## 10.12

Determine all the points in $E_{11}(1,6)$, in other words find solutions $(x, y)$ to the equation $y^2 = x^3 + x + 6(mod\ 11)$.

| $x$ | $x^3 + x + 6(mod\ 11)$ | $y$ (quadratic residue of $x$) |
|---|---|---|
| 0 | 6 | {} |
| 1 | 8 | {} |
| 2 | 5 | {4,7} |
| 3 | 3 | {5,6} |
| 4 | 8 | {} |
| 5 | 4 | {2,9} |
| 6 | 8 | {} |
| 7 | 4 | {2,9} |
| 8 | 9 | {3,8} |
| 9 | 7 | {} |
| 10 | 4 | {2,9} |

Therefore, the points in $E_7(2,1)$ 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

What are the negatives of the following points over $\mathbb{Z}_{17}$? $P = (5,8)$, $Q = (3,0)$, and $R = (0,6)$

$-P = (5,9)$

$-Q = (3,0)$

$-R = (0,11)$

## 10.14

$E_{11}(1,6)$, point $G = (2,7)$, compute multiples of $G$ from $2G$ through $13G$.

| $N \times G$ | $P$ | $Q$ | $\lambda$ | $R_x$ | $R_y$ | $R$ |
|---|---|---|---|---|---|---|
| $2 \times G = G + G$ | (2,7) | (2,7) | $\frac{3 * 2^2 + 1}{2 * 7} = 8$ | $8^2 - 2 - 2 = 5$ | $8(2 - 5) - 7 = 2$ | (5,2) |
| $3 \times G = G + 2G$ | (2,7) | (5,2) | $\frac{7 - 2}{2 - 5} = 2$ | $2^2 - 2 - 5 = 8$ | $2(2 - 8) - 7 = 3$ | (8,3) |
| $4 \times G = G + 3G$ | (2,7) | (8,3) | $\frac{7 - 3}{2 - 8} = 3$ | $3^2 - 2 - 8 = 10$ | $10(2 - 10) - 7 = 2$ | (10,2) |
| $5 \times G = G + 4G$ | (2,7) | (10,2) | $\frac{7 - 2}{2 - 10} = 9$ | $9^2 - 2 - 10 = 3$ | $9(2 - 3) - 7 = 6$ | (3,6) |
| $6 \times G = G + 5G$ | (2,7) | (3,6) | $\frac{7 - 6}{2 - 3} = 10$ | $10^2 - 2 - 3 = 7$ | $10(2 - 7) - 7 = 9$ | (7,9) |
| $7 \times G = G + 6G$ | (2,7) | (7,9) | $\frac{7 - 9}{2 - 7} = 7$ | $7^2 - 2 - 7 = 7$ | $7(2 - 7) - 7 = 2$ | (7,2) |

| | | | | | | |
|---|---|---|---|---|---|---|
| $8 \times G = G + 7G$ | (2,7) | (7,2) | $\frac{7-2}{2-7} = 10$ | $10^2 - 2 - 7 = 3$ | $10(2-3) - 7 = 5$ | (3,5) |
| $9 \times G = G + 8G$ | (2,7) | (3,5) | $\frac{7-5}{2-3} = 9$ | $9^2 - 2 - 3 = 10$ | $9(2-10) - 7 = 9$ | (10,9) |
| $10 \times G = G + 9G$ | (2,7) | (10,9) | $\frac{7-9}{2-10} = 3$ | $3^2 - 2 - 10 = 8$ | $3(2-8) - 7 = 8$ | (8,8) |
| $11 \times G = G + 10G$ | (2,7) | (8,8) | $\frac{7-8}{2-8} = 2$ | $2^2 - 2 - 8 = 5$ | $2(2-5) - 7 = 9$ | (5,9) |
| $12 \times G = G + 11G$ | (2,7) | (5,9) | $\frac{7-9}{2-5} = 8$ | $8^2 - 2 - 5 = 2$ | $8(2-2) - 7 = 4$ | (2,4) |
| $13 \times G = G + 12G$ | (2,7) | (2,4) | $\frac{3 * 2^2 + 1}{2 * 7} = 8$ | $8^2 - 2 - 2 = 5$ | $8(2-5) - 7 = 2$ | (5,2) |

## 10.15

a. $P_B = n_B \times G = 7 \times (2,7) = (7,2)$
b. $C_m = \{kG, P_m + kP_B\} = \{3 \times (2,7), (10,9) + 3 \times (7,2)\} = \{(8,3), (10,2)\}$
c. $P_m = C_2 - n_B \times C_1 = (10,2) - 7 \times (8,3) = (10,9)$