ALGEBRA E LOGICA (Pareschi e Schoof) 2º esonero Roma 30 aprile 2003, 14:00–15:30.

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

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare ed essenziali.* NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 7.5 punti.

1. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 53$.
   (a) Cifrare il messaggio "24", cioè calcolare il resto della divisione per 143 del numero 24^{53} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 24^{53});
   (b) Determinare un esponente E che consente di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(24^{53})^E \equiv 24 \pmod{143}$.

(a) Siccome $53 \equiv 3 \pmod{10}$, abbiamo per il Teorema di Fermat che $x = 24^{53} \equiv 2^3 \equiv 8 \pmod{11}$. Similmente, $53 \equiv 5 \pmod{12}$ e quindi $x = 24^{53} \equiv (-2)^5 \equiv -32 \equiv 7 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 85 \pmod{143}$. (b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 53 \equiv 1 \pmod{10 \cdot 12}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$\begin{aligned}
1 \cdot 120 + 0 \cdot 53 &= 120,\\
0 \cdot 120 + 1 \cdot 53 &= 53,\\
1 \cdot 120 - 2 \cdot 53 &= 14,\\
-3 \cdot 120 + 7 \cdot 53 &= 11,\\
4 \cdot 120 - 9 \cdot 53 &= 3,\\
-15 \cdot 120 + 34 \cdot 53 &= 2,\\
19 \cdot 120 - 43 \cdot 53 &= 1.
\end{aligned}$$

L'esponente cercato è quindi $E = -43 + 120 = 77$.

2. Sia $f : \mathbf{N} \to \mathbf{Z}$ una funzione fissata.
   (a) Esprimere la proposizione "*f è iniettiva*" usando quantificatori e connettivi logici.
   (b) Esprimere la proposizione "*f non è iniettiva*" usando quantificatori e connettivi logici, in modo tale che non ci siano negazioni davanti a quantificatori.

(a) $\forall x \in \mathbf{N} \forall y \in \mathbf{N}\ x \neq y \to f(x) \neq f(y)$
oppure: $\forall x \in \mathbf{N} \forall y \in \mathbf{N}\ f(x) = f(y) \to x = y$.
(b) $\exists x \in \mathbf{N} \exists y \in \mathbf{N} (x \neq y) \wedge (f(x) = f(y))$

3. In un'algebra di Boole si consideri l'operazione $x \oplus y := xy' + x'y$.
   (a) Esprimere l'espressione booleana $(xy) \oplus (z \oplus x')$ come somma di prodotti.
   (b) Determinare un'espressione *minimale* come somma di prodotti dell'espressione booleana $(xy) \oplus (z \oplus x')$.

(a) $(xy) \oplus (z \oplus x') = (xy)(z \oplus x')' + (xy)'(z \oplus x')$
$\stackrel{DN}{=} (xy)(zx + z'x')' + (xy)'(zx + z'x')$
$\stackrel{DM}{=} (xy)(zx)'(z'x')' + (x' + y')(zx + z'x')$
$\stackrel{DM+DN}{=} (xy)(z' + x')(z + x) + (x' + y')(zx + z'x')$
$\stackrel{D}{=} xyz'z + xyz'x + xyx'z + xyx'x + x'zx + x'z'x' + y'zx + y'z'x'$
$\stackrel{C+Co+I}{=} xy0 + xyz' + 0yz + 0xy + 0z + x'z' + xy'z + x'y'z'$
$\stackrel{L}{=} xyz' + x'z' + xy'z + x'y'z' \stackrel{A}{=} xyz' + x'z' + xy'z.$

(dove: DN=doppia negazione, DM=De Morgan, D=distributività, C=commutatività, Co=complemento, I=idempotenza, L= limitatezza, A=assorbimento).

(Alternativamente, si può pervenire al risultato trovando esplicitamente la "tabella di verità" dell'espressione, pervenendo direttamente alla espressione in somma di prodotti completata: $xyz' + x'yz' + x'y'z' + xy'z$.)

(b) Il consenso dei prodotti fondamentali xyz' e $x'z'$ è yz'. quindi l'espressione di (a) è equivalente a $xyz' + x'z' + xy'z + yz' \stackrel{A}{=} x'z' + xy'z + yz'$.

4. Dato un numero naturale m, si denoti $\mathbf{D}_n = \{k \in \mathbf{N} : k \text{ divide } m\}$. Si consideri il reticolo $(\mathbf{D}_m, \wedge, \vee)$, dove $k \wedge h = \text{mcd}(k, h)$ e $k \vee h = \text{mcm}(k, h)$ per $k, h \in \mathbf{D}_n$.
   (a) Stabilire se $\mathbf{D}_{42}$ è un reticolo con complemento. In caso affermativo stabilire se è un reticolo con complemento unico.
   (b) Stabilire se $\mathbf{D}_{45}$ è un reticolo con complemento. In caso affermativo stabilire se è un reticolo con complemento unico.

(a) $\mathbf{D}_{42}$ è un reticolo con complemento unico. Infatti dal fatto che $42 = 2 \cdot 3 \cdot 7$ è prodotto di primi distinti, segue che , dato $x \in \mathbf{D}_{42}$, $x' := 42/x$ è tale che $mcm = (x, x') = 42$ e $mcd(x, x') = 1$ ed e' l'unico elemento di $\mathbf{D}_{42}$ tale proprietà.
(b) $\mathbf{D}_{45}$ non è un reticolo con complemento. Per esempio, 3 non ha complemento. Infatti l'unico elemento $y \in \mathbf{D}_{45}$, diverso da 1, tale che $mcd(3, y) = 1$ è 5, ma $mcm(3, 5) \neq 45$.