Gateway to Mathematics: Number Theory
Math 11N, Lecture 1, Spring 2019

Instructor: Will Conley
Email: wconley@ucla.edu
Office: MS 6939
Office Hours: Mon 2:00–3:30, Thurs 4:00–5:30
Any other time by appointment
My Website: http://www.math.ucla.edu/~wconley/

Lectures: MWF 10:00–10:50 am, MS 6221
Discussion sections: Tue, 10:00–10:50 am, MS 5233
Course Website: https://ccle.ucla.edu/course/view/19S-MATH11N-1

Prerequisite: Math 31B

Textbook: There is no textbook for this course, because we will be creating our own as we go. The instructor will provide the definitions of new concepts, a few motivating examples, and the statements of theorems. The students will provide the proofs.

Grading: Your final average in this class will be computed based on the following scheme:

- Homework: 20%
- Presenting proofs in class: 25%
- Quizzes: 20%
- Final exam: 35%

A final average of 90% or higher will guarantee you at least an A−, a final average of 80% or higher will guarantee you at least a B−, and a final average of 70% or higher will guarantee you at least a C−. However, final letter grades may be (and usually are) curved by adjusting these cut-offs lower. In other words, final grades may be curved, but the curve can only help you, not hurt you. If everyone in the class earns above 90%, everyone in the class will get an A or A−.

Homework: Homework problems will be assigned each week, and will be posted on the course website. They will be collected each Tuesday in your discussion section, and returned promptly (most likely the following Tuesday, sooner if possible). Late homework will not be accepted, but your lowest homework score will be dropped.

In-class presentations: At the end of each lecture, or shortly thereafter, one or more unproved statements will be assigned for the next lecture. It will be your job to prove as many of them as you can, and be prepared to present your proofs in the next lecture. I will keep track of how many times each student presents a proof, so that everyone ends up presenting roughly the same number of times. 80% of this part of your grade will simply be based on effort: if you present your attempts at proofs enough times throughout the quarter, that will guarantee you 20 out of 25 points, even if they are not all correct proofs. The remaining 20% of this part of your grade (5 out of 25 points) will be based on the correctness of the proofs you present in class.
Quizzes: In place of one or more midterms, you will take a quiz in your discussion section every other week (that is, during the even-numbered weeks of the quarter). These quizzes will usually require around 25 minutes. Since the homework and the in-class presentations will (hopefully) provide assessment and feedback (that is, they should let me and you know how you are doing in the class), the primary purpose of the quizzes is to give you practice for the final exam. That is, they will give you some practice in solving problems and writing short proofs under a time constraint. There will be no make-ups for missed quizzes, but your lowest quiz score will be dropped. This way, you can miss one quiz without it hurting your grade. On some of the quizzes, you will be allowed to use a calculator. A basic four-function calculator will suffice, although you may use a scientific calculator if you wish. However, it may not be a programmable or graphing calculator, nor any kind of device that can communicate with other devices (such as a cell phone or smart watch).

Final exam: The final exam will be on Wednesday, June 12, from 8:00 to 11:00 am. This date was set by the university months in advance, and cannot be changed. In accordance with university policies, you must take the final exam in order to pass the class. Make-ups for the final exam are permitted only under exceptional circumstances, as outlined in the UCLA student handbook. For the final exam, you will be allowed to use a calculator. The same rules as outlined in the previous section apply here as well.

Notice about academic integrity

From the office of the Dean of Students:
“With its status as a world-class research institution, it is critical that the University uphold the highest standards of integrity both inside and outside the classroom. As a student and member of the UCLA community, you are expected to demonstrate integrity in all of your academic endeavors. Accordingly, when accusations of academic dishonesty occur, The Office of the Dean of Students is charged with investigating and adjudicating suspected violations. Academic dishonesty, includes, but is not limited to, cheating, fabrication, plagiarism, multiple submissions or facilitating academic misconduct.”

Students are expected to be aware of the University policy on academic integrity in the UCLA Student Conduct Code:
Please note the sections on (1) cheating, (2) plagiarism, and (3) unauthorized study aids.

Violation of course policy involving plagiarism, cheating, or possession of course materials during exams will be referred to the Dean of Students, who will be encouraged to take strong action. Do not cheat! The penalties can be very harsh. Do not believe it if you hear that “everyone does it.” You generally do not hear about the punishments because they are kept confidential. If you are found responsible by the Dean of Students for violating course policy, cheating on any course materials, or giving or receiving unauthorized help, a zero will be assigned for the entire assignment. No exceptions will be made! Past examples of penalties also include loss of an entire term of credit and suspension for several terms. If you plan to apply to graduate or professional school, such a negative mark on your record may be a major obstacle to admission.
## Course Outline (Tentative)

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Meeting #</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mon Apr 1</td>
<td>1</td>
<td>What is number theory?</td>
</tr>
<tr>
<td></td>
<td>Wed Apr 3</td>
<td>2</td>
<td>Pythagorean triples, rational points on the circle, and stereographic projection.</td>
</tr>
<tr>
<td></td>
<td>Fri Apr 5</td>
<td>3</td>
<td>Intro to proofs: Propositional logic.</td>
</tr>
<tr>
<td></td>
<td>Mon Apr 8</td>
<td>4</td>
<td>Intro to proofs: Propositional logic.</td>
</tr>
<tr>
<td>2</td>
<td>Wed Apr 10</td>
<td>5</td>
<td>Intro to proofs: Existential and universal quantifiers: “there exists” and “for all”.</td>
</tr>
<tr>
<td></td>
<td>Fri Apr 12</td>
<td>6</td>
<td>Intro to proofs: direct proof, proof by contrapositive, proof by contradiction.</td>
</tr>
<tr>
<td></td>
<td>Mon Apr 15</td>
<td>7</td>
<td>Intro to proofs: direct proof, proof by contrapositive, proof by contradiction.</td>
</tr>
<tr>
<td></td>
<td>Wed Apr 17</td>
<td>8</td>
<td>Divisibility, and the division-with-remainder theorem.</td>
</tr>
<tr>
<td></td>
<td>Fri Apr 19</td>
<td>9</td>
<td>Intro to proofs: Proof by induction. Weak and strong induction.</td>
</tr>
<tr>
<td></td>
<td>Mon Apr 22</td>
<td>10</td>
<td>Proof of the division-with-remainder theorem.</td>
</tr>
<tr>
<td>4</td>
<td>Wed Apr 24</td>
<td>11</td>
<td>Greatest common divisors.</td>
</tr>
<tr>
<td></td>
<td>Fri Apr 26</td>
<td>12</td>
<td>The Euclidean algorithm.</td>
</tr>
<tr>
<td></td>
<td>Mon Apr 29</td>
<td>13</td>
<td>Solving linear equations in the integers: Bézout's identity.</td>
</tr>
<tr>
<td>5</td>
<td>Wed May 1</td>
<td>14</td>
<td>The extended Euclidean algorithm.</td>
</tr>
<tr>
<td></td>
<td>Fri May 3</td>
<td>15</td>
<td>Prime numbers and factorization.</td>
</tr>
<tr>
<td></td>
<td>Mon May 6</td>
<td>16</td>
<td>Unique factorization: the fundamental theorem of arithmetic.</td>
</tr>
<tr>
<td></td>
<td>Wed May 8</td>
<td>17</td>
<td>Unique factorization: the fundamental theorem of arithmetic. Other ways of writing prime factorizations.</td>
</tr>
<tr>
<td></td>
<td>Fri May 10</td>
<td>18</td>
<td>Arithmetic modulo $n$.</td>
</tr>
<tr>
<td>7</td>
<td>Mon May 13</td>
<td>19</td>
<td>Arithmetic modulo $n$.</td>
</tr>
<tr>
<td></td>
<td>Wed May 15</td>
<td>20</td>
<td>Raising to a power modulo $p$: Fermat's Little Theorem.</td>
</tr>
<tr>
<td></td>
<td>Fri May 17</td>
<td>21</td>
<td>Raising to a power modulo $n$: Euler's Theorem.</td>
</tr>
<tr>
<td></td>
<td>Mon May 20</td>
<td>22</td>
<td>Raising to a power modulo $n$: Euler's Theorem. Computing the Euler $\phi$ function.</td>
</tr>
<tr>
<td>8</td>
<td>Wed May 22</td>
<td>23</td>
<td>Computing the Euler $\phi$ function.</td>
</tr>
<tr>
<td></td>
<td>Fri May 24</td>
<td>24</td>
<td>Solving systems of congruence equations: the Chinese remainder theorem.</td>
</tr>
<tr>
<td></td>
<td>Mon May 27</td>
<td>Holiday</td>
<td>Memorial Day</td>
</tr>
<tr>
<td>9</td>
<td>Wed May 29</td>
<td>25</td>
<td>Formulas for computing the Euler $\phi$ function.</td>
</tr>
<tr>
<td></td>
<td>Fri May 31</td>
<td>26</td>
<td>Equivalence relations, and equivalence classes.</td>
</tr>
<tr>
<td></td>
<td>Mon Jun 3</td>
<td>27</td>
<td>The quotient of a set by an equivalence relation.</td>
</tr>
<tr>
<td>10</td>
<td>Wed Jun 5</td>
<td>28</td>
<td>The First Isomorphism Theorem for sets.</td>
</tr>
<tr>
<td></td>
<td>Fri Jun 7</td>
<td>29</td>
<td>The RSA public-key cryptosystem.</td>
</tr>
<tr>
<td>Finals</td>
<td>Wed Jun 12</td>
<td>Final Exam</td>
<td>8:00-11:00 am</td>
</tr>
</tbody>
</table>