TEN 2018. Esercizi 5.

Alcuni di questi esercizi richiedono PARI/GP. Alcuni verranno discussi venerdi' 11 gennaio 2019.

1. Siano dati $x = 2222574487$ e $y = 46375$. Determinare gli ordini di $\bar{x}$ e $\bar{y}$ nei gruppi $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_7, +)$, $(\mathbb{Z}_{11}, +)$.

2.(a) Verificare che $\varphi(n)$ è pari, per ogni intero $n > 2$.
(b) Verifcare che se $p|n$, allora $\varphi(p)|\varphi(n)$.

3. Determinare tutti i generatori di $(\mathbb{Z}_{686}, +)$.

4.(a) Calcolare $\varphi(616)$;
(b) Scrivere $\mathbb{Z}_{616}^*$ come prodotto di gruppi ciclici.

5.(a) Scrivere $\mathbb{Z}_{120}^*$ come prodotto di gruppi ciclici.
(b) Scrivere $\mathbb{Z}_{10!}^*$ come prodotto di gruppi ciclici (ricordare che $\mathbb{Z}_p^*$ è ciclico, per ogni p primo; $\mathbb{Z}_{p^k}^*$ è ciclico, per ogni primo $p > 2$).

6.(a) Sia p un primo, $p \equiv 3 \bmod 4$, e sia a un quadrato in $\mathbb{Z}_p^*$. Mostrare che le radici quadrate di a sono $\pm a^{(p+1)/4}$;
(b) Sia p un primo, $p \equiv 5 \bmod 8$, e sia a un quadrato in $\mathbb{Z}_p^*$. Mostrare che $a^{(p-1)/4} = \pm 1$.

7. Sia $p = 976909$ primo e sia $x = 755017$.
   (a) Determinare se x è un quadrato modulo p.
   (b) Determinare un quadrato modulo p (ricordare che la meta' delle classi resto di $\mathbb{Z}_p^*$ sono quadrati).

8. Sia $n = 1159 = 19 \cdot 61$.
   (a) Determinare se $x = 1092$ è un quadrato modulo p.
   (b) Mostrare che $x = 5$ è un quadrato modulo n.
   (c) Quante sono le radici quadrate di x?

9. Sia p un primo, $p \equiv 3 \bmod 4$, e sia a un quadrato in $\mathbb{Z}_p^*$.
   (a) Mostrare che le radici quadrate di a sono $\pm a^{(p+1)/4}$;