SOLUZIONI DEL COMPITO DI ARITMETICA

12 giugno 2014

Esercizio 1.
Sia P l'insieme delle parole di lunghezza 3 che si possono scrivere con 26 lettere. Contare le coppie ordinate (α, β) con $\alpha, \beta \in P$ tali che α, β non hanno lettere in comune.

SOLUZIONE: Per contare le coppie (α, β) che verificano le condizioni richieste distinguiamo 3 casi.
- α si scrive con una sola lettera: le parole α di questo tipo sono 26 (una per ogni lettera dell'alfabeto) e in questo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 25 lettere rimanenti, quindi per β ci sono 25^3 possibili scelte.
- α si scrive con due lettere: le parole α di questo tipo sono $\binom{26}{2} \cdot 2 \cdot \frac{3!}{2!}$ (i modi per scegliere 2 lettere dell'alfabeto moltiplicati per il numero di parole di lunghezza 3 che si possono scrivere con 2 lettere) e in questo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 24 lettere rimanenti, quindi per β ci sono 24^3 possibili scelte.
- α si scrive con 3 lettere distinte: le parole α di questo tipo sono $\binom{26}{3} \cdot 3!$ (i modi per scegliere 3 lettere dell'alfabeto moltiplicati per il numero di permutazioni di 3 lettere) e in questo caso β sarà una qualsiasi parola di lunghezza 3 che si può scrivere con le 23 lettere rimanenti, quindi per β ci sono 23^3 possibili scelte.

In totale la cardinalità dell'insieme cercato è:

$$26 \cdot 25^3 + \binom{26}{2} \cdot 2 \cdot \frac{3!}{2!} \cdot 24^3 + \binom{26}{3} \cdot 3! \cdot 23^3.$$

Esercizio 2.
Contare le soluzioni modulo 2^{10} della seguente congruenza:

$$x^5 - 16x \equiv 0 \pmod{2^{10}}.$$

SOLUZIONE: Osservando l'equazione si vede che ogni soluzione x deve essere pari. Sia quindi $x = 2y$. Sostituendo abbiamo

$$2^5 y^5 - 2^5 y \equiv 2^5 y(y^4 - 1) \equiv 0 \pmod{2^{10}},$$

da cui otteniamo $y(y^4 - 1) \equiv 0 \pmod{2^5}$. Osserviamo che uno solo tra y e $y^4 - 1$ è pari, quindi si ha $y \equiv 0 \pmod{2^5}$, oppure $y^4 - 1 \equiv 0 \pmod{2^5}$.
La congruenza $y \equiv 0 \pmod{2^5}$ dà le soluzioni $x \equiv 0 \pmod{2^6}$ che costituiscono 2^4 classi modulo 2^{10}.

Consideriamo la congruenza $y^4 - 1 \equiv 0 \pmod{2^5}$. Fattorizzando si ha

$$y^4 - 1 \equiv (y-1)(y+1)(y^2+1) \equiv 0 \pmod{2^5}.$$

Chairamente in questo caso y, quindi è dispari i fattori $y-1$, $y+1$ e y^2+1 sono sono tutti e tre pari. Però è immediato vedere che $y^2+1 \equiv 2 \pmod 4$ cioè y^2+1 è divisibile per 2 ma non per 4 quindi l'equazione è equivalente a

$$(y-1)(y+1) \equiv 0 \pmod{2^4}.$$

Ora, essendo $y-1$ e $y+1$ due numeri pari consecutivi uno sarà divisibile esattamente per 2 quindi le soluzioni sono $y \equiv 1 \pmod{2^3}$ e $y \equiv -1 \pmod{2^3}$. Questo caso dà le soluzioni $x = 2y \equiv \pm 2 \pmod{2^4}$ quindi questo caso dà $2 \cdot 2^6 = 2^7$ soluzioni modulo 2^{10}.
La congruenza assegnata haquindi $2^4 + 2^7 = 144$ soluzioni modulo 2^{10}.

Esercizio 3.
Siano m e n interi positivi e sia d il loro massimo comune divisore. Indichiamo con il gruppo degli omomorfismi da $\mathbb{Z}/m\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ con l'operazione di somma.
a) Dimostrare che $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.
b) Determinare il sottogruppo di ordine 12 di $\mathrm{Hom}(\mathbb{Z}/360\mathbb{Z}, \mathbb{Z}/420\mathbb{Z})$.

Soluzione: a) Dalla teoria svolta sappiamo che, poiché $\mathbb{Z}/m\mathbb{Z}$ è ciclico ed è generato da $\bar{1}$, un omomorfismo $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ è completamente definito una volta assegnato il valore di $\varphi(\bar{1}) = \bar{a}$ con la condizione che $\mathrm{ord}(\bar{a})|m$ (questo assegnamento definisce l'omomorfismo $\bar{k} \mapsto \varphi(\bar{k}) = k\bar{a}$). Dato che $a \in \mathbb{Z}/n\mathbb{Z}$ la condizione $\mathrm{ord}(\bar{a})|m$ è equivalente alla condizione $\mathrm{ord}(\bar{a})|(m,n) = d$. Gli omomorfismi cerati sono quindi tanti quanti gli elementi di $\mathbb{Z}/n\mathbb{Z}$ il cui ordine divide d (quindi sono d) e sono definiti da $\varphi(\bar{k}) = k\bar{a}$ con $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ e $\mathrm{ord}(a)|d$.
Da quanto detto segue che la funzione $\Phi : \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ definita da $\Phi(\varphi) = \varphi(\bar{1})$ ha come immagine il sottogruppo di ordine d di $\mathbb{Z}/n\mathbb{Z}$. Per avere la tesi basta mostrare che è un omomorfismo iniettivo. È immediato vedere che è un omomorfismo, infatti $\forall \varphi_1, \varphi_2, \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ si ha $\Phi(\varphi_1 + \varphi_2) = (\varphi_1 + \varphi_2)(\bar{1}) = \varphi_1(\bar{1}) + \varphi_2(\bar{1}) = \Phi(\varphi_1) + \Phi(\varphi_2)$. Per l'iniettività basta osservare che $\Phi(\varphi) = \bar{0}$ se e solo se $\varphi(\bar{1}) = \bar{0}$ e quindi se e solo se $\varphi(\bar{k}) = k\bar{0} = \bar{0}$, cioè φ è l'omomorfismo nullo.

b) Per il punto (a) esiste un solo sottogruppo di ordine 12 (in quanto $12|(360, 420) = 60$) ed è quello che, con l'isomorfismo dato, corrisponde al sottogruppo di ordine 12 di $\mathbb{Z}/420\mathbb{Z}$, cioè a $\langle \overline{35} \rangle$. Il sottogruppo richiesto è quindi costituito dagli omomorfismi $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ definiti da $\varphi(\bar{1}) = \bar{a}$ con $a \equiv 0 \pmod{35}$.

Esercizio 4.
Siano p un primo, $a \in \mathbb{F}_p^*$ e $f(x) = (x^4 - a)(x^4 + a) \in \mathbb{F}_p[x]$.

a) Dimostrare che se $p \equiv 3 \pmod 4$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ ha grado 2.
b) Mostrare che si possono scegliere a e p con $p \equiv 1 \pmod 4$ tali che il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ abbia grado 1,2 o 4.

SOLUZIONE: a) Sia $\alpha \in \bar{\mathbb{F}}_p$ una radice di $f(x)$, allora $\alpha^4 = \pm a \in \mathbb{F}_p^*$, quindi $\text{ord}(\alpha)|4(p-1)|p^2-1$ (l'ultima relazione segue dall'ipotesi $p \equiv 3 \pmod 4$). Ne segue che ogni radice α di $f(x)$ appartiene a $\mathbb{F}_{p^2}$. Resta quindi da mostrare che $f(x)$ non ha tutte le radici in $\mathbb{F}_p$. Infatti, $x^4 - a$ ha una radice in $\mathbb{F}_p$ se e solo se $a = b^4$ con $b \in \mathbb{F}_p$ in tal caso però $-a$ non è una quarta potenza in $\mathbb{F}_p$ (non è neppure un quadrato) perchè -1 non è un quadrato, in quanto $p \equiv 3 \pmod 4$. Un discorso analogo vale cambiando a con $-a$, quindi il campo di spezzamento cercato è $\mathbb{F}_{p^2}$.

b) Sia $a = 1$, allora $f(x) = x^8 - 1$ e il suo campo di spezzamento su $\mathbb{F}_p$ è $\mathbb{F}_{p^k}$ dove k è l'ordine di p in $(\mathbb{Z}/8\mathbb{Z})^*$. Ne segue che per $p \equiv 1 \pmod 8$ (ad esempio $p = 17$) si ha $k = 1$ e per $p \equiv 5 \pmod 8$ (ad esempio $p = 5$) si ha $k = 2$.
Resta da mostrare che possiamo realizzare un campo di spezzamento di grado 4. Consideriamo $a = 2$ e $p = 5$; si ha $f(x) = (x^4 - 2)(x^4 + 2)$. Poiché ne' 2 ne' -2 sono quadrati modulo 5, non sono neanche quarte potenze e quindi $f(x)$ non ha radici in $\mathbb{F}_5$. Rimane da escudere la possibilità che entrambi i polinomi $x^4 - 2$ e $x^4 + 2$ si fattorizzino come prodotto di due polinomi (irriducibili) di grado 2. Questo può essere mostrato con il calcolo diretto: supponiamo che

$$x^4-2 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd$$

uguagliando i coefficienti si ha

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ ad + bc = 0 \\ bd = 2 \end{cases}$$

e, svolgendo i calcoli, si vede che questo sistema non ha soluzione in $\mathbb{F}_5$.
Un altro modo per vedere l'irriducibilità di $x^4 - 2$ e di $x^4 + 2$ è osservare che se $\alpha \in \mathbb{F}_{5^k}$ è una radice di $f(x)$, allora $\alpha^4 = \pm 2$, quindi $\text{ord}(\alpha^4) = 4$ quindi $\text{ord}(\alpha) = 4r$. Dalla formula $\text{ord}(\alpha^4) = \frac{\text{ord}(\alpha)}{(4,\text{ord}(\alpha))}$ si ottiene $r = 4$, cioè $\text{ord}(\alpha) = 16$. Ne segue che $16|5^k - 1$ e quindi $k = 4$.