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.**

<table>
<thead>
<tr>
<th></th>
<th>Units</th>
<th>Hours per Unit</th>
<th>Benchmark Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>3</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>Seminar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laboratory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 division in \( \mathbb{Z} \)
- 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:

<table>
<thead>
<tr>
<th>GE Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (English Language, Communication, Critical Thinking)</td>
<td></td>
</tr>
<tr>
<td>B (Mathematics &amp; Sciences)</td>
<td></td>
</tr>
<tr>
<td>C (Fine Arts, Literature, Languages &amp; Cultures)</td>
<td></td>
</tr>
<tr>
<td>D (Social Perspectives)</td>
<td></td>
</tr>
<tr>
<td>E (Human Psychological and Physiological Perspectives)</td>
<td></td>
</tr>
<tr>
<td>INTERDISCIPLINARY</td>
<td></td>
</tr>
</tbody>
</table>
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.*


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**