

Per alcuni di questi esercizi è necessario PARI/GP.

1. Sia p primo e siano $\bar{a}$ e $\bar{b}$ radici primitive di $\mathbf{Z}_p^*$. Dimostrare che $\log_{\bar{a}} \bar{b}$ è invertibile modulo $p-1$.
2. Sia $p = 227$.
 - (a) Verificare che $\bar{a} = \bar{2}$ è una radice primitiva in $\mathbf{Z}_p^*$.
 - (b) Calcolare $\log_{\bar{a}} \bar{3}$, $\log_{\bar{a}} \bar{5}$, $\log_{\bar{a}} \bar{7}$, servendosi delle relazioni modulo p

$$2^{20} \equiv 3^2 \cdot 7, \quad 2^{57} \equiv 3 \cdot 5, \quad 2^{128} \equiv 3 \cdot 7^2.$$
 - (c) Calcolare $\log_{\bar{a}} \overline{100}$.
3. Sia $p = 47$. Determinare una radice primitiva $\bar{a} \in \mathbf{Z}_{47}^*$. Calcolare $\log_{\bar{a}} 11$.
4. Sia $p = 439$.
 - (a) Verificare che $\bar{a} = \overline{17}$ è la più piccola radice primitiva in $\mathbf{Z}_p^*$.
 - (b) Calcolare $\log_{\bar{a}} \overline{100}$.
5. Sia $p = 1061$.
 - (a) Determinare una radice primitiva $\bar{a}$ di $\mathbf{Z}_p^*$;
 - (b) Determinare $\log_{\bar{a}} \overline{101}$ con Baby-Step-Giant-Step, oppure con un mini calcolo dell'indice (aiutarsi con il file <http://www.mat.uniroma2.it/geo2/TEN/relazioni.rtf>).
6. Sia $p = 1061$ e sia $E(\mathbf{Z}_p)$ la curva ellittica su $\mathbf{Z}_p$ di equazione $Y^2 = X^3 + X + 582$.
 - (a) Verificare che la curva $E(\mathbf{Z}_p)$ ha ordine primo $\#E(\mathbf{Z}_p) = 1031$, e che i punti $A = [1013, 631]$ e $Q = [489, 315]$ appartengono a $E(\mathbf{Z}_p)$.
 - (b) Calcolare il logaritmo discreto di Q in base A .
7. Siano dati il numero primo $p = 1291799$ e la radice primitiva $\bar{a} = \overline{17}$ in $\mathbf{Z}_p^*$.
 - (a) Criptare il messaggio $m = 100$ col metodo El Gamal e spedirlo al signor Rossi, utente con chiavi pubbliche $(p, \bar{a}, E = 277353)$ e chiave segreta $D = 54865$.
 - (b) Decifrare il messaggio con la chiave segreta di Rossi: verificare che è effettivamente il messaggio originale.
 - (c) Una spia intercetta il messaggio criptato (c_1, c_2) diretto a Rossi e lo cambia in $(c_1, 3c_2)$. Cosa riceve Rossi?
8. Siano dati il numero primo $p = 41022299$ e la radice primitiva $\bar{a} = \bar{2}$ in $\mathbf{Z}_p^*$ ed i tre utenti Bianchi, Rossi e Verdi, con chiavi segrete $m_R = 111$, $m_B = 222$ e $m_V = 333$.
 - (a) Qual è la chiave condivisa dopo il *Diffie-Hellman key exchange* fra Bianche e Rossi?
 - (b) Qual è la chiave condivisa dopo il *Diffie-Hellman key exchange* a tre fra Bianche, Rossi e Verdi?
9. Sia $p = 1291799$. Costruire una curva ellittica $E(\mathbf{Z}_p)$ su $\mathbf{Z}_p$ di ordine primo ed un punto $A = [x, y] \in E(\mathbf{Z}_p)$ (automaticamente un generatore) (aiutarsi con il file <http://www.mat.uniroma2.it/geo2/TEN/ECsearch.rtf>).
10. Trovate molti altri esercizi sul logaritmo discreto (con soluzione) nei testi d'esame degli anni passati.

p primo

a radice primitiva

Supponiamo che a^m modulo p sia B -smooth

$$a^m \equiv p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \pmod{p}$$

con p_i primi della factor base. La relazione corrispondente è

$$m \log a \equiv \alpha_1 \log p_1 + \dots + \alpha_k \log p_k \pmod{p-1}.$$

Condideriamo adesso a^{mn} modulo p :

$$a^{mn} \equiv (p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k})^n \pmod{p}$$

e passando alla relazione corrispondente

$$nm \log a \equiv n(\alpha_1 \log p_1 + \dots + \alpha_k \log p_k) \pmod{p-1}$$