Homework 6

1) Let n be a positive integer. Show that if n is composite then there exists a prime divisor of n that is less than or equal to $\sqrt{n}$.

2)

3.15. Use the Miller–Rabin test on each of the following numbers. In each case, either provide a Miller–Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that are not Miller–Rabin witnesses for n.

(a) $n = 1105$. (Yes, 5 divides n, but this is just a warm-up exercise!)

(b) $n = 294409$

(c) $n = 294439$

3)

3.17. The function $\pi(X)$ counts the number of primes between 2 and X.

(a) Compute the values of $\pi(20)$, $\pi(30)$, and $\pi(100)$.

(b) Write a program to compute $\pi(X)$ and use it to compute $\pi(X)$ and the ratio $\pi(X)/(X/\ln(X))$ for $X = 100$, $X = 1000$, $X = 10000$, and $X = 100000$. Does your list of ratios make the prime number theorem plausible?

4) Recall that

Pohlig-Hellman algorithm tells us that the discrete logarithm problem is easy to solve if ord(g) is a product of small prime powers.

In particular, Diffie-Hellman is easy to break if $p-1$ is a product of small prime powers

Hence, for Diffie-Hellman exchange protocol, we should choose p such that $p = 2q+1$ where q is prime and use g such that $\mathrm{ord}(g) = q$.

Such prime p is called safe prime.

Describe an algorithm to geneate a safe prime.

5) Let p be a prime. Show that $n = 2p+1$ is a prime if and only if $2^{n-1} \equiv 1 \mod n$.