ N\ is\ \sqrt{p}$ complexity. Because L_1 runs for N times and L_2 runs for N times with calculating of multiplicative inverse which costs $logN$. So, Finally, the total time complexity is $O(N\ LogN)$, $where\ N\ is\ \sqrt{p}$.

2. **Do problem 6.18 in the textbook.**

Ans.
https://drive.google.com/file/d/1IVsa-b1Pi2J87LXLwwGCDfOlitbmkJhG/view?usp=sharing

3. **Implement the Rabin-Miller algorithm where the input is assumed to be an integer given in binary (see Problem 6.11) - you may use the implementation given here.**

Ans.
https://drive.google.com/file/d/1gg3E1Y9tVXJXpUwHMUqWtRIHCdWAfDIc/view?usp=sharing

4. **Run the following experiment: if n is not prime, compute how many witnesses (of compositeness) there are. Plot the results for many n's, and hypothesize on a good asymptotic approximation to the function fw (n) = m where m is the number of witnesses for a given n (of course, m = 0 if n is prime).**

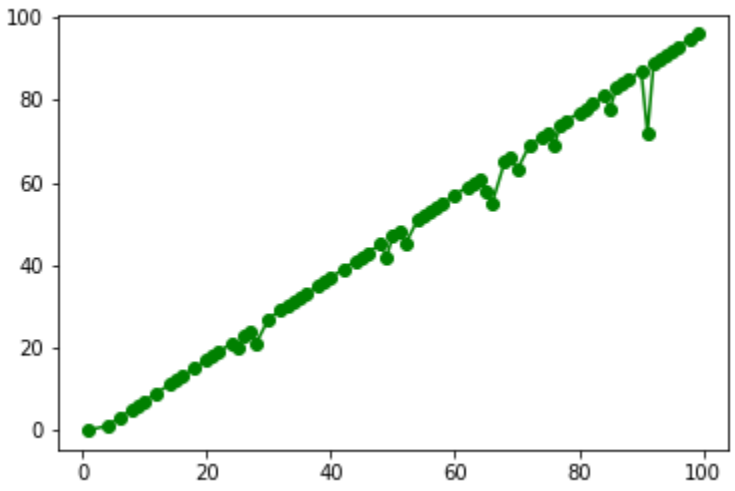
Ans. Monier showed the proportion of Miller–Rabin witnesses for p(2p − 1) tends to 75% if we can let p → ∞, and it's expected that we can: it is conjectured that p and 2p − 1 are both prime for infinitely many primes p ≡ 3 mod 4. This 75% is probably sharp as an asymptotic lower bound.

A good approximation of the upper bound is n, and the lower bound is $\frac{3n}{4}$ *or* 75%

We are observing a behavior that $f_w(n) = m$ acts like $m = n - 2$ for any appropriate number passing Rabin-Miller. Our implementation may possess a source of error, but based on it, this is the function we would hypothesize.

The Rabin-Miller implementation described below contains code to run this experiment as its default behavior.

Witnesses of Compositeness



https://drive.google.com/file/d/1eoP9eAiKo7ZFMuky11B8oGyhVXWenY2P/view?usp=sharing