These solutions aren’t intended to be comprehensive. Make sure to ask me if you have any questions or find any typos. In a few cases you might have gotten full credit if your answers didn’t quite match what’s here as long as you demonstrated the required knowledge in a later part of the problem.

Some people seemed to get caught by surprise by a few problems, so I’ve also noted where we’ve run across each topic before; that might help you figure out what will be on the next exam. Remember that there won’t be a perfect correlation between exam problems and graded homework problems. Only 4 problems are graded on each assignment, roughly 1-2 per chapter, and there are often many more concepts in a chapter than that. Some things will get covered on both exams and homework, but other ideas will only be graded on one or the other.

(1) (i): The answer could vary according to whether you allowed \(a\) and \(b\) to be greater than \(n\) or not. (This comes down to whether you want to use the “official” definition of \(\mathbb{Z}/n\) or our intuitive definition for this class.) I accepted answers which were correct in either setting. If we assume that \(a, b < n\) then this is only true for \(n\) prime. Otherwise let \(n = pq\), in which case

\[pq = n = 0 \mod n\]

This concept of “zero divisor” has been mentioned in lecture multiple times, and this problem is very similar to 9.17 on the homework. (It’s also related to 9.19.)

(ii): The requirement is that \(\gcd(m, n) = 1\). This was proved in class for both integers and polynomials, and was needed in homework problems from Chapter 6.

(iii): You can compute that \(\gcd(47, 33) = 1 = -7 \cdot 47 + 10 \cdot 33\), so

\[10 \cdot 33 = 1 + 7 \cdot 47 = 1 \mod 47\]

Hence 10 is the multiplicative inverse of 33 in \(\mathbb{Z}/47\). This process was covered in class for both integers and polynomials and appeared on the homework multiple times. Everybody did well on this.

(2) (i): \(d(x) = x^6 + x^4 + x^2 + 1\), and dividing \(d(x)\) by \(g(x)\) results in a remainder of \(r(x) = 1 \cdot x^2 + 1 \cdot x + 0 \cdot 1\), so the CRC is 110. This was the main point of Chapter 5, and everybody did well on this problem.

(ii): We proved in class that this only occurs if \(g(x)|x^7 - 1\), and doing the division shows that this is the case. This is very similar to 5.08.

(iii): We proved that CRCs can detect certain burst errors in class, and I said during the lecture that it was a good candidate for a test question. Because there are just three errors, right in a row,

\[e = 0 \ldots 01110 \ldots 0\]
\[e(x) = 0 + \ldots + 0 + x^{j+2} + x^{j+1} + x^j + 0 + \ldots + 0\]
\[= x^j(x^2 + x + 1)\]

Our CRC will only fail to detect this burst error if \(g(x)|e(x)\). We know \(g(x)\) can’t divide \(x^j\), because \(g\) has a constant term. It can’t divide \((x^2 + x + 1)\) because its degree is higher than 2. Hence \(g(x)\) can’t divide \(e(x)\) and the error is detected.
(3) (i): This is homework problem 6.14, and it’s a very special case \((a = 1, b = \pm 1)\) of the proposition on page 96, which we proved in class. I also mentioned on the study guide that divisibility gives a good source of short proofs for exam questions. Almost everybody did very well on this problem.

(ii): I mentioned in the study guide that you should be able to define \(\mathbb{F}_{p^n}\) after we did it in class. This problem deals with \(\mathbb{F}_{49} = \mathbb{F}_{7^2}\). Essentially,

\[
\mathbb{F}_{49} = \mathbb{F}_7[x]/(x^2 - 3)
\]

A general element is a polynomial with coefficients in \(\mathbb{F}_7\) which has been reduced mod \(P(X)\), so its degree is less than \(\deg(P) = 2\). Thus \(\mathbb{F}_{49} = \{a + bx \mid a, b \in \mathbb{F}_7\}\). The last part here was only worth two points: \(x\) serves as \(\sqrt{3}\), because

\[
\begin{align*}
x^2 - 3 &= 0 \mod P(x) \\
x^2 &= 3 \mod P(x)
\end{align*}
\]

(4) (i): We computed the volume of a Hamming sphere in class, and it’s used as part of the Hamming Bound. Homework 4 has related problems as well. In this case,

\[
V = \left(1 + \binom{3}{1} + \binom{3}{2}\right) = (1 + 3 + 3) = 7
\]

Having computed that there are 7 words contained in the Hamming sphere of radius 2 centered at any point, I ought to have 7 words in my list:

000, 001, 010, 100, 110, 101, 011

In a binary code of length 3, spheres of radius 2 contain all but one of the possible strings. (Centered at 000, the sphere contained everything but 111.) Hence any binary code of length 3 with (non-overlapping) spheres of radius 2 can have just one single codeword. That’s not very useful if you want to send information across. You can’t even answer a yes/no question!

(ii): We covered the Hamming Bound in lecture, and it appears on Homework 4 and the study guide. Everybody did well with this problem, other than a few mixups with the values of \(q, n, l\), etc. Note that \(d = 2e + 1 = 3\), so \(e = 1\).

\[
6 \left(1 + (3 - 1)\binom{3}{1}\right) = 6 \cdot 7 = 42 \nleq 27 = 3^3
\]

So such a code cannot exist.

(iii): We defined this two ways in class, and it’s on Homework 4. One definition was more geometric (none of the spheres overlap, and every possible string is contained in a codeword). Algebraically, a perfect code is one in which equality is achieved in the Hamming Bound.