THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Suggested Solution to Assignment 3

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

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{\operatorname{ord}_p(\alpha)}$$

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

Ans:

Let $0 \leq y_1, y_2 < \operatorname{ord}_p(\alpha)$ such that $y_1 = L_\alpha(\beta_1)$ and $y_2 = L_\alpha(\beta_2)$.

Then, we have $\beta_1 = \alpha^{y_1}$, $\beta_2 = \alpha^{y_2}$ and so $\beta_1\beta_2 = \alpha^{y_1+y_2}$.

By the fact that $\alpha^m \equiv \alpha^n \pmod{p}$ implies that $m \equiv n \pmod{\operatorname{ord}_p(\alpha)}$, we have

$$L_\alpha(\beta_1\beta_2) \equiv y_1 + y_2 \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{\operatorname{ord}_p(\alpha)}.$$

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

Ans:

Note $p - 1 = 1200 = 2^4 \times 3 \times 5^2$. Let $x = L_{11}(2)$.

Express $x = x_0 + 2x_1 + 4x_2 + 8x_3 + \cdots$, where $0 \leq x_i \leq 1$.

$$\begin{aligned}
11^{x_0+2x_1+4x_2+8x_3+\cdots} &\equiv 2 \pmod{1201} \\
\left(11^{x_0+2x_1+4x_2+8x_3+\cdots}\right)^{600} &\equiv 2^{600} \pmod{1201} \\
\left(11^{600}\right)^{x_0} \cdot \left(11^{1200}\right)^{x_1+2x_2+4x_3+\cdots} &\equiv 2^{600} \pmod{1201} \\
(-1)^{x_0} &\equiv 1 \pmod{1201} \\
\therefore \quad x_0 &= 0
\end{aligned}$$

Then,

$$\begin{aligned}
11^{2x_1+4x_2+8x_3+\cdots} &\equiv 2 \pmod{1201} \\
\left(11^{2x_1+4x_2+8x_3+\cdots}\right)^{300} &\equiv 2^{300} \pmod{1201} \\
\left(11^{600}\right)^{x_1} \cdot \left(11^{1200}\right)^{x_2+2x_3+4x_4+\cdots} &\equiv 2^{300} \pmod{1201} \\
(-1)^{x_1} &\equiv 1 \pmod{1201} \\
\therefore \quad x_1 &= 0
\end{aligned}$$

Then,

$$\begin{aligned}
11^{4x_2+8x_3+\cdots} &\equiv 2 \pmod{1201} \\
\left(11^{4x_2+8x_3+\cdots}\right)^{150} &\equiv 2^{150} \pmod{1201} \\
\left(11^{600}\right)^{x_2} \cdot \left(11^{1200}\right)^{x_3+2x_4+4x_5+\cdots} &\equiv 2^{150} \pmod{1201} \\
(-1)^{x_2} &\equiv -1 \pmod{1201} \\
\therefore \quad x_2 &= 1
\end{aligned}$$

Then,

$$\begin{aligned}
11^{4+8x_3+\cdots} &\equiv 2 \pmod{1201} \\
11^{8x_3+\cdots} &\equiv 11^{-4} \times 2 \pmod{1201} \\
11^{8x_3+\cdots} &\equiv 729 \pmod{1201} \\
\left(11^{8x_3+\cdots}\right)^{75} &\equiv 729^{75} \pmod{1201} \\
\left(11^{600}\right)^{x_3} \cdot \left(11^{1200}\right)^{x_4+2x_5+\cdots} &\equiv 729^{75} \pmod{1201} \\
(-1)^{x_3} &\equiv -1 \pmod{1201} \\
\therefore \qquad x_3 &= 1
\end{aligned}$$

Therefore, $x \equiv 12 \pmod{16}$.

Next, express $x = x_0 + 3x_1 + 9x_2 + 27x_3 + \cdots$, where $0 \leq x_i \leq 2$.

$$\begin{aligned}
11^{x_0+3x_1+9x_2+27x_3+\cdots} &\equiv 2 \pmod{1201} \\
\left(11^{x_0+3x_1+9x_2+27x_3+\cdots}\right)^{400} &\equiv 2^{400} \pmod{1201} \\
\left(11^{400}\right)^{x_0} \cdot \left(11^{1200}\right)^{x_1+3x_2+9x_3+\cdots} &\equiv 2^{400} \pmod{1201} \\
(570)^{x_0} &\equiv 570 \pmod{1201} \\
\therefore \qquad x_0 &= 0
\end{aligned}$$

Therefore, $x \equiv 1 \pmod{3}$.

Similarly, express $x = x_0 + 5x_1 + 25x_2 + \cdots$, where $0 \leq x_i \leq 4$.

$$\begin{aligned}
11^{x_0+5x_1+25x_2+\cdots} &\equiv 2 \pmod{1201} \\
\left(11^{x_0+5x_1+25x_2+\cdots}\right)^{240} &\equiv 2^{240} \pmod{1201} \\
\left(11^{240}\right)^{x_0} \cdot \left(11^{1200}\right)^{x_1+5x_2+\cdots} &\equiv 2^{240} \pmod{1201} \\
1062^{x_0} &\equiv 105 \pmod{1201}
\end{aligned}$$

We can compute $1062^0 \equiv 1$, $1062^1 \equiv 1062$, $1062^2 \equiv 105$, $1062^3 \equiv 1018$ and $1062^4 \equiv 216$.

Therefore, $x_0 = 2$.

Then,

$$\begin{aligned}
11^{2+5x_1+\cdots} &\equiv 2 \pmod{1201} \\
11^{5x_1+\cdots} &\equiv 11^{-2} \times 2 \pmod{1201} \\
11^{5x_1+\cdots} &\equiv 536 \pmod{1201} \\
\left(11^{5x_1+\cdots}\right)^{48} &\equiv 536^{48} \pmod{1201} \\
\left(11^{240}\right)^{x_1} \cdot \left(11^{1200}\right)^{x_2+5x_3+\cdots} &\equiv 536^{48} \pmod{1201} \\
1062^{x_1} &\equiv 1062 \pmod{1201} \\
\therefore \qquad x_1 &= 1
\end{aligned}$$

Therefore, $x \equiv 7 \pmod{25}$.

By Chinese remainder theorem, $L_{11}(2) = 1132$.

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

   Ans:

   Choose a positive integer N such that $N^2 \geq p - 1 = 30$. Take $N = 6$ and construct the following table:

j	0	1	2	3	4	5
$3^j \pmod{31}$	1	3	9	27	19	26

   By extended Euclidean algorithm, $3 \times 21 + 31 \times (-2) = 1$ and so $3^{-1} \equiv 21 (\bmod\, 31)$. Then, we construct the following table.

k	0	1	2	3	4	5
$14 \times 3^{-6k} \pmod{31}$	14	28	25	19	7	14

   Therefore, we have

$$
\begin{aligned}
3^5 &\equiv 19 \equiv 14 \times 3^{-18} \pmod{31} \\
3^{23} &\equiv 14 \pmod{31}
\end{aligned}
$$

   Therefore, $L_3(14) = 23$.

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.)

   Ans:

   We have $83 \times 7^4 \equiv 352 \equiv 2^6 \times 11 \pmod{601}$.

   Therefore,

$$
\begin{aligned}
L_7(83) + 4 &\equiv 5L_7(2) + L_7(11) \pmod{600} \\
L_7(83) &\equiv -4 + 5(432) + 157 \pmod{600} \\
L_7(83) &\equiv 513 \pmod{600}
\end{aligned}
$$

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

   Ans:

   Let I be an ideal of $\mathbb{Z}$. Suppose that $I = \{0\}$, then $I = 0\mathbb{Z}$.

   Now, suppose that I contains an element m other than 0. Then, we claim that I must contain some positive integers.

   If m is positive, we are done. Otherwise, we have $-m > 0$ is also an element of I.

   Among those positive integers, we let d be the least positive integer such that $d \in I$ and we claim that $I = d\mathbb{Z}$ (i.e. ideal generated by d).

Firstly, $d \in I$ and so $d\mathbb{Z} \subset I$. Suppose that there exists $a \in I \backslash d\mathbb{Z}$. Then, a is not an multiple of d. By Euclidean algorithm, there exist unique integers q and r with $0 < r < d$ ($r \neq 0$ since a is not a multiple of d) such that $a = qd + r$.

Then, we have $0 < r < d$ with $r = a - dq \in I$ which contradicts to the assumption that d is the least positive integer such that $d \in I$.

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

   Ans:

   Let $p(x) \in \mathbb{R}[x]$ which is not a multiple of x^2+1 and $\gcd(p(x), x^2+1) = d(x)$ where $\deg d(x) > 0$.

   Since $d(x)$ is a factor of x^2+1 and x^2+1 does not have any linear factor, $d(x)$ can only be x^2+1. It implies that $x^2+1 = d(x)|p(x)$ which is a contradiction.

   (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.)

   Ans:

   Let I be an ideal such that $\langle x^2+1 \rangle$ is a proper subset of I. Then, there exists a polynomial $p(x) \in I \backslash \langle x^2+1 \rangle$, i.e. $p(x)$ is not a multiple of x^2+1.

   By (a), we have $\gcd(p(x), x^2+1) = 1$. By extended Euclidean algorithm, there exist unique $a(x), b(x) \in \mathbb{R}[x]$ such that $1 = p(x)a(x) + (x^2+1)b(x)$.

   Since both $p(x)$ and x^2+1 are in I, we have $1 \in I$ which implies that $I = \mathbb{R}[x]$. Therefore, $\langle x^2+1 \rangle$ is a maximal ideal of $\mathbb{R}[x]$.

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.

   Ans:

   The points on E are: $(3,2)$, $(3,5)$, $(5,2)$, $(5,5)$, $(6,2)$, $(6,5)$ and ∞.

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

   Ans:

   $(3,2) + (5,5) = (3,5)$ and $2(3,2) = (5,2)$.

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

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

   Ans:

   $(1,5) + (9,3) = (15,8)$

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

   Ans:

   $(9,3) + (9,-3) = \infty$.

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

   Ans:

   $(1,5) - (9,3) = (1,5) + (9,-3) = (10,4)$

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

Ans:

$k = 5$.

(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.

Ans: By Lagrange's theorem, we have $20 \,|\, |E|$.

By Hasses' theorem, we have $||E| - 20| < 2\sqrt{19}$.

Therefore, $|E| = 20$ is the only possible integer which satisfies the above two conditions.