COGNOME .... **NOME** .... Data di nascita.................. Risolvere gli esercizi negli spazi predisposti. Tutte le risposte devono essere motivate da spiegazioni *chiare ed essenziali.* Non verranno valutate affermazioni non motivate. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 6 punti.

1. Sia $a \in \mathbf{R}$ tale che $0 < a < 1$. Dimostrare per induzione che $(1-a)^n < \frac{1}{1+na}$, per ogni $n \geq 1$.

Soluzione. Sia $a \in (0,1)$. Passo base: Per $n = 1$ la disuguaglianza da dimostrare e': $1 - a < \frac{1}{1+a}$, che si verifica osservando che, moltiplicando e dividendo il primo membro per $1 + a$, essa è equivalente a $\frac{1-a^2}{1+a} < \frac{1}{1+a}$, e quindi a $1 - a^2 < 1$.
Passo induttivo: l'ipotesi e': $(1-a)^n < \frac{1}{1+na}$. La tesi e': $(1-a)^{n+1} < \frac{1}{1+(n+1)a}$.
Per dimostrare la tesi, si scrive il primo membro $(1-a)^{n+1} = (1-a)^n(1-a)$. Per ipotesi induttiva (e usando che $1 - a > 0$), si ha che $(1-a)^{n+1} = (1-a)^n(1-a) < \frac{1-a}{1+na}$. Dunque, per dimostrare la tesi, e' sufficiente dimostrare che: $\frac{1-a}{1+na} \leq \frac{1}{1+(n+1)a}$, per ogni $n \geq 1$. Portando i membri di quest'ultima disuguaglianza a comune denominatore, si vede che essa e' equivalente a

$$\frac{(1-a)(1+(n+1)a)}{(1+na)(1+(n+1)a} \leq \frac{1+na}{(1+na)(1+(n+1)a)},$$

e quindi a: $(1-a)(1+(n+1)a) < 1 + na$, cioé: $1 + na - (n+1)a^2 < 1 + na$, che è banalmente vera per ogni $n \geq 1$.

2. Dato un numero naturale n, si denoti, come al solito, $\mathbf{D}_n = \{k \in \mathbf{N} \mid k \text{ divide } n\}$.
Sia $A = \mathbf{D}_6 \times \mathbf{D}_{15}$. Si considerino le relazioni R ed S su A cosı̀ definite: dati (a,b) e (c,d) in A:
(i) $(a,b)\,R\,(c,d)$ se $m.c.m.(a,b) = m.c.m.(c,d)$; e (ii) $(a,b)\,S\,(c,d)$ se $m.c.m.(a,c) = m.c.m.(b,d)$.
(a) Stabilire se R è una relazione di equivalenza su A e, in caso affermativo, descrivere esplicitamente tutte le classi di equivalenza. (b) Stabilire se S è una relazione di equivalenza su A e, in caso affermativo, descrivere esplicitamente tutte le classi di equivalenza.

Soluzione. (a) Rifessività: dato $(a,b) \in A$, $m.c.m.(a,b) = m.c.m.(a,b)$;
Simmetria: dati $(a,b),(c,d) \in A$, se $m.c.m.(a,b) = m.c.m.(c,d)$ allora $m.c.m.(c,d) = m.c.m.(a,b)$.
Transitività: dati $(a,b),(c,d),(e,f) \in A$, se $m.c.m.(a,b) = m.c.m.(c,d)$ e $m.c.m.(c,d) = m.c.m.(e,f)$ allora $m.c.m.(a,b) = m.c.m.(e,f)$.
Quindi R è una relazione di equivalenza su A.
Le classi di equivalenza corrispondono a tutti i $m.c.m.$ tra un elemento di D_6 e un elemento di $\mathbf{D_{15}}$. Risultano essere otto, e precisamente:

$$\{(1,1)\}, \quad \{(1,3),(3,3),(3,1)\}, \quad \{(1,5)\}, \quad \{(1,15),(3,5),(3,15)\}, \quad \{(2,1)\},$$
$$\{(2,3),(6,1),(6,3)\}, \quad \{(2,5)\}, \quad \{(2,15),(6,5),(6,15)\}$$

3. Determinare tutti gli $x \in \mathbf{Z}$ tali che $\begin{cases} x \equiv 58^{193} & \pmod{55} \\ 2x \equiv 6 & \pmod{8} \end{cases}$

Soluzione. Innanzitutto si osservi che la seconda equazione è equivalente a: $x \equiv 3 \pmod 4$. Dunque, per il Teorema Cinese dei Resti, la soluzione è unica modulo $55 \cdot 4 = 220$.
Si ha che $58 \equiv 3 \pmod{55}$. Per il teorema cinese dei resti, l'equazione $x \equiv 3^{193} \pmod{55}$ èd equivalente al sistema $\begin{cases} x \equiv 3^{193} & \pmod 5 \\ x \equiv 3^{193} & \pmod{11} \end{cases}$. Poichè, $193 \equiv 1 \pmod 4$, per il Teorema di Fermat, $3^{193} \equiv 3 \pmod 5$.

Allo stesso modo, $3^{193} \equiv 3^3 \equiv 5 \pmod{11}$. In conclusione, il sistema è equivalente a: $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod 4 \end{cases}$.

Si trova che la soluzione è $x = 203 + 220k$, $k \in \mathbf{Z}$.

4. Si consideri il reticolo $A = \mathbf{D}_4 \times \mathbf{D}_6$, ordinato mediante la relazione "$\leq$" seguente: dati (a, b) e (c, d) in A, $(a, b) \leq (c, d)$ se a divide c e b divide d.
(a) Determinare gli elementi irriducibili e gli atomi di A. (b) Stabilire quali dei seguenti reticoli sono isomorfi tra loro: A, $\mathbf{D}_{60}$, $\mathbf{D}_{72}$ e, in caso di reticoli isomorfi, stabilire quanti sono gli isomorfismi ed esibirne esplicitamente uno. (c) Esibire, se esiste, un elemento di A senza complemento.

Soluzione. (a) Atomi: $(1, 2)$, $(1, 3)$, $(2, 1)$. Irriducibili: $(1, 2)$, $(1, 3)$, $(2, 1)$, $(4, 1)$.
(b) $\mathbf{D}_{60}$ e $\mathbf{D}_{72}$ non sono isomorfi, perchè hanno fattorizzazioni in primi di tipo diverso: $60 = 2^2 \cdot 3 \cdot 5$, $72 = 2^3 \cdot 3^2$. Oppure, più semplicemnte, perchè, ad esempio, $\mathbf{D}_{60}$ ha tre atomi, mentre $\mathbf{D}_{72}$ solo due.
Si vede invece che A e $\mathbf{D}_{60}$ sono isomorfi. Gli isomorfismi sono due. Per vedere ciò, si osservi che l'atomo $(2, 1)$ di A deve corrispondere necessariamente all'atomo 2 di $\mathbf{D}_{60}$, in quanto, al di sopra di esso c'è l'irriducibile (non atomo) $(4, 1)$ di A , che deve corrispondere necessariamente all'irriducibile (non atomo) 4 di $\mathbf{D}_{60}$. Quindi un isomorfismo tra A e $\mathbf{D}_{60}$ deve mandare $(1, 2)$ in 3 e $(1, 3)$ in 5 o, viceversa, $(1, 2)$ in 5 e $(1, 3)$ in 2. Vi sono quindi solo due possibilità.
Esplicitamente, nel primo caso, si ottiene l'isomorfismo $f : A \to \mathbf{D}_{60}$ così definito: $f((1, 1)) = 1$, $f((1, 2)) = 3$, $f((1, 3)) = 5$, $f((2, 1)) = 2$, $f((4, 1)) = 4$, $f((1, 6)) = 15$, $f((2, 2)) = 6$, $f((2, 3)) = 10$, $f((2, 6)) = 30$, $f((4, 2)) = 24$, $f((4, 3)) = 20$, $f((4, 6)) = 60$.
(c) Ad esempio, $(2, 1)$ (se non lo si vede direttamente, ci si può aiutare usando quanto si sa sul reticolo $\mathbf{D}_{60}$).

5. Si consideri la funzione booleana $F(x, y, z) = xy' + xyz' + x'yz'$.
(a) Scrivere $F(x, y, z)$ come somma di tutte le sue implicanti prime.
(b) Determinare un'espressione minimale di $F(x, y, z)$.

Soluzione. (a) Applicando il metodo del consenso:
$xy' + xyz' + x'yz' = xy' + xyz' + x'yz' + xz' = xy' + x'yz' + xz' = xy' + x'yz' + xz' + yz' = xy' + xz' + yz'$. Il metodo del consenso non può essere più applicato. Quindi xy', xz', yz' sono le implicanti prime di $F(x, y, z)$.
(b) $xy' = xy'z + xy'z'$. $xz' = xyz' + xy'z'$. $yz' = xyz' + x'yz'$.
Solo gli addendi $xyz' + xy'z'$ di xz' appaiono tra gli altri addendi, e quindi xz' è superfluo. Dunque $xy' + yz'$ è un'espressione minimale di $F(x, y, z)$.