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 $\sqrt{n}$.

1a) Show that n being composite has a (nontrivial) divisor $\leq \sqrt{n}$.

If n is composite, then n must have a nontrivial divisor $d \neq 1, n$

Supose $d > \sqrt{n}$, then $q = \frac{n}{d} < \frac{n}{\sqrt{n}} = \sqrt{n}$

b) Show that n being composite has a prime divisor $\leq \sqrt{n}$.

From (a) there exists a divisor q of n that is $\leq \sqrt{n}$.

So, the prime divisor of q must also divides n and is also $\leq \sqrt{n}$.

2) Write computer program

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) $n = 294439$

If n is composite, Miller Rabin test aims to find a witness. To get 10 numbers which are not Miller Rabin witness, use $k=10$.

Algorithm

Algorithm
Inputs: n: a value to test for primality, $n>3$; k: a parameter that determines the number of times to test for primality
Output: *composite* if n is composite, otherwise "strong *probably prime*"

$n-1 = 2^e q$
q is odd

repeat k times:

pick a number between $[2, n-2]$
Test if $a^q \not\equiv 1 \bmod n$ and $a^{2^i q} \not\equiv -1 \bmod n$ for $0 \le i < e$.
If yes, return "composite".

If composite is not return, return "strong probable prime"

3) Use calculator

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?

$$\pi(x) \approx \frac{x}{\ln(x)}$$

If I want to know the number of primes of 1024 bit, $\pi(2^{1024}-1) - \pi(2^{1023})$

$$= \frac{2^{1024}-1}{\ln(2^{1024}-1)} - \frac{2^{1023}}{\ln(2^{1023})}$$

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 $ord(g) = q$.

Such prime p is called safe prime.

Describe an algorithm to geneate a large safe prime.

Give informal analysis of the complexity and accuracy.

probability a N is a prime $\sim \frac{1}{\ln(N)}$

probability that $n \in (\frac{1}{2}N, \frac{3}{2}N)$ is a prime $\sim \frac{1}{\ln(N)}$

probability a number N is a safe prime ?

$q = 2$, $p = 5$

$q = 3$, $p = 7$

$q = 5$, $p = 11$

$q = 7$, $p = 15$

$q = 11$, $p = 23$

$q = 13$, $p = 27$

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

$\rightarrow$ If $n = 2p+1$ is a prime, then $2^{n-1} \equiv 1 \mod n$.

proof: By Fermat's little theorem.

If n is prime, then $a^{n-1} \equiv 1 \mod n$

for $\gcd(a, n) = 1$.

$\leftarrow$ If $2^{n-1} \equiv 1 \mod n$, then $n = 2p+1$ is prime.

Proof Attempt 1: Assume that n is not prime.

Then there exists a prime $\underline{q}$ that divides n.

$$2^{n-1} \equiv 1 \mod q$$

$$2^{2p} \equiv 1 \mod q$$

exponent lives in $q-1$.

If $\gcd(p, q-1) = 1$, then $\exists\, p^{-1}$.

$$2^{2p \cdot p^{-1}} \equiv 1^{p^{-1}} \mod q$$

$$2^{2} \equiv 1 \mod q$$

$q = 3$

This implies that n is a power of 3.

n can not be 3 because otherwise $p = 1$ which is not prime.

How about $n = 3^i$ where $i \geq 2$?

Proof Attempt 2:

Assume that n is not prime.

Then there exists a prime $q < n$ that divides n.

$$2^{n-1} \equiv 1 \mod q^e$$

$$2^{2p} \equiv 1 \mod q^e$$

Where e is the largest exponent such that q^e divides n

Exponent lives in modulo $\varphi(q^e)$

If $\gcd(p, \varphi(q^e)) = 1$, then p^{-1} exist.

$$2^{2p \cdot p^{-1}} \equiv 1 \mod q^e$$

$$2^2 \equiv 1 \mod q^e$$

$$3 \equiv 0 \mod q^e$$

Which implies $q^e \mid 3$.

This can only happen when $q = 3$, $e = 1$.

The proof requires that $\gcd(p, q-1) = 1$.

Is it true ?

- $p=2$, $q=3$, $\gcd(p, q-1) = 2$

- So, we should consider only odd prime p.

  For even prime p, $p=2$ and $n=5$

  which is prime.

- Let p be odd prime.

  If $\gcd(p, q-1) \neq 1$, then it is p.

  and $p \mid q-1$.

- Show that $p \nmid q-1$.

  Recall that p is odd prime, q is

  prime and $q \mid 2p+1$, $q < 2p+1$

- Hence, $\gcd(p, q-1) = 1$