SOLUZIONI DEL COMPITO DI ARITMETICA

13 gennaio 2014

Esercizio 1.

a) Contare le stringhe $(a_0, \dots, a_9)$, con $a_i \in \{0, 1, 2, 3, 4\}$ per ogni i, in cui gli a_i pari sono più degli a_i dispari.

b) Determinare la cardinalità dell'insieme

$$\big\{(a_0, \dots, a_9) \in \{0, 1, 2, 3, 4\}^{10} \,\big|\, \sum_{i=0}^{9} (-1)^i a_i \equiv 0 \pmod 6\big\}.$$

SOLUZIONE: (a) Le stringhe che hanno k coordinate pari sono $\binom{10}{k} \cdot 3^k \cdot 2^{10-k}$: infatti le costruisco scegliendo k posti sui 10 possibili e mettendo in questi valori pari (ognuno ha 3 possibilità: 0,2,4), nei rimanenti $10-k$ posti metto valori dispari (ho 2 valori a disposizione: 1,3). Le stringhe cercate sono quelle in cui ci sono 6,7,8,9 oppure 10 coordinate pari e sono quindi:

$$\sum_{k=6}^{10} \binom{10}{k} \cdot 3^k \cdot 2^{10-k} = 3^7 \cdot 2827.$$

(b) Possiamo interpretare le stringhe cercate come le coordinate in base 5 di un numero naturale: $(a_0, \dots, a_9) \to a_0 + a_1 5 + \cdots + a_9 5^9$. Ricordando la dimostrazione del criterio di divisibilità per 11 di un numero scritto in base 10, e osservando che $5 \equiv -1 \pmod 6$, abbiamo che

$$(a_0, \dots, a_9) \in X \iff a_0 + a_1 5 + \cdots + a_9 5^9 \equiv \sum_{i=0}^{9} (-1)^i a_1 \equiv 0 \pmod 6$$

Cioè le stringhe in X sono quelle che sono le coordinate di un multiplo di 6. Le stringhe con 10 coordinate corrispondono ai numeri naturali n con $0 \le n < 5^{10}$ e tra questi i multipli di 6 sono $\lceil \frac{5^{10}}{6} \rceil$.

Osservazione: Il teorema di Eulero garantisce che $5^2 \equiv 1 \pmod 6$, di conseguenza $5^{10} \equiv 1 \pmod 6$. Ne segue che $\lceil \frac{5^{10}}{6} \rceil = \frac{5^{10}-1}{6} + 1 = \frac{(5^5-1)(5^5+1)}{6} + 1 = \frac{(5^5-1)(5+1)(5^4-5^3+5^2-5+1)}{6} + 1 = (5^5-1)(5^4-5^3+5^2-5+1) + 1 = 5^9 - 5^8 + 5^7 - 5^6 + 5^5 - 5^4 + 5^3 - 5^2 + 5$.

Esercizio 2.

Risolvere il seguente sistema di congruenze

$$\begin{cases} x^2 - 4x + 3 \equiv 0 & \pmod{15} \\ 30x \equiv -6 & \pmod{81} \end{cases}$$

SOLUZIONE: Spezziamo la prima congruenza con il teorema cinese e otteniamo

$$\begin{cases} x^2+x+3 & \equiv 0 \pmod 5 \\ x^2-x & \equiv 0 \pmod 3 \\ 30x & \equiv -6 \pmod{81} \end{cases}.$$

Risolviamo ora le singole equazioni:
- $x^2+x+3 \equiv 0 \pmod 5$: poiché 5 è primo applico la formula risolutiva per le equazioni di secondo grado e ottengo $x = 1, 3$.
- $x^2 - x \equiv x(x-1) \equiv 0 \pmod 3$ se e solo se $x \equiv 0, 1 \pmod 3$ (per verifica diretta oppure osservando che 3 è primo e quindi vale il principio di annullamento del prodotto).
- $30x \equiv -6 \pmod{81}$: dividendo per 6 otteniamo $5x \equiv -1 \pmod{27}$ e moltiplicando per 11 che è l'inverso di 5, ricaviamo $x \equiv 16 \pmod{27}$. Il sistema assegnato è equivalente all'unione dei sistemi:

$$\begin{cases} x & \equiv 1, 3 \pmod 5 \\ x & \equiv 0, 1 \pmod 3 \\ x & \equiv 16 \pmod{27} \end{cases}.$$

Per $x \equiv 0 \pmod 3$ il sottosistema dato dalle ultime 2 equazioni, e quindi il sistema, non ha soluzione. Il sottosistema

$$\{x \equiv 1 \pmod 3 x \equiv 16 \pmod{27}$$

ha invece soluzione $x \equiv 16 \pmod{27}$ (infatti $16 \equiv 1 \pmod 3$). Le soluzioni del sistema iniziale sono quindi le due classi modulo $5 \cdot 27 = 135$ che risolvono i due sistemi

$$\{x \equiv 1 \pmod 5 x \equiv 16 \pmod{27} \qquad \{x \equiv 3 \pmod 5 x \equiv 16 \pmod{27}.$$

È semplice verificare che le due soluzioni sono $x \equiv 16 \pmod{135}$ e $x \equiv 43 \pmod{135}$.

Esercizio 3.
Sia G in gruppo, sia p un numero primo e siano H e K due distinti sottogruppi normali di indice p tali che $H \cap K = \{id\}$.
a) Dimostrare che $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
b) Determinare il numero di sottogruppi di G di ordine p.

SOLUZIONE: (a)
Per ipotesi gruppi G/H e G/K hanno ordine p e quindi sono isomorfi a $\mathbb{Z}/p\mathbb{Z}$. Per mostrare la tesi basta provare che $G \cong G/H \times G/K$.
Sia $\varphi : G \to G/H \times G/K$ definita da $g \to (gH, gK)$.
φ è un omomorfismo perché: $\varphi(xy) = (xyH, xyK) = (xHyH, xKyK) = (xH, xK)(yH, yK) = \varphi(x)\varphi(y)$.

φ è iniettivo: infatti $Ker\varphi = \{g \in G \,|\, (gH, gK) = (H, K)\} = H \cap K = \{e\}$.
φ è surgettivo: basta mostrare che $|G| = p^2$. Poiché G si immerge in $G/H \times G/K$ che ha cardinalità p^2, basta escludere che $|G| = p$, e questo è vero perchè G ha due sottogruppi distinti di indice p.
(b) Poiché p è primo, i sottogruppi di ordine p sono tutti ciclici e quindi il loro numero è uguale al numero degli elementi di ordine p di G diviso per $\Phi(p)$.
Poiché gli isomorfismi conservano l'ordine degli elementi, è equivalente contare gli elementi di ordine p in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$: qui ce ne sono $p^2 - 1$ (tutti tranne l'identità). In G ci sono quindi $\frac{p^2-1}{\Phi(p)} = p + 1$ sottogruppi di ordine p.

Esercizio 4.
Sia $f(x) = x^9 - 1$.
a) Dimostrare che $f(x)$ ha un fattore irriducibile di grado 6 su $\mathbb{F}_{11}$.
b) Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ e su $\mathbb{Q}(\zeta_3)$, dove $\zeta_3 \in \mathbb{C}$ è una radice terza primitiva dell'unità.

Soluzione: (a) $f(x) = (x-1)(x^2+x+1)(x^6+x^3+1)$, dobbiamo quindi mostrare che $h(x) = x^6 + x^3 + 1$ è irriducibile su $\mathbb{F}_{11}$.
Il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_{11}$ è $\mathbb{F}_{11^d}$ dove d è l'ordine moltiplicativo di 11 modulo 9: si calcola che $d = 6$. Ne segue che, detto C_9 l'insieme delle radici di $f(x)$ in una fissata chiusura algebrica di $\mathbb{F}_{11}$, si ha $\mathbb{F}_{11}[C_9] = \mathbb{F}_{11^6}$. Sappiamo inoltre che C_9 è un gruppo moltiplicativo finito, e quindi è ciclico; sia $C_9 = \langle\alpha\rangle$, allora $\mathbb{F}_{11^6} = \mathbb{F}_{11}[\alpha]$. Da questo segue che il polinomio minimo di α, che è un divisore di $f(x)$, ha grado 6 e quindi e proprio $h(x)$ che è per questo irriducibile.
(b) $f(x) = (x-1)(x^2+x+1)(x^6+x^3+1)$ e questi fattori sono irriducibili in $\mathbb{Z}[x]$ perché lo sono modulo 11. Per il lemma di Gauss questi fattori sono irriducibili anche in $\mathbb{Q}[x]$. Sia ζ_9 una radice nona primitiva di 1, le radici di $f(x)$ sono quindi $\{\zeta_9^i \,|\, 1 = 0, \ldots, 8\}$. Il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è quindi $\mathbb{Q}(\zeta_9)$ e il suo grado è il grado del polinomio minimo μ di ζ_9 su $\mathbb{Q}$. Sappiamo che $\mu | f$, inoltre $\zeta_9^3 \neq 1$ quindi $\mu(x) | \frac{f(x)}{x^3-1} = x^6 + x^3 + 1$: essendo questo polinomio irriducibile si ha $\mu(x) = x^6 + x^3 + 1$ e quindi il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è 6.
Sia $K = \mathbb{Q}(\zeta_3)$, allora il campo di spezzameto di $f(x)$ su K è $K(\zeta_9) = \mathbb{Q}(\zeta_9)$. Poiché $[K : \mathbb{Q}] = 2$ (il polinomio minimo di ζ_3 su $\mathbb{Q}$ è $x^2 + x + 1$), usando la formula delle torri si ottiene che $[\mathbb{Q}(\zeta_9) : K] = 3$.