

2

$$(2 + n)^{-1} \bmod n^2; n = 17$$

$$19^{-1} \bmod 289$$

Need to calculate **modular multiplicative inverse**

$$x \equiv 19^{-1} \bmod 289$$

$$19x - 289y = 1$$

Using extended Euclidean algorithm. Let's set: $x_0 = 1, x_1 = 0$

$q = \left\lfloor \frac{r_{i-1} - r_{i-2}}{r_{i-2}} \right\rfloor$	$r_i = r_{i-1} - qr_{i-2}$	$t_{i+1} = t_{i-1} - q_it_i$
	19	0
	289	1
15	4	-15
4	3	61
1	1	-76
3	0	289

Solution is -76 ; $19 * (-76) = 1 - 289 * 5$.

1

$$Y^2 = X^3 + 2X + 4 \bmod 11; P : (10, 10); \text{find } 3P$$