Number Theory
Final Syllabus

<u>Week 1:</u>

Day 1: Introduction to number theory, number systems, intro to proofs, Pythagoras history, the Grand Assumptions. Study Hall: Classroom computer.

Day 2: More Grand Assumptions, definitions of WOP and POMI, examples of POMI, WOP implies POMI, Fibonacci and Lucas numbers, the golden ratio.

Day 3: Eratosthenes, definition of greatest common divisor, relatively prime, and a | b, the Division Theorem, the Euclidean Algorithm (defined, and that it yields the gcd of a and b), the Euclid Pythagoras skit.

Day 4: Calculator race, Greeker proof that $\sqrt{2}$ is irrational, the Diophantus skit, intro to linear Diophantine equations, aX + bY = 1 has a solution iff gcd (a, b) = 1.

Day 5: Using the EA to solve the LDEs, general solution of the original problem, advanced LDEs, library time to start work on research projects.

<u>Week 2:</u>

Day 1: Conclusion of LDEs, the q-ness Lemma, proof of the Fundamental Theorem of Arithmetic, WIFL skit to introduce continued fractions. Study hall: proofs that there are infinitely many primes.

Day 2: Conclusion of CFs, the silent mod 15 routine, intro to modular arithmetic, intro to congruences mod n and to equivalence relations. Study hall: The IOUNE (In-class Open-book Untimed Nonevaluative Exercise).

Day 3: The Publisher's Theorem, library time for projects, the Martian skit, the Chinese Remainder Theorem, working on mod n tables. Study hall: ICTEE #1 (In-class Closed-book Timed Evaluative Exercise).

Day 4: Definition of Z/nZ, that it's a ring and + and * are well-defined, gcd(a, n) = 1 iff the a row of Z/nZ contains all elements of Z/nZ, gcd(a, n) = 1 iff a had a multiplicative inverse in Z/nZ, Z/nZ is a field iff n is prime, definition of phi(n).

Day 5: Fermat's Little Theorem, definition of order in Z/nZ, primitive roots mod p, the National Plumbers lecture/skit. Study hall on Sunday: Euler's Theorem, proof and examples.

Week 3:

Day 1: RSA Cryptography, the theory and the decryption competition, work on projects.

Day 2: Quadratic residues, definition of $x^{(p-1)/2}$ is congruent to 1 mod p for p prime if x is a quadratic residue, definition of the Legendre symbol, “a crash p” is congruent to $a^{(p-1)/2}$ mod p, x^2 is congruent to -1 mod p for some x iff p is congruent to 1 mod 4, statement of quadratic reciprocity, Gauss and Diophantus skit, complex numbers: intro, geometric representation, DeMoivre’s Theorem. Study hall: ICTEE #2.

Day 3: Intro to the Gaussian integers. Z[i] is a commutative ring, definition of units, norm, norm is multiplicative, Gaussian Linear Combination Lemma, Gaussian primes, Mrs. Krabappel’s Division Theorem for Z[i], Gaussian potatoes, Gaussian Fundamental Theorem of Arithmetic part 1. Study hall: Work on projects.

Day 4: GFTOA part 2: uniqueness, a prime p in Z will be prime in Z[i] iff p is congruent to 3 mod 4, Fermat’s Two-Square Theorem, the generalization to N, projects in the afternoon and in study hall.

Day 5: $Z[(-6)^{(1/2)}]$ is not a UFD, the last projects.