PRIMA PROVETTA DI ALGEBRA A
TRENTO, 16 APRILE 2020

Istruzioni:

(1) Questo compito consiste di **due facciate** e **sei esercizi**.
(2) Risolvete *tutti* gli esercizi seguenti.
(3) *Giustificate*, possibilmente in modo *conciso ed esauriente*, le risposte che date:
   (a) dovete *dimostrare* solo quello che vi chiediamo esplicitamente di dimostrare;
   (b) ma se fate uso di un risultato, *citatelo* esplicitamente.
(4) **Scrivete** nome, cognome e numero di matricola su ogni singola pagina che consegnate.
(5) **Scrivete la soluzione di ogni esercizio su una pagina** (o più pagine) **a parte:** un solo esercizio per ogni pagina. Scrivete in testa a ogni pagina l'intestazione "Esercizio x", se la risoluzione dell'Esercizio x sta tutta in quella pagina, altrimenti "Esercizio x.1", "Esercizio x.2', ecc. se l'esercizio viene svolto su più pagine
(6) Alla fine
   (a) **fate una scansione (va benissimo usare una delle tante app per smartphone) separata di ogni esercizio** in file PDF o JPEG,
   (b) date ai file i nomi
      (i) `CognomeNome1.pdf`, `CognomeNome2.pdf`, ecc., oppure
      (ii) `CognomeNome1.jpg`, `CognomeNome2.jpg`, ecc.,
   (c) **inviate come allegati entro mezz'ora dal termine della prova** (termine che a sua volta è tre ore dopo la dichiarazione ufficiale (!) di inizio)
      (i) le soluzioni degli esercizi 1-3 a `andrea.caranti@unitn.it`, e
      (ii) le soluzioni degli esercizi 4-6 a `s.ugolini@unitn.it`

Esercizio 1.

(1) Si diano le definizioni di massimo comun divisore e minimo comune multiplo di due interi.
(2) Si enuncino i quattro lemmi aritmetici.
(3) Si dimostri la formula

$$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

per ogni $a, b \in \mathbf{Z}$, con $a, b \geq 0$.

Esercizio 2. Sia $n \geq 2$ un intero.

(1) Si definisca la relazione di congruenza modulo n.
(2) Per $a \in \mathbf{Z}$, si definisca la classe di congruenza $[a]$ di a modulo n, e si dica da quali elementi è composta.
(3) Siano $a, r \in \mathbf{Z}$, con $0 \leq r < n$. Si mostri che sono equivalenti
   (a) $[a] = [r]$, e
   (b) r è il resto della divisione di a per n.

Esercizio 3.

(1) Sia A un anello con unità, $a \in A$.
   (a) Si dica quando a è invertibile.
   (b) Nel caso A sia commutativo, si dica quando a è uno 0-divisore.
(2) Sia $n \geq 2$ un intero, e $\mathbf{Z}/n\mathbf{Z}$ l'insieme delle classi di congruenza modulo n. Sia $a \in \mathbf{Z}$. Si mostri che vale
   (a) $[a]$ è invertibile in $\mathbf{Z}/n\mathbf{Z}$ se e solo se $\gcd(a, n) = 1$
   (b) $[a]$ è uno 0-divisore in $\mathbf{Z}/n\mathbf{Z}$ se e solo se $\gcd(a, n) > 1$

Esercizio 4.

(1) Sia $A \neq \emptyset$ un insieme, R una relazione di equivalenza su A, e per ogni $a \in A$ sia $[a] = \{ x \in A : xRa \}$ la sua classe di equivalenza.
   (a) Si mostri che $a \in [a]$ per ogni $a \in A$.
   (b) Si mostri che per $a, b \in A$ sono equivalenti
      (i) aRb,
      (ii) $a \in [b]$,
      (iii) $[a] \subseteq [b]$, e
      (iv) $[a] = [b]$.
   (c) Si mostri che $A/R = \{ [a] : a \in A \}$ è una partizione di A.
(2) Si enunci e si dimostri il (primo) teorema di biiezione fra insiemi.

Esercizio 5. Si dica se i seguenti sistemi di congruenze sono risolubili, e in caso affermativo se ne trovino *tutte* le soluzioni.

$$\begin{cases} x \equiv 11 \pmod{13} \\ x \equiv 28 \pmod{55} \end{cases} \quad \begin{cases} x \equiv 18 \pmod{396} \\ x \equiv 28 \pmod{253} \end{cases} \quad \begin{cases} x \equiv 17 \pmod{396} \\ x \equiv 28 \pmod{253} \end{cases}$$

Esercizio 6.

(1) Si definisca la funzione φ di Eulero.
(2) Si enunci il primo teorema di isomorfismo di anelli.
(3) Siano $m, n \geq 2$ interi tali che $\gcd(m, n) = 1$.
   (a) Si usi il primo teorema di isomorfismo di anelli per mostrare che la funzione
   $$f : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$
   $$[x]_{mn} \mapsto ([x]_m, [x]_n)$$
   è un isomorfismo di anelli.
   (b) Si mostri che f stabilisce una biiezione fra
   $$U(\mathbf{Z}/mn\mathbf{Z})$$
   e
   $$U(\mathbf{Z}/m\mathbf{Z}) \times U(\mathbf{Z}/n\mathbf{Z}) \subseteq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$
   (c) Se ne deduca la formula
   $$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{se } \gcd(m, n) = 1$$
   per la funzione di Eulero.

.