Introduction to Number Theory

Spring 2016

Homework # 9
Last Updated: April 13, 2016
Due Date: Thursday April 21st (right before the midterm).

This is the final homework assignment that I will collect and grade. The first half is for the "new material" since last week. The second half, consisting of optional ungraded problems, serves to remind you what we've covered and indicate what sort of things might be on the exam.

FRINT Chapter 20:

(1) 20.1
(2) 20.2 a,b,c
(3) 20.3 a,b

FRINT Chapter 21:

(4) 21.1
(5) 21.4

FRINT Chapter 22:

(6) 22.1
(7) 22.7

I encourage you to review the lecture notes I posted concerning the Gaussian integers, as we covered a good amount of material not covered in the course textbook.

On the Gaussian Integers:

(8) Of the primes in $\mathbb{Z}$ less than 30, which can be written as a sum of squares? Which are also Gaussian primes? How are these related?
(9) Factor 165 into a product of **Gaussian** primes.
(10) Notice that $13 = (2+3i)(2-3i) = (3+2i)(3-2i)$. Is this a counterexample to unique factorization in $\mathbb{Z}[i]$?

Material Concerning the Midterm

Since the first midterm, we have covered the following.

(1) Euler's Theorem
(2) The Chinese Remainder Theorem
(3) Mersenne primes and perfect numbers
(4) The sum-of-divisors σ function
(5) Solving congruences of the form $x^k \equiv a \pmod{p}$
(6) RSA (and other) encryption
(7) Gaussian integers (and other integer rings)

(8) Primes as sums of squares
(9) Quadratic reciprocity

You might notice that the material from the first midterm — consisting roughly of modular arithmetic, some first properties of the integers, the Euclidean algorithm, and Fermat's little Theorem — all still remain very important and have been continually used. So you should think of this midterm as being cumulative in content, even though the focus is entirely on material covered since the first midterm.

In the book, this means that we've learned Chapters 1-23 (excluding Chapter 19), Chapters 35-36, additional material related to cryptography, and additional material related to the Gaussian integers and other integer-like rings. You are responsible for all this material.

The format of this midterm will be roughly like the first midterm. It will consist of a mixture of computational problems and some proof-style problems. Yet as you have developed more capable and as the material has become more structural, the line between computation and proof has blurred. There will still be a selection of somewhat more involved proofs at the end, of which you choose some number to do.

There are few topics that I can guarantee will be represented. The Chinese Remainder Theorem will appear (probably a few times in different contexts). We've focused a lot on the Gaussian integers and integer rings for the last 3 weeks, and they will certain appear a few times, both computationally and proof-wise.

On this midterm, **there will be no use of calculators**. This means that there are a few topics that I won't ask. For instance, I will not ask you to use repeated squaring to compute $a^k \pmod{m}$ for some really large k (I could ask for small k with cleverly chosen a and m, of course). I won't ask you to do a "real" appliction of RSA, as the numbers are too bad too quickly.

I have begun drafting the midterm, and I think it will be a nice midterm. If you have any questions, I encourage you to ask. Good luck, and I'll see you in class.