Elementi di Algebra e Logica (Geatti-Pareschi) 2^0 Appello di recupero,   21.9.2004

COGNOME........................   NOME...................................

Inserire le risposte negli spazi predisposti, accompagnadole con spiegazioni chiare ed essenziali. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

---

1. *Sia $F = \{n \in \mathbf{Z}$ tali che $n \equiv 0$ (mod 7)$\}$. (a) Stabilire quali tra i seguenti insiemi hanno la stessa cardinalità: $\mathbf{Z}$, $\mathbf{R}\times\mathbf{R}$, F, $\mathbf{Q}$, $\mathbf{R}$.*
(b) Tra gli insiemi del punto (a), sceglierne a piacere uno con la stessa cardinalità di F (diverso da F) e scrivere una funzione biettiva da tale insieme a F.

Si ha

$$F = \{n \in \mathbf{Z} \text{ tali che } n \equiv 0 \text{ (mod 7)}\} = \{n = 7k, \quad k \in \mathbf{Z}\}.$$

In particolare, F è in corrispondenza biunivoca con gli interi mediante l'applicazione

$$g: \mathbf{Z} \longrightarrow F, \quad k \mapsto 7k.$$

Gli insiemi $\mathbf{Z}$, $\mathbf{Q}$, F hanno tutti la stessa cardinalità che è quella del numerabile. Gli insiemi $\mathbf{R}$ e $\mathbf{R}\times\mathbf{R}$ hanno la stessa cardinalià, che è quella del continuo. La cardinalità del continuo è superiore a quella del numerabile, cosi gli insiemi $\mathbf{Z}$, $\mathbf{Q}$, F non hanno la stessa cardinalità degli insiemi $\mathbf{R}$ e $\mathbf{R}\times\mathbf{R}$.

2. *Sia A l'insieme dei numeri naturali maggiori o uguali a 2. Si consideri la relazione su A definita come segue: dati $a, b \in A$, si ha che aRb se e solo se $mcd(a,b) > 1$. (a) Stabilire, dimostrandole o mostrando un controesempio, se R gode delle seguenti proprietà: riflessività, simmetria, antisimmetria, transitività. (b) Determinare l'insieme di tutti gli elementi in relazione con 18.*

(a) R è riflessiva: per ogni $a > 1$, vale $mcd(a,a) = a > 1$;
(b) R è simmetrica: per ogni $a, b > 1$, vale $mcd(a,b) = mcd(b,a) > 1$;
(c) R non è antisimmetrica: $mcd(a,b) > 1$ e $mcd(b,a) > 1$ non implica $a = b$ (vedi (b) ...);
(d) R non è transitiva: $mcd(a,b) > 1$ e $mcd(b,c) > 1$ non implica $mcd(a,c) > 1$. Basta prendere ad esempio $a = 2$, $b = 6$, $c = 15$.

3. *Dimostrare per induzione che $n^3 + 3n^2 + 5n$ è divisibile per 3, per ogni $n \geq 1$.*

Chiamiamo $P(n)$ la proposizione "$n^3 + 3n^2 + 5n$ *è divisibile per* 3".
$P(1)$ è vera: infatti $1 + 3 + 5 = 9$ è divisibile per 3.
Dimostriamo che se $P(n)$ è vera (ipotesi induttiva), anche $P(n+1)$ è vera:

$$(n+1)^3 + 3(n+1)^3 + 5(n+1) = \ldots\ldots = (n^3 + 3n^2 + 5n) \; + \; 3n^2 + 9n + 9.$$

È evidente che $3n^2 + 9n + 9$ è divisibile per 3; dunque assumendo $n^3 + 3n^2 + 5n$ divisibile per 3, anche $(n+1)^3 + 3(n+1)^3 + 5(n+1)$ è divisibile per 3, come richiesto.

4. *Si consideri il sistema crittografico RSA di modulo $143\,(= 11 \cdot 13)$ ed esponente $D = 113$. (a) Cifrare il messaggio "54", cioè calcolare il resto della divisone per 143 del numero 54^{113}.*
(b) Determinare un esponente E che consenta di decifrare il messaggio precedente. In altre parole, determinare un numero naturale E tale che $(54^{113})^E \equiv 54$ (mod 143).

(a) Osserviamo che $x \equiv 54^{113} \mod 143$ se e solo se

$$\begin{cases} x \equiv 54^{113} \mod 11 \\ x \equiv 54^{113} \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv (-1)^{113} \mod 11 \\ x \equiv 2^{113} \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv (-1)^{3} \mod 11 \\ x \equiv 2^{5} \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv -1 \mod 11 \\ x \equiv 6 \mod 13. \end{cases}$$

Per calcolare le potenze qui sopra, abbiamo usato il fatto che il gruppo moltiplicativo $\mathbf{Z}_{11}^*$ ha ordine 10, che il gruppo moltiplicativo $\mathbf{Z}_{13}^*$ ha ordine 12 e poi abbiamo applicato il teorema di Lagrange (Piccolo Teorema di Fermat).

Le soluzioni del sistema di congruenze $\begin{cases} x \equiv -1 \mod 11 \\ x \equiv 6 \mod 13 \end{cases}$ sono date da tutti gli interi della forma $x = 32 + k143,\ k \in \mathbf{Z}$. Il resto cercato è dunque 32 (compreso fra 0 e 143) e il messaggio cifrato risulta appunto $\widetilde{m} = 32$.

(b) L'esponente cercato si trova risolvendo la congruenza

$$113 \cdot E \equiv 1 \mod (11-1)(13-1) \quad \Leftrightarrow \quad 113 \cdot E \equiv 1 \mod 120.$$

Poiché $mcd(113, 120) = 1$, la congruenza ha soluzione. Usando l'algoritmo euclideo, troviamo ad esempio $E = 17$.

5. *Si consideri la seguente proposizione:*
$P: \ \big(\exists x \in \mathbf{R} \forall y \in \mathbf{R}^+\ (x + y = 2 \vee xy > 0)\big) \wedge \big(\forall x \in \mathbf{R}(\exists y \in \mathbf{R}^+\ x + y > 0) \vee (\forall y \in \mathbf{R}^+\ x^2 y > 0)\big).$
(a) Stabilire se P è vera o falsa.
(b) Scrivere la negazione di P in modo che non ci siano negazioni davanti a quantificatori o ad espressioni contenenti connettivi logici.

(a) P è vera: sono vere infatti sia

$$\big(\exists x \in \mathbf{R} \forall y \in \mathbf{R}^+\ (x + y = 2 \vee xy > 0)\big)$$

che

$$\big(\forall x \in \mathbf{R}(\exists y \in \mathbf{R}^+\ x + y > 0) \vee (\forall y \in \mathbf{R}^+\ x^2 y > 0)\big).$$

Nel primo caso è facile vedere che esiste almeno un $x \in \mathbf{R}$ tale che $xy > 0$, per ogni $y \in \mathbf{R}^+$. (ad esempio $x = 1$). Nel secondo caso, si ha che per ogni $x \neq 0$, vale $x^2 y > 0$, per ogni $y \in \mathbf{R}^+$. D'altra parte, se $x = 0$, esiste $y \in \mathbf{R}^+$ tale che $x + y > 0$ (ad esempio $y = 2$). Cosi̇̀ anche la seconda proposizione è vera, e P è vera come richiesto.
(b) la negazione di P è data da

$$\big(\forall x \in \mathbf{R} \exists y \in \mathbf{R}^+\ (x + y \neq 2 \wedge xy \leq 0)\big) \vee \big(\exists x \in \mathbf{R}(\forall y \in \mathbf{R}^+\ x + y \leq 0) \wedge (\exists y \in \mathbf{R}^+\ x^2 y \leq 0)\big).$$