SOLUZIONI DEL COMPITO DI ARITMETICA
13 febbraio 2014

Esercizio 1.
Sia $\mathbb{N}_{100} = \{1, 2, \dots, 100\}$. Determinare la cardinalità dei seguenti insiemi:
a) $X = \{A \subseteq \mathbb{N}_{100} \mid \max A - \min A = 60\}$.
b) $Y = \{f : \mathbb{N}_{100} \to \mathbb{N}_{100} \mid f(1) \cdot f(2) \cdots f(100) \not\equiv 0 \pmod{10}\}$.
Soluzione: a) Siano $A \in X$, $a = \min A$ e $b = \max A$. Allora $b = 60 + a$, e, poiché $b \leq 100$, per a abbiamo 40 scelte (gli interi tra 1 e 40). Gli insiemi $A \in X$ con $\min A = a$ e $\max A = b$ si costruiscono scegliendo $A \setminus \{a, b\}$ come un qualsiasi sottoinsieme di $\{a + 1, \dots, a + 59\}$, e per questa scelta ci sono quindi 2^{59} possibilità. Abbiamo quindi $|X| = 40 \cdot 2^{59} = 2^{62} \cdot 5$.
b) Siano C_2 e C_5 i sottoinsiemi di $\mathbb{N}_{100}$ formati rispettivamente degli interi che non sono multipli di 2 e di 5. Poniamo $Y_i = \{f \in Y \mid f(\mathbb{N}_{100}) \subseteq C_i\}$ per $i = 2, 5$; si ha $Y = Y_2 \cup Y_5$ e $Y_2 \cap Y_5 = \{f \in Y \mid f(\mathbb{N}_{100}) \subseteq C_2 \cap C_5\}$, quindi $|Y| = |Y_2 \cup Y_5| = |Y_2| + |Y_5| - |Y_2 \cap Y_5| = |C_2|^{100} + |C_5|^{100} - |C_2 \cap C_5|^{100}$. Ora $|C_2| = 50$, $|C_5| = 80$ e $|C_2 \cap C_5| = 40$ perché i non multipli di 5 sono metà pari e metà dispari (si può vedere anche osservando che il sistema formato dalle due equazioni $x \equiv 1 \pmod 2$ e $x \equiv a \pmod 5$ ha 10 soluzioni in $\mathbb{N}_{100}$ per a=1,2,3,4). Abbiamo quindi $Y = 50^{100} + 80^{100} - 40^{100}$.

Esercizio 2.
Determinare il numero di soluzioni modulo 1001 della congruenza

$$x^{101} \equiv x \pmod{1001}.$$

Soluzione: Per il teorema cinese del resto, la congruenza assegnata è equivalente al sistema

$$\begin{cases} x(x^{100} - 1) & \equiv 0 \pmod 7 \\ x(x^{100} - 1) & \equiv 0 \pmod{11} \\ x(x^{100} - 1) & \equiv 0 \pmod{13} \end{cases}$$

Indichiamo con p un numero primo e contiamo le soluzioni della generica equazione $x(x^{100} - 1) \equiv 0 \pmod p$: poiché p è primo questo prodotto è 0 se e solo se uno dei due fattori è 0, quindi $x \equiv 0 \pmod p$ oppure $x^{100} \equiv 1 \pmod p$. Le soluzioni dell'equazione $x^{100} \equiv 1 \pmod p$ sono gli elementi di $(\mathbb{Z}/p\mathbb{Z})^*$ il cui ordine divide 100, e quindi, poiché l'ordine di un elemento divide l'ordine del gruppo, sono gli elementi il cui ordine divide $(100, p - 1)$. Essendo $(\mathbb{Z}/p\mathbb{Z})^*$ un gruppo ciclico (perché p è primo) di ordine multiplo di

$(100, p-1)$, contiene esattamente $(100, p-1)$ soluzioni dell'equazione $x^{100} \equiv 1 \pmod{p}$. In tutto l'equazione ha quindi $(100, p-1)+1$ soluzioni.
Da questo segue che le tre equazioni del sistema hanno rispettivamente $(100, 6)+1 = 3$ soluzioni modulo 7, $(100, 10)+1 = 11$ soluzioni modulo 11 e $(100, 12)+1 = 5$ modulo 13. Le soluzioni del sistema si ottengono mettendo a sistema ogni una qualsiasi soluzione modulo 7 con una qualsiasi soluzione modulo 11 e con una qualsiasi soluzione modulo 13. Le soluzioni si trovano quindi risolvendo i $3 \cdot 11 \cdot 5 = 165$ sistemi del tipo

$$\begin{cases} x \equiv a & \pmod{7} \\ x \equiv b & \pmod{11} \\ x \equiv c & \pmod{13} \end{cases}$$

Per il teorema cinese del resto ognuno di questi sistemi ha un'unica soluzione modulo $7 \cdot 11 \cdot 13 = 1001$ e le soluzioni di sistemi diversi sono diverse, quindi le soluzioni dell'equazione assegnata sono 165.

Esercizio 3.
Sia G un gruppo abeliano e sia k un intero maggiore di 1. Poniamo $G^k := \{g^k \mid g \in G\}$.
a) Mostrare che G^k è un sottogruppo di G e che nel gruppo G/G^k tutti gli elementi hanno ordine finito.
b) Sia G un gruppo ciclico di ordine n, calcolare la cardinalità di G/G^k.
c) Dare un esempio di un gruppo G tale che $G/G^{10} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.
SOLUZIONE: a) G^k è un sottogruppo di G: infatti, $e = e^k \in G^k$; $\forall a^k, b^k \in G^k$ si ha $a^k b^k = (ab)^k$ perché G è abeliano, quindi $a^k b^k = (ab)^k \in G^k$. Infine $\forall a^k \in G^k$ si ha $(a^k)^{-1} = (a^{-1})^k \in G^k$, quindi G^k è un sottogruppo di G e poiché G è abeliano è anche normale.
Consideriamo il quoziente G/G^k e sia xG^k un suo elemento: allora, per come è definita l'operazione sul quoziente, si ha $(xG^k)^k = x^k G^k = G^k$, quindi l'ordine di un qualsiasi elemento del quoziente è un divisore di k, e quindi è finito.
b) Sia $G \cong \mathbb{Z}/n\mathbb{Z}$ allora $G^k \cong \langle [k]_n \rangle$ che è quindi un gruppo ciclico di ordine uguale a $\mathrm{ord}[k]_n = \frac{n}{(n,k)}$. Ne segue che $|G/G^k| = |G|/|G^k| = (n, k)$. Sappiamo anche che G/G^k è ciclico perché quoziente di un gruppo ciclico quindi $G/G^k \cong \mathbb{Z}/(n, k)\mathbb{Z}$.
c) Consideriamo il gruppo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, allora $G^{10} = \{(0, 0)\}$ infatti per ogni $(a, b) \in G$ si ha $10(a, b) = (10a, 10b) = (0, 0)$. Per tale gruppo chiaramente $G/G^k = G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.
Più in generale se $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si ha che $G^k = \{(ka, kb) \mid (a, b) \in G\} = \mathbb{Z}/\frac{m}{(m,k)}\mathbb{Z} \times \mathbb{Z}/\frac{n}{(n,k)}\mathbb{Z}$ e $G/G^k \cong \mathbb{Z}/(m, k)\mathbb{Z} \times \mathbb{Z}/(n, k)\mathbb{Z}$. Ne segue che, per $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si ha $G/G^{10} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ se e solo se $(m, 10) = 2$ e $(n, 10) = 10$.

Esercizio 4.
Sia $\alpha \in \mathbb{C}$ una radice del polinomio $f(x) = x^4 + x + 1$.

a) Determinare il polinomio minimo di $\frac{1}{\alpha+1}$ e di α^2 su $\mathbb{Q}$.

b) Determinare il campo di spezzamento del polinomio $f(x)$ su $\mathbb{F}_5$.

SOLUZIONE: a) Il polinomio $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e quindi per il lemma di Gauss anche in $\mathbb{Q}[x]$) perché lo è modulo 2. Infatti, è banale verificare che 0 e 1 non sono radici modulo 2, quindi il polinomio non ha fattori di primo grado. Se non fosse irriducibile dovrebbe essere prodotto di due polinomi irriducibili di grado 2: l'unico polinomio irriducibile di grado 2 di $\mathbb{F}_2[x]$ è x^2+x+1 e si ha $(x^2+x+1)^2 = x^4+x^2+1 \neq f(x)$, quindi $f(x)$ è irriducibile. Da questo ricaviamo che $f(x)$ è il polinomio minimo di α, quindi $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$; poiché $\mathbb{Q}(\frac{1}{\alpha+1}) = \mathbb{Q}(\alpha)$ il polinomio minimo di $\frac{1}{\alpha+1}$ avrà grado 4. Il polinomio minimo di $\alpha+1$ è $g(x) = f(x-1) = (x-1)^4+(x-1)+1 = x^4-4x^3+6x^2-3x+1$, il polinomio minimo di $\frac{1}{\alpha+1}$ è il suo reciproco $h(x) = x^4-3x^3+6x^2-4x+1$.
Osserviamo che $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ infatti, chiaramente $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$, inoltre dall' equazione $f(\alpha) = 0$ si ricava $\alpha = -\alpha^4 - 1 \in \mathbb{Q}(\alpha^2)$ che dà l'altro contenimento. Abbiamo quindi che il polinomio minimo di α^2 su $\mathbb{Q}$ ha grado 4. Questo può essere calcolato in vari modi, ad esempio osservando che $\alpha^4+1 = -\alpha$ da cui, elevando al quadrato ambo i membri, si ottiene $\alpha^8+2\alpha^4+1 = \alpha^2$, quindi il polinomio x^4+2x^2-x+1 si annulla in α^2 e ne è il polinomio minimo perché è monico ed è irriducibile perché è di grado minimo. Calcoliamo il polinomio minimo di α^2 anche in un altro modo: sappiamo che sarà del tipo $\mu(x) = x^4+ax^3+bx^2+cx+d$, dobbiamo ricavare $a,b,c,d \in \mathbb{Q}$ in modo tale che $\alpha^8+a\alpha^6+b\alpha^4+c\alpha^2+d = 0$. Usando la relazione data dal polinomio minimo di α si calcola che $\alpha^4 = -\alpha-1$, $\alpha^6 = -\alpha^3-\alpha^2$ e $\alpha^8 = \alpha^2+2\alpha+1$, da questo si ha $\mu(\alpha^2) = -a\alpha^3+(1-a+c)\alpha^2+(2-b)\alpha+1-b+d = 0$. Poiché $1,\alpha,\alpha^2,\alpha^3$ sono linearmente indipendenti l'equazione è verificata se e solo se $a=0, b=2, c=-1$ e $d=1$.
b) Il campo di spezzamento di $f(x)$ su $\mathbb{F}_5$ è $\mathbb{F}_{5^d}$ dove d è il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$ in $\mathbb{F}_5[x]$. Cerco le radici di $f(x)$: valuto il polinomio $f(x)$ in $0, \pm1, \pm2$ e vedo che l'unico valore in cui il polinomio si annulla è -2. Per il teorema di Ruffini $x+2|f(x)$. Si calcola $f(x) = (x+2)(x^3+3x^2-x+3)$. Le possibili radici del fattore di terzo grado sono da ricercarsi tra quelle di $f(x)$, quindi l'unica possibile radice è -2: si ha $(-2)^3+3(-2)-(-2)+3 \neq 0$ quindi x^3+3x^2-x+3 non ha radici. Ma un polinomio di grado 3 che non ha radici è irriducibile, quindi $f(x) = (x+2)(x^3+3x^2-x+3)$ è la fattorizzazione di $f(x)$. Abbiamo quindi che il campo di spezzamento di $f(x)$ su $\mathbb{F}_5$ è $\mathbb{F}_{5^3}$.