ALGEBRA 1
Prima prova di accertamento - 6 novembre 2006

Tema A

Esercizio 1

Siano X un insieme non vuoto ed $F = \{f : X \to \{0,1\}\}$ l'insieme delle funzioni di X nell'insieme con due elementi $\{0,1\}$. Per ogni sottoinsieme $A \subseteq X$ definiamo la funzione $\chi_A \in F$ ponendo $\chi_A(x) = 1$ se $x \in A$, $\chi_A(x) = 0$ se $x \notin A$.

Si provi che la posizione $\chi : A \mapsto \chi_A$ definisce una biiezione dell'insieme $\mathcal{P}(X)$ dei sottoinsiemi di X su F.

Soluzione

La posizione $\chi : A \mapsto \chi_A$ è chiaramente una funzione ben posta. Dobbiamo dimostrarne la suriettività e la iniettività.

Iniettività: dati due elementi diversi del dominio, dobbiamo dimostrare che hanno immagini diverse.

Siano A e B due elementi del dominio, cioè due sottoinsiemi di X. Supponiamo che A non coincida con B. Esiste quindi almeno un elemento $x \in X$ tale che $x \in A$, $x \notin B$ oppure $x \in B$, $x \notin A$. Assumiamo senza perdita di generalità che $x \in A$, $x \notin B$. Questo comporta che $\chi_A(x) = 1$, $\chi_B(x) = 0$ e $\chi_A \neq \chi_B$, pertanto $A \neq B$.

Suriettività: dato un elemento f del codominio, dobbiamo dimostrare che esiste un elemento A del dominio tale che $\chi(A) = \chi_A$ sia proprio f.

Sia f una funzione $X \to \{0,1\}$. Consideriamo il sottoinsieme $f^{-1}(1)$ di X. La nostra intenzione è di mostrare che questo è l'elemento del dominio cercato. Infatti $\chi_{f^{-1}(1)}(x) = 1$ se e solo se $x \in f^{-1}(1)$ se e solo se $f(x) = 1$ e $\chi_{f^{-1}(1)}(x) = 0$ se e solo se $x \notin f^{-1}(1)$ se e solo se $f(x) = 0$. Pertanto $\chi(f^{-1}(1)) = \chi_{f^{-1}(1)} = f$ come desiderato.

Esercizio 2

Sia $m = p^k$ un intero > 1 potenza del numero primo p. Si provi che nell'anello $\mathbb{Z}/m\mathbb{Z}$ ogni elemento non invertibile è nilpotente (in un anello, un elemento a si dice nilpotente se esiste un intero positivo r tale che $a^r = 0$).

Supponiamo ora che m sia divisibile per due primi distinti p e q. È vero che in questo caso $\mathbb{Z}/m\mathbb{Z}$ ha elementi non invertibili che non sono nilpotenti?

Soluzione

Sia $[n]$ un elemento non invertibile in $\mathbb{Z}/p^k\mathbb{Z}$. Deve essere che $MCD(n, p^k) \neq 1$ e pertanto che $p \mid n$. Si ha quindi che $p^k \mid n^k$ e perciò $[n]^k = [n^k] = [0]$. Si ha dunque che $[n]$ è nilpotente.

Sia ora m divisibile per due primi distinti p e q. Siccome $MCD(p, m) \neq 1$, si ha che $[p]$ non è invertibile in $\mathbb{Z}/m\mathbb{Z}$. Siccome $q \nmid p$ si ha che $q \nmid p^k$ per ogni $k > 0$ e pertanto che $m \nmid p^k$ per ogni $k > 0$. Questo vuol dire che $[p]^k = [p^k] \neq [0]$ per ogni $k > 0$. Si ha dunque che $[p]$ non è nilpotente.

Esercizio 3

Nell'insieme $X = \mathbb{R}^2 \setminus \{(0,0)\}$ definiamo la relazione ρ ponendo $(a,b)\rho(c,d)$ se e solo se $ad = bc$.
a) Si provi che ρ è un'equivalenza.
b) Si descriva e si disegni sul piano cartesiano la classe di $(1,-2)$ modulo ρ.

Soluzione

a) Per dimostrare che ρ è un'equivalenza, dobbiamo vedere che è riflessiva, simmetrica e transitiva.

Osserviamo che la riflessività è ovvia in quanto $(a,b)\rho(a,b)$ se e solo se $ab = ba$.

La simmetria è altrettanto immediata in quanto $(a,b)\rho(c,d)$ se e solo se $ad = bc$ se e solo se $cb = da$ se e solo se $(c,d)\rho(a,b)$.

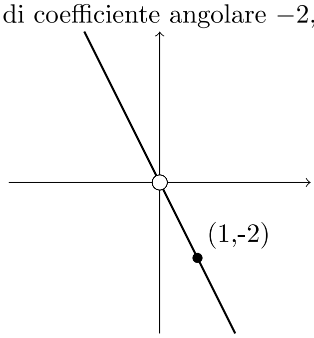
Per la transitività bisogna fare qualche calcolo in più. Supponiamo che $(a,b)\rho(c,d)$ e che $(c,d)\rho(e,f)$. Allora $ad = bc$ e $cf = de$. Segue $adf = bcf = bde$.

Abbiamo due possibilità: o $d = 0$ o $d \neq 0$.

Se $d = 0$ allora $c \neq 0$ e $ad = bc = 0$, da cui $b = 0$, ma anche $cf = de = 0$, da cui $f = 0$. Pertanto $af = 0 = be$ e dunque $(a,b)\rho(e,f)$.

Se $d \neq 0$ si può semplificarlo in $bde = adf$: si ottiene $be = af$, cioè $(a,b)\rho(e,f)$.

b) La classe di $(1,-2)$ modulo ρ è l'insieme $\{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid (1,-2)\rho(x,y)\} = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid 1 \cdot y = -2 \cdot x\} = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid y = -2x\}$ che è la retta passante per l'origine di coefficiente angolare -2, origine esclusa.



Esercizio 4

Dimostrare che per ogni $n \geq 1$ si ha

$$2^3 + 4^3 + \ldots + (2n)^3 = 2n^2(n+1)^2.$$

Soluzione

La dimostrazione procede per induzione su n.

Se $n = 1$ si ha che $2^3 = 2 \cdot 1^2(1+1)^2$ e il passo base è verificato.

Supponiamo di aver dimostrato che $2^3+4^3+\ldots+(2n)^3 = 2n^2(n+1)^2$ per qualche $n > 1$ e facciamo vedere che $2^3 + 4^3 + \ldots + (2n)^3 + (2(n+1))^3 = 2(n+1)^2(n+2)^2$.

Per ipotesi induttiva si ha che $2^3 + 4^3 + \ldots + (2n)^3 + (2(n+1))^3 = 2n^2(n+1)^2 + (2(n+1))^3$ e raccogliendo si ha $2^3 + 4^3 + \ldots + (2n)^3 + (2(n+1))^3 = 2(n+1)^2(n^2 + 4(n+1)) = 2(n+1)^2(n^2 + 4n + 4) = 2(n+1)^2(n+2)^2$.

Esercizio 5

Siano a e b due numeri interi fissati. Consideriamo la funzione $\varphi_{a,b} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\varphi_{a,b}(x,y) = ax - by$.

a) Si discuta la iniettività di $\varphi_{a,b}$ al variare di a e b.
b) Si discuta la suriettività di $\varphi_{a,b}$ al variare di a e b.
c) Nel caso $a = 6$, $b = 9$ si calcoli un elemento dell'insieme $\varphi_{a,b}^{-1}(3)$.
d) Nel caso $a = 6$, $b = 9$ si descriva tutto l'insieme $\varphi_{a,b}^{-1}(3)$.

Soluzione

a) La funzione non è mai iniettiva. Infatti se $a = 0$ e $b = 0$ la funzione manda tutte le coppie di interi in 0 e pertanto non è iniettiva. Se invece uno tra a e b è diverso da zero, allora le coppie $(0, 0)$ e (b, a) sono due elementi diversi del dominio. Ciononostante si ha che $\varphi_{a,b}(0, 0) = 0 = \varphi_{a,b}(b, a)$.
b) Se il massimo comune divisore tra a e b è 1, allora esistono due interi λ e μ tali che $\lambda a+\mu b = 1$. In questo caso vogliamo far vedere che la funzione $\varphi_{a,b}$ è suriettiva. Infatti, dato un elemento x del codominio, la coppia $(x\lambda, -x\mu)$ viene mandata in x (come si vede facilmente da $\varphi_{a,b}(x\lambda, -x\mu) = x\lambda a-(-x\mu)b = x(\lambda a+\mu b) = x\cdot 1 = x$.

Viceversa se il massimo comune divisore tra a e b è maggiore di 1, vediamo che $\varphi_{a,b}$ non è suriettiva. Infatti se fosse suriettiva 1 apparterrebbe all'immagine, cioè esisterebbe una coppia di interi (x, y) tale che $\varphi_{a,b}(x, y) = 1$, pertanto esisterebbe una coppia di interi (x, y) tale che $ax + b(-y) = 1$. Ma $ax + b(-y)$ è divisibile per il massimo comune divisore di a e b che è maggiore di 1, contraddizione.

La contraddizione nasce dall'aver supposto che $\varphi_{a,b}$ sia suriettiva. Ne concludiamo che non lo è.
c) Si ha per esempio che $9-6 = 3$, cioè che $(-1)a-(-1)b = 3$. Pertanto $(-1, -1) \in \varphi_{a,b}^{-1}(3)$.
d) Abbiamo una soluzione particolare $(-1)6 - (-1)9 = 3$. Consideriamo ora una soluzione generale $6x - 9y = 3$. Scriviamo $x = -1 + \alpha$ e $y = -1 + \beta$, da cui $-6 + 6\alpha + 9 - 9\beta = 3$, cioè $6\alpha - 9\beta = 0$, che è equivalente a $2\alpha = 3\beta$, cioè $\alpha = 3n$, $\beta = 2n$ per qualche intero n. Pertanto tutte e sole le soluzioni di $6x - 9y = 3$ si ricavano aggiungendo alla soluzione particolare $(-1, -1)$ un elemento del tipo $(3n, 2n)$. L'insieme cercato è quindi $\varphi_{a,b}^{-1}(3) = \{(-1 + 3n, -1 + 2n) \mid n \in \mathbb{Z}\}$.

Esercizio 6

Si risolvano i seguenti sistemi di congruenze in $\mathbb{Z}$.

$$a)\begin{cases} x \equiv 45 \pmod{89} \\ 3x \equiv 7 \pmod{10} \end{cases} \qquad b)\begin{cases} 5x \equiv 12 \pmod{35} \\ x \equiv 12 \pmod{41} \end{cases}$$

Soluzione

a) Risolviamo la seconda congruenza. In $\mathbb{Z}/10\mathbb{Z}$ la classe di 3 è invertibile con la classe di 7 come inverso, pertanto la seconda congruenza è equivalente a $7 \cdot 3x \equiv 7 \cdot 7 \pmod{10}$ che è equivalente a $x \equiv 9 \pmod{10}$. Pertanto le singole congruenze hanno soluzioni. Vediamo se il sistema ne ha.

Notiamo innanzitutto che $MCD(89, 10) = 1$ e che pertanto il teorema cinese del resto ci assicura l'esistenza di soluzioni. Per trovarle risolviamo le congruenze $10x \equiv 45 \pmod{89}$ (che ha soluzione $x \equiv 49 \pmod{89}$) e $89x \equiv 9 \pmod{10}$ (che ha soluzione $x \equiv 1 \pmod{10}$). Una soluzione particolare è quindi $10 \cdot 49 + 89 \cdot 1 = 579$ e la soluzione generale è $579 + k890$ dove $k \in \mathbb{Z}$.
b) La prima congruenza non ha soluzioni in quanto $MCD(5, 35) = 5$ che non divide 12. Nemmeno il sistema, quindi, ha soluzioni.

ALGEBRA 1
Prima prova di accertamento - 6 novembre 2006

Tema B

Esercizio 1

Siano X un insieme non vuoto ed $F = \{f : X \to \{0, 1\}\}$ l'insieme delle funzioni di X nell'insieme con due elementi $\{0, 1\}$. Per ogni funzione $f \in F$ consideriamo il sottoinsieme $f^{-1}(1)$ di X.

Si provi che la posizione $\phi : f \mapsto f^{-1}(1)$ definisce una biiezione di F sull'insieme $\mathcal{P}(X)$ dei sottoinsiemi di X.

Soluzione

La posizione $\phi : f \mapsto f^{-1}(1)$ è chiaramente una funzione ben posta. Dobbiamo dimostrarne la suriettività e la iniettività.

Iniettività: dati due elementi diversi del dominio, dobbiamo dimostrare che hanno immagini diverse. Equivalentemente dobbiamo dimostrare che due elementi del dominio che hanno la stessa immagine sono uguali.

Siano f e g due elementi del dominio, cioè due funzioni di X in $\{0, 1\}$. Supponiamo $\phi(f) = \phi(g)$ cioè $f^{-1}(1) = g^{-1}(1)$ e chiamiamo A questo sottoinsieme di X. Allora se $x \in A$ risulta $f(x) = 1$ e anche $g(x) = 1$, mentre se $x \notin A$ dev'essere $f(x) \neq 1$ e anche $g(x) \neq 1$. Siccome il codominio di f e di g è $\{0, 1\}$, dire $f(x) \neq 1$ è dire $f(x) = 0$; lo stesso per $g(x)$. In conclusione $f(x) = g(x)$ per ogni $x \in X$, cioè $f = g$.

Suriettività: dato un elemento A del codominio, dobbiamo dimostrare che esiste un elemento f del dominio tale che $\phi(f) = f^{-1}(1)$ sia proprio A.

Sia A un sottoinsieme di X. Consideriamo la funzione $f \colon X \to \{0, 1\}$ definita da $f(x) = 1$ se $x \in A$ e $f(x) = 0$ se $x \notin A$. La nostra intenzione è di mostrare che questo è l'elemento del dominio cercato. Infatti $x \in \phi(f)$ se e solo se $x \in f^{-1}(1)$ se e solo se $f(x) = 1$ se e solo se $x \in A$ come desiderato.

Esercizio 2

Sia m un intero > 1 divisibile per due primi distinti p e q. Si provi che l'anello $\mathbb{Z}/m\mathbb{Z}$ contiene elementi non invertibili che non sono nilpotenti (in un anello, un elemento a si dice nilpotente se esiste un intero positivo r tale che $a^r = 0$).

Supponiamo ora che $m = p^k$ sia potenza di un primo p. È vero che in questo caso tutti gli elementi non invertibili di $\mathbb{Z}/m\mathbb{Z}$ sono nilpotenti?

Soluzione

Sia m un intero divisibile per due primi distinti p e q. Siccome $MCD(p, m) \neq 1$, si ha che $[p]$ non è invertibile in $\mathbb{Z}/m\mathbb{Z}$. Siccome $q \nmid p$ si ha che $q \nmid p^k$ per ogni $k > 0$ e pertanto che $m \nmid p^k$ per ogni $k > 0$. Questo vuol dire che $[p]^k = [p^k] \neq [0]$ per ogni $k > 0$. Si ha dunque che $[p]$ non è nilpotente.

Sia ora $[n]$ un elemento non invertibile in $\mathbb{Z}/p^k\mathbb{Z}$. Deve essere che $MCD(n, p^k) \neq 1$ e pertanto che $p \mid n$. Si ha quindi che $p^k \mid n^k$ e perciò $[n]^k = [n^k] = [0]$. Si ha dunque che $[n]$ è nilpotente.

Esercizio 3

Nell'insieme $X = \mathbb{R}^2$ definiamo la relazione σ ponendo $(a,b)\sigma(c,d)$ se e solo se $a+d = b+c$.

a) Si provi che σ è un'equivalenza.

b) Si descriva e si disegni sul piano cartesiano la classe di $(-1,2)$ modulo σ.

Soluzione

a) Per dimostrare che σ è un'equivalenza, dobbiamo vedere che è simmetrica, transitiva e riflessiva.

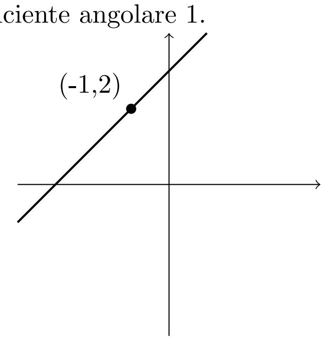
Osserviamo che la riflessività è ovvia in quanto $(a,b)\sigma(a,b)$ se e solo se $a+b = b+a$.

La simmetria è altrettanto immediata in quanto $(a,b)\sigma(c,d)$ se e solo se $a+d = b+c$ se e solo se $c+b = d+a$ se e solo se $(c,d)\sigma(a,b)$.

Per la transitività bisogna fare qualche calcolo in più. Supponiamo che $(a,b)\sigma(c,d)$ e che $(c,d)\sigma(e,f)$. Allora $a+d = b+c$ e $c+f = d+e$.

Si ha che $c = a+d-b$ e pertanto che $d+e = c+f = a+d-b+f$. Segue che $b+d+e = a+d+f$ da cui $b+e = a+f$, cioè che $(a,b)\sigma(e,f)$.

b) La classe di $(-1,2)$ modulo σ è l'insieme $\{(x,y) \in \mathbb{R}^2 \mid (-1,2)\sigma(x,y)\} = \{(x,y) \in \mathbb{R}^2 \mid -1+y = 2+x\} = \{(x,y) \in \mathbb{R}^2 \mid y = x+3\}$ che è la retta passante per $(3,0)$ di coefficiente angolare 1.



Esercizio 4

Dimostrare che per ogni $n \geq 1$ si ha

$$1^3 + 3^3 + \ldots + (2n-1)^3 = n^2(2n^2-1).$$

Soluzione

La dimostrazione procede per induzione su n.

Se $n = 1$ si ha che $1^3 = 1^2(2 \cdot 1^2 - 1)$ e il passo base è verificato.

Supponiamo di aver dimostrato che $1^3 + 3^3 + \ldots + (2n-1)^3 = n^2(2n^2-1)$ per qualche $n > 1$ e facciamo vedere che $1^3 + 3^3 + \ldots + (2n-1)^3 + (2n+1)^3 = (n+1)^2(2(n+1)^2-1)$.

A sinistra per ipotesi induttiva si ha che $1^3 + 3^3 + \ldots + (2n-1)^3 + (2n+1)^3 = n^2(2n^2-1) + (2n+1)^3 = 2n^4 - n^2 + 8n^3 + 12n^2 + 6n + 1 = 2n^4 + 8n^3 + 11n^2 + 6n + 1$.

Sviluppando a destra si ha $(n+1)^2(2(n+1)^2-1) = (n^2+2n+1)(2n^2+4n+1) = 2n^4 + 4n^3 + 2n^2 + 4n^3 + 8n^2 + 4n + n^2 + 2n + 1 = 2n^4 + 8n^3 + 11n^2 + 6n + 1$. Un semplice confronto tra i due risultati ottenuti ci fa concludere la dimostrazione.

Esercizio 5

Siano a e b due numeri interi fissati. Consideriamo la funzione $\varphi_{a,b}\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, $\varphi_{a,b}(x,y)=ax+by$.
a) Si discuta la iniettività di $\varphi_{a,b}$ al variare di a e b.
b) Si discuta la suriettività di $\varphi_{a,b}$ al variare di a e b.
c) Nel caso $a=4$, $b=6$ si calcoli un elemento dell'insieme $\varphi_{a,b}^{-1}(2)$.
d) Nel caso $a=4$, $b=6$ si descriva tutto l'insieme $\varphi_{a,b}^{-1}(2)$.

Soluzione

a) La funzione non è mai iniettiva. Infatti se $a=0$ e $b=0$ la funzione manda tutte le coppie di interi in 0 e pertanto non è iniettiva. Se invece uno tra a e b è diverso da zero, allora le coppie $(0,0)$ e $(-b,a)$ sono due elementi diversi del dominio. Ciononostante si ha che $\varphi_{a,b}(0,0)=0=\varphi_{a,b}(-b,a)$.
b) Se il massimo comune divisore tra a e b è 1, allora esistono due interi λ e μ tali che $\lambda a+\mu b=1$. In questo caso vogliamo far vedere che la funzione $\varphi_{a,b}$ è suriettiva. Infatti, dato un elemento x del codominio, la coppia $(x\lambda,x\mu)$ viene mandata in x (come si vede facilmente da $\varphi_{a,b}(x\lambda,x\mu)=x\lambda a+x\mu b=x(\lambda a+\mu b)=x\cdot 1=x$.

Viceversa se il massimo comune divisore tra a e b è maggiore di 1, vediamo che $\varphi_{a,b}$ non è suriettiva. Infatti se fosse suriettiva 1 apparterrebbe all'immagine, cioè esisterebbe una coppia di interi (x,y) tale che $\varphi_{a,b}(x,y)=1$, pertanto esisterebbe una coppia di interi (x,y) tale che $ax+by=1$. Ma $ax+by$ è divisibile per il massimo comune divisore di a e b che è maggiore di 1, contraddizione.

La contraddizione nasce dall'aver supposto che $\varphi_{a,b}$ sia suriettiva. Ne concludiamo che non lo è.
c) Si ha per esempio che $6-4=2$, cioè che $(-1)a+1\cdot b=2$. Pertanto $(-1,1)\in\varphi_{a,b}^{-1}(2)$.
d) Abbiamo una soluzione particolare $(-1)4+1\cdot 6=2$. Consideriamo ora una soluzione generale $4x+6y=2$. Scriviamo $x=-1+\alpha$ e $y=1+\beta$, da cui $-4+4\alpha+6+6\beta=2$, cioè $4\alpha+6\beta=0$, che è equivalente a $2\alpha=-3\beta$, cioè $\alpha=3n$, $\beta=-2n$ per qualche intero n. Pertanto tutte e sole le soluzioni di $4x+6y=2$ si ricavano aggiungendo alla soluzione particolare $(-1,1)$ un elemento del tipo $(3n,-2n)$. L'insieme cercato è quindi $\varphi_{a,b}^{-1}(2)=\{(-1+3n,1-2n)\mid n\in\mathbb{Z}\}$.

Esercizio 6

Si risolvano i seguenti sistemi di congruenze in $\mathbb{Z}$.

$$a)\begin{cases} 7x\equiv 12 \pmod{35} \\ x\equiv 12 \pmod{37} \end{cases} \qquad b)\begin{cases} x\equiv 29 \pmod{78} \\ 7x\equiv 3 \pmod{13} \end{cases}$$

Soluzione

a) La prima congruenza non ha soluzioni in quanto $MCD(7,35)=7$ che non divide 12. Nemmeno il sistema, quindi, ha soluzioni.
b) Risolviamo la seconda congruenza. In $\mathbb{Z}/13\mathbb{Z}$ la classe di 7 è invertibile con la classe di 2 come inverso, pertanto la seconda congruenza è equivalente a $2\cdot 7x\equiv 2\cdot 3 \pmod{13}$ che è equivalente a $x\equiv 6 \pmod{13}$. Pertanto le singole congruenze hanno soluzioni. Vediamo se il sistema ne ha.

Notiamo innanzitutto che $MCD(78,13)=13$ e che pertanto il teorema cinese del resto non ci assicura l'esistenza di soluzioni (ma potrebbero ciononostante esserci!).

Proviamo a trovarle: dobbiamo risolvere le congruenze $78x \equiv 6 \pmod{13}$ (che è equivalente a $0x \equiv 6 \pmod{13}$ e perciò non ha soluzione) e $13x \equiv 29 \pmod{78}$ (che non ha soluzione in quanto $MCD(13, 78) = 13$che non divide 29). Il sistema pertanto non ha soluzioni.