Università degli Studi Roma Tre
Anno Accademico 2008/2009
AL1 - Algebra 1
Correzione della seconda prova in itinere

Esercizio 1. Dobbiamo determinare quali numeri complessi $\rho e^{i\theta}$ sono soluzioni dell'equazione assegnata. Quindi: $(\rho e^{i\theta})^6 = 3 \Leftrightarrow \rho^6 e^{6i\theta} = 3$. Due numeri complessi scritti in forma polare sono uguali se hanno lo stesso modulo e se gli argomenti differiscono per multipli di 2π. Perciò $\rho = \sqrt[6]{3}$ e $6\theta = 2k\pi \Leftrightarrow \theta = \frac{k\pi}{3}$. Si avranno soluzioni distinte per $k = 0, 1, 2, 3, 4, 5$. Esplicitando i calcoli, le soluzioni complesse z_k per $0 \leq k \leq 5$ sono:

$z_0 = \sqrt[6]{3}$,

$z_1 = \sqrt[6]{3} e^{i\frac{\pi}{3}} = \sqrt[6]{3}\left(\cos\frac{\pi}{3} + i \sin\frac{\pi}{3}\right) = \sqrt[6]{3}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$,

$z_2 = \sqrt[6]{3} e^{i\frac{2\pi}{3}} = \sqrt[6]{3}\left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right) = \sqrt[6]{3}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$,

$z_3 = \sqrt[6]{3} e^{i\pi} = -\sqrt[6]{3}$,

$z_4 = \sqrt[6]{3} e^{i\frac{4\pi}{3}} = \sqrt[6]{3}\left(\cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3}\right) = \sqrt[6]{3}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)$,

$z_5 = \sqrt[6]{3} e^{i\frac{5\pi}{3}} = \sqrt[6]{3}\left(\cos\frac{5\pi}{3} + i \sin\frac{5\pi}{3}\right) = \sqrt[6]{3}\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)$.

Le soluzioni reali dell'equazione sono solo z_0 e z_3, dato che le altre z_i hanno parte immaginaria non nulla.

Esercizio 2. Per il teorema cinese del resto, essendo 5 e 7 coprimi, il sistema è certamente risolubile (e ha un'unica soluzione modulo $5 \cdot 7 = 35$).

Risolviamolo per sostituzione. Dalla prima congruenza otteniamo $X = 3 + 5h$, al variare di $h \in \mathbb{Z}$. Sostituendo tali valori nella seconda congruenza otteniamo: $3 + 5h \equiv 2 \mod 7 \Leftrightarrow 5h \equiv 6 \mod 7 \Leftrightarrow h \equiv 4 \mod 7$, quindi h deve essere del tipo $4 + 7k$ al variare di k in $\mathbb{Z}$. Perciò $X = 3 + 5(4 + 7k) = 23 + 35k$ al variare di k in $\mathbb{Z}$. Le soluzioni nell'intervallo $[10, 100]$ si ottengono per $k = 0, 1, 2$ e sono, rispettivamente, $23, 58, 93$.

Esercizio 3. Base dell'induzione: per $n = 2$ $F_2 = 2 = \frac{32}{16} > \left(\frac{5}{4}\right)^2 = \frac{25}{16}$, quindi in questo caso la disuguaglianza è verificata.

Supponiamo allora che la disuguaglianza sia verificata per ogni k con $2 \leq k \leq n$ e dimostriamola per $n + 1$: $F_{n+1} = F_n + F_{n-1} > \left(\frac{5}{4}\right)^n + \left(\frac{5}{4}\right)^{n-1} = \left(\frac{5}{4}\right)^{n-1}\left(\frac{5}{4} + 1\right) = \left(\frac{5}{4}\right)^{n-1}\left(\frac{36}{16}\right) > \left(\frac{5}{4}\right)^{n-1}\left(\frac{25}{16}\right) = \left(\frac{5}{4}\right)^{n-1}\left(\frac{5}{4}\right)^2 = \left(\frac{5}{4}\right)^{n+1}$.

Esercizio 4. Applicando l'algoritmo euclideo delle divisioni successive otteniamo:

$105 = 39 \cdot 2 + 27$
$39 = 27 \cdot 1 + 12$
$27 = 12 \cdot 2 + 3$
$12 = 3 \cdot 4 + 0$

Essendo 3 l'ultimo resto non nullo si ha che $MCD(105, 39) = 3$.

La relativa identità di Bézout è: $3 = 3 \cdot 105 - 8 \cdot 39$.

Esercizio 5. Si consulti il libro di testo.

Esercizio 6. Per la definizione di campo si consulti il libro di testo.

Per dimostrare che $A := \mathbb{Z}/6\mathbb{Z}$ non è un campo basta produrre un esempio di un elemento $a \in A$ non nullo e non invertibile. Sia, ad esempio, $a := [3]_6$. Chiaramente $a \neq [0]_6$. Inoltre se a fosse invertibile allora esisterebbe $b := [x]_6$, con $x \in \mathbb{Z}$ tale che $ab = [1]_6$, i.e. $3x \equiv 1 \mod 6$ da cui $\exists h \in \mathbb{Z}$ t.c. $1 = 3x + 6h$: assurdo, dato che $MCD(3, 6) = 3$.

Esercizio 7. $\sigma = (1\ 2\ 5\ 7\ 3)$, $\tau = (1\ 3\ 4)(5\ 7)$.

Ricordiamo che una permutazione si dice pari se è possibile scriverla come prodotto di un numero pari di trasposizioni, dispari altrimenti. Tale definizione, come visto a lezione, è ben posta. $\sigma = (1\ 3)(1\ 7)(1\ 5)(1\ 2)$, quindi σ è una permutazione pari; $\tau = (1\ 4)(1\ 3)(5\ 7)$, quindi τ è una permutazione dispari.

$\sigma^2\tau = (1\ 2\ 7\ 3\ 4\ 5)$, $\tau^5 = (1\ 3\ 4)^5(5\ 7)^5$ (cicli disgiunti commutano) $= (1\ 4\ 3)(5\ 7)$, $\sigma^{-1} = (3\ 7\ 5\ 2\ 1) = (1\ 3\ 7\ 5\ 2)$.

Esercizio 8. Per la definizione di gruppo si consulti il libro di testo.

Un esempio di gruppo abeliano infinito è $(\mathbb{Z}, +)$. Un esempio di gruppo non abeliano finito è $(S_3, \circ)$, gruppo delle permutazioni su 3 elementi. $|S_3| = 3! = 6$ e inoltre S_3 non è commutativo: ad esempio $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$.

Esercizio 9. Per la definizione della funzione ϕ di Eulero si consulti il libro di testo.

Per calcolare il valore di $\phi(60000)$ useremo le seguenti due proprietà di ϕ:

* se $a, b \in \mathbb{N}_+$ sono coprimi (i.e. $MCD(a, b) = 1$) allora $\phi(ab) = \phi(a)\phi(b)$,

** se p è un numero primo e $\alpha \in \mathbb{N}_+$ allora $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

$60000 = 2^5 \cdot 3 \cdot 5^4$, perciò: $\phi(2^5 \cdot 3 \cdot 5^4) =^* \phi(2^5 \cdot 3)\phi(5^4) =^* \phi(2^5)\phi(3)\phi(5^4) =^{**} (2^5 - 2^4)(3 - 1)(5^4 - 5^3) = 16 \cdot 2 \cdot 500 = 16000$.