Chapter 8 作业.

1. 椭圆曲线 $y^2 \equiv x^3+x+6 \pmod{11}$，取 $p=(2,7)$，计算 $2p、3p、\cdots 13p$.

(1) $\lambda_1 = \frac{3\times 2^2+1}{2\times 7} \pmod{11} \equiv 8$ $\quad \therefore x_3 = 8^2-2-2 \pmod{11} \equiv 5$

$y_3 \equiv 8\times(2-5)-7 \pmod{11} \equiv 2$

$\therefore 2p=(5,2)$

(2) $3p=2p+p$: $x_2 \equiv -\frac{5}{3} \pmod{11} \equiv -20 \pmod{11} \equiv 2 \pmod{11}$

$\therefore x_3 \equiv 4-5-2 \pmod{11} \equiv 8$

$y_3 \equiv 2(-6)-7 \pmod{11} \equiv 3$ $\quad \therefore 3p=(8,3)$.

(3) $4p=p(2,7)+3p(8,3)$ $\quad \therefore \lambda_3 = -\frac{2}{3} \pmod{11} = 3 \pmod{11}$

$\therefore x_3 \equiv 9-2-8 \pmod{11} \equiv 10$

$y_3 \equiv 3\cdot(2-10)-7 \equiv 2$ $\quad \therefore 4p=(10,2)$.

---

(4) 同理可得 $5p=(3,6)$, $6p=(7,9)$, $7p=(7,2)$, $8p=(3,5)$.

$9p=(10,9)$, $10p=(8,8)$, $11p=(5,9)$, $12p=(2,4)$

(5) $13p=p(2,7)+12p(2,4)$

$\because p(2,7)$ 与 $12p(2,4)$ 的 x 坐标相同，用垂直于 x 轴的直线通过这两点，可看作是在无穷远点与椭圆曲线相交 $\therefore 13p=0$