TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 3

Esercizio 3.1. Sia $n \geq 2$ un intero. Si mostri che

- se n è primo, allora $\mathbf{Z}/n\mathbf{Z}$ è un campo,
- se n non è primo, allora $\mathbf{Z}/n\mathbf{Z}$ non è un dominio.

Esercizio 3.2. Si consideri $n = 12827$, e le classi $[a] = [4064], [4085] \in \mathbf{Z}/n\mathbf{Z}$. Per ognuna di esse, si dica se è invertibile (esibendo in tal caso come "prova" l'inverso) o se è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Esercizio 3.3. Si trovino gli inversi di tutti gli elementi diversi da zero di $\mathbf{Z}/19\mathbf{Z}$.

Esercizio 3.4. Si dica quali elementi di $\mathbf{Z}/35\mathbf{Z}$ sono invertibili e quali sono divisori dello zero, indicando per ognuno una "prova", nel senso dell'Esercizio 3.2.

Esercizio 3.5 (Facoltativissimo). Si trovi un anello con unità A e un elemento $a \in A$ tale che esistano $b, c \in A$, con $b \neq 0$, tali che $ba = 0$ e $ca = 1$.
(SUGGERIMENTO: Si può considerare uno spazio vettoriale V su $\mathbf{Q}$ che abbia una base numerabile $v_0, v_1, v_2, \ldots$. Sia A l'anello delle funzioni lineari $V \to V$. Consideriamo $a \in A$ che manda $v_i \mapsto v_{i+1}$.)

Esercizio 3.6. Sia A un anello commutativo con unità. Si mostri che un elemento di A non può essere contemporaneamente invertibile e un divisore dello zero
C'è una contraddizione fra questo esercizio e l'Esercizio 3.5?

Esercizio 3.7. 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 3.8. Enunciate a dimostrate il Lemma dei Cassetti.

Esercizio 3.9. Si mostri che la funzione $f : \mathbf{N} \to \mathbf{N}$ data da $x \mapsto x + 1$ è iniettiva, ma non suriettiva, e la funzione $g : \mathbf{N} \to \mathbf{N}$ data da

$$f(x) = \begin{cases} x - 1 & \text{se } x > 0, \\ 15 & \text{se } x = 0 \end{cases}$$

è suriettiva ma non iniettiva. Si calcolino le composizioni $g \circ f$ e $g \circ f$.

Esercizio 3.10 (Del tutto facoltativo). Sia A un anello finito, non necessariamente commutativo. Supponiamo che in A ci sia un elemento a che non è uno 0-divisore, nel senso che per ogni $b \in A$ si ha che da $ab = 0$ segue $b = 0$ e da $ba = 0$ segue $b = 0$.

(1) Si mostri che le funzioni $A \to A$ definite da $x \mapsto ax$ e $y \mapsto ya$ sono iniettive e dunque suriettive. Dunque ogni elemento b di A si scrive nella forma $b = ax$ e anche nella forma $b = ya$, per opportuni $x, y \in A$.

(2) Si mostri che esistono elementi $e, f \in A$ tali che $ae = a = fa$.
(3) Si mostri che $be = b = fb$ per ogni $b \in A$.
(4) Si mostri che $e = f$, e che questo è l'elemento neutro 1 per il prodotto.
(5) Si mostri che esistono $b, c \in A$ tali che $ba = 1 = ac$.
(6) Si mostri che $b = c$, e che questo elemento è l'inverso di a.
(7) Si mostri che gli elementi di A che non sono 0-divisori (nel senso detto più sopra) sono invertibili.

Esercizio 3.11. Si mostri che se A è un anello commutativo con unità, e A è finito, allora un elemento di A o è invertibile, o è uno 0-divisore.

Esercizio 3.12.

(1) Si mostri che un campo è sempre un dominio.
(2) Si mostri che $\mathbf{Z}$ è un dominio che non è un campo.
(3) Si mostri che un dominio finito è un campo.

Esercizio 3.13. Dimostrate che se ho una soluzione particolare x_0 di un sistema di congruenze

$$\begin{cases} x \equiv a & (\text{mod } m) \\ x \equiv b & (\text{mod } n), \end{cases}$$

allora le soluzioni del sistema sono tutti gli x tali che

$$x \equiv x_0 \pmod{\operatorname{lcm}(m, n)}.$$

In altre parole, due congruenze (se hanno soluzione) equivalgono a una.

Esercizio 3.14. Sia n un numero intero positivo, che conoscete. Sapete anche che n è il prodotto di due numeri primi distinti p, q, che però non conoscete.

- Mostrate che se qualcuno vi dice p, q, allora siete in grado di calcolare $\varphi(n)$.
- Mostrate che se qualcuno vi dice $\varphi(n)$, allora siete in grado di calcolare p, q, al solo prezzo di risolvere un'equazione di secondo grado.

Esercizio 3.15. Mostrate che se p è un numero primo, e $e > 0$, allora

$$\varphi(p^e) = (p-1)p^{e-1}.$$

Esercizio 3.16. Si enunci e si dimostri il criterio perché esista una soluzione del sistema di congruenze

$$\begin{cases} x \equiv a & (\text{mod } m) \\ x \equiv b & (\text{mod } n). \end{cases}$$

Esercizio 3.17. Si dica se i seguenti sistemi di congruenze sono risolubili, e in caso affermativo se ne trovino *tutte* le soluzioni.

$$\begin{cases} x \equiv 17 & (\text{mod } 89) \\ x \equiv 28 & (\text{mod } 55) \end{cases} \quad \begin{cases} x \equiv 17 & (\text{mod } 6766) \\ x \equiv 28 & (\text{mod } 1094) \end{cases} \quad \begin{cases} x \equiv 18 & (\text{mod } 6766) \\ x \equiv 28 & (\text{mod } 1094) \end{cases}$$

Esercizio 3.18. Si trovi un numero che

- diviso per 3 dia resto 1;
- diviso per 5 dia resto 2;

- diviso per 7 dia resto 3;
- diviso per 11 dia resto 4;

(SUGGERIMENTO: Traducete ogni condizione in una congruenza. Poi magari considerate l'Esercizio 3.13.)