CALIFORNIA STATE UNIVERSITY CHANNEL ISLANDS

NEW COURSE PROPOSAL

PROGRAM AREAS _____MATH

1. **Catalog Description of the Course.** *[Include the course prefix, number, full title, and units. Provide a course narrative including prerequisites and corequisites. If any of the following apply, include in the description: Repeatability (May be repeated to a maximum of ___ units); time distribution (Lecture ___ hours, laboratory ___ hours); non-traditional grading system (Graded CR/NC, ABC/NC). Follow accepted catalog format.]*

MATH 482. NUMBER THEORY AND CRYPTOGRAPHY (3)
Three hours of lecture per week.
Prerequisite: MATH 300.
Divisibility, Prime Numbers, Unique factorization theorem, congruences, solutions of linear congruences, solutions of quadratic congruences, Fermat's Little Theorem, Wilson's Theorem, Euler's *phi* function. Cryptography.

2. **Mode of Instruction.**

	Units	Hours per Unit	Benchmark Enrollment
Lecture	___3_____	___1_____	__24_____
Seminar	_____	_____	_____
Laboratory	_____	_____	_____
Activity	_____	_____	_____

3. **Justification and Learning Objectives for the Course.** (Indicate whether required or elective, and whether it meets University Writing, and/or Language requirements) *[Use as much space as necessary]*

The course is an elective for Mathematics majors.

Through this course, students will be able to

- Prove the basic properties of divison in **Z**
- Establish properties of prime numbers
- Discuss and use the unique factorization theorem
- Use the congruence formalism
- Use the Wilson's, Fermat's and Euler's Theorems for theoretical and computational purposes
- Solve linear and quadratic congruence equations
- Apply basic Number Theory to construct ciphers
- Express ideas of Number Theory and its application in oral and written form.

This course is not designed to satisfy the University Writing or Language requirements.

4. **Is this a General Education Course** **NO**
If Yes, indicate GE category:

A (English Language, Communication, Critical Thinking)	
B (Mathematics & Sciences)	
C (Fine Arts, Literature, Languages & Cultures)	
D (Social Perspectives)	
E (Human Psychological and Physiological Perspectives)	
INTERDISCIPLINARY	

5. Course Content in Outline Form. *[Be as brief as possible, but use as much space as necessary]*

Divisibility: Theoretical Definitions and first principles,
Prime Numbers: Basic theorems about primes
Unique factorization theorem: Proof and consequences
Congruences: Introduction to Congruence Calculus .
Solutions of congruence equations: Techniques for solving linear and quadratic equations
Fermat's Little Theorem, Wilson's Theorem, Euler's *phi* function
Cryptography: Introduction to ciphers, Simple ciphers based on Number theory, Introduction to RSA

6. References. *[Provide 3 - 5 references on which this course is based and/or support it.]*

Vanden Eynden, Charles, *Elementary number theory*, Boston : McGraw-Hill, c2001

7. List Faculty Qualified to Teach This Course.

All Mathematics Faculty

8. Frequency.

a. Projected semesters to be offered: Fall ___X__ Spring _X____ Summer _____

9. New Resources Required.

a. Computer (data processing), audio visual, broadcasting needs, other equipment

None

b. Library needs

None

c. Facility/space needs

None

10. Consultation.

Attach consultation sheet from all program areas, Library, and others (if necessary)

11. If this new course will alter any degree, credential, certificate, or minor in your program, attach a program modification.

Ivona Grzegorczyk 1/8/03

Proposer of Course Date