ALGEBRA E LOGICA (Geatti) 2^o esonero Roma, 3 febbraio 2009, ore 9,30 – 11,30.

Cognome .... **Nome** ....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 5 punti.

1. *Calcolare il resto della divisione di* 3456^{452} *per 7.*

Sol. Osserviamo innazitutto che $3456 \equiv 5 \mod 7$. Inoltre, poiché 7 è primo, per il Piccolo Teorema di Fermat vale $5^6 \equiv 1 \mod 7$. In totale abbiamo

$$3456^{452} \equiv 5^{452} \equiv 5^{6\cdot 75} \cdot 5^2 \equiv 4 \mod 7.$$

2. *Scrivere l'enunciato del Piccolo Teorema di Fermat. Usando il Piccolo Teorema di Fermat, verificare che* $n = 12$ *non è primo.*

Sol. PTF: Sia p un numero primo. Allora $x^{p-1} \equiv 1 \mod p$, per ogni $x \in \mathbb{Z}$ con $mcd(x,p) = 1$. Per verificare che 12 non è primo basta esibire un intero x, con $mcd(x,12) = 1$, tale che $x^{11} \not\equiv 1 \mod 12$. Ad esempio, per $x = 5$ troviamo $5^{11} \equiv 5 \mod 12$. Ciò conferma che 12 non è un numero primo.

3. *Il signor Rossi desidera ricevere messaggi criptati e adotta il criptosistema RSA.*
   (a) Preparare per il signor Rossi un kit di chiavi pubbliche N, E e chiave segreta D, con $N = 51$ e $D = 7$.
   (b) Il signor Rossi riceve il messaggio criptato $m = 13$. Lo decripta con la sua chiave segreta. Cosa trova?
   (c) Vogliamo inviare al signor Rossi il messaggio $m = 19$ e lo criptiamo. Che cosa gli inviamo?

Sol. (a) La chiave pubblica $N = 51$ è il prodotto dei primi $p = 3$ e $q = 17$. La chiave mancante E è data dall'inverso di D modulo $(p-1)(q-1) = 2 \cdot 16 = 32$:

$$E \equiv D^{-1} \equiv 23 \text{ mod } 32.$$

(b) Rossi calcola

$$m^D \equiv 13^7 \equiv 4 \mod 51.$$

Dunque il messaggio decriptato è 4.
(c) Il messaggio criptato che spediamo a Rossi è

$$m^E \equiv 19^{23} \equiv 43 \mod 51.$$

4. *Si consideri il reticolo (D_{30}, mcd, mcm).*
   (a) Verificare che $6 \in D_{30}$ e determinare $\{x \in D_{30} \mid x\text{“} \leq \text{”}6\}$, dove “ $\leq$ ” è la relazione di ordine parziale indotta su D_{30} dalle operazioni di reticolo.
   (b) Determinare limite inferiore e limite superiore di D_{30}.
   (c) Determinare se D_{30} è un reticolo complementato e se il complemento è unico (per ogni elemento di D_{30} esibire un eventuale complemento).

Sol. (a) Abbiamo che $30 = 2 \cdot 3 \cdot 5$ e il reticolo dei divisori di 30 è dato da

$$D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

In particolare $6 \in D_{30}$. La relazione di ordine parziale indotta dalle operazioni di reticolo è data da $a\text{“} \leq \text{”}b$ se $mcd(a,b) = a$, e ciò equivale a richiedere che a divide b: $a|b$. L'insieme $\{x \in D_{30} \mid x\text{“} \leq \text{”}6\}$ coincide con l'insieme dei divisori di 6: $\{, 1, 2, 3, 6\}$.
(b) Il limite inferiore di D_{30} è 1: infatti $mcd(1,a) = 1$, per ogni $a \in D_{30}$;

Il limite inferiore di D_{30} è 30: infatti $mcd(a, 30) = a$, per ogni $a \in D_{30}$.
(Vedi anche il diagramma di Hasse che è un "cubo" sospeso per uno dei vertici)

(c) Poiché 30 è il prodotto di tre primi distinti, D_{30} è un reticolo booleano: è limitato, distributivo e complementato. Ne segue che il complemento di ogni elemento è unico: $\bar{a} = \frac{30}{a}$.
Si verifica infatti che $mcd(a, \frac{30}{a}) = 1$ e $mcm(a, \frac{30}{a}) = 30$.
Nel nostro caso abbiamo: $\bar{1} = 30$, $\bar{2} = 15$, $\bar{3} = 10$, $bar5 = 6$.

5. *In un'algebra di Boole $(A, +, \cdot, ')$ siano date le espressioni Booleane*
$E: \ xz + xy'z' + xyz' \qquad\qquad F: \ xyz + x'z + yz'.$
   (a) Determinare se E ed F sono equivalenti;
   (b) Determinare se F è somma di implicanti primi;
   (c) Determinare se F è in forma minimale.

Sol. (a) Passando alla forma normale disgiuntiva (che è *unica*) delle due espressioni, troviamo rispettivamente

$$E \sim xyz + xy'z + xy'z' + xyz', \qquad\qquad F \sim xyz + x'yz + x'y'z + xyz' + x'yz'.$$

Poiché le espressioni trovate sono diverse, E ed F non sono equivalenti.
(b) Poiché si possono applicare dei passi non banali del metodo del consenso ad F, possiamo subito concludere che $F: \ xyz + x'z + yz'$ non è somma di implicanti primi.
(c) (c) In particolare $F: \ xyz+x'z+yz'$ non è in forma minimale (ogni forma minimale è somma di implicanti primi).

Applicando il metodo del consenso ad $F: \ xyz + x'z + yz'$, troviamo:

$$Q_{12} = yz, \qquad F + Q_{12} = xyz + x'z + yz' + yz = x'z + yz' + yz = x'z + (z + z')y = x'z + y.$$

Dunque $x'z + y$ è somma di tutti gli implicanti primi di F.
Completando i due termini, troviamo

$$x'z(y + y') = x'yz + x'y'z, \qquad (x + x')(z + z')y = xyz + xyz' + x'yz + x'yz'.$$

Poiché nessune dei due è "contenuto" nell'altro, abbiamo che $x'z + y$ è anche una forma minimale.

6. *Sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione data da $f(t) = e^t$. Considerare il seguente enunciato*
$P(t): \qquad \forall y \in]0, +\infty[\ \ \exists t \in \mathbb{R}: \ f(t) = y \bigwedge t > 0.$
   (a) Determinare se $P(t)$ è vero;
   (b) Determinare la negazione di $P(t)$ (non ci devono essere negazioni davanti ad un quantificatore o davanti ad un'espressione contenente connettivi logici).

Sol. (a) In parole povere $P(t)$ dice che la funzione esponenziale ristretta ai reali positivi $\exp :]0, +\infty[\to]0, +\infty[$ è suriettiva. Questo è falso: infatti la funzione esponenziale non assume nessun valore $y \ \in]0, 1]$ sui reali positivi.
(b) La negazione di $P(t)$ è la seguente:

$$\neg P(t): \quad \exists y \in]0, +\infty[\ \ \forall t \in \mathbb{R}: \ f(t) \neq y \bigvee t \leq 0.$$