Intro to Quantum Computing : ECES 622 - Winter 2012

Homework 1: Team effort , Max: 100 pts
Due date: January 16, 2012, in class.

In class, we talked about the fundamental theorem of arithmetic which states that any natural number can be decomposed as a unique product of prime numbers. The prime numbers play a fundamental role in quantum computing, especially in problems related to cryptography systems. In the next few exercises, you will investigate the prime numbers in a little more detail. This is a very fascinating field in which many simple assertions or conjectures have been made which have yet to be proven or disproven. It has been shown a long time ago that there is an infinite number of primes. As of January 2000, the best known exact result was that there were exactly 2,220,819,602,560,918,840 primes less than $10^{20}$.

**Problems**

(1) (20 pts) First read the few pages attached as an appendix which come from the book by Sarah Flannery, *In code, a mathematical journey* published by Algonquin, books of Chapel Hill. These pages describe the *Sieve of Erathostenes* which is the earliest scheme to find out which natural numbers are prime numbers. That scheme works very well for generating the prime numbers with a fairly small number of digits, but becomes time consuming when natural numbers with a large numbers (several tens) of digits are involved.

Once you have read and understood the *Sieve of Erathostenes*, use it to enumerate all the prime numbers less than 500, starting with 2, the smallest prime number.

(2) (20pts) The fundamental theorem of arithmetic says that any positive integer can be decomposed as some product of prime numbers. Find the prime factorization of the following integers: (1) 45, (2), 129, (3) 5254. Explain the procedure you used to find these factors.

(3) (20 pts) Over the centuries, people have tried to come up with some generic formulas which would automatically generate some, if not all, prime numbers

One of the early attempts included the conjecture by Euler that all the numbers of the form

$$E(n) = n^2 - n + 41 \tag{1}$$

are primes. Show that it is not the case for E(41) and E(42) by finding the primal decomposition of these these two numbers, i.e, prove that they are the product of two prime numbers.

(4) (20pts) Another mathematician (Mersenne) claimed that the numbers now known under his name

$$M(n) = 2^n - 1 \tag{2}$$

are prime numbers. Prove that it is not the case by finding the prime decomposition of the first 9 Mersenne numbers, M(n) for n=1 to 9.

(5) (20 pts) The Hilbert numbers are the natural numbers (apart from 1) which can be written as 4x(natural number) + 1.

(a) Determine all the Hilbert numbers also referred to as Hilbert primes less or equal to 100.

(b) Show that if you multiply any 2 Hilbert numbers you will always get another Hilbert number.

(c) 1617 is a Hilbert number (show it). It can be completely factored as a product of Hilbert primes in two different ways, i.e,

$$1617 = H_1 X H_2 = H_3 X H_4 \tag{3}$$

Find the values of $H_1$,$H_2$,$H_3$,$H_4$.