NUMBER THEORY: CLASS 6

1. Exercise

1) Factor 10961 using Fermat factorization method.

Note: $\lceil\sqrt{10961}\rceil = 114, 114^2 = 12996$ and $115^2 = 13225$.

2) Find computational complexity of Fermat factorization method on number n. Assume that finding whether an n binary digits is a perfect square takes $O((log(n))^2)$ bits operation.

3) The theorem states:
If $2^n - 1$ is a prime then n is a prime.
Show that the converse is not always true by find a prime p such that $2^p - 1$ is not a prime.

The commands: $isprime(n)$; and $ifactor(n)$; in Maple program might be helpful.

4) The theorem states:
If $2^n + 1$ is a prime ≥ 5 then $n = 2^k$ for some positive integer k.
Show that the converse is not always true by find an integer k such that $2^{2^k} + 1$ is not a prime.

5) Show there are infinitely many prime of the form $6n + 5$.

Date: Tuesday, September 16, 2008.