SOLUZIONI DEL COMPITO DI ARITMETICA
11 settembre 2014

Cognome e nome: .....

Numero di matricola: .....

Esercizio 1.
Consideriamo un dado a 6 facce, in cui le facce siano numerate da 1 a 6, ed associamo ad un lancio del dado il punteggio corrispondente al valore della faccia. Calcolare la probabilità che, dopo n lanci dello stesso dado, la somma dei punteggi ottenuti sia un multiplo di 7.

SOLUZIONE: Indichiamo con T_k il punteggio totalizzato con i primi k lanci, e con P_k la probabilità che T_k sia divisibile per 7. Vogliamo calcolare P_n. Ovviamente $T_n = T_{n-1} + i$, dove $i \in \{1, \dots, 6\}$ è il punteggio ottenuto con l'n-esimo lancio, quindi $T_n \equiv 0 \pmod 7$ se e solo se $i \equiv -T_{n-1} \pmod 7$. Ne segue che se $T_{n-1} \equiv 0 \pmod 7$ non è possibile ottenere un multiplo di 7 e quindi la probabilità è 0, mentre se $T_{n-1} \not\equiv 0 \pmod 7$ c'è un unico valore di i che permette di totalizzare un multiplo di 7 e quidi la probabilità è $\frac{1}{6}$.
Abbiamo quindi dimostrato che P_n verifica la seguente relazione di ricorrenza:

$$P_n = \frac{1}{6}(1 - P_{n-1}).$$

Poiché si ha $P_1 = 0$ e $P_2 = \frac{1}{6}$, si ricava che $P_3 = \frac{6-1}{6^2}$ e si può congetturare che

$$P_n = \frac{1}{6^{n-1}} \sum_{i=0}^{n-2} 6^i (-1)^{n+i}.$$

Questa espressione di P_n può essere facilmente dimostrata per induzione usando la formula di ricorrenza.

Esercizio 2.
Determinare, al variare del parametro intero a, il numero di soluzioni modulo 90 del seguente sistema di congruenze.

$$\begin{cases} 3x \equiv a + 1 \pmod 9 \\ (x-1)(x-a) \equiv 0 \pmod{15}. \end{cases}$$

SOLUZIONE: La prima equazione ha soluzione se e solo se $3 = (3,9)|a+1$ cioè $a \equiv 2 \pmod 3$. Quindi se $a \not\equiv 2 \pmod 3$ la prima equazione, e quindi il sistema, non ha soluzione. Assumiamo quindi $a \equiv 2 \pmod 3$, allora $a = 2+3b$ con $b \in \mathbb{Z}$: la prima equazione diventa $x \equiv b+1 \pmod 3$. Usando il teorema cinese ottengo che la seconda equazione è equivalente al sistema

$$\begin{cases} (x-1)(x-a) \equiv 0 \pmod 3 \\ (x-1)(x-a) \equiv 0 \pmod 5; \end{cases}$$

poiché 3 e 5 sono numeri primi, posso applicare a entrambe le equazioni il principio di annullamento del prodotto, quindi le soluzioni della prima equazione sono $x \equiv 1 \pmod 3$ e $x \equiv a \equiv 2 \pmod 3$, e quelle della seconda sono $x \equiv 1 \pmod 5$ e $x \equiv a \equiv 2+3b \pmod 5$. Otteniamo quindi che il sistema è equivalente a

$$\begin{cases} x \equiv b+1 \pmod 3 \\ x \equiv 1,2 \pmod 3 \\ x \equiv 1, 3b+2 \pmod 5 \end{cases}$$

ed è quindi risolubile se e solo se c' è compatibilità tra le due equazioni modulo 3. In particolare, se $b \equiv 2 \pmod 3$, ($a \equiv 8 \pmod 9$) non ci sono soluzioni; se $b \equiv 0 \pmod 3$, cioè $a = 2+3b \equiv 2 \pmod 9$, il sistema assegnato è equivalente a

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1, 3b+2 \pmod 5 \end{cases}$$

mentre se $b \equiv 1 \pmod 3$, cioè $a = 2+3b \equiv 5 \pmod 9$, il sistema assegnato è equivalente a

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1, 3b+2 \pmod 5 \end{cases}.$$

Contiamo il numero di soluzioni del primo sistema: se le due soluzioni dell'equazione modulo 5 coincidono, cioè se $2+3b \equiv 1 \pmod 5$, ovvero $b \equiv 3 \pmod 5$, abbiamo che il sistema ha un'unica soluzione modulo 15, quindi ha 6 soluzioni modulo 90. Se invece $b \not\equiv 3 \pmod 5$ il sistema ha due soluzioni modulo 15, quindi 12 soluzioni modulo 90. Lo stesso discorso vale per il secondo sistema.
Mettendo insieme le condizioni trovate possiamo quindi concludere che:
- se $a \equiv 0, 1 \pmod 3$ la prima equazione e quindi il sistema non ha soluzione;
- se $a \equiv 2 \pmod 3$ dobbiamo distinguere ulteriori casi:

- se $a \equiv 8 \pmod 9$ non c'e compatibilità tra le due equazioni modulo 3, quindi il sistema non ha soluzione;
- se $a \equiv 2 \pmod 9$ il sistema ha soluzione e modulo 90 ha 6 soluzioni se $a \equiv 11 \pmod{45}$ mentre ne ha 12 altrimenti (cioè se $a \equiv 2, 20, 29, 38 \pmod{45}$);
- se $a \equiv 5 \pmod 9$ il sistema ha soluzione e modulo 90 ha 6 soluzioni se $a \equiv -4 \pmod{45}$ mentre ne ha 12 altrimenti(cioè se $a \equiv 5, 14, 23, 32 \pmod{45}$).

Esercizio 3.
Sia G un gruppo e sia $\Delta = \{(x, x) \mid x \in G\}$.
a) Dimostrare che Δ è un sottogruppo di $G \times G$.
b) Dimostrare che Δ è normale in $G \times G$ se e solo se G è abeliano.
c) Dimostrare che, se G è abeliano, $G \times G/\Delta$ è isomorfo a G.

SOLUZIONE: (a) Sia $e \in G$ l'identià, allora (e, e) è l'identità di $G \times G$ e appartiene a Δ. Siano (x, x) e $(y, y) \in \Delta$, allora chiaramente $(x, x)(y, y) = (xy, xy) \in \Delta$. Infine, sia $(x, x) \in \Delta$; il suo inverso in $G \times G$ è l'elemento (x^{-1}, x^{-1}) ed è chiaro che tale elemento appartiene a Δ che è quindi un sottogruppo di $G \times G$.
(b) Chiaramente se G è abeliano anche $G \times G$ lo è, quindi tutti i suoi sottogruppi sono normali. Viceversa, supponiamo che Δ sia normale in $G \times G$, allora per ogni $g \in G$ e per ogni $x \in G$ si ha $(g, e)(x, x)(g^{-1}, e) = (gxg^{-1}, x) \in \Delta$ e questo implica che $\forall g, x \in G$ vale $gxg^{-1} = x$, cioè il gruppo G è abeliano.
(c) Consideriamo la mappa $\varphi : G \times G \to G$ definita da $\varphi((x, y)) = xy^{-1}$. Poiché G è abeliano questa mappa è un omomorfismo, infatti $\varphi((x, y)(a, b)) = \varphi((xa, yb)) = xa(yb)^{-1} = xab^{-1}y^{-1} = xy^{-1}ab^{-1} = \varphi((x, y))\varphi((a, b))$. Inoltre l'omomorfismo è chiaramente surgettivo in quanto $\varphi((x, e)) = x$ per ogni $x \in G$. Osserviamo anche che $ker\varphi = \{(x, y) \mid xy^{-1} = e\} = \Delta$. Dal teorema di omomorfismo otteniamo quindi che $G \times G/\Delta \cong G$.

Esercizio 4.
Sia $f(x) = (x^{15} - 1)(x^{12} - 1)$.
a) Determinare, il grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_2$ e su $\mathbb{F}_7$.
b) Determinare quali sono i possibili valori del grado del campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ al variare di p fra i numeri primi.

SOLUZIONE: Ricordiamo che se $(n, p) = 1$ il grado del campo di spezzamento su $\mathbb{F}_p$ del polinomio $x^n - 1$ coincide con l'ordine moltiplicativo di p modulo n. Ne segue che se $p \neq 2, 3, 5$ il grado cercato è il mcm tra l'ordine moltiplicativo di p modulo 15 e l'ordine moltiplicativo di p modulo 12, o, equivalentemente,

la minima soluzione positiva del seguente sistema

$$\begin{cases} p^x \equiv 1 \pmod{15} \\ p^x \equiv 1 \pmod{12}. \end{cases}$$

Usando il teorema cinese il sistema diventa

$$\begin{cases} p^x \equiv 1 \pmod{3} \\ p^x \equiv 1 \pmod{4} \\ p^x \equiv 1 \pmod{5} \end{cases}.$$

È immediato verificare che $x = 4$ risolve il sistema quindi la minima soluzione positiva sarà un divisore di 4. Vediamo che tutti i divisori di 4 sono gradi possibili.
Per $p = 7$ applicando quanto sopra si verifica subito che il grado del campo di spezzamento è 4.
Il grado del campo di spezzamento su $\mathbb{F}_p$ è 2 se $p \equiv -1 \pmod 5$ (infatti $p^2 \equiv 1 \pmod 3$ e $p^2 \equiv 1 \pmod 4$ per ogni primo maggiore di 3) e possiamo ad esempio scegliere $p = 19$. Il grado del campo di spezzamento sarà invece 1 se e solo se $3|p-1$, $4|p-1$ e $5|p-1$ cioè se e solo se $60|p-1$. Poiché 61 è primo, allora il campo di spezzamento di $f(x)$ sul campo $\mathbb{F}_{61}$ ha grado 1.
Resta da considerare il caso $p = 2$: $f(x) = (x^{15} - 1)(x^3 - 1)^4$ e , poichè $3|15$ allora $x^3 - 1|x^{15} - 1$, quindi il grado del campo di spezzamento di $f(x)$ coincide con l'ordine di 2 in $(\mathbb{Z}/15\mathbb{Z})^*$, che si vede facilmente essere 4.
Per completare la casistica rimangono da considerare i primi 3 e 5: per $p = 3$ si ha $f(x) = (x^5 - 1)^3(x^4 - 1)^3$: poiché l'ordine moltiplicativo di 3 modulo 5 è 4 e modulo 4 è 2 si ha che il grado del campo di spezzamento è 4. Per $p = 5$ si ha $f(x) = (x^3 - 1)^5(x^{12} - 1)$ e con lo stesso ragionamento si ottiene che il grado del campo di spezzamento è 2.