Suggested reading: Trappe-Washington 6.4, 7.2, 18.1–2.

For this assignment, please write out your steps to show how you are applying the alogrithms. You are welcome to use computer software for the computations.

1. (a) Describe the Exponent Factorization Method (Chapter 6.4). What additional information do we need to use this factorization method that is usually prohibitively difficult to obtain?
   (b) Suppose I know that $2^{900} \equiv 1 \pmod{9191}$. Use the Exponent Factorization Method to factor 9191.
2. Trappe-Washington Chapter 7 Problem 5(a).
3. (a) Describe the Pohlig-Hellman Algorithm for computing discrete logarithms (Chapter 7.2.1). In the notation in the textbook, in lecture we described how to compute x_0. Be sure to complete the description by carefully explaining how we can find x_1, x_2, etc.
   (b) Let $p = 71$. The congruence class $11 \pmod{71}$ is a primitive root. Use the Pohlig-Hellman Algorithm to solve $11^x \equiv 30 \pmod{71}$ for the exponent $x \pmod{70}$.
4. (a) Describe the Baby Step, Giant Step method for computing discrete logarithms (Chapter 7.2.2).
   (b) Using this method with $N = 10$, find all solutions x to $5^x \equiv 2 \pmod{97}$. Note that 5 is a primitive root of the prime 97.
5. Trappe–Washington Chapter 7 Problem 12.
6. (a) Describe the Index Calculus method of computing discrete logarithms (Chapter 7.2.3).
   (b) Given that 3 is a primitive root of the prime 101, find all solutions x of $3^x \equiv 96 \pmod{101}$ using the Index Calculus. It may help you to know:

$$\begin{aligned}
3^1 &\equiv 3 \pmod{101} \\
3^{16} &\equiv 16 \pmod{101} \\
3^{21} &\equiv 50 \pmod{101} \\
3^{22} &\equiv 49 \pmod{101} \\
3^{27} &\equiv 90 \pmod{101} \\
3^{30} &\equiv 6 \pmod{101}
\end{aligned}$$

7. Let $\mathcal{A}$ be an alphabet of of q symbols (also called letters). In your own words:
   (a) Define a q-ary code of length n.
   (b) Define the *Hamming distance* d on $\mathcal{A}^n$, and explain what it means to say that d is a metric.
   (c) Define the *Hamming sphere*, the closed ball $B(c, r)$ of radius r around the word c in the Hamming distance. Compute the sets $B(0100, 2) \subseteq (\mathbb{Z}/2\mathbb{Z})^4$ and $B(11, 1) \subseteq (\mathbb{Z}/4\mathbb{Z})^2$. Here, 0100 abbreviates the vector (0,1,0,0), and 11 abbreviates (1,1).
   (d) Define the *minimum distance* $d(C)$ of a code C. What does $d(C)$ tell you about the code?
   (e) Define *nearest neighbour decoding.*
   (f) Define an (n, M, d) code.
   (g) Define the *code rate* of a code C. What does the code rate tell you about C?
8. Determine (n, M, d) and the code rate R of the following codes:
   (a) Let $\mathcal{A}$ be an alphabet of q letters, and let $C = \mathcal{A}^n$ be the set of all q-ary n-tuples.

(b) Let $\mathcal{A} = \mathbb{Z}/q\mathbb{Z}$ and let C be the set of all words $(a_1, a_2, \ldots a_n)$ in $\mathcal{A}^n$ such that

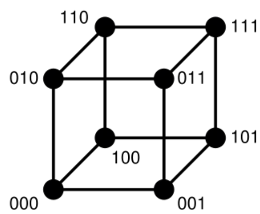
$$a_1 + a_2 + \ldots + a_n \equiv 0 \pmod{q}.$$

(c) Let $\mathcal{A}$ be the alphabet on q elements $\{0, 1, \ldots q-1\}$. Let C be the length-n repetition code

$$\{(0, 0, \ldots, 0), (1, 1, \ldots, 1), \ldots (q-1, q-1, \ldots, q-1)\} \subseteq \mathcal{A}^n.$$

(d) Let $\mathcal{A}$ be the alphabet on q elements $\{0, 1, \ldots q-1\}$, and let C be the set of all words of the form $(a, a, a, \ldots, a, 0, 0, 0, \ldots 0)$ having k copies of $a \in \mathcal{A}$ and $(n-k)$ copies of 0.

9. Here is a schematic of $(\mathbb{Z}/2\mathbb{Z})^3$, with a line drawn between all points of Hamming distance 1.



(a) Recopy the picture. Using a different colour, connect all points of Hamming distance 2. Using a third colour, connect points of Hamming distance 3.

(b) Make an analogous schematic of $(\mathbb{Z}/2\mathbb{Z})^4$ and of $(\mathbb{Z}/3\mathbb{Z})^2$, with lines drawn between all points of Hamming distance 1.

(c) Choose a binary length 4 code C in $(\mathbb{Z}/2\mathbb{Z})^4$ of minimum distance $d(C) = 3$ including at least 2 codewords. In your schematic of $(\mathbb{Z}/2\mathbb{Z})^4$, colour each codeword, and draw a Hamming sphere of radius 2 around each codeword. Interpret what "minimum distance 3" means in terms of these Hamming spheres and the geometry of your picture. Explain why your code can detect $s = 2$ errors.

(d) In your diagram of $(\mathbb{Z}/2\mathbb{Z})^4$, draw Hamming sphere of radius 1 around each codeword. Explain why your code can correct $t = 1$ error.

(e) Write a proof (in your own words) of the following result, which appears on page 400.

Theorem 1.1. *1. A code C can detect up to s errors if $d(C) \geq s + 1$.*
2. A code C can correct up to t errors if $d(C) \geq 2t + 1$.

10. Let $\mathcal{A}$ be an alphabet of of q symbols (eg, $\mathcal{A} = \mathbb{Z}/q\mathbb{Z}$).

(a) How many elements are there in $\mathcal{A}^n$?

(b) Let w be a fixed word in $\mathcal{A}^n$. How many words in $\mathcal{A}^n$ are Hamming distance 0 from w? How many words in $\mathcal{A}^n$ are Hamming distance exactly 1 from w?

(c) For $m \geq 0$ in $\mathbb{Z}$, how many words in $\mathcal{A}^n$ are Hamming distance exactly m from w?

(d) How many words are in the ball $B(w, r)$ for fixed radius $r \geq 0$?

(e) Prove the Hamming Bound, the theorem on page 404.

If you're not sure how to proceed, start by working out the answer for some small values of q and n. Recall that $\binom{a}{b} = \frac{a!}{(b!)(a-b)!}$ is the number of ways to select a subset of b (unordered) elements from a set of a elements.

11. Read Example 4 in Section 18.1, on the Hamming [7,4] code. Complete Trappe–Washington Chapter 18 Problem 1.