Math 116 Homework 6

Jerry Liu, 404474229

March 3, 2016

Book Problems

Problem. 1.

Part. a.

Solution.
$p - 1 = 12 = 2^2 \cdot 3$, $L_\alpha(\beta) = L_2(3) \Rightarrow \alpha = 2$ and $\beta = 3$
Let $L_2(3) = x = x_0 + x_1 \cdot 2$ with $0 \leq x_i \leq q - 1 = 1$, $2^x \equiv 3 \pmod{13}$
Let $q = 2$, raise both sides by $\frac{p-1}{q} = \frac{12}{2} = 6$, $3^6 \equiv 2^{x_0 \cdot 6} \pmod{13}$
Since $3^6 \equiv 1 \pmod{13}$, and when $k = 0$, $2^{6 \cdot k} \equiv 3^6 \equiv 1 \pmod{13}$, $x_0 = 0$
$\alpha^{-x_0} = 2^{-0} = 1$, $\beta_1 \equiv \beta\alpha^{-x_0} \equiv \beta \equiv 3 \pmod{p}$, raise both sides by $\frac{12}{4} = 3$
$2^{x_1 \cdot 3} \equiv 3^3 \equiv 1 \pmod{13} \Rightarrow x_1 = 0$. So $x \equiv x_0 + x_1 \cdot 2 \equiv 0 \pmod{4}$.
Let$q = 3$, raise both sides by $\frac{p-1}{q} = 4$, write $x = x_0$. $2^{x_0 \cdot 4} \equiv 3^4 \equiv 3 \pmod{13}$
When $k = 1$, $2^{4 \cdot k} \equiv 3 \pmod{13}$. So $x \equiv 1 \pmod{3}$. By CRT, $x \equiv 4 \pmod{12}$

Part. b.

Proof.
$2^7 \equiv 128 \equiv -2 \equiv 11 \pmod{13} \Rightarrow L_2(11) = 7$ □

Problem. 3.

Solution.
We know $5^{611} \equiv 1222 \equiv -1 \pmod{1223} \Rightarrow (-1)^x \equiv (5^{611})^x \equiv (5^x)^{611} \equiv 3^{611} \equiv 1 \pmod{1223}$
$\Rightarrow (-1)^x \equiv 1 \pmod{1223} \Rightarrow x$ is even.

Problem. 5.

Part. a.

Proof.
Let α be a primitive root for prime p, $\beta_1, \beta_2, x, y, z \in \mathbb{Z}$ such that $\alpha^x \equiv \beta_1, \alpha^y \equiv \beta_2, \alpha^z \equiv \beta_1\beta_2$.
By *Proposition* 3.7, $\alpha^x\alpha^y \equiv \alpha^z \pmod{p}$ if and only if $x + y \equiv z \pmod{p-1}$
$\Rightarrow L_\alpha(x) + L_\alpha(y) \equiv L_\alpha(z) \Rightarrow L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2)$. □

Part. b.

Proof.
$\alpha^x \equiv \alpha^y \pmod{p} \Leftrightarrow \alpha^{x-y} \equiv 1 \pmod{p}$
By 3.13.20(d), $\alpha^{x-y} \equiv 1 \pmod{p}$ if and only if $\text{ord}_p(\alpha) \mid x - y \Leftrightarrow x \equiv y \pmod{\text{ord}_p(\alpha)}$
$\Rightarrow \alpha^{\beta_1\beta_2} \equiv \alpha^{\beta_1} \cdot \alpha^{\beta_2} \pmod{p} \Leftrightarrow L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{\text{ord}_p(\alpha)}$ □

Problem. 6.

Part. a.

Solution.
$L_2(24) = L_2(2^3 \cdot 3) = L_2(2^3) + L_2(3) = 3 + 69 = 72$

Part. b.

Solution.
$L_2(5) = 24 \Rightarrow 2^24 \equiv 5 \pmod{101} \Rightarrow 5^3 \equiv 2^{24 \cdot 3} 2^7 2 \equiv 24 \pmod{101} \Rightarrow L_2(24) = 72.$

Problem. 7.

Solution.
We know when $p = 137$, $L_3(44) = 6$ and $L_3(2) = 10$. $L_3(44) = L_3(2^2 \cdot 11) = 2L_3(2) + L_3(11)$
$\Rightarrow L_3(11) \equiv L_3(44) - 2L_3(2) \equiv 6 - 2 \cdot 10 \equiv 122 \pmod{136} \Leftrightarrow 3^{122} \equiv 11 \pmod{137} \Rightarrow x = 122$

Problem. 8.

Part. a.

Solution.
Even if Eve can access to the file, she has to compute the discrete log for $L_2(2^x) \pmod{p}$ to get x. Since p is a very large prime, she cannot use *Pohlig-Hellman Algorithm* to find anything significant. Therefore it is very hard to compute the discrete log.

Part. b.

Solution.
Since p has only 5-digit, Eve can literally use brute force to find the password.
In other words, Eve can compute $2^n \pmod{p}$ for $k = 1, 2, \ldots, p-1$ to find $2^x \pmod{p}$.
Therefore the system is insecure.

Problem. 10.

Solution.
Since $\gcd(b, p-1) = 1$, $\exists\, x, y \in \mathbb{Z}$ such that $bx + (p-1)y = 1$. Since p is a prime, $\alpha^{p-1} \equiv 1 \pmod{p}$
Since Eve knows x_2, p and b,
$(x_2)^x \equiv (x_2)^x \cdot 1 \equiv (x_2)^x \cdot 1^y \equiv (\alpha^b)^x \cdot (\alpha^{p-1})^y \equiv \alpha^{bx+(p-1)y} \equiv \alpha^1 \equiv \alpha \pmod{p}$

Problem. 11.

Solution.
$m \equiv tr^{-a} \equiv 6 \cdot 7^{-6} \equiv 6 \cdot (7^{-1})^6 \equiv 6 \cdot 5^6 \equiv 12 \pmod{17}$