CMU 15-252 **Fall 2017**

HOMEWORK 5
DUE OCT 20 BY EMAIL

---

1. Read the notes on Polynomials and Error-Correcting Codes posted on the course webpage.

2. Tai wants to send us a message consisting of 3 numbers $m_0, m_1, m_2 \in \mathbb{F}_{11}$. The channel he will send over is very noisy, so he uses the Reed–Solomon encoding. He interprets his message as the coefficients of a polynomial $P(x) = m_0 + m_1 x + m_2 x^2$ of degree at most 2, evaluates this polynomial on all eleven elements in $\mathbb{F}_{11}$, and sends the results $P(0), \ldots, P(10)$.

   (a) Suppose that, because of noise, we cannot make out the first, third, fourth, fifth, seventh, ninth, tenth and eleventh number sent; i.e., we receive

   $$(??, y_1 = P(1), ??, ??, ??, y_5 = P(5), ??, y_7 = P(7), ??, ??, ??, ??).$$

   Luckily this is enough for us to decode the message. Decode the message for $y_1 = 0$, $y_5 = 8$, $y_7 = 6$.

   (b) Suppose Tai did his eleven polynomial evaluations mod 12 rather than mod 11. Suppose we again received

   $$(??, y_1 = P(1), ??, ??, ??, y_5 = P(5), ??, y_7 = P(7), ??, ??, ??, ??).$$

   Why can't we recover Tai's message in this case? Explain where the solution from lecture would break down, and more concretely, find two different messages that are consistent with the above received information.

3. To launch the missile, it is necessary to enter the secret code into the keypad. The secret code is Trump's favorite number S, which is between the number 0 and the (hyuge) number 100 000 000 000 000 002 inclusive. (Note: $p = 100\,000\,000\,000\,000\,003$ is a prime number.) The president has 11 generals. The president wants it to be the case that if any 6 generals get together, they can figure out S and launch the missile; however, if only 5 or fewer of them collaborate, they have no clue what S is. (Note: there is nothing special about 6 and 11.) The president does the following:

   - Picks c_1, c_2, c_3, c_4, c_5 independently and uniformly at random between 0 and $p-1$.
   - Defines the polynomial $Q(x) = S + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5$.
   - Tells the ith general the value $Q(i) \bmod p$, for $i = 1 \ldots 11$.

   The generals know that the president has done this; they just don't know S (or the values $c_1, \ldots, c_5$).

   (a) Prove that if any 6 generals combine their information, they can figure out S.

   (b) Prove that if any 5 generals get together, they cannot determine any information about S. The way we formalize this as follows: For each list of 5 distinct generals $g_1, \ldots, g_5 \in \{1, 2, 3, \ldots, 11\}$ (identifying them by the evaluation value they get), for each possible value of the secret S, and for each possible 5-tuple $y_1, \ldots, y_5 \in \mathbb{F}_p$, we have

   $$\mathbf{Pr}[Q(g_1) = y_1 \wedge \cdots \wedge Q(g_5) = y_5] = 1/p^5,$$

   where the probability is over the choice of coefficients c_i.