

NUMBER THEORY

Math 522

Michael E. O'Sullivan

Preparing for the Final Exam

I. Cumulative Material

- Prove simple properties of the Fibonacci numbers.
- Convert from one base to another.
- Compute in a given base (addition, multiplication in bases 2, 3).
- Compute the gcd of two integers using the Euclidean algorithm. Write the gcd as a linear combination of the two integers.
- Solve a linear diophantine equation.
- Use divisibility rules.
- The unique factorization theorem is one of the most fundamental results in number theory. Be able to use it in a variety of contexts.
- Solve a linear congruence in one variable.
- Solve a system of linear congruences modulo n in two variables.
- Solve a system of congruences in one variable with different moduli using the algorithm from the Chinese remainder theorem.
- The Chinese remainder theorem is another of the fundamental results in number theory. Be able to use it in a variety of contexts.

II. New Material

- Know and be able to use the properties of the Euler phi function.
- Use Fermat's little theorem and Euler's theorem.
- Understand the RSA cryptosystem.
- Find the gcd of two polynomials modulo a prime p using the Euclidean algorithm. Write the gcd as a sum of multiples of the two polynomials.
- Be able to compute the order of an integer a modulo m for $(a, m) = 1$.
- Modulo a prime, understand and be able to use primitive roots and discrete logs.

No calculators can be used on the final exam.