Math 3CY3, Test 3

Bradd Hart, Nov. 28, 2018

There are 5 questions and each question is worth 5 marks. Please write complete answers to all of the questions in the test booklet provided. Partial credit may be given for your work. Unless otherwise noted, you need to justify your solutions in order to receive full credit. Please be sure to include your name and student number on all sheets of paper that you hand in.

1. (a) 2 is a generator for F_p where $p = 3989$. Assume that

$$L_2(3925) = 2000 \text{ and } L_2(1046) = 3000.$$

   Determine $L_2(3925 \cdot 1046)$.

   (b) Compute $L_5(2)$ in F_{17}.

2. Suppose Bob chooses the finite field F_{16}, picks a generator g and makes the triple $(F_{16}, g, 3)$ public. Alice picks an integer a between 1 and 15 and sends Bob the information $(g^3)^a$. Eve intercepts Alice's message to Bob. Can Eve recover Alice's integer a?

3. Suppose that b is a non-zero element of F_{37} and you know that $b^4 = 1$ in F_{37}. We know 2 is a generator of F_{37}. What are the possible values of $L_2(b)$?

4. Consider the elliptic curve over F_7 given by $y^2 = x^3 - x + 1$.

   (a) List all the points on this elliptic curve.

   (b) Compute $(1,1) + (1,1)$ and $(1,1) + (0,-1)$ where $+$ represents the addition on the elliptic curve.

5. (a) In the field F_{601}, we know that

$$7^{300} \equiv 600, 7^{200} \equiv 576 \text{ and } 7^{120} \equiv 423 \bmod 601.$$

   Explain why you know that 7 is a generator for F_{601}.

   (b) Based on your answer, describe a general procedure for determining if g is a generator for F_p where p is a prime.