Make Up

Nolan Pofi

Prob 2:
10.12

y	y^2 mod 11
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

QR(11) = {1,3,4,5,9}

x	$x^3 + x + 6$ mod 11	Y
0	6	none
1	8	none
2	5	(4,7)
3	3	(5,6)
4	8	none
5	4	(2,9)
6	8	none
7	4	(2,9)
8	9	none
9	7	none
10	4	(2,9)

Points are {(2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)}

10.13
-P = (5,-8) = (5,9)
-Q = (3,-0) = (3,0)
-R = (0,-6) = (0,11)

10.14

2G = (2,7) + (2,7)

$m = \frac{3(2)^2+1}{2*7} = \frac{13}{14} \mod 11 = \frac{2}{3} \mod 11 = 2*4 \mod 11 = 8$

$x = 8^2 - 2 - 2 \mod 11 = 5$

$y = 8(2-5) - 7 \mod 11 = 2$

2G = (5,2)

3G = (5,2) + (2,7)

$m = \frac{7-2}{2-5} = \frac{5}{-3} \mod 11 = \frac{5}{8} \mod 11 = 5*7 \mod 11 = 2$

$x = 2^2 - 5 - 2 \mod 11 = 8$

$y = 2(5-8) - 2 \mod 11 = 3$

3G = (8,3)

4G = (8,3) + (2,7)

$m = \frac{7-3}{2-8} = \frac{4}{-6} \mod 11 = \frac{4}{5} \mod 11 = 4*9 \mod 11 = 3$

$x = 3^2 - 8 - 2 \mod 11 = 10$

$y = 3(8-10) - 3 \mod 11 = 2$

4G = (10,2)

5G = (10,2) + (2,7)

$m = \frac{7-2}{2-10} = \frac{5}{-8} \mod 11 = \frac{5}{3} \mod 11 = 5*4 \mod 11 = 9$

$x = 9^2 - 10 - 2 \mod 11 = 3$

$y = 9(10-3) - 2 \mod 11 = 6$

5G = (3,6)

6G = (3,6) + (2,7)

$m = \frac{7-6}{2-3} = \frac{1}{-1} \mod 11 = \frac{1}{10} \mod 11 = 1*10 \mod 11 = 10$

$x = 10^2 - 3 - 2 \mod 11 = 7$

$y = 10(3-7) - 6 \mod 11 = 9$

6G = (7,9)

7G = (7,9) + (2,7)

$m = \frac{7-9}{2-7} = \frac{-2}{-5} \mod 11 = \frac{9}{6} \mod 11 = 9*2 \mod 11 = 7$

$x = 7^2 - 7 - 2 \mod 11 = 7$

$y = 7(7-7) - 9 \mod 11 = 2$

7G = (7,2)

8G = (7,2) + (2,7)

$m = \frac{7-2}{2-7} = \frac{5}{-5} \mod 11 = \frac{5}{6} \mod 11 = 2*2 \mod 11 = 10$

$x = 10^2 - 3 - 2 \mod 11 = 3$

$y = 10(7-3) - 2 \mod 11 = 5$

8G = (3,5)

9G = (3,5) + (2,7)
m = $\frac{7-5}{2-3} = \frac{2}{-1} \mod 11 = \frac{5}{10} \mod 11 = 2 * 10 \mod 11 = 9$
x = $9^2 - 3 - 2 \mod 11 = 10$
y = $9(3 - 10) - 5 \mod 11 = 9$
9G = (10,9)

10G = (10,9) + (2,7)
m = $\frac{7-9}{2-10} = \frac{-2}{-8} \mod 11 = \frac{9}{3} \mod 11 = 9 * 4 \mod 11 = 3$
x = $3^2 - 10 - 2 \mod 11 = 8$
y = $3(10 - 8) - 9 \mod 11 = 8$
10G = (8,8)

11G = (8,8) + (2,7)
m = $\frac{7-8}{2-8} = \frac{-1}{-6} \mod 11 = \frac{10}{5} \mod 11 = 10 * 9 \mod 11 = 2$
x = $2^2 - 8 - 2 \mod 11 = 5$
y = $2(8 - 5) - 8 \mod 11 = 9$
11G = (5,9)

12G = (5,9) + (2,7)
m = $\frac{7-9}{2-5} = \frac{-2}{-3} \mod 11 = \frac{9}{8} \mod 11 = 9 * 7 \mod 11 = 8$
x = $8^2 - 5 - 2 \mod 11 = 2$
y = $8(5 - 2) - 9 \mod 11 = 4$
12G = (2,4)

13G = (2,4) + (2,7)
m = $\frac{7-4}{2-2} = \frac{3}{0} \mod 11 = 3/0$
x = $2 + 0 \mod 11 = 2$
y = $4 + 3 \mod 11 = 7$
13G = (2,7)

10.15
calculations done using values from prev problem since same curve.
a).
$P_B = n_B \times G$
$P_B = 7G =$ (7,2)

b).
$C_m = \{kG, P_m + kP_B\}$
= {3G,(10,9) + 3(7,2)}
= {(8,3),(10,9) + (3,5)}
= {(8,3),(10,2)}

$P_m = \{kP_B - n_B(kG, P_m)\}$
= (10,2) - (3,5)
= (10,2) + (3,-5)

= (10,2) + (3,6)
= (10,9)

prob 3
31531, 485827, 15485863 are all prime
520482 is not prime and factors to (3 ,173494)