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 $\bar{g}^{\frac{p-1}{d}} \not\equiv 1 \mod p$, per tutti i divisori primi distinti di $p-1$;
   (b) Quante radici primitive ci sono in $\mathbf{Z}_p^*$?

Sol. (a) Vedi Nota radici primitive.

(b) Vedi Nota radici primitive (Osservazione sulla Formula di Gauss): Nel gruppo ciclico $\mathbf{Z}_p^*$ ci sono $\varphi(p-1)$ elementi di ordine $p-1$, ossia $\varphi(p-1)$ radici primitive.

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 $\mathbf{Z}_p^*$.

Sol. (a) Abbiamo $p - 1 = 78 = 2 \cdot 3 \cdot 13$. Usiamo il criterio dell'esercizio 1. Calcolando

$$\bar{2}^{78/13} = \bar{2}^6 \equiv \overline{64}, \quad \bar{2}^{78/3} = \bar{2}^{26} \equiv \overline{23}, \quad \bar{2}^{78/2} = \bar{2}^{39} \equiv \bar{1} \mod 79$$

troviamo che $\bar{2}$ non è una radice primitiva di $\mathbf{Z}_{79}^*$.

(b) Calcolando

$$\bar{3}^{78/13} = \bar{3}^6 \equiv \overline{18}, \quad \bar{3}^{78/3} = \bar{3}^{26} \equiv \overline{23}, \quad \bar{3}^{78/2} = \bar{3}^{39} \equiv \overline{78} \mod 79$$

troviamo che $\bar{3}$ è una radice primitiva di $\mathbf{Z}_{79}^*$.

3. Trovare una radice primitiva $\bar{g}$ in $\mathbf{Z}_p^*$, per $p = 71, 101, 113$.

Sol. - $p = 71$, $p - 1 = 70 = 2 \cdot 5 \cdot 7$. In questo caso la più piccola radice primitiva di $\mathbf{Z}_{71}^*$ è $\bar{g} = \bar{7}$.
Verifica: $\bar{7}^{10} \equiv \overline{45}, \quad \bar{7}^{14} \equiv \overline{54}, \quad \bar{7}^{35} \equiv \overline{70} \mod 71$.

- $p = 101$, $p - 1 = 100 = 2^2 \cdot 5^2$. In questo caso la più piccola radice primitiva di $\mathbf{Z}_{101}^*$ è $\bar{g} = \bar{2}$.
Verifica: $\bar{2}^{20} \equiv \overline{95}, \quad \bar{2}^{50} \equiv \overline{100} \equiv \overline{-1} \mod 101$.

- $p = 113$, $p - 1 = 112 = 2^4 \cdot 7$. In questo caso la più piccola radice primitiva di $\mathbf{Z}_{113}^*$ è $\bar{g} = \bar{3}$.
Verifica: $\bar{3}^{16} \equiv \overline{49}, \quad \bar{3}^{56} \equiv \overline{112} \equiv \overline{-1} \mod 113$.

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 $i \equiv j \mod p-1$.
   (b) Verificare che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori (modulo $p-1$).
   (c) Verificare che $\log \overline{-1} = \frac{p-1}{2}$.

Sol. (a) Se $i = j + k(p-1)$, con $k \in \mathbf{Z}$, vale $\bar{g}^i = \bar{g}^j \cdot \bar{g}^{k(p-1)}$. Poiché per il Piccolo Teorema di Fermat $\bar{g}^{p-1} \equiv \bar{1} \mod p$, allora anche $\bar{g}^{k(p-1)} \equiv \bar{1} \mod p$ e $\bar{g}^i = \bar{g}^j \mod p$.
Supponiamo viceversa che $\bar{g}^i = \bar{g}^j \mod p$. Allora $\bar{g}^{i-j} \equiv \bar{1} \mod p$. Poiché $\bar{g}$ è una radice primitiva, l'ordine di $\bar{g}$ in $\mathbf{Z}_p^*$ è uguale a $p-1$. Ne segue che $i - j = k(p-1)$, per $k \in \mathbf{Z}$.

(b) Siano $i = \log \bar{a}$ e $j = \log \bar{b}$. Ciò significa che $\bar{g}^i = \bar{a}$ e $\bar{g}^j = \bar{b}$. Ne segue che

$$\bar{g}^i \cdot \bar{g}^j = \bar{g}^{i+j} = \bar{a} \cdot \bar{b} = \overline{ab}$$

ed in particolare

$$i + j = \log \overline{ab} \mod (p-1).$$

(c) Sia i l'intero, unico modulo $(p-1)$, tale che $\bar{g}^i \equiv \overline{-1}$. Elevando al quadrato, troviamo $\bar{g}^{2i} \equiv \bar{1}$, da cui seguono (vedi punto (a) di questo esercizio) $2i = (p-1)k$ ed $i = \frac{p-1}{2}k$, con $k \in \mathbf{Z}$. Osserviamo che k in realtà deve essere *dispari*, altrimenti $\frac{k}{2}$ sarebbe intero ed avremmo $\bar{g}^i \equiv \bar{g}^{\frac{p-1}{2}k} \equiv \bar{1}$.

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 $\bar{a} \in \mathbf{Z}_p^*$.

Sol. Sia $\bar{a} \in \mathbf{Z}_p^*$. Poiché $\bar{g}$ e $\bar{g}'$ sono due radici primitive, esistono interi i e j tali che

$$\bar{a} = \bar{g}^i = (\bar{g}')^j.$$

D'altra parte anche $\bar{g}' = \bar{g}^m$, per un $m \in \mathbf{Z}$. Ne segue che $\bar{a} = \bar{g}^i = \bar{g}^{mj}$ e

$$\log_{\bar{g}} \bar{a} = m \log_{\bar{g}'} \bar{a}, \qquad m = \log_{\bar{g}} \bar{g}'.$$

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.

Sol. Sia $\bar{x}$ un quadrato, ossia $\bar{x} = \bar{a}^2$, per qualche $\bar{a} \in \mathbf{Z}_p^*$. Scrivendo $\bar{a} = \bar{g}^m$, con $m \in \mathbf{Z}$, troviamo $\bar{x} = \bar{a}^2 = \bar{g}^{2m}$. Ne segue che $\log \bar{x} = 2m \mod p-1$ è pari.
Viceversa, se $\log \bar{x} = 2m \mod p-1$ è pari, allora $\bar{x} = \bar{g}^{2m} = (\bar{g}^m)^2$, ossia $\bar{x}$ è il quadrato di $\bar{g}^m$.

7. Sia $p = 79$ e sia fissata la radice primitiva $\bar{g} = \bar{3}$. Calcolare $\log \overline{-1}$, $\log \bar{3}$, $\log \bar{2}$, $\log \bar{5}$, $\log \bar{7}$, $\log \overline{41}$, $\log \overline{43}$ in tale base.

Sol. Direttamente dalla definizione troviamo $\log \overline{-1} = \frac{p-1}{2} = 39$, $\quad \log \bar{3} = 1$.
Determiniamo $\log \bar{5}$ col calcolo dell'indice. Dalle relazioni

$$\bar{1} \equiv \overline{80} \equiv \bar{2}^4 \cdot \bar{5}, \qquad \bar{2} \equiv \overline{81} \equiv \bar{3}^4 \mod 79$$

estraendo i logaritmi in base $\bar{3}$, troviamo

$$\begin{cases} 4 \log \bar{2} + \log \bar{5} \equiv \bar{0} \mod 78 \\ \log \bar{2} - 4 \log \bar{3} \equiv \bar{0} \mod 78. \end{cases}$$

Da ciò ricaviamo

$$\log \bar{2} \equiv 4, \quad \log \bar{5} \equiv -4 \log \bar{2} \equiv -16 \equiv 62 \mod 78.$$

Determiniamo adesso $\log \bar{7}$. Dalle relazioni

$$\bar{7} \equiv \overline{86} \equiv \bar{2} \cdot \overline{43}, \qquad \bar{3} \cdot \overline{43} \equiv \overline{129} \equiv \bar{2} \cdot \bar{5}^2 \mod 79$$

estraendo i logaritmi in base $\bar{3}$, troviamo

$$\begin{cases} \log \bar{2} - \log \bar{7} + \log \overline{43} \equiv \bar{0} \mod 78 \\ \log \bar{2} - \log \bar{3} + 2 \log \bar{5} - \log \overline{43} \equiv \bar{0} \mod 78. \end{cases}$$

Da ciò ricaviamo

$$\log \bar{7} \equiv 53, \qquad \log \overline{43} = 49 \mod 78.$$

Determiniamo infine $\log \overline{41}$. Dalla relazione

$$\bar{3} \equiv \overline{82} \equiv \bar{2} \cdot \overline{41}, \mod 79$$

estraendo i logaritmi in base $\bar{3}$, troviamo

$$\log \overline{41} = \log \bar{3} - \log \bar{2} = -3 = 75 \mod 78.$$

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.

Sol. (a) Abbiamo $p - 1 = 82 = 2 \cdot 41$. Poiché $\bar{2}^2 \equiv 4 \not\equiv \bar{1} \mod 83$ e $\bar{2}^{41} \equiv \overline{82} \equiv \overline{-1} \not\equiv \bar{1} \mod 83$, abbiamo che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{83}^*$.
(b) Calcolare $\log \bar{7}$ in base $\bar{g} = \bar{2}$ col calcolo dell'indice. Scegliamo i numeri $-1, 2, 3, 5, 7$ e cerchiamo delle relazioni fra i rispettivi logaritmi. Osserviamo intanto che $\log \bar{2} = 1$ e $\log \overline{-1} = 41$. Dalle relazioni

$$\bar{1} = \overline{84} = \bar{2}^2 \cdot \bar{3} \cdot \bar{7}, \qquad \overline{-1} \cdot \bar{2} = \overline{81} = \bar{3}^7,$$

estraendo il logaritmo troviamo

$$\begin{cases} 2\log \bar{2} + \log \bar{3} + \log \bar{7} = 0 \\ \log \overline{-1} + \log \bar{2} - 4 \log \bar{3} = 0 \end{cases} \Leftrightarrow \begin{cases} \log \bar{3} + \log \bar{7} = -2 \\ 4 \log \bar{3} = 42 \end{cases} \mod 82. \qquad (*)$$

ATTENZIONE: le relazioni (*) non ci permettono di ricavare $\log \bar{3}$ e $\log \bar{7}$. Infatti, il logaritmo in $\mathbf{Z}_{83}^*$ è definito modulo 82, quindi il sistema lineare (*) è un sistema a coefficienti in $\mathbf{Z}_{82}$ e per risolverlo dobbiamo evitare di dividere per elementi non invertibili in $\mathbf{Z}_{82}$. Ad esempio, non possiamo ricavare $\log \bar{3}$ dalla relazione $4 \log \bar{3} = 42 \mod 82$, perché dovremmo dividere per 4 e 4 non è invertibile modulo 82 (infatti $mcd(4, 82) \neq 1$).
Dobbiamo allora aggiungere altre equazioni al sistema....
Dalle relazioni

$$\bar{2} \cdot \bar{7}^2 = \overline{98} = \overline{15} = \bar{3} \cdot \bar{5}, \qquad \bar{3} \cdot \bar{5}^2 = \overline{75} = \overline{-8} = \overline{-1} \cdot \bar{2}^3,$$

estraendo il logaritmo ricaviamo

$$\begin{cases} \log \bar{2} + 2\log \bar{7} = \log \bar{3} + \log \bar{5} \\ \log \bar{3} + 2\log \bar{5} = \log \overline{-1} + 3\log \bar{2}. \end{cases}$$

Mettendo insieme queste equazioni con quelle precedenti, otteniamo il nuovo sistema

$$\begin{cases} \log \bar{3} + \log \bar{7} = -2 \\ \log \bar{3} + \log \bar{5} - 2\log \bar{7} = 1 \\ \log \bar{3} + 2\log \bar{5} = 44 \end{cases} \Leftrightarrow \begin{cases} \log \bar{3} = -2 - \log \bar{7} \\ \log \bar{5} = 3 + 3\log \bar{7} \\ 5\log \bar{7} = 40. \end{cases}$$

Osserviamo che $\gcd(5, 82) = 1$, quindi in questo caso possiamo dividere per 5 e ricavare $\log \bar{7} = 8$ dalla terza equazione del sistema. Ricaviamo poi $\log \bar{5} = 27$ e $\log \bar{3} = -10 = 72 \mod 82$.

9. Sia $p = 23$.
   (a) Determinare una radice primitiva $\bar{g} \in \mathbf{Z}_p^*$.
   (b) Calcolare $\log \bar{2}$ in tale base.

Sol. (a) Abbiamo $p - 1 = 22 = 2 \cdot 11$. Poiché $\bar{5}^2 \equiv \bar{2} \not\equiv \bar{1}$ e $\bar{5}^{11} \equiv \overline{-1} \not\equiv \bar{1}$ abbiamo che $\bar{5}$ è una radice primitiva in $\mathbf{Z}_{23}^*$.
(b) Calcoliamo $\log \bar{2}$ in base $\bar{g} = \bar{5}$ col metodo baby-step-giant-step. In altre parole risolviamo l'equazione

$$\bar{5}^x = \bar{2} \quad \Leftrightarrow \quad x = \log_{\bar{5}} \bar{2} \quad \text{in } \mathbf{Z}_{23}^*.$$

Fissiamo $m = 5 \sim \sqrt{23}$ e indici $0 \leq j, i < m$ che parametrizzano rispettivamente le due liste $\{\bar{g}^j\}_{j=0,\ldots,m-1}$ (baby steps) e $\{\bar{a}\bar{g}^{-mi}\}_{i=0,\ldots,m-1}$ (giant steps), con $\bar{a} = \bar{2}$ e $\bar{g} = \bar{5}$:

$$\bar{5}^0 = \bar{1}, \quad \bar{5}^1 = \bar{5}, \quad \bar{5}^2 = \bar{2}, \quad \bar{5}^3 = \overline{10}, \quad \bar{5}^4 = \bar{4} \qquad \mod 23$$

$$\bar{2} \cdot \bar{5}^0 = \bar{2}, \quad \bar{2} \cdot \bar{5}^{-5} = \bar{7}, \quad \bar{2} \cdot \bar{5}^{-10} = \overline{13}, \quad \bar{2} \cdot \bar{5}^{-15} = \overline{11}, \quad \bar{2} \cdot \bar{5}^{-20} = \bar{4} \qquad \mod 23.$$

Già dalla prima lista troviamo $\bar{5}^2 = \bar{2}$, che equivale a $\log_{\bar{5}} \bar{2} = 2$.

ATTENZIONE: In generale, una volta trovato il logaritmo cercato oppure alla prima coincidenza fra le due liste ci si ferma. Qui calcoliamo interamente le due liste per illustrare il metodo.

Con lo stesso metodo calcoliamo adesso $\log_{\bar{5}} \bar{3}$ ossia risolviamo $\bar{5}^x = \bar{3}$.
La prima lista resta la stessa:

$$\bar{5}^0 = \bar{1}, \quad \bar{5}^1 = \bar{5}, \quad \bar{5}^2 = \bar{2}, \quad \bar{5}^3 = \overline{10}, \quad \bar{5}^4 = \bar{4} \qquad \text{mod } 23;$$

la seconda diventa $\{\bar{a}\bar{g}^{-mi}\}_{i=0,\dots,m-1}$ (giant steps), con $\bar{a} = \bar{3}$ e $\bar{g} = \bar{5}$:

$$\bar{3} \cdot \bar{5}^0 = \bar{3}, \quad \bar{3} \cdot \bar{5}^{-5} = \overline{22}, \quad \bar{3} \cdot \bar{5}^{-10} = \bar{8}, \quad \bar{3} \cdot \bar{5}^{-15} = \bar{5}, \quad \bar{3} \cdot \bar{5}^{-20} = \bar{6} \qquad \text{mod } 23.$$

Confrontando le due liste troviamo

$$\bar{5}^1 = \bar{5} = \bar{3} \cdot \bar{5}^{-15} \quad \Leftrightarrow \quad \bar{5}^{16} = \bar{3},$$

da cui

$$\log_{\bar{5}} \bar{3} = 16.$$

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.

Sol. (a) Abbiamo $p - 1 = 58 = 2 \cdot 29$. Poiché $\bar{2}^2 \equiv 4 \not\equiv \bar{1} \mod 59$ e $\bar{2}^{29} \equiv \overline{58} \equiv \overline{-1} \not\equiv \bar{1} \mod 59$, abbiamo che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{59}^*$.

(b) Calcoliamo $\log \bar{3}$ rispetto alla radice primitiva $\bar{2}$ col calcolo dell'indice. Osserviamo innanzitutto che $\log \bar{2} = 1$ e $\log(-1) = 29$. Fissiamo i numeri $2, 3, 5, -1$ e cerchiamo delle relazioni fra i rispettivi logaritmi. Dalle relazioni

$$\bar{1} = \overline{60} = \bar{2}^2 \cdot \bar{3} \cdot \bar{5}, \qquad \bar{5} = \overline{64} = \bar{2}^6,$$

estraendo il logaritmo troviamo

$$\begin{cases} 2\log \bar{2} + \log \bar{3} + \log \bar{5} = 0 \mod 58 \\ \log \bar{5} = 6 \log \bar{2} \mod 58. \end{cases}$$

Ne ricaviamo $\log \bar{5} = 6$ e $\log \bar{3} = -\log \bar{5} - 2\log \bar{2} = -8 = 50 \mod 58$.
Prova: $\bar{2}^{50} \equiv 3 \mod 59$.

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 $\log \bar{2}$, $\log \bar{5}$, $\log \overline{11}$. (Usare il calcolo dell'indice oppure baby-steps-giant-steps).

Sol. (a) Abbiamo $p - 1 = 36 = 2^2 \cdot 3^2$. Poiché $\bar{2}^{12} \equiv \overline{26} \not\equiv \bar{1}$ e $\bar{2}^{18} \equiv \overline{36} \not\equiv \bar{1}$ abbiamo che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{23}^*$.

(b) Per definizione, $\log_{\bar{2}} \bar{2} = 1$. Per calcolare gli altri logaritmi, usiamo baby-step-giant-step.
Fissiamo $m = 6 \sim \sqrt{36}$ e indici $0 \le j, i < m$ che parametrizzano rispettivamente le due liste $\{\bar{g}^j\}_{j=0,\dots,m-1}$ (baby steps) e $\{\bar{a}\bar{g}^{-mi}\}_{i=0,\dots,m-1}$ (giant steps), con $\bar{g} = \bar{2}$ e $\bar{a} = \bar{5}$ e $\bar{a} = \overline{11}$.
La prima lista è

$$\bar{2}^0 = \bar{1}, \quad \bar{2}^1 = \bar{2}, \quad \bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{8}, \quad \bar{2}^4 = \overline{16}, \quad \bar{2}^5 = \overline{32} \qquad \text{mod } 37;$$

per $\bar{a} = \bar{5}$ la seconda lista è data da:

$$\bar{5}\cdot\bar{2}^0 = \bar{5}, \quad \bar{5}\cdot\bar{2}^{-6} = \overline{18}, \quad \bar{5}\cdot\bar{2}^{-12} = \overline{13}, \quad \bar{5}\cdot\bar{2}^{-18} = \overline{32}, \quad \bar{5}\cdot\bar{2}^{-24} = \overline{19}, \quad \bar{5}\cdot\bar{2}^{-30} = \overline{24} \qquad \text{mod } 37.$$

Confrontando le due liste, troviamo $\bar{2}^5 = \overline{32} = \bar{5}\cdot\bar{2}^{-18} = \overline{32}$, da cui

$$\log_{\bar{2}} \bar{5} = 23.$$

Per calcolare $\log \overline{11}$, la prima lista resta invariata. Per $\bar{a} = \overline{11}$, a seconda lista diventa

$$\overline{11}\cdot\bar{2}^0 = \overline{11}, \quad \overline{11}\cdot\bar{2}^{-6} = \overline{10}, \quad \overline{11}\cdot\bar{2}^{-12} = \overline{36}, \quad \overline{11}\cdot\bar{2}^{-18} = \overline{26}, \quad \overline{11}\cdot\bar{2}^{-24} = \overline{27}, \quad \overline{11}\cdot\bar{2}^{-30} = \bar{1} \qquad \text{mod } 37.$$

Confrontando le due liste, troviamo $\bar{2}^0 = \bar{1} = \overline{11}\cdot\bar{2}^{-30} = \bar{1}$, da cui

$$\log_{\bar{2}} \overline{11} = 30.$$

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 $\bar{g}^b = \overline{28}$, Rossi usa il suo esponente segreto r e spedisce a Bianchi $\bar{g}^r = \overline{21}$. Qual è il codice segreto comune di Bianchi e Rossi??

Sol. Anche conoscendo le chiavi pubbliche $p = 97$ e $\bar{g} = \bar{5}$, per scoprire il codice segreto comune di Bianchi e Rossi a partire dalle stringhe $\overline{28}$ e $\overline{21}$ che viaggiano in chiaro fra i due utenti, dobbiamo calcolare i logaritmi $x = \log_{\bar{5}} \overline{28}$ e $y = \log_{\bar{5}} \overline{21}$ in $\mathbf{Z}_{97}^*$ (vedi Diffie-Hellmann-Merkle key-exchange). Dopodiché il codice segreto sarà dato da $\bar{5}^{xy}$. Usiamo usiamo baby-step-giant-step. Fissiamo $m = 10 \sim \sqrt{97}$ e indici $0 \leq j, i < m$ che parametrizzano rispettivamente le due liste $\{\bar{g}^j\}_{j=0,\ldots,m-1}$ (baby steps) e $\{\bar{a}\bar{g}^{-mi}\}_{i=0,\ldots,m-1}$ (giant steps), con $\bar{g} = \bar{5}$ e $\bar{a} = \overline{28}$ e $\bar{a} = \overline{21}$.
La prima lista è data da:

$$\bar{5}^0 = \bar{1}, \quad \bar{5}^1 = \bar{5}, \quad \bar{5}^2 = \overline{25}, \quad \bar{5}^3 = \overline{28}, \quad \bar{5}^4 = \overline{43}, \quad \bar{5}^5 = \overline{21}, \quad \bar{5}^6 = \overline{8}, \quad \bar{5}^7 = \overline{40}, \quad \bar{5}^8 = \overline{6}, \quad \bar{5}^9 = \overline{30} \qquad \text{mod } 97;$$

per $\bar{a} = \overline{28}$, la seconda lista è data da:

$$\overline{28}\cdot\bar{5}^0 = \overline{28}, \quad \overline{28}\cdot\bar{5}^{-10} = \overline{17}, \quad \overline{28}\cdot\bar{5}^{-20} = \overline{90}, \quad \overline{28}\cdot\bar{5}^{-30} = \overline{20}, \quad \overline{28}\cdot\bar{5}^{-40} = \overline{26}, \quad \overline{28}\cdot\bar{5}^{-50} = \overline{92}, \quad \overline{28}\cdot\bar{5}^{-60} = \overline{42},$$

$$\overline{28}\cdot\bar{5}^{-70} = \overline{74}, \quad \overline{28}\cdot\bar{5}^{-80} = \overline{38}, \quad \overline{28}\cdot\bar{5}^{-90} = \overline{30}.$$

Confrontando le due liste troviamo $\bar{5}^3 = \overline{28}\cdot\bar{5}^0 = \overline{28}$, da cui

$$\log_{\bar{5}} \overline{28} = 3.$$

ATTENZIONE: abbiamo calcolato interamente entrambe le liste più che altro per illustrare il metodo. In questo caso, già dal quarto elemento della prima lista si ottiene il logaritmo $\log_{\bar{5}} \overline{28} = 3$.
Inoltre dal sesto elemento della prima lista si ottiene il logaritmo $\log_{\bar{5}} \overline{21} = 5$.
Il codice segreto di Bianchi e Rossi risulta quindi

$$\bar{5}^{3\cdot 5} = \overline{46} \mod 97.$$

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 classe primitiva $\bar{g} = \bar{3}$ e il numero $E = 26$.
    (a) Una spia è riuscita però a ricostruire la sua chiave segreta D. Qual è?
    (b) Rossi riceve da Bianchi un messaggio composto dalle seguenti tre stringhe:
    $$(c_1, c_2) = (\bar{9}, \overline{15}), \qquad (d_1, d_2) = (\overline{27}, \overline{25}), \qquad (e_1, e_2) = (\overline{19}, \overline{19}).$$
    Che cosa gli ha mandato a dire?
    (c) Riusciamo a ricostruire il messaggio di Bianchi anche senza sapere la chiave segreta di Rossi?

Sol. (a) La chiave segreta di Rossi è data da $D = \log_{\bar{3}} \overline{26}$ in $\mathbf{Z}_{31}^*$. Calcoliamo D usando il calcolo dell'indice. Osserviamo che $\log \bar{3} = 1$ e $\log \overline{-1} = 15$. Inoltre $\log \overline{26} = \log \bar{2} + \log \overline{13}$. Dalle relazioni
$$-1 \equiv 30 = 2 \cdot 3 \cdot 5, \quad -5 = (-1) \cdot 5 \equiv 26 = 2 \cdot 13 \quad 5 \equiv 36 = 2^2 \cdot 3^2 \quad 8 \equiv 39 = 3 \cdot 13 \qquad \mod 31$$
troviamo
$$\begin{cases} \log \bar{2} + \log \bar{5} = 14 \\ \log \bar{2} - \log \bar{5} + \log \overline{13} = 15 \\ 2 \log \bar{2} - \log \bar{5} = -2 \\ 3 \log \bar{2} - \log \overline{13} = 1 \end{cases} \mod 30$$
da cui ricaviamo, *dividendo solo per scalari invertibili modulo 30,*
$$\log \overline{13} = 11, \quad \log \bar{5} = 20, \quad \log \bar{2} = 24$$
e dunque
$$D = \log \overline{26} = \log \overline{13} + \log \bar{2} = 11 + 24 = 35 \equiv 5 \qquad \mod 30.$$
(b) Ricostruiamo i tre messaggi calcolando
$$c_2 \cdot c_1^{-D} = \overline{15} \cdot \bar{9}^{-5} \equiv \overline{13}, \qquad d_2 \cdot d_1^{-D} = \overline{25} \cdot \overline{27}^{-5} \equiv \bar{6}, \qquad e_2 \cdot e_1^{-D} = \overline{19} \cdot \overline{19}^{-5} \equiv \overline{10} \qquad \mod 31.$$
Dalla tabella troviamo che Bianchi ha mandato a Rossi il seguente messaggio
$$C\ 6\ ?$$
(c) Un messaggio criptato è della forma $(\bar{g}^\mu, m \cdot E^\mu)$. Per leggerlo possiamo cercare di determinare μ e poi ottenere $m \equiv m \cdot E^\mu \cdot E^{-\mu}$. Si tratta comunque di risolvere un logaritmo discreto in $\mathbf{Z}_p^*$...

14. Bianchi ha chiavi pubbliche il primo $p' = 59$, la classe primitiva $\bar{g}' = \bar{2}$ e il numero $E' = 5$. Rossi gli risponde con le due stringhe
$$(f_1, f_2) = (\overline{12}, \overline{16}) \qquad (r_1, r_2) = (\overline{12}, \bar{6}).$$
    (a) La spia è riuscita però a ricostruire anche la chiave segreta di Bianchi D'. Qual è?
    (b) Cosa gli ha risposto Rossi?
    (c) Riusciamo a ricostruire la risposta di Rossi anche senza sapere la chiave segreta di Bianchi?

Sol. (a) La chiave segreta di Bianchi è data da $D' = \log_{\bar{2}} \bar{5}$ in $\mathbf{Z}_{59}^*$. Calcoliamo D' usando il calcolo dell'indice. Dalla relazione $64 = 2^6 \equiv 5 \mod 59$ ricaviamo direttamente
$$D' = \log_{\bar{2}} \bar{5} = 6.$$
(b) Rossi ha risposto a Bianchi inviandogli un messaggio costituito dai seguenti numeri
$$f_2 \cdot f_1^{-D'} = \overline{16} \cdot \overline{12}^{-6} \equiv \overline{17}, \qquad r_2 \cdot r_1^{-D'} = \bar{6} \cdot \overline{12}^{-6} \equiv \overline{58} \qquad \mod 59.$$
(c) Come sopra...In questo caso si trova $\mu = 52 = \log_{\bar{2}} \overline{12}$.