**18.781 Theory of Numbers  Fall Semester, 2005**

**Class meetings:** Monday, Wednesday, and Friday 2:00–3:00, in 2-102.

**Text:** John Stillwell, *Elements of Number Theory*. You should try to read the text *before* class as well as after. Both your own understanding and your of catching the lecturer in a *faux pas* will be greatly increased. I mentioned Hardy and Wright's *Introduction to the Theory of Numbers* as a recommended text not because it is a good source for the material on the syllabus, but because it is a wonderful source for a huge amount of additional mathematics.

**Lecturer:** David Vogan, 2-281. Telephone: 617-253-4991. E-mail: dav@math.mit.edu. My office hours are Wednesday 3–4, Thursday 3–4, or by appointment. (But in practice I'll be in my office most of the time 9–5 weekdays, and dropping in is fine.)

**Homework** will be assigned in most classes. Problems assigned during each week will be collected at the beginning of the first class of the following week. You are free to consult your friends and any other sources while working on the problems, but you should write up your solutions entirely on your own. This is a place to show your understanding without time pressure.

**Exams:** There will be two exams during the lecture hour, on October 7 and November 9. There will be a three-hour final exam. The exams will all be closed book.

**Grading:** Each hour exam will be worth 100 points, the final exam will be worth 150 points, and the problem sets will be worth a total of 150 points.

**Schedule**

| | | | |
|---|---|---|---|
| Wed 9/7 | Lecture 1 | 1.1–1.5 | Division with remainder |
| Fri 9/9 | Lecture 2 | 1.6–1.9 | Diophantine equations |
| Mon 9/12 | Lecture 3 | 2.1–2.3 | The Euclidean algorithm |
| Wed 9/14 | Lecture 4 | 2.4–2.6 | Prime factorization |
| Fri 9/16 | Lecture 5 | 2.7–2.9 | The map of relatively prime pairs |
| Mon 9/19 | Holiday | | |
| Wed 9/21 | Lecture 6 | 3.1-3.3 | Modular arithmetic |
| Fri 9/23 | Lecture 7 | 3.4–3.6 | Fermat's little theorem |
| Mon 9/26 | Lecture 8 | 3.7–3.10 | Repeating decimals |
| Wed 9/28 | Lecture 9 | 4.1–4.7 | RSA |
| Fri 9/30 | Lecture 10 | | Linear algebra mod $p$ |
| Mon 10/3 | Lecture 11 | | Continued fractions and $1 + \sqrt{2}$ |
| Wed 10/5 | Lecture 12 | | Review |
| Fri 10/7 | Lecture 13 | | **Exam 1 on Chapters 1–4** |
| Mon 10/10 | Holiday | | |
| Wed 10/12 | Lecture 14 | 5.1–5.4 | Pell's equation |
| Fri 10/14 | Lecture 15 | .5.–5.6 | Dirichlet's pigeonhole principle |
| Mon 10/17 | Lecture 16 | 5.7–5.9 | John Conway's river |
| Wed 10/19 | Lecture 17 | 6.1–6.4 | Gaussian integers |
| Fri 10/21 | Lecture 18 | 6.5–6.8 | Sums of two squares |
| Mon 10/24 | Lecture 19 | 7.1–7.3 | Quadratic integers |
| Wed 10/26 | Lecture 20 | 7.4–7.6 | Unique factorization? |
| Fri 10/28 | Lecture 21 | 7.7–7.8 | Fermat's last theorem for $n = 3$ |

| | | | |
|---|---|---|---|
| Mon 10/31 | Lecture 22 | 8.1–8.3 | Quaternions |
| Wed 11/2 | Lecture 23 | 8.4–8.6 | Hurwitz integers |
| Fri 11/4 | Lecture 24 | 8.7–8.9 | Sums of four squares |
| Mon 11/7 | Lecture 25 | | Review |
| Wed 11/9 | Lecture 26 | | **Exam 2 on Chapters 1–8** |
| Fri 11/11 | Holiday | | |
| Mon 11/14 | Lecture 27 | 9.1–9.2 | Quadratic reciprocity |
| Wed 11/16 | Lecture 28 | 9.3–9.5 | Integer square roots of two |
| Fri 11/18 | Lecture 29 | 9.6–9.7 | Chinese remainder theorem |
| Mon 11/21 | Lecture 30 | 9.8–9.9 | Proof of quadratic reciprocity |
| Wed 11/23 | Lecture 31 | | Hundreds of other proofs |
| Fri 11/25 | Holiday | | |
| Mon 11/28 | Lecture 32 | 10.1–10.3 | Rings |
| Wed 11/30 | Lecture 33 | 10.4–10.6 | Algebraic integers |
| Fri 12/2 | Lecture 34 | 11.1–11.3 | Ideals and divisibility |
| Mon 12/5 | Lecture 35 | 11.4–11.6 | Non-principal ideals |
| Wed 12/7 | Lecture 36 | 11.7–11.9 | What is ideal factorization? |
| Fri 12/9 | Lecture 37 | 12.1–12.3 | Prime ideals |
| Mon 12/12 | Lecture 38 | 12.4–12.6 | Ideal factorization works |
| Wed 12/14 | Lecture 39 | 12.7–12.9 | Ideal classes |
| week of 12/15–12/19 | | | **Final Exam** |