Algebra e Logica (Schoof) 5^o appello 28 agosto 2018, ore 10:00–12:00.

COGNOME ..... *NOME* .....

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 5 punti.

1. (a) Sia n quadrato di un numero primo. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?
   (b) Sia n prodotto di due primi dispari distinti. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?

2. Un *numero di Carmichael* è un numero naturale n che è composto, e per cui si ha che $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$. Dimostrare che $561 = 3 \cdot 17 \cdot 11$ è un numero di Carmichael.

3. Sia A un insieme di cardinalità 8 e sia $R \subset A \times A$ una relazione. Supponiamo che R sia una relazione di equivalenza ed anche un ordinamento parziale. Quante classi di equivalenza ci sono?

4. Determinare il resto della divisione di 101^{103} per 107. (I numeri 101, 103 e 107 sono primi.)

5. La banca usa il sistema RSA per comunicare con i clienti. Il modulo è uguale per tutti i clienti e ogni cliente A ha la sua chiave pubblica personale E_A, che è sempre un numero primo. Supponiamo che due clienti A e B cifrino lo stesso messaggio m con loro chiavi personali. Se un avversario intercetta i due messaggi cifrati, come può velocemente recuperare il messaggio originale m?

6. Siano x, y, z variabili Booleane. Dimostrare che le seguenti espressioni Booleane non sono equivalenti, esibendo espliciti controesempi:
   (a) $\forall y \, \forall x \, \exists z \, f(x, y, z)$;
   (b) $\forall x \, \exists z \, \forall y \, f(x, y, z)$;
   (c) $\exists z \, \forall x \, \forall y \, f(x, y, z)$.
   (Sugg. Per esempio, le espressioni Booleane $\forall u \, \exists v \, f(u, v)$ e $\exists v \, \forall u \, f(u, v)$ non sono equivalenti, perché se prendo per $f(u, v)$ la formula $u = v$, allora la prima affermazione è vera, ma la seconda no).

Soluzioni.

1. Questo è l'esercizio 6 del foglio 5.
2. Questo è l'esercizio 7 del foglio 3.
3. Se $a, b \in A$, con $(a, b) \in R$, allora per simmetria anche $(b, a) \in R$. L'anti-simmetria implica quindi che $a = b$. Le classi di equivalenza sono quindi $\{a\}$, per $a \in A$. Ce ne sono otto.
4. $101^{103} \equiv (-6)^{-3} \equiv -\frac{1}{216} \equiv -\frac{1}{2} \equiv 53 \pmod{107}$.
5. L'avversario intercetta m^{E_A} e m^{E_B}. Poiché conosce anche le chiavi pubbliche E_A e E_B, può usare l'algoritmo euclideo per calcolare velocemente $u, v \in \mathbf{Z}$ con $uE_A + vE_B = 1$ e dedurre $(m^{E_A})^u (m^{E_B})^v = m^{uE_A + vE_B} = m$.
6. Per $f(x, y, z) = (x = z)$, le affermazioni (a) e (b) sono vere, mentre (c) è falsa. Quindi (c) non è equivalente ad (a) e neanche a (b). Per $f(x, y, z) = (y = z)$, l'affermazione (a) è vera, ma (b) no. Quindi, (a) e (b) non sono equivalenti.