Teoria elementare dei numeri. 4. Logaritmo discreto; gruppi abeliani. Roma, 10 novembre 2005.

1. Calcolare una radice primitiva g modulo 61. Calcolare i logaritmi discreti (rispetto alla radice primitiva g) $\log(2)$, $\log(47)$ e $\log(-1)$.

2. Dimostrare: per ogni primo p e ogni radice primitiva g modulo p, il logaritmo discreto di $\overline{-1} \in \mathbf{Z}_p^*$ è uguale a $(p-1)/2$.

3. Sia p un primo e sia g una radice primitiva modulo p. Dimostrare: per ogni $\overline{x} \in \mathbf{Z}_p^*$ si ha che $\overline{x}$ è quadrato in $\mathbf{Z}_p^*$ se e solo se $\log(x)$ è *pari*.

4. Per i numeri primi 23, 191, 8761, 44000003, 280000000572000000077, calcolare una radice primitiva.

5. Sia p un numero primo. Sia g una radice primitiva modulo p e sia $\log_g$ il logaritmo discreto rispetto a g (cioè se $x \in \mathbf{Z}_p^*$ è uguale a g^i, allora $\log_g(x) = i$). Sia g' una seconda radice primitiva e sia $\log_{g'}$ il logaritmo discreto rispetto a g'. Far vedere che esiste $c \in \mathbf{Z}$ tale che per ogni $x \in \mathbf{Z}_p^*$ si ha che $\log_{g'}(x) = c \log_g(x)$.

6. Per $m = 2, 4, 6, 8, 10, 12 \ldots$
   (a) determinare
   $$e(m) = \max\{n \in \mathbf{Z}_{>0} : \overline{x}^m = \overline{1} \text{ per ogni } \overline{x} \in \mathbf{Z}_n^*\};$$
   (Per esempio: $e(2) = 24$, $e(4) = 240$, $e(6) = 504$, ...)
   (b) per $n = e(m)$, scrivere $\mathbf{Z}_n^*$ come prodotto di gruppi ciclici (a meno di isomorfismo).

7. Scrivere i seguenti gruppi come prodotto di gruppi ciclici (a meno di isomorfismo): $\mathbf{Z}_{24}^*$, $\mathbf{Z}_{30}^*$, $\mathbf{Z}_{10001}^*$, $\mathbf{Z}_{25}^*$.

8. Dimostrare che non esiste nessun $n \in \mathbf{Z}_{>0}$ tale che $\mathbf{Z}_n^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

9. Sia p un numero primo e sia p^k una potenza di p.
   (a) Se $p \neq 2$, dimostrare che $\mathbf{Z}_{p^k}^*$ è un gruppo ciclico.
   (b) Dimostrare che per $k \geq 2$ si ha che $\mathbf{Z}_{2^k}^* \cong \mathbf{Z}_2 \times \mathbf{Z}_{\,2^{k-2}}$.

10. Sia G un gruppo commutativo finito. Dimostrare che le seguenti affermazioni sono equivalenti:
    (1) $G \cong \mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_t}$;
    (2) esistono elementi $x_1, \ldots, x_t \in G$ rispettivamente di ordine $n_1, \ldots, n_t$ che hanno la seguente proprietà: per ogni $g \in G$ esistono unici esponenti interi $i_1, \ldots, i_t$ con $0 \leq i_1 < n_1$, ..., $0 \leq i_t < n_t$ tali che
    $$x = x_1^{i_1} \cdot \ldots \cdot x_t^{n_t}.$$

11. (a) Dimostrare che $\mathbf{Z}_{60}^* \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.
    (b) Esibire elementi $x_1, x_2, x_3 \in \mathbf{Z}_{60}^*$ di ordine 4, 2, 2 rispettivamente, che hanno le proprietà degli elementi dell'esercizio 10 (2) con $G = \mathbf{Z}_{60}^*$.

12. Sia G un gruppo commutativo finito.
    (a) Sia $g \in G$. Dimostrare che $\mathrm{ord}(g)$ divide $\#G$.
    (b) Sia $H \subset G$ sottogruppo. Dimostrare che $\#H$ divide $\#G$.

13. (Cauchy) Sia G un gruppo commutativo finito a sia p un divisore primo di $\#G$. Dimostrare che esiste $g \in G$ di ordine p.