SOLUZIONI DEL COMPITO DI ARITMETICA
7 luglio 2014

Esercizio 1.
Sia $X = \{1, 2, \dots, 100\}$. Calcolare la cardinalità dei seguenti insiemi:

a) $\big\{(A, B) \in \mathcal{P}(X)^2 \big|\ |A \cup B| = 40 \text{ e } |A| = 10\big\}$;

b) $\big\{A \in \mathcal{P}(X) \big|\ |A| = 5 \text{ e } \prod_{x\in A} x \equiv 0 \pmod 9\big\}$

Soluzione: (a) Possiamo costruire le coppie (A, B) cercate scegliendo i 40 elementi di $A \cup B$ ($\binom{100}{40}$ scelte), scegliendo poi tra questi i 10 elementi che formano A (e questo si può fare in $\binom{40}{10}$ modi), infine scegliendo il sottoinsieme di A che rappresenta l'intersezione con B (per questo abbiamo 2^{10} scelte). Ne segue che la cardinalità cercata è $\binom{100}{40}\binom{40}{10}2^{10}$.
(b) Chiamiamo Γ l'insieme di cui cerchiamo la cardinalità, e poniamo $\Sigma = \big\{A \in \mathcal{P}(X) \big|\ |A| = 5 \text{ e } \prod_{x\in A} x \not\equiv 0 \pmod 9\big\}$.
Allora $\#\Gamma = \binom{100}{5} - \#\Sigma$. Per calcolare la cardinalità di Σ consideriamone la partizione data da:
$\Sigma_3 = \big\{A \in \mathcal{P}(X) \big|\ |A| = 5 \text{ e } \prod_{x\in A} x \not\equiv 0 \pmod 3\big\}$ e
$\Sigma_9 = \big\{A \in \mathcal{P}(X) \big|\ |A| = 5 \text{ e } \prod_{x\in A} x \equiv 0 \pmod 3 \text{ e } \prod_{x\in A} x \not\equiv 0 \pmod 9\big\}$.
Ora $\#\Sigma_3 = \binom{100-33}{5}$ (scelgo i 5 elementi di A tra i 100-33 elementi non divisibili per 3) e $\#\Sigma_9 = \binom{100-33}{4}\cdot 22$ in quanto si tratta di scegliere 4 elementi non divisibili per 3 e il quinto divisibile per 3 e non per 9 (per questo le scelte sonno tra i 33 elementi multipli di 3 meno gli 11 che sono multipli di 9). Otteniamo quindi che:

$$\#\Gamma = \binom{100}{5} - \binom{100-33}{5} - \binom{100-33}{4}\cdot 22.$$

Esercizio 2.
Determinare i valori del parametro intero a per cui il seguente sistema di congruenze ha soluzione:

$$\begin{cases} 2^x \equiv 3^{x+a^2} \pmod{17} \\ 3x \equiv a^{23} \pmod{24} \end{cases}$$

SOLUZIONE: Risolviamo la prima congruenza: si calcola che $\text{ord}(2) = 8$, $\text{ord}(3) = 16$ e $2 = 3^{14}$, da cui si ottiene $3^{14x} = 3^{x+a^2} \pmod{17}$ che è equivalente a $14x \equiv x + a^2 \pmod{16}$. Risolvendo si ottiene $x \equiv 5a^2 \pmod{16}$.
La congruenza $3x \equiv a^{23} \pmod{24}$ ha soluzione se e solo se $3 = (3, 24)|a^{23}$ cioè se e solo se $a \equiv 0 \pmod{3}$. In tal caso il sistema diventa:

$$\begin{cases} x \equiv 5a^2 \pmod{16} \\ 3x \equiv a^{23} \pmod{3} \\ 3x \equiv a^{23} \pmod{8} \end{cases}$$

poiché la seconda equazione è sempre verificata, e la terza puo' essere risolta come $x \equiv 3a^{23} \pmod{8}$, il sistema è risolubile se e solo se $8 = (16, 8)|5a^2 - 3a^{23}$, cioè se $5a^2 - 3a^{23} \equiv 0 \pmod{8}$.
Ora $a^2(5 - 3a^{21}) \equiv 0 \pmod{8} \iff a^2 \equiv 0 \pmod{8}$ oppure $5 - 3a^{21} \equiv 0 \pmod{8}$ in quanto se dei due fattori se uno è pari l'altro è dispari. Risolvendo si ha:
- $a^2 \equiv 0 \pmod{8} \iff a \equiv 4 \pmod{4}$;
- $5 - 3a^{21} \equiv 0 \pmod{8} \iff a^{21} \equiv -1 \pmod{8} \iff a \equiv -1 \pmod{8}$ dove abbiamo usato che a è dispari quindi $a^2 \equiv 1 \pmod{8}$.
Mettendo insieme le condizioni trovate si ha che il sistema è risolubile se e solo se:

$$\begin{cases} a \equiv 0 \pmod{3} \\ a \equiv 0 \pmod{4} \end{cases} \quad \text{oppure} \quad \begin{cases} a \equiv 0 \pmod{3} \\ a \equiv -1 \pmod{8} \end{cases}$$

e risolvendo si calcola che il sistema è risolubile se $a \equiv 0, 12, 15 \pmod{24}$, mentre non è risolubile per le altre classi modulo 24.

Esercizio 3.
Sia G un gruppo abeliano e sia H il suo sottoinsieme formato da tutti gli elementi di ordine finito.
a) Dimostrare che H è un sottogruppo di G e mostrare con un esempio che H può essere infinito.
b) Dimostrare che G/H è isomorfo a G se e solo se H è banale.

SOLUZIONE: (a) Vediamo che H è un sottogruppo di G:
- $e \in H$ in quanto l'identità del gruppo ha sempre ordine 1.
- siano $a, b \in H$, e sia $\text{ord}(a) = m$, $\text{ord}(b) = n$. Allora $(ab)^{mn} = a^{mn}b^{mn} = e$, quindi ab ha ordine finito e appartiene ad H;
- se $a \in H$ anche $a^{-1} \in H$ perché $\text{ord}(a) = \text{ord}(a^{-1})$.

Sia $G = \mathbb{C}^*$ allora $H = \{z \in \mathbb{C}^* \mid z^n = 1 \text{ per qualche } n\}$. Poiché per ogni $n \in \mathbb{N}$ il polinomio $x^n - 1$ ha n radici in $\mathbb{C}$ e queste appartengono ad H, si ha che $|H| \geq n$ per ogni $n \in \mathbb{N}$, quindi H è infinito.
(b) Chiaramente se H è banale $G/H \cong G$. Sia ora $\phi : G \to G/H$, un omomorfismo di gruppi. Sia $g \in G$ con $\text{ord}(g) = n$, allora posto $\phi(g) = xH$ si ha $x^nH = (\phi(g))^n = \phi(g^n) = \phi(e) = H$ cioè $x^n \in H$. Questo assicura che x^n ha ordine finito: se chiamiamo d tale ordine, ne segue che anche x ha ordine finito in quanto $x^{nd} = e$. Allora $x \in H$, cioè per ogni omomorfismo $\phi : G \to G/H$ si ha che $H \subseteq Ker\phi$, quindi ϕ può essere iniettivo solo se H è banale.

Esercizio 4.
Sia p un primo dispari, e sia $f(x) = x^6 + ax^3 + b \in \mathbb{F}_p[x]$.
a) Dimostrare che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$ può essere solo 1 o 3.
b) Dimostrare che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ non può essere ne' 4 ne' 5.
c) Mostrare che se $p \equiv 2 \pmod 3$ il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ non può essere 3.

Soluzione: (a) Siano $\Delta = a - 4b^2$, $\alpha = \frac{-a+\sqrt{\Delta}}{2}$ e $\beta = \frac{-a-\sqrt{\Delta}}{2}$. Si ha $\mathbb{F}_p(\sqrt{\Delta}) \subseteq \mathbb{F}_{p^2}$ e quindi $f(x) = (x^3 - \alpha)(x^3 - \beta)$ in $\mathbb{F}_{p^2}[x]$. Ora osserviamo che ogni binomio del tipo $x^3 - \gamma$ di $\mathbb{F}_{p^2}[x]$ è irriducibile o è prodotto di tre fattori di grado 1. Infatti, se $p = 3$ si ha $x^3 - \gamma = (x - \gamma^3)^3$; se invece $p > 3$ si ha $3|p^2 - 1$ quindi l'omomorfismo di $\mathbb{F}_{p^2}^*$ in se', definito da $z \mapsto z^3$, è una funzione 3 a 1, quindi gli elementi che sono cubi hanno 3 radici cubiche in $\mathbb{F}_{p^2}$. Possiamo quindi concludere che il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$ è 1 se sia α che β sono cubi, altrimenti è 3.
(b) Sia $\mathbb{F}_{p^k}$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$. Da quanto dimostrato al punto (a) segue che il campo di spezzamento di $f(x)$ su $\mathbb{F}_{p^2}$, e quindi anche quello su $\mathbb{F}_p$, è contenuto in $\mathbb{F}_{p^6}$. La relazione $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^6}$ implica $k|6$. In particolare $k \neq 4, 5$.
(c) Come prima sia $\mathbb{F}_{p^k}$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$. Al punto (a) abbiamo visto che $\mathbb{F}_p(\sqrt{\Delta}) \subseteq \mathbb{F}_{p^k}$, quindi se fosse $k = 3$ si avrebbe $\sqrt{\Delta} \in \mathbb{F}_p$, e $f(x) = (x^3 - \alpha)(x^3 - \beta)$ in $\mathbb{F}_p[x]$. Per $p \equiv 2 \pmod 3$, l'applicazione $z \mapsto z^3$ è un isomorfismo di $\mathbb{F}_p^*$, quindi sia $x^3 - \alpha$ che $x^3 - \beta$ sono prodotto di un fattore lineare e di uno irriducibile di grado 2, quindi in questo caso il campo di spezzamento non può avere grado 3.