Math 214:Numbers, equations, and proofs
Fall 2008

Instructor: Alireza Salehi Golsefidy, Fine 510, 8-4230.
Tentative Office Hours: 3:00-3:50 pm Tu-Th (Fine 510)
E-mail: asalehi@math.princeton.edu

Grader: Andrew Yang
Office: Fine hall 511
Office Hours: 3:00-4:00 pm Wed.
E-mail: ayang@math.princeton.edu

Math 214 home page: www.math.princeton.edu/∼asalehi/NumThe.html
Homework assignments will be available on-line.

1 What is Math 214?

Math 214[1] is a course in classical number theory. At the end of this course, beside getting familiar with beautiful number theoretical arguments, you are supposed to learn how to communicate your thoughts in a rigorous way with the mathematical community.

2 Grading

The grading for the course is **not** the same as that given in the registrar's website. The grade is divided as follows:

- 50% homework.
- 20% midterm.
- 30% final.

Both the midterm and the final will be takehome.

[1] This course is developed by Jordan Ellenberg, now a professor at the University of Wisconsin. The syllabus and the content are largely due to him and J. R. Getz.

3 Homework

Each week, I will assign a set of homework exercises, which will be due at the beginning of Thursday classes.

The best way to learn the material, and with the same token to learn how to write what you have in mind is *completing the homework exercises.*

You are encouraged to collaborate on your problem sets. However you have to write up your solutions individually. When collaborating with someone, or using a book as a reference, you should mention her/his name, or the name of the book, respectively, in your assignment. Otherwise, it is considered a breach of your honor code.

What usually works best is to spend some time working on the problems on your own, then meeting with your study group to share ideas, compare progress, and brainstorm about the more difficult problems.

Handwritten assignments are acceptable. However, you are encouraged to learn LaTeX. It is a special version of TeX program, designed by D. Knuth to produce high-quality typesetting for mathematics. The program is free, and there are also free editors. I use TeXShop on my mac. On your PC, you can use LED, which is free, or WinEdt. It is pretty easy to work with LaTeX, especially if you use the header part of a written article. You also may find L. Lamport's *A Document preparation system LaTeX* a useful source.

Please staple your homework.

4 Tests

You are not allowed to collaborate, or use books for your midterm or final exams.

5 Textbook

The textbook for the course is *An Introduction to the Theory of Numbers,* 5th ed., by Niven, Zuckerman, and Montgomery. A copy will be on reserve in the library, together with copies of two other excellent textbooks, *An Introduction to the Theory of Numbers* by Hardy and Wright and *A Friendly Introduction to Number Theory* by Silverman. Silverman's book is rather lax about rigorous proof, but is extremely friendly and has a nice emphasis on computation and examples. The Hardy and Wright book is an acknowledged classic–well-written and rich in historical context which NZM lacks. However, it is written in a more austere and mathematical style which may be difficult for newcomers to mathematical prose. I recommend giving both books a look.

You should do your first pass through the week's reading *before* the corresponding lectures.

6 Schedule

1. **11 Sep:** Introduction: which numbers are the sums of two squares? Primes and factorization.

   Read: 1.2,1.3

2. **15 Sep – 19 Sep:** Unique factorization, Euclid's algorithm, Congruences and Euler's ϕ function: Euler's theorem and Fermat's "little" theorem. and modular arithmetic.

   Read: 1.2 and 1.3 again, 2.1

3. **22 Sep – 26 Sep:** Mod m numbers. Chinese Remainder Theorem.

   Read: 2.2, 2.3.

4. **29 Sep – 3 Oct:** Number theory and public-key cryptography: the RSA algorithm, Solutions of polynomials modulo prime powers, Hensel's lemma.

   Read: 2.5, 2.6, 2.7.

5. **6 Oct – 10 Oct:** Primitive roots.

   Read: 2.8

6. **13 Oct – 17 Oct:** Quadratic residue, Quadratic reciprocity.

   Read: 3.1, 3.2

7. **20 Oct – 24 Oct:** Great integer function, Arithmetic functions, Convolution, and Möbius inversion, Midterm.

   Read: 4.1, 4.2, 4.3

8. **3 Nov – 7 Nov:** Geometry of numbers, Sum of four squares.

   Read: 6.4

9. **10 Nov – 14 Nov:** Continued fractions.

   Read: 7.1, 7.2, 7.3, 7.4, 7.5

10. **17 Nov - 21 Nov:** Continued fractions (continued!). Solutions to Pell's equation $x^2 - dy^2 = 1$.

    Read: 7.6, 7.7, 7.8

11. **24 Nov – 28 Dec:** Quadratic fields, Failure of unique factorization.

    Read: 9.5, 9.6, 9.7

12. **1 Dec – 5 Dec:** Quadratic fields (continued).

    Read: 9.9, 9.10

13. **8 Dec – 12 Dec:** Cyclotomic polynomials, Primes in the arithmetic progression $\{nk + 1\}$.

    Read: TBA