THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Assignment 3 (Due date: 8 Mar, 2018)

1. Let p be a prime number and $1 \leq \alpha \leq p-1$. Show that

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \qquad (\mathrm{mod}\ \mathrm{ord}_p(\alpha))$$

   where $\mathrm{ord}_p(\alpha)$ is the least positive integer such that $\alpha^{\mathrm{ord}_p(\alpha)} \equiv 1 \pmod p$.

2. Let $p = 1201$. Use the Pohlig-Hellman algorithm to find $L_{11}(2)$.

3. Let $p = 31$. Use the baby step, giant step to find $L_3(14)$.

4. Let $p = 601$. Use the index calculus to find $L_7(83)$.

   (Hint: you may make use the pre-computation step in the lecture notes.)

5. Show that an ideal of $\mathbb{Z}$ must be of the form $n\mathbb{Z}$, where n is an integer.

6. (a) If $p(x) \in \mathbb{R}[x]$ which is not a multiple of x^2+1, show that $\gcd(p(x), x^2+1) = 1$.

   (b) Show that the ideal $\langle x^2+1 \rangle$ (i.e. ideal generated by x^2+1) is a maximal ideal of $\mathbb{R}[x]$.
   (Remark: Therefore, $\mathbb{R}[x]/\langle x^2+1 \rangle$ is a field.)

7. Let E be the elliptic curve given by the equation $y^2 \equiv x^3 - 2 \pmod 7$.

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

   (b) Find $(3,2) + (5,5)$ and $2(3,2)$.

8. Let E be the elliptic curve given by the equation $y^2 \equiv x^3 + 2x + 3 \pmod{19}$.

   (a) Find $(1,5) + (9,3)$.

   (b) Find $(9,3) + (9,-3)$.

   (c) Using the result in (b), find $(1,5) - (9,3)$.

   (d) Find an integer k such that $k(1,5) = (9,3)$.

   (e) Suppose that the order of $(1,5)$ is 20, i.e. $n = 20$ is the least positive integer such that $n(1,5) = \infty$. Show that E has exactly 20 points.