NUMBER THEORY: FIRST MIDTERM

The first midterm will be on Tuesday September 23. There will be six problems. Four problems will be from (or very similar) the note in the lecture, problems after class or homework 1 - 3.

Review session is on Monday September 22 from 5-7 at my office, Tome 241. I will mostly answer the questions you have.

1. Topics

Computational Complexity Analysis:

Big O notation
Exponential time VS Polynomial time algorithm.

Algorithm

Primality test of integer n by checking divisibility of all the primes $\leq \sqrt{n}$.
The Euclidean algorithm to find $gcd(a, b)$.
The Fermat factorization algorithm.

Others

Solving linear recurrence relation
Solving identities (For example Fibonacci identities)
Solving linear diophantine equation
Infinitude of primes of the form $an + b$, when $gcd(a, b) = 1$
Irrationality (or integer) of $\sqrt[k]{a}$, $\sqrt{a} + \sqrt{b}$, $\log_a b$
Mersenne prime, $2^n - 1$ and Fermat prime, $2^n + 1$
Generating function.

Date: Friday, September 19, 2008.