# MAT 321-1
# Main Topics for Test 2

## Test date: Tuesday, April 10

## Factorization

Be able to:

- find the standard prime factorization of an integer
- use the standard prime factorizations to find the gcd and lcm of two integers
- use the standard prime factorization to find the number of divisors of an integer
- deduce the prime factorization form of an integer, given the number of its positive integer divisors
- perform the Pollard Rho method of factorization (with Maple)

## Chinese Remainder Theorem and applications

Be able to:

- solve a system of congruences by the iterative method (by hand)
- solve a system of congruences using Maple's **chrem** command
- solve problems involving applications to computer arithmetic

## Euler's Phi Function

Be able to:

- find (by hand) and interpret Euler's Phi Function of an integer
- calculate the probability that a randomly chosen integer between 1 and n is relatively prime to n
- show certain values of $\varphi(n)$ are impossible

## General cryptology

Be able to:

- encipher, decipher and break shift transformation ciphers
- encipher and decipher affine transformation ciphers
- encipher and decipher exponentiation ciphers

## RSA public key cryptosystems

Be able to:

- construct and test the conditions for the public and private portions of an RSA key
- encipher and decipher signed and unsigned RSA messages

---

*To print a copy of your Maple worksheet to turn in with your test:*

1. *make sure your name is on it,*
2. *after you print it, Dr. Spackman will retrieve it from the printer and deliver it to you at your seat.*