Alcuni esercizi svolti

ESERCIZIO: (es. 3 del secondo foglio)
Se $k = 0$ allora $mcd(a, k) = a$ e x^k e' l'identita' del gruppo, che ha ordine $1 = a/mcd(a, k)$. Ora supponiamo $k \neq 0$. Chiamiamo s l'ordine di $x^k (\mathrm{mod} n)$ in $\mathbb{Z}_n^*$ (si ha $s \geq 1$). Si ha

$$(x^k)^s = 1(\mathrm{mod} n) \Rightarrow x^{ks} = 1(\mathrm{mod} n)$$

quindi $ks \neq 0$ e' un multiplo di dell'ordine di $x(\mathrm{mod} n)$. Allora

$$a|ks \Rightarrow \frac{a}{mcd(a,k)} | \frac{k}{mcd(a,k)} \cdot s.$$

Se b, c, d sono interi non nulli e $b|c \cdot d$ e $mcd(b, c) = 1$ allora $b|d$. Applicando questo fatto troviamo che $\frac{a}{mcd(a,k)}|s$. Possiamo dimostrare $s|\frac{a}{mcd(a,k)}$ mostrando che $(x^k)^{\frac{a}{mcd(a,k)}} = 1(\mathrm{mod} n)$. Ma

$$(x^k)^{\frac{a}{mcd(a,k)}} = x^{k\frac{a}{mcd(a,k)}} = 1(\mathrm{mod} n)$$

dato che $k\frac{a}{mcd(a,k)}$ e' un multiplo di a.

ESERCIZIO: *In un gruppo ciclico di ordine n ci sono esattamente $\phi(d)$ elementi di ordine d per ogni d divisore di n.*
E' facile vedere che se x e' un generatore del gruppo allora (cfr. esercizio 3) $x^{n/d}$ genera un sottogruppo di ordine d. Ma (cfr. esercizio 3) $x^{n/d \cdot t}$ ha ordine d per ogni $1 \leq t < d$ coprimo con d (questi elementi sono chiaramente distinti). Quindi per ogni d che divide n ci sono almeno $\phi(d)$ elementi di ordine d. Che ci sono alpiu' $\phi(d)$ elementi di ordine d segue da un ragionamento globale: basta infatti utilizzare la formula $\sum_{d|n} \phi(d) = n$.

ESERCIZIO: (es. 1 del secondo foglio)
Il gruppo $\mathbb{Z}_{13}^*$ e' generato dalla classe di 2 perche' moltiplicando $2(\mathrm{mod} 13)$ con se stesso otteniamo le classi di $2, 4, -5, 3, 6, -1, -2, -4, 5, -3, -6, 1$. Quindi l'ordine della classe di 2 e' 12 e per calcolare gli ordini degli altri elementi possiamo usare l'esercizio 3 del secondo foglio.
Il gruppo Z_{13} ha la classe di 0 che ha ordine 1. Gli altri elementi essendo coprimi con 13 hanno ordine 13.

ESERCIZIO: (es. 4 del secondo foglio)
Ricordiamo alcuni fatti di teoria:

- L'ordine di un elemento di un gruppo divide l'ordine del gruppo.
- In un prodotto di gruppi abeliani finiti l'ordine di un elemento e' il minimo comune multiplo degli ordini delle coordinate.
- Sia dato un gruppo ciclico di ordine n. Allora per ogni d divisore di n tale gruppo contiene uno e uno solo sottogruppo di ordine d (inoltre esso risulta ciclico e contiene tutti gli elementi di ordine d).
- Sia $a \geq 1$ e p un numero primo dispari. Allora il gruppo $\mathbb{Z}_{p^a}^*$ e' isomorfo al prodotto $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{a-1}}$ ed in particolare e' ciclico (nota: il prodotto di due gruppi ciclici con ordini coprimi tra loro e' ciclico).
- Se a e b sono coprimi allora $\mathbb{Z}_{ab}^*$ e' isomorfo al prodotto $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ e un isomorfismo si ottiene mandando $x(\mathrm{mod} ab)$ nell'elemento $(x(\mathrm{mod} a), x(\mathrm{mod} b))$ per ogni intero $0 \leq x < ab$.

Chiaramente H e' chiuso rispetto all'operazione (che e' la moltiplicazione delle classi di congruenza), contiene l'identita' $(1(\mathrm{mod}n))$ e contiene gli inversi (moltiplicativi) dei suoi elementi quindi H e' un sottogruppo. Notare che H sono gli elementi di $\mathbb{Z}_n^*$ con ordine che divide 2. Sappiamo che $\mathbb{Z}_n^*$ e' isomorfo al prodotto dei gruppi $\mathbb{Z}_{p^{a_p}}^*$ dove p varia tra i d divisori primi di n e dove $\prod p^{a_p} = n$. Basta vedere che ciascuno di questi gruppi contiene esattamente un elemento di ordine 2. Infatti gli elementi di ordine che divide 2 in un prodotto di gruppi abeliani finiti sono gli elementi le cui coordinate hanno ciascuna ordine che divide 2. Allora per ogni coordinata possiamo allora prendere o l'elemento di ordine 2 oppure l'identita' (che e' l'unico elemento di ordine 1) e quindi abbiamo ottenuto 2^d elementi.
Per ipotesi n e' dispari quindi per ogni primo p che divide n si ha $p \neq 2$. Allora per ogni p primo che divide n il gruppo $\mathbb{Z}_{p^{a_p}}^*$ e' isomorfo al prodotto $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{a_p-1}}$ che e' il prodotto di un gruppo ciclico di ordine pari e di un gruppo ciclico di ordine dispari. Il primo (essendo ciclico e dato che 2 divide l'ordine del gruppo) contiene uno e uno solo sottogruppo di ordine 2 (che inoltre contiene tutti gli elementi di ordine 2) e quindi deduciamo che contiene un solo elmento di ordine 2. Il secondo non contiene elementi di ordine 2 dato che l'ordine di un elemento divide l'ordine del gruppo (che in questo caso e' un numero dispari). Allora esiste un unico elemento di ordine 2 in $\mathbb{Z}_{p^{a_p}}^*$ dato che esso deve avere come coordinate l'elemento di ordine 2 di $\mathbb{Z}_{p-1}$ e l'identita' (cioe' l'elemento di ordine 1) di $\mathbb{Z}_{p^{a_p-1}}$.
Sia adesso $n = 91 = 7 \cdot 13$. Sappiamo che H ha ordine 4. Un elemento e' l'identita' (l'elemento di ordine 1) gli altri 3 elementi hanno ordine 2. Si ha $\mathbb{Z}_7^* = \mathbb{Z}_6$ e $\mathbb{Z}_{13}^* = \mathbb{Z}_{12}$. L'elemento di ordine 2 di $\mathbb{Z}_7^*$ e' la classe di -1 (sapendo l'unicita' basta verificare che la classe di -1 ha ordine 2). L'elemento di ordine 2 di $\mathbb{Z}_{13}^*$ e' la classe di -1 (sapendo l'unicita' basta verificare che la classe di -1 ha ordine 2). I quattro elementi cercati sono le soluzioni delle seguenti congruenze:

$$x = (-1)(\mathrm{mod}7), x = (-1)(\mathrm{mod}13);$$

$$x = (1)(\mathrm{mod}7), x = (-1)(\mathrm{mod}13);$$

$$x = (-1)(\mathrm{mod}7), x = (1)(\mathrm{mod}13);$$

$$x = (1)(\mathrm{mod}7), x = (1)(\mathrm{mod}13).$$

Tali soluzioni sono $x = (-1)(\mathrm{mod}91)$, $x = (-27)(\mathrm{mod}91)$,$x = (27)(\mathrm{mod}91)$ $x = (1)(\mathrm{mod}91)$.