Deadline: 2009/11/17

Note: Please hand in this homework and 10/27 speech reflection to OPLab 503D by deadline

Homework: 9.2, 9.4, 10.1, 10.13, 10.16

Reference solutions:

9.3 5

10.2
a. $\phi(11) = 10$
210 = 1024 = 1 mod 11
If you check 2n for n < 10, you will find that none of the values is 1 mod 11.
b. 6, because 26 mod 11 = 9
c. K = 36 mod 11= 3

10.11
a. First we calculate R = P + Q, using Equations (10.3).
Δ = (8.5 – 9.5)/(–2.5 + 3.5) = – 1
xR = 1 + 3.5 + 2.5 = 7
yR = –8.5 – (–3.5 – 7) = 2
R = (7, 2)
b. For R = 2P, we use Equations (10.4), with a = –36
xr = [(36.75 – 36)/19]2 + 7 ≈ 7
yR = [(36.75 – 36)/19](–3.5 – 7) –9.5 ≈ 9.9

10.15 We follow the rules of addition described in Section 10.4. To compute 2G = (2, 7) + (2, 7), we first compute

$$\lambda = (3 \times 2^2 + 1)/(2 \times 7) \bmod 11$$
$$= 13/14 \bmod 11 = 2/3 \bmod 11 = 8$$

Then we have

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$$

$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$

2G = (5, 2)

Similarly, 3G = 2G + G, and so on. The result:

2G = (5, 2)	3G = (8, 3)	4G = (10, 2)	5G = (3, 6)
6G = (7, 9)	7G = (7, 2)	8G = (3, 5)	9G = (10, 9)
10G = (8, 8)	11G = (5, 9)	12G = (2, 4)	13G = (2, 7)