

pow_in	bit	function calls	operation	pow_out
2	-	MONT_SQR	Mp(2, 2)	3
3	-	MONT_SQR	Mp(3, 3)	5
5	0	MONT_SQR	Mp(5, 5)	9
9	1	MONT_SQR, MMUL_ONE	Mp(9, Mp(9,0))	16