TEN 2008. Gruppi abeliani finiti.

In questa nota richiamiamo alcuni fatti sui gruppi abeliani finiti. Questi fatti possone essere applicati al gruppo $\mathbb{Z}_n^*$ delle classi resto modulo n che ammettono inverso moltiplicativo, come al gruppo dei punti di una curva ellittica su un campo finito $\mathbb{Z}_p$, con p primo.

Definizione. Sia G un gruppo abeliano finito di ordine n. Si dice che G è ciclico se esiste un elemento $g \in G$ tale che

$$G = \{g,\ g^2, \ldots, g^{n-1},\ g^n = e\}.$$

L'elemento g si dice *generatore* di G. Ha ordine n e le sue potenze esauriscono tutto G.

Esempio 1. Per ogni intero positivo n, il gruppo additivo $(\ \mathbb{Z}_n, +)$ è un gruppo ciclico di ordine n. Infatti

$$\mathbb{Z}_n = \{\bar{1},\ \bar{2},\ \ldots,\ \overline{n-1},\ \bar{n} = \bar{0}\}.$$

Poiché vale $a \cdot \bar{1} = \bar{a}$, la classe $\bar{1}$ è un generatore del gruppo. Notare che in questo caso, dove l'operazione è la somma, le potenze corrispondono ai multipli del generatore.

Esempio 2. Sia $G = \mathbb{Z}_m \times \mathbb{Z}_n$, con $\gcd(m, n) = 1$. Il gruppo $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico.

Esempio 3. Sia $G = \mathbb{Z}_m \times \mathbb{Z}_n$, con $\gcd(m, n) \neq 1$. Sia $(\bar{x}, \bar{y})$, con $\bar{x} \in \mathbb{Z}_m$ e $\bar{y} \in \mathbb{Z}_n$, un elemento qualunque di $\mathbb{Z}_m \times \mathbb{Z}_n$. Allora l'ordine di $(\bar{x}, \bar{y})$ divide il minimo comune multiplo $\mathrm{mcm}(m, n)$. In particolare tale ordine è minore di mn ed il gruppo $\mathbb{Z}_m \times \mathbb{Z}_n$ non è ciclico.

Esempio 4. Per ogni intero positivo n, il gruppo moltiplicativo $(\ \mathbb{Z}_n^*, \cdot)$ è un gruppo abeliano finito di ordine $\varphi(n)$. Se n è primo, allora $\mathbb{Z}_n^*$ è ciclico. In generale, per n arbitrario il gruppo $\mathbb{Z}_n^*$ non è ciclico.

Teorema. *Sia G un gruppo abeliano finito di ordine $n = p_1^{k_1} p_2^{k_2} \dots p_\alpha^{k_\alpha}$, dove i p_i sono primi distinti e i k_i sono interi positivi. Allora G è isomorfo al prodotto diretto*

$$G \cong G_1 \times G_2 \times \ldots \times G_\alpha,$$

dove G_i è un gruppo abeliano di ordine $p_i^{k_i}$.

Fatto 1. Sia G un gruppo di ordine p primo. Allora G è un gruppo ciclico ed è isomorfo a $\mathbb{Z}_p$.

Fatto 2. Sia G un gruppo il cui ordine è il prodotto di primi distinti $n = p_1 \cdot p_2 \cdot \ldots \cdot p_\alpha$. Allora G è un gruppo ciclico ed è isomorfo a

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_\alpha} \cong \mathbb{Z}_{p_1 p_2 \ldots p_\alpha}$$

(il secondo isomorfismo segue dal Teorema Cinese del Resto).

Fatto 3. Sia G un gruppo il cui ordine è potenza di un primo $n = p^k$. In questo caso G non è necessariamente ciclico. Per G ci sono infatti tutte le seguenti possibilità:

$$G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \ldots \times \mathbb{Z}_{p^{a_m}}, \qquad a_1 + a_2 + \ldots + a_m = k.$$

Ad esempio, ci sono:

$\mathbb{Z}_{p^k}$;

$\mathbb{Z}_p \times \mathbb{Z}_{p^{k-1}}, \quad \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^{k-2}}, \quad \ldots \quad \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^{k-a}}$;

$\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^{k-3}}, \ \ldots$;

Solo nel primo caso G è ciclico. Negli altri casi G non è ciclico.
In un caso concreto, ragionando sull'ordine degli elementi di G possiamo tentare di determinare quale fra queste possibilità si verifica.

Esempio 1. Sia p un numero primo e sia $G = \mathbb{Z}_p^*$. Il Teorema della Radice Primitiva ci dice che il gruppo $G = \mathbb{Z}_p^*$ è ciclico.
Notare che il gruppo G ha ordine $\varphi(p) = p - 1$, che non è primo; quindi il fatto che G sia ciclico è tutt'altro che scontato.

Esempio 2. Sia p un numero primo e sia $G = \mathbb{Z}_{p^k}^*$. Il gruppo $G = \mathbb{Z}_{p^k}^*$ è ciclico per ogni $p \neq 2$ (vedi Nota sulla radice primitiva).

Per $p = 2$, si hanno le seguenti possibilità:
$\mathbb{Z}_2^* = \{\bar{1}\}$ è ciclico;
$\mathbb{Z}_{2^2}^* = \mathbb{Z}_4^* = \{\bar{1}, \overline{-1}\}$ è ciclico;
$\mathbb{Z}_{2^3}^* = \mathbb{Z}_8^* = \{\bar{1}, \ \bar{3}, \ \bar{5}, \ \bar{7}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico (tutti gli elementi hanno ordine 2);
$\mathbb{Z}_{2^k}^*$ è un gruppo di ordine 2^{k-1} isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. In particolare non è ciclico.

Esempio 3. Siano p e q primi distinti e sia $G = \mathbb{Z}_{pq}^*$.
Il gruppo G ha ordine $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Il Teorema Cinese del Resto ci dice che $\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Dunque G è prodotto di due gruppi ciclici. Si ha che G stesso è ciclico se e solo se

$$\gcd(p-1, q-1) = 1 \quad \Leftrightarrow \quad p = 2 \text{ oppure } q = 2.$$

Notare che per $p, q > 2$, si ha che $p - 1$ e $q - 1$ sono entrambi pari...