MAT 321-1
Main Topics for the Final Exam
Tuesday, May 8, 8:00 – 11:00 am, BR 164

<u>In addition</u> to the topics listed on the Main Topics for Tests 1 and 2, are these (covered after Test 2):

Order and primitive roots

Be able to:

- find the order of a mod m, both by hand and with Maple
- find all primitive roots mod m, both by hand and with Maple
- determine, by its prime factorization, whether an integer has a primitive root or not
- determine efficiently by hand whether an integer is a primitive root mod m or not

Applications of primitive roots

Be able to:

- use Maple to perform the primitive root primality test, on large primes n, when some information is known about the prime factors of n-1, and find the "certificate of primality" for such primes
- find the period of a pseudo-random number generator
  - experimentally with Maple
  - by formula for linear congruential and pure congruential generators

Proofs

I will ask you to write one of the following proofs on the final exam:

- Euclid's proof that there are infinitely many primes
- (RSA decoding) If $C \equiv P^e \bmod n$ and $ed \equiv 1 \bmod \phi(n)$, then $P \equiv C^d \bmod n$
- $ord_m a \mid x$ if and only if $a^x \equiv 1 \bmod m$

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

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

<u>No books, notes, Web or saved Maple worksheets are permitted on the Final Exam. All computer work must be done starting with a blank Maple worksheet.</u>