Carthage Mathematics Department
Course Summary for Math 3240: Number Theory

1. Credits: 4
2. Semesters Offered: As demand dictates
3. Text(s): *Elementary Number Theory* (6th Ed.), by David Burton
4. Topics Covered:
    a. Primes: distribution, Prime Number Theorem, primality testing, pseudoprimes
    b. Divisibility: gcd and lcm, Euclidean algorithm, factorization, divisibility testing
    c. Congruences: Chinese Remainder Theorem, Polynomial congruence, Wilson's theorem, Fermat's little theorem, primitive roots
    d. Arithmetic Functions: Euler's totient function; number & sum of divisors functions; perfect & amicable numbers
    e. Cryptology: substitution ciphers, Vigenère cipher, public key cryptography
    f. Diophantine Equations: Pell's equation, Fermat's Last Theorem, sums of squares/powers
    g. Other topics (optional): calendar systems, history of important theorems/mathematicians, Möbius inversion, quadratic reciprocity, cyclotomy, check digit schemes, irrational and transcendental numbers
5. Skills Enhanced:
    a. Computation: Students will design and implement basic algorithms for the purposes of (i) evaluating theorems and/or searching for counterexamples, (ii) implementing primality/divisibility tests, (iii) implementing cryptographic schemes, and (iv) other relevant topics of the instructor's interest. In the process, students will become familiar with a computing language, and basic programming concepts such as recursion, iteration, and time complexity.
    b. Proof writing: Students will write regular mathematical proofs, usually (but not necessarily) taken from class homework. These will be typewritten, and typically not more than 1 page in length for each proof. The main goal of these assignments is for students to learn how to express mathematical ideas using the formality and rigorous logic that mathematics requires.
    c. Oral presentation: Students will regularly present their work (from a variety of assignments) to the class. In addition to practicing presentation skills, this will permit students to critique each other's work, and participate in the critical inquiry that is crucial to the functioning of the mathematics community.
6. Sample Syllabus:
   Chapters 1-8. [Note: several sections should be omitted based on time and preference.]

7. Course Goals: By the end of the course, students should be able to do the following:
    a. State and prove basic theorems of elementary number theory: infinitude of primes, fundamental theorem of arithmetic, Euclid's lemma.
        i. Assessment: Homework assignments and exams include questions that require this knowledge.
    b. Use time complexity arguments to evaluate the relative efficiency of factoring algorithms.
        i. Assessment: Exams and quizzes include questions that require this ability.
    c. Write and implement basic algorithms designed to factor and/or test primality of large numbers.
        i. Assessment: Formal writing assignments are evaluated for computational correctness & success as well as correctness of writing.
    d. Write proofs using the correct number-theoretic notation and form.
        i. Assessment: Homework assignments are evaluated for competence of writing as well as mathematical correctness.

e. Assess the benefits and drawbacks of the various ID number verification and encoding methods using modular arithmetic arguments
    i. Assessment: Exams and quizzes include questions that require this ability.
f. Distinguish between substitution, block, and exponentiation ciphers, and analyze their security based on their mathematical complexity.
    i. Assessment: Homework and writing assignments address these topics, and require an understanding of these ciphers in order to obtain a satisfactory grade.