CISC 822 Homework 1, due Thursday, Sept 25.

Solving 7 of the 8 problems correctly will be considered a full submission. Solving the 8th correctly will be considered "extra credit".

The first two questions rely on these facts.

Fact 1: Every finite field has a generator (primitive element), which is an element g such that every nonzero element a of the field is of the form $a = g^k$ for some k in $0..q-2$, where q is the cardinality (size) of the field.

Definition: The order of an element a in a group (written multiplicatively) is the least positive k such that $a^k = 1$.

Fact 2: The order of an element of a group divides the order (size) of the group. In particular, in the multiplicative group consisting of the nonzero elements of GF(q), the order of an element divides $q - 1$.

1. Find the least prime $p > 3$ such that 2 and 3 are not primitive in $F = \mathbb{Z}_p$.

2. Find a prime p and irreducible polynomial $f(x)$ in $\mathrm{GF}_p[x]$ such that x is not primitive in $\mathrm{GF}(p^d) = \mathrm{GF}(p)[x]/ < f(x) >$, where d is the degree of f. Hint: Stick to small p and d. Polynomials of degree 2 and 3 are irreducible iff they have no root in the coefficient field.

3. Definition: A Toeplitz matrix is one in which $a_{i,j} = a_{k,l}$ whenever $i - j = k - l$. In other words it is constant along each diagonal.

   Polynomial multiplication can be reduced to Toeplitz matrix times vector product as in this example: The product $\sum_{i=0}^{3} a_i x^i \times \sum_{i=0}^{3} b_i x^i = \sum_{i=0}^{6} c_i x^i$ is obtained by this product:

$$\begin{pmatrix} a_0 & 0 & 0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_2 & a_1 & a_0 & 0 \\ a_3 & a_2 & a_1 & a_0 \\ 0 & a_3 & a_2 & a_1 \\ 0 & 0 & a_3 & a_2 \\ 0 & 0 & 0 & a_3 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{pmatrix}$$

   Show that the converse is true: Toeplitz matrix times vector product can be linear time reduced to polynomial multiplication. That is to say, do a $m \times n$ Toeplitz matrix times n-vector product by doing a polynomial multiplication (on $\mathrm{O}(m+n)$ degree polynomials) plus an amount of additional work linear in m and n.

   Hint: You may find it helpful to first treat the case of a triangular Toeplitz matrix. In this case the method can be a little simpler. Besides, this is the case that came up in class vis a vis reducing quotient and remainder to multiplication.

4. Chapter 2, Exercise 8.

5. Chapter 2, Exercise 9.

6. Chapter 3, Exercises 11 and 13.
7. Chapter 4, Exercise 1.
8. Chapter 4, Exercise 22.