

## DEPARTMENT OF MATHEMATICS SYLLABUS

Course # & Name: Mathematics 115A: Number Theory

Recommended Text(s) & Price: Rosen's "Elementary Number Theory and Its Applications," 4<sup>th</sup> Edition. (\$116.00)

Prepared by: Jesus deLoera      UPC Approval Date: March 2003  
Matt Nelsenador

| Lecture(s) | Sections          | Comments/Topics   |
|------------|-------------------|---|
| 1-3        | ch 1.1-1.4        | Well-ordering principle, induction, divisibility, prime numbers |
| 4-5        | ch. 3.1-3.3       | Greatest common divisor, Euclidean algorithm                    |
| 6-7        | ch. 3.4           | Fundamental theorem of arithmetic                               |
| 8          | ch. 3.5           | Factorization methods, sieve methods, Fermat numbers            |
| 9-10       | ch. 3.6           | Linear Diophantine equations                                    |
| 11-12      | ch. 4.1-4.2       | Congruences   |
| 13-15      | ch. 4.3           | Linear congruences, Chinese remainders theorem                  |
| 16-18      | ch. 6.1           | Fermat's little theorem, Wilson's theorem                       |
| 19-20      | ch. 6.3, ch. 7.1  | Euler's theorem, Euler-Phi function                             |
| 20-22      | ch. 8.1, 8.4, 8.5 | Public-key encryption (RSA)                                     |

### Additional Notes:

Essentially covers Rosen Ch. 1, 3-6, 8