Math 110 Final Exam
Fall 2016

The exam will be due by midnight on Wednesday, December 14. The exam should be sent electronically to gunnar@math.stanford.edu. Please make the subject line "M110final". Do not consult any books or internet resources other than Trappe and Washington.

1. (10 points) How many 27th roots of unity are there in a field with 2197 elements? How many primitive roots?

2. (15 points) You receive the encrypted message

OFJDFEJWOHGFJHFZUJD

You know that the encryption is performed using an affine transformation $x \rightarrow ax + b$, for a 27 letter alphabet, including a blank. You also know that the first word is I, i.e I followed by a blank. The alphabet is converted to numerical values via

$A \rightarrow 0, B \rightarrow 1, \ldots, Z \rightarrow 25, \text{Blank} \rightarrow 26$

Decode the message.

3. (10 points) Find the decomposition of $X^5 + 1$ (coefficients in $\mathbb{Z}/2$) into irreducible factors. For each factor, prove that it is irreducible. For each irreducible factor $g$, describe the code with generating polynomial $g$ in more familiar terms.

4. (15 points) Let $F$ denote the field $\mathbb{Z}/19$.
   
   (a) Which of the numbers 7 and 13 are primitive roots in $F$?
   
   (b) Verify that 2 is a primitive root in $F$.
   
   (c) For each of the numbers 3, 9, and 17, determine its discrete log based on the primitive root 2.

5. (15 points) Suppose that we have the 18 letter alphabet

$\{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, \text{Blank}\}$

and that we represent it numerically via

$A \rightarrow 0, B \rightarrow 1, \ldots, Q \rightarrow 16, \text{Blank} \rightarrow 17$

Suppose further that we encrypt the numbers by the rule $n \rightarrow 2^n \mod 19$. Decrypt the received message

$9, 10, 1, 11, 10, 9, 3, 10, 15, 1$

6. (10 points) Evaluate the Legendre symbols $\left(\frac{3083}{3911}\right)$ and $\left(\frac{43691}{65537}\right)$. 

1
7. (25 points)

(a) Consider the elliptic curve defined by the equation $y^2 = x^3 - 1$ over the field $\mathbb{Z}/7$. Find the number of points on the curve, and give a multiplication table for the multiplication operation on the set of points. Is there a single element that generates the set of points? If so, give the element, and if not, explain why.

(b) Consider the same equation defined over the field $\mathbb{Z}/11$. Find the number of points, and list them. How many elements of the curve have order two? Is there a point that generates the whole curve?