Algebra 1

Prima prova parziale

Esercizio 1. Calcolare le ultime tre cifre del numero 14^{301}.

Risoluzione:
Bisogna determinare l'unico intere $0 \leq x < 1000$ tale che

$$x \equiv 14^{301} \mod 1000.$$

Possiamo usare il Teorema cinese del resto. Scriviamo $1000 = 2^3 \times 5^3 = 8 \times 125$ e dunque dobbiamo trovare l'unica soluzione $0 \leq x < 1000$ del sistema

$$\begin{cases} x \equiv 14^{301} \mod 8 \\ x \equiv 14^{301} \mod 125 \end{cases}$$

La prima equazione ci dice che $x \equiv 0 \mod 8$ dunque $x = 8y$. La seconda diventa dunque

$$8y \equiv 14^{301} \mod 125.$$

Ora $\phi(125) = 5^3 - 5^2 = 100$. Dunque $301 = 3\phi(125) + 1$. Per il teorema di Eulero Fermat si ha che la nostra equazione diventa

$$4y \equiv 7 \mod 125.$$

Ora $31 \times 4 = 125 - 1$ Dunque $y \equiv -7 \times 31 = -217 \equiv 33 \mod 125$ e

$$x = 33 \times 8 = 264$$

Esercizio 2. Risolvere il sistema di congruenze

$$\begin{cases} 8x \equiv 16 & \mod 28 \\ 7x \equiv 4 & \mod 11 \\ 227x \equiv 7 & \mod 15 \end{cases}$$

Risoluzione: Dato che $28, 11, 15$ sono a due a due coprimi possiamo applicare il Teorema cinese del resto. Ora con semplici manipolazioni vediamo che il nostro sistema è equivalente al sistema

$$\begin{cases} x \equiv 2 & \mod 7 \\ x \equiv -1 & \mod 11 \\ x \equiv 1 & \mod 5 \\ x \equiv -1 & \mod 3 \end{cases}$$

Consideriamo i due sistemi

$$\begin{cases} x \equiv -1 & \mod 11 \\ x \equiv -1 & \mod 3 \end{cases} \qquad \begin{cases} x \equiv 2 & \mod 7 \\ x \equiv 1 & \mod 5 \end{cases}$$

Il primo ha soluzioni $x = -1 + 33y$. Il secondo ha soluzioni $x = 16 + 35t$.

Ma ora $17 = 33 \times 9 - 35 \times 8$ ovvero $16 + 35 \times 8 = -1 + 33 \times 9 = 296$ e

$$x = 296 + 1155k$$

Esercizio 3. Si consideri il gruppo

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Q}, ac = 1 \right\}$$

e il suo sottogruppo

$$U = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} | c \in \mathbb{Q}\}.$$

Si dimostri che

1. U è normale in B,
2. $U \simeq \mathbb{Q}$,
3. $B/U \simeq \mathbb{Q}^*$.

Risoluzione: 1) Prendiamo

$$g = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in B$$

e notiamo che

$$g^{-1} = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}$$

Allora

$$g \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & a^2 c \\ 0 & 1 \end{pmatrix} \in U$$

Dunque U è normale.

2) Definiamo $\psi : \mathbb{Q} \to U$ mediante

$$\psi(c) = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

ψ è ovviamente biunivoca e inoltre

$$\psi(c_1 + c_2) = \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix} = \psi(c_1)\psi(c_2).$$

Dunque ψ è un isomorfismo.

3) Definiamo $f : B \to \mathbb{Q}^*$ mediante

$$f\left(\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right) = a$$

f è suriettiva. Ora

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 a_2^{-1} \\ 0 & a_1^{-1} a_2^{-1} \end{pmatrix}$$

Da cui segue subito che f è un omomorfismo. Inoltre Ker$f = U$. Dal teorema di omomorfismo, $B/U \simeq \mathbb{Q}^*$.

Esercizio 4. Sia p un primo e G un p-sottogruppo di $GL(n, \mathbb{Z}_p)$. Dimostrare che esiste un vettore non nullo $v \in (\mathbb{Z}_p)^n$ tale che $Av = v$ per ogni $A \in G$.

Risoluzione: Essendo G un p gruppo, se consideriamo G come gruppo di trasformazioni lineari di $(\mathbb{Z}_p)^n$ e prendiamo l'insieme $Fix((\mathbb{Z}_p)^n)$ dei vettori fissati da G otteniamo che

$$|Fix((\mathbb{Z}_p)^n)| \equiv |(\mathbb{Z}_p)^n| = p^n \equiv 0 \mod p.$$

Ora $0 \in (\mathbb{Z}_p)^n$ è certamente fissato dunque $|Fix((\mathbb{Z}_p)^n)| > 0$ è un multiplo non nullo di p. C'è dunque un vettore non nullo $v \in (\mathbb{Z}_p)^n$ con $Av = v$ per ogni $\in G$.

Esercizio 5.

- Sia $\sigma = (1,8)(1,4,2,3)(1,8)(1,2,3)(5,7,4,6,8)(1,3,2) \in S_8$. Sia H il sottogruppo generato da σ. Determinare n in modo tale che esista un isomofismo $H \to \mathbb{Z}_n$ e scrivere esplicitamente un tale isomorfismo.
- Determinare le struttura cicliche delle permutazioni pari di ordine quattro in S_8.

Risoluzione: Per rispondere alla prima domanda bisogna calcolare l'ordine n di σ Ora

$$\sigma = (1,8)(1,4,2,3)(1,8)(1,2,3)(5,7,4,6,8)(1,3,2) = (8,4,2,3)(5,7,4,6,8) = (5,7,2,3,8)(4,6)$$

Dunque σ ha partizione $[5,2]$ e il suo ordine è $o(\sigma) = n = 10$.
Definiamo allora $\phi : H \to \mathbb{Z}/n$ mediante $\phi(\sigma^h) = [h]$.

Per rispondere al secondo quesito bisogna elencare le partizioni $[p_1 \geq p_2 \geq \cdots \geq p_s]$ con $p_1 = 4$, $p_i \in \{1,2,4\}$, un numero pari di $p_i > 1$ e $p_1 + p_2 + \cdots + p_s = 8$.

Esse sono $[4,4]$ e $[4,2,1,1]$.

Esercizio 6. Sia G in gruppo e $F : G \to G$ un omomorfismo di gruppi tale che $F \circ F = F$. Dimostrare che $G = Im(F) \cdot Ker(F)$ e che $Im(F) \cap Ker(F) = \{1\}$.

Risoluzione:

Sia $g \in G$. Consideriamo $h = g^{-1}F(g)$.

$$F(h) = F(g^{-1})F \circ F(g) = F(g)^{-1}F(g) = 1$$

Dunque $h \in KerF$ e $g = F(g)h^{-1} \in Im(F) \cdot Ker(F)$.

Sia ora $g \in Im(F) \cap Ker(F)$. Per ipotesi esiste h con $g = F(h)$ e $F(g) = 1$. Allora

$$1 = F(g) = F \circ F(h) = F(h) = g$$

e $g = 1$.