# *Math 5251 Error correcting codes and finite fields*
# *Midterm #2*

*Spring 2023, Trevor Karn*

*Due April 5, 2023, by 4:00pm via Canvas or Hardcopy*

**Instructions:** This is an open book, open library, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. All sources used must be cited. In particular, Artificial Intelligence, class notes, and textbook use must be cited.

1. (30 points total; 5 points each) **True or False.** Your answers must by justified either by counter examples or proofs to recieve full credit.
   (a) In $\mathbb{Z}/9920736$, the element $100000000000000000000$ has a multiplicative inverse.
   (b) In $\mathbb{Z}/9920736$, the element $100000000000000000001$ has a multiplicative inverse.
   (c) There exists an integer $m > 2$ for which $\mathbb{Z}/(m^2-1)$ is a field.
   (d) $x^6+x^5+x^4+x^2+2x+2$ is an irreducible polynomial in $\mathbb{Z}/4[x]$.
   (e) $x^6+x^4+x^2+x+1$ is an irreducible polynomial in $\mathbb{Z}/2[x]$.
   (f) Let $g(x) = x^6+x^2+x+1 \in \mathbb{F}_2[x]$ be the generator polynomial for a cyclic redundancy check. If you receive a transmission corresponding to the polynomial
   $$\tilde{d}(x) = x^{12}+x^8+x^7+x^5+x^4+x^2,$$
   there has been an error in transmission.
2. (a) (10 points) The integer 8009 is prime, and so $\frac{1}{100} \in \mathbb{Z}/8009$. Express $\frac{1}{100}$ as an integer modulo 8009, using the extended Euclid algorithm.
   (b) (10 points) The polynomials
   $$f(x) = x^2+x$$
   $$g(x) = x^7+x^2+1$$
   in $\mathbb{F}_2[x]$ have no common factors. Thus, there exist polynomials $a(x), b(x) \in \mathbb{F}_2[x]$ satisfying
   $$a(x)f(x)+b(x)g(x) = 1.$$
   Find $a(x), b(x)$ explicitly, using the extended Euclid algorithm.
3. Let $C \subseteq (\mathbb{F}_7)^9$ be the following $\mathbb{F}_7$-linear code:
   $$C = \{\mathbf{x} = [x_1,\ldots,x_9] \in (\mathbb{F}_7)^9 : x_1 = 2x_2 = x_3,\ 4x_4 = x_5 = 6x_6,\ x_7 = 2x_8 = 3x_9\}$$
   For each of the following, justify your answer.
   (a) (5 points) What is the dimension $k = \dim_{\mathbb{F}_7}(C)$?
   (b) (5 points) What is the 7-ary rate of $C$?
   (c) (5 points) What is the minimum distance $d(C)$?
   (d) (5 points) How many errors can this code detect, using minimum distance decoding? How many can it correct?

(e) (5 points) Write down a generator matrix $G$ for $\mathcal{C}$.

(f) (5 points) Suppose you receive the message $[2, 4, 2, 1, 1, 6, 2, 2, 3]$. Decode the message using minimum distance decoding.

4. (a) (5 points) Find a representative for 9999 for in $\mathbb{Z}/37$. (Justify the validity of your answer.)

(b) (5 points) Do the same for 999700029999 in $\mathbb{Z}/37$.

(c) (10 points) Prove that if a number $N$ is written in decimal notation with digits $a_\ell a_{\ell-1} \cdots a_2 a_1 a_0$ (so that $a_0$ is the ones digit, $a_1$ is the tens digit, $a_2$ the hundreds digit, etc.), then in $\mathbb{Z}/37$ one has

$$N = \cdots + a_5 a_4 a_3 + a_2 a_1 a_0.$$

For example, in $\mathbb{Z}/37$, one has $41,246,789,963 = 41 + 246 + 789 + 963$, so we interpret $a_5 a_4 a_3$ as a 3 digit number, *not* a product $a_5 \times a_4 \times a_3$.