Name:Chao Jiang
ECE5563 — Spring 2015 **HW 6** Due: Apr. 1

Problem 1

Derivation of equation 10.3, 10.4 of textbook. For two distinct points, $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$, the slop of the line l that joins them is $\triangle = (y_Q - y_P)/(x_Q - x_P)$. Now we will do additions over elliptic curves.

Ans: For equation 10.3

(1) Suppose the equation of line l is $y = \alpha x + \beta$, we can get $\alpha = \triangle$, and $\beta = y_P - \alpha x_P$ considering the two points P, Q on the line l.

(2) There is one intersection point $(x_R, \alpha x_R + \beta)$ between l and the curves. we can get the points by $(\alpha x + \beta)^2 = x^3 + ax + b$.

(3) Due to the property of monic polynomial, we know that the sum of the roots is equal to minus the coefficient of the second-to-highest power. so $x_R + x_Q + x_P = -(-\alpha^2) \implies x_R = \alpha^2 - x_P - x_Q$. so we get the point $-(X + P)$, thus Q is $X + P = (x_R, -(\alpha x_R + \beta))$

$$\begin{aligned} x_R &= \triangle^2 - x_P - x_Q \\ y_R &= -y_P + \triangle(x_P - x_R) \end{aligned} \tag{10.3}$$

For equation 10.4

(1) When $P = Q$, $\triangle = \alpha = \frac{\partial y}{\partial x}$ at point $P = (x_P, y_P)$.

(2) Computing the derivative of equation $y^2 = x^3 + ax + b$, at P we get $\alpha = \frac{3x_P^2 + a}{2y_P}$

(3) So we get the equation 10.4

$$\begin{aligned} x_R &= \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P \\ y_R &= \left(\frac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P \end{aligned} \tag{10.4}$$

Problem 10.1

Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.

a. If user A has private key $X_A = 5$, what is As public key Y_A ?
$Y_A = 7^5 \bmod 71 = 51$

b. If user B has private key $X_B = 12$, what is Bs public key Y_B ?
$Y_B = 7^12 \bmod 71 = 4$

c. What is the shared secret key?
$YK = 4^5 \bmod 71 = 30$

Problem 10.10

On the elliptic curve over the real numbers $y^2 = x^3 - 36x$, let $P = (-3.5, 9.5)$ and $Q = (-2.5, 8.5)$. Find $P + Q$ and $2P$.

Ans: For $R = P + Q$:

$$\begin{aligned} \triangle &= (8.5 - 9.5)/(-2.5 + 3.5) = -1 \\ x_R &= \triangle - x_P - x_Q = 1 + 3.5 + 2.5 = 7 \\ y_R &= -y_P + \triangle(x_P - x_R) = -8.5 - (-3.5 - 7) = 2 \\ R &= P + Q = (7, 2) \end{aligned}$$

For $R = 2P$: we know that $a = -36$, applying the equation 10.4

$$\begin{aligned} x_R &= [(36.75 - 36)/19]^2 + 7 \approx 7 \\ y_R &= [(36.75 - 36)/19](-3.5 - 7) - 9.5 \approx 9.9 \\ R &= 2P = (7, 9.9) \end{aligned}$$

Problem 10.11

Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over Z_{17} ?

Ans: $(4a^3 + 27b^2) \bmod p = 4(10)^3 + 27(5)^2 \bmod 17 = 4675 \bmod 17 = 0$.

This elliptic curve does not satisfy the condition of Equation (10.6), so it does not defined a group over Z_{17}