NUMBER THEORY: SECOND MIDTERM

The second midterm will be on Tuesday November 11. There will be eight problems. Six problems will be from (or very similar) the note during the lectures, problems after classes or homework 4 - 7.

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

1. Topics

Primality Test
Pseudoprime, Strong Pseudoprime

Factorization Algorithm
Pollard Rho method
Mersene Number, Fermat Number

Ohters
Solving Linear Congruence Equation
Chinese Remainder Theorem
Fermat's Little Theorem, Wilson's Theorem, Euler's Theorem
$\phi(n), \sigma(n), \tau(n)$, perfect number

Date: Friday, November 7, 2008.

2. Summary of Theorems

1. **Congruence**

Assume $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then
i) $a + c \equiv b + d \bmod m$
ii) $a - c \equiv b - d \bmod m$
iii) $ac \equiv bd \bmod m$

iii) also implies $a^k \equiv b^k \bmod m$ for a non-negative integer k.

2. **Chinese Remainder Theorem**
Solving the system of linear congruence

$x \equiv a_1 \bmod m_1$
$x \equiv a_2 \bmod m_2$
...
$x \equiv a_r \bmod m_r$

or
$b_1 x \equiv a_1 \bmod m_1$
$b_2 x \equiv a_2 \bmod m_2$
...
$b_r x \equiv a_r \bmod m_r$

3. **Perfect number**
$2^k - 1$ is prime and $N = 2^{k-1}(2^k - 1)$ if and only if N is an even perfect number.

4. **Pollard Rho Method**

Lemma Assume n to be a composite number and r be a factor of n. Let λ be a positive real number and $l = 1 + \lfloor \sqrt{2\lambda r} \rfloor$.
The chance that $x_0, x_1, ..., x_l$ are all distinct (mod r) is less than $e^{-\lambda}$.

Theorem Given a composite number n, the rho method will reveal the factor r in $O(n^{\frac{1}{4}}(log(n))^3)$ bit operations with a high probability (Chance of success is at least $1 - e^{-\lambda}$ using notation in the previous lemma).

5. **Special Congruence**

Fermat's Little Theorem
Let p be a prime and a is a positive integer such that p does not divide a.
$a^{p-1} \equiv 1 \mod p$.

Wilson's Theorem
Let p be a prime.
$(p-1)! \equiv -1 \mod p$.

Euler's Theorem
If m is a positive integer and a is an integer with $gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \mod m$.

6. **Mersene prime related**

Theorem If p is a prime dividing $b^n - 1$, then either
i) $p|b^d - 1$ for some proper divisor d of n or
ii)$p \equiv 1 \mod n$.

7. **Carmichael Number related theorems**

1) Carmichael number is square free.
2) Assume n is square free.
n is a Carmichael number if and only if $(p-1)|(n-1)$ for every prime factor p of n.
3) Carmichael number must be the product of at least 3 distinct primes.

8. **Multiplicative function**

Theorem $\phi(n)$ is a multiplicative function.
Theorem $\sigma(n)$ is a multiplicative function.
Theorem $\tau(n)$ is a multiplicative function.