Your secon exam is on November 15th. It will cover everything from the first test through the material we covered in class on Wednesday, November 8th. Roughly speaking this includes chapters 5, 6, 8, 9, 10, 11, and 13. That's a lot of chapters, but it's not as bleak as it looks: we skipped some of chapter 6, and almost all of chapter 8; chapter 10 is essentially parts of chapter 6 all over again, except with polynomials; and so on.

Because we're covering "just enough" of these different topics to discuss codes, I can't ask a lot of in-depth theoretical problems on the test, but there will be a few conceptual questions where you have to interpret definitions or use theorems to prove modest results. You can also expect a few computational questions. A list of possible topics would include:

Chapter 5: You should know how to compute CRCs and know something about their analysis—what errors can it detect and why?—both in general and for a specific generating polynomial $g(x)$.

Chapters 6 and 10: The most important topics in chapter 6 are the Euclidean Algorithm, gcd's, $\mathbb{Z}/m$, and their interconnections. (By "interconnections" I mean things like x has a multiplicative inverse in $\mathbb{Z}/m$ if and only if $\gcd(x, m) = 1$, and if so, you can find x^{-1} by running the Euclidean Algorithm backwards.) These ideas all depend on the early ideas in the chapter, like divisibility, and recall that I said divisibility leads to lots of nice short little proofs where you simply write down the definitions and rearrange things.

Chapter 10 is essentially the same material, but using polynomials instead of integers. So you don't have to learn a lot of new concepts in chapter 10, but you should make sure you're comfortable using the same algorithms and ideas with either polynomials or numbers. We also covered Fermat's Little Theorem, the Euler ϕ-function, and Euler's Theorem. Also remember some basic properties of $\mathbb{Z}$ and $\mathbb{Z}/m$ (see chapter 9).

Chapter 8: We pretty much covered just enough of chapter 8 so that we could use the idea of a "group" in the definition of "ring."

Chapter 9: We spent a little more time on rings than on groups. You should remember some of the different properties a ring can have, like whether it has zero divisors, an example of a ring where unique factorization fails, and so on. (See $\mathbb{Z}$, $\mathbb{Z}/m$ and $\mathbb{Z}[\sqrt{-5}]$ in chapter 6.) You should definitely know the definition of field, as well as basic examples. (See also $\mathbb{Z}/p$ in chapter 6 and chapter 11.)

Chapter 11: You should know how to define $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$ for $n > 1$. The first is easier, because it's just $\mathbb{Z}/p$; the second is a little trickier. You should be comfortable working with elements of $\mathbb{F}_{p^n}$ both as polynomials and as $\mathbb{F}[\alpha]$ where α is a root of the equation $P(x) = 0 \bmod P(x)$.

Chapter 13: We spent a fair amount of time on this chapter and also added some geometric ideas into the mix. From most important to least important, I'd rank the bounds like this: Hamming, GV, Singleton, where Singleton is far below the other two. It gets a little tricky remembering what's *necessary* and what's *sufficient*, so pay attention to that when studying or you might use the wrong bound when trying to prove something. We also covered definitions and pictures of Hamming spheres and balls and computed their volume, which appears as part of the inequality in Hamming's Bound.

Jonathan Rogness <rogness@math.umn.edu> November 11, 2006