

Quarter Square Multiplication

$$1. \quad xy = -\frac{(x-y)^2}{4} + \frac{(x+y)^2}{4} \longrightarrow (*)$$

$$2 \cdot 3$$

$$\begin{array}{r} 11 \\ \times 7 \\ \hline 6 \end{array}$$

n	0	1	2	3	4	5
$\lfloor \frac{n^2}{4} \rfloor$	0	0	1	1	4	6

Gives all xy when

$$x-y, x+y \in [0, 4]$$

Eg. $2 \cdot 2 = -0 + 4$

$$x, y \in \mathbb{Z} \Rightarrow (x+y)^2 \equiv (x-y)^2 \pmod{4} \leftarrow \text{Video} \longrightarrow (1)$$

$$a \equiv b \pmod{n}$$

$$n \mid a-b$$

$$(x+y)^2 = 4q + r$$

$$(x-y)^2 = 4q_1 + r_1$$

where $r, r_1 \in [0, 4]$

$$(1) \Rightarrow r = r_1$$

$$\Rightarrow \frac{(x+y)^2}{4} = q + \frac{r}{4}$$

$$\& \frac{(x-y)^2}{4} = q_1 + \frac{r}{4}$$

$$\longrightarrow (2)$$

$$\Rightarrow \lfloor \frac{(x+y)^2}{4} \rfloor = q \quad \& \quad \lfloor \frac{(x-y)^2}{4} \rfloor = q_1$$

$$\Rightarrow \lfloor \frac{(x+y)^2}{4} \rfloor - \lfloor \frac{(x-y)^2}{4} \rfloor = \underline{q - q_1} \longrightarrow (3)$$

$$(3), (*), (2) \Rightarrow \text{LHS of } (3) = xy.$$