

Teoria dei numeri - Congruenze (mod p) 1

Esercizio 1. In ogni riga sono dati due interi a ed m . Scrivere il ciclo delle potenze di a modulo m .

a	m	Ciclo delle potenze di a mod m
2	5	
2	7	
2	17	
3	27	
5	30	
6	22	
2	99	
-3	50	

Esercizio 2. Dati un intero a e un primo p , calcolare $\text{ord}_p(a)$.

a	p	ord_p(a)	a	p	ord_p(a)
2	11		2	7	
7	31		3	31	
4	47		8	47	
10	101		2	101	
5	37		2	37	

Esercizio 3. Per ognuno dei seguenti numeri primi, elencare i generatori mod p tra 1 e $p - 1$.

Primo	Generatori
7	
11	
13	
31	
47	
97	
211	