Introduction to Number Theory

Spring 2016

Some Additional Problems
Last Updated: April 20, 2016

Here are a few suggested problems that you might consider doing, if you find that you are bored while studying or preparing.

(1) Which of the following primes can be represented as a sum of two squares: $3, 7, 31, 67, 97$? How do you know? Do you remember how we proved this?
(2) FRINT Problem 11.7 on the Chinese Remainder Theorem. (It's always good to practice the CRT, as these problems require some nice understanding of how modular arithmetic works.)
(3) We've encountered many multiplicative functions in this course. Which ones do you remember? Do you remember how to show that each one is multiplicative? For instance, understanding that $\gcd(m, n) = 1$ means that $\varphi(mn) = \varphi(m)\varphi(n)$ led us to understand the Chinese Remainder Theorem.
(4) Do you remember how to find *all* the solutions to $12x \equiv 4 \pmod 1)6$? We so frequently count the number of solutions, or know whether or not there are solutions. But do you remember how to find them?
(5) Compute each of the following Legendre symbols: $\left(\frac{13}{37}\right), \left(\frac{21}{41}\right), \left(\frac{6}{13}\right)$.
(6) FRINT problem 35.6.
(7) What is the RSA protocol. What theorems and ideas became involved in the proof? Do you remember how they all fit together?
(8) Factor 210 into a product of Gaussian primes. Can you show that each of the Gaussian primes are, in fact, primes?
(9) What is the remainder when $2^{2017} + 3^{2018}$ is divided by 60?
(10) Show that $n^5 \equiv n \pmod 6$ for all integers n.
(11) Prove or Disprove: If $\gcd(a, b) = 1$, then $\gcd(a, \gcd(b, c)) = 1$.

Of course, I recommend that you also study your homework problems and their solutions. At the end of the day, remember — in the grand scheme of things, midterms matter much less than the ideas in the course itself. Even as you study, try to remember what's really important. And I hope you can also remember that math can be interesting and intriguing, as long as you're willing to look.