10.12

| X | $y^2 = X^3 + 2x + 1$ | $y^2$ |
|---|---|---|
| 0 | 1 | 1, 6 |
| 1 | 4 | 2, 5 |
| 2 | 13 mod 7 = 6 | — |
| 3 | 34 mod 7 = 6 | — |
| 4 | 73 mod 7 = 3 | — |
| 5 | 136 mod 7 = 3 | — |
| 6 | 229 mod 7 = 5 | — |
| ∞ | | ∞ |

$0^2 \bmod 7 = 0$
$1^2 \bmod 7 = 1$
$2^2 \bmod 7 = 4$
$3^2 \bmod 7 = 2$
$4^2 \bmod 7 = 1$
$5^2 \bmod 7 = 4$
$6^2 \bmod 7 = 1$

Points on $E_7(2,1) = \{(0,1)\ (0,6)\ (1,2)\ (1,5)\}$

10.13 $P = (3,5)$ $-P = (3, -5 \bmod 7) = (3,2)$
$P = (2,5)$ $-P = (2, -5 \bmod 7) = (2,2)$
$P = (5,0)$ $-P = (5,0)$

10.14 $G = (3,2)$ $E_{11}(1,7)$

$2G = G + G = (3,2) + (3,2)$

$m = \frac{3(3)^2 + 1}{2(2)} = 7$

$x = 7^2 - 3 - 3 = 43 \bmod 11 = 10$
$y = 7(3-10) - 2 = -51 \bmod 11 = 4$

$2G = (10,4)$

$3G = 2G + G = (10,4) + (3,2)$

$m = \frac{4-2}{10-3} = \frac{2}{7} = \frac{4}{14} = \frac{4}{3} = \frac{16}{12} = 5$

$x = 5^2 - 10 - 3 = 12 \bmod 11 = 1$
$y = 5(10-1) - 4 = 41 \bmod 11 = 8$

$3G = (1,8)$

$4G = 3G + G = (1,8) + (3,2)$

$m = \frac{8-2}{1-3} = \frac{6}{-2} = \frac{6}{9} = \frac{2}{3} = \frac{8}{12} = 8$

$x = 8^2 - 1 - 3 = 60 \bmod 11 = 5$

$y = 8(1-5) - 8 = -40 \bmod 11 = 4$

$4G = (5,4)$

$5G = 4G + G = (5,4) + (3,2)$

$m = \frac{4-2}{5-3} = \frac{2}{2} = 1$

$x = 1^2 - 5 - 3 = -7 \bmod 11 = 4$

$y = 1(5-4) - 4 = -3 \bmod 11 = 8$

$\boxed{5G = (4,8)}$

$6G = 5G + G = (4,8) + (3,2)$

$m = \frac{8-2}{4-3} = 6$

$x = 6^2 - 4 - 3 = 29 \bmod 11 = 7$

$y = 6(4-7) - 8 = -26 \bmod 11 = 7$

$\boxed{6G = (7,7)}$

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

$m = \frac{7-2}{7-3} = \frac{5}{4} = \frac{15}{12} = 4$

$x = 4^2 - 7 - 3 = 6$

$y = 4(7-6) - 7 = -3 \bmod 11 = 8$

$\boxed{7G = (6,8)}$

$8G = 7G + G = (6,8) + (3,2)$

$m = \frac{8-2}{6-3} = \frac{6}{3} = 2$

$x = 2^2 - 6 - 3 = -5 \bmod 11 = 6$

$y = 2(6-6) - 8 = -8 \bmod 11 = 3$

$\boxed{8G = (6,3)}$

$9G = 8G + G = (6,3) + (3,2)$

$m = \frac{3-2}{6-8} = \frac{1}{3} = \frac{4}{12} = 4$

$x = 4^2 - 6 - 3 = 7$

$y = 4(6-7) - 3 = -7 \bmod 11 = 4$

$\boxed{9G = (7,4)}$

---

$10G = 9G + G = (7,4) + (3,2)$

$m = \frac{4-2}{7-3} = \frac{2}{4} = \frac{6}{12} = 6$

$x = 6^2 - 7 - 3 = 26 \bmod 11 = 4$

$y = 6(7-4) - 4 = 14 \bmod 11 = 3$

$\boxed{10G = (4,3)}$

---

$11G = 10G + G = (4,3) + (3,2)$

$m = \frac{3-2}{4-3} = 1$

$x = 1^2 - 4 - 3 = -6 \bmod 11 = 5$

$y = 1(4-5) - 3 = -4 \bmod 11 = 7$

$\boxed{11G = (5,7)}$

---

$12G = 11G + G = (5,7) + (3,2)$

$m = \frac{7-2}{5-3} = \frac{5}{2} = \frac{30}{12} = 8$

$x = 8^2 - 5 - 3 = 56 \bmod 11 = 1$

$y = 8(5-1) - 7 = 25 \bmod 11 = 3$

$\boxed{12G = (1,3)}$

---

$13G = 12G + G = (1,3) + (3,2)$

$m = \frac{3-2}{1-3} = \frac{1}{-2} = -\frac{6}{12} = -6 = 5$

$x = 5^2 - 1 - 3 = 21 \bmod 11 = 10$

$y = 5(1-10) - 3 = -48 \bmod 11 = 7$

$\boxed{13G = (10,7)}$

0.15

a) $P_B = P_0 \times 6$

$P_0 = 7 \times (3,2) = (6,8)$ from 10.14

b) $C_m = \{K_G, P_m + KP_0\}$

$C_m = \{5 \times (3,2), (10,7) + 5 \times (6,8)\}$

$C_m = \{(4,8), (10,7) + (4,8)\}$

$m = \frac{7-8}{10-4} = \frac{-1}{6} = \frac{10}{6} = \frac{20}{12} = 9$

$x = 9^2 - 10 - 4 = 67 \bmod 11 = 1$

$y = 9(10-1) - 7 = 74 \bmod 11 = 8$

$C_m = \{(4,8), (1,8)\}$

$5 \times (6,8) = 2 \times (6,8) + 3 \times (6,8)$

$2 \times (6,8) = (6,8) + (6,8)$

$m = \frac{3(6)^2 + 1}{2(8)} = \frac{109}{16} = \frac{10}{5} = 2$

$x = 2^2 - 6 - 6 = -8 \bmod 11 = 3$

$y = 2(6-3) - 8 = -2 \bmod 11 = 9$

$3 \times (6,8) = (3,9) + (6,8)$

$m = \frac{9-8}{3-6} = \frac{1}{-3} = \frac{-4}{12} = -4 \bmod 11 = 7$

$x = 7^2 - 3 - 6 = 40 \bmod 11 = 7$

$y = 7(3-7) - 9 = -37 \bmod 11 = 7$

$5 \times (6,8) = (7,7) + (3,9)$

$m = \frac{9-7}{3-7} = \frac{2}{-4} = \frac{-6}{12} = -6 \bmod 11 = 5$

$x = 5^2 - 7 - 3 = 15 \bmod 11 = 4$

$y = 5(7-4) - 7 = 8$

$5 \times (6,8) = (4,8)$

c) $C_m = \{(4,8), (1,8)\}$

$P_m = (1,8) - n_D \times (4,8)$

$n_D \times (4,8) = 7 \times (4,8) = (7,10)$

$2 \times (4,8) = (4,8) + (4,8) = (4,3)$

$m = \frac{3(4)^2+1}{2(8)} = \frac{48}{16} = \frac{5}{5} = 1$

$x = 1^2 - 4 - 4 = -7 \bmod 11 = 4$

$y = 1(4-4) - 8 = -8 \bmod 11 = 3$

$4 \times (4,8) = 2 \times (4,3) = (4,8)$

$m = \frac{3(4)^2+1}{2(3)} = \frac{49}{6} = \frac{5}{6} = \frac{10}{12} = 10$

$x = 10^2 - 4 - 4 = 92 \bmod 11 = 4$

$y = 10(4-4) - 3 = -3 \bmod 11 = 8$

$8 \times (4,8) = (4,8) + (4,8) = (4,3)$

$7 \times (4,8) = 8 \times (4,8) - (4,8)$

$= (4,3) + (4,3) = (4,8)$

---

$P_m = (1,8) - (4,8)$

$P_m = (1,8) + (4, -8 \bmod 11)$

$P_m = (1,8) + (4,3)$

$m = \frac{8-3}{1-4} = \frac{5}{-3} = -\frac{20}{12} = -20 = 2$

$x = 2^2 - 1 - 4 = -1 \bmod 11 = 10$

$y = 2(1-10) - 8 = -26 \bmod 11 = 7$

$\boxed{P_m = (10,7)}$