

TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 5

Esercizio 5.1. 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 5.2. 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

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

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

Esercizio 5.3. Si dica se i seguenti sistemi di congruenze sono risolvibili, 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 5.4. Siano m, n interi positivi, con $\text{gcd}(m, n) = 1$. Si mostri che la funzione

$$f : \mathbf{Z}/mn\mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ [x]_{mn} \mapsto ([x]_m, [x]_n)$$

è ben definita, ed è una biiezione.

Esercizio 5.5. Siano $x, m, n \in \mathbf{Z}$, con $\text{gcd}(m, n) = 1$. Si mostri che sono equivalenti

- (1) $\text{gcd}(x, mn) = 1$, e
- (2) $\text{gcd}(x, m) = 1$ e $\text{gcd}(x, n) = 1$.

Esercizio 5.6. Si mostri che la funzione di Eulero è moltiplicativa nel senso della teoria dei numeri, cioè che vale

$$(1) \quad \varphi(mn) = \varphi(m)\varphi(n)$$

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

Si mostri con un esempio che (1) non vale in generale se $\text{gcd}(m, n) > 1$.

La parte facoltativa dell'esercizio è stata spostata nell'Esercizio 6.8

Esercizio 5.7. Siano $(G, \cdot, 1)$ e $(H, \cdot, 1)$ gruppi, $f : G \rightarrow H$ una funzione.

- (1) Si dica quando f è un morfismo, e quando un isomorfismo.
- (2) Si mostri che se f è un morfismo, allora $f(1) = 1$.
- (3) Si mostri che se f è un morfismo, allora $f(a^{-1}) = f(a)^{-1}$ per $a \in G$.

Esercizio 5.8.

(1) Sia (H, \circ, f) un gruppo, e G un insieme.

Sia $\varphi : G \rightarrow H$ una biiezione.

Si mostri che con l'operazione

$$x * y = \varphi^{-1}(\varphi(x) \circ \varphi(y))$$

G diventa un gruppo, con elemento neutro $e = \varphi^{-1}(f)$.

Questo fatto si chiama *trasporto di struttura*, nel senso che sto definendo un'operazione su G in termini di un'operazione su H , cioè sto *trasportando* la struttura di gruppo da H a G , tant'è che alla fine φ diventa un isomorfismo. È alla base di esercizi tipo il seguente.

(2) Si mostri che

$$(\mathbf{Z}, *, 1)$$

è un gruppo, ove per $x, y \in \mathbf{Z}$

$$x * y = x + y - 1.$$

Esercizio 5.9. Siano A, B insiemi *finiti*. Sia B^A l'insieme delle funzioni da A a B . Si mostri che

$$|B^A| = |B|^{|A|},$$

ove conviene convenire che ai fini della formula sia $0^0 = 1$.