PRIMA PROVETTA DI ALGEBRA
TRENTO, 16 OTTOBRE 2015

Nota: Questi sono gli esercizi delle quattro diverse versioni della provetta che sono state assegnate. L'esercizio $x.y$ è l'esercizio x della versione y.

Esercizio 1.1. Si mostri che gli unici numeri interi che dividono ogni numero intero sono 1 e -1.

Esercizio 1.2. Si mostri che 0 è l'unico numero intero che sia divisibile per ogni numero intero.

Esercizio 1.3. Si mostri che gli unici numeri interi che dividono ogni numero intero sono 1 e -1.

Esercizio 1.4. Si mostri che 0 è l'unico numero intero che sia divisibile per ogni numero intero.

Esercizio 2.1. Si definisca la relazione di congruenza modulo n sugli interi.

Per ogni $a \in \mathbf{Z}$, sia $[a] = \{ x \in \mathbf{Z} : x \equiv a \pmod{n} \}$ la sua classe di congruenza.

Si mostri che $[a] = \{ a + n \cdot t : t \in \mathbf{Z} \}$.

(**Attenzione!** *Non ci si può appellare a risultati generali sulle relazioni di equivalenza, occorre usare direttamente la definizione.*)

Esercizio 2.2. Si definisca la relazione di congruenza modulo n sugli interi.

Si mostri, *usando direttamente la definizione*, che la congruenza è una relazione di equivalenza.

(**Attenzione!** *Non ci si può appellare a risultati generali sulle relazioni di equivalenza, occorre usare direttamente la definizione.*)

Esercizio 2.3. Si definisca la relazione di congruenza modulo n sugli interi.

Sia $n > 0$. Si mostri che sono equivalenti, per $a, b \in \mathbf{Z}$:

(1) $a \equiv b \pmod{n}$;
(2) a e b divisi per n danno lo stesso resto.

(**Attenzione!** *Non ci si può appellare a risultati generali sulle relazioni di equivalenza, occorre usare direttamente la definizione.*)

Esercizio 2.4. Si definisca la relazione di congruenza modulo n sugli interi.

Sia $n > 0$, e sia $[a] = \{ x \in \mathbf{Z} : x \equiv a \pmod{n} \}$ la classe di congruenza di $a \in \mathbf{Z}$ modulo n. Si mostri che sono equivalenti

(1) $a \equiv b \pmod{n}$;
(2) $[a] = [b]$.

(**Attenzione!** *Non ci si può appellare a risultati generali sulle relazioni di equivalenza, occorre usare direttamente la definizione.*)

Esercizio 3.1. Si dia la definizione di elementi invertibili e 0-divisori in un anello commutativo con unità.

Si *enunci* la caratterizzazione degli elementi invertibili e 0-divisori in $\mathbf{Z}/n\mathbf{Z}$, per $n \geq 2$.

Si consideri $n = 841$.

Per ognuna delle classi $[a] = [217], [348] \in \mathbf{Z}/n\mathbf{Z}$, si dica

- se $[a]$ è invertibile (esibendo in tal caso come "prova" l'inverso), oppure
- se $[a]$ è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Si calcoli anche il minimo comune multiplo

- fra 841 e 217, e
- fra 841 e 348,

spiegando quale formula si usa.
(**Attenzione!** *In questo esercizio è* obbligatorio *usare l'algoritmo di Euclide esteso, e riportare tutti i passaggi.*)

Esercizio 3.2. Si dia la definizione di elementi invertibili e 0-divisori in un anello commutativo con unità.

Si *enunci* la caratterizzazione degli elementi invertibili e 0-divisori in $\mathbf{Z}/n\mathbf{Z}$, per $n \geq 2$.

Si consideri $n = 841$.

Per ognuna delle classi $[a] = [209], [667] \in \mathbf{Z}/n\mathbf{Z}$, si dica

- se $[a]$ è invertibile (esibendo in tal caso come "prova" l'inverso), oppure
- se $[a]$ è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Si calcoli anche il minimo comune multiplo

- fra 841 e 209, e
- fra 841 e 667,

spiegando quale formula si usa.
(**Attenzione!** *In questo esercizio è* obbligatorio *usare l'algoritmo di Euclide esteso, e riportare tutti i passaggi.*)

Esercizio 3.3. Si dia la definizione di elementi invertibili e 0-divisori in un anello commutativo con unità.

Si *enunci* la caratterizzazione degli elementi invertibili e 0-divisori in $\mathbf{Z}/n\mathbf{Z}$, per $n \geq 2$.

Si consideri $n = 841$.

Per ognuna delle classi $[a] = [69], [580] \in \mathbf{Z}/n\mathbf{Z}$, si dica

- se $[a]$ è invertibile (esibendo in tal caso come "prova" l'inverso), oppure
- se $[a]$ è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Si calcoli anche il minimo comune multiplo

- fra 841 e 69, e
- fra 841 e 580,

spiegando quale formula si usa.
(**Attenzione!** *In questo esercizio è* obbligatorio *usare l'algoritmo di Euclide esteso, e riportare tutti i passaggi.*)

Esercizio 3.4. Si dia la definizione di elementi invertibili e 0-divisori in un anello commutativo con unità.

Si *enunci* la caratterizzazione degli elementi invertibili e 0-divisori in $\mathbf{Z}/n\mathbf{Z}$, per $n \geq 2$.

Si consideri $n = 841$.

Per ognuna delle classi $[a] = [211], [551] \in \mathbf{Z}/n\mathbf{Z}$, si dica

- se $[a]$ è invertibile (esibendo in tal caso come "prova" l'inverso), oppure
- se $[a]$ è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Si calcoli anche il minimo comune multiplo

- fra 841 e 211, e
- fra 841 e 551,

spiegando quale formula si usa.
(**Attenzione!** *In questo esercizio è* obbligatorio *usare l'algoritmo di Euclide esteso, e riportare tutti i passaggi.*)

Esercizio 4.1. Si dica se i seguenti sistemi di congruenze sono risolubili, spiegando perché. Qualora un sistema abbia soluzione, *le si trovino tutte*, giustificando la risposta.

$$\begin{cases} x \equiv 1 & \pmod{217} \\ x \equiv 15 & \pmod{203} \end{cases} \qquad \begin{cases} x \equiv 11 & \pmod{217} \\ x \equiv 24 & \pmod{203} \end{cases}$$

(**Attenzione!** *In questo esercizio è* obbligatorio *usare il metodo visto a lezione.*)

Esercizio 4.2. Si dica se i seguenti sistemi di congruenze sono risolubili, spiegando perché. Qualora un sistema abbia soluzione, *le si trovino tutte*, giustificando la risposta.

$$\begin{cases} x \equiv 2 & \pmod{187} \\ x \equiv 24 & \pmod{253} \end{cases} \qquad \begin{cases} x \equiv 11 & \pmod{187} \\ x \equiv 35 & \pmod{253} \end{cases}$$

(**Attenzione!** *In questo esercizio è* obbligatorio *usare il metodo visto a lezione.*)

Esercizio 4.3. Si dica se i seguenti sistemi di congruenze sono risolubili, spiegando perché. Qualora un sistema abbia soluzione, *le si trovino tutte*, giustificando la risposta.

$$\begin{cases} x \equiv 2 & \pmod{143} \\ x \equiv 27 & \pmod{221} \end{cases} \qquad \begin{cases} x \equiv 10 & \pmod{143} \\ x \equiv 49 & \pmod{221} \end{cases}$$

(**Attenzione!** *In questo esercizio è* obbligatorio *usare il metodo visto a lezione.*)

Esercizio 4.4. Si dica se i seguenti sistemi di congruenze sono risolubili, spiegando perché. Qualora un sistema abbia soluzione, *le si trovino tutte*, giustificando la risposta.

$$\begin{cases} x \equiv 2 & \pmod{221} \\ x \equiv 36 & \pmod{187} \end{cases} \qquad \begin{cases} x \equiv 20 & \pmod{221} \\ x \equiv 50 & \pmod{187} \end{cases}$$

(**Attenzione!** *In questo esercizio è* obbligatorio *usare il metodo visto a lezione.*)

Esercizio 5.1. Si enunci il criterio di divisibilità per 7, dandone un cenno di dimostrazione.

Si consideri il numero decimale $a = 14376x$, ove x è una cifra decimale incognita. Si trovi x, se esiste, in modo che a sia divisibile per $2, 3, 4, 7, 9, 11$. (Intendo per uno alla volta, non necessariamente per tutti contemporaneamente.)

Esercizio 5.2. Si enunci il criterio di divisibilità per 7, dandone un cenno di dimostrazione.

Si consideri il numero decimale $a = 15476x$, ove x è una cifra decimale incognita. Si trovi x, se esiste, in modo che a sia divisibile per $2, 3, 4, 7, 9, 11$. (Intendo per uno alla volta, non necessariamente per tutti contemporaneamente.)

Esercizio 5.3. Si enunci il criterio di divisibilità per 7, dandone un cenno di dimostrazione.

Si consideri il numero decimale $a = 13276x$, ove x è una cifra decimale incognita. Si trovi x, se esiste, in modo che a sia divisibile per $2, 3, 4, 7, 9, 11$. (Intendo per uno alla volta, non necessariamente per tutti contemporaneamente.)

Esercizio 5.4. Si enunci il criterio di divisibilità per 7, dandone un cenno di dimostrazione.

Si consideri il numero decimale $a = 16576x$, ove x è una cifra decimale incognita. Si trovi x, se esiste, in modo che a sia divisibile per $2, 3, 4, 7, 9, 11$. (Intendo per uno alla volta, non necessariamente per tutti contemporaneamente.)

Esercizio 6.1. Sia A un anello commutativo (dunque $ab = ba$ per ogni $a, b \in A$) con unità.

Si mostri che un elemento di A non può essere contemporaneamente invertibile, e anche un divisore dello zero.

Esercizio 6.2. Sia $A \neq \{ 0 \}$ un anello commutativo con unità.

Si mostri che sono equivalenti:

(1) A è un dominio, ovvero in A vale la *legge di annullamento del prodotto*, ovvero se $a, b \in A$, e $ab = 0$, allora o $a = 0$, o $b = 0$, e
(2) l'unico 0-divisore in A è 0.

Esercizio 6.3. Sia A un anello commutativo (dunque $ab = ba$ per ogni $a, b \in A$) con unità.

Si mostri che un elemento di A non può essere contemporaneamente invertibile, e anche un divisore dello zero.

Esercizio 6.4. Sia $A \neq \{ 0 \}$ un anello commutativo con unità.

Si mostri che sono equivalenti:

(1) A è un dominio, ovvero in A vale la *legge di annullamento del prodotto*, ovvero se $a, b \in A$, e $ab = 0$, allora o $a = 0$, o $b = 0$, e
(2) l'unico 0-divisore in A è 0.

Esercizio 7.1.

(1) *Si enunci* il Primo Teorema di Isomorfismo per gli Anelli, nella prima forma.

(2) Si enunci il Teorema Cinese dei Resti, come isomorfismo fra due anelli.
(3) Si utilizzi il Primo Teorema di Isomorfismo per gli Anelli per *dimostrare* il Teorema Cinese. (Non c'è bisogno di dimostrare che il prodotto diretto di anelli è un anello.)
(4) Usando il Teorema Cinese, si mostri che

$$\text{se } \gcd(m, n) = 1, \text{ allora } \varphi(mn) = \varphi(m)\varphi(n).$$

(Qui φ è la funzione di Eulero.)

Esercizio 7.2.

(1) *Si enunci* il Primo Teorema di Isomorfismo per gli Anelli, nella prima forma.
(2) Si enunci il Teorema Cinese dei Resti, come isomorfismo fra due anelli.
(3) Si utilizzi il Primo Teorema di Isomorfismo per gli Anelli per *dimostrare* il Teorema Cinese. (Non c'è bisogno di dimostrare che il prodotto diretto di anelli è un anello.)
(4) Usando il Teorema Cinese, si mostri che

$$\text{se } \gcd(m, n) = 1, \text{ allora } \varphi(mn) = \varphi(m)\varphi(n).$$

(Qui φ è la funzione di Eulero.)

Esercizio 7.3.

(1) *Si enunci* il Primo Teorema di Isomorfismo per gli Anelli, nella prima forma.
(2) Si enunci il Teorema Cinese dei Resti, come isomorfismo fra due anelli.
(3) Si utilizzi il Primo Teorema di Isomorfismo per gli Anelli per *dimostrare* il Teorema Cinese. (Non c'è bisogno di dimostrare che il prodotto diretto di anelli è un anello.)
(4) Usando il Teorema Cinese, si mostri che

$$\text{se } \gcd(m, n) = 1, \text{ allora } \varphi(mn) = \varphi(m)\varphi(n).$$

(Qui φ è la funzione di Eulero.)

Esercizio 7.4.

(1) *Si enunci* il Primo Teorema di Isomorfismo per gli Anelli, nella prima forma.
(2) Si enunci il Teorema Cinese dei Resti, come isomorfismo fra due anelli.
(3) Si utilizzi il Primo Teorema di Isomorfismo per gli Anelli per *dimostrare* il Teorema Cinese. (Non c'è bisogno di dimostrare che il prodotto diretto di anelli è un anello.)
(4) Usando il Teorema Cinese, si mostri che

$$\text{se } \gcd(m, n) = 1, \text{ allora } \varphi(mn) = \varphi(m)\varphi(n).$$

(Qui φ è la funzione di Eulero.)