

1. Sia  $p > 2$  un numero primo e sia  $\bar{g} \in \mathbf{Z}_p^*$ .
  - (a) Verificare che  $\bar{g}$  è una radice primitiva di  $\mathbf{Z}_p^*$  se e solo se  $\bar{g}^{\frac{p-1}{d}} \neq 1 \pmod{p}$ , per tutti i divisori primi distinti di  $p-1$ ;
  - (b) Quante radici primitive ci sono in  $\mathbf{Z}_p^*$ ?
2. Sia  $p = 79$ .
  - (a) Determinare se  $\bar{2}$  è una radice primitiva in  $\mathbf{Z}_p^*$ .
  - (b) Verificare che  $\bar{3}$  è una radice primitiva in  $\mathbf{Z}_p^*$ .
3. Trovare una radice primitiva  $\bar{g}$  in  $\mathbf{Z}_p^*$ , per  $p = 71, 101, 113$ .
4. Sia  $p$  un numero primo e sia  $\bar{g}$  una radice primitiva in  $\mathbf{Z}_p^*$ . Il *logaritmo discreto*  $\log \bar{a}$  di  $\bar{a} \in \mathbf{Z}_p^*$  in base  $\bar{g}$  è un intero  $j$  tale che  $\bar{g}^j = \bar{a}$  modulo  $p$ .
  - (a) Verificare che il logaritmo discreto in base  $\bar{g}$  è ben definito modulo  $p-1$ , ossia  $\bar{g}^i = \bar{g}^j$  se e solo se  $i \equiv j \pmod{p-1}$ .
  - (b) Verificare che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori (modulo  $p-1$ ).
  - (c) Verificare che  $\log \bar{-1} = \frac{p-1}{2}$ .
5. Sia  $p$  un numero primo e siano  $\bar{g}$  e  $\bar{g}'$  due radici primitive in  $\mathbf{Z}_p^*$ . Siano  $\log_g$  il logaritmo in base  $g$  e  $\log_{g'}$  il logaritmo in base  $g'$ . Verificare che esiste  $c \in \mathbf{Z}$  tale che  $\log_g \bar{a} = c \log_{g'} \bar{a}$ , per ogni  $\bar{a} \in \mathbf{Z}_p^*$ .
6. Sia  $p \neq 2$  un numero primo sia  $\bar{g}$  una radice primitiva in  $\mathbf{Z}_p^*$ . Verificare che  $\bar{x}$  è un quadrato in  $\mathbf{Z}_p^*$  se e solo se il logaritmo discreto è pari.
7. Sia  $p = 79$  e sia fissata la radice primitiva  $\bar{g} = \bar{3}$ . Calcolare  $\log \bar{-1}$ ,  $\log \bar{3}$ ,  $\log \bar{2}$ ,  $\log \bar{5}$ ,  $\log \bar{7}$ ,  $\log \bar{41}$ ,  $\log \bar{43}$  in tale base.
8. Sia  $p = 83$  e sia  $\bar{g} = \bar{2}$ .
  - (a) Verificare che  $\bar{2}$  è una radice primitiva in  $\mathbf{Z}_p^*$ .
  - (b) Calcolare  $\log \bar{7}$  in tale base.
9. Sia  $p = 23$ .
  - (a) Determinare una radice primitiva  $\bar{g} \in \mathbf{Z}_p^*$ .
  - (b) Calcolare  $\log \bar{2}$  in tale base.
10. Sia  $p = 59$ .
  - (a) Verificare che  $\bar{2}$  è una radice primitiva in  $\mathbf{Z}_p^*$ .
  - (b) Calcolare  $\log \bar{3}$  in tale base.
11. Sia  $p = 37$ .
  - (a) Verificare che  $\bar{2}$  è una radice primitiva in  $\mathbf{Z}_p^*$ .
  - (b) Fissata la base  $\bar{g} = \bar{2}$ , calcolare  $\log \bar{2}$ ,  $\log \bar{5}$ ,  $\log \bar{11}$ . (Usare il calcolo dell'indice oppure baby-steps-giant-steps).
12. Il signor Bianchi e il signor Rossi vogliono condividere un codice segreto senza il rischio che venga intercettato. Si accordano sul primo  $p = 97$  e la radice primitiva  $\bar{g} = \bar{5}$  (è la più piccola...verificare...). Bianchi usa il suo esponente segreto  $b$  e spedisce a Rossi  $\bar{g}^b = 28$ , Rossi usa il suo esponente segreto  $r$  e spedisce a Bianchi  $\bar{g}^r = 21$ . Qual è il codice segreto comune di Bianchi e Rossi??

Consideriamo adesso la seguente tabella di conversione.

1	2	3	4	5	6	7	8	9	?	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
01	02	03	04	05	06	07	08	09	10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	-	-
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	-	-

13. Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema ElGamal. Le sue chiavi pubbliche sono il primo  $p = 31$ , la radice primitiva  $\bar{g} = \bar{3}$  e il numero  $E = 26$ .
- Una spia è riuscita però a ricostruire la sua chiave segreta  $D$ . Qual è?
  - Rossi riceve da Bianchi un messaggio composto dalle seguenti tre stringhe:

$$(c_1, c_2) = (\bar{9}, \bar{15}), \quad (d_1, d_2) = (\bar{27}, \bar{25}), \quad (e_1, e_2) = (\bar{19}, \bar{19}).$$

Che cosa gli ha mandato a dire?

- Riusciamo a ricostruire il messaggio di Bianchi anche senza sapere la chiave segreta di Rossi?
14. Bianchi ha chiavi pubbliche il primo  $p' = 59$ , la radice primitiva  $\bar{g}' = \bar{2}$  e il numero  $E' = 5$ . Rossi gli risponde con le due stringhe

$$(f_1, f_2) = (\bar{12}, \bar{16}) \quad (r_1, r_2) = (\bar{12}, \bar{6}).$$

- La spia è riuscita però a ricostruire anche la chiave segreta di Bianchi  $D'$ . Qual è?
- Cosa gli ha risposto Rossi?
- Riusciamo a ricostruire la risposta di Rossi anche senza sapere la chiave segreta di Bianchi?