SOLUZIONI DEL 1° COMPITINO DI ARITMETICA
9 novembre 2017

Esercizio 1.
Sia $X = \{1, 2, \dots, 100\}$.

1. Quanti sono i sottoinsiemi $A = \{a, b, c\}$ di X di 3 elementi tali che $a + b + c$ è un numero pari?
2. Quanti sono i sottoinsiemi $B = \{a, b, c\}$ di X di 3 elementi tali che $a + b + c$ è divisibile per 3?

Soluzione:

1. Osserviamo che $a+b+c$ è pari se e solo se siamo in uno dei due casi seguenti: a, b, c sono tutti pari, oppure esattamente uno di essi è pari. Determiniamo il numero dei sottoinsiemi A in questi due casi.

   (a) Tutti gli elementi di A sono pari: in tal caso stiamo semplicemente contando i sottoinsiemi di tre elementi di $\{2, 4, 6, 8, \dots, 100\}$, e questi sono $\binom{50}{3}$.

   (b) Esattamente un elemento di A è pari: tale elemento può essere scelto in 50 modi, mentre i rimanenti due elementi (dispari) possono essere scelti in modo arbitrario nell'insieme $\{1, 3, 5, 7, \dots, 99\}$, cosa che può essere fatta in $\binom{50}{2}$ modi.

   La risposta è dunque $\binom{50}{3} + 50\binom{50}{2} = 80850$.

2. La somma $a + b + c$ è divisibile per 3 se e solo siamo in uno dei due casi seguenti: $a \equiv b \equiv c \pmod 3$, oppure a, b, c sono congrui, in qualche ordine, a $0, 1, 2$ modulo 3. Determiniamo il numero dei sottoinsiemi B in questi due casi.

   (a) se $a \equiv b \equiv c \pmod 3$, allora stiamo scegliendo un sottoinsieme di 3 elementi di uno degli insiemi $\{3, 6, 9, 12, \dots, 99\}$ (se $a \equiv b \equiv c \equiv 0 \pmod 3$), $\{1, 4, 7, 10, \dots, 100\}$ (se $a \equiv b \equiv c \equiv 1 \pmod 3$), o $\{2, 5, 8, 11, \dots, 98\}$ (se $a \equiv b \equiv c \equiv 2 \pmod 3$). Nei tre casi, questa scelta può essere fatta in $\binom{33}{3}$, $\binom{34}{3}$, $\binom{33}{3}$ modi diversi.

   (b) Senza perdita di generalità (dal momento che stiamo considerando insiemi, e non terne ordinate) possiamo supporre $a \equiv 0 \pmod 3, b \equiv 1 \pmod 3, c \equiv 2 \pmod 3$. Ci sono dunque 33 scelte per a, 34 scelte per b, e 33 scelte per c, per un totale di $33^2 \cdot 34$ scelte.

La risposta in questo caso è quindi $33^2 \cdot 34 + 2\binom{33}{3} + \binom{34}{3} = 53922$.

Nota. La soluzione si considera completa anche se le risposte non sono state espresse in forma numerica come 80850 e 53922.

Esercizio 2.
Determinare l'insieme degli interi positivi n per i quali $\phi(n) = 16$ (dove ϕ è la funzione di Eulero).

Soluzione: Scriviamo $n = p_1^{e_1} \cdots p_k^{e_k}$ con i p_i primi distinti e gli esponenti e_i positivi. Si ha allora $\phi(n) = (p_1 - 1)p_1^{e_1-1} \cdots (p_k - 1)p_k^{e_k-1}$. Osserviamo che se un esponente e_i è maggiore o uguale a 2 il corrispondente primo p_i divide $\phi(n) = 16$, da cui deduciamo che l'unico primo che può dividere n con esponente 2 o più è $p = 2$. Osserviamo inoltre che se p_i è un divisore primo di n, allora $p_i - 1$ divide $\phi(n) = 16$, e dunque $p_i - 1$ è uno fra $1, 2, 4, 8, 16$. Siccome $8 + 1 = 9$ non è primo, questo ci dice che p_i è uno fra 2, 3, 5 e 17. Distinguiamo quattro casi a seconda del più grande divisore primo di n.

- $17 \mid n$: in tal caso si ha $16 = \phi(n) = \phi(17)\phi(n/17) = 16\phi(n/17)$, ovvero $\phi(n/17) = 1$. È noto che $\phi(m) = 1$ solo per $m = 1, 2$, dunque $n/17 \in \{1, 2\}$ e perciò $n \in \{17, 34\}$. Entrambi questi numeri rispettano effettivamente $\phi(n) = 16$.

- $5 \mid n, 17 \nmid n$. Similmente si ottiene $16 = \phi(n) = \phi(5)\phi(n/5)$, da cui $\phi(n/5) = 4$ e $n/5 = m$ è divisibile solo per fattori 2 e 3 (quest'ultimo con esponente al più 1). Dal momento che $\phi(2^a) = 2^{a-1}$ e $\phi(2^a \cdot 3) = 2^a$, troviamo che $m \in \{8, 12\}$ e di conseguenza $n \in \{40, 60\}$.

- 3 è il più grande fattore primo di n: chiaramente $n > 3$ (dato che $\phi(3) \neq 16$), quindi abbiamo $n = 2^a \cdot 3$ con $a > 0$ e di conseguenza $\phi(n) = 2^a$, da cui $a = 4$. L'unica soluzione in questo caso è $n = 2^4 \cdot 3 = 48$.

- 2 è il più grande fattore primo di n: allora $n = 2^a$ è una potenza di 2 (con esponente $a > 0$), e $\phi(n) = 2^{a-1}$ è uguale a 16 se e solo se $a = 5$, da cui l'ultima soluzione $m = 32$.

In conclusione, l'insieme richiesto è $\{17, 32, 34, 40, 48, 60\}$.

Esercizio 3.
Determinare, in funzione del parametro $a \in \mathbb{Z}$, le soluzioni del seguente sistema di congruenze:

$$\begin{cases} 3^x \equiv 7^a \pmod{11} \\ (a+3)x \equiv 2 \pmod{5} \end{cases}$$

Soluzione: Iniziamo studiando la prima congruenza del sistema. Calcoliamo intanto le prime potenze di 7 modulo 11: si ha $7^0 \equiv 1 \pmod{11}$, $7^1 \equiv 7 \pmod{11}$, $7^2 \equiv 5 \pmod{11}$, $7^3 \equiv 2 \pmod{11}$, $7^4 \equiv 3 \pmod{11}$, $7^5 \equiv -1 \pmod{11}$. Questo calcolo ci permette già di dimostrare che l'ordine moltiplicativo di 7 modulo 11 è uguale a 10: infatti, detto h tale ordine moltiplicativo, si ha che $h \mid \varphi(11) = 10$, e d'altro canto h non è uguale né a 1 (ovviamente), né a 2 (dal momento che $7^2 \not\equiv 1 \pmod{11}$), né a 5 (dal momento che $7^5 \not\equiv 1 \pmod{11}$), dunque l'unica possibilità è effettivamente $h = 10$. Sfruttando la congruenza $3 \equiv 7^4 \pmod{11}$ possiamo riscrivere la prima congruenza del sistema come $7^{4x} \equiv 7^a \pmod{11}$, e moltiplicando entrambi i membri per l'inverso di 7^a ci riconduciamo a studiare $7^{4x-a} \equiv 1 \pmod{11}$, ovvero, sfruttando le proprietà dell'ordine moltiplicativo, $4x - a \equiv 0 \pmod{10}$. Dal momento che un numero è divisibile per 10 se e solo se è divisibile per 2 e per 5 (o anche come applicazione del Teorema Cinese del Resto), vediamo che questa congruenza è equivalente alle due congruenze $4x - a \equiv 0 \pmod 2$ e $4x - a \equiv 0 \pmod 5$, ovvero

$$\begin{cases} a \equiv 0 \pmod 2 \\ x \equiv -a \pmod 5. \end{cases}$$

Sostituendo la prima congruenza del sistema originale con queste due condizioni ci siamo allora ricondotti a studiare

$$\begin{cases} a \equiv 0 \pmod 2 \\ x \equiv -a \pmod 5 \\ (a+3)x \equiv 2 \pmod 5. \end{cases}$$

Usando la seconda condizione per sostituire x con $-a$ nella terza equazione, troviamo che a deve rispettare $-a(a+3) \equiv 2 \pmod 5$, ovvero $-(a+1)(a+2) \equiv 0 \pmod 5$. Dal momento che 5 è primo, il prodotto $(a+1)(a+2)$ è divisibile per 5 se e solo se uno dei due fattori lo è, quindi l'ultima congruenza può essere sostituita con la condizione "$a \equiv 4 \pmod 5$ oppure $a \equiv 3 \pmod 5$". A questo punto, l'unica condizione rimasta che riguardi x è la semplice congruenza $x \equiv -a \pmod 5$. Combinando le condizioni modulo 2 e modulo 5 che riguardano a in un'unica congruenza modulo 10 arriviamo allora alla seguente conclusione:

- per $a \equiv 4 \pmod{10}$ le soluzioni del sistema sono tutti e soli gli interi x tali che $x \equiv 1 \pmod 5$;
- per $a \equiv 8 \pmod{10}$ le soluzioni del sistema sono tutti e soli gli interi x tali che $x \equiv 2 \pmod 5$;
- in tutti gli altri casi, il sistema non ha soluzioni.