Math 495R Homework 20

(1) Recall that in Homework 15, you wrote a function `xgcd(a, n)` that returns integers `d, x, y` where d is the greatest common divisor of a and n and satisfies $d = ax + ny$. If we work in $\mathbb{Z}_n$, this equation becomes $d \equiv ax \pmod{n}$, or $\overline{d} = \overline{ax}$. If a and n are relatively prime, so that $d = 1$, we find that our x satisfies $ax \equiv 1 \pmod{n}$, and dividing by a in $\mathbb{Z}_n$ is the same as multiplying by its reciprocal x.

Let p be prime, and let A be a matrix with entries in $\mathbb{Z}_p$. Modify your program from Lab 17, replacing division by an integer a with multiplication by the inverse of $a \pmod{p}$, so that it gives the inverse of A as a matrix with entries in $\mathbb{Z}_p$. Your output should be a matrix with integer entries, which can be interpreted as elements of $\mathbb{Z}_p$.

(2) Write a function which takes a prime p and a positive integer n and a list of integers $x_1, x_2, \ldots, x_n$ and returns the matrix

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \pmod{p}.$$

Your matrix should be a list of lists, as we have done in previous assignments.

(3) You should have received a secret message consisting of three numbers x, y, p. This message cannot be decoded unless at least four people work together, but any set of four students from the class should be able to decrypt the message. Here p is a large prime and (x, y) is a point on a cubic polynomial, so that $y \equiv M + a_1 x + a_2 x^2 + a_3 x^3 \pmod{p}$ for some unknown values M, a_1, a_2, a_3. By combining your secret message with the secret messages of three other students, you should have enough information to solve the system of equations

$$\begin{aligned} y_1 &\equiv M + s_1 x_1 + s_2 x_1^2 + s_3 x_1^3 \pmod{p}, \\ y_2 &\equiv M + s_1 x_2 + s_2 x_2^2 + s_3 x_2^3 \pmod{p}, \\ y_3 &\equiv M + s_1 x_3 + s_2 x_3^2 + s_3 x_3^3 \pmod{p}, \\ y_4 &\equiv M + s_1 x_4 + s_2 x_4^2 + s_3 x_4^3 \pmod{p}, \end{aligned}$$

or (in matrix form)

$$\begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{bmatrix} \begin{bmatrix} M \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \equiv \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} \pmod{p}.$$

Find the number $M \pmod{p}$ and use your function `int2string100` to find the secret message.