

Student Number: XXXXXXXXXXName: Bryan Hoang

7. (10 points)

(a) **Answer:**Table 1: Computing $19 \cdot (24, 14)$ on $Y^2 = X^3 + 23X + 13 \pmod{83}$.

Step i	n	$Q = 2^i P$	R
0	19	$(24, 14)$	\mathcal{O}
1	9	$(30, 8)$	$(24, 14)$
2	4	$(24, 69)$	$(30, 75)$
3	2	$(30, 75)$	$(30, 75)$
4	1	$(24, 14)$	$(30, 75)$
5	0	$(30, 8)$	$(24, 69)$

Therefore, $\boxed{19 \cdot (24, 14) = (24, 69)}$.