CR410 - Esercizi (primo foglio)

AA 2014/2015

9 Marzo 2015

1. In ciascuno dei seguenti casi calcolare l'inverso aritmetico di a in due mode: con l'algoritmo esteso di Euclide e con il Piccolo Teorema di Fermat:
   (a) $p = 31 \qquad a = 7;$
   (b) $p = 101 \qquad a = 90;$
   (c) $p = 103 \qquad a = 56.$
2. Effettuare una simulazione di ciascuno dei tre crittosistemi seguenti con primi di tre cifre decimali.
   (a) Scambio Chiavi Diffie Hellman
   (b) Crittosistema Massey Omura
   (c) Crittosistema ElGamal
3. Trovare tutte le radici primitive in $\mathbf{F}_{11}^*$, $\mathbf{F}_{13}^*$, $\mathbf{F}_{19}^*$ e $\mathbf{F}_{23}^*$.
4. Dimostrare che se $p = 2q + 1$ è primo con q primo allora $\mathbf{F}_p^*$ ammette $q - 1$ radici primitive. E' vero anche il contrario (cioè che se $\mathbf{F}_p^*$ ammette esattamente $(p - 3)/2$ radici primitive, allora $p = 2q + 1$ con q primo)?
5. Dimostrare che se $p = 2q + 1$ è primo con q primo e se $g \in \mathbf{F}_p^*$ è tale che $g \not\equiv \pm 1 \bmod p$ e $g^q \not\equiv 1 \bmod p$, allora g è una radice primitiva modulo p.
6. Sia G un gruppo ciclico e sia $|G| = q_1^{\alpha_1} \cdots p_s^{\alpha_s}$ la fattorizzazione unica. Dimostrare che $g \in G$ è una radice primitiva (i.e. un generatore) se e solo se $g^{|G|/q_j} \neq 1$ per ogni $j = 1, \ldots, s$.